eHerkenning

Inhoudsopgave

1. Afsprakenstelsel eHerkenning . . . 6
1.1 Algemeen . . . 8
1.1.1 Algemene introductie . . . 9
1.1.1.1 Historie en status van eHerkenning . . . 11
1.1.1.1.1 Versie 1.1 . . . 11
1.1.1.1.2 Versie 1.2 . . . 11
1.1.1.1.3 Versie 1.3 . . . 12
1.1.1.1.4 Versie 1.4 . . . 12
1.1.1.1.5 Versie 1.5 . . . 12
1.1.1.1.6 Versie 1.6 . . . 12
1.1.1.1.7 Versie 1.7 . . . 12
1.1.1.1.8 Versie 1.8 . . . 13
1.1.1.2 Wat is eHerkenning? . . . 13
1.1.1.2.1 Gedrag netwerk eHerkenning op hoofdlijnen . . . 13
1.1.1.2.2 Kernbegrippen van eHerkenning . . . 14
1.1.1.2.3 Afsprakenstelsel eHerkenning en ontwerpprincipes . . . 15
1.1.1.3 Hoe werkt eHerkenning? . . . 16
1.1.1.3.1 Werking van netwerk eHerkenning op hoofdlijnen . . . 17
1.1.1.3.2 Deelnemers: rollen en verantwoordelijkheden . . . 18
1.1.1.3.3 Mogelijke vervulling van rollen door deelnemers . . . 20
1.1.1.4 Werking aanvullende features . . . 21
1.1.1.4.1 Werking attribuutverstrekking . . . 21
1.1.1.4.2 Werking ketenmachtigingen . . . 22
1.1.1.4.3 Werking SSO . . . 22
1.1.1.5 Hoe aansluiten op eHerkenning? . . . 22
1.1.1.5.1 Aansluiten als dienstafnemer (bedrijf) . . . 23
1.1.1.5.2 Aansluiten als dienstverlener . . . 24
1.1.1.5.3 Aansluiten als deelnemer . . . 24
1.1.1.5.4 Aansluiten op attribuutverstrekking . . . 25
1.1.1.5.5 Aansluiten op ketenmachtigingen . . . 25
1.1.1.6 Bijlage – Overzicht gebruikte standaarden . . . 25
1.1.1.7 Bijlage – Toepassingen uitgangspunten en randvoorwaarden . . . 26
1.1.2 Begrippenlijst eHerkenning . . . 30
1.1.2.1 Aanvullende feature . . . 38
1.1.2.2 Afgeschermde kopie WID . . . 38
1.1.2.3 Afsprakenstelsel (AS) . . . 38
1.1.2.4 Akte . . . 39
1.1.2.5 Attribuutcatalogus (AC) . . . 39
1.1.2.6 Authenticatie (authenticeren) . . . 39
1.1.2.7 Authenticatiedienst (AD) . . . 39
1.1.2.8 Authenticatiemiddel . . . 39
1.1.2.9 Authenticatieverklaring . . . 39
1.1.2.10 Autorisatie . . . 40
1.1.2.11 Bedrijf . . . 40
1.1.2.12 Beheerder . . . 40
1.1.2.13 Beheerorganisatie (BO) . . . 41
1.1.2.14 Beroepsbeoefenaar . . . 41
1.1.2.15 Betrouwbaarheidsniveau . . . 41
1.1.2.16 Bevoegdheid . . . 41
1.1.2.17 BSN . . . 41
1.1.2.18 Certificatie (certificeren) . . . 41
1.1.2.19 Controle van bevoegdheid . . . 42
1.1.2.20 Dataminimalisatie . . . 42
1.1.2.21 Deelnemer . . . 42
1.1.2.22 Dienstafnemer . . . 42
1.1.2.23 Dienstencatalogus (DC) . . . 43
1.1.2.24 Dienstverlener (DV) . . . 43
1.1.2.25 eHerkenning (eH) . . . 43
1.1.2.26 eHerkenningsdiensten . . . 43
1.1.2.27 eHerkenningsmakelaar (HM) . . . 43
1.1.2.28 eHerkenningsnetwerk . . . 44
1.1.2.29 Gebruiker . . . 44
1.1.2.30 Geïnformeerde uitdrukkelijke toestemming . . . 44
1.1.2.31 Gemachtigde . . . 44
1.1.2.32 Handelsregister . . . 44
1.1.2.33 Hergebruik . . . 45
1.1.2.34 Herkenning . . . 45
1.1.2.35 Identificatie (identificeren) . . . 45
1.1.2.36 Identificerend kenmerk . . . 45

1.1.2.37 Identificerend nummer . . . 45
1.1.2.38 Identiteit . . . 46
1.1.2.39 Identity provider (SAML) . . . 46
1.1.2.40 Intermediaire partij . . . 46
1.1.2.41 Intern pseudoniem . . . 46
1.1.2.42 Ketenverklaring . . . 46
1.1.2.43 Klachten- en geschillen-commissie . . . 46
1.1.2.44 Koppelvlak . . . 47
1.1.2.45 Machtiging (machtigen) . . . 47
1.1.2.46 Machtigingenregister (MR) . . . 47
1.1.2.47 Machtiging-verklaring . . . 47
1.1.2.48 Middelenuitgever (MU) . . . 47
1.1.2.49 Natuurlijk persoon . . . 48
1.1.2.50 Netwerk (voor eHerkenning) . . . 48
1.1.2.51 Niet natuurlijk persoon . . . 48
1.1.2.52 Onderneming . . . 48
1.1.2.53 Ondertekendienst . . . 48
1.1.2.54 Overheidsdienstverlener . . . 49
1.1.2.55 Partij . . . 49
1.1.2.56 PKI (Public Key Infrastructure) . . . 49
1.1.2.57 Privépersoon . . . 49
1.1.2.58 Pseudoniem . . . 49
1.1.2.59 Rechtspersoon . . . 50
1.1.2.60 Rol . . . 50
1.1.2.61 Service provider (SP) . . . 50
1.1.2.62 Single Sign On (SSO) . . . 50
1.1.2.63 Specifiek pseudoniem . . . 50
1.1.2.64 Stelselraad eHerkenning . . . 51
1.1.2.65 Tactisch overleg . . . 51
1.1.2.66 Toegang verlenen . . . 51
1.1.2.67 Uitvoerend natuurlijk persoon (UNP) . . . 51
1.1.2.68 User consent . . . 51
1.1.2.69 Verklaring . . . 52
1.1.2.70 Vertegenwoordigde . . . 52
1.1.2.71 Vertegenwoordigde dienstafnemer . . . 52
1.1.2.72 Vertegenwoordiger . . . 52
1.1.2.73 Vertegenwoordiging (vertegenwoordigen) . . . 52
1.1.2.74 Vestiging . . . 53
1.1.2.75 Wettelijke vertegenwoordiging . . . 53
1.1.2.76 WID document . . . 53
1.1.2.77 Wilsuiting . . . 53
1.1.2.78 Zelfstandige Zonder Personeel (ZZP) . . . 53
1.2 Juridica . . . 54
1.2.1 Juridisch kader . . . 55
1.2.1.1 Organen en taakverdeling . . . 57
1.2.1.1.1 Stelselraad eHerkenning (gremium) . . . 59
1.2.1.1.2 Tactisch Overleg (gremium) . . . 59
1.2.1.1.3 Operationeel Overleg (gremium) . . . 60
1.2.1.1.4 Klachten- en geschillencommissie . . . 60
1.2.1.1.5 Bekostiging . . . 60
1.2.1.2 Nalevingsbeleid . . . 60
1.2.1.2.1 Besluit inzake sancties . . . 62
1.2.1.2.2 Opleggen van sancties . . . 63
1.2.1.2.3 Sancties . . . 63
1.2.1.2.4 Schorsing . . . 63
1.2.1.2.5 Beëindiging van de Deelnemersovereenkomst . . . 63
1.2.1.2.6 Spoedprocedure . . . 64
1.2.1.2.7 Sancties tegen de beheerorganisatie of EZ . . . 64
1.2.1.2.8 Compensatieregeling . . . 64
1.2.1.2.9 Uitgangspunten compensatieregeling . . . 65
1.2.1.3 Toetredingseisen . . . 67
1.2.1.4 Juridische structuur afsprakenstelsel eHerkenning . . . 68
1.2.1.5 Aanvullende verplichtingen . . . 68
1.2.1.6 Vertegenwoordiging, volmacht en machtiging . . . 69
1.2.1.6.1 Privaatrechtelijke vertegenwoordiging . . . 70
1.2.1.6.2 Publiekrechtelijke vertegenwoordiging . . . 70
1.2.1.6.3 Ketenmachtiging . . . 70
1.2.1.7 Aansprakelijkheid . . . 71
1.2.1.8 Betrouwbaarheidsniveaus . . . 71
1.2.1.9 Rol van eHerkenningsmakelaars . . . 72
1.2.2 Gebruiksvoorwaarden eHerkenning . . . 72
1.2.2.1 Artikel 1. Definities . . . 73
1.2.2.2 Artikel 2. Toepassingsgebied . . . 74
1.2.2.3 Artikel 3. Tussentijdse beëindiging van de Overeenkomst door beëindiging deelname . . . 75
1.2.2.4 Artikel 4. Beperking van aansprakelijkheid . . . 75
1.2.2.5 Artikel 5. Geheimhouding . . . 75
1.2.2.6 Artikel 6. Achterhalen netwerkfalen . . . 75

1.2.2.7 Artikel 7. Overdraagbaarheid rechten en verplichtingen Overeenkomst . . . 75
1.2.2.8 Artikel 8. Toepasselijk recht . . . 76
1.2.2.9 Artikel 9. Geschillen . . . 76
1.2.2.10 Artikel 10. Dienstafnemer . . . 76
1.2.2.11 Artikel 11. Beveiligingsverplichting van de Dienstafnemer . . . 76
1.2.2.12 Artikel 12. Toezicht van de Dienstafnemer op gedragingen van personen . . . 76
1.2.2.13 Artikel 13. Vervulling rol(len) door de Dienstafnemer . . . 77
1.2.2.14 Artikel 14. Vaststellen openstellingsbesluit . . . 77
1.2.2.15 Artikel 15. Melding onregelmatigheden . . . 77
1.2.2.16 Artikel 16. Beveiliging . . . 77
1.2.2.17 Artikel 17. SSO . . . 77
1.2.2.18 Artikel 18. Beveiliging . . . 78
1.2.2.19 Artikel 19. Betrouwbaarheidsniveaus . . . 78
1.2.2.20 Artikel 20. Informatieverplichting . . . 78
1.2.2.21 Artikel 21. Privacy . . . 78
1.2.2.22 Artikel 22. Cookies . . . 78
1.2.2.23 Artikel 23. Verplichtingen van de Herkenningsmakelaar . . . 78
1.2.2.24 Artikel 24. Verplichtingen van de Authenticatiedienst . . . 79
1.2.2.25 Artikel 25. Verplichtingen van de Middelenuitgever . . . 79
1.2.2.26 Artikel 26. Verplichtingen van het Machtigingenregister . . . 79
1.2.2.27 Artikel 27. Verplichtingen van de Ondertekendienst . . . 80
1.3 Organisatie . . . 80
1.3.1 Operationeel handboek . . . 81
1.3.1.1 Helpdesk . . . 83
1.3.1.2 Proces aanpassen attribuutcatalogus . . . 84
1.3.1.3 Proces beheren simulator . . . 85
1.3.1.4 Proces beheren testnetwerk . . . 86
1.3.1.5 Proces certificaatwissel . . . 87
1.3.1.6 Proces change en release . . . 88
1.3.1.7 Proces contentmanagement . . . 93
1.3.1.8 Proces distributie en publicatie van documenten . . . 95
1.3.1.9 Proces doorvoeren nieuwe dienstencatalogus . . . 96
1.3.1.10 Proces en randvoorwaarden uitvoering penetratietesten . . . 98
1.3.1.11 Proces incidentmanagement . . . 98
1.3.1.12 Proces managementinformatie . . . 102
1.3.1.13 Proces meldingenbeheer . . . 103
1.3.1.14 Proces metadata . . . 105
1.3.1.15 Proces naleving . . . 107
1.3.1.16 Proces onderhoud cookieserver . . . 111
1.3.1.17 Proces toetreden . . . 111
1.3.1.18 Proces uittreden . . . 116
1.3.1.19 Proces wijziging rechtspersoon . . . 119
1.3.2 Businessmodel . . . 119
1.3.3 Handboek huisstijl . . . 120
1.3.3.1 Doel, kernboodschap en uitgangspunten . . . 121
1.3.3.2 Richtlijnen publiciteit . . . 122
1.3.3.3 Promokit . . . 123
1.3.3.4 Bijlage – Regels en richtlijnen van de visuele identiteit eHerkenning . . . 123
1.3.4 Service level . . . 124
1.3.4.1 Service level definities . . . 126
1.3.4.1.1 Calamiteit . . . 126
1.3.4.1.2 Gegarandeerde openstellingsduur . . . 126
1.3.4.1.3 Onderhoudswindow . . . 126
1.3.4.1.4 Rapportageperiode . . . 126
1.3.4.1.5 Verstoring . . . 126
1.3.4.1.6 Werkdag . . . 127
1.3.4.2 Beschrijving service level . . . 127
1.3.4.2.1 Communicatie over onderhoud . . . 127
1.3.4.2.2 Beschikbaarheid . . . 127
1.3.4.2.3 Performance . . . 127
1.3.4.2.4 Onderhoud . . . 127
1.3.4.2.5 Ondersteuning . . . 128
1.3.4.2.6 Logging . . . 128
1.3.4.2.7 Verplichtingen bij verstoringen . . . 128
1.3.4.2.8 Verplichtingen bij calamiteiten . . . 128
1.3.4.2.9 Rapportages . . . 128
1.3.4.2.10 Controle op service level . . . 129
1.4 Techniek en functionaliteit . . . 129
1.4.1 Use cases . . . 130
1.4.1.1 Use cases voor Gebruik . . . 132
1.4.1.1.1 GUC1 Gebruiken eHerkenning als dienstafnemer . . . 133
1.4.1.1.2 GUC2 Gebruiken eHerkenning als vertegenwoordiger . . . 134
1.4.1.1.3 GUC3 Aantonen identiteit . . . 135
1.4.1.1.4 GUC4 Aantonen bevoegdheid . . . 137
1.4.1.1.5 Aanvullende eisen eHerkenningsmakelaar . . . 141
1.4.1.1.6 Aanvullende eisen authenticatiedienst . . . 142
1.4.1.1.7 Aanvullende eisen authenticatiedienst die SSO ondersteunt . . . 142

1.4.1.1.8 Aanvullende eisen machtigingenregister . . . 142
1.4.1.1.9 Aanvullende eisen machtigingenregister dat ketenmachtigingen ondersteunt . . . 142
1.4.1.1.10 Use case overschrijdende alternatieve scenario's . . . 143
1.4.1.2 Use cases voor Administratie . . . 146
1.4.1.2.1 AUC1 Aansluiten dienst . . . 146
1.4.1.2.2 AUC2 Verkrijgen authenticatiemiddel . . . 147
1.4.1.2.3 AUC3 Registreren bevoegdheid . . . 147
1.4.1.2.4 AUC4 Registreren attribuut . . . 148
1.4.1.2.5 AUC5 Registreren identificerend kenmerk beroepsbeoefenaar . . . 148
1.4.1.3 Gebruikersinterface . . . 148
1.4.1.3.1 Dialoogbeschrijving . . . 148
1.4.1.3.2 Aanvullende eisen aan eHerkenningsmakelaarschermen . . . 149
1.4.1.3.3 Toegankelijkheid . . . 149
1.4.2 Interface specifications . . . 149
1.4.2.1 Interface specifications DV-HM 1.7 . . . 152
1.4.2.2 Interface specifications HM-AD 1.7 . . . 161
1.4.2.3 Interface specifications HM-MR 1.7 . . . 169
1.4.2.4 Interface specifications HM-MR 1.7 chain authorization . . . 178
1.4.2.5 General requirements . . . 179
1.4.2.6 Information security requirements . . . 180
1.4.2.6.1 Digital signature . . . 180
1.4.2.6.2 Encryption . . . 180
1.4.2.6.3 PKIoverheid . . . 181
1.4.2.6.4 Secure connection . . . 181
1.4.2.6.5 Synchronize system clocks . . . 181
1.4.2.7 Error handling . . . 181
1.4.2.8 Single sign-on and user sessions . . . 182
1.4.2.9 Attributes and elements . . . 183
1.4.2.9.1 EntityID . . . 184
1.4.2.9.2 Level of assurance . . . 185
1.4.2.9.3 OIN format . . . 185
1.4.2.9.4 Pseudonyms . . . 186
1.4.2.9.5 SAML attribute elements . . . 187
1.4.2.9.6 ServiceID . . . 189
1.4.2.9.7 XACML attribute elements . . . 189
1.4.2.10 SAML metadata . . . 192
1.4.2.11 Service catalog . . . 202
1.4.3 Attribuutverstrekking . . . 206
1.4.3.1 Identificerende kenmerken . . . 207
1.4.3.1.1 EntityConcernedID:KvKnr . . . 208
1.4.3.1.2 EntityConcernedID:Pseudo . . . 208
1.4.3.1.3 EntityConcernedID:RSIN . . . 209
1.4.3.1.4 EntityConcernedID:SubdossierNr . . . 209
1.4.3.1.5 EntityConcernedID:Vestigingsnr . . . 209
1.4.3.2 Attribuutcatalogus . . . 210
1.4.3.3 Attribuutcatalogus in XML formaat . . . 210
1.4.4 Testing . . . 216
1.4.4.1 Requirements for testing . . . 218
1.4.4.1.1 Acquire test means . . . 219
1.4.4.1.2 Announce chain test . . . 219
1.4.4.1.3 Exchange metadata . . . 219
1.4.4.1.4 Process service catalog . . . 219
1.4.4.2 Network monitoring . . . 220
1.4.4.3 Simulator test cases . . . 220
1.4.4.3.1 Generic simulator test cases . . . 220
1.4.4.3.2 Simulator test cases eHerkenningsmakelaar . . . 221
1.4.4.3.3 Simulator test cases Authenticatiedienst . . . 227
1.4.4.3.4 Simulator test cases Machtigingenregister . . . 230
1.4.4.4 Chain test cases . . . 232
1.4.4.4.1 Chain test cases eHerkenningsmakelaar . . . 232
1.4.4.4.2 Chain test cases Authenticatiedienst . . . 235
1.4.4.4.3 Chain test cases Machtigingenregister . . . 237
1.5 Beveiliging . . . 238
1.5.1 Betrouwbaarheidsniveaus en registratie-eisen . . . 239
1.5.1.1 Betrouwbaarheidsniveaus eHerkenning . . . 240
1.5.1.2 Betrouwbaarheidsniveaus van authenticatiemiddelen . . . 241
1.5.1.3 Intrekkingsverzoeken . . . 242
1.5.1.4 Betrouwbaarheidsniveaus van bevoegdheden . . . 242
1.5.1.4.1 Toepassing STORK raamwerk op bevoegdheden . . . 243
1.5.1.4.2 Het registratieproces van bevoegdheden . . . 244
1.5.1.4.3 De inhoud van een bevoegdheid . . . 245
1.5.1.4.4 Detailvereisten . . . 246
1.5.1.4.5 Vereisten betrouwbaarheidsaspect eerste registratie . . . 247
1.5.1.4.6 Vereisten betrouwbaarheidsaspect herhaalde registratie . . . 252
1.5.1.4.7 M - Synthese betrouwbaarheidsniveau van bevoegdheden . . . 254
1.5.1.4.8 Scoring . . . 254
1.5.1.5 Opbouw betrouwbaarheidsniveaus eHerkenning . . . 255

1.5.1.6 Toepassing betrouwbaarheidsniveaus op aanvullende features 255
1.5.1.6.1 Registratie-eisen attributen 255
1.5.1.6.2 Gebruikersgedefinieerde attributen 256
1.5.1.7 STORK niveaus 256
1.5.1.7.1 Betrouwbaarheidsniveau 1 257
1.5.1.7.2 Betrouwbaarheidsniveau 2 257
1.5.1.7.3 Betrouwbaarheidsniveau 3 258
1.5.1.7.4 Betrouwbaarheidsniveau 4 259
1.5.2 Informatiebeveiliging en privacy 260
1.5.2.1 Afspraken over verantwoordelijkheid en verantwoording 261
1.5.2.2 Maatregelen voor informatiebeveiliging 262
1.5.2.3 Beheer Stelselrisicoanalyse en Gemeenschappelijk Normenkader Informatiebeveiliging 263
1.5.2.4 Implementatie Gemeenschappelijk Normenkader Informatiebeveiliging en certificatie 264
1.5.2.5 Eisen ten aanzien van archivering en opvraging 264
1.5.2.6 Eisen aan de classificatie van informatie 266
1.5.2.7 Eisen aan screening van medewerkers 267
1.5.2.8 Beleid en doel penetratietesten 269
1.5.2.9 Bijlage - Toelichting ISO 27001 certificatie 269
1.5.3 Normenkader Stelselaudit 270
1.5.4 Stelsel risicoanalyse 271
1.5.4.1 Algemene risico's 273
1.5.4.2 Risico's van de Beheerorganisatie 277
1.5.4.3 Risico's van de Herkenningsmakelaar 278
1.5.4.4 Risico's voor de Authenticatiedienst 281
1.5.4.5 Risico's voor het Machtigingenregister 283
1.5.4.6 Risico's in de relatie DV-HM 285
1.5.4.7 Risico's in de relatie HM-AD 285
1.5.4.8 Risico's in de relatie HM-MR 286
1.5.5 Gemeenschappelijk normenkader informatiebeveiliging eHerkenning 286
1.6 Templates en formulieren 287
1.6.1 Checklist chain test 288
1.6.2 Checklist simulator test 290
1.6.3 Template deelnemersovereenkomst 296
1.6.4 Template incidentrapport 300
1.6.5 Template verzoek tot (uitbreiding) toetreding eHerkenning 302
1.6.6 Template vrijwaring penetratietest 305
1.6.7 Template wijziging rechtspersoon deelnemer 309
1.6.8 Template zelfverklaring 311

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Afsprakenstelsel eHerkenning

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Omwille van de leesbaarheid van de tekst is overal 'hij' geschreven waar 'hij of zij' bedoeld wordt.

De woorden "MOET", "MAG NIET", "ZOU MOETEN", "ZOU NIET MOETEN", en "MAG" in dit document moeten worden geïnterpreteerd gelijk aan hun Engelstalige equivalenten ("MUST", "MUST NOT / SHALL NOT", "SHOULD", "SHOULD NOT" en "MAY") als beschreven in RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt). Waar deze exacte termen bedoeld zijn worden ze in hoofdletters weergegeven. De betekenis van deze woorden is:

- MOET: een absolute vereiste
- MAG NIET: een absoluut verbod
- ZOU MOETEN: sterke wens, tenzij er valide reden is in specifiek geval af te wijken
- ZOU NIET MOETEN: ongewenst, tenzij er valide reden is om het in specifiek geval toe te laten
- MAG: een vrije keuze, een optie

Op deze pagina vindt u de meest actuele versie van het Afsprakenstelsel eHerkenning. Het afsprakenstelsel is een set van technische, functionele, juridische en organisatorische afspraken die gelden in het netwerk eHerkenning. Deze afspraken hebben als doel om samenwerking en zekerheid in het netwerk eHerkenning te garanderen. Tegelijkertijd bieden de afspraken ook voldoende vrijheid aan de aanbieders om competitieve proposities te leveren aan hun klanten.

Er zijn afspraken gemaakt over de naleving van het Afsprakenstelsel eHerkenning. Dit is van essentieel belang om de werking van het netwerk en het vertrouwen in het netwerk te waarborgen. De beheerorganisatie eHerkenning beheert het afsprakenstelsel en ziet toe op de naleving ervan. Deze onafhankelijke beheerorganisatie is door het Ministerie van Economische Zaken aangesteld.

Het Afsprakenstelsel eHerkenning wordt inhoudelijk compleet beschreven in onderstaande documenten:

Algemeen

Hier vindt u de algemene introductie op het Afsprakenstelsel eHerkenning. Dit document beschrijft de werking van eHerkenning en geeft tevens een overzicht van de andere onderdelen van het afsprakenstelsel.

- Algemene introductie — Dit document geeft op hoofdlijnen inzicht in het afsprakenstelsel en de werking van het netwerk.
- Begrippenlijst eHerkenning — Binnen eHerkenning wordt één begrippenlijst gehanteerd. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden. Datzelfde geldt ook andersom: waar in dit document de zelfstandige-naamwoords-vorm van een werkwoord wordt gehanteerd, heeft deze dezelfde betekenis als het gedefinieerde werkwoord.

Juridica

Hier vindt u de juridische documenten van het Afsprakenstelsel eHerkenning: het juridisch kader en de gebruiksvoorwaarden. Deze documenten bevatten informatie over de besturing van eHerkenning, de naleving van het afsprakenstelsel, de overeenkomst tussen de beheerorganisatie en de aanbieders en de minimale gebruiksvoorwaarden waaronder de dienstverleners en ondernemers eHerkenning mogen gebruiken.

- Juridisch kader — Beschrijft het juridisch kader, het besturingsmodel en de controle op en monitoring van de naleving van het afsprakenstelsel.
- Gebruiksvoorwaarden eHerkenning — Deze Gebruiksvoorwaarden zijn van toepassing op het verlenen van diensten door Deelnemers aan Dienstverleners en Dienstafnemers in het kader van het Netwerk voor eHerkenning.

Organisatie

Hier vindt u de organisatorische documenten van het Afsprakenstelsel eHerkenning: het operationele handboek, de service level, het businessmodel en het handboek huisstijl. Deze documenten bevatten informatie over de stelselbrede beheerprocessen, de algemene service level die eHerkenning hanteert en het gebruik van het beeldmerk eHerkenning bij externe communicatie.

- Operationeel handboek — Dit document beschrijft de operationele beheerprocessen voor het netwerk. Deze processen hebben als doel om het merk eHerkenning te beheren. Onder merkbeheer valt onder andere het beheren van de documentatie van het afsprakenstelsel, de relaties in het netwerk, het technische netwerk, digitale sleutels, toetreding en wensen of wijzigingen.
- Businessmodel — Dit document beschrijft het businessmodel voor eHerkenning. Onder het businessmodel worden verstaan de afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen die samen het netwerk voor eHerkenning invullen. Het is bedoeld voor deelnemers en dienstverleners.
- Handboek huisstijl — Dit document beschrijft de huisstijl afspraken en afspraken over marketingcommunicatie die deelnemers hebben gemaakt. Het is bedoeld voor deelnemers en dienstverleners.
- Service level — Dit document beschrijft de service level afspraken die deelnemers hebben gemaakt die beschrijven welk service level ten minste aan hun klanten wordt bieden. Het is bedoeld voor deelnemers en dienstverleners.

Techniek en functionaliteit

Hier vindt u de technische documenten van het Afsprakenstelsel eHerkenning: de koppelvlakspecificaties, de use cases, testen voor dienstverleners en testen voor deelnemers. Deze documenten bevatten informatie over welke standaarden worden gehanteerd, de functionaliteit, de berichten en koppelvlakken die eHerkenning ondersteunt en de testen die worden uitgevoerd.

- Use cases — Beschrijft de functionaliteit van eHerkenning in detail.
- Interface specifications — This section describes the interface specifications for the traffic between all roles in the network. The messages are based on SAML 2.0, or XACML where applicable.
- Attribuutverstrekking — Een dienstverlener of een herkenningsmakelaar kan in een authenticatieverzoek ook een verzoek om attributen doen. De AD, MR of HM kan als attribuutverstrekker optreden. Zij mogen alleen attributen aanbieden die in dit document beschreven worden.
- Testing — This document describes the tests that (aspiring) participants must perform.

Beveiliging

Hier vindt u de documenten over de beveiliging van het Afsprakenstelsel eHerkenning: het informatiebeveiligingsbeleid, de stelselrisicoanalyse, het normenkader en de betrouwbaarheidsniveaus. Deze documenten bevatten informatie over de normen ten aanzien van veiligheid en de maatregelen die worden genomen om het vertrouwen en de continuïteit in het netwerk te borgen.

- Betrouwbaarheidsniveaus en registratie-eisen — Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast. Het gaat in op de wijze waarop dit aansluit op het STORK raamwerk. Het is bedoeld voor deelnemers en dienstverleners.
- Informatiebeveiliging en privacy — In het netwerk voor eHerkenning wordt informatie verwerkt die vertegenwoordigers van dienstafnemers toegang geeft tot diensten van dienstverleners. Informatiebeveiliging is essentieel voor de continuïteit van het stelsel en moet daarom worden beschouwd als integraal onderdeel van de bedrijfsvoering van de deelnemers in het netwerk en de beheerorganisatie van het netwerk.
- Normenkader Stelselaudit
- Stelsel risicoanalyse
- Gemeenschappelijk normenkader informatiebeveiliging eHerkenning — Gedetailleerde uitwerking van de vereiste maatregelen voor informatiebeveiliging.

Templates en formulieren

- Checklist chain test

- Checklist simulator test
- Template deelnemersovereenkomst — De overeenkomst tussen deelnemers en beheerorganisatie op basis waarvan deelnemers gehouden zijn het afsprakenstelsel toe te passen. Deze deelnemersovereenkomst verwijst naar het afsprakenstelsel maar is er (strikt genomen) zelf geen onderdeel van.
- Template incidentrapport
- Template verzoek tot (uitbreiding) toetreding eHerkenning
- Template vrijwaring penetratietest
- Template wijziging rechtspersoon deelnemer
- Template zelfverklaring

Naast deze inhoudelijke documentatieset stelt het programma eHerkenning overigens ook materialen ter beschikking voor andere doelen en andere doelgroepen. Bijvoorbeeld bedoeld om interesse te creëren voor aansluiting bij het netwerk voor eHerkenning. Of om als bedrijf of dienstafnemende overheidsorganisatie (overheids)diensten te gaan afnemen, gebruikmakend van eHerkenning. Zie hiervoor www.eHerkenning.nl.

Algemeen

Hier vindt u de algemene introductie op het Afsprakenstelsel eHerkenning. Dit document beschrijft de werking van eHerkenning en geeft tevens een overzicht van de andere onderdelen van het afsprakenstelsel.

Deze categorie bevat de volgende onderdelen:

- Algemene introductie — Dit document geeft op hoofdlijnen inzicht in het afsprakenstelsel en de werking van het netwerk.
- Begrippenlijst eHerkenning — Binnen eHerkenning wordt één begrippenlijst gehanteerd. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden. Datzelfde geldt ook andersom: waar in dit document de zelfstandige-naamwoords-vorm van een werkwoord wordt gehanteerd, heeft deze dezelfde betekenis als het gedefinieerde werkwoord.

Algemene introductie

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Steeds meer bedrijven en instellingen maken gebruik van de digitale dienstverlening van de overheid. Bijvoorbeeld bij het aanvragen van een bouwvergunning of om hun belastingaangifte digitaal af te handelen.

Meestal worden bij deze diensten vertrouwelijke gegevens uitgewisseld. eHerkenning maakt het bij de uitwisseling van deze gegevens mogelijk om de betrokken partijen te authenticeren, identificeren en toegang te (doen) verlenen.

eHerkenning is een gestandaardiseerd, elektronisch middel voor de authenticatie van bedrijven, beroepsbeoefenaren, organisaties en privépersonen wanneer zij digitaal diensten afnemen van (overheids)dienstverleners. Net zoals DigiD dat authenticatiemiddel nu al is voor burgers. De eerste dienstverleners die via eHerkenning diensten aanbieden zijn overheidsinstanties. Daartoe is het toepassingsgebied van eHerkenning echter niet beperkt; iedere dienstverlener die aan de eisen voldoet, kan op eHerkenning aansluiten. In het vervolg wordt onder de term dienstverlener tevens overheidsdienstverlener verstaan.

Bedrijven en andere organisaties kunnen met eHerkenning bij steeds meer dienstverleners terecht en hebben niet meer voor iedere taak een ander authenticatiemiddel nodig. Zo wordt een "digitale sleutelbos" vermeden, en verminderen de administratieve lasten.

De dienstverlener op zijn beurt weet door eHerkenning precies met welke dienstafnemer zij zaken doet en of de betreffende persoon bevoegd is om namens die dienstafnemer zaken te doen met de dienstverlener. Zelf hoeft de dienstverlener daarvoor geen eigen authenticatiemiddel uit te geven en te beheren, en zo verminderen ook de uitvoeringslasten.

Voor Nederland is een verdere ontwikkeling van e-diensten van groot belang (Zie bijvoorbeeld het rapport van de commissie Wallage/Postma (2007), dat de aanzet gaf aan het Nationaal Uitvoeringsprogramma). Elektronische herkenning van bedrijven, organisaties en personen is daarvoor cruciaal. Vandaar dat het ministerie van EZ in 2009 het initiatief heeft genomen om de evidente belangen van bedrijven en (overheids)dienstverleners bij eHerkenning te bundelen. Inmiddels is dit beleid verankerd in de Digitale Agenda (§ 2.2 http://www.rijksoverheid.nl/onderwerpen/ict/documenten-en-publicaties/kamerstukken/2011/05/17/digitale-agendanl.html 17 mei 2011) en zijn er in kader van de Overheidsbrede implementatieagenda voor dienstverlening en e-overheid (iNUP) (30 mei 2011: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/05/30/aanbiedingsbrief-overheidsbrede-implem) afspraken gemaakt met gemeenten en andere overheden over de implementatie.

Kern van de oplossing: netwerk voor eHerkenning

De kern van de oplossing is een netwerk voor eHerkenning, waarin partijen – de zogenaamde deelnemers – samenwerken om eHerkenningsdiensten te leveren. In dat netwerk nemen partijen deel die authenticatiemiddelen uitgeven en bijbehorende diensten verlenen. Bestaande en toekomstige authenticatiemiddelen – zoals gebruikersnaam/wachtwoorden, card readers, VPN tokens, maar ook mobiele telefoons met TANs – kunnen zo worden gebruikt. Ook nemen partijen deel die machtigingen van bedrijven en organisaties registreren en hierover informatie verstrekken. Bijvoorbeeld het feit dat firma F haar werkneemster mevrouw Pietersen machtigt om namens firma F belastingaangifte te doen. Via het netwerk worden partijen met hun authenticatiemiddelen en machtigingen gekoppeld aan dienstverleners die hun diensten elektronisch willen ontsluiten en bedrijven en andere organisaties die diensten van deze dienstverleners willen afnemen.

Basis van het netwerk: afsprakenstelsel eHerkenning

Om een dergelijk netwerk voor eHerkenning tot stand te brengen, te laten functioneren en evolueren, is een set van afspraken nodig: het afsprakenstelsel eHerkenning. Deze afsprakenset is minimaal van opzet, genoeg om samenwerking en zekerheid in het netwerk eHerkenning te garanderen, en tegelijk zo ruim dat het voldoende vrijheid biedt om competitieve proposities van de deelnemers mogelijk te maken. Daartoe bevat het afsprakenstelsel allereerst bepalingen over de te leveren dienstverlening, de soorten rollen in het netwerk en de relaties tussen die rollen. Verder bevat het afspraken over de precieze werking van het netwerk: technische relaties, ondersteunde functionaliteit, kwaliteit van gegevens en dienstverlening. Ook zijn afspraken opgenomen over de onderliggende infrastructuur: welke standaarden worden gehanteerd, en welke berichten en koppelvlakken worden ondersteund. Tenslotte bevat het afspraken over beheer en beveiliging, inclusief de organisatie daarvan. Dat omvat tevens afspraken over de handhaving van de gemaakte afspraken, wat van essentieel belang is om de werking van het netwerk en het vertrouwen in het netwerk conform het afsprakenstelsel te waarborgen.

Doel en doelgroep van dit document

Binnen de totale documentatieset van het afsprakenstelsel geeft dit document op hoofdlijnen inhoudelijk inzicht in gedrag en werking van het afsprakenstelsel en het netwerk voor eHerkenning. Tevens vormt het de inleiding van de inhoudelijke documentatie van het Afsprakenstelsel eHerkenning.

De doelgroepen voor dit document zijn:

1. beslisser: degene die beslist over aansluiting op eHerkenning, als deelnemer of in de rol van dienstverlener;
2. adviseur: degene die de beslisser inhoudelijk adviseert;
3. implementator: degene die aansluiting op (een deel van) het afsprakenstelsel eHerkenning in de breedste zin wil implementeren (juridisch, technisch, organisatorisch, procesmatig, etc.) en/of dit wil managen, in de rol van deelnemer of dienstverlener.

Voor beslisser en adviseur zou de inhoud toereikend moeten zijn. Voor de implementator bevat het al die zaken die voor een implementatie van belang zijn; voor vragen die specifiek zijn voor bijvoorbeeld technische aansluiting zijn ook andere delen van de documentatieset noodzakelijk. Voor een eerste oriëntatie voor bedrijven is de promokit (www.eherkenning.nl/overheden/eherkenning-voor-overheden/promokit) van eHerkenning te gebruiken.

Historie en status van eHerkenning

- Versie 1.1
- Versie 1.2
- Versie 1.3
- Versie 1.4
- Versie 1.5
- Versie 1.6
- Versie 1.7
- Versie 1.8

Versie 1.1

In opdracht van het Ministerie van EZ heeft het programma eHerkenning het proces georganiseerd om met geïnteresseerde marktpartijen te komen tot versie 1.1 van het afsprakenstelsel eHerkenning. Dit is gebeurd met een iteratief werkgroepproces, waarbij zowel marktpartijen als dienstverleners hun inbreng leverden. De behoeften van dienstverleners werden hierbij vertegenwoordigd door de Gebruikersraad. (Voorafgaand aan oprichting van de Gebruikersraad vervulde het Launching Customer overleg deze functie. Gedurende 2010 bestond dit "Launching Customer" overleg uit Agentschap NL, Kamer van Koophandel, LNV. Immigratie- en Naturalisatiedienst (IND), Belastingdienst. Inspectie Verkeer en Waterstaat, Dimpact, IPO (Inter Provinciaal Overleg), OLO (Omgevingsloket Online) en Antwoord voor bedrijven.)

Het aldus gezamenlijk gerealiseerde afsprakenstelsel is vervolgens tijdelijk in beheer genomen door Stichting ICTU (zie voor de verdere uitwerking van de inrichting van het het beheer Organen en taakverdeling. In 2012 is het beheer overgedragen aan Logius). De verantwoordelijkheid voor het beheer van het afsprakenstelsel eHerkenning omvat ook het verder regisseren van de doorontwikkeling van dat afsprakenstelsel.

Immers, de toepassing van afsprakenstelsel eHerkenning versie 1.1 levert nu al bewezen unieke en waardetoevoegende oplossingen, onder andere in de proefimplementatie bij Agentschap NL. Zo verschaft het zekerheid of de persoon met wie de dienstverlener zaken doet wel is voor wie hij of zij zich uitgeeft. Ook maakt het duidelijk of deze persoon wel bevoegd is om voor het handelende Nederlandse bedrijf deze (overheids)diensten af te nemen.

Tegelijk liggen er breed gedragen wensen voor uitbreidingen van eHerkenning na versie 1.0. Zo dienen – alleen al vanwege EU-richtlijnen – ook buitenlandse bedrijven eHerkenning te kunnen gaan gebruiken, niet alleen Nederlandse. Verder ligt er het voornemen voor uitbreiding van eHerkenningsfunctionaliteit met bijvoorbeeld ondertekendiensten, waarbij de afnemer van de dienst zijn wilsuiting – bijvoorbeeld een belastingaangifte of vergunningsaanvraag – elektronisch kan bekrachtigen. Ook is het ondersteunen van een keten van machtigingen gewenst – niet alleen firma F die haar eigen werkneemster Pietersen kan machtigen, maar ook firma F die accountantsfirma A machtigt, die op haar beurt haar werkneemster Elimami machtigt om namens firma F belastingaangifte te doen. Tenslotte ligt er de behoefte om eHerkenning voor machine-to-machine communicatie geschikt te maken. Evenzovele zaken die om regie vragen door de beheerorganisatie van het afsprakenstelsel.

Versie 1.2

Gedurende 2011 is het aantal bedrijven dat eHerkenning gebruikt en het aantal dienstverleners dat aangesloten is sterk gegroeid. In deze versie 1.2 is de functionaliteit uitgebreid met attribuutverstrekking, wordt vastgelegd hoe optionele functionaliteit beschreven wordt en worden diverse RfCs uit het reguliere beheerproces verwerkt. Vanaf deze versie mogen meerdere versies van koppelvlakken binnen het netwerk toegepast worden voor zover deze in het afsprakenstelsel beschreven zijn.

Concreet betekent dat dat versie 1.1 van de koppelvlakken gedurende deze versie mag bestaan naast versie 1.2. Tevens zijn tekstuele verbeteringen doorgevoerd en enkele inconsistenties tussen documenten opgelost. Deze laatste zaken betreffen geen inhoudelijke wijzigingen.

Versie 1.3

Deze versie omvat een aantal RfCs met functionele wijzigingen die voortbouwen op versie 1.2, waaronder ten aanzien van attribuutverstrekking en foutafhandeling. Daarnaast bevat deze versie een grote hoeveelheid tekstuele verbeteringen op basis van het reviewcommentaar van de vier banken die intentieverklaring eHerkenning hebben onderschreven, alsook diverse verbeteringen rond beheer en het implementatieproces voor nieuwe versies. Tevens zijn de teksten ten aanzien van governance aangepast aan hetgeen per eind 2011 afgesproken is aangaande het beleggen van de beheerorganisatie bij Logius.

Versie 1.4

Deze versie omvat een aantal RfCs met functionele wijzigingen die voortbouwen op versie 1.3 voor o.a. toepassing van nieuwe KvK vestigingsnummer betere aansluiting op de voor overheid verplichte webrichtlijnen, voor het faciliteren van G2G gebruik. De term "bedrijf" die afkomstig was uit de beginfase is daarbij door het algemenere "dienstafnemer" vervangen, wel is in voorbeelden onveranderd uitgegaan van de belangrijkste doelgroep, namelijk bedrijven. Nieuwe versies van de deelnemersovereenkomst en gebruiksvoorwaarden en verder uitgewerkte procesbeschrijvingen van enkele cruciale beheerprocessen. In deze versie is tevens de nieuwe governance van het afsprakenstelsel verwerkt.

Versie 1.5

Deze versie omvat een aantal RfCs die de Betrouwbaarheidsniveaus van eHerkenning meer in lijn brengen met de internationale STORK norm. Daarnaast bevat deze versie RFCs die pilotbare functionaliteit bevatten voor B2C dienstverlening en attributen voor beroepsbeoefenaren. Verder bevat deze versie een vernieuwd Juridisch Kader inclusief nalevingsbeleid en gebruiksvoorwaarden. Beheerprocessen rond change- en releasemanagement, metadata, dienstencatalogus en penetratietesten zijn in meer detail beschreven.

Versie 1.6

Deze versie is een tussenversie waarin veel onderdelen van het afsprakenstelsel zijn opgeschoond maar die geen nieuwe functionaliteit bevat. Het is tevens de eerste nieuwe versie die is vastgesteld onder beheer van Logius. Alle pilotbare functionaliteit is uit het afsprakenstelsel verwijderd, evenals de verwijzigingen naar non-standaard koppelvlakken. De koppelvlakdocumenten zijn ontdubbeld. Procesbeschrijvingen zijn aangevuld en aangescherpt en de informatiebeveiligingsdocumenten zijn geactualiseerd. De eisen aan verwerken van (kopie) WID documenten zijn verduidelijkt . Tenslotte is de deelnemersovereenkomst geactualiseerd.

Versie 1.7

Deze versie bevat verschillende nieuwe functionaliteiten, te weten Single Sign On (SSO), uitgebreide attribuutverstrekking, ketenmachtigingen, ondersteuning van B2C authenticatiediensten en authenticatie van beroepsbeoefenaren. Voor deelnemers en dienstverleners is dit optionele functionaliteit waarvoor zij separaat kunnen toetreden. Ook is in deze versie het koppelvlak DV-HM verder gestandaardiseerd zodat dienstverleners gebruik kunnen maken van standaard SAML pakketten om aan te sluiten op eHerkenning. Daarnaast is de compensatieregeling voor migraties verder uitgewerkt en het Juridisch Kader verder aangescherpt.

Versie 1.8

Versie 1.8 bevat een aanscherping van enkele processen in het Operationeel handboek, alsmede wijzigingen in het Juridisch kader. In technische zin bevat deze versie een verscherping van de afspraken over het automatisch verspreiden van de netwerkmetadata en de dienstencatalogus. De koppelvlakspecificaties blijven gelijk aan die van 1.7.

Wat is eHerkenning?

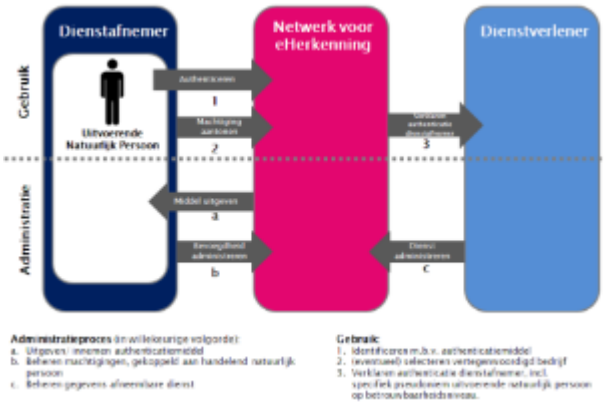
Het gebruikersperspectief

Dit hoofdstuk belicht eHerkenning vanuit het perspectief van de op het netwerk aangesloten gebruiker: de Dienstverlener (DV) en de Dienstafnemer. De dienstafnemer is een bedrijf, rechtspersoon, privépersoon, beroepsbeoefenaar of een afnemende overheidsorganisatie. De focus is dus de "buitenkant" van eHerkenning (black-box): hoe is het gedrag van afsprakenstelsel en netwerk voor eHerkenning voor die gebruiker? Daartoe wordt eerst het gedrag van het netwerk op hoofdlijnen beschreven; wat krijgen de gebruikers, en wat moeten ze ervoor doen? Dan wordt ingezoomd op kernbegrippen van eHerkenning, zoals netwerk, identificatie, authenticatie en bevoegdheid. Tenslotte wordt de notie van het afsprakenstelsel verder inhoudelijk uitgewerkt: wat voor soort afspraken omvat dit, hoe ontwikkelt het zich, en wat zijn de uitgangspunten en ontwerpprincipes ervan.

Overigens worden gaandeweg diverse begrippen van eHerkenning ingevoerd en beschreven. De exacte definities daarvan zijn terug te vinden in de Begrippenlijst eHerkenning. In communicatie aangaande het afsprakenstelsel, het netwerk en de daarmee gerealiseerde diensten is het niet toegestaan deze begrippen een andere betekenis te geven dan opgenomen in het afsprakenstelsel.

Gedrag netwerk eHerkenning op hoofdlijnen

Het netwerk voor eHerkenning levert eHerkenningsdiensten aan gebruikers. Deze eHerkenningsdiensten zorgen voor vertrouwen (met een bekend betrouwbaarheidsniveau) aangaande identiteiten en bevoegdheden.



Er zijn twee typen gebruikers:

- dienstafnemer: een partij die elektronische diensten afneemt van een dienstverlener. Een dienstafnemer wordt daarbij vertegenwoordigd door de "man of vrouw achter de knoppen" of is dat zelf. Deze laatste, die namens die dienstafnemer handelt wordt aangeduid met 'uitvoerend natuurlijk persoon';
- dienstverlener: een partij die elektronische diensten aanbiedt aan dienstafnemers.

Het netwerk voor eHerkenning levert één dienst aan gebruikers die op dat netwerk aangesloten zijn, namelijk "authenticatie dienstafnemer". De inhoud van deze dienst verschilt afhankelijk van de aard van de dienstafnemer. Als de dienstafnemer een privépersoon is of een beroepsbeoefenaar die namens zichzelf handelt, dan omvat de dienst het volgende:

- zekerheid of de uitvoerend dienstafnemer wel is voor wie hij zich uitgeeft; daartoe dient de uitvoerend natuurlijk persoon zich te identificeren aan het netwerk met een authenticatiemiddel;

Als er sprake is van vertegenwoordiging van de dienstafnemer dan omvat de dienst twee onderdelen:
zekerheid of de uitvoerend natuurlijk persoon wel is voor wie hij zich uitgeeft; daartoe dient de uitvoerend natuurlijk persoon zich te identificeren aan het netwerk met een authenticatiemiddel;

- zekerheid of die uitvoerend natuurlijk persoon wel bevoegd is om namens de dienstafnemer deze dienst bij de dienstverlener af te nemen, waarbij die bevoegdheid direct of via een intermediaire partij kan zijn verstrekt.

Op basis van deze onderdelen verstrekt het netwerk vervolgens een verklaring over de authenticatie en de gecontroleerde bevoegdheid aan de dienstverlener. De dienstverlener kan vervolgens op basis van die verklaring toegang verlenen.

In het dagelijkse gebruik van het netwerk werken deze eHerkenningsdiensten als volgt samen (zie Figuur). De uitvoerend natuurlijk persoon wil een elektronische dienst afnemen bij een dienstverlener, bijvoorbeeld het doen van belastingaangifte of het aanvragen van een subsidie of vergunning. Op een website of in een applicatie identificeert hij zich daartoe met een authenticatiemiddel (zoals een gebruikersnaam-wachtwoord-combinatie, een VPN-token, een card / card readercombinatie of een mobiele telefoon met TANs). Het netwerk authenticeert de uitvoerend natuurlijk persoon, en controleert of hij inderdaad bevoegd is deze dienstafnemer te vertegenwoordigen. Mocht dit nodig zijn, dan biedt het netwerk de uitvoerend natuurlijk persoon de mogelijkheid om te selecteren namens welke dienstafnemer hij nu gaat handelen. Zijn authenticatie en bevoegdheid in orde, dan verstrekt het netwerk aan de dienstverlener (1) een identificerend kenmerk van de dienstafnemer en (2) een referentie naar de identiteit van de uitvoerend natuurlijk persoon: een specifiek pseudoniem – niet de identiteit van de uitvoerend natuurlijk persoon zelf! Op basis van deze informatie weet de dienstverlener dat de uitvoerend natuurlijk persoon een bepaalde dienstafnemer vertegenwoordigt en ook mag vertegenwoordigen voor de betreffende dienst en kan de dienstverlener beslissen of hij de uitvoerend natuurlijk persoon toegang tot de dienst verleent.

De volgende vormen van bevoegdheden kunnen voorkomen:

- Bevoegdheid namens een bedrijf of rechtspersoon. Het bedrijf of de rechtspersoon is dienstafnemer en de uitvoerend natuurlijk persoon is bevoegd de betreffende dienst voor die dienstafnemer af te nemen;
- Bevoegdheid zelf een dienst af te nemen. De uitvoerend natuurlijk persoon kan alleen zichzelf authenticeren en treedt zelf als dienstafnemer op;
- Bevoegdheid zelf een dienst af te nemen als beroepsbeoefenaar. De uitvoerend natuurlijk persoon kan alleen zichzelf authentiseren als beroepsbeoefenaar met een kenmerk afkomstig uit het betreffende beroepskwalificatieregister en treedt zelf als dienstafnemer op.
- Bevoegdheid namens een andere natuurlijk persoon. Deze ander is de dienstafnemer.

Om dat dagelijks gebruik mogelijk te maken dienen in het netwerk drie administraties te worden bijgehouden, namelijk (a) een dienstencatalogus, (b) een middelenadministratie en (c) een machtigingenregister. De dienstverlener publiceert de bij hem afneembare diensten in deze dienstencatalogus; per dienst staat daarin welk betrouwbaarheidsniveau de dienstverlener minimaal eist om toegang te verlenen tot deze dienst en welk soort dienstafnemers toegang kan krijgen tot de dienst. Door het netwerk wordt uitgifte van authenticatiemiddelen vastgelegd in de administratie van de middelenuitgever en wordt een machtigingenregister bijgehouden, inclusief de daarbij behorende betrouwbaarheidsniveaus. In het machtigingenregister ligt tevens vast op basis van welk authenticatiemiddelen een uitvoerend natuurlijk persoon een bevoegdheid gebruikt. Tijdens het gebruik kan het netwerk – volgens het principe van de zwakste schakel – afleiden of het betrouwbaarheidsniveau van het geheel van verklaringen ten minste voldoet het door de dienstverlener gevraagde betrouwbaarheidsniveau.

Overigens: om gebruik te kunnen maken van het netwerk dient de gebruiker aangesloten te zijn. Hoe aansluiten op eHerkenning? beschrijft welke eenmalige werkzaamheden voor het aansluiten van een gebruiker nodig zijn. Wat is eHerkenning? en Hoe werkt eHerkenning? beschrijven de continue werkzaamheden van gebruiker en netwerk.

Kernbegrippen van eHerkenning

Het netwerk voor eHerkenning strekt zich uit van enerzijds de relatie met dienstafnemers die gebruik maken van eHerkenning tot anderzijds het koppelvlak met dienstverleners die eHerkenning vereisen als waarborg voor de door hen aangeboden diensten. Binnen het netwerk zijn verschillende rollen gedefinieerd, die door deelnemers worden ingevuld (zie Hoe werkt eHerkenning?). Door het zo invullen van rollen door deelnemers worden de benodigde eHerkenningsdiensten geleverd, en kan het netwerk functioneren. Het afsprakenstelsel reguleert dit netwerk (zie Juridisch kader).

In de Gedrag netwerk eHerkenning op hoofdlijnen geïntroduceerde eHerkenningsdiensten zijn de volgende termen van belang:

- identificatie, zoals dit gebeurt door de dienstafnemer, en daarbinnen door de uitvoerend natuurlijk persoon. Onder identificatie wordt verstaan het "noemen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden"; de entiteit is hier iedere schakel in de machtigingsketen beginnende met de dienstafnemer tot en met de uitvoerend natuurlijk persoon. Het noemen van attributen gebeurt voor de uitvoerend natuurlijk persoon m.b.v. een authenticatiemiddel en voor de verdere schakels op basis van de in het machtigingenregister vastgelegde kenmerken en de context is het netwerk voor eHerkenning. Identificatie is dus de "claim" dat in een bepaalde context "iets" of iemand (een partij) aangeduid of bedoeld wordt. Let wel: identificatie zegt dus niet of deze claim juist is! In het geval van een ketenmachtiging moet iedere schakel in de keten geïdentificeerd worden.

- authenticatie verklaart op een bepaald betrouwbaarheidsniveau dat de partij werkelijk is wie hij claimt te zijn. Onder authenticatie wordt dan ook verstaan "het staven van een geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau". Aan authenticatie gaat dus altijd identificatie vooraf.
- bevoegdheid van de uitvoerend natuurlijk persoon namens de dienstafnemer, mogelijk op grond van een machtigingsketen. De bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet, hetzij een volmacht (privaatrecht), hetzij een machtiging (bestuursrecht). Een bevoegdheid kan eventueel ingeperkt zijn tot bepaalde rechtshandelingen, of een bepaalde relevante omvang ten aanzien van rechtshandelingen; dit kan ook toegepast worden wanneer privé-personen zich authenticeren voor een dienstafname en het gebruik van hun authenticatiemiddel willen beperken tot bepaalde diensten. In eHerkenning wordt als synoniem van bevoegdheid de term machtiging gebruikt, en als synoniem van bevoegdhedenregister de term machtigingenregister.
- toegangsverlening is een proces onder verantwoordelijkheid van de dienstverlener, waarin die voor een uitvoerend natuurlijk persoon bepaalt tot welke diensten deze toegang krijgt, of welke acties deze mag uitvoeren. Dit gebeurt op grond van door het netwerk verstrekte verklaringen en mogelijke controles van andere relevante toegangsrechten die door de dienstverlener zelf zijn vastgelegd. In het bijzonder vindt controle van bevoegdheden plaats, door in een machtigingenregister bestaan en reikwijdte van de vertegenwoordigingsrelatie na te gaan. Dit vooronderstelt dat de dienstverlener al met voldoende zekerheid weet met welke uitvoerend natuurlijk persoon hij van doen heeft; authenticatie gaat dan ook vooraf aan toegangsverlening.

Toelichting op enkele formelere definities

Als verdieping worden nu de formele definities besproken van de begrippen partij, dienstafnemer, vertegenwoordiging en betrouwbaarheidsniveaus (zie verder Begrippenlijst eHerkenning).
Het begrip partij wordt in het afsprakenstelsel bewust gebruikt als algemene term. Onder partij wordt een persoon of samenwerkingsverband van personen verstaan (partij is een generalisatie van het juridische begrip persoon inclusief samenwerkingsverbanden van personen). Partij wordt zowel gebruikt in de beschrijving van het afsprakenstelsel waar het gaat om partijen die gebruikers zijn van het netwerk of die deelnemer zijn aan het netwerk als bij het aanduiden van degenen waarop de herkenning betrekking heeft, bijvoorbeeld partij A machtigt partij B. Als categorieën van partijen onderkent het afsprakenstelsel: (handelende) bedrijven, dienstverleners, deelnemers, uitvoerend natuurlijk personen, privépersonen, beroepsbeoefenaren, beheerorganisatie, certificeerders en toezichthouders.

Voor eHerkenning is het essentieel dat partijen precies en uniek geïdentificeerd kunnen worden. Indien bijvoorbeeld een grotere organisatie die uit meerdere rechtspersonen bestaat eHerkenning toepast, dan zal steeds duidelijk moeten zijn welk van deze rechtspersonen de dienst wil afnemen.

In de context van het afsprakenstelsel wordt onder dienstafnemers alle vormen van ondernemingen, instellingen, rechtspersonen, overheidsorganisaties, privépersonen en beroepsbeoefenaren verstaan. In een meer precieze juridische definitie is dit de verzameling van eenmanszaken c.q. natuurlijke personen die een onderneming drijven en niet-natuurlijke personen. Dienstafnemers zijn de gebruikers die eHerkenning toepassen bij het afnemen van diensten van dienstverleners. De dienstverleners die eHerkenning vereisen als waarborg voor elektronische diensten die zij aanbieden en de deelnemers aan het afsprakenstelsel vallen strikt genomen ook onder de definitie van dienstafnemer. Waar over dienstafnemer wordt gesproken worden echter alleen de dienstafnemers bedoeld die eHerkenning gebruiken bij het afnemen van diensten.

Onder vertegenwoordiging wordt verstaan de rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde partij (de vertegenwoordiger of gemachtigde) in naam van een andere partij (de vertegenwoordigde dienstafnemer) met een derde verrichte handeling (dienst) aan de vertegenwoordigde dienstafnemer worden toegerekend. De laatste in een eventuele keten van vertegenwoordigingen is altijd de uitvoerende natuurlijke persoon. In deze versie van eHerkenning worden ketens van maximaal twee niveaus van vertegenwoordiging ondersteund.

Het afsprakenstelsel hanteert vijf vastomschreven betrouwbaarheidsniveaus (Opbouw betrouwbaarheidsniveaus eHerkenning) o m de mate van betrouwbaarheid aan te duiden van identificatie, authenticatie en bevoegdheidsvastlegging. Ieder hoger betrouwbaarheidsniveau stelt steeds verdergaande eisen aan registratie en benutting. Ten behoeve van interoperabiliteit binnen de Europese Unie baseert het netwerk voor eHerkenning haar terminologie en processen voor betrouwbaarheidsniveaus op het STORK raamwerk (Generieke identificatie en authenticatie, doorontwikkeling van eerdere activiteiten in het kader van IDABC. Het raamwerk is vastgelegd in STORK deliverable D2.3 – Quality authenticator scheme, Hoofdstuk 1 (als achtergrond) en Hoofdstuk 2 (daadwerkelijke beschrijving). eHerkenning bouwt voort op STORK's criteria voor authenticatiemiddelen en voegt daaraan criteria voor bevoegdheden toe. Het onderdeel Betrouwbaarheidsniveaus en registratie-eisen werkt dit inhoudelijk uit, gaat in op toekomstige ontwikkelingen van het raamwerk en hoe dit eHerkenning beïnvloedt.

Afsprakenstelsel eHerkenning en ontwerpprincipes

Leidend voor gedrag en werking van netwerk en afsprakenstelsel eHerkenning én de toekomstige ontwikkeling ervan, zijn de volgende uitgangspunten en ontwerpprincipes:

- Alle aangesloten bedrijven en andere dienstafnemers dienen binnen het netwerk voor eHerkenning terecht te kunnen bij alle aangesloten dienstverleners.

- Het afsprakenstelsel maakt het mogelijk dat bestaande en nieuwe methoden en oplossingen voor identificatie, authenticatie, vertegenwoordiging en autorisatie worden toegepast voor eHerkenning. Deze flexibiliteit is nodig om zowel de complexiteit recht te doen als om de snelle ontwikkelingen op dit gebied te kunnen benutten.
- Gezien de grote diversiteit aan bedrijven, andere dienstafnemers en vormen van vertegenwoordiging waarvoor het afsprakenstelsel eHerkenningsdiensten moet leveren dienen schaalbaarheid en uitbreidbaarheid in het ontwerp verankerd te zijn.
- Het afsprakenstelsel beschrijft de minimaal noodzakelijke verantwoordelijkheden voor een netwerk voor eHerkenning, waar mogelijk verbijzonderd naar de rollen die door deelnemers in dat netwerk worden ingevuld.
- De koppelvlakken tussen het netwerk en haar gebruikers zijn onderdeel van het netwerk en worden beschreven in het afsprakenstelsel.
- Het afsprakenstelsel gaat uit van een marktmodel voor de invulling van deze rollen, dat wil zeggen dat meerdere deelnemers – deels in concurrentie, deels in coöperatie met elkaar – de rollen kunnen invullen en dat daarbij enkel gereguleerd wordt wat minimaal noodzakelijk is voor het functioneren van het geheel. Het afsprakenstelsel dient deelnemers ruimte te bieden voor het leveren van additionele diensten.
- Non-discriminatie, openheid voor nieuwe deelnemers en keuzevrijheid van gebruikers.
- Een dienstverlener sluit contracten met één type deelnemer (de zogeheten eHerkenningsmakelaar), die eHerkenningsdiensten levert op basis van het netwerk voor eHerkenning.
- Het afsprakenstelsel voorziet in machtigingen van dienstafnemers aan zowel natuurlijke personen als aan andere bedrijven, rechtspersonen en organisaties en in het vastleggen of beperken van de eigen bevoegdheden voor e-diensten door privépersonen en beroepsbeoefenaren. In versie 1.7 is dit beperkt tot de machtiging van maximaal twee schakels.
- Het afsprakenstelsel voldoet aan wet- en regelgeving en houdt rekening met de internationale standaarden en ontwikkelingen.
- In het bijzonder garandeert het netwerk – conform de Wet bescherming persoonsgegevens – privacy en dataminimalisatie, door persoonsgegevens niet meer te verzamelen en te bewerken en niet langer te bewaren dan nodig voor het doel waarvoor die persoonsgegevens verkregen werden en door enkel die persoonsgegevens te verstrekken die gevraagd worden door de dienstverlener en waarvoor de betrokkene toestemming heeft gegeven ("privacy by design").
- Het netwerk voldoet aan professionele normen voor informatiebeveiliging.
- Het afsprakenstelsel maakt naast business-to-government en government-to-government ook business-to-business en business-to-consumer e-diensten mogelijk.
- Het afsprakenstelsel is de gezamenlijke verantwoordelijkheid van de deelnemers en de overheid waarbij ieders verantwoordelijkheden worden beschreven. De deelnemers zijn in beginsel private c.q. marktpartijen die elk één of meer in het afsprakenstelsel gedefinieerde rollen vervullen. De betrokkenheid van de overheid is drieledig: eHerkenning is essentieel voor de e-diensten van de overheid, de overheid neemt verantwoordelijkheid voor het borgen van het vertrouwen in het afsprakenstelsel door toezicht en voor de continuïteit van de eHerkenningsdiensten door het strategische beheer in een publiek – private samenwerking vorm te geven, de daarvoor benodigde benoemingen te doen en reglementen vast te stellen. Daarnaast speelt het ministerie van Economische Zaken een stimulerende rol in de ontwikkeling.
- Bestuur van het afsprakenstelsel en toezicht op het afsprakenstelsel en de wijze waarop dit in een beheerorganisatie belegd is, zijn beschreven in het afsprakenstelsel zelf.

Zie voor uitwerking hiervan Bijlage – Toepassingen uitgangspunten en randvoorwaarden.

Hoe werkt eHerkenning?

Het deelnemersperspectief

Dit hoofdstuk belicht eHerkenning vanuit het perspectief van de aangesloten deelnemers, die rollen invullen en daarmee het netwerk eHerkenning daadwerkelijk laten functioneren. De focus is dus de "binnenkant" van eHerkenning (white-box): hoe is de werking van afsprakenstelsel en netwerk voor eHerkenning? Daartoe wordt eerst de werking van het netwerk op hoofdlijnen beschreven; hoe werken de rollen onderling zo samen in termen van geleverde diensten, dat het in Wat is eHerkenning? beschreven gedrag van het netwerk voor de aangesloten gebruikers tot stand komt? Dan wordt ingezoomd op de vier verschillende rollen die eHerkenning kent, namelijk middelenuitgever, authenticatiedienst, machtigingenregister en eHerkenningsmakelaar. Tenslotte wordt ingegaan op manieren waarop de rollen kunnen worden vervuld door concrete deelnemers. De optioneel aan te bieden zogenoemde aanvullende features worden in deze beschrijving niet inbegrepen en komen daarna in Werking aanvullende features aan de orde.

Overigens: om rollen te vervullen in het netwerk dient de deelnemer daarop aangesloten te zijn. Hoe aansluiten op eHerkenning? beschrijft welke eenmalige werkzaamheden voor het aansluiten van een deelnemer in één of meer rollen nodig zijn. Dit hoofdstuk beschrijft de continue werkzaamheden van de rollen.

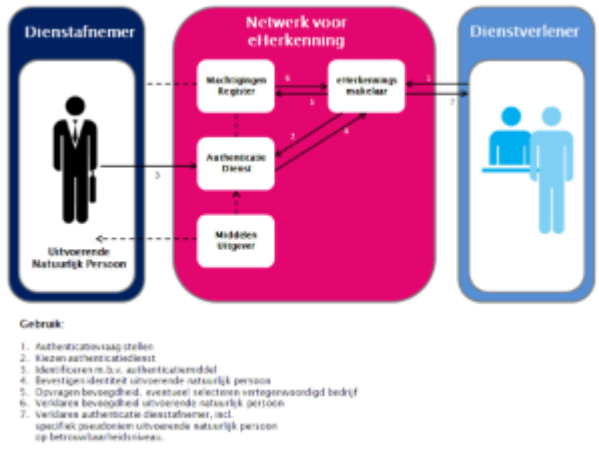
- Werking van netwerk eHerkenning op hoofdlijnen
- Deelnemers: rollen en verantwoordelijkheden
- Mogelijke vervulling van rollen door deelnemers

Werking van netwerk eHerkenning op hoofdlijnen

De werking van het netwerk eHerkenning is op hoofdlijnen als volgt. Zoals in Gedrag netwerk eHerkenning op hoofdlijnen wordt besproken: uiteindelijk dient het netwerk in het gebruik aan de dienstverlener op het gevraagde betrouwbaarheidsniveau te verklaren over de authenticatie van de dienstafnemer en een specifiek pseudoniem mee te geven van de nu voor die dienstafnemer bevoegde uitvoerend natuurlijk persoon. Bijvoorbeeld een verklaring met als inhoud [KvK-nummer = 1234, specifiek pseudoniem = Abcd, betrouwbaarheidsniveau = 3].

Om zo'n verklaring voor elkaar te krijgen is een keten van berichten en administraties nodig, zoals hier weergegeven. Het meest voorkomende geval wordt in de lopende tekst toegelicht met een eenvoudig voorbeeld, waar de (uitvoerend natuurlijk) persoon Bouchra namens één bedrijf gemachtigd is.

Samenwerking deelnemers in netwerk eHerkenning



Als beginpunt wordt hier gekozen een op het netwerk aangesloten dienstverlener, die een nieuwe of bestaande dienst – bijvoorbeeld het doen van belastingaangifte of het aanvragen van een subsidie of vergunning – via eHerkenning toegankelijk wil gaan maken. Met "beheren gegevens afneembare dienst" legt de dienstverlener de kenmerken van die bij hem afneembare dienst vast in de Dienstencatalogus (DC) van het netwerk. Eén van die kenmerken is het betrouwbaarheidsniveau dat hij minimaal eist om een dienstafnemer toegang te verlenen tot deze dienst. In de dienstencatalogus wordt ook vastgelegd welke soorten dienstafnemers een bepaalde dienst kunnen afnemen. Bepaalde diensten kunnen niet voor privépersonen of niet voor beroepsbeoefenaren zijn.

Dan komt de dienstafnemer, in dit voorbeeld een bedrijf, in het spel. Een op het netwerk aangesloten bedrijf dat toegang wil krijgen tot een dienst van een dienstverlener dient zaken rond authenticatiemiddelen en bevoegdheden te regelen. Een uitvoerend natuurlijk persoon krijgt door een middelenuitgever een nieuw authenticatiemiddel uitgereikt, of hij kan een bestaand authenticatiemiddel bij een middelenuitgever laten registreren. Uit tabel 1 blijkt bijvoorbeeld dat aan de uitvoerend natuurlijk persoon met het interne pseudoniem AB..10 het VPN-token VP678 is uitgereikt als authenticatiemiddel met betrouwbaarheidsniveau 3. Deze natuurlijke persoon heet in werkelijkheid Bouchra Elimami.

Tabel 1: Middelenadministratie

intern pseudoniem	authenticatiemiddel	middel-ID	betrouwbaarheidsniveau
AB..10	VPN-token	VP678	3
AB..11	user-pass	acc: vjansen	1
AB..12	mobiele tel	0612345678	2

Vervolgens dient de intermediaire partij bevoegdheden te administreren bij het machtigingenregister. Deze bevoegdheid kan ruim zijn – "Bouchra mag alles namens bedrijf BVoorbeeld" – of specifiek "Bouchra mag namens bedrijf BVoorbeeld ziekmeldingen doen en subsidies aanvragen". Een bevoegdheid kan daarbij tevens worden beperkt tot één of meer vestigingen van het bedrijf. Indien de bevoegdheid specifieke diensten benoemt, zal het machtigingenregister deze diensten vermelden in de terminologie van de dienstencatalogus. Tabel 2 toont het (kleine en sterk vereenvoudigde) deel van het machtigingenregister

dat o.a. uitvoerend natuurlijk persoon Bouchra Elimami met intern pseudoniem AB..10 bevoegd verklaart om voor de intermediaire partij met KvK-nummer 1234 de diensten B en C af te nemen. Bij afname van dienst B zal zij extern bekend staan met het specifieke pseudoniem Abcd.

Tabel 2: Machtigingenadministratie

bedrijf-ID (KvK-nr)	uitvoerend natuurlijk persoon	intern pseudoniem	bevoegd voor	specifiek pseudoniem
1234	Bouchra Elimami	AB..10	Dienstverlener X, Dienst B	Abcd
1234	…	…	Dienstverlener X, Dienst B	…
1234	Bouchra Elimami	AB..10	Dienstverlener Y, Dienst C	Xyz0
1234	…	…	Dienstverlener Y, Dienst C	…

Nu kan het dagelijks gebruik beginnen. De uitvoerend natuurlijk persoon wil een elektronische dienst afnemen bij een dienstverlener. Op een website of in een applicatie identificeert hij zich daartoe met een authenticatiemiddel. Zo wil Bouchra dienst B afnemen, en zich daarbij identificeren met haar VPN-token. Op de website van de dienstverlener kiest zij voor dienst B, waarop de eHerkenningsmakelaar haar de vraag voorlegt welke authenticatiedienst zij wil gebruiken. Bouchra wordt vervolgens doorgestuurd naar de website van de authenticatiedienst. Indien Bouchra al eerder een authenticatiedienst heeft geselecteerd en deze keuze heeft vastgelegd dan kan deze stap worden overgeslagen.

De authenticatiedienst ontvangt de gewenste wijze van identificeren en raadpleegt de gegevens van de middelenuitgever. In het voorbeeld van Bouchra logt zij in met haar VPN-token, en wordt uit de middelenadministratie duidelijk dat zij met een betrouwbaarheidsniveau 3 het interne pseudoniem AB..10 heeft. De authenticatiedienst meldt nu aan de eHerkenningsmakelaar dat de uitvoerend natuurlijk persoon met intern pseudoniem AB..10 geauthenticeerd is met betrouwbaarheidsniveau 3.

Vervolgens legt de eHerkenningsmakelaar aan het machtigingenregister de vraag voor of de geauthenticeerde uitvoerend natuurlijk persoon bevoegd is tot afname van de geselecteerde dienst, en zo ja, of deze bevoegdheid op het gevraagde betrouwbaarheidsniveau is geregistreerd. Het machtigingenregister meldt terug dat deze uitvoerend natuurlijk persoon inderdaad bevoegd is voor de genoemde dienst, en meldt daarbij ook met welk specifiek pseudoniem deze uitvoerend natuurlijk persoon aangeduid dient te worden. Mocht deze uitvoerend natuurlijk persoon voor méér dienstafnemers mogen handelen, dan zal het machtigingenregister de namen van deze dienstafnemers voorleggen aan de uitvoerend natuurlijk persoon, zodat die kan selecteren voor welk dienstafnemer hij deze keer wil handelen. Op dezelfde wijze zal wanneer een ketenmachtiging geverifieerd wordt waar nodig een aan de uitvoerende natuurlijk persoon gevraagd worden de bedoelde te selecteren. In het geval van Bouchra legt de eHerkenningsmakelaar aan het machtigingenregister de vraag voor of de persoon met intern pseudoniem AB..10 bevoegd is voor het afnemen van dienst B namens bedrijf met KvK-nummer 1234. Het machtigingenregister ziet dat de persoon met intern pseudoniem AB..10 op dit moment alleen bevoegd is voor bedrijf met KvK-nummer 1234 op te treden, en inderdaad daarvoor ook dienst B mag afnemen. Hierdoor kan het machtigingenregister nu direct aan de eHerkenningsmakelaar terugmelden dat de uitvoerend natuurlijk persoon met specifiek pseudoniem "Abcd" bevoegd is om dienst B af te nemen namens bedrijf met KvK-nummer 1234, en dat deze verklaring gedaan wordt met betrouwbaarheidsniveau 3.

Nu authenticatie en bevoegdheid aantoonbaar op orde zijn, kan de eHerkenningsmakelaar de eHerkenningsdienst afronden. Hij verstrekt daartoe, onder vermelding van het behaalde betrouwbaarheidsniveau, aan de dienstverlener (1) een identificerend kenmerk van de intermediaire partij en (2) een referentie naar de identiteit van de uitvoerend natuurlijk persoon: een specifiek pseudoniem - niet de identiteit van de uitvoerend natuurlijk persoon zelf! In het geval van Bouchra verklaart de eHerkenningsmakelaar dus dat bedrijf met KvK-nummer 1234 geauthenticeerd is met betrouwbaarheidsniveau 3, en bij het afnemen van dienst B vertegenwoordigd zal worden door de met pseudoniem "Abcd" aangeduide uitvoerend natuurlijk persoon.

Hiermee is het werk van het netwerk eHerkenning voor de afname van deze dienst ten einde. De dienstverlener is nu aan zet om te beslissen of hij de (voor hem uit het netwerk eHerkenning niet met name bekende) uitvoerend natuurlijk persoon toegang tot de dienst verleent.

Deelnemers: rollen en verantwoordelijkheden

Zoals hierboven aangegeven, onderscheidt het netwerk de volgende rollen:

- middelenuitgever: heeft de verantwoordelijkheid voor het uitgeven van authenticatiemiddelen, het identificeren en bij uitgifte authenticeren van natuurlijke personen;
- authenticatiedienst: heeft de verantwoordelijkheid voor het authenticeren van uitvoerend natuurlijk personen;
- machtigingenregister: heeft de verantwoordelijkheid voor het registreren en onderhouden van bevoegdheden en het controleren van bevoegdheden;
- eHerkenningsmakelaar: vormt het koppelpunt tussen het netwerk voor eHerkenning en de dienstverleners, en heeft een routeer- en navigatiefunctie in het netwerk; dit reduceert het aantal relaties tussen dienstverleners enerzijds en authenticatiediensten en machtigingenregisters anderzijds.

Van iedere rol worden nu op hoofdlijnen de verantwoordelijkheden aangegeven, voor zover deze verplicht zijn voor alle deelnemers. Voor toetredingseisen wordt verwezen naar Toetredingseisen en voor details over de functionaliteit naar Use cases.

Verantwoordelijkheden middelenuitgever

De middelenuitgever moet de volgende functionaliteit aanbieden:

- uitgifte, beheer en intrekking van authenticatiemiddelen en het zorgvuldig vastleggen van alle daarvoor conform de betrouwbaarheidsniveaus geregistreerde gegevens in een administratie;
- het ten behoeve van uitgifte identificeren en authenticeren van natuurlijke personen;
- ondersteunen van één of meerdere betrouwbaarheidsniveaus;
- doorgeven van benodigde informatie aan één of meer authenticatiediensten op basis van vastgelegde afspraken;
- optioneel: het ten behoeve van uitgifte identificeren en authenticeren van natuurlijke personen in hun rol als beroepsbeoefenaar.

Verantwoordelijkheden authenticatiedienst

Een authenticatiedienst moet:

- een online interface bieden aan uitvoerend natuurlijk personen zodat die zich als onderdeel van eHerkenning met hun authenticatiemiddel kunnen laten authenticeren;
- logoutberichten verwerken en de uitvoerend natuurlijk persoon een scherm tonen met een bevestiging nadat logout heeft plaatsgevonden (indien de authenticatiedienst geen SSO ondersteunt of heeft uitgevoerd dan volstaat het tonen van het bevestigingsscherm);
- de eisen aangaande betrouwbaarheidsniveaus conform het deel betrouwbaarheidsniveaus toepassen en tevens voldoen aan de eisen in Use cases

Verantwoordelijkheden machtigingenregister

Een machtigingenregister moet de volgende functionaliteit leveren:

- registratie van de identificerende kenmerken van dienstafnemers die bevoegdheden laten vastleggen en hun beheerders;
- registratie van de identificerende kenmerken van uitvoerend natuurlijke personen die bevoegd zijn om namens een

dienstafnemer bepaalde elektronische diensten af te nemen bij dienstverleners;
- het conform het uitgangspunt van dataminimalisatie beperken van de informatie die over de uitvoerend natuurlijk persoon wordt verstrekt, met name door het toekennen van specifieke pseudoniemen aan uitvoerend natuurlijke personen;
- een proces (in welke vorm dan ook) voor het opvoeren, onderhouden en intrekken van registraties voor bevoegdheden.

Onder registratie wordt telkens verstaan een ingerichte administratie inclusief een proces voor opvoeren, beheren en verwijderen van gegevens.

Een machtigingenregister moet bij registratie en gebruik de eisen aangaande betrouwbaarheidsniveaus toepassen conform Betrouwbaarheidsniveaus en registratie-eisen.

Verantwoordelijkheden eHerkenningsmakelaar

Een eHerkenningsmakelaar moet:

- aan dienstverleners een gestandaardiseerd koppelvlak leveren waarover eHerkenningsdiensten kunnen worden geïnitieerd en gevraagde verklaringen kunnen worden geleverd.
- voor authenticatiediensten en machtigingenregisters tenminste de twee meest recente gestandaardiseerde koppelvlakken ondersteunen zolang dit voor migratie noodzakelijk is.
- aan uitvoerend natuurlijke personen een online interface leveren om de uitvoerend natuurlijk persoon in staat te stellen indien nodig een authenticatiedienst of een machtigingenregister te selecteren.
- zowel het koppelvlak voor online bevragen van machtigingenregisters als het koppelvlak voor verificatie van de volgende schakel aan een machtigingenregister ondersteunen. Indien een eHerkenningsmakelaar deze verificatie niet kan uitvoeren mag deze eHerkenningsmakelaar geen diensten bedienen waarvan in dienstencatalogus is vastgelegd dat ze ketenmachtigingen toelaten.
- in staat zijn om op basis van een authenticatieverklaring en een of meer machtigingsverklaringen ontvangen van machtigingsregisters een verklaring aan de dienstverlener over authenticatie en ketenmachtiging samen te stellen. Voorafgaand aan verstrekking moet de eHerkenningsmakelaar de consistentie van alle verklaringen en gespecificeerde informatie controleren.
- uitvoerend natuurlijk personen bij de selectie van de authenticatiedienst de optie bieden om deze instelling te bewaren. Iedere eHerkenningsmakelaar moet zorgen dat een uitvoerend natuurlijk persoon waarvoor de selectie van de authenticatiedienst bewaard is, deze vraag niet opnieuw voorgelegd krijgt.
- SSO ondersteunen en daartoe vragen met SSO doorgeven aan een authenticatiedienst en logoutberichten verwerken en doorsturen naar de authenticatiedienst.

Mogelijke vervulling van rollen door deelnemers

Elk van de genoemde rollen mag door meerdere deelnemers worden vervuld. Ook mag één deelnemer meerdere rollen vervullen Voor elk van de rollen die zij invullen zijn deelnemers verplicht de afspraken over het implementeren van nieuwe versies te volgen, tenzij het afsprakenstelsel het naast elkaar bestaan van meerdere versie van koppelvlakken expliciet toestaat. Doordat de rollen technisch zodanig ingericht zijn dat zij om kunnen gaan met optionele functionaliteit hoeven aanvullende features niet tot technische wijzigingen te leiden voor deelnemers die deze features niet implementeren.

Tussen de rollen in het netwerk c.q. tussen de deelnemers die de rollen invullen bestaan relaties. Dit zijn contractuele relaties, hetzij op basis van een bilateraal contract, hetzij via het contract dat deelnemers met de beheerorganisatie van het netwerk sluiten; zie hiervoor Hoe aansluiten op eHerkenning? en Juridisch kader. Daarnaast betreffen de relaties de koppelvlakken die noodzakelijk zijn voor het gebruik van eHerkenning en de daarvoor benodigde administratie.

Deze laatste koppelvlakrelaties tussen de rollen onderling en die met gebruikers zijn als volgt:

- Een eHerkenningsmakelaar MOET relaties hebben met alle authenticatiediensten en alle machtigingenregisters.
- Authenticatiediensten en machtigingenregisters MOETEN ieder een relatie hebben met alle eHerkenningsmakelaars.
- Een middelenuitgever MOET een relatie hebben met tenminste één authenticatiedienst.
- Een authenticatiedienst MOET een relatie hebben met tenminste één middelenuitgever.

Formele beschrijving van de gebruiks- en administratierelaties (koppelvlakrelaties)

Hierin wordt strikt onderscheid gemaakt tussen een rol uit het netwerk enerzijds, en de deelnemer (een concrete partij) die één of meer van die rollen vervult. Er zijn precies vier rollen, die telkens in het enkelvoud zullen worden aangeduid.

- Een deelnemer die de rol van eHerkenningsmakelaar vervult, MOET relaties hebben met iedere andere deelnemer die de rol van authenticatiedienst en/of machtigingenregister vervult.

- Andersom, een deelnemer die de rol van authenticatiedienst en/of machtigingenregister vervult, MOET steeds een relatie hebben met iedere andere deelnemer die de rol van eHerkenningsmakelaar vervult.
- Een deelnemer die de rol van middelenuitgever vervult, MOET een relatie hebben met tenminste één deelnemer die de rol van authenticatiedienst vervult.
- Een deelnemer die de rol van authenticatiedienst vervult, MOET een relatie hebben met tenminste één deelnemer die de rol van middelenuitgever vervult.

Aan het netwerk mogen rollen worden toegevoegd. eHerkenningsmakelaars ZOUDEN met alle deelnemers die een dergelijke nieuwe rol vervullen een relatie MOETEN aangaan. Per nieuwe rol moet als onderdeel van het wijzigingsproces bepaald worden met welke andere rollen relaties moeten bestaan.

Werking aanvullende features

- Werking attribuutverstrekking
- Werking ketenmachtigingen
- Werking SSO

Werking attribuutverstrekking

De aanvullende feature attribuutverstrekking voegt aan de werking van eHerkenning in het gebruikersperspectief toe dat gegevens onder geïnformeerde uitdrukkelijke toestemming van de betrokkene doorgegeven kunnen worden in de door eHerkenning aan dienstverleners verstrekte verklaringen. Het betreft gegevens die bij de registratie of later verstrekt zijn of die tijdens de authenticatie in een neutraal en betrouwbaar register kunnen worden gevalideerd. Deze gegevens kunnen dan door de ontvangende dienstverlener benut worden om de dienst te personaliseren, in communicatie over de dienstafname via andere kanalen en in andere dienstverlening (op voorwaarde dat de betrokkene is geïnformeerd over het gebruik van zijn gegevens conform de Wbp). Het betreft bijvoorbeeld NAW- en contactgegevens of gegevens van de vertegenwoordigde dienstafnemer.

In het deelnemersperspectief voegt de aanvullende feature attribuutverstrekking de volgende verantwoordelijkheden toe aan bestaande rollen.

Verantwoordlijkheden middelenuitgever

Registreren van door aanvrager van het authenticatiemiddel verstrekte persoonsgegevens behorende bij de houder van het middel. Deze persoonsgegevens kunnen zelfverklaard zijn of geverifieerd tijdens de registratie of op een later moment op een bepaald betrouwbaarheidsniveau. Voorafgaand aan het doorgeven van persoonsgegevens aan de dienstverlener vragen om user consent met mogelijkheid daarbij aan te geven dat dit niet tijdens iedere authenticatie gevraagd hoeft te worden voor verstrekking van betreffende persoonsgegeven aan betreffende dienstverlener.

Verantwoordelijkheden authenticatiedienst

Na een geslaagde authenticatie verstrekken van attributen over de geauthenticeerde uitvoerend natuurlijk persoon indien dit door de dienstverlener gevraagd wordt en indien het op grond van bij middelenuitgever of authenticatiedienst geregistreerde user consent of tijdens authenticatie gevraagde consent is toegestaan.
Indien attribuutverstrekking wordt aangeboden moet aan houders van authenticatiemiddelen steeds inzage, correctie en intrekking geboden kunnen worden van de over hen geregistreerde persoonsgegevens en of er toestemming is verleend voor het zonder steeds opnieuw vragen verstrekken van deze persoonsgegevens (dit inzageproces kan elektronisch of op papier worden aangeboden).

Verantwoordelijkheden machtigingenregister

- Registreren van gegevens van de vertegenwoordigde dienstafnemer of intermediaire partij gegevens welke verstrekt kunnen worden binnen de context van een machtiging. Deze kunnen zelfverklaard zijn, geverifieerd tijdens registratie of op een later moment of gevalideerd op het moment van authenticatie;
- per gegeven registreren van user consent van de wettelijke vertegenwoordiger of machtigingenbeheerder voor het daadwerkelijk verstrekken van die gegevens aan alle dienstverleners (indien gewenst kan worden geregistreerd dat een gegeven alleen aan specifieke dienstverlener(s) mag worden geleverd);
- na aantreffen van machtiging verstrekken van attributen behorende bij de context waarop de machtiging betrekking heeft indien dit door de dienstverlener gevraagd wordt en indien het op grond van geregistreerde user consent is toegestaan (indien user consent niet vooraf is geregistreerd moet dit op moment van transactie worden gevraagd).

Indien attribuutverstrekking wordt aangeboden moet aan vertegenwoordigde dienstafnemers of intermediaire partijen waarvoor machtiging worden geregistreerd en hun beheerders inzage, correctie en mogelijkheid tot verwijderen geboden kunnen worden van de over hen geregistreerde (persoons)gegevens en of er toestemming is verleend voor het zonder steeds opnieuw vragen verstrekken van deze gegevens (dit inzageproces kan elektronisch of op papier worden aangeboden).

Verantwoordelijkheden eHerkenningsmakelaar

Het registreren welke attributen een dienstverlener wil uitvragen bij iedere authenticatie. Het doorgeven van attributen precies zoals ze ontvangen zijn van authenticatiediensten of machtigingenregisters.

Werking ketenmachtigingen

De vereisten voor het leveren van eHerkenningsdiensten gebaseerd op ketenmachtigingen moeten door eHerkenningsmakelaars als verplichte functionaliteit worden ondersteund (zie Verantwoordelijkheden eHerkenningsmakelaar), tenzij deze alleen diensten bedient waarvan in dienstencatalogus vastligt dat ze geen ketenmachtigingen toelaten. Een deelnemer met een machtigingenregister is echter vrij of zijn machtigingenregister wordt aangevuld met de aanvullende feature ketenmachtigingen.

Verantwoordelijkheden machtigingenregister met ketenmachtigingen

Een machtigingenregister dat ketenmachtigingen kan ondersteunen vult dezelfde verantwoordelijkheden in als een standaard machtigingenregister (zie Verantwoordelijkheden machtigingenregister) en daarnaast:

- registratie van de identificerende kenmerken van partijen die geen natuurlijk persoon zijn en die bevoegd zijn om namens een vertegenwoordigde dienstafnemer bepaalde elektronische diensten af te nemen bij dienstverleners;
- vastleggen in welk volgend machtigingenregister een volgend deel van een keten zich bevindt;
- vastleggen van beperkingen van de strekking van machtigingen die specifiek zijn voor ketenmachtigingen (Bij uitbreiding naar meer schakels moeten de controles aangaande kennisgeving bij substitutie hier worden toegevoegd.). In het bijzonder dat een dienst "voor derden" mag worden uitgevoerd door betreffende gemachtigde en de mogelijkheid om de vertegenwoordigde dienstafnemer waarvoor de ketenmachtiging benut mag worden te specificeren;
- ondersteunen van het koppelvlak voor verificatie van de volgende schakel in geval van ketenmachtiging en de uitbreidingen voor het doorgeven van informatie over de intermediaire partij (zie Interface specifications HM-MR 1.7 chain authorization).

Werking SSO

Single Sign On is een functionaliteit die door alle eHerkenningsmakelaars ondersteund moet worden. Voor authenticatiediensten is het een aanvullende feature met de volgende verantwoordelijkheden.

Verantwoordelijkheden authenticatiedienst

Een authenticatiedienst mag uitvoerend natuurlijk personen opties bieden om aangelogd te blijven voor dienstverleners (SSO). Voor diensten waarvoor betrouwbaarheidsniveau 4 vereist is mag deze optie niet worden geboden. Indien deze optie wordt aangeboden moet een authenticatiedienst vanaf de eerste authenticatie met SSO het maximum AD-tijdsverloop bewaken. Een volgende authenticatie op basis van SSO zou moeten worden gegeven indien deze binnen dit maximum AD-tijdsverloop valt tenzij een logoutbericht is ontvangen of er sprake is van afgedwongen authenticatie. Na het ontvangen van een logoutbericht mag geen authenticatie op basis van SSO meer worden gegeven.

Hoe aansluiten op eHerkenning?

In de voorgaande hoofdstukken is beschreven hoe eHerkenning in het dagelijkse gebruik werkt. Om van eHerkenning gebruik te maken moeten dienstafnemers (bedrijven en andere organisaties) en dienstverleners aansluiten. Dat is in principe een eenmalige activiteit en wordt in dit hoofdstuk toegelicht. Partijen die eHerkenningsdiensten willen leveren conform het afsprakenstelsel, de deelnemers dus, doorlopen ook een aansluiting, zij treden toe tot het netwerk. Dit wordt in Aansluiten als deelnemer beschreven.

Bij dit toetreden speelt de beheerorganisatie. waarin de ondersteunende rollen aangaande beheer en toezicht zijn belegd, een belangrijke rol. Zie hiervoor Juridisch kader.

Aansluiten als dienstafnemer (bedrijf)

Dienstafnemers sluiten aan op eHerkenning door te zorgen dat zijzelf of vertegenwoordigers van de dienstafnemer beschikken over een voor eHerkenning bruikbaar authenticatiemiddel en door in geval van vertegenwoordiging ervoor te zorgen dat de hun vertegenwoordigingsbevoegdheden in een machtigingenregister vast zijn gelegd.

De relatie tussen de dienstafnemer en de middelenuitgevers en machtigingenregisters

Een dienstafnemer mag middelen bij meer dan één middelenuitgever aanschaffen en bevoegdheden in meerdere machtigingenregisters laten vastleggen. In het algemeen zal dat echter niet het geval zijn. Omdat de registratieprocedures voor het verkrijgen van authenticatiemiddelen en het vastleggen van bevoegdheden gedeeltelijk dezelfde gegevens betreffen kan het voorkomen dat middelenuitgever en machtigingenregister samenwerken door de benodigde registraties in één proces aan bedrijven aan te bieden.

Middelenuitgevers en machtigingenregisters hanteren gebruikersvoorwaarden en mogelijk is er sprake van een contract met de dienstafnemer. Deze contracten bevatten onder andere bepalingen over het zorgvuldig omgaan met authenticatiemiddelen, over aansprakelijkheid en over de kosten. Het afsprakenstelsel stelt minimumeisen aan deze voorwaarden omdat dit voor de betrouwbaarheid noodzakelijk is. De voorwaarden moeten naar het afsprakenstelsel verwijzen. Deze contracten leggen de verantwoordelijkheid voor het tijdig doorgeven van wijzigingen in de bevoegdheden (bijvoorbeeld bij uit dienst gaan) bij de dienstafnemer en indien relevant bij de uitvoerend natuurlijk persoon.

Wanneer een dienstafnemer het gebruik van eHerkenning wil beëindigen kan zij bevoegdheden en eventueel authenticatiemiddelen laten intrekken.

De verschillen in de registratieprocedures per betrouwbaarheidsniveau zijn te vinden in Informatiebeveiliging en privacy.

Verwerven van authenticatiemiddelen

Het netwerk voor eHerkenning is zo opgezet dat veel verschillende soorten authenticatiemiddelen gebruikt kunnen worden, bijvoorbeeld gebruikersnaam/wachtwoorden, card / card readercombinaties, VPN tokens, maar ook mobiele telefoons met TANs. Afhankelijk van de diensten waarvoor eHerkenning gebruikt gaat worden dienen de authenticatiemiddelen aan een bepaald betrouwbaarheidsniveau te voldoen. De beheerorganisatie maakt een steeds actueel overzicht van de tot eHerkenning toegelaten authenticatiemiddelen openbaar, zie www.eherkenning.nl/bedrijven/aanvragen/aanbieders.

Om een authenticatiemiddel te verwerven, selecteert de dienstafnemer een middelenuitgever en levert aan die middelenuitgever de gegevens van de uitvoerend natuurlijk persoon die het authenticatiemiddel gaat gebruiken. Conform de eisen van het betrouwbaarheidsniveau van het authenticatiemiddel wordt de identiteit van de uitvoerend natuurlijke persoon vastgesteld. Vervolgens wordt het authenticatiemiddel daadwerkelijk aan de uitvoerend natuurlijk persoon verstrekt. De procedure daarvoor varieert per betrouwbaarheidsniveau.

Hergebruik authenticatiemiddelen

Het is mogelijk dat de uitvoerend natuurlijk persoon reeds over een geschikt authenticatiemiddel beschikt. Om bestaande authenticatiemiddelen te hergebruiken binnen eHerkenning dient de partij die deze middelen uitgeeft en beheert toe te treden als deelnemer aan eHerkenning (zie Aansluiten als deelnemer) en wel (minstens) in de rol van middelenuitgever. Na die toetreding, waarmee ook aan de toetredingseisen is voldaan, kunnen reeds eerder door deze partij uitgegeven middelen gebruikt worden binnen eHerkenning op het betrouwbaarheidsniveau waar ze technisch en procedureel aan voldoen. Om zo'n eerder uitgegeven authenticatiemiddel daadwerkelijk in gebruik te nemen voor eHerkenning dient de uitvoerend natuurlijk persoon die dat wil de eerste keer een (aanvullende) eHerkenning-gebruiksovereenkomst voor dit middel af te sluiten.

Vastleggen bevoegdheden bij een machtigingenregister

Authenticatiemiddelen maken het mogelijk iemand in een elektronisch contact te herkennen. Om een uitvoerend natuurlijk persoon namens een dienstafnemer te laten handelen is het nodig dat die bevoegdheid wordt vastgelegd op een wijze die bij gebruik door eHerkenning raadpleegbaar is. Het is mogelijk om deze bevoegdheid te beperken tot één of meer vestigingen van de dienstafnemer. Het vastleggen van een bevoegdheid gebeurt doordat de dienstafnemer deze bevoegdheden en de gegevens over de personen die bevoegd zijn laat registeren in een machtigingenregister. Deze registratie moet door de dienstafnemer of door een daartoe bevoegde vertegenwoordiger van de dienstafnemer gebeuren. In het machtigingenregister wordt tevens de

koppeling gelegd tussen het authenticatiemiddel van de uitvoerend natuurlijk persoon en deze bevoegdheid. Op basis van die gegevens samen kan het netwerk met een bepaald betrouwbaarheidsniveau verklaren dat iemand met een bepaald authenticatiemiddel namens een bepaald bedrijf, eventueel beperkt tot één of meer vestigingen daarvan, mag handelen voor de afname van een bepaalde dienst.

De procedure voor het vastleggen van bevoegdheden varieert naar gelang het betrouwbaarheidsniveau. Hoe hoger het niveau, des te meer bewijzen dienen overlegd te worden. Indien een dienstafnemer meerdere verschillende uitvoerend natuurlijke personen met eHerkenning wil laten werken, kan het een beheerder laten vastleggen die de bevoegdheden van al deze gemachtigden beheert. Uiteraard dient de vastlegging van deze beheerder tenminste op hetzelfde betrouwbaarheidsniveau te gebeuren. De beheerorganisatie publiceert een actueel overzicht van de voor eHerkenning geschikte machtigingenregisters op www.eHerkenning.nl. Dit is hetzelfde overzicht als voor middelenuitgevers, de deelnemers maken zelf de gecombineerde proposities inzake authenticatiemiddelen en machtigingen inzichtelijk.

Aansluiten als dienstverlener

Dienstverleners gebruiken eHerkenning om een veilige toegang en gebruik van hun elektronische diensten door bedrijven mogelijk te maken. Daartoe neemt de dienstverlener het gestandaardiseerde koppelvlak van eHerkenning op in de toegang tot deze diensten. De dienstverlener heeft slechts met één rol van het netwerk te maken, de zogeheten eHerkenningsmakelaar. De dienstverlener selecteert een partij die deze eHerkenningsmakelaar levert en sluit daarmee een contract. De dienstverlener kan vervolgens aansluiten op het netwerk eHerkenning zodra zij haar systemen gereed heeft en er een positieve test op de werking van de eHerkenning koppelvlakspecificaties voor "Dienstverlener – eHerkenningsmakelaar" is uitgevoerd. De eHerkenningsmakelaar zorgt er vervolgens voor dat iedere keer dat de dienst wordt aangeroepen eerst via het netwerk voor eHerkenning de vereiste verklaringen worden geleverd.

Omdat het voor alle eHerkenningsmakelaars verplicht is alle achterliggende authenticatiediensten en machtigingenregisters te ontsluiten, kan de dienstverlener een eHerkenningsmakelaar selecteren ongeacht de toepassing of klantgroep.

Voorafgaand aan het aansluiten moet de dienstverlener bepalen welk betrouwbaarheidsniveau voor de diensten waarvoor eHerkenning wordt toegepast noodzakelijk is.
Dienstverleners geven bij registratie van dienst in de dienstencatalogus op of zij beogen een dienst met SSO toegankelijk te maken.

Als onderdeel van de aansluiting dient tevens bepaald te worden hoe de diensten die aangeboden worden gedefinieerd zijn, zodat machtigingenregisters bevoegdheden voor specifieke diensten kunnen vastleggen. Daarbij geeft de dienstverlener ook op welk soort dienstafnemers toegang kan krijgen tot de dienst.

In het contract met de eHerkenningsmakelaar kunnen zaken vastliggen aangaande de ondersteuning die geleverd wordt bij het realiseren van de technische aansluiting, aangaande het service level etc.

In Interface specifications DV-HM 1.7 is het koppelvlak tussen dienstverlener en eHerkenningsmakelaar technisch beschreven en de specificatie van de dienstencatalogus uitgewerkt.

Verantwoordelijkheden dienstverlener

Een dienstverlener:

- moet zich houden aan de technische beveiligingseisen van het toegepaste koppelvlak en aan de beveiligingsrichtlijnen van het NCSC;
- is zelf verantwoordelijk voor het controleren van de herkomst van ontvangen berichten;
- moet vanaf het moment dat een uitvoerend natuurlijk persoon toegang heeft, op basis van een vraag waarvoor SSO is toegestaan, een logoutknop bieden.

Aansluiten als deelnemer

Het netwerk voor eHerkenning is een netwerk waarmee meerdere partijen gezamenlijk eHerkenningsdiensten leveren. Voor de werking van het netwerk is het noodzakelijk dat per rol een bepaalde minimale functionaliteit geleverd wordt en zijn verbindingen tussen de systemen waarmee deze rollen worden gerealiseerd noodzakelijk. Deze zaken dienen voorafgaand aan het moment waarop een deelnemer toetreedt te worden ingericht. In Deelnemers: rollen en verantwoordelijkheden werden deze eisen per rol beschreven.

De juridische kant van de benodigde samenwerking en de toetredingseisen worden toegelicht in Juridisch kader. Het toetredingsproces wordt uitgewerkt in Proces toetreden.

Deelnemers worden betrokken in besturing op de verschillende niveaus. Deze afvaardiging kan getrapt plaatsvinden. Zie

Organen en taakverdeling.

Aansluiten op attribuutverstrekking

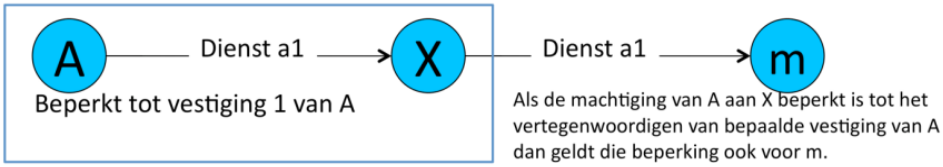
Voordat attribuutverstrekking toegestaan is, dient de uitvoerend natuurlijk persoon of vertegenwoordigde dienstafnemer/intermediair hiervoor expliciet user consent te geven aan de betreffende deelnemer. De uitvoerend natuurlijk persoon kan toestemming geven voor het verstrekken van gegevens bij gebruik van zijn persoonsgebonden authenticatiemiddel. Alternatief kan het de wettelijke vertegenwoordiger of beheerder of gemachtigde van een vertegenwoordigde dienstafnemer/intermediaire partij zijn die deze user consent geeft voor gegevens aangaande de vertegenwoordigde dienstafnemer respectievelijk intermediaire partij of de met de machtiging verbonden context. Deze context kan zowel de vertegenwoordigde dienstafnemer/intermediair betreffen als de gemachtigde.

Het is niet toegestaan aan uitvoerend natuurlijk personen of wettelijke vertegenwoordigers vooraf globaal toestemming te vragen voor verstrekken van alle mogelijke attributen. De user consent dient specifiek te zijn voor een bepaald attribuut en mag beperkt zijn tot een bepaalde machtiging. Nadat de eerste keer met de verstrekking van een bepaald attribuut is ingestemd mag de betrokkene aangeven dat dit in vervolg voor dat specifieke doel niet opnieuw gevraagd hoeft te worden. Het bewaren van deze instelling is gebonden aan de termijn als gespecificeerd in BR456 Doorlooptijd van mutaties van bevoegdheden (PT).

Aansluiten op ketenmachtigingen

Bij ketenmachtigingen functioneert de "laatste" schakel, de machtiging aan de uitvoerende natuurlijk persoon, net als bij een enkelvoudige machtiging (wanneer er geen sprake is van een keten). De registraties hiervoor worden uitgevoerd onder verantwoordelijkheid van de uitvoerende dienstafnemer conform Aansluiten als dienstafnemer (bedrijf).

De andere schakels kunnen op een ander moment worden vastgelegd. Het kan zijn dat deze schakel(s) in een ander machtigingsregister worden vastgelegd. In alle gevallen blijft de eis dat een bevoegdheid alleen door of namens de wettelijke vertegenwoordiger van de vertegenwoordigde partij kan worden opgegeven aan het machtigingsregister.



Het is mogelijk om deze bevoegdheid te beperken tot één vestiging van de vertegenwoordigde dienstafnemer. Dit leidt tot een machtigingsketen op grond waarvan een uitvoerend natuurlijk persoon de betreffende vestiging van de vertegenwoordigde dienstafnemer mag vertegenwoordigen.

De procedure voor het vastleggen van bevoegdheden varieert naar gelang het betrouwbaarheidsniveau. Hoe hoger het niveau des te meer bewijzen dienen overlegd te worden. Een vertegenwoordigde dienstafnemer kan een beheerder laten vastleggen die zijn bevoegdheden beheert. Uiteraard dient de vastlegging van deze beheerder tenminste op hetzelfde betrouwbaarheidsniveau te gebeuren. De beheerorganisatie publiceert een actueel overzicht van de voor eHerkenning geschikte machtigingenregisters die ketenmachtigingen ondersteunen op www.eHerkenning.nl.

Bijlage - Overzicht gebruikte standaarden

Deze bijlage bevat een lijst met externe standaarden die in het afsprakenstelsel benut worden. In deze lijst wordt opgenomen welke versie van de standaard toegepast wordt in deze versie van het afsprakenstelsel. In deze lijst wordt tevens de samenhang met voor Nederlandse overheid geldende lijsten van standaarden van College Standaardisatie weergegeven. In de tekst van het afsprakenstelsel worden de versies van standaarden niet steeds herhaald. Indien er van een standaard een nieuwe versie is dan wordt het toepassen van die nieuwe versie via het gewone beheerproces behandeld. Indien het een nieuwe versie betreft waarvoor een pas-toe-of-leg-uit regime geldt dan zal dat een belangrijk argument zijn bij het behandelen van het voorstel om de nieuwe versie toe te passen.

- CAdES: uitbreiding op de CMS Signatures standaard voor het formaat van geavanceerde elektronische handtekeningen. Binnen de EU in de besluitvoorbereiding gekozen als één van de standaarden voor het formaat van geavanceerde of gekwalificeerde elektronische handtekeningen (ETSI TS 101 733)
- CMS (RFC 3852) Signatures: standaard voor het digitaal ondertekenen of versleutelen van een willekeurige berichtinhoud
- DSS: protocol voor het zetten of valideren van een digitale handtekening

- ETSI TS 101 456: eisen aan certificaatuitgevende instanties van gekwalificeerde certificaten
- ETSI TS 102 042: eisen aan certificaatuitgevende instanties
- ETSI TS 102 231: Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information: standaard voor specificatie van een lijst per EU-lidstaat met benoeming van partijen die gekwalificeerde certificaten uitgeven
- HTTP/1.1: protocol voor communicatie tussen een webclient en server
- NEN-ISO/IEC 27001:2005: Managementsystemen voor informatiebeveiliging - Eisen
- NEN-ISO/IEC 27002: Code voor informatiebeveiliging
- NORA 3.0, de Nederlandse Overheid Referentie Architectuur: set aan inrichtingsprincipes, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid
- OSB / DigiKoppeling: Overheidsservicebus, set gestandaardiseerde koppelvlakken voor gebruik binnen de overheid
- PAdES: specificatie voor het formaat van geavanceerde elektronische handtekeningen in PDF. Omvat ISO 32000-1. Binnen de EU in de besluitvoorbereiding gekozen als één van de standaarden voor het formaat van geavanceerde of gekwalificeerde elektronische handtekeningen (ETSI 102 778)
- PKIoverheid Programma van Eisen versie 3.3 (juli 2012): onder meer een set afspraken omtrent gebruik van certificaten voor communicatie binnen en met de overheid.
- RFC 3161: gestandaardiseerde manier van het zetten van een tijdstempel ten behoeve van een digitale handtekening
- SAML: XML gebaseerde standaard voor het uitwisselen van identiteitsinformatie zoals authenticatie, bevoegdheden en attributen tussen verschillende domeinen
- SOAP: protocol voor het uitwisselen van gestructureerde informatie ten behoeve van webservices
- SSL/TLS 1.0 en hoger: encryptie protocollen voor het beveiligen van communicatie over netwerken
- STORK Quality authenticator scheme D2.3 versie 1.7
- UDDI: op XML gebaseerd register waarmee bedrijven zichzelf en hun services vindbaar en kenbaar kunnen maken
- WBP AV23: Handreiking "Achtergrondstudies en Verkenningen 23" - College Bescherming Persoonsgegevens
- Webrichtlijnen versie 2.02 - 1 juli 2011
- X.509: gestandaardiseerde manier voor het opslaan van certificaatinformatie ten behoeve van een
- Public Key Infrastructure
- XACML 2.0: open standaard om richtlijnen met betrekking tot toegang te definiëren en deze te bevragen
- XAdES: uitbreiding op de XML Digital Signature standaard voor het formaat van geavanceerde elektronische handtekeningen in XML. Binnen de EU in de besluitvoorbereiding gekozen als één van de standaarden voor het formaat van geavanceerde of gekwalificeerde elektronische handtekeningen
- XML: gestructureerd documentformaat
- XML Schema: een taal voor het beschrijven van de structuur van XML documenten
- XML Signature: standaard die beschrijft hoe digitale handtekeningen over XML documenten gezet kunnen worden
- XML Encryption: standaard die beschrijft hoe XML documenten versleuteld kunnen worden
- XSLT: taal die gebruikt wordt om XML documenten om te zetten in anders gevormde XML documenten

Bijlage - Toepassingen uitgangspunten en randvoorwaarden

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel
1. Het netwerk voor eHerkenning moet de mogelijkheid bieden om zowel bestaande als nieuwe methoden en oplossingen voor identificatie, authenticatie en autorisatie van natuurlijke personen in hun rol als vertegenwoordiger van een bedrijf of instelling te gebruiken.	De keuze voor de netwerk oplossing (Hoe werkt eHerkenning?) en Deelnemers: rollen en verantwoordelijkheden waarin per rol meerdere deelnemers naast elkaar mogen bestaan en het feit dat het afsprakenstelsel alleen datgene beschrijft wat minimaal noodzakelijk is voor werkende eHerkenningsdiensten maakt hergebruik van bestaande authenticatiemiddelen mogelijk. Toepassen van (bestaande) bedrijfseigen voorzieningen is voorzien maar nog niet uitgewerkt.
2. Het netwerk voor eHerkenning moet bedrijven en instellingen de mogelijkheid bieden om machtigingen van personen te registreren en te onderhouden.	De wijze waarop het netwerk hierin voorziet wordt op hoofdlijnen beschreven in Aansluiten als dienstafnemer (bedrijf) en voorbeelden zijn gegeven in Use cases. Het afsprakenstelsel laat de wijze waarop deelnemers de registratieprocessen vormgegeven vrij en beschrijft enkel de eisen waaraan voldaan moet worden om authenticatiemiddelen en bevoegdheden op een bepaald betrouwbaarheidsniveau te laten classificeren in deel Informatiebeveiliging.

3. Binnen het netwerk voor eHerkenning moeten de verantwoordelijkheden voor het registreren en onderhouden van machtigingen en het authenticeren van natuurlijke personen als twee aparte functies in het netwerk kunnen worden belegd.	Het netwerk onderkent losstaande rollen (Deelnemers: rollen en verantwoordelijkheden), waaronder deze twee en beschrijft verantwoordelijkheden, functies en eisen uitgesplitst naar deze rollen (Aansluiten als deelnemer). Wat betreft de betrouwbaarheidsniveaus wordt onderscheid gemaakt tussen de toepassing van het Europese STORK raamwerk voor authenticatiemiddelen (zie STORK niveaus) en de voor eHerkenning specifieke toepassing op het registreren en onderhouden van bevoegdheden in deel Informatiebeveiliging.
4. Het netwerk voor eHerkenning moet aansluiten bij reeds bestaande en bewezen technologische standaarden en toepassingen.	Bestaande authenticatiemiddelen en bijbehorende toepassingen kunnen via de rollen van middelenuitgever en authenticatiedienst worden ontsloten. Voor berichtenverkeer binnen het netwerk en naar de gebruikers wordt de SAML standaard conform de lijst van het Forum Standaardisatie toegepast. Op specifieke punten wordt gebruik gemaakt van de uitbreidingsmogelijkheden binnen de SAML standaard. Dat betreft uitbreidingen die niet als "bewezen" beschouwd kunnen worden. Wel kan gesteld worden dat de proefimplementaties voldoende ruimte bieden om deze aspecten te testen. Verder wordt op specifieke punten de XACML standaard toegepast op een wijze waarvoor hetzelfde geldt. De volledige lijst van toegepaste standaarden is te vinden in Bijlage – Overzicht gebruikte standaarden.
5. Rollen, rechten en verantwoordelijkheden van partijen moeten nauwkeurig worden beschreven in het afsprakenstelsel.	Deze beschrijving is te vinden in Deelnemers: rollen en verantwoordelijkheden. Op basis van de procesbeschrijvingen in het Operationeel handboek is vastgelegd welke functionaliteit de verschillende rollen in detail leveren. De verantwoordelijkheden aangaande de beheerorganisatie zijn uitgewerkt in het Juridisch kader. Tenslotte bepaalt het afsprakenstelsel dat gewerkt wordt met modelcontracten. In deze modelcontracten en de statuten van de beheerorganisatie ligt een nadere juridische uitwerking van rechten en verantwoordelijkheden vast.
6. Binnen het netwerk voor eHerkenning moeten varianten mogelijk zijn voor de elektronische herkenning van bedrijven en instellingen en moet de mogelijkheid blijven bestaan voor het leveren van additionele diensten met mogelijk toegevoegde waarde door partijen in het netwerk.	Aangezien het afsprakenstelsel alleen de minimaal noodzakelijke elementen van het netwerk beschrijft en de voor functioneren van het netwerk noodzakelijke koppelvlakken geeft, kunnen deelnemers per rol varianten implementeren en variëren door diensten aan te bieden die meer dan één rol omvatten. Daarnaast omvat de netwerkopzet een routeringsfunctie (de eHerkenningsmakelaar) die achtereenvolgens de informatie die benodigd is voor een eHerkenningsdienst ophaalt bij de verschillende andere rollen. Aanvullende diensten kunnen worden toegevoegd zonder het in het afsprakenstelsel vastgelegde deel te beïnvloeden door de eHerkenningsmakelaar nog andere diensten (c.q. rollen) die al dan niet onderdeel van het afsprakenstelsel worden (zoals een ondertekendienst) te laten uitvragen.
7. Binnen het netwerk voor eHerkenning moet sprake zijn van zorgvuldige afhandeling van gegevens met het oog op privacy, dataminimalisatie en veiligheid.	De in deel Informatiebeveiliging weergegeven betrouwbaarheidsniveaus bieden de basis voor proportionele beschouwing van welk niveau van veiligheid voor welke toepassing nodig is. In de toetredingsprocedure wordt op diverse manieren gecontroleerd of de processen en systemen dienovereenkomstig zijn ingericht. Ten behoeve van dataminimalisatie wordt voor de identificerende kenmerken van natuurlijk personen gebruik gemaakt van privacy enhancing technieken in de vorm van pseudoniemen. De scheiding van verantwoordelijkheden per rol maakt mogelijk dat gegevens enkel in die rol worden verwerkt en vastgelegd waar dit strikt nodig is. Voor deze versie is de beschrijving beperkt tot de situaties waarin de dataminimalisatie maximaal is doorgevoerd (maximale privacybescherming). Door dit als basis te nemen en in latere versies uitgebreidere diensten te definiëren die voor die situaties waarin de dienstverlener de daartoe benodigde wettelijke toestemming heeft de pseudoniemen aan elkaar relateren of omzetten in een BSN is sprake van een architectuur die in de basis BSN loos en op basis van maximale privacy functioneert maar – op basis van specifieke toestemming van de betrokken natuurlijk persoon – uitgebreidere persoonsgegevens kan leveren. Deze uitbreiding is beschreven in de vorm van attribuutverstrekking en identificerende kenmerken voor specifieke beroepsgroepen naast het specifiek pseudoniem.

8. Het netwerk voor eHerkenning moet optimale keuzevrijheid voor bedrijven en instellingen en overheidsdienstverleners bieden.	Aannemende dat er daadwerkelijk een markt met per rol meerdere concurrerende aanbieders tot stand komt, bestaat er keuzevrijheid aan beide zijden van het netwerk: zowel voor bedrijven die kunnen kiezen ten aanzien van te gebruiken authenticatiemiddelen (en daarmee voor middelenuitgevers en authenticatiediensten) en het te gebruiken machtigingenregister, als voor overheidsdienstverleners die kunnen kiezen uit meerdere eHerkenningsmakelaars. Door alle-op-alle relaties tussen beide zijden van het netwerk te verplichten (Deelnemers: rollen en verantwoordelijkheden) wordt het ontstaan van geïsoleerde eilanden binnen het netwerk voorkomen. In de governance van de beheerorganisatie zijn waarborgen opgenomen die eerlijk speelveld voor de deelnemers borgen, zoals benoemingsrecht en goedkeuring stelselwijzigingen door EZ, transparante toetredingsprocedure, klachtencommissie en bepalingen over openbaarmaking en geheimhouding.
9. In het kader van non-discriminatie moet iedereen die dit wil mogen toetreden tot het netwerk voor eHerkenning. Toetreding moet geschieden op basis van gelijke condities en onder de voorwaarde dat de gemaakte afspraken in het afsprakenstelsel worden nagekomen.	Het afsprakenstelsel stelt forse eisen aan partijen die willen toetreden. Deze eisen zijn gezien het belang van vertrouwen proportioneel en voor allen gelijk. De klachtenregeling, uitgevoerd door de onafhankelijke Klachten- en geschillencommissie, vormt het interne instrument om daarop toe te zien. De eisen zelf in het afsprakenstelsel zijn op transparante wijze na een formele marktconsultatie tot stand gekomen.
10. In de opzet van het netwerk voor eHerkenning moet de waarborging van de gemaakte afspraken en het nakomen daarvan worden geregeld.	Na de toetreding waarin eisen worden gecontroleerd dienen, deze controles worden tenminste iedere 3 jaar herhaald, relevante controles worden bij wijziging herhaald en voor een deel van de eisen gelden externe certificaties met een eigen geldigheidsduur.
11. Er moet zoveel mogelijk aansluiting worden gezocht bij internationale ontwikkelingen. Hierbij zal zoveel mogelijk worden gewerkt met oplossingen die gangbaar zijn binnen de EU-context.	Toepassing van de STORK betrouwbaarheidsniveaus vloeit voort uit EU standaardisatie. De verdere standaardisatie van de koppelvlakken van eHerkenning wordt via het Forum Standaardisatie ingebracht, nu reeds wordt voor de koppelvlakken een standaard van de vastgestelde lijst (SAML) toegepast.
12. De rollen binnen het afsprakenstelsel moeten zoveel mogelijk worden ingevuld door marktpartijen. Indien voor de invulling van bepaalde rollen onvoldoende interesse is bij marktpartijen, zal de overheid deze rollen (doen) invullen.	Voor alle rollen zijn meerdere marktpartijen toegetreden die actief bijdragen aan verdere uitwerking van het afsprakenstelsel.
13. Het afsprakenstelsel moet dusdanig worden opgesteld dat er sprake is van een 'level playing field' en er gelijke kansen zijn voor partijen om mee te doen in het netwerk voor eHerkenning.	Zie punt 9.

14. Het afsprakenstelsel is de basis voor een netwerk voor eHerkenning van business-to-government. Het afsprakenstelsel kan daarnaast wellicht op termijn gebruikt worden voor het bieden van een oplossing voor de herkenningsbehoefte voor government-to-government en business-to-business.	Het afsprakenstelsel bevat geen elementen die toepassing in B2B gebruik verhinderen, evenmin voor G2G. Wel zullen voor B2B gebruik mogelijk nadere eisen gesteld moeten worden en mogelijk aangepaste modelcontracten moeten worden opgesteld. Tevens is verdere uitwerking van het OIN nummerformaat in relatie tot gebruik van KvK nummer, RSIN nummer en verdere Europese standaardisatie van belang.
15. Alle bedrijven en instellingen moeten binnen het netwerk voor eHerkenning terecht kunnen bij alle aangesloten overheidsdienstverleners.	De verplichte alle-op-alle relaties in het netwerk maken dit mogelijk (Deelnemers: rollen en verantwoordelijkheden).
16. Het herkenningsproces moet worden ingericht volgens het privacy by design principe. Dit houdt in dat persoonsgegevens niet vaker mogen worden gebruikt dan noodzakelijk is voor het doel waarvoor de persoonsgegevens verkregen worden. Dit is conform de Wet bescherming persoonsgegevens.	Zie punt 7. De toegepaste privacy enhancing technieken leiden er toe dat alleen die gegevens die per se nodig zijn voor een bepaalde dienst worden uitgewisseld. De basiswerking van eHerkenning is dat daarbij geen uniek identificerend kenmerk van uitvoerend natuurlijk personen wordt verstrekt. In latere uitbreidingen kan dit als een extra laag, die enkel met toestemming van de betrokkene wordt benut, worden toegevoegd.
17. Wettelijke en professionele normen voor informatiebeveiliging.	Hoofdstuk 6 beschrijft de belangrijkste normen die worden toegepast en de afspraken ten aanzien van een netwerkbreed beveiligingsplan en een normenkader waarin meer gedetailleerde eisen gesteld kunnen worden. Er is bepaald dat continue verantwoording over beveiliging plaatsvindt. Het afnemen van diensten van Govcert door de beheerorganisatie wordt momenteel verder onderzocht.
18. Nederlandse wet- en regelgeving voor zover van toepassing.	Bij uitwerking van het Juridisch kader is rekening gehouden met toepasselijke wet- en regelgeving.
19. Europese regelgeving voor zover van toepassing.	Bij uitwerking van het Juridisch kader is rekening gehouden met toepasselijke wet- en regelgeving.
20. Er moet worden waar mogelijk gebruik gemaakt van open standaarden (comply or explain).	Alle in Bijlage - Overzicht gebruikte standaarden genoemde standaarden welke in het afsprakenstelsel expliciet of impliciet (kunnen) worden toegepast zijn open. Het afsprakenstelsel vereist op geen enkele manier het gebruik van enige standaard of werkwijze die niet open is. Echter wat betreft de interne werking van systemen van deelnemers verbiedt het afsprakenstelsel de toepassing van gesloten standaarden niet. Het afsprakenstelsel zelf tenslotte is, als samenstelsel waarin voorgeschreven wordt hoe meerdere standaarden in een specifieke onderlinge samenhang moeten worden toegepast, een "standaard". Het afsprakenstelsel zelf en latere versies wordt openbaar gemaakt en om verdere standaardisatie te bevorderen wordt met het Forum Standaardisatie samengewerkt om de aspecten van het "afsprakenstelsel als standaard" die daarvoor in aanmerking komen formeel te standaardiseren.

21. Er is een level playing field (gelijk speelveld) aanwezig voor het (kunnen) inzetten van open source-oplossingen.	De in het afsprakenstelsel toegepaste open standaarden leveren geen belemmeringen op voor het toepassen van open standaarden bij de gebruikers van eHerkenning of bij de deelnemende marktpartijen. Deze laatste worden uiteraard vrijgelaten in hun eigen afweging om hun rollen al dan niet op basis van open source oplossingen te implementeren. De testvoorziening van het netwerk die in beheer is bij de beheerorganisatie is geheel op basis van open source oplossingen gerealiseerd, hetgeen een aanvullend bewijs levert voor het feit dat er geen belemmeringen in het afsprakenstelsel zitten ten aanzien van open source oplossingen. Afhankelijk van de vraag welke oplossingen door marktpartijen en dienstverleners in de proefimplementatie worden ingezet, komen daaruit gegevens over elementen in de koppelvlakken die bepaalde oplossingen (al dan niet gesloten) zouden kunnen bevoordelen. (Op voorhand is niet uit te sluiten dat er elementen in de koppelvlakken blijken te zitten die in bepaalde implementaties meer of minder goed conform de officiële standaard zijn geïmplementeerd. Zowel bij gesloten source als bij open source oplossingen kan het voorkomen dat dergelijke elementen bestaan en dat dit "toevallig" leidt tot het onbedoeld uitsluiten van een specifieke oplossing. Dergelijke onvolkomenheden kunnen in het geval van open source producten met een goed functionerende community en in het geval van gesloten source producten van een leverancier die bereidwillige service verleent worden opgelost. Dit aspect kan in de evaluaties van de proefimplementaties nader worden beschouwd en is ook reeds geëvalueerd in de technische review door Novay en Surfnet.)

Begrippenlijst eHerkenning

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Binnen eHerkenning wordt één begrippenlijst gehanteerd. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden. Datzelfde geldt ook andersom: waar in dit document de zelfstandige-naamwoords-vorm van een werkwoord wordt gehanteerd, heeft deze dezelfde betekenis als het gedefinieerde werkwoord.

Aanvullende feature

Een in het Afsprakenstelsel (AS) beschreven dienst of aanvulling op andere dienst waarvan het deelnemers vrij staat deze al dan niet aan te bieden, welke echter indien aangeboden conform de in het afsprakenstelsel opgenomen eisen moet worden aangeboden.

Afgeschermde kopie WID

Kopie WID document waarbij de bijzondere persoonsgegevens, te weten pasfoto, BSN en nationaliteit, zijn afgeschermd.

Afsprakenstelsel (AS)

Het geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek. procedures en regels aangaande het Netwerk (voor eHerkenning) in een bepaalde vastgestelde versie. Het doel is betrouwbare authenticatie en verstrekking van identiteitsinformatie op basis van de eHerkenningsdiensten van een goed gereguleerd netwerk voor eHerkenning.

Akte

Een getekend geschrift dat een bewijsbestemming heeft. Een akte heeft als bijzondere eigenschap dat deze in een juridische procedure dwingende bewijskracht heeft. Een elektronische vorm hiervan kan een document zijn, getekend met een elektronische handtekening volgens de wet op de elektronische handtekeningen.

Attribuutcatalogus (AC)

Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle via het netwerk verkrijgbare optionele attributen bevat inclusief de aanduiding waarmee zij opgevraagd kunnen worden.

Authenticatie (authenticeren)

De controle (het staven) van de (een) geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau.

Authenticatiedienst (AD)

Een vereiste Rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de natuurlijk persoon gebruikte Authenticatiemiddel.

Authenticatiemiddel

Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.

Authenticatieverklaring

Een Verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een Authenticatie (authenticeren) die heeft plaatsgevonden in de context van een bepaalde handeling of dienst.

Autorisatie

Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren.

Bedrijf

Dienstafnemer

Beheerder

Een uitvoerend natuurlijk persoon met de specifieke bevoegdheid om namens een dienstafnemer bevoegdheden van andere personen te laten registreren, schorsen, in te trekken of anderszins bijbehorende registratieprocessen uit te voeren.

Beheerorganisatie (BO)

De Beheerorganisatie van het Afsprakenstelsel die verantwoordelijk is voor het faciliteren van het beheer en de doorontwikkeling van het Afsprakenstelsel, alsmede de controle op en het monitoren van de naleving van het Afsprakenstelsel door de Dienstverleners en de Deelnemers op basis van het door eHerkenning (eH) vastgestelde nalevingsbeleid.

Beroepsbeoefenaar

Een natuurlijk persoon die een gereglementeerd beroep uitoefent overeenkomstig met EU richtlijn 2005/36/EG (http://ec.europa.eu/internal_market/qualifications/policy_developments/legislation_en.htm http://ec.europa.eu/internal_market/qualifications/policy_developments/legislation_en.htm)

Betrouwbaarheidsniveau

Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het middel zelf en het gebruik van het middel (het authenticatiemechanisme).

Bevoegdheid

Het recht van een persoon om een handeling te verrichten.

BSN

Burgerservicenummer: Persoonlijke identificatie van de Nederlandse overheid voor natuurlijke personen.

Certificatie (certificeren)

Een brede (zowel technisch als niet-technisch) evaluatie van de beveiligingseigenschappen van een informatiesysteem of, zoals in het kader van de PKI voor de overheid, een managementsysteem uitgevoerd door een onafhankelijke derde. Certificatie wordt uitgevoerd als een onderdeel van een proces, waarbij wordt nagegaan in welke mate een managementsysteem overeenkomt met een vastgestelde verzameling van eisen (ETSI TS 101 456).

Controle van bevoegdheid

Controle van bevoegdheid zoals deze blijkt uit een in een machtigingenregister geregistreerde vertegenwoordigingsrelatie. Reden van het onderscheid tussen machtiging sec en controle van bevoegdheid is dat de machtiging ook kan bestaan los van het machtigingenregister.

Dataminimalisatie

Het zodanig inrichten van een gegevensverwerking dat er zo weinig mogelijk identificerende gegevens bekend hoeven te zijn bij zo weinig mogelijk partijen.

Deelnemer

Een partij die conform hetgeen daarover in het afsprakenstelsel is vastgelegd één of meer rollen vervult binnen het netwerk voor eHerkenning. Deelnemers kunnen rollen voor eigen gebruik en/of voor gebruik door derden vervullen.

Dienstafnemer

Een partij die eHerkenning gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm

Dienstencatalogus (DC)

Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle diensten, inclusief de onderverdeling in subdiensten en eventuele samengestelde diensten bevat, welke voor het vastleggen van bijzondere machtigingen, dat wil zeggen machtigingen die zich beperken tot bepaalde diensten, minimaal noodzakelijk is.

Dienstverlener (DV)

Een Partij die elektronische diensten aanbiedt aan dienstafnemers waarvoor eHerkenningsdiensten voorwaardelijk zijn. Dit kan zowel een Overheids-dienst-verlener als een private zijn.

eHerkenning (eH)

Herkenning

eHerkenningsdiensten

Diensten voor Herkenning, te weten: Authenticatie (authenticeren), controle van Bevoegdheid, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.

eHerkenningsmakelaar (HM)

Een vereiste Rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die het single point of contact vormt waarlangs dienstverleners eHerkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de dienstverleners te ontkoppelen van de interne berichten binnen het netwerk en die optreedt als routeerder naar alle deelnemende authenticatiediensten, machtigingenregisters en (toekomstige) ondertekendiensten.

eHerkenningsnetwerk

Synoniem voor Netwerk (voor eHerkenning).

Gebruiker

Een dienstverlener of dienstafnemer die eHerkenning gebruikt om respectievelijk de toegang tot een van haar diensten mee te beveiligen of toegang te vragen tot een dergelijke dienst met het oog op het afnemen van die dienst.

Geïnformeerde uitdrukkelijke toestemming

Gemachtigde

De partij die (op grond van wet of machtiging c.q volmacht) bevoegd is om in naam van de vertegenwoordigde bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de vertegenwoordigde.

Handelsregister

Voor in Nederland gevestigde bedrijven is dit de Nederlandse basisregistratie van ondernemingen en rechtspersonen die inschrijfplichtig zijn in Nederland, voor andere EU lidstaten is dat het vergelijkbare openbare register van het betreffende land.

Hergebruik

Hergebruik van authenticatiemiddelen: Het toepassen van eerder voor andere doeleinden en onder eigen voorwaarden uitgegeven authenticatiemiddelen binnen eHerkenning op basis van aanmelding van het authenticatiemiddel door de houder ervan.

Herkenning

In deze context wordt onder (electronische) herkenning verstaan: ieder van de functies van het netwerk voor eHerkenning gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen dienstverleners en bedrijven en de daarin betrokken uitvoerend natuurlijke personen.

Identificatie (identificeren)

Het noemen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden. In de context van eHerkenning gaat het over identificatie van partijen.

Identificerend kenmerk

Een reeks karakters waarmee iets of iemand (een partij) in een bepaalde context uniek wordt aangeduid. Indien het kenmerk enkel uit cijfers bestaat wordt ook van Identificerend nummer gesproken.

Identificerend nummer

Een Identificerend kenmerk dat bestaat uit cijfers

Identiteit

De volledige maar dynamische set van alle attributen behorende bij een bepaalde entiteit die het mogelijk maakt betreffende entiteit van andere te onderscheiden. Elke entiteit heeft maar één identiteit. De identiteit behoort toe aan de entiteit.

Identity provider (SAML)

Een vorm van een service provider die identiteitsgegevens aanmaakt, onderhoud en beheert ten behoeve van partijen en hen authenticeert ten behoeve van andere service providers in de context van een federatie.

Intermediaire partij

Een partij die bevoegd is te handelen op grond van een aan hem verleende machtiging en die deze machtiging op grond van substitutie heeft doorgegeven aan een derde.

Intern pseudoniem

Pseudoniem dat gedurende een langere periode toegepast wordt en enkel binnen eHerkenning gebruikt wordt zonder een specifiek werkingsdomein.

Ketenverklaring

Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een keten van bevoegdheden die aantoont dat een bepaalde uitvoerend natuurlijk persoon een bepaalde vertegenwoordigde dienstafnemer vertegenwoordigt ten behoeve van een bepaalde handeling of dienst op grond van controle van de gehele keten in machtigingenregisters

Klachten- en geschillen-commissie

Een onafhankelijke klachten- en geschillencommissie die tot taak heeft het afhandelen van klachten en geschillen die tussen partijen ontstaan bij de uitvoering van eHerkenningsdiensten en niet in onderling overleg door de partijen kunnen worden opgelost. De klachten- en geschillencommissie [A1] is ingesteld door het Ministerie van EZ, op voordracht van de Stelselraad.

Koppelvlak

Een koppelvlak is de verbinding tussen twee systemen. Om een koppelvlak te realiseren zijn nodig (a) specificaties en (b) implementaties in mensen en middelen. In de context van eHerkenning (eH) levert het Afsprakenstelsel (AS) de specificaties (a), het netwerk verzorgt de implementaties (b).

Machtiging (machtigen)

Een herroepbare bevoegdheid die een vertegenwoordigde verleent aan een andere partij (de gemachtigde) om in naam van eerstgenoemde rechtshandelingen te verrichten.

Machtigingenregister (MR)

Een vereiste Rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de Uitvoerend natuurlijk persoon (UNP) verstrekken van machtigingsverklaringen).

Machtiging-verklaring

Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een in een geregistreerde machtiging zoals deze gecontroleerd is in een Machtigingen-register ten behoeve van een bepaalde handeling of dienst.

Middelenuitgever (MU)

Een vereiste rol binnen het netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het uitgeven van Authenticatiemiddelen conform de eisen van het gespecificeerde Betrouwbaarheidsniveau.

Natuurlijk persoon

Een individueel menselijk wezen en subject van rechten en drager van plichten.

Netwerk (voor eHerkenning)

De verzameling onderling verbonden componenten die gereguleerd worden door het Afsprakenstelsel (AS) en gezamenlijk eHerkenningsdiensten leveren en daartoe bestaan uit tenminste één invulling door een Deelnemer van de rollen eHerkenningsmakelaar (HM), Machtigingenregister (MR), Authenticatiedienst (AD) en Middelenuitgever (MU), mogelijk aangevuld met verdere rollen voor eHerkenningsdiensten zoals een ondertekendienst, hun onderlinge verbindingen, de verbindingen tot en met het koppelvlak met die

Niet natuurlijk persoon

Hetzij een rechtspersoon, hetzij een samenwerkingsverband van natuurlijke personen en/of niet-natuurlijke personen.

Onderneming

Een onderneming in de zin van de Handelsregisterwet 2007 of een onderneming conform de voorschriften van een andere EU lidstaat welke ingeschreven is in het handelsregister van betreffende lidstaat.

Ondertekendienst

Een (voorziene) rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het doen van de wilsuiting, het valideren ervan en het verstrekken van het bijbehorende associatiebewijs.

Overheidsdienstverlener

Een Dienstverlener (DV) die onderdeel van de Nederlandse overheid is. Voor zover zaken zowel overheidsdienstverleners als private dienstverleners kunnen betreffen wordt gesproken van “dienstverleners”.

Partij

Een persoon of samenwerkingsverband die in de context van eHerkenning (eH) voorkomt of zou kunnen voorkomen en die zonodig uniek geïdentificeerd en geauthenticeerd kan worden.

PKI (Public Key Infrastructure)

Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op ‘public key cryptografie’. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

Privépersoon

Een Natuurlijk persoon, echter uitsluitend voor situaties en dienstafnames bij niet-overheidsdienstverleners c.q. in B2C diensten.

Pseudoniem

Een arbitrair Identificerend kenmerk dat op basis van een bewerking van een ander identificerend kenmerk wordt geproduceerd op een wijze die steeds hetzelfde pseudoniem oplevert bij hetzelfde kenmerk zonder dat deze laatste herleid kan worden uit het pseudoniem. Er kunnen meerdere pseudoniemen bestaan bij één Identificerend kenmerk, ieder met een eigen werkingsdomein. In dat geval zijn twee pseudoniemen van hetzelfde kenmerk in verschillende domeinen niet aan elkaar te relateren.

Rechtspersoon

Een juridische eenheid en subject van rechten en drager van plichten. Iets is een rechtspersoon op grond van de wet of omdat het conform wettelijke vereisten is ontstaan, een rechtspersoon heeft een bepaalde rechtsvorm.

Rol

Eén van de verantwoordelijkheden die binnen het Netwerk (voor eHerkenning) voorkomt die gezamenlijk met de andere rollen eHerkenningsdiensten levert.

Service provider (SP)

Een rol die vervuld wordt door een afgebakend en actief onderdeel van een systeem dat diensten aanbiedt aan partijen of aan andere onderdelen van dat systeem.

Single Sign On (SSO)

Een functie die door eHerkenning (eH) wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel, waardoor een authenticatie van een uitvoerend natuurlijk persoon wordt hergebruikt, waardoor deze uitvoerend natuurlijk persoon niet opnieuw hoeft in te loggen.

Specifiek pseudoniem

Pseudoniem dat gedurende een langere periode toegepast wordt in een specifiek werkingsdomein. Een dienstverlenerspecifiek pseudoniem is steeds hetzelfde voor dezelfde Dienstverlener (DV) in wiens context het gebruikt wordt, een dienstafnemerspecifiek pseudoniem is steeds hetzelfde voor de context van één dienstafnemer etc.

Stelselraad eHerkenning

Het strategische overleg inzake de publiek- private samenwerking ten behoeve van eHerkenning, waarvoor de beheerorganisatie het secretariaat voert en waarvoor de minister van Economische Zaken een onafhankelijke voorzitter benoemt en het Instellingsbesluit besturing eHerkenning vaststelt.

Tactisch overleg

Het tactische overleg aangaande beheer van het Afsprakenstelsel, dat wordt georganiseerd door de beheerorganisatie en binnen de grenzen van jaarplan, opdracht van ministerie van Economische Zaken en in Operationeel handboek vastgelegde procedures de beheerorganisatie tactisch bestuurt.

Toegang verlenen

Een proces onder verantwoordelijkheid van de dienstverlener waarin op grond van door eHerkenning verstrekte verklaringen en mogelijke controles van andere relevante toegangsrechten die door de dienstverlener zelf zijn vastgelegd bepaald wordt of een uitvoerend natuurlijk persoon toegang krijgt tot een bepaalde dienst of gerechtigd is een bepaalde actie uit te voeren.

Uitvoerend natuurlijk persoon (UNP)

Een Natuurlijk persoon die namens een Dienstafnemer handelt (die dienstafnemer heet dan: vertegenwoordigde dienstafnemer) op basis van een bevoegdheid tot vertegenwoordiging van die dienstafnemer. In het kader van eHerkenning (eH) betreft dit handelen het afnemen van een dienst bij een dienstverlener.

User consent

De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten

Verklaring

Een elektronisch vastgelegd bericht dat gevraagde identiteitsinformatie en attributen bevat conform de koppelvlakspecificaties en waarvoor een bepaalde Deelnemer aantoonbaar instaat.

Vertegenwoordigde

De partij die de vertegenwoordiger de bevoegdheid heeft verleend om in naam van eerstgenoemde te handelen.

Vertegenwoordigde dienstafnemer

Dienstafnemer die niet zelf handelt maar zich laat vertegenwoordigen. De vertegenwoordigde dienstafnemer is de eerste partij in een keten van machtigingen.

Vertegenwoordiger

De Partij die bevoegd is om een andere partij (de vertegenwoordigde) te vertegenwoordigen in het verrichten van handelingen met derden.

Vertegenwoordiging (vertegenwoordigen)

De rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde Partij (de Vertegenwoordiger of Gemachtigde) in naam van een andere partij (de Vertegenwoordigde dienstafnemer) met een derde verrichte handeling aan de vertegenwoordigde worden toegerekend. De Bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet hetzij een volmacht (privaatrecht) hetzij uit een machtiging (bestuursrecht). Zo'n bevoegdheid kan eventueel ingeperkt zijn tot bepaa

Vestiging

Een vestiging is een onderdeel van een Dienstafnemer met een afbakening die in een Handelsregister is opgenomen.

Wettelijke vertegenwoordiging

Een Vertegenwoordiging (vertegenwoordigen) die voortvloeit uit de wet zonder dat er sprake is van het toekennen van een volmacht of machtiging door de Vertegenwoordigde.

WID document

Een geldig document als bedoeld in Wet ter voorkoming van witwassen en financieren van terrorisme artikel 11, lid 1 en nader gespecificeerd in de Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme artikel 4 lid 1.

Wilsuiting

Een wilsuiting is een elektronische handtekening die de elektronisch vastgelegde gegevens waarop de wilsuiting betrekking heeft, verbindt met de elektronische gegevens op basis waarvan de Uitvoerend natuurlijk persoon (UNP) die de wilsuiting afgeeft op ieder moment nadien geauthenticeerd kan worden.

Zelfstandige Zonder Personeel (ZZP)

Een ZZP-er is een ondernemer die geen personeel in dienst heeft en zijn Onderneming niet drijft in een samenwerkingsverband of in een rechtspersoon waarin andere personen participeren.

Aanvullende feature

Een in het Afsprakenstelsel (AS) beschreven dienst of aanvulling op andere dienst waarvan het deelnemers vrij staat deze al dan niet aan te bieden, welke echter indien aangeboden conform de in het afsprakenstelsel opgenomen eisen moet worden aangeboden.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel

Afgeschermde kopie WID

Kopie WID document waarbij de bijzondere persoonsgegevens, te weten pasfoto, BSN en nationaliteit, zijn afgeschermd.

Herkomst
Eigen definitie conform Richtsnoeren CBP

Afsprakenstelsel (AS)

Het geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek. procedures en regels aangaande het Netwerk (voor eHerkenning) in een bepaalde vastgestelde versie. Het doel is betrouwbare authenticatie en verstrekking van identiteitsinformatie op basis van de eHerkenningsdiensten van een goed gereguleerd netwerk voor eHerkenning.

Herkomst
Eigen definitie naar analogie van definitie van PKI

Akte

Een getekend geschrift dat een bewijsbestemming heeft. Een akte heeft als bijzondere eigenschap dat deze in een juridische procedure dwingende bewijskracht heeft. Een elektronische vorm hiervan kan een document zijn, getekend met een elektronische handtekening volgens de wet op de elektronische handtekeningen.

(Naar wetboek van burgerlijke rechtsvordering art. 156 lid 1.)

Attribuutcatalogus (AC)

Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle via het netwerk verkrijgbare optionele attributen bevat inclusief de aanduiding waarmee zij opgevraagd kunnen worden.

Zie ook Attribuutcatalogus.

Herkomst
Eigen definitie analoog aan dienstencatalogus

Authenticatie (authenticeren)

De controle (het staven) van de (een) geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau.

Herkomst
Analoog aan KPMG[1], Modinis[2], opdrachtformulering Vraagstuk eHerkenning bedrijven en instellingen d.d. 10-1-2008, NTP Authorisation Policy (AP) v1.1. Definitie is tevens analoog aan PKIoverheid[3] alwaar opgemerkt wordt: In de Wet EH wordt de term "Authentificatie" gebruikt. Het oorspronkelijke Engelstalige woord is "Authentication". In alle technische vakliteratuur wordt dit echter vertaald met "Authenticatie". In dit document wordt dit laatste dan ook gehanteerd.

Voetnoten:
1. Forum Standaardisatie, Verkenning Authenticatie, KPMG R.2007.ISC.18 (2007)
2. Modinis, Common Terminological Framework for Interoperable Electronic Identity Management (2005)
3. PKIoverheid, Programma van Eisen deel 4: Definities en Afkortingen, versie 2.1, 11 januari 2010

Authenticatiedienst (AD)

Een vereiste Rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de natuurlijk persoon gebruikte Authenticatiemiddel.

T.o.v. de definitie in Vraagstuk eHerkenning bedrijven en instellingen is hier onderscheid gemaakt in middelenuitgever enerzijds en authenticatiedienst anderzijds.

Authenticatiemiddel

Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.

Herkomst
Analoog aan KPMG

Authenticatieverklaring

Een Verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een Authenticatie (authenticeren) die heeft plaatsgevonden in de context van een bepaalde handeling of dienst.

Herkomst
Eigen definitie

Autorisatie

Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren.

Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie.

Nota bene
Autorisatie is geen synoniem voor machtiging

Herkomst
Analoog aan Modinis / PKI overheid begrippenlijst (2005) waarbij autorisatie overeenkomt met betekenis 1 en toegang verlenen met betekenis 2 / Van Dale Groot woordenboek van de Nederlandse taal 14, maar specifiek gemaakt voor de context van eHerkenning.

Tevens analoog aan Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (saml-glossary-2.0-os). PKI overheid hanteert een algemenere definitie die niet in strijd is met bovenstaande.

Bedrijf

Een partij die eHerkenning gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm

- natuurlijk persoon die een onderneming drijft (een eenmanszaak), of
- een niet natuurlijk persoon conform de identificatie waarmee het is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land, of
- een natuurlijk persoon die als privépersoon een dienst afneemt van een dienstverlener (voor afname van overheidsdiensten als burger wordt DigiD gebruikt), of
- een beroepsbeoefenaar

Een dienstafnemer is de uitvoerende natuurlijk persoon of wordt vertegenwoordigd door een uitvoerend natuurlijk persoon.

Nota bene: In proposities aan bedrijven is het toegestaan de abstracte term “dienstafnemer” concreet te maken en te vervangen door “bedrijf”.

Herkomst
Herkomst: o.a. gebaseerd op Hrw 2007 en BW deel 3, artikel 15d en BAO artikel 47 lid 1.

Beheerder

Een uitvoerend natuurlijk persoon met de specifieke bevoegdheid om namens een dienstafnemer bevoegdheden van andere personen te laten registreren, schorsen, in te trekken of anderszins bijbehorende registratieprocessen uit te voeren.

Herkomst
Eigen definitie

Beheerorganisatie (BO)

De Beheerorganisatie van het Afsprakenstelsel die verantwoordelijk is voor het faciliteren van het beheer en de doorontwikkeling van het Afsprakenstelsel, alsmede de controle op en het monitoren van de naleving van het Afsprakenstelsel door de Dienstverleners en de Deelnemers op basis van het door eHerkenning (eH) vastgestelde nalevingsbeleid.

Zie ook Nalevingsbeleid.

Herkomst
Eigen definitie

Beroepsbeoefenaar

Een natuurlijk persoon die een gereglementeerd beroep uitoefent overeenkomstig met EU richtlijn 2005/36/EG (http://ec.europa.eu/internal_market/qualifications/policy_developments/legislation_en.htm)

Herkomst
Gebaseerd op EU Richtlijn 2005/36/EG

Betrouwbaarheidsniveau

Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het middel zelf en het gebruik van het middel (het authenticatiemechanisme).

Herkomst
Vertaald uit engels van STORK “assurance level” en aangepast aan terminologie afsprakenstelsel.

Er bestaat nog verschil van mening in de werkgroepen over de vertaling van assurance in zekerheid dan wel betrouwbaarheid. Er is gekozen voor betrouwbaarheidsniveaus omdat deze term ook door PKIoverheid gehanteerd wordt, echter zonder daar expliciet te zijn gedefinieerd.

Bevoegdheid

Het recht van een persoon om een handeling te verrichten.

Herkomst
Eigen definitie

BSN

Burgerservicenummer: Persoonlijke identificatie van de Nederlandse overheid voor natuurlijke personen.

Herkomst
Gebaseerd op Artikel 1 sub b Wabb: het aan een natuurlijk persoon toegekende nummer.

Certificatie (certificeren)

Een brede (zowel technisch als niet-technisch) evaluatie van de beveiligingseigenschappen van een informatiesysteem of, zoals in het kader van de PKI voor de overheid, een managementsysteem uitgevoerd door een onafhankelijke derde. Certificatie wordt uitgevoerd als een onderdeel van een proces, waarbij wordt nagegaan in welke mate een managementsysteem overeenkomt met een vastgestelde verzameling van eisen (ETSI TS 101 456).

Herkomst
PKIoverheid (en ETSI TS 101 456).

Nota bene: in sommige Europese richtlijnen, waaronder de richtlijn elektronisch handtekening wordt dit als accreditatie aangeduid.

Controle van bevoegdheid

Controle van bevoegdheid zoals deze blijkt uit een in een machtigingenregister geregistreerde vertegenwoordigingsrelatie. Reden van het onderscheid tussen machtiging sec en controle van bevoegdheid is dat de machtiging ook kan bestaan los van het machtigingenregister.

Herkomst
Eigen definitie

Dataminimalisatie

Het zodanig inrichten van een gegevensverwerking dat er zo weinig mogelijk identificerende gegevens bekend hoeven te zijn bij zo weinig mogelijk partijen.

Herkomst
Eigen definitie

Deelnemer

Een partij die conform hetgeen daarover in het afsprakenstelsel is vastgelegd één of meer rollen vervult binnen het netwerk voor eHerkenning. Deelnemers kunnen rollen voor eigen gebruik en/of voor gebruik door derden vervullen.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel

Dienstafnemer

Een partij die eHerkenning gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm

- natuurlijk persoon die een onderneming drijft (een eenmanszaak), of
- een niet natuurlijk persoon conform de identificatie waarmee het is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land, of
- een natuurlijk persoon die als privépersoon een dienst afneemt van een dienstverlener (voor afname van overheidsdiensten als burger wordt DigiD gebruikt), of
- een beroepsbeoefenaar

Een dienstafnemer is de uitvoerende natuurlijk persoon of wordt vertegenwoordigd door een uitvoerend natuurlijk persoon.

Nota bene: In proposities aan bedrijven is het toegestaan de abstracte term “dienstafnemer” concreet te maken en te vervangen door “bedrijf”.

Herkomst
Herkomst: o.a. gebaseerd op Hrw 2007 en BW deel 3, artikel 15d en BAO artikel 47 lid 1.

Dienstencatalogus (DC)

Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle diensten, inclusief de onderverdeling in subdiensten en eventuele samengestelde diensten bevat, welke voor het vastleggen van bijzondere machtigingen, dat wil zeggen machtigingen die zich beperken tot bepaalde diensten, minimaal noodzakelijk is.

Zie ook Service catalog.

Herkomst
Eigen definitie

Dienstverlener (DV)

Een Partij die elektronische diensten aanbiedt aan dienstafnemers waarvoor eHerkenningsdiensten voorwaardelijk zijn. Dit kan zowel een Overheids-dienst-verlener als een private Dienstverlener (DV)zijn.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel.

eHerkenning (eH)

In deze context wordt onder (electronische) herkenning verstaan: ieder van de functies van het netwerk voor eHerkenning gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen dienstverleners en bedrijven en de daarin betrokken uitvoerend natuurlijke personen.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel. Generalisatie van de begrippen authenticatie, bevoegdheid en wilsuiting.

eHerkenningsdiensten

Diensten voor Herkenning, te weten: Authenticatie (authenticeren), controle van Bevoegdheid, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel.

eHerkenningsmakelaar (HM)

Een vereiste Rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die het single point of contact vormt waarlangs dienstverleners eHerkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de dienstverleners te ontkoppelen van de interne berichten binnen het netwerk en die optreedt als routeerder naar alle deelnemende authenticatiediensten, machtigingenregisters en (toekomstige) ondertekendiensten.

Herkomst
Eigen definitie

eHerkenningsnetwerk

Synoniem voor Netwerk (voor eHerkenning).

Herkomst
Eigen definitie

Gebruiker

Een dienstverlener of dienstafnemer die eHerkenning gebruikt om respectievelijk de toegang tot een van haar diensten mee te beveiligen of toegang te vragen tot een dergelijke dienst met het oog op het afnemen van die dienst.

Nota bene: onder gebruikers wordt dus beide zijden van het netwerk verstaan.

Herkomst
Eigen definitie specifiek voor de context van het Afspraken-stelsel

Geïnformeerde uitdrukkelijke toestemming

De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.

Herkomst
Naar Wet bescherming persoonsgegevens

Gemachtigde

De partij die (op grond van wet of machtiging c.q volmacht) bevoegd is om in naam van de vertegenwoordigde bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de vertegenwoordigde.

Voorzover gemachtigde een natuurlijk persoon is, geldt geen beperking ten aanzien van het voorkomen van niet ingezetenen als gemachtigde. Zo kan ook een buitenlandse natuurlijke persoon gemachtigde zijn.

Herkomst
Artikel 3:60 lid 1 BW; Artikel 2:1 lid 1 AWB.

Handelsregister

Voor in Nederland gevestigde bedrijven is dit de Nederlandse basisregistratie van ondernemingen en rechtspersonen die inschrijfplichtig zijn in Nederland, voor andere EU lidstaten is dat het vergelijkbare openbare register van het betreffende land.

Een overzicht van deze openbare registers is gegeven in BAO bijlage 5.

Herkomst
Eigen definitie o.b.v. Handelsregisterwet 2007

Hergebruik

Hergebruik van authenticatiemiddelen: Het toepassen van eerder voor andere doeleinden en onder eigen voorwaarden uitgegeven authenticatiemiddelen binnen eHerkenning op basis van aanmelding van het authenticatiemiddel door de houder ervan.

Herkomst
Eigen definitie

Herkenning

In deze context wordt onder (electronische) herkenning verstaan: ieder van de functies van het netwerk voor eHerkenning gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen dienstverleners en bedrijven en de daarin betrokken uitvoerend natuurlijke personen.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel. Generalisatie van de begrippen authenticatie, bevoegdheid en wilsuiting.

Identificatie (identificeren)

Het noemen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden. In de context van eHerkenning gaat het over identificatie van partijen.

Herkomst
Analoog aan KPMG, NTP Authorisation Policy (AP) v1.1. Nota bene: definitie van PKIoverheid spreekt van “vaststellen” van de identiteit. De hier gebruikte definitie is preciezer en heeft niet het risico dat vaststellen geassocieerd wordt met authenticeren.

Identificerend kenmerk

Een reeks karakters waarmee iets of iemand (een partij) in een bepaalde context uniek wordt aangeduid. Indien het kenmerk enkel uit cijfers bestaat wordt ook van Identificerend nummer gesproken.

Herkomst
Eigen definitie

Identificerend nummer

Een Identificerend kenmerk dat bestaat uit cijfers

Herkomst
Eigen definitie

Identiteit

De volledige maar dynamische set van alle attributen behorende bij een bepaalde entiteit die het mogelijk maakt betreffende entiteit van andere te onderscheiden. Elke entiteit heeft maar één identiteit. De identiteit behoort toe aan de entiteit.

Herkomst
Analoog aan KPMG en Modinis

Identity provider (SAML)

Een vorm van een service provider die identiteitsgegevens aanmaakt, onderhoud en beheert ten behoeve van partijen en hen authenticeert ten behoeve van andere service providers in de context van een federatie.

Herkomst
Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (saml-glossary-2.0-os)

Intermediaire partij

Een partij die bevoegd is te handelen op grond van een aan hem verleende machtiging en die deze machtiging op grond van substitutie heeft doorgegeven aan een derde.

Herkomst
Eigen definitie

Intern pseudoniem

Pseudoniem dat gedurende een langere periode toegepast wordt en enkel binnen eHerkenning gebruikt wordt zonder een specifiek werkingsdomein.

Herkomst
Eigen definitie gebaseerd op definitie van pseudoniem en Persistent Pseudoniem (SAML glossary)

Ketenverklaring

Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een keten van bevoegdheden die aantoont dat een bepaalde uitvoerend natuurlijk persoon een bepaalde vertegenwoordigde dienstafnemer vertegenwoordigt ten behoeve van een bepaalde handeling of dienst op grond van controle van de gehele keten in machtigingenregisters

Herkomst
Eigen definitie

Klachten- en geschillen-commissie

Een onafhankelijke klachten- en geschillencommissie die tot taak heeft het afhandelen van klachten en geschillen die tussen partijen ontstaan bij de uitvoering van eHerkenningsdiensten en niet in onderling overleg door de partijen kunnen worden opgelost. De klachten- en geschillencommissie [A1] is ingesteld door het Ministerie van EZ, op voordracht van de Stelselraad.

Herkomst
Eigen definitie

Koppelvlak

Een koppelvlak is de verbinding tussen twee systemen. Om een koppelvlak te realiseren zijn nodig (a) specificaties en (b) implementaties in mensen en middelen. In de context van eHerkenning (eH) levert het Afsprakenstelsel (AS) de specificaties (a), het netwerk verzorgt de implementaties (b).

Synoniem met Engelse term 'interface'.

Herkomst
Eigen definitie

Machtiging (machtigen)

Een herroepbare bevoegdheid die een vertegenwoordigde verleent aan een andere partij (de gemachtigde) om in naam van eerstgenoemde rechtshandelingen te verrichten.

Een machtiging kan algemeen of bijzonder zijn. Een bijzondere machtiging is beperkt tot bepaalde rechtshandelingen of een bepaalde relevante omvang ten aanzien van rechtshandelingen.
Machtiging kan worden gezien als synoniem aan volmacht zij het dat de term machtiging voornamelijk in bestuursrechtelijke context wordt gebruikt.

Herkomst
Eigen definitie gebaseerd op Modinis

Machtigingenregister (MR)

Een vereiste Rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de Uitvoerend natuurlijk persoon (UNP) verstrekken van machtigingsverklaringen).

Herkomst
Eigen definitie

Machtiging-verklaring

Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een in een geregistreerde machtiging zoals deze gecontroleerd is in een Machtigingen-register ten behoeve van een bepaalde handeling of dienst.

Herkomst
Eigen definitie

Middelenuitgever (MU)

Een vereiste rol binnen het netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en

die de verantwoordelijkheid heeft voor het uitgeven van Authenticatiemiddelen conform de eisen van het gespecificeerde Betrouwbaarheidsniveau.

Herkomst
Eigen definitie

Natuurlijk persoon

Een individueel menselijk wezen en subject van rechten en drager van plichten.

Iedere natuurlijk persoon is een persoon in de zin van de hier gegeven definitie van persoon.

Herkomst
Eigen definitie overeenkomstig Catalogus Nieuw Handelsregister

Netwerk (voor eHerkenning)

De verzameling onderling verbonden componenten die gereguleerd worden door het Afsprakenstelsel (AS) en gezamenlijk eHerkenningsdiensten leveren en daartoe bestaan uit tenminste één invulling door een Deelnemer van de rollen eHerkenningsmakelaar (HM), Machtigingenregister (MR), Authenticatiedienst (AD) en Middelenuitgever (MU), mogelijk aangevuld met verdere rollen voor eHerkenningsdiensten zoals een ondertekendienst, hun onderlinge verbindingen, de verbindingen tot en met het koppelvlak met dienstverleners en de processen voor uitgifte van middelen, registratie van bevoegdheden en aanmelding voor hergebruik vanuit bedrijven, inclusief de benodigde voorzieningen voor beheer conform het Afsprakenstelsel (AS).

Herkomst
Eigen definitie

Niet natuurlijk persoon

Hetzij een rechtspersoon, hetzij een samenwerkingsverband van natuurlijke personen en/of niet-natuurlijke personen.

Niet iedere niet natuurlijke persoon is een persoon in de zin van de hier gegeven definitie van persoon, samenwerkingsverbanden zijn namelijk verbanden van personen maar zelf geen persoon.

Herkomst
Eigen definitie, overeenkomstig Catalogi Basisregistraties (www.stelselcatalogus.nl)

Onderneming

Een onderneming in de zin van de Handelsregisterwet 2007 of een onderneming conform de voorschriften van een andere EU lidstaat welke ingeschreven is in het handelsregister van betreffende lidstaat.

Herkomst
Handelsregisterwet 2007

Ondertekendienst

Een (voorziene) rol binnen het Netwerk (voor eHerkenning) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het doen van de wilsuiting, het valideren ervan en het verstrekken van het

bijbehorende associatiebewijs.

In de huidige versie is de rol ondertekendienst nog niet uitgewerkt maar wordt deze waar relevant wel benoemd.

Herkomst
Eigen definitie

Overheidsdienstverlener

Een Dienstverlener (DV) die onderdeel van de Nederlandse overheid is. Voor zover zaken zowel overheidsdienstverleners als private dienstverleners kunnen betreffen wordt gesproken van “dienstverleners”.

Herkomst
Eigen definitie

Partij

Een persoon of samenwerkingsverband die in de context van eHerkenning (eH) voorkomt of zou kunnen voorkomen en die zonodig uniek geïdentificeerd en geauthenticeerd kan worden.
Voorbeelden van partijen zijn: Deelnemers, dienstverleners, bedrijven, vertegenwoordigden, gemachtigden, …

De term wordt gehanteerd als generalisatie.

Herkomst
Gebaseerd op Identified Entity Party (STORK Glossary and Acronyms v6.0), Principal en System Entity (SAML glossary) en Identifiable Entity (Modinis) en vervolgens specifiek gemaakt voor eHerkenning.

PKI (Public Key Infrastructure)

Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op ‘public key cryptografie’. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

Herkomst
PKIoverheid

Privépersoon

Een Natuurlijk persoon, echter uitsluitend voor situaties en dienstafnames bij niet-overheidsdienstverleners c.q. in B2C diensten.

Herkomst
Eigen definitie

Pseudoniem

Een arbitrair Identificerend kenmerk dat op basis van een bewerking van een ander identificerend kenmerk wordt geproduceerd op een wijze die steeds hetzelfde pseudoniem oplevert bij hetzelfde kenmerk zonder dat deze laatste herleid kan worden uit het pseudoniem. Er kunnen meerdere pseudoniemen bestaan bij één Identificerend kenmerk, ieder met een eigen werkingsdomein. In dat geval zijn twee pseudoniemen van hetzelfde kenmerk in verschillende domeinen niet aan elkaar te relateren.

Herkomst
Gebaseerd op Modinis

Rechtspersoon

Een juridische eenheid en subject van rechten en drager van plichten. Iets is een rechtspersoon op grond van de wet of omdat het conform wettelijke vereisten is ontstaan, een rechtspersoon heeft een bepaalde rechtsvorm.

Scope: Rechtspersonen welke niet in een handelsregister of vergelijkbaar openbaar register van enige EU lidstaat zijn ingeschreven conform de voorschriften van betreffend land vallen buiten de scope van eHerkenning.

Herkomst
Definitie conform Catalogus Basisregistraties

Rol

Eén van de verantwoordelijkheden die binnen het Netwerk (voor eHerkenning) voorkomt die gezamenlijk met de andere rollen eHerkenningsdiensten levert.

Indien rol voorkomt zonder de toevoeging rol in het netwerk of rol in het netwerk voor eHerkenning dan is de term rol algemener bedoeld dan hier gedefinieerd.

Herkomst
Eigen definitie specifiek voor het afsprakenstelsel

Service provider (SP)

Een rol die vervuld wordt door een afgebakend en actief onderdeel van een systeem dat diensten aanbiedt aan partijen of aan andere onderdelen van dat systeem.

Herkomst
Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (saml-glossary-2.0-os)

Single Sign On (SSO)

Een functie die door eHerkenning (eH) wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel, waardoor een authenticatie van een uitvoerend natuurlijk persoon wordt hergebruikt, waardoor deze uitvoerend natuurlijk persoon niet opnieuw hoeft in te loggen.

Herkomst
Deze definitie komt overeen met de definitie bij DigiD

Specifiek pseudoniem

Pseudoniem dat gedurende een langere periode toegepast wordt in een specifiek werkingsdomein. Een dienstverlenerspecifiek pseudoniem is steeds hetzelfde voor dezelfde Dienstverlener (DV) in wiens context het gebruikt wordt, een dienstafnemerspecifiek pseudoniem is steeds hetzelfde voor de context van één dienstafnemer etc.

Herkomst
Eigen definitie

Stelselraad eHerkenning

Het strategische overleg inzake de publiek- private samenwerking ten behoeve van eHerkenning, waarvoor de beheerorganisatie het secretariaat voert en waarvoor de minister van Economische Zaken een onafhankelijke voorzitter benoemt en het Instellingsbesluit besturing eHerkenning vaststelt.

Zie ook Stelselraad eHerkenning (gremium).

Herkomst
Eigen definitie

Tactisch overleg

Het tactische overleg aangaande beheer van het Afsprakenstelsel, dat wordt georganiseerd door de beheerorganisatie en binnen de grenzen van jaarplan, opdracht van ministerie van Economische Zaken en in Operationeel handboek vastgelegde procedures de beheerorganisatie tactisch bestuurt.

Herkomst
Eigen definitie

Toegang verlenen

Een proces onder verantwoordelijkheid van de dienstverlener waarin op grond van door eHerkenning verstrekte verklaringen en mogelijke controles van andere relevante toegangsrechten die door de dienstverlener zelf zijn vastgelegd bepaald wordt of een uitvoerend natuurlijk persoon toegang krijgt tot een bepaalde dienst of gerechtigd is een bepaalde actie uit te voeren.

Herkomst
Eigen definitie

Uitvoerend natuurlijk persoon (UNP)

Een Natuurlijk persoon die namens een Dienstafnemer handelt (die dienstafnemer heet dan: vertegenwoordigde dienstafnemer) op basis van een bevoegdheid tot vertegenwoordiging van die dienstafnemer. In het kader van eHerkenning (eH) betreft dit handelen het afnemen van een dienst bij een dienstverlener.

Herkomst
Eigen definitie specifiek voor de context van het afsprakenstelsel

User consent

De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.

Herkomst
Naar Wet bescherming persoonsgegevens

Verklaring

Een elektronisch vastgelegd bericht dat gevraagde identiteitsinformatie en attributen bevat conform de koppelvlakspecificaties en waarvoor een bepaalde Deelnemer aantoonbaar instaat.

Afhankelijk van de betreffende identiteitsinformatie wordt gesproken van een authenticatieverklaring, een machtigingsverklaring of een Ketenverklaring. Een verklaring kan andere verklaringen omvatten en voor de aantoonbaarheid vereisen, dan wordt gesproken over een verklaring over x en y waarbij de wijze waarop de verklaringen in elkaar grijpen in detail in de Interface specifications is beschreven.

Herkomst
Eigen definitie

Vertegenwoordigde

De partij die de vertegenwoordiger de bevoegdheid heeft verleend om in naam van eerstgenoemde te handelen.

Herkomst
Artikel 3:60 lid 1 BW; Analoog aan AP1.1. Zie definitie vertegenwoordiging

Vertegenwoordigde dienstafnemer

Dienstafnemer die niet zelf handelt maar zich laat vertegenwoordigen. De vertegenwoordigde dienstafnemer is de eerste partij in een keten van machtigingen.

Herkomst
Eigen definitie

Vertegenwoordiger

De Partij die bevoegd is om een andere partij (de vertegenwoordigde) te vertegenwoordigen in het verrichten van handelingen met derden.

Herkomst
Zie definitie vertegenwoordiging

Vertegenwoordiging (vertegenwoordigen)

De rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde Partij (de Vertegenwoordiger of Gemachtigde) in naam van een andere partij (de Vertegenwoordigde dienstafnemer) met een derde verrichte handeling aan de vertegenwoordigde worden toegerekend. De Bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet hetzij een volmacht (privaatrecht) hetzij uit een machtiging (bestuursrecht). Zo'n bevoegdheid kan eventueel ingeperkt zijn tot bepaalde rechtshandelingen, of een bepaalde relevante omvang ten aanzien van rechtshandelingen.

In privaatrechtelijke context wordt naast het begrip vertegenwoordiger, agent of gevolmachtigde gehanteerd in plaats van gemachtigde.

Herkomst
Conform juridische toets prof. A. Mohr

Vestiging

Een vestiging is een onderdeel van een Dienstafnemer met een afbakening die in een Handelsregister is opgenomen.

Herkomst
Eigen definitie

Wettelijke vertegenwoordiging

Een Vertegenwoordiging (vertegenwoordigen) die voortvloeit uit de wet zonder dat er sprake is van het toekennen van een volmacht of machtiging door de Vertegenwoordigde.

Voorbeelden zijn: de bestuurder(s) van een Rechtspersoon, de curator, de ouders van een minderjarige.

Herkomst
Eigen definitie

WID document

Een geldig document als bedoeld in Wet ter voorkoming van witwassen en financieren van terrorisme artikel 11, lid 1 en nader gespecificeerd in de Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme artikel 4 lid 1.

Dat wil zeggen onder andere een Nederlands of buitenlands paspoort, een Nederlandse identiteitskaart of rijbewijs, een rijbewijs uitgegeven door een andere EU lidstaat en vreemdelingendocumenten, allen mits geldig.

Herkomst
Eigen definitie

Wilsuiting

Een wilsuiting is een elektronische handtekening die de elektronisch vastgelegde gegevens waarop de wilsuiting betrekking heeft, verbindt met de elektronische gegevens op basis waarvan de Uitvoerend natuurlijk persoon (UNP) die de wilsuiting afgeeft op ieder moment nadien geauthenticeerd kan worden.

Herkomst
Eigen definitie

Zelfstandige Zonder Personeel (ZZP)

Een ZZP-er is een ondernemer die geen personeel in dienst heeft en zijn Onderneming niet drijft in een samenwerkingsverband of in een rechtspersoon waarin andere personen participeren.

Herkomst
Eigen definitie

Juridica

Hier vindt u de juridische documenten van het Afsprakenstelsel eHerkenning: het juridisch kader en de gebruiksvoorwaarden. Deze documenten bevatten informatie over de besturing van eHerkenning, de naleving van het afsprakenstelsel, de overeenkomst tussen de beheerorganisatie en de aanbieders en de minimale gebruiksvoorwaarden waaronder de dienstverleners en ondernemers eHerkenning mogen gebruiken.

Deze categorie bevat de volgende onderdelen:

- Juridisch kader — Beschrijft het juridisch kader, het besturingsmodel en de controle op en monitoring van de naleving van het afsprakenstelsel.
- Gebruiksvoorwaarden eHerkenning — Deze Gebruiksvoorwaarden zijn van toepassing op het verlenen van diensten door Deelnemers aan Dienstverleners en Dienstafnemers in het kader van het Netwerk voor eHerkenning.

Juridisch kader

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

eHerkenning is gericht op het leveren van "vertrouwen". Duidelijke juridische kaders dragen daar aan bij evenals een goed georganiseerde besturing gebaseerd op duidelijke rollen en verantwoordelijkheden zoals uitgewerkt in Organen en taakverdeling.

Bovendien zijn de wettelijke eisen aangaande betrouwbaarheid van e-diensten, aangaande identificatie en ondertekening van belang voor het begrip en de uitwerking van de door het netwerk voor eHerkenning te leveren eHerkenningsdiensten.

Wet- en regelgeving

Het afsprakenstelsel baseert zich op bestaande Europese en Nederlandse wet- en regelgeving.

Het juridisch kader inzake het afsprakenstelsel eHerkenning is, behalve in toepasselijke wet- en regelgeving, verder uitgewerkt in het afsprakenstelsel zelf en de bijbehorende deelnemersovereenkomsten (Template deelnemersovereenkomst) en Gebruiksvoorwaarden eHerkenning.

Leeswijzer

- Aansprakelijkheid — Binnen het afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten binnen de rol die hij vervult. Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. De deelnemers mogen en kunnen niet afwijken van deze algemene regels. Hoe deze regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval.
- Aanvullende verplichtingen — In aanvulling op de juridisch bindende verplichtingen uit de genoemde documenten (Afsprakenstelsel eHerkenning, Template deelnemersovereenkomst en Gebruiksvoorwaarden eHerkenning) gelden specifiek nog de onderstaande verplichtingen voor de deelnemers en de dienstverleners
- Betrouwbaarheidsniveaus — Het vaststellen van het voor een bepaalde dienst vereiste Betrouwbaarheidsniveau wordt bepaald door de dienstverlener. Dit geldt zowel voor een publiek- als een privaatrechtelijke dienstverlener. De overheidsdienstverlener moet ter naleving van de Awb invulling geven aan de norm van een betrouwbare en vertrouwelijke communicatie.
- Juridische structuur afsprakenstelsel eHerkenning — Het afsprakenstelsel geldt voor alle partijen die deelnemen aan of gebruik maken van eHerkenning. Het afsprakenstelsel is vastgelegd in een aantal documenten. Zie Afsprakenstelsel eHerkenning voor een opsomming van deze documenten. In al deze documenten kunnen voor een of meer partijen juridisch bindende verplichtingen zijn neergelegd. Vanzelfsprekend moeten alle juridisch bindende verplichtingen door de betreffende partij worden nageleefd.
- Nalevingsbeleid — Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het netwerk voor eHerkenning. Naleving gebeurt zo veel mogelijk in goed onderling overleg tussen de beheerorganisatie en de betrokken deelnemer of dienstverlener. Het kan echter noodzakelijk zijn om een correcte naleving af te dwingen via het opleggen van sancties.
- Organen en taakverdeling — In de besturing van eHerkenning worden drie lagen onderscheiden:
- Rol van eHerkenningsmakelaars — De Herkenningsmakelaars hebben een speciale rol ten opzichte van de bij hen aangesloten dienstverleners. De eHerkenningsmakelaars fungeren namelijk als centraal aanspreekpunt voor zowel de dienstverlener als de beheerorganisatie. Dit brengt onder andere met zich mee dat de eHerkenningsmakelaar alle benodigde informatie aan de dienstverlener en de beheerorganisatie moet verstrekken. Deze informatie betreft in ieder geval: de gegevens van de contactpersoon voor calamiteiten en ernstige incidenten
- Toetredingseisen — Alle deelnemers aan het afsprakenstelsel dienen te voldoen aan de algemene toetredingseisen. De toetredingseisen worden gesteld om een aantal redenen. De belangrijkste daarvan is de wetenschap dat het netwerk alleen goed zal kunnen functioneren als afnemers van diensten voldoende

vertrouwen hebben in het afsprakenstelsel. Vertrouwen in het afsprakenstelsel en in de eHerkenningsdiensten die in kader van het afsprakenstelsel geleverd worden vereist vertrouwen in de individuele deelnemers. Het afsp

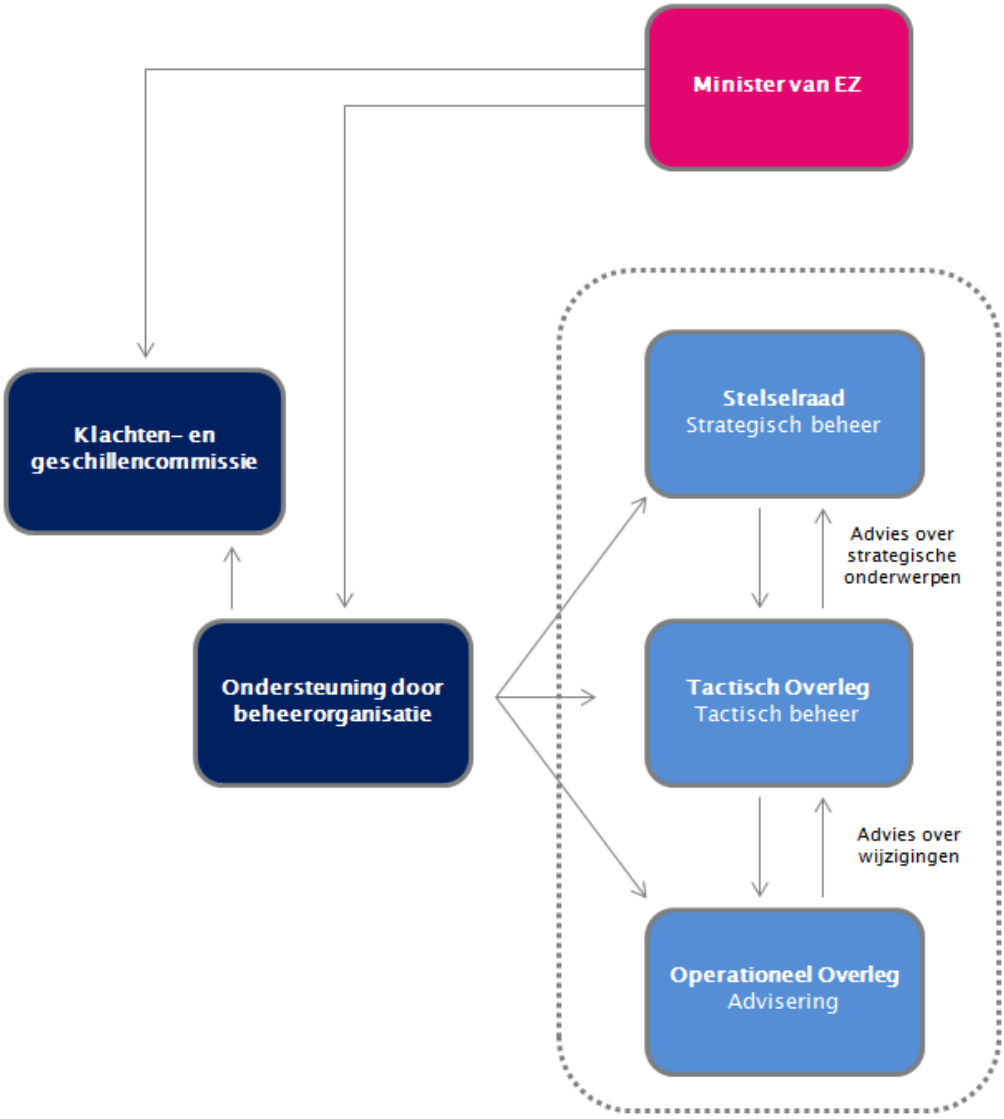
- Vertegenwoordiging, volmacht en machtiging — Vertegenwoordiging is binnen het afsprakenstelsel zowel op grond van het burgerlijk recht als op grond van het bestuursrecht van belang. De privaatrechtelijke kant doet zich voor bij vertegenwoordiging van rechtspersonen en natuurlijke personen. De publiekrechtelijke kant is van belang bij vertegenwoordiging van bestuursorganen.

Organen en taakverdeling

In de besturing van eHerkenning worden drie lagen onderscheiden:

1. Strategisch beheer. Dit omvat o.a. de continuïteit van het afsprakenstelsel, eHerkenning als voorziening voor e-diensten van de overheid, het bredere gebruik van eHerkenning, het stellen van kaders wat betreft belangrijke wijzigingen en lange termijn doorontwikkeling van het afsprakenstelsel .
2. Tactisch beheer. Dit omvat o.a. het managen van het wijzigingenbeheer van het afsprakenstelsel, indien nodig het managen van incidenten en , de algemene communicatie over eHerkenning.
3. Operationeel beheer. Dit omvat het voorbereiden van wijzigingen op het afsprakenstelsel, het in stand houden van de technische voorzieningen van de beheerorganisatie voor dagelijks gebruik van het netwerk en voor testen en conformiteitstoetsen.

Daarnaast bestaat er de losstaande invalshoek van naleving en toetreding/uittreding, deze wordt behandeld in Nalevingsbeleid en Toetredingseisen.



Op basis van bovenstaande ordening zijn voor de besturing van eHerkenning de hieronder beschreven organen met bijbehorende verantwoordelijkheden ingericht.

Bekostiging

De bekostiging van de beheerorganisatie inclusief het secretariaat van de besturingsstructuur van eHerkenning is onderdeel van de beheeropdracht van het Ministerie van EZ aan Logius.

Klachten- en geschillencommissie

Er bestaat een onafhankelijke klachten- en geschillencommissie waarvan de leden worden benoemd door het ministerie van EZ op voordracht van de Stelselraad eHerkenning (gremium).

Operationeel Overleg (gremium)

Het Operationeel Overleg bereidt onder meer wijzigingen van het afsprakenstelsel voor, zogeheten Requests For Change (RFC's). Het Operationeel Overleg brengt advies uit aan het Tactisch Overleg (gremium) over (de impact van) nieuwe wijzigingen en de (samenstelling van) releases op het netwerk.

Stelselraad eHerkenning (gremium)

De Stelselraad eHerkenning is het strategische orgaan. De Stelselraad eHerkenning is een overleggremium dat tot taak heeft onderwerpen aan de orde te stellen overeenkomstig het door haar opgestelde strategisch meerjarenplan. Ook kunnen onderwerpen worden ingebracht van strategische aard, zoals financiering, doorontwikkeling, vraagstukken van transparantie, toezicht, veiligheid en van internationale aard.

Tactisch Overleg (gremium)

Het Tactisch Overleg is een afvaardiging van alle deelnemers, dienstverleners en dienstafnemers en heeft tot taak tactische onderwerpen aan de orde te stellen overeenkomstig het vastgestelde jaarplan.

Stelselraad eHerkenning (gremium)

De Stelselraad eHerkenning is het strategische orgaan. De Stelselraad eHerkenning is een overleggremium dat tot taak heeft onderwerpen aan de orde te stellen overeenkomstig het door haar opgestelde strategisch meerjarenplan. Ook kunnen onderwerpen worden ingebracht van strategische aard, zoals financiering, doorontwikkeling, vraagstukken van transparantie, toezicht, veiligheid en van internationale aard.

In de Stelselraad eHerkenning zijn Deelnemers, Dienstverleners en Dienstafnemers afgevaardigd.

> In deze afvaardiging wordt aangenomen dat overheidsorganisaties die eHerkenning voor G2G gebruiken afgevaardigd zijn via de lijn van de overheidsdienstverleners en dat marktpartijen die eHerkenning B2B gebruiken afgevaardigd zijn via de lijn van de dienstafnemers.

> Hiermee wordt het advies van prof. T. Ottervanger opgevolgd die in zijn notitie van 8 april 2011 " Mededingingsrechtelijke beoordeling Afsprakenstelsel v 0.8 eHerkenning" adviseerde dat "De samenstelling van het bestuur (of een ander nog in te richten orgaan dat formeel de leiding heeft in het Afsprakenstelsel)", in casu de opvolger van het kernteam, gewijzigd dient te worden, bijvoorbeeld door onafhankelijke personen of een goede afspiegeling van alle rollen. Dezelfde afspiegeling wordt gehanteerd voor de opvolger van het bestuur van de tijdelijke beheerorganisatie.

In deze afvaardiging wordt aangenomen dat overheidsorganisaties die eHerkenning voor G2G gebruiken afgevaardigd zijn via de lijn van de overheidsdienstverleners en dat marktpartijen die eHerkenning B2B gebruiken afgevaardigd zijn via de lijn van de dienstafnemers. Hiermee wordt het advies van prof. T. Ottervanger opgevolgd die in zijn notitie van 8 april 2011 "Mededingingsrechtelijke beoordeling Afsprakenstelsel v 0.8 eHerkenning" adviseerde dat "De samenstelling van het bestuur (of een ander nog in te richten orgaan dat formeel de leiding heeft in het Afsprakenstelsel)", in casu de opvolger van het kernteam, gewijzigd dient te worden, bijvoorbeeld door onafhankelijke personen of een goede afspiegeling van alle rollen. Dezelfde afspiegeling wordt gehanteerd voor de opvolger van het bestuur van de tijdelijke beheerorganisatie.

De Stelselraad eHerkenning kent een onafhankelijke voorzitter. Het Instellingsbesluit besturing eHerkenning beschrijft de wijze van afvaardiging, de stemverhoudingen, de positie van de minister en de relatie met de beheerorganisatie. De Minister van EZ benoemt de onafhankelijke voorzitter en stelt het Instellingsbesluit besturing eHerkenning vast; daarmee staat zij borg voor de continuïteit van eHerkenning. De beheerorganisatie voert het secretariaat van de Stelselraad eHerkenning. Agenda's en vergaderstukken van de Stelselraad eHerkenning worden tijdig bekendgemaakt aan al de in de raad afgevaardigde partijen.

De Stelselraad eHerkenning is een samenwerkingsverband zonder rechtspersoonlijkheid en is geen bestuursorgaan in de zin van de Awb.

Tactisch Overleg (gremium)

Het Tactisch Overleg is een afvaardiging van alle deelnemers, dienstverleners en dienstafnemers en heeft tot taak tactische onderwerpen aan de orde te stellen overeenkomstig het vastgestelde jaarplan.

Daarnaast kunnen ook overige tactische of operationele onderwerpen worden ingebracht zoals veiligheidsincidenten, het beheer van de website en vraagstukken ten aanzien van het wijzigingsproces. Ook ervaringen van eindgebruikers kunnen aan de orde komen. Zonodig kan het Tactisch Overleg (werk)groepen instellen om operationele kwesties uit te werken. De beheerorganisatie voert het secretariaat van het Tactisch Overleg.

Operationeel Overleg (gremium)

Het Operationeel Overleg bereidt onder meer wijzigingen van het afsprakenstelsel voor, zogeheten Requests For Change (RFC's). Het Operationeel Overleg brengt advies uit aan het Tactisch Overleg (gremium) over (de impact van) nieuwe wijzigingen en de (samenstelling van) releases op het netwerk.

De beheerorganisatie voert het secretariaat van het Operationeel Overleg.

Klachten- en geschillencommissie

Er bestaat een onafhankelijke klachten- en geschillencommissie waarvan de leden worden benoemd door het ministerie van EZ op voordracht van de Stelselraad eHerkenning (gremium).

Een klacht wordt hier gedefinieerd als: een uiting van ongenoegen, gericht aan de klachten- geschillencommissie met betrekking tot de eHerkenningsdienstverlening van een deelnemer, een dienstverlener, een dienstafnemer en/of de dienstverlening van de beheerorganisatie.

Een geschil wordt gedefinieerd als:een onenigheid tussen twee of meer partijen naar aanleiding van de uitvoering van eHerkenningsdiensten.

Klachten en geschillen tussen partijen kunnen aan deze klachten- en geschillencommissie worden voorgelegd wanneer de betrokken partijen in onderling overleg niet zelf tot een oplossing kunnen komen.

De commissie geeft naar aanleiding van een klacht of een geschil een advies aan betrokken partijen. De partij aan wie het advies is gericht, neemt dit advies in overweging en voert het advies uit, tenzij zwaarwegende redenen zich hiertegen verzetten. De partij die het betreft informeert de klachten- en geschillen commissie binnen twee weken na dagtekening van ontvangst van het advies of, en zo ja, het advies wordt overgenomen. Het niet overnemen van het advies wordt met redenen omkleed. Het staat partijen uiteraard te allen tijde vrij om, in plaats van een beroep te doen op de klachten- en geschillencommissie, hun zaak aan de civiele rechter voor te leggen.

Het secretariaat van de klachten- en geschillencommissie wordt uitgevoerd door het Bureau van de commissie. De klachten- en geschillencommissie incl. het Bureau (secretariaat) dienen onafhankelijk en onpartijdig te zijn. Daarom dient het Bureau op enige afstand van mogelijk betrokken partijen te worden gepositioneerd.

Zie ook reglement KGC 23 maart 14.pdf

Bekostiging

De bekostiging van de beheerorganisatie inclusief het secretariaat van de besturingsstructuur van eHerkenning is onderdeel van de beheeropdracht van het Ministerie van EZ aan Logius.

Nalevingsbeleid

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het netwerk voor eHerkenning. Naleving gebeurt zo veel mogelijk in goed onderling overleg tussen de beheerorganisatie en de betrokken deelnemer of dienstverlener. Het kan echter noodzakelijk zijn om een correcte naleving af te dwingen via het opleggen van sancties.

Monitoring en controle

Tot de taken van de beheerorganisatie behoort de monitoring en controle van de naleving van het afsprakenstelsel door de deelnemers en de dienstverleners. De beheerorganisatie monitort de prestaties van eHerkenning en voert de naleving uit.

Dit onderdeel beschrijft de wijze waarop wordt zorg gedragen voor naleving van het afsprakenstelsel. Voor de procesbeschrijving, zie Proces naleving.

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het netwerk voor eHerkenning. Naleving gebeurt zo veel mogelijk in goed onderling overleg tussen de beheerorganisatie en de betrokken deelnemer of dienstverlener. Het kan echter noodzakelijk zijn om een correcte naleving af te dwingen via het opleggen van sancties.

Reikwijdte

Naleving heeft betrekking op alle onderdelen van het afsprakenstelsel. Naleving heeft daarom betrekking op de productie-omgeving en op de afspraken over de testomgeving.

Dit betekent ook dat de controle en monitoring op de naleving van het afsprakenstelsel niet beperkt is tot bepaalde afspraken, zoals bijvoorbeeld de naleving van de Service Levels of de normenkaders, maar zich uitstrekt tot het gehele afsprakenstelsel. Ook het Juridisch Kader en het incidentmanagement en de meest recente releases van het afsprakenstelsel, maar ook bijvoorbeeld de Template deelnemersovereenkomst en de Gebruiksvoorwaarden eHerkenning worden gecontroleerd en gemonitord op naleving.

> Naleving vormt een onderdeel van het afsprakenstelsel dat privaatrechtelijk van aard is. Daarmee zijn beslissingen met betrekking tot controle en monitoring op de naleving van het afsprakenstelsel ook privaatrechtelijk.

Bevoegdheid tot opleggen van sancties

Als onderdeel van de controle en monitoring op de naleving van het afsprakenstelsel kan het nodig zijn, indien overleg niet tot een correcte naleving heeft geleid, om één of meer sancties op te leggen.

De bevoegdheid tot het opleggen van sancties komt aan de beheerorganisatie toe, als uitvloeisel van de taak om het merk te beheren. In verband met de waarborging van het publieke belang en de aanzienlijke consequenties komt de bevoegdheid tot het opleggen van bepaalde sancties, namelijk schorsing, de beëindiging van de deelnemersovereenkomst en het toepassen van de spoedprocedure, toe aan het ministerie van EZ. Zie ook Sancties voor de te onderscheiden sancties.

De beheerorganisatie en EZ behandelen informatie van een deelnemer / dienstverlener of een derde vertrouwelijk.

Informatie over naleving

De beheerorganisatie zal zich ter zake terdege (laten) informeren over de naleving van (een of meer afspraken van) het afsprakenstelsel. Deze informatie kan afkomstig zijn uit alle mogelijke bronnen. Zo kan de informatie bijvoorbeeld worden verkregen uit de diverse rapportages die in het kader van het afsprakenstelsel worden overgelegd, maar ook uit informatie die beschikbaar is bij de beheerorganisatie of uit openbare bronnen. Op grond van het afsprakenstelsel is de deelnemer/dienstverlener gehouden om aan de beheerorganisatie alle informatie te verstrekken om de naleving van het afsprakenstelsel te kunnen controleren en/of te monitoren.

Besluit inzake sancties

Indien de deelnemer/dienstverlener na het verstrijken van gestelde redelijke termijn de betreffende afspraak uit het afsprakenstelsel volgens de beheerorganisatie alsnog niet of niet volledig naleeft en de beheerorganisatie ter zake een sanctie wil opleggen, zal de beheerorganisatie beslissen of het opleggen van een sanctie nodig is. Deze beslissing wordt genomen door andere personen dan degenen die tot dan toe namens de beheerorganisatie betrokken waren bij de monitoring en de procedure bij vermoedelijke niet-naleving. Door deze functiescheiding wordt een onafhankelijke en objectieve beoordeling van het dossier gewaarborgd. Deze nieuwe betrokkenen van de beheerorganisatie zullen het gehele dossier opnieuw bekijken en aan de hand van hun bevindingen beslissen of het opleggen van een sanctie in hun ogen de beste methode is om in het betreffende geval naleving van het afsprakenstelsel te bewerkstelligen.

Indien de beheerorganisatie van mening is dat het opleggen van de sancties schorsing of beëindiging van de deelnemersovereenkomst aan de orde is, zal zij het dossier voorleggen aan en bespreken met EZ . EZ neemt een beslissing over het eventueel opleggen van de sancties van schorsing of beëindiging van de deelnemersovereenkomst.

Het opleggen van sancties

De beheerorganisatie c.q. EZ neemt een beslissing over het opleggen van een of meer sancties aan de deelnemer/dienstverlener. De beslissing tot het opleggen van een sanctie wordt de deelnemer/dienstverlener schriftelijk en met redenen omkleed meegedeeld door de beheerorganisatie. De beheerorganisatie neemt in deze beslissing in ieder geval de volgende informatie op:

- bedrijfsnaam van de betrokken deelnemer/dienstverlener;
  - vermelding van de afspraak uit het afsprakenstelsel die niet is nagekomen;
  - omschrijving van de feiten waaruit blijkt dat de betreffende afspraak uit het afsprakenstelsel niet is nagekomen;
  - de reactie van de betrokken deelnemer/dienstverlener (eventueel met verwijzing naar overgelegde documentatie);
  - de redelijke termijn waarin de deelnemer/dienstverlener na het afgeven van de formele waarschuwing alsnog

aan de betreffende afspraak uit het afsprakenstelsel kon voldoen;
- de opgelegde (combinatie van) sanctie(s).

Beroep

Tegen de beslissing van de beheerorganisatie of EZ tot het opleggen van een of meer sancties staat beroep open bij de bevoegde civiele rechter.

Meer lezen?

- Beëindiging van de Deelnemersovereenkomst — Als uiterste sanctie in geval van het niet naleven van het afsprakenstelsel, kan EZ in verband met het publieke belang besluiten om de Deelnemersovereenkomst met de deelnemer te beëindigen, zoals is voorzien in artikel 5.2 van de deelnemersovereenkomst. Het is evident dat deze uiterste sanctie slechts in zeer bijzondere omstandigheden wordt gehanteerd, indien de deelnemer naar het oordeel van EZ het afsprakenstelsel niet kan of wil naleven.
- Besluit inzake sancties — Indien de deelnemer/dienstverlener na het verstrijken van gestelde redelijke termijn de betreffende afspraak uit het afsprakenstelsel volgens de beheerorganisatie alsnog niet of niet volledig naleeft en de beheerorganisatie ter zake een sanctie wil opleggen, zal de beheerorganisatie beslissen of het opleggen van een sanctie nodig is.
- Compensatieregeling — Naast bovenbedoelde sancties geldt voor de niet-naleving (niet, niet goed, niet volledig of niet tijdig) van implementatiemaatregelen een wederkerige compensatieregeling. Deze regeling is van toepassing bij implementatieplannen waarbij in het voortraject van de totstandkoming duidelijke afspraken zijn gemaakt over de inhoud, de deadline, de concrete maatregelen die de verschillende betrokkenen moeten nemen en de hoogte van de compensatie.
- Opleggen van sancties — De beheerorganisatie c.q. EZ neemt een beslissing over het opleggen van een of meer sancties aan de deelnemer/dienstverlener.
- Sancties — Sancties kunnen voor een bepaalde termijn worden opgelegd. Na afloop van de termijn kan de sanctie worden verlengd of kunnen er nieuwe of aanvullende sancties worden opgelegd. Er kunnen meer sancties tegelijkertijd worden opgelegd. Aan de sancties kunnen voorwaarden en voorschriften worden verbonden.
- Sancties tegen de beheerorganisatie of EZ — EZ als opdrachtgever van de beheerorganisatie en de beheerorganisatie als opdrachtnemer en uitvoerder van de beheertaken, monitoren en controleren de correcte naleving van het afsprakenstelsel. Zij beogen hiermee een belangrijke elektronische netwerk voor het (laten) verrichten van elektronische diensten mogelijk te maken. Vanuit deze rol hebben zij alleen belang bij het slagen van het afsprakenstelsel en geen enkel belang bij het niet-naleven ervan.
- Schorsing — Schorsing kan door EZ in verband met het publieke belang worden opgelegd als zelfstandige sanctie of als bijkomende sanctie in geval van toepassing van de spoedprocedure of de eventuele beëindiging van de Deelnemersovereenkomst. Schorsing betekent dat de betreffende deelnemer tijdelijk niet in het netwerk eHerkenning zit en het merk eHerkenning niet mag voeren.
- Spoedprocedure — Deze uitzonderlijke procedure wordt door EZ in verband met het publieke belang alleen gebruikt indien vanwege zwaarwegende omstandigheden of dringende spoed de normale nalevingsprocedure, zoals hierboven is beschreven, niet gebruikt kan worden. Voorbeelden van dergelijke omstandigheden zijn een acute en ernstige schending van de verplichtingen uit het afsprakenstelsel en de deelnemersovereenkomst, de acute en ernstige aantasting van de beschikbaarheid, betrouwbaarheid, integriteit en vertrouweli
- Uitgangspunten compensatieregeling

Besluit inzake sancties

Indien de deelnemer/dienstverlener na het verstrijken van gestelde redelijke termijn de betreffende afspraak uit het afsprakenstelsel volgens de beheerorganisatie alsnog niet of niet volledig naleeft en de beheerorganisatie ter zake een sanctie wil opleggen, zal de beheerorganisatie beslissen of het opleggen van een sanctie nodig is.

Deze beslissing wordt genomen door andere personen dan degenen die tot dan toe namens de beheerorganisatie betrokken waren bij de monitoring en de procedure bij vermoedelijke niet-naleving.

Door deze functiescheiding wordt een onafhankelijke en objectieve beoordeling van het dossier gewaarborgd. Deze nieuwe betrokkenen van de beheerorganisatie zullen het gehele dossier opnieuw bekijken en aan de hand van hun bevindingen beslissen of het opleggen van een sanctie in hun ogen de beste methode is om in het betreffende geval naleving van het afsprakenstelsel te bewerkstelligen.

Indien de beheerorganisatie van mening is dat het opleggen van de sancties schorsing of beëindiging van de deelnemersovereenkomst aan de orde is, zal zij het dossier voorleggen aan en bespreken met EZ. EZ neemt een beslissing over het eventueel opleggen van de sancties van schorsing of beëindiging van de deelnemersovereenkomst.

Opleggen van sancties

De beheerorganisatie c.q. EZ neemt een beslissing over het opleggen van een of meer sancties aan de deelnemer/dienstverlener.

De beslissing tot het opleggen van een sanctie wordt de deelnemer/dienstverlener schriftelijk en met redenen omkleed meegedeeld door de beheerorganisatie. De beheerorganisatie neemt in deze beslissing in ieder geval de volgende informatie op:

- bedrijfsnaam van de betrokken deelnemer/dienstverlener;
- vermelding van de afspraak uit het afsprakenstelsel die niet is nagekomen;
- omschrijving van de feiten waaruit blijkt dat de betreffende afspraak uit het afsprakenstelsel niet is nagekomen;
- de reactie van de betrokken deelnemer/dienstverlener (eventueel met verwijzing naar overgelegde documentatie);
- de redelijke termijn waarin de deelnemer/dienstverlener na het afgeven van de formele waarschuwing alsnog aan de betreffende afspraak uit het afsprakenstelsel kon voldoen;
- de opgelegde (combinatie van) sanctie(s).

Sancties

Sancties kunnen voor een bepaalde termijn worden opgelegd. Na afloop van de termijn kan de sanctie worden verlengd of kunnen er nieuwe of aanvullende sancties worden opgelegd. Er kunnen meer sancties tegelijkertijd worden opgelegd. Aan de sancties kunnen voorwaarden en voorschriften worden verbonden.

De beheerorganisatie kan één of meer van de onderstaande sancties opleggen:

- een formele waarschuwing;
- uitsluiting bij pilots en nieuwe ontwikkelingen;
- verbod om nieuwe gebruikers aan te nemen;
- verbod om nieuwe dienstverleners te bedienen;

EZ kan een of meer van de onderstaande sancties opleggen:

- Schorsing;
- Beëindiging van de Deelnemersovereenkomst;
- Spoedprocedure

Bij het opleggen van een sanctie en de keuze daarvan houdt de beheerorganisatie c.q. EZ rekening met alle omstandigheden van het geval, waaronder de ernst van de overtreding, de inhoud van de niet-nageleefde afspraak, het publieke belang, de gevolgen van het niet-naleven van de afspraak voor het netwerk van eHerkenning en alle betrokken partijen, eventuele recidive van de deelnemer/dienstverlener, de maatschappelijke en publicitaire consequenties.

Schorsing

Schorsing kan door EZ in verband met het publieke belang worden opgelegd als zelfstandige sanctie of als bijkomende sanctie in geval van toepassing van de spoedprocedure of de eventuele beëindiging van de Deelnemersovereenkomst. Schorsing betekent dat de betreffende deelnemer tijdelijk niet in het netwerk eHerkenning zit en het merk eHerkenning niet mag voeren.

De deelnemer is tijdelijk volledig afgesloten. Als zelfstandige sanctie wordt schorsing alleen opgelegd indien er sprake is van een ernstige schending van het afsprakenstelsel en de Deelnemersovereenkomst, een ernstige schending van de beschikbaarheid, betrouwbaarheid, integriteit en vertrouwelijkheid van eHerkenning, een ernstige aantasting van de reputatie en het imago van eHerkenning, het niet binnen de gestelde redelijke termijn alsnog in overeenstemming met het afsprakenstelsel handelen of het weigeren een niet-naleving van het afsprakenstelsel ongedaan te maken.

Een beschrijving van het proces tot schorsing is opgenomen in Proces uittreden.

Beëindiging van de Deelnemersovereenkomst

Als uiterste sanctie in geval van het niet naleven van het afsprakenstelsel, kan EZ in verband met het publieke belang besluiten

om de Deelnemersovereenkomst met de deelnemer te beëindigen, zoals is voorzien in artikel 5.2 van de deelnemersovereenkomst. Het is evident dat deze uiterste sanctie slechts in zeer bijzondere omstandigheden wordt gehanteerd, indien de deelnemer naar het oordeel van EZ het afsprakenstelsel niet kan of wil naleven.

Hiervan is bijvoorbeeld sprake bij een ernstige schending van het afsprakenstelsel en de Deelnemersovereenkomst, een ernstige schending van de beschikbaarheid, betrouwbaarheid, integriteit en vertrouwelijkheid van eHerkenning, een ernstige aantasting van de reputatie en het imago van eHerkenning, het niet binnen de gestelde redelijke termijn alsnog in overeenstemming met het afsprakenstelsel handelen of het weigeren een niet-naleving van het afsprakenstelsel ongedaan te maken.

Voorafgaand aan deze sanctie tot beëindiging van de Deelnemersovereenkomst zal de deelnemer/dienstverlener worden geschorst, teneinde een onderzoek door een onafhankelijk bureau te laten uitvoeren.

Beëindiging van de Deelnemersovereenkomst heeft tot gevolg dat het de voormalig deelnemer niet meer is toegestaan gebruik te maken van het merk eHerkenning, niet meer is toegestaan zich te presenteren als deelnemer/dienstverlener aan eHerkenning en het technisch onmogelijk wordt gemaakt om deel te nemen aan het netwerk voor eHerkenning.

Spoedprocedure

Deze uitzonderlijke procedure wordt door EZ in verband met het publieke belang alleen gebruikt indien vanwege zwaarwegende omstandigheden of dringende spoed de normale nalevingsprocedure, zoals hierboven is beschreven, niet gebruikt kan worden. Voorbeelden van dergelijke omstandigheden zijn een acute en ernstige schending van de verplichtingen uit het afsprakenstelsel en de deelnemersovereenkomst, de acute en ernstige aantasting van de beschikbaarheid, betrouwbaarheid, integriteit en vertrouwelijkheid van eHerkenning en een acute en ernstige aantasting van de reputatie en het imago van eHerkenning.

Indien zich een dergelijke situatie van zwaarwegende omstandigheden of dringende spoed voordoet, zal EZ in principe altijd eerst een schorsing opleggen. Alleen indien op voorhand duidelijk is dat een schorsing, gelet op alle betrokken belangen en omstandigheden, geen adequate remedie kan zijn, is het voor EZ mogelijk direct te besluiten de Deelnemersovereenkomst te beëindigen.

Behalve indien dit vanwege de betreffende omstandigheden niet mogelijk is, zal bij een schorsing aan een onafhankelijke onderzoeksbureau opdracht gegeven worden om op korte termijn de betreffende situatie te onderzoeken alsmede om te beschrijven op welke wijze de deelnemer/dienstverlener het afsprakenstelsel volledig kan naleven. Na ontvangst van het rapport van dit onderzoeksbureau neemt EZ een beslissing. De beslissing kan inhouden het opheffen van de schorsing, het voortzetten van de schorsing (al dan niet met gewijzigde voorwaarden) en de beëindiging van de Deelnemersovereenkomst.

Sancties tegen de beheerorganisatie of EZ

EZ als opdrachtgever van de beheerorganisatie en de beheerorganisatie als opdrachtnemer en uitvoerder van de beheertaken, monitoren en controleren de correcte naleving van het afsprakenstelsel. Zij beogen hiermee een belangrijke elektronische netwerk voor het (laten) verrichten van elektronische diensten mogelijk te maken. Vanuit deze rol hebben zij alleen belang bij het slagen van het afsprakenstelsel en geen enkel belang bij het niet-naleven ervan.

Bovendien is de vraag wie deze sancties dan zou opleggen. Om deze redenen kunnen aan de beheerorganisatie of aan EZ geen sancties worden opgelegd, behalve voor zover dat bepaald is in Sancties.

Het is wel mogelijk om een klacht in te dienen bij de Klachten- en geschillencommissie tegen het optreden en de beslissingen van de beheerorganisatie in het kader van de controle en monitoring op de naleving van het afsprakenstelsel.

Als een Deelnemer of een Dienstverlener het niet eens is met een beslissing van EZ kan de zaak worden voorgelegd aan de civiele rechter, inclusief een vordering tot schadevergoeding.

Compensatieregeling

Naast bovenbedoelde sancties geldt voor de niet-naleving (niet, niet goed, niet volledig of niet tijdig) van implementatiemaatregelen een wederkerige compensatieregeling. Deze regeling is van toepassing bij implementatieplannen waarbij in het voortraject van de totstandkoming duidelijke afspraken zijn gemaakt over de inhoud, de deadline, de concrete maatregelen die de verschillende betrokkenen moeten nemen en de hoogte van de compensatie.

De automatische sanctie bij het niet-naleven van dergelijke implementatiemaatregelen bestaat uit het opleggen van een

passende compensatie, met een maximum van € 10.000,- per implementatiemaatregel.

De compensatie wordt als volgt onderverdeeld:

- bij een implementatiemaatregel met prioriteit Laag: per dag een compensatie van € 250,- met een maximum van € 2.500,-, verspreid over 10 werkdagen.
- bij een implementatiemaatregel met prioriteit Midden: per dag een compensatie van € 500,- met een maximum van € 5.000,-, verspreid over 10 werkdagen.
- bij een implementatiemaatregel met prioriteit Hoog: per dag een compensatie van € 1.000,-- met een maximum van € 10.000,-, verspreid over 10 werkdagen.

Indien na 10 werkdagen de desbetreffende maatregel nog niet is geïmplementeerd zal de beheerorganisatie overeenkomstig het bepaalde in Besluit inzake sancties beslissen of het opleggen van verdere sancties nodig is, tenzij door partijen een beroep wordt gedaan op de uitzondering zoals verwoord in Uitgangspunten compensatieregeling aangaande het aanpassen van het implementatieplan.

Bovenbedoelde compensatie kan zowel aan de deelnemers, dienstverleners als aan de beheerorganisatie worden opgelegd.

De uitgangspunten van de compensatieregeling zijn opgenomen in Uitgangspunten compensatieregeling. Het implementatieplan, waarin de afspraken over de concrete maatregelen, bijbehorende deadlines en bijbehorende prioriteiten zijn vastgelegd, vindt plaats in een afzonderlijk document. Dit implementatieplan wordt vastgesteld in het Tactisch Overleg conform Proces change en release.

Uitgangspunten compensatieregeling

Het uitgangspunt van de compensatieregeling is dat partijen de verplichtingen die op grond van het implementatieplan op hen rusten, uit zichzelf goed naleven. Alle partijen hebben er immers belang bij dat de afspraken die in een implementatieplan worden neergelegd, door alle betrokkenen worden uitgevoerd. De partijen zijn bovendien zelf betrokken bij het opstellen van de implementatieplannen. Daardoor kunnen zij meebeslissen over de afspraken die gelden voor de uitvoering van het implementatieplan. De compensatieregeling is dus bedoeld voor de gevallen waarin één of meer partijen ondanks de afspraken een implementatieplan niet naleven.

Duidelijke afspraken

De afspraken in het implementatieplan moeten voldoende duidelijk en specifiek zijn om te kunnen beoordelen of een partij de afspraken naleeft. Zie voor het proces om te komen tot een duidelijk en gezamenlijk vastgesteld implementatieplan waaraan alle partijen zijn gebonden het "Proces change en release", zie Proces change en release.

Aan een partij die zich geconformeerd heeft aan het implementatieplan, maar zich er vervolgens niet aan houdt, kan in overeenstemming met het nalevingsbeleid – als gevolg van niet naleving van het afsprakenstelsel – een sanctie worden opgelegd. Zie ook Nalevingsbeleid.

Functiescheiding

De beheerorganisatie kan zowel compensatieplichtige als compensatiegerechtigde zijn. Om in deze gevallen een onafhankelijke en objectieve beoordeling van het dossier te waarborgen, wordt (evenals bij de beoordeling van de beheerorganisatie om al dan niet een sanctie op te leggen aan een deelnemer of een dienstverlener) de beoordeling en het nemen van de beslissing door andere personen genomen dan degene die betrokken waren bij de niet naleving. Voor deze functiescheiding richt de beheerorganisatie intern een proces in.

Welke maatregelen

In een implementatieplan staan maatregelen die nodig zijn om het plan uit te voeren. Lang niet alle maatregelen vallen onder de compensatieregeling. De compensatieregeling geldt alleen voor die maatregelen die van aanzienlijk belang zijn voor andere partijen om hun eigen planning te halen. Dit betekent bijvoorbeeld dat een maatregel die betrekking heeft op de oplevering binnen de eigen testomgeving van een partij, niet onder de compensatieregeling valt. Welke maatregelen onder de compensatieregeling vallen, is opgenomen in het implementatieplan.

Concrete maatregelen

In het implementatieplan moet worden vastgelegd welke partij welke maatregel moet nemen. Hoe duidelijker wordt omschreven om welke maatregel het gaat, des te beter kan worden beoordeeld of de betreffende partij zijn verplichtingen op dit punt naleeft.

Deadline

De concrete datum waarop de maatregelen uitgevoerd moeten zijn, moet eenduidig worden vastgelegd.

Hoogte van de compensatie

In het nalevingsbeleid zijn drie soorten compensaties vastgesteld, die afhangen van het risico dat de niet-naleving van de betreffende maatregel uit het implementatieplan heeft: hoog, midden, laag. Het risico wordt bepaald aan de hand van verschillende factoren, zoals urgentie, belang van de maatregel, wederzijdse afhankelijkheid en impact op het Afsprakenstelsel.

Gelet op het vorenstaande wordt voor de beheerorganisatie de volgende indeling gehanteerd:

- een implementatiemaatregel met betrekking tot de publicatie van technische omschrijvingen/koppelvlakspecificaties in het afsprakenstelsel wordt gekwalificeerd als prioriteit Hoog;
- een implementatiemaatregel die betrekking heeft op het beschikbaar stellen en beschikbaar houden van een testtool/simulator wordt gekwalificeerd als prioriteit Midden;
- een implementatiemaatregel die betrekking heeft op de levering van aanvullende tools wordt gekwalificeerd als prioriteit Laag.

Voor de Deelnemers wordt de volgende indeling gehanteerd:

- een implementatiemaatregel die betrekking heeft op beschikbaar stellen van systemen in de productieomgeving wordt gekwalificeerd als prioriteit Hoog;
- een implementatiemaatregel die betrekking heeft op beschikbaar stellen van systemen in de acceptatieomgeving wordt gekwalificeerd als prioriteit Midden;
- een implementatiemaatregel die betrekking heeft op beschikbaar stellen van systemen in de acceptatieomgeving voor een beperkt aantal Deelnemers, bijvoorbeeld bij pilots wordt gekwalificeerd als prioriteit Laag.

Toepassing

Nadat de compensatieregeling voor het implementatieplan is vastgesteld en vastgelegd, is het de taak van de beheerorganisatie om te controleren of iedere partij die een implementatiemaatregel moet uitvoeren, deze verplichting wel naleeft (en daarmee een potentiële compensatiegerechtigde wordt) of niet (niet, niet goed, niet volledig of niet tijdig) naleeft en daarmee een compensatieplichtige wordt. In het geval deelnemers met elkaar of met de beheerorganisatie van mening verschillen over het al dan niet, niet goed, niet volledig of niet tijdig naleven van een maatregel, dient in alle redelijkheid en in samenspraak met alle deelnemers en de beheerorganisatie naar een oplossing te worden gezocht.

Het overzicht van de verschuldigde compensatiebedragen, behorende bij een vastgestelde mijlpaal in het implementatieplan, alsmede welke partij compensatiegerechtigd is, wordt door de beheerorganisatie bijgehouden.

Indien een partij compensatieplichtig wordt, communiceert de beheerorganisatie automatisch aan de compensatieplichtige partij het compensatiebedrag dat hij verschuldigd is als gevolg van het overschrijden van de desbetreffende mijlpaal – overeenkomstig het vastgestelde implementatieplan. Dit gebeurt door middel van een zogenaamde 'Vooraankondiging verschuldigd compensatiebedrag' (hierna: vooraankondiging).

Het uitgangspunt is dat er geen uitzonderingen worden gemaakt ten aanzien van het verschuldigd worden van de compensatie. Er kan alleen een uitzondering worden gemaakt in het geval deze uitzonderingspositie unaniem door alle compensatiegerechtigden wordt geaccordeerd. De partij die gebruik wenst te maken van deze uitzondering draagt zelf zorg voor een unaniem akkoord van de andere betrokken partijen en overlegt het bewijs hiervan aan de beheerorganisatie. Zie ook Proces change en release.

Indien door een niet-tijdige levering van de eerste partij in de keten vervolgens een keten van niet-naleving ontstaat, wordt het implementatieplan alleen aangepast indien alle partijen in de keten hiertoe unaniem besluiten. Op eerste verzoek van één van de partijen in de keten die gebruik wenst te maken van deze uitzondering start de beheerorganisatie een inventarisatie ten aanzien van de vraag over de wenselijkheid van een aanpassing van het implementatieplan. In het geval wordt vastgesteld dat alle betrokken partijen hiermee akkoord gaan, wordt het implementatieplan aangepast in overeenstemming met het proces dat hiervoor is opgenomen in Proces change en release.

Indien unaniem is besloten tot wijziging van het implementatieplan worden de nieuwe deadlines wederom gekoppeld aan compensatiebedragen. Deze compensatiebedragen worden in overeenstemming met de compensatieregeling door de beheerorganisatie bijgehouden en door middel van de vooraankondiging aan de desbetreffende partij(en) gecommuniceerd. Dit kan betekenen dat als een bepaalde maatregel voor de tweede maal niet wordt gehaald, hier wederom het compensatiebedrag voor in rekening wordt gebracht. Anderzijds geldt dat ook voor dit aangepast implementatieplan partijen een beroep kunnen doen op de voornoemde uitzonderingsmogelijkheden.

Indien de compensatieplichtige door de beheerorganisatie een compensatie opgelegd krijgt, is het de compensatieplichtige partij toegestaan om, in overeenstemming met hetgeen daarover bepaald is in het Nalevingsbeleid, een klacht in te dienen bij

de klachten- en geschillencommissie of een rechtszaak aanhangig te maken bij de civiele rechter.
Betrokken partijen kunnen ook gebruik maken van de klachten- en geschillenprocedure in het geval de beheerorganisatie besluit niet tot het opleggen van een compensatie over te gaan. Dit geldt uiteraard ook ten aanzien van de beslissing om zichzelf in een bepaald geval geen de compensatie op te leggen.

Op het moment dat de release van het Afsprakenstelsel eHerkenning – waarop het implementatieplan betrekking heeft – feitelijk wordt opgeleverd, is de beheerorganisatie ervoor verantwoordelijk dat het totaal overzicht van te betalen en te ontvangen compensatiebedragen aan deelnemers ter beschikking wordt gesteld. Zie ook het proces dat hiervoor is opgenomen in Proces change en release.

Het totaaloverzicht van verschuldigde compensatiebedragen biedt inzicht in:

- welke partij voor welk bedrag compensatieplichtig is op basis van welke niet gehaalde maatregel(en);
- welke partij voor welk bedrag compensatiegerechtigd is op basis van welke niet gehaalde maatregel(en) van welke partij(en).

De opbrengst van de compensatiebedragen wordt in gelijke gedeeltes verdeeld over alle compensatiegerechtigde partijen die:

1. op grond van het betreffende implementatieplan één of meer implementatiemaatregelen moesten nemen waarop de compensatieregeling van toepassing is en daarnaast
2. één of meer van deze implementatiemaatregelen goed hebben nageleefd.

Dat wil zeggen dat ook partijen die een andere implementatiemaatregel moesten uitvoeren en dit goed hebben gedaan, meedelen in de opbrengsten van de compensatie. Tegelijkertijd betekent het dat partijen die alleen maatregelen moesten nemen die niet onder de compensatieregeling vallen, niet compensatiegerechtigd zijn en dus ook niet meedelen in de opbrengst.

De compensatieplichtige partijen zijn na ontvangst van het totaal overzicht van de verschuldigde compensatiebedragen zelf verantwoordelijk voor de betaling aan de compensatiegerechtigden. De betaling moet worden verricht binnen dertig dagen na dagtekening van ontvangst van het totaaloverzicht,

In het geval niet wordt overgegaan tot betaling, staat het betrokken partijen vrij gebruik te maken van de klachten- en geschillencommissie danwel een rechtszaak aanhangig te maken bij de civiele rechter, danwel de beheerorganisatie te verzoeken overeenkomstig Nalevingsbeleid het nalevingsbeleid toe te passen.

Toetredingseisen

Alle deelnemers aan het afsprakenstelsel dienen te voldoen aan de algemene toetredingseisen. De toetredingseisen worden gesteld om een aantal redenen. De belangrijkste daarvan is de wetenschap dat het netwerk alleen goed zal kunnen functioneren als afnemers van diensten voldoende vertrouwen hebben in het afsprakenstelsel. Vertrouwen in het afsprakenstelsel en in de eHerkenningsdiensten die in kader van het afsprakenstelsel geleverd worden vereist vertrouwen in de individuele deelnemers. Het afsprakenstelsel moet dus voorzien in duidelijke inhoudelijke eisen op basis waarvan deelnemers mogen toetreden (en uittreden).

Algemene toetredingseisen

Het is van belang dat de deelnemer identificeerbaar is en kan voldoen aan zijn verplichtingen. Daarvoor is het volgende nodig:

- De deelnemer drijft een onderneming en is ingeschreven in het Nederlandse Handelsregister
- De deelnemer hanteert binnen eHerkenning uitsluitend een geregistreerde handelsnaam.
- De deelnemer verkeert niet in staat van faillissement, aan hem is geen surséance van betaling verleend en voor hem geldt geen schuldsaneringsregeling. Ook is ten aanzien van de deelnemer geen faillissement aangevraagd en heeft de deelnemer niet opgehouden zijn schulden te betalen.

Als combinaties van deelnemers willen toetreden dan is dat mogelijk. In dat geval dienen alle deelnemers te voldoen aan de toetredingseisen.

Wanneer een deelnemer bij het vervullen van zijn rol (mede) gebruik maakt van andere marktpartijen, hoofd- of onderaannemers of partijen waarmee een ander verband bestaat, dan hoeven deze andere partijen niet toe te treden tot het afsprakenstelsel. De deelnemer moet dat natuurlijk wel. In dat geval geldt de eis dat de deelnemer aansprakelijk is voor de nakoming van alle verplichtingen van deze combinatie wat betreft eHerkenningsdiensten en dat alleen de deelnemer eHerkenningsdiensten verricht. De deelnemer dient de eHerkenningsdiensten op eigen naam uit te voeren. De beheerorganisatie kan naleving van het afsprakenstelsel door de deelnemer op grond van het nalevingsbeleid monitoren en controleren.

Indien de combinatie onder een gemeenschappelijke naam eHerkenningsdiensten wil verrichten, dienen de leden van de combinatie vanaf de start van deelname zodanig samen te werken dat ieder van de combinanten hoofdelijk aansprakelijk is voor

de volledige en correcte nakoming van alle verbintenissen jegens de beheerorganisatie. Alle combinanten dienen te voldoen aan de toetredingseisen. Bij wijziging in de samenstelling van de combinatie moet de toetredingsprocedure voor nieuwe combinanten opnieuw worden doorlopen.

Ter bevordering van de kwaliteit van eHerkenningsdienstverlening, dient bij het leveren van eHerkenningsdiensten betrokken personeel voldoende bekwaam te zijn. Daarvoor is het volgende nodig:

De deelnemer heeft op basis van CV's van personeel aangetoond over voldoende opleiding en ervaring te beschikken om aan het afsprakenstelsel te kunnen voldoen, met name op de volgende gebieden: juridisch, techniek, standaarden en het aanbieden van online diensten. Het betreffende personeel hoeft niet in een arbeidsrelatie tot de deelnemer te staan, het gaat erom dat de deelnemer kan aantonen dat het personeel dat bij het leveren van eHerkenningsdiensten betrokken is, voldoende opgeleid en ervaren is. Een deelnemer kan op andere wijze invulling geven aan het aantonen van kwalificaties van de mensen waarvan zij gebruik maken die relevant zijn in kader van eHerkenning.

Wat betreft de toetredingsprocedure geldt dat:

- De deelnemer de toetredingsprocedure als beschreven in het afsprakenstelsel dient te accepteren en met goed gevolg dient te doorlopen. Het voorafgaand aan de toetreding succesvol doorlopen van de testen van de conformiteit van technische voorzieningen is hier onderdeel van.
- De deelnemer alle processen en procedures die noodzakelijk zijn voor het leveren van eHerkenningsdiensten op het gespecificeerde betrouwbaarheidsniveau volledig dient te hebben gedocumenteerd en dienaangaande de door de beheerorganisatie opgestelde zelfverklaring dient in te vullen en op te leveren. Wanneer een deelnemer relevante wijzigingen aanbrengt kan het zijn dat onderdelen van de toetredingsprocedure herhaald moeten worden.
- De deelnemer beschikt over de certificaties die expliciet voor het afsprakenstelsel noodzakelijk zijn of die uit toepasselijke wet- en regelgeving volgen.
- De deelnemer de deelnemersovereenkomst dient te ondertekenen en deze volledig dient te accepteren.

Juridische structuur afsprakenstelsel eHerkenning

Het vertrouwen dat partijen in elkaar stellen bij gebruik van het Netwerk (voor eHerkenning) is gebaseerd op overeenkomsten die worden gesloten tussen:

1. De Beheerorganisatie (BO) en de Deelnemers;
2. De deelnemers en degenen aan wie diensten worden verleend

De samenwerking van partijen is daarbij gebaseerd op de volgende documenten:

1. Beheer Afsprakenstelsel eHerkenning samen met
2. de Template deelnemersovereenkomst, en
3. de Gebruiksvoorwaarden eHerkenning

Het afsprakenstelsel geldt voor alle partijen die deelnemen aan of gebruik maken van eHerkenning. Het afsprakenstelsel is vastgelegd in een aantal documenten. Zie Afsprakenstelsel eHerkenning voor een opsomming van deze documenten. In al deze documenten kunnen voor een of meer partijen juridisch bindende verplichtingen zijn neergelegd. Vanzelfsprekend moeten alle juridisch bindende verplichtingen door de betreffende partij worden nageleefd.

De deelnemersovereenkomst bevat de basisafspraken tussen de beheerorganisatie en de deelnemers. Deze overeenkomst is voor alle deelnemers gelijk. Deze overeenkomst zorgt ervoor dat de deelnemers gebonden zijn om de op hen rustende verantwoordelijkheden en verplichtingen zorgvuldig uit te voeren en binden de deelnemers ook aan de besturings- en nalevingsafspraken die noodzakelijk zijn voor het borgen van het vertrouwen. Deelnemers mogen alleen eHerkenningsdiensten verrichten indien zij deze deelnemersovereenkomst hebben gesloten met de beheerorganisatie.

De gebruiksvoorwaarden zijn van toepassing op alle overeenkomsten die een deelnemer (Middelenuitgever (MU), Authenticatiedienst (AD) of Machtigingenregister (MR) sluit met een Dienstafnemer, en op alle overeenkomsten die een deelnemer (eHerkenningsmakelaar (HM) of ondertekendienst) sluit met een Dienstverlener (DV). De deelnemers zijn, binnen de kaders van het afsprakenstelsel, vrij om zelf met de dienstafnemers of dienstverleners in een overeenkomst nadere afspraken te maken over de inhoud en de omvang van hun dienstverlening. Een deelnemer dient echter wel altijd de gebruiksvoorwaarden van toepassing te verklaren tussen hem en de dienstafnemer of tussen hem en de dienstverlener, maar in de verdere inrichting van zijn overeenkomst is hij vrij.

Alle bovenstaande relaties zijn privaatrechtelijk van aard.

Aanvullende verplichtingen

In aanvulling op de juridisch bindende verplichtingen uit de genoemde documenten (Afsprakenstelsel eHerkenning, Template deelnemersovereenkomst en Gebruiksvoorwaarden eHerkenning) gelden specifiek nog de onderstaande verplichtingen voor de deelnemers en de dienstverleners

:

- Informatieplicht deelnemer: verstrekking van alle noodzakelijke informatie aan de beheerorganisatie met betrekking tot deelname aan het netwerk voor eHerkenning.
- Beveiliging- en auditverplichtingen: De deelnemers en dienstverleners zijn verantwoordelijk voor de beveiliging en controle van de eigen netwerkverbindingen en systemen en voldoen aan de auditverplichtingen, conform wet- en regelgeving en zoals vastgelegd in het afsprakenstelsel.
- Intellectuele eigendom: Alle Intellectuele Eigendom voor alle soorten zaken die worden ontwikkeld door, voor of namens de beheerorganisatie, komen toe aan de beheerorganisatie behoudens hetgeen hierover is bepaald in het document Interface specifications. De deelnemers en dienstverleners dienen zich te onthouden van inbreuken op de Intellectuele Eigendomsrechten van zaken die door, voor of namens de beheerorganisatie zijn ontwikkeld.
- Geheimhouding: Partijen dienen strikte geheimhouding in acht nemen ten aanzien van vertrouwelijke informatie en informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt. Naleving van deze verplichting zal geen vrijwaring van strafrechtelijke vervolging met zich meebrengen.
- Klachtenregeling: Indien goed onderling overleg tussen partijen niet tot oplossing van het geschil leidt, kan elke partij een klacht voorleggen aan de onafhankelijke klachten- en geschillencommissie. Zie het reglement klachten- en geschillencommissie.
- Wijziging Gebruiksvoorwaarden eHerkenning: De beheerorganisatie is gerechtigd de Gebruiksvoorwaarden te wijzigen nadat deze zijn vastgesteld overeenkomstig de change en release cyclus van eHerkenning. Deelnemers communiceren de gewijzigde Gebruiksvoorwaarden eHerkenning richting hun klanten.
- Overdraagbaarheid rechten en verplichtingen afsprakenstelsel: Partijen zijn niet bevoegd hun rechten en verplichtingen uit het afsprakenstelsel over te dragen aan een derde, behalve na schriftelijke toestemming van diens wederpartij en voor zover de afspraken neergelegd in het afsprakenstelsel zich niet tegen deze overdracht verzetten. In het geval deelnemer zijn rechten en plichten wil overdragen, dient de overnemende Partij eveneens toegetreden te zijn tot het netwerk voor eHerkenning als deelnemer in dezelfde rol en op hetzelfde betrouwbaarheidsniveau.
- Merkenrecht: het ministerie van Economische Zaken (EZ) is, om zijn verantwoordelijkheden voor eHerkenning waar te kunnen maken, eigenaar van het merkenrecht betreffende eHerkenning. De Staat der Nederlanden is dus eigenaar van het merk 'eHerkenning'. Het merkenrecht is gekoppeld aan toe- en uittreding en daarmee een belangrijk sturingsinstrument voor EZ. In het afsprakenstelsel is een transparante procedure vastgelegd die potentiële deelnemers gelijke kansen biedt rond toetreding. In het afsprakenstelsel is eveneens een procedure voor vrijwillige en onvrijwillige uittreding opgenomen. Bij onvrijwillige uittreding wordt het publieke belang van het stelsel op objectieve en onderbouwde gronden gewogen tegen de belangen van de deelnemer en diens gebruikers. In de praktijk zal EZ deze bevoegdheden niet veelvuldig gebruiken. De governance van het afsprakenstelsel voorziet in procedures die onder meer de normale gang van zaken omtrent toe- en uittreding en uitvoering van het nalevingsbeleid op zich nemen.
- De informatietaak van de beheerorganisatie: publicatie wat conform het afsprakenstelsel verstrekt dient te worden en bescherming van concurrentiegevoelige informatie.

Vertegenwoordiging, volmacht en machtiging

Het netwerk voor eHerkenning moet het mogelijk maken om de vertegenwoordigingsbevoegdheid van de uitvoerende natuurlijke persoon te controleren. Vertegenwoordiging (vertegenwoordigen) is de overkoepelende term voor de situatie waarin de ene Natuurlijk persoon (de Vertegenwoordiger) de Bevoegdheid heeft om in naam van een andere persoon (de Vertegenwoordigde) een rechtshandeling te verrichten met het gevolg dat die ander is gebonden door de rechtshandeling.

Vertegenwoordiging is binnen het afsprakenstelsel zowel op grond van het burgerlijk recht als op grond van het bestuursrecht van belang. De privaatrechtelijke kant doet zich voor bij vertegenwoordiging van rechtspersonen en natuurlijke personen. De publiekrechtelijke kant is van belang bij vertegenwoordiging van bestuursorganen.

Voor de wijze waarop een vertegenwoordigingsbevoegde kenbaar maakt namens een ander te handelen bestaan geen vaste vormen. Het Burgerlijk Wetboek legt wel vast dat degene die gevraagd wordt bevoegdheid te vertrouwen (hier: de dienstverlener) een schriftelijke onderbouwing kan vragen of een bevestiging van de vertegenwoordigde. Voor overheidsdienstverleners volgt dit eveneens uit art. 2.1 Algemene Wet Bestuursrecht.

Elektronisch gebruik van vertegenwoordigingsbevoegdheden vereist vastlegging in elektronische vorm. De partij die verantwoordelijk is voor deze registratie is het machtigingsregister. Deze moet bewijs vastleggen dat de elektronische bevoegdheid is terug te voeren op de wil van de vertegenwoordigde dienstafnemer om zich op die wijze te laten vertegenwoordigen of op wettelijke vertegenwoordiging.

Bij de vastlegging in elektronische vorm wordt de strekking van de vertegenwoordigingsbevoegdheid uitgedrukt in termen van

de elektronische diensten die de bevoegde namens de vertegenwoordigde mag uitvoeren. Deze vastlegging is de verantwoordelijkheid van de vertegenwoordigde dienstafnemer. Deze moet de strekking correct opgeven aan het machtigingsregister. Het machtigingsregister controleert dat de strekking niet breder is dan uit het meegeleverde bewijs blijkt. (Naast deze beperking kunnen er nog andere beperkingen aan de strekking bestaan).

Een vertegenwoordigingsbevoegdheid eindigt door herroeping door de vertegenwoordigde of doordat hetzij de vertegenwoordigingsbevoegde, hetzij de vertegenwoordigde overlijdt, opgeheven wordt, onder curatele komt, failliet wordt verklaard of in schuldsanering komt. Dit moet tevens leiden tot beëindiging van iedere elektronische registratie van betreffende vertegenwoordigingsbevoegdheid.
In een machtigingsregister vastgelegde bevoegdheden worden beschouwd als informatie die alleen gedeeld mag worden met de betrokkenen: de vertegenwoordigde, degene die laat registreren en de bevoegde. Verklaringen worden alleen verstrekt voor dienstverleners die de in een bevoegdheid opgenomen dienst aanbieden en in de dienstencatalogus hebben laten registreren.

Privaatrechtelijke vertegenwoordiging

Vertegenwoordigingsbevoegdheid kan ontstaan op grond van de wet of op grond van volmacht. Voorbeelden van vertegenwoordiging op grond van de wet zijn:

- vertegenwoordiging van minderjarigen door ouders of voogd;
- vertegenwoordiging van onder curatele gestelden door een curator;
- vertegenwoordiging van rechtspersonen zoals verenigingen, stichtingen, NV's en BV's, door hun bestuurders;
- vertegenwoordiging door een zaakwaarnemer die andermans belangen waarneemt.

Volmacht is de bevoegdheid die een volmachtgever verleent aan een ander, de gevolmachtigde, om in zijn naam rechtshandelingen te verrichten. Hieronder wordt ook verstaan het in ontvangst nemen van een verklaring. Het gaat erom dat voor de derde duidelijk is dat de gevolmachtigde als vertegenwoordiger voor een ander, namelijk de volmachtgever, optreedt. Met het geven van een volmacht blijft de bevoegdheid van de volmachtgever om zelf te handelen te allen tijde bestaan.

Een volmacht kan uitdrukkelijk of stilzwijgend worden verleend. De wet maakt een onderscheid tussen de algemene volmacht en de bijzondere volmacht. Een rechtshandeling verricht door de gevolmachtigde, binnen de grenzen van zijn volmacht en in naam van de volmachtgever, bindt de volmachtgever. De gevolmachtigde "valt er tussenuit". Juridisch zijn de volmachtgever en de derde aan elkaar gebonden. Indien de gevolmachtigde buiten zijn volmacht handelt, is de volmachtgever toch gebonden indien hij de betreffende rechtshandeling bekrachtigt, of indien er sprake is van de schijn van volmachtverlening, dan wel de schijn van vertegenwoordigingsbevoegdheid. De schijn van volmachtverlening doet zich voor indien een pseudo-gevolmachtigde zonder een toereikende volmacht handelt en de derde op grond van een verklaring of gedraging van de pseudo-volmachtgever heeft aangenomen en onder de gegeven omstandigheden redelijkerwijs mocht aannemen dat er wel een toereikende volmacht was verleend.

Publiekrechtelijke vertegenwoordiging

De Machtiging (machtigen) heeft de volgende juridische achtergrond. In bestuursrechtelijke verhoudingen kan een ieder zich ter behartiging van zijn belangen in het verkeer met bestuursorganen:

- laten bijstaan; of
- door een gemachtigde laten vertegenwoordigen.

Door te spreken van machtiging in plaats van volmacht wenst de wetgever aan te geven dat de regeling van volmacht niet rechtstreeks van toepassing is maar alleen "voor zover de aard van de rechtshandeling of de rechtsbetrekking zich daartegen niet verzet". In de documentatie van eHerkenning wordt de term machtiging ook in meer algemene zin gebruikt wanneer vertegenwoordigingsbevoegdheid bedoeld is.

Ketenmachtiging

Bij ketenmachtigingen gaat het om het doorgeven van een volmacht. Dit wordt ook het recht op substitutie genoemd. Het uitgangspunt van het recht op substitutie is dat dit recht expliciet door de volmachtgever aan de gemachtigde moet worden verleend. Vervolgens kan de gemachtigde, op grond van dit recht op substitutie, de volmacht doorgeven. De substituut volmacht kan zowel aan een natuurlijk persoon als aan een onderneming of rechtspersoon worden verleend. De volmachtgever dient in de volmacht aan de gevolmachtigde op te nemen of de gevolmachtigde al dan niet met toestemming van de volmachtgever de volmacht aan een ander (substituut volmacht) mag verlenen.

Een ander uitgangspunt bij het recht op substitutie is dat de volmachtgever tenminste op de hoogte moet worden gesteld in het

geval substitutie plaatsvindt zodat hij kan bepalen of hij de vertegenwoordigingsbevoegd van de substituut gevolmachtigde wil handhaven.

Dit uitgangspunt geldt o.m. niet voor de bevoegde die zijn werknemer inzet om de aan hem verleende bevoegdheden te gebruiken. Verder kan in een overeenkomst door een vertegenwoordigde "anders bepaald" worden.

Een vertegenwoordigde weet dus wie namens hem zou kunnen handelen, met uitzondering mogelijk van de laatste schakel, indien dit een werknemer is van de één na laatste bevoegde. Andersom wordt er van uitgegaan dat degene die als bevoegde optreedt dit met een helder doel voor ogen doet, namelijk het realiseren van een rechtshandeling voor de vertegenwoordigde, derhalve kan er van uitgegaan worden dat deze de hele keten naar zich toe kent.

In een keten van vertegenwoordiging kent eenieder de keten "boven" hem. Ieder kent ook degene aan wie hij zelf een bevoegdheid heeft verleend op grond van substitutie. De vertegenwoordigde tenslotte kent de hele keten, met uitzondering van de laatste schakel indien dit een werknemer van de bevoegde betreft en voorzover niet anders bepaald bij overeenkomst.

De vertegenwoordigde moet een bevoegdheid en een verleend recht van substitutie te allen tijde kunnen intrekken. Eveneens moet een bevoegde die substitutie heeft verleend deze kunnen intrekken. Derhalve moet een geregistreerde bevoegdheid te allen tijde kunnen worden ingetrokken door degene die daartoe gerechtigd is.

Evenals bij een volmacht blijft bij een substituut volmacht, de volmachtgever bevoegd de rechtshandelingen waarvoor volmacht is verleend te verrichten, De bevoegdheid om zelf te handelen blijft ook voor de gemachtigde bestaan. Dit is slechts anders als tussen partijen is overeengekomen, bijvoorbeeld in een overeenkomst tot lastgeving, dat de volmachtgever voor de duur van die overeenkomst zelf niet meer bevoegd is de betreffende rechtshandelingen te verrichten.

Het is mogelijk het recht van substitutie ook van toepassing te verklaren op vormen van vertegenwoordiging die niet voortvloeien uit volmacht, zoals machtigingen voor publiekrechtelijke taken of mandatering binnen een overheidsorganisatie. Door voor het publiekrechtelijke domein te spreken van machtiging in plaats van volmacht, wenst de wetgever aan te geven dat de regeling van volmacht niet rechtstreeks van toepassing is maar alleen "voor zover de aard van de rechtshandeling of de rechtsbetrekking zich daartegen niet verzet". Zie ook artikel 3:79 BW. Een dergelijke beperking kan bijvoorbeeld zijn gelegen in specifieke wet en regelgeving voor een overheidsdienstverleners.

Aansprakelijkheid

Binnen het afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten binnen de rol die hij vervult. Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. De deelnemers mogen en kunnen niet afwijken van deze algemene regels. Hoe deze regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval.

De deelnemer kan zijn aansprakelijkheid beperken in de overeenkomst die hij sluit met een dienstafnemer of met een dienstverlener. Daarbij blijft hij gebonden aan de algemene regels van het Nederlandse recht inzake aansprakelijkheid en schadevergoeding.

Betrouwbaarheidsniveaus

Het vaststellen van het voor een bepaalde dienst vereiste Betrouwbaarheidsniveau wordt bepaald door de dienstverlener. Dit geldt zowel voor een publiek- als een privaatrechtelijke dienstverlener. De overheidsdienstverlener moet ter naleving van de Awb invulling geven aan de norm van een betrouwbare en vertrouwelijke communicatie.

De dienstverlener zal dus steeds bij het aanbieden van een dienst een risicoanalyse moeten uitvoeren en na moeten gaan welke maatregelen moeten worden genomen om de elektronische communicatie voldoende betrouwbaar en vertrouwelijk te laten plaatsvinden. Onderdeel hiervan is een keuze voor het vereiste betrouwbaarheidsniveau voor een bepaalde dienst waarvoor eHerkenningsdiensten worden gebruikt. Naast het vaststellen van het door de dienstverlener gekozen betrouwbaarheidsniveau zal de overheidsdienstverlener nog andere maatregelen moeten nemen om een dienst conform de vereisten van de Awb betrouwbaar elektronisch aan te bieden. De extra te treffen maatregelen zijn afhankelijk van het betrouwbaarheidsniveau.

Waar eHerkenning wordt toegepast voor e-diensten buiten de overheid (B2B en B2C) gelden de specifieke Awb eisen uiteraard niet. In geval van B2B en B2C diensten geldt dat middelenuitgevers, machtigingenregisters en ook de betreffende dienstverleners een "dienst van de informatiemaatschappij" en/of een zogenaamde 'dienst op afstand' I als gedefinieerd in het Burgerlijk Wetboek) aanbieden. Deze partijen zijn zelf verantwoordelijk om aan de daarbij behorende informatieplichten en plichten ten aanzien van de totstandkoming van een rechtsgeldige overeenkomst, zoals opgenomen in het Burgerlijk Wetboek, te voldoen.

Rol van eHerkenningsmakelaars

De Herkenningsmakelaars hebben een speciale rol ten opzichte van de bij hen aangesloten dienstverleners. De eHerkenningsmakelaars fungeren namelijk als centraal aanspreekpunt voor zowel de dienstverlener als de beheerorganisatie. Dit brengt onder andere met zich mee dat de eHerkenningsmakelaar alle benodigde informatie aan de dienstverlener en de beheerorganisatie moet verstrekken. Deze informatie betreft in ieder geval: de gegevens van de contactpersoon voor calamiteiten en ernstige incidenten eHerkenning, de gegevens van de contactpersoon voor communicatie betreffende de dienstverlener en eindgebruiker over eHerkenning en de gegevens van de contactpersoon voor (door)ontwikkeling eHerkenning.

De eHerkenningsmakelaar mag alleen eHerkenningsdiensten verlenen aan dienstverleners die zijn toegelaten tot het netwerk van eHerkenning. De eHerkenningsmakelaar voert deze test uit. Voorts beoordeelt de eHerkenningsmakelaar gedurende de looptijd van de overeenkomst met de dienstverlener, of de dienstverlener blijft voldoen aan de op hem rustende verplichtingen op grond van het afsprakenstelsel.

Indien de eHerkenningsmakelaar hieromtrent twijfelt of van mening is dat dit niet langer het geval is, geeft hij dit terstond door aan de beheerorganisatie. Indien de beheerorganisatie dit verzoekt, zal de eHerkenningsmakelaar terstond zijn dienstverlening aan de dienstverlener schorsen of beëindigen.

Gebruiksvoorwaarden eHerkenning

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Deze Gebruiksvoorwaarden zijn van toepassing op het verlenen van diensten door Deelnemers aan Dienstverleners en Dienstafnemers in het kader van het Netwerk voor eHerkenning.

- Artikel 1. Definities
- Artikel 2. Toepassingsgebied
- Artikel 3. Tussentijdse beëindiging van de Overeenkomst door beëindiging deelname
- Artikel 4. Beperking van aansprakelijkheid
- Artikel 5. Geheimhouding
- Artikel 6. Achterhalen netwerkfalen
- Artikel 7. Overdraagbaarheid rechten en verplichtingen Overeenkomst
- Artikel 8. Toepasselijk recht
- Artikel 9. Geschillen
- Artikel 10. Dienstafnemer
- Artikel 11. Beveiligingsverplichting van de Dienstafnemer
- Artikel 12. Toezicht van de Dienstafnemer op gedragingen van personen
- Artikel 13. Vervulling rol(len) door de Dienstafnemer
- Artikel 14. Vaststellen openstellingsbesluit
- Artikel 15. Melding onregelmatigheden
- Artikel 16. Beveiliging
- Artikel 17. SSO
- Artikel 18. Beveiliging
- Artikel 19. Betrouwbaarheidsniveaus
- Artikel 20. Informatieverplichting
- Artikel 21. Privacy
- Artikel 22. Cookies
- Artikel 23. Verplichtingen van de Herkenningsmakelaar
- Artikel 24. Verplichtingen van de Authenticatiedienst
- Artikel 25. Verplichtingen van de Middelenuitgever
- Artikel 26. Verplichtingen van het Machtigingenregister
- Artikel 27. Verplichtingen van de Ondertekendienst

Artikel 1. Definities

Alle in deze Gebruiksvoorwaarden met een hoofdletter geschreven begrippen hebben de volgende betekenis.

- Afsprakenstelsel: het geheel aan afspraken op gebied van organisatie, besturing, controle, naleving, beheer, architectuur, toepassingen, techniek, procedures en regels aangaande het Netwerk voor eHerkenning in een bepaalde vastgestelde versie. Het doel is betrouwbare authenticatie, registratie van machtigingen en verstrekking van identiteitsinformatie op basis van de eHerkenningsdiensten van een goed gereguleerd Netwerk voor eHerkenning.
- Authenticatiedienst: een vereiste rol binnen het Netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de handelende natuurlijk persoon gebruikte authenticatiemiddel.
- Authenticatiemiddel: een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een Partij kan plaatsvinden.
- Beheerorganisatie: de Beheerorganisatie van het Afsprakenstelsel die verantwoordelijk is voor het faciliteren van het beheer en de doorontwikkeling van het Afsprakenstelsel, alsmede de controle op en de het monitoren van de naleving van het Afsprakenstelsel door de Dienstverlener en de Deelnemers op basis van het door eHerkenning vastgestelde nalevingsbeleid.
- Betrouwbaarheidsniveau: een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het middel zelf en het gebruik van het middel (het authenticatiemechanisme).

- Beveiligingsincident: een gebeurtenis die een bedreiging vormt of kan vormen voor de betrouwbaarheid, vertrouwelijkheid of beschikbaarheid van eHerkenning.
- Deelnemer: een Partij die conform hetgeen daarover in het Afsprakenstelsel is vastgelegd één of meer rollen vervult binnen het Netwerk voor eHerkenning.
- Dienstafnemer: een bedrijf of een overheidsorganisatie die eHerkenning gebruikt om een dienst af te nemen bij een Dienstverlener. De Dienstafnemer is een partij van de vorm natuurlijk persoon die een onderneming drijft (een eenmanszaak) of van de vorm niet natuurlijk persoon conform de identificatie waarmee hij is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land.
- Dienstverlener: een Partij die elektronische diensten aanbiedt aan Dienstafnemers waarvoor eHerkenningsdiensten voorwaardelijk zijn.
- Gebruiker: een Dienstverlener of Dienstafnemer die eHerkenning gebruikt om respectievelijk de toegang tot een van haar diensten mee te beveiligen of toegang te vragen tot een dergelijke dienst met het oog op het afnemen van die dienst.
- Gemachtigde: de Partij die (op grond van wet of machtiging c.q. volmacht) bevoegd is om in naam van de vertegenwoordigde bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de vertegenwoordigde.
- Herkenning: ieder van de functies van het Netwerk voor eHerkenning gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen Dienstverleners en Dienstafnemers en de daarin betrokken handelende natuurlijke personen.
- eHerkenningsdiensten: diensten voor herkenning, te weten: authenticatie, machtiging, controle van bevoegdheden, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.
- Herkenningsmakelaar: een rol binnen het Netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die het single point of contact vormt voor de Dienstverlener en waarlangs Dienstverleners Herkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de Dienstverleners te ontkoppelen van de interne berichten binnen het Netwerk en die optreedt als routeerder naar alle deelnemende Authenticatiediensten, Machtigingenregisters en Ondertekendiensten.
- Machtigingenbeheerder: een handelende natuurlijk persoon met de bevoegdheid om namens een Dienstafnemer machtigingen te registreren, te schorsen, in te trekken en anderszins bijbehorende registratieprocessen uit te voeren.
- Machtigingenregister: een vereiste rol binnen het Netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de handelende natuurlijk persoon verstrekken van machtigingsverklaringen).
- Middelenuitgever: een vereiste rol binnen het Netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die de verantwoordelijkheid heeft voor het uitgeven van authenticatiemiddelen conform de eisen van het gespecificeerde betrouwbaarheidsniveau.
- Netwerk voor eHerkenning: De verzameling onderling verbonden componenten die gereguleerd worden door het Afsprakenstelsel en gezamenlijk eHerkenningsdiensten leveren en daartoe bestaan uit tenminste één invulling door een Deelnemer van de rollen eHerkenningsmakelaar, Machtigingenregister, Authenticatiedienst en Middelenuitgever, mogelijk aangevuld met verdere rollen voor eHerkenningsdiensten zoals een Ondertekendienst, hun onderlinge verbindingen, de verbindingen tot en met het koppelvlak met Dienstverleners en de processen voor uitgifte van middelen, registratie van bevoegdheden en aanmelding voor hergebruik vanuit Dienstafnemers, inclusief de benodigde voorzieningen voor beheer conform het Afsprakenstelsel.
- Ondertekendienst: een rol binnen het Netwerk voor eHerkenning die door een Deelnemer aan het Afsprakenstelsel wordt ingevuld en die de verantwoordelijkheid heeft voor het doen van de wilsuiting, het valideren ervan en het verstrekken van het bijbehorende associatiebewijs.
- Overeenkomst: de overeenkomst tussen de Dienstafnemer en de Deelnemer, of de overeenkomst tussen de Dienstverlener en de Deelnemer, op grond waarvan de Deelnemer Herkenningsdiensten verleent en waarop de Gebruiksvoorwaarden van toepassing zijn.
- Partij: de Deelnemer, de Dienstafnemer en de Dienstverlener.
- SSO: functie die door eHerkenning wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel, waardoor authenticatie van een handelend natuurlijk persoon wordt hergebruikt, waardoor deze handelend natuurlijk persoon niet opnieuw hoeft in te loggen.
- Gebruiksvoorwaarden: deze gebruiksvoorwaarden.

Artikel 2. Toepassingsgebied

De Deelnemer dient deze Gebruiksvoorwaarden van toepassing te verklaren op de Overeenkomst die de Dienstafnemer en de Dienstverlener in het kader van het Netwerk voor eHerkenning sluiten met een Deelnemer.

Een Deelnemer kan één of meer van de volgende rollen vervullen.

- De Middelenuitgever geeft authenticatiemiddelen uit en identificeert natuurlijke personen.
- De Authenticatiedienst authenticeert personen.

- De Ondertekendienst faciliteert het doen van wilsuitingen en legt wilsuitingen vast.
- Het Machtigingenregister faciliteert het registreren, onderhouden en controleren van machtigingen.
- De Herkenningsmakelaar vervult een routeer- en navigeerfunctie en vormt het koppelpunt tussen het Netwerk voor eHerkenning en de Dienstverleners.

Artikel 3. Tussentijdse beëindiging van de Overeenkomst door beëindiging deelname

De Overeenkomst eindigt van rechtswege indien en zodra de deelname van de Deelnemer aan het Netwerk voor eHerkenning eindigt. De Deelnemer stelt de Dienstafnemer en/of de Dienstverlener met wie de Deelnemer een Overeenkomst is aangegaan, door middel van een aangetekende brief direct op de hoogte van deze beëindiging.

Indien de in dit artikel bedoelde tussentijdse beëindiging zich voordoet, is de Deelnemer verplicht alle medewerking te verlenen om de continuïteit van de verlening van eHerkenningsdiensten door andere Deelnemers zeker te stellen.

Artikel 4. Beperking van aansprakelijkheid

De aansprakelijkheid van een Partij jegens de andere Partij is beperkt tot het eigen handelen en/of nalaten in het kader van (de rol binnen) het Afsprakenstelsel.

In het kader van de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

Artikel 5. Geheimhouding

5.1 Partijen zullen strikte geheimhouding in acht nemen ten aanzien van vertrouwelijke informatie en informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, die in het kader van de uitvoering van de Overeenkomst wordt uitgewisseld, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt.

Artikel 6. Achterhalen netwerkfalen

6.1 Onder een netwerkfalen wordt verstaan het niet naar behoren verlopen van een transactie tussen de Dienstafnemer en de Dienstverlener, bijvoorbeeld als gevolg van een Beveiligingsincident dan wel naar aanleiding van de onjuiste verwerking en/of doorgeleiding van:

- de authenticatie van een handelend natuurlijk persoon en/of de Dienstafnemer;
- de registratie van een machtiging;
- een wilsuiting.

6.2 Ingeval van een vermoeden van een netwerkfalen, ondernemen de Dienstafnemer, de Dienstverlener en de Herkenningsmakelaar achtereenvolgens de volgende stappen, totdat de oorzaak van het netwerkfalen is achterhaald of alle stappen zijn doorlopen.

1. de Dienstafnemer gaat na of het netwerkfalen te herleiden is tot een handelen of nalaten van een Gemachtigde die namens de Dienstafnemer handelt.
2. de Dienstafnemer neemt contact op met de Dienstverlener, doet melding van een vermoeden van netwerkfalen en verzoekt de Dienstverlener na te gaan of het vermoeden gestaafd kan worden.
3. De Dienstverlener gaat na of het netwerkfalen te herleiden is tot een handelen of nalaten van de Dienstverlener.
4. De Dienstverlener verzoekt de door hem ingeschakelde Herkenningsmakelaar na te gaan tot welke oorzaak het netwerkfalen is te herleiden.
5. De Herkenningsmakelaar gaat na tot welke oorzaak het netwerkfalen is te herleiden. Indien de Herkenningsmakelaar het netwerkfalen herleidt tot een handelen of nalaten van een andere Deelnemer, en de Herkenningsmakelaar hierover geen overeenstemming bereikt met deze Deelnemer, dient de Herkenningsmakelaar een klacht in bij de klachtencommissie.
6. De Herkenningsmakelaar stelt de Beheerorganisatie op de hoogte van het netwerkfalen.

Artikel 7. Overdraagbaarheid rechten en verplichtingen Overeenkomst

7.1 Partijen zijn niet bevoegd hun rechten en verplichtingen uit de Overeenkomst over te dragen aan een derde, behalve na schriftelijke toestemming van de wederpartij. In het geval een Deelnemer zijn rechten en plichten uit de Overeenkomst wil overdragen, dient de overnemende partij eveneens toegelaten te zijn aan het netwerk voor eHerkenning als Deelnemer in dezelfde rol.

Artikel 8. Toepasselijk recht

8.1 Op deze Gebruiksvoorwaarden is Nederlands recht van toepassing.

Artikel 9. Geschillen

9.1 Alle geschillen die tussen Partijen ontstaan bij de uitvoering van de Overeenkomst, inclusief geschillen met betrekking tot het verhalen van schade, zullen Partijen eerst door middel van onderling overleg trachten te beslechten.

9.2 Indien goed onderling overleg niet tot oplossing van het geschil leidt, zullen Partijen het geschil ter beslechting voorleggen aan de klachten- en geschillencommissie. Zie het reglement van de klachten- en geschillencommissie.

Artikel 10. Dienstafnemer

10.1 De Dienstafnemer voldoet aan alle op hem rustende verplichtingen op grond van het afsprakenstelsel.

10.2 De Dienstafnemer dient aan de Deelnemer tijdig juiste en volledige informatie aan te leveren, indien de Deelnemer daarom verzoekt.

10.3 Indien de Dienstafnemer niet tijdig, dan wel onjuiste en/of onvolledige informatie verstrekt, dan kan dit niet aan de Deelnemer worden toegerekend, tenzij de Deelnemer wist of behoorde te weten dat er sprake is van onjuiste en/of onvolledige informatie en de Deelnemer deze informatie niettemin heeft verwerkt.

10.4 De Dienstafnemer geeft direct alle relevante mutaties door aan de Deelnemer, en trekt direct daaraan gerelateerde Authenticatiemiddelen en machtigingen in of blokkeert deze.

10.5 Indien ten aanzien van een Authenticatiemiddel en/of een machtiging sprake is van onbevoegd of anderszins onjuist gebruik, of indien dit wordt vermoed, doet de Dienstafnemer direct na kennisname melding van aan de betreffende Middelenuitgever, dan wel trekt de Dienstafnemer de registratie van de betreffende machtiging in.

10.6 Indien een Dienstverlener voor het gebruik van een dienst de functionaliteit SSO toestaat, is het de keuze van de Dienstafnemer om al dan niet van deze functionaliteit gebruik te maken.

Artikel 11. Beveiligingsverplichting van de Dienstafnemer

11.1 De Dienstafnemer draagt zorg voor de voldoende beveiliging van de netwerkverbindingen en de systemen die onder diens verantwoordelijkheid vallen en door de Dienstafnemer worden gebruikt in het kader van eHerkenning.

11.2 De Dienstafnemer meldt het aan de Deelnemer indien er een vermoeden is van een Beveiligingsincident. De Deelnemer meldt dit vermoeden van een Beveiligingsincident aan de Beheerorganisatie.

Artikel 12. Toezicht van de Dienstafnemer op gedragingen van personen

12.1 De Dienstafnemer ziet toe op en is verantwoordelijk voor de handelend natuurlijk persoon die optreedt namens de Dienstafnemer. De Dienstafnemer laat geen werkwijze toe die leidt tot onzorgvuldig handelen van zijn vertegenwoordigers,

zoals het gebruik van persoonsgebonden Authenticatiemiddelen door meerdere personen, het onbevoegd gebruik van persoonsgebonden Authenticatiemiddelen, het gebruik van Authenticatiemiddelen voor een ander doel dan het doel waarvoor zij zijn afgegeven, etc.

12.2 De Dienstafnemer ziet er op toe dat degene die het als Machtigingenbeheerder heeft aangewezen zorgvuldig handelt bij de verstrekking en het beheren van die machtigingen alsmede dat deze machtigingen zorgvuldig worden gebruikt.

Artikel 13. Vervulling rol(len) door de Dienstafnemer

13.1 Indien de Dienstafnemer zelf één of meer rollen binnen het Netwerk voor eHerkenning vervult, gelden voor hem alle verplichtingen die aan de desbetreffende rol zijn verbonden.

Artikel 14. Vaststellen openstellingsbesluit

14.1 De Dienstverlener voldoet aan alle op hem rustende verplichtingen op grond van het afsprakenstelsel; het nalevingsbeleid is van toepassing op de dienstverlener.

14.2 De Dienstverlener maakt kenbaar dat hij de elektronische weg heeft opengesteld en geeft daarbij aan welke diensten langs elektronische weg kunnen worden afgenomen.

14.3 In het openstellingbesluit maakt de Dienstverlener een keuze voor één of meer Betrouwbaarheidsniveaus. Bij het maken van de keuze voor één of meer Betrouwbaarheidsniveaus kan de Handreiking Betrouwbaarheidsniveau van het Forum Standaardisatie als handreiking worden gebruikt. De keuze voor een Betrouwbaarheidsniveau is de uitsluitende verantwoordelijkheid van de Dienstverlener. De Deelnemer is niet aansprakelijk voor schade die ontstaat ten gevolge van een door de Dienstverlener vastgesteld Betrouwbaarheidsniveau. Dit laat de aansprakelijkheid van de Deelnemer voor de eigen dienstverlening onverlet.

Artikel 15. Melding onregelmatigheden

15.1 In het geval de Dienstverlener ten aanzien van aan haar verstrekte herkenningsgegevens onregelmatigheden constateert of een vermoeden daarvan heeft, doet de Dienstverlener hiervan direct melding aan de Herkenningsmakelaar waarmee zij een Overeenkomst heeft afgesloten.

Artikel 16. Beveiliging

16.1 De Dienstverlener is verantwoordelijk voor de beveiliging en controle van de eigen systemen, netwerken die worden gebruikt, de website en de koppeling met de Herkenningsmakelaar. De Dienstverlener voldoet aan de eisen van het Afsprakenstelsel inzake onder meer de beveiliging van de verbinding en haar systemen, de website en de koppeling met de Herkenningsmakelaar.

16.2 Voor zover de Dienstverlener een publiekrechtelijk rechtspersoon is, wordt door deze overheidsdienstverlener – naast de door eHerkenning in het Afsprakenstelsel bekendgemaakte (technische) eisen en voor geschreven beveiligingsmaatregelen – tevens voldaan aan de door het National Cyber Security Center vastgestelde eisen ten aanzien van beveiliging voor elektronische dienstverlening.

16.3 Indien naar het oordeel van de Beheerorganisatie de Dienstverlener niet voldoet aan de in artikel 16.1 en 16.2 bedoelde beveiligingseisen is de Beheerorganisatie gerechtigd, overeenkomstig het nalevingsbeleid zoals opgenomen in het Afsprakenstelsel, maatregelen te nemen. Het nemen van een dergelijke maatregel wordt door de Beheerorganisatie met redenen omkleed.

16.4 De Dienstverlener geeft toestemming tot een controle door een door de Beheerorganisatie aan te wijzen auditeur bij het redelijke vermoeden of na het veroorzaken van een Beveiligingsincident.

Artikel 17. SSO

17.1 eHerkenning ondersteunt SSO. De Dienstverlener is verantwoordelijk voor de keuze om SSO al dan niet toe te staan voor zijn dienstverlening.

17.2 De Dienstverlener geeft bij registratie van de dienst in de dienstencatalogus op of deze SSO toestaat.

17.3 De Dienstverlener zorgt voor laagdrempelige en adequate informatieverstrekking over het gebruik en de werking van SSO aan de Dienstafnemer.

Artikel 18. Beveiliging

18.1 De Deelnemer is verantwoordelijk voor de beveiliging en controle van de netwerkverbindingen en systemen die hij gebruikt in het kader van eHerkenning. De Deelnemer voldoet daarbij aan de eisen van het Afsprakenstelsel.

Artikel 19. Betrouwbaarheidsniveaus

1.1 De Deelnemer ondersteunt de Betrouwbaarheidsniveaus zoals vastgelegd in de Overeenkomst.

Artikel 20. Informatieverplichting

20.1 De Deelnemer is verplicht alle informatie, waaronder informatie over de Overeenkomst, te verstrekken aan de Beheerorganisatie voor zover deze informatie voor de Beheerorganisatie noodzakelijk is om (voortzetting van) deelname aan het Netwerk voor eHerkenning te kunnen beoordelen, naleving van de afspraken van het Afsprakenstelsel te kunnen controleren, dan wel indien dit noodzakelijk is vanwege een geschillen- of klachtenprocedure.

Artikel 21. Privacy

21.1 De Deelnemer gebruikt aan hem verstrekte informatie slechts voor het doel waarvoor deze informatie aan hem is verstrekt. De Deelnemer verstrekt geen informatie aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Overeenkomst informatie mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken.

21.2 De Deelnemer verwerkt uitsluitend persoonsgegevens indien en voor zover dit noodzakelijk is ter uitvoering van de Overeenkomst.

21.3 De Deelnemer verstrekt geen persoonsgegevens die betrekking hebben op de handelend natuurlijk persoon, tenzij:

- de Dienstverlener of de Dienstafnemer deze gegevens opvraagt in het kader van een juridische procedure; of
- er sprake is van een vordering van een bevoegde opsporingsinstantie of toezichthouder; en
- een en ander geschiedt conform de geldende rechtsregels inzake de verstrekking van persoonsgegevens.

21.4 De verwerking van persoonsgegevens in het kader van uitvoering van de Overeenkomst, geschiedt door de Deelnemer overeenkomstig de bepalingen van de Wet bescherming persoonsgegevens.

Artikel 22. Cookies

22.1 Bij bepaalde instellingen die de Gebruiker zelf kiest, wordt gebruik gemaakt van functionele cookies, dat wil zeggen cookies waarvoor geen expliciete toestemming vereist is. Deze cookies worden niet gebruikt voor andere doeleinden dan het faciliteren van de door de Gebruiker gekozen instelling.

Artikel 23. Verplichtingen van de Herkenningsmakelaar

23.1 De Herkenningsmakelaar routeert binnen het Netwerk voor eHerkenning eHerkenningsdiensten ten behoeve van een Dienstverlener conform de Overeenkomst en overeengekomen service levels.

23.2 De Herkenningsmakelaar sluit een duidelijke Service Level Agreement met de Dienstverlener af. Deze Service Level Agreement kan onderdeel uitmaken van de Overeenkomst.

23.3 De Herkenningsmakelaar is verantwoordelijk voor het testen van de Dienstverlener opdat de Dienstverlener, alvorens hij wordt aangesloten op eHerkenning, aan alle in het Afsprakenstelsel opgenomen specificaties voor het gebruik van eHerkenning voldoet. De Herkenningsmakelaar levert een handelende natuurlijk persoon een online interface om de handelende natuurlijk persoon in staat te stellen de voor de keuze van een Authenticatiedienst, een Machtigingenregister en een Ondertekendienst noodzakelijke gegevens te kunnen selecteren.

23.4 De Herkenningsmakelaar draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen. De Herkenningsmakelaar is het centrale aanspreekpunt voor de Dienstverlener en de Beheerorganisatie, onder andere in het geval van calamiteiten of een Beveiligingsincident bij een Dienstverlener. De Herkenningsmakelaar verstrekt als centraal aanspreekpunt de Dienstverlener en de Beheerorganisatie alle benodigde informatie.

23.5 De Herkenningsmakelaar sluit alleen aan het Netwerk voor eHerkenning toegelaten Authenticatiediensten en Machtigingenregisters aan en houdt deze aangesloten, een en ander conform hetgeen hiertoe is vastgelegd in het Afsprakenstelsel.

23.6 De Herkenningsmakelaar verleent alleen eHerkenningsdiensten aan Dienstverleners die zijn toegelaten tot het Netwerk van eHerkenning. De Herkenningsmakelaar beoordeelt of de Dienstverlener voldoet aan de voor de Dienstverlener geldende verplichtingen van het Afsprakenstelsel en geeft het terstond door aan de Beheerorganisatie indien dit naar zijn mening niet het geval is. De Herkenningsmakelaar is gehouden de dienstverlening aan de Dienstverlener te schorsen of te beëindigen indien de Beheerorganisatie dit verzoekt.

Artikel 24. Verplichtingen van de Authenticatiedienst

24.1 De Authenticatiedienst is verantwoordelijk voor het authenticeren van personen op basis van hun Authenticatiemiddel.

24.2 De Authenticatiedienst verwerkt een Authenticatievraag conform de Overeenkomst en overeengekomen service levels.

24.3 De Authenticatiedienst ziet erop toe dat Authenticatievragen alleen worden verwerkt indien zij kunnen worden verwerkt aan de hand van toegelaten Authenticatiemiddelen van toegelaten Middelenuitgevers.

24.4 De Authenticatiedienst draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.

24.5 De Authenticatiedienst biedt voorts aan een handelend natuurlijk persoon een online interface om als onderdeel van eHerkenningsdiensten het Authenticatiemiddel te gebruiken teneinde handelende natuurlijke personen zich te laten authenticeren.

Artikel 25. Verplichtingen van de Middelenuitgever

25.1 De Middelenuitgever biedt de volgende functionaliteiten aan handelende natuurlijke personen en/of de Dienstafnemer:

- de uitgifte en het beheer en de intrekking van Authenticatiemiddelen;
- het ten behoeve van de uitgifte identificeren en authenticeren van handelende natuurlijke personen;
- het ondersteunen van één of meer Betrouwbaarheidsniveaus;
- het doorgeven van benodigde informatie aan één of meer Authenticatiediensten conform het Afsprakenstelsel.

25.2 De Middelenuitgever verwerkt Authenticatievragen conform de Overeenkomst en overeengekomen service levels.

25.3 De Middelenuitgever draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.

Artikel 26. Verplichtingen van het Machtigingenregister

26.1 Het Machtigingenregister levert de volgende functionaliteiten aan de Dienstafnemer:

- de registratie van identificerende kenmerken van de Dienstafnemer;
- de registratie van identificerende kenmerken van handelende natuurlijke personen die door de Dienstafnemer zijn of worden gemachtigd om namens de Dienstafnemer elektronische verklaringen af te leggen en/of in ontvangst te nemen;

- het toekennen van pseudoniemen aan handelende natuurlijk personen waarbij de eisen van dataminimalisatie aantoonbaar worden gevolgd;
- het registreren van machtigingen die door de Dienstafnemer zijn afgegeven, waarbij de koppeling met identificerende kenmerken en/of pseudoniemen aantoonbaar is terug te voeren op de in de registratiefase door de Dienstafnemer, of namens deze de Machtigingenbeheerder, verschafte gegevens;
- een proces, in welke vorm dan ook, voor het opvoeren, onderhouden en intrekken van registraties van machtigingen, dat voldoet aan de in het Afsprakenstelsel gedefinieerde Betrouwbaarheidsniveaus.

26.2 Het Machtigingenregister zorgt voor vastlegging van duidelijke afspraken over de validatie van de vertegenwoordigingsbevoegdheid van de handelend natuurlijk persoon van de Dienstafnemer voor zover het een publiekrechtelijke rechtspersoon betreft.

26.3 Het Machtigingenregister voorkomt dat een ingetrokken of geblokkeerde registratie van een machtiging als geldige registratie wordt verwerkt.

26.4 Het Machtigingenregister zorgt voor een verwerking van registraties van machtigingen conform de Overeenkomst en overeengekomen service levels.

26.5 Het Machtigingenregister draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.

Artikel 27. Verplichtingen van de Ondertekendienst

27.1 De Ondertekendienst biedt aan handelend natuurlijke personen een online interface om als onderdeel van een Herkenningsdienst een wilsuiting te faciliteren.

27.2 De Ondertekendienst hanteert hetzelfde Betrouwbaarheidsniveau als het Betrouwbaarheidsniveau waar het Authenticatiemiddel dat wordt gebruikt om een elektronische wilsuiting te doen, aan voldoet.

27.3 De Ondertekendienst faciliteert de vastlegging van wilsuitingen conform de Overeenkomst en overeengekomen service levels.

27.4 De Ondertekendienst draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.

Organisatie

Hier vindt u de organisatorische documenten van het Afsprakenstelsel eHerkenning: het operationele handboek, de service level, het businessmodel en het handboek huisstijl. Deze documenten bevatten informatie over de stelselbrede beheerprocessen, de algemene service level die eHerkenning hanteert en het gebruik van het beeldmerk eHerkenning bij externe communicatie.

Deze categorie bevat de volgende onderdelen:

- Operationeel handboek — Dit document beschrijft de operationele beheerprocessen voor het netwerk. Deze processen hebben als doel om het merk eHerkenning te beheren. Onder merkbeheer valt onder andere het beheren van de documentatie van het afsprakenstelsel, de relaties in het netwerk, het technische netwerk, digitale sleutels, toetreding en wensen of wijzigingen.
- Businessmodel — Dit document beschrijft het businessmodel voor eHerkenning. Onder het businessmodel worden verstaan de afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen die samen het netwerk voor eHerkenning invullen. Het is bedoeld voor deelnemers en dienstverleners.
- Handboek huisstijl — Dit document beschrijft de huisstijl afspraken en afspraken over marketingcommunicatie die deelnemers hebben gemaakt. Het is bedoeld voor deelnemers en dienstverleners.
- Service level — Dit document beschrijft de service level afspraken die deelnemers hebben gemaakt die beschrijven welk service level ten minste aan hun klanten wordt bieden. Het is bedoeld voor deelnemers en dienstverleners.

Operationeel handboek

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Dit document beschrijft de operationele beheerprocessen voor het netwerk. Deze processen hebben als doel om het merk eHerkenning te beheren. Onder merkbeheer valt onder andere het beheren van de documentatie van het afsprakenstelsel, de relaties in het netwerk, het technische netwerk, digitale sleutels, toetreding en wensen of wijzigingen.

De juridische afbakening van de beheerorganisatie staat beschreven in Juridisch kader.

Dit document is primair geschreven voor de beheerorganisatie en de deelnemers. Daarnaast is het ook ter inzage voor het Ministerie van Economische Zaken (opdrachtgever voor eHerkenning) en iedere andere organisatie die interesse heeft in eHerkenning.

Leeswijzer

- Helpdesk — De beheerorganisatie beschikt over een helpdesk specifiek voor de deelnemers van eHerkenning. Deze helpdesk is het eerste meldpunt in geval van vragen, issues of andere problemen binnen het netwerk.
- Proces aanpassen attribuutcatalogus — In de Attribuutcatalogus zijn alle attributen en identificerende kenmerken opgenomen die worden onderscheiden binnen eHerkenning. De beheerorganisatie beheert de attribuutcatalogus. Dit proces beschrijft hoe wijzigingen op de attribuutcatalogus worden doorgevoerd.
- Proces beheren simulator — De simulator is door de beheerorganisatie ontwikkeld om deelnemer en dienstverleners een simulatortest te laten uitvoeren. Hiermee worden koppelvlakken gesimuleerd.
- Proces beheren testnetwerk — Het testnetwerk is een netwerk van alle deelnemers. Het heeft als functie om nieuwe systemen van nieuwe toetreders of deelnemers te kunnen onderwerpen aan ketentesten. Hiermee kan in een netwerk dat zich, op hoofdlijnen gedraagt als het productienetwerk, worden gecontroleerd of aan alle eisen wordt voldaan.
- Proces certificaatwissel — Het uitgangspunt is dat er één certificaat per deelnemer in de metadata is opgenomen. Echter, de deelnemers en de beheerorganisatie hebben de mogelijkheid om uit voorzorg meerdere certificaten op te geven. Dit maakt het netwerk minder kwetsbaar wanneer een certificaat gewisseld moet worden.
- Proces change en release — Het Afsprakenstelsel eHerkenning is aan wijzigingen onderhevig. Het proces change- en releasemanagement heeft als doel te besluiten over welke wijzigingen wel of niet worden doorgevoerd en deze vervolgens door te voeren.
- Proces contentmanagement — Voor een consistente externe communicatie is het van belang om een proces voor contentmanagement te hebben. Hiermee wordt de content van externe communicatie over eHerkenning structureel getoetst aan het afsprakenstelsel en de deelnemersovereenkomst. Bij het opstellen van nieuwe content of het wijzigen van bestaande content is dit proces van toepassing.
- Proces distributie en publicatie van documenten — De beheerorganisatie verricht algemene communicatie activiteiten voor eHerkenning. Een van die activiteiten is het publiceren van het afsprakenstelsel eHerkenning en andere bij eHerkenning berustende informatie (dit betekent documenten met de classificatie 'eHerkenning openbaar'). De deelnemers en de beheerorganisatie gebruiken de documentatie voor het beheer van eHerkenning. Andere geïnteresseerde partijen kunnen de openbare documenten ook inzien.
- Proces doorvoeren nieuwe dienstencatalogus — In de dienstencatalogus zijn alle diensten van aangesloten dienstverleners opgenomen die worden onderscheiden binnen eHerkenning. De beheerorganisatie beheert de geaggregeerde dienstencatalogus. Dit proces beschrijft hoe wijzigingen op de dienstencatalogus worden doorgevoerd.
- Proces en randvoorwaarden uitvoering penetratietesten — Procesbeschrijving en voorwaarden waaronder penetratietesten binnen het stelsel van eHerkenning worden uitgevoerd.
- Proces incidentmanagement — In elke organisatie komen incidenten voor. Afhankelijk van het type incident en de ernst zullen passende maatregelen moeten worden getroffen. eHerkenning heeft een proces voor incidentmanagement om incidenten en calamiteiten netwerkbreed op gestructureerde wijze af te handelen.

- Proces managementinformatie — Managementinformatie over het gebruik van het netwerk en de werking van het afsprakenstelsel wordt door middel van rapportages verzameld en verspreid. De rapportages worden o.a. gebruikt om de groei van het netwerk te monitoren op het gebied van aansluitingen, uitgifte van middelen en aantallen berichten.
- Proces meldingenbeheer — De beheerorganisatie is aanspreekpunt voor zaken met betrekking tot de ontwikkeling en implementatie van het Afsprakenstelsel eHerkenning. snippet.issues functioneert als portaal voor het maken van meldingen. Bij het melden van een incident moet het proces incidentmanagement als basis genomen worden.
- Proces metadata — In het Herkenning netwerk wordt SAML metadata gebruikt voor het beschrijven van de URLs en certificaten die worden gebruikt op de verschillende koppelvlakken. Actuele metadata is van belang om twee redenen:
- Proces naleving — Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het netwerk voor eHerkenning. Het nalevingsbeleid is er op gericht om een correcte naleving van het afsprakenstelsel te verzekeren. Dit gebeurt zo veel mogelijk in goed onderling overleg tussen de beheerorganisatie en de betrokken deelnemer of dienstverlener. Het kan echter noodzakelijk zijn om een correcte naleving af te dwingen via het opleggen van sancties.
- Proces onderhoud cookieserver — Voor de werking van Single Sign On heeft iedere eHerkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein *.eherkenning.nl. De DNS van het gezamenlijke domein wordt beheerd door beheerorganisatie.
- Proces toetreden — Nieuwe partijen kunnen geïnteresseerd zijn in deelname aan het netwerk voor eHerkenning. Het toetredingsproces beschrijft de stappen die genomen moeten worden om deel te mogen nemen aan het netwerk eHerkenning en het merk eHerkenning te mogen voeren. Ook in andere situaties kan er sprake zijn van toetreding. In al die gevallen moet het toetredingsproces worden gevolgd.
- Proces uittreden — Voor geïnteresseerde partijen is er een toetredingsproces dat zij kunnen doorlopen indien zij deelnemer van eHerkenning willen worden. Uiteraard kunnen deelnemers ook uittreden. De deelnemer heeft na de uittreding geen rechten meer als deelnemer van eHerkenning. Dit betekent dat de betreffende partij het merk niet meer mag voeren en geen onderdeel meer is van het technische netwerk van eHerkenning.
- Proces wijziging rechtspersoon — Wanneer een deelnemer de rechtspersoon wil wijzigen, maakt hij dit kenbaar aan de beheerorganisatie door middel van het formulier Template wijziging rechtspersoon deelnemer. mailto:info@eherkenning.nl.

Helpdesk

De beheerorganisatie beschikt over een helpdesk specifiek voor de deelnemers van eHerkenning. Deze helpdesk is het eerste meldpunt in geval van vragen, issues of andere problemen binnen het netwerk.

De helpdesk kan in principe niet gebruikt worden door gebruikers van eHerkenning. Zij wenden zich tot de dienstverlener of tot de deelnemer waarmee zij een relatie hebben.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Melding helpdesk

Toelichting processtappen

1. Melding helpdesk	
Input	Vraag, probleem, issue van een deelnemer

Activiteit	1. De deelnemer meldt zijn vraag, probleem of issue aan de helpdesk van de beheerorganisatie per e-mail: info@eherkenning.nl. 2. De beheerorganisatie formuleert indien mogelijk direct een oplossing. Indien dit niet mogelijk is, wordt de vraag verder in de beheerorganisatie uitgezet. 3. De beheerorganisatie beantwoordt de vraag van de deelnemer of verstuurt een voortgangsbericht.
Output	Oplossing voor vraag, probleem of issue van de deelnemer
Wie?	• Beheer officer van de beheerorganisatie • Indien nodig, andere experts in de beheerorganisatie • Deelnemers

Proces aanpassen attribuutcatalogus

In de Attribuutcatalogus zijn alle attributen en identificerende kenmerken opgenomen die worden onderscheiden binnen eHerkenning. De beheerorganisatie beheert de attribuutcatalogus. Dit proces beschrijft hoe wijzigingen op de attribuutcatalogus worden doorgevoerd.

Overzicht processtappen

- 1. Aanleveren verzoek nieuw attribuut/identificerend kenmerk
- 2. Beoordelen aanvraag
- 3. Publiceren nieuwe Attribuutcatalogus
- 4. Nieuwe attribuutcatalogus doorvoeren

Toelichting processtappen

1. Aanleveren verzoek nieuw attribuut/identificerend kenmerk	
Input	Wens tot wijzigen van attribuutcatalogus, bijvoorbeeld voor introductie van een nieuw attribuut.
Activiteit	Deelnemers (in de rol van HM, MR of AD) leveren de gewenste wijziging op de attribuutcatalogus aan bij de beheerorganisatie door het aanmaken van een issue in Mantis met een compleet tekstvoorstel voor een nieuwe paragraaf.
Output	Aangeleverde attribuutbeschrijving (incl. naam, omschrijving, korte omschrijving, formaat, betrouwbaarheidsniveaus, bron) OF beschrijving identificerend kenmerk (incl. naam, omschrijving, formaat, wel/niet ketenmachtigingen, criteria, bronregister, proces voor aansluiten op bronregister). Door deze wijze van aanleveren wordt de beheerorganisatie automatisch geïnformeerd.
Wie?	Technisch beheerders van de deelnemers

2. Beoordelen aanvraag	
Input	Aangeleverde attribuutbeschrijving of beschrijving identificerend kenmerk

Activiteit	• De beheerorganisatie wijst het betreffende Mantis issue binnen 2 werkdagen toe aan zichzelf en geeft aan op welke dag, uiterlijk 2 weken na creatie van het Mantis issue, een nieuwe attribuutcatalogus zal worden gepubliceerd indien het verzoek wordt goedgekeurd, zodat andere deelnemers de tijd hebben om eventuele eigen wijzigingen op de attribuutcatalogus aan te leveren. • De beheerorganisatie controleert de aangeleverde wijziging(en) op conformiteit met de criteria voor attributen/identificerende kenmerken. • De beheerorganisatie controleert of het gevraagde attribuut/kenmerk voldoende uniek is en niet teveel overlap heeft met bestaande attributen/kenmerken. • De beheerorganisatie controleert of er geen juridische of beveiligingstechnische belemmeringen zijn voor opnemen van het attribuut/kenmerk. De beheerorganisatie besluit zelfstandig over het goedkeuren of afkeuren van de aanvraag en publiceert het resultaat op Mantis. Indien de beheerorganisatie niet tot een oordeel kan komen, legt de beheerorganisatie de aanvraag voor aan het Operationeel Overleg (dit kan ook schriftelijk). Een meerderheidsbesluit in het Operationeel Overleg bepaalt dan of de aanvraag wel of niet wordt goedgekeurd.
Output	Goedgekeurde of afgekeurde aanvraag
Wie?	Change manager beheerorganisatie

3. Publiceren nieuwe Attribuutcatalogus	
Input	Goedgekeurde aanvragen
Activiteit	• De beheerorganisatie verwerkt de goedgekeurde aanvragen in een nieuwe versie van het XML-document voor de attribuutcatalogus en een nieuwe versie van het document Attribuutcatalogus van het afsprakenstelsel. Het XML-document is leidend. • De beheerorganisatie publiceert de nieuwe attribuutcatalogus (Attribuutverstrekking) • Daarnaast wordt het XML-document gepubliceerd op de daarvoor bestemde URL.
Output	Gepubliceerde nieuwe attribuutcatalogus en de XML representatie daarvan
Wie?	Technisch beheerder van de beheerorganisatie

4. Nieuwe attribuutcatalogus doorvoeren	
Input	Gepubliceerde nieuwe attribuutcatalogus
Activiteit	• De deelnemers halen de nieuwe attribuutcatalogus op. • Alle deelnemers voeren de attibuutcatalogus door binnen 2 weken na publicatie.
Output	Doorgevoerde nieuwe attribuutcatalogus.
Wie?	Technisch beheerders deelnemers

Proces beheren simulator

De simulator is door de beheerorganisatie ontwikkeld om deelnemer en dienstverleners een simulatortest te laten uitvoeren. Hiermee worden koppelvlakken gesimuleerd.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technische beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Beheer simulator

Toelichting processtappen

1. Beheer simulator	
Input	Nieuwe versie afsprakenstelsel
Activiteit	1. De beheerorganisatie past de simulator aan op de nieuwe versie van het afsprakenstelsel 2. Wanneer de nieuwe versie van de simulator beschikbaar is, stelt de beheerorganisatie de deelnemers per e-mail hiervan op de hoogte.
Output	• Nieuwe versie simulator • Bericht aan de deelnemers
Wie?	• Beheerorganisatie, technische beheerder • Deelnemers, technische beheerders
Opmerkingen	De simulator is te vinden op https://extranet.eherkenning.nl/simulator/ . De handleiding van de simulator is ook opgenomen op deze website.

Proces beheren testnetwerk

Het testnetwerk is een netwerk van alle deelnemers. Het heeft als functie om nieuwe systemen van nieuwe toetreders of deelnemers te kunnen onderwerpen aan ketentesten. Hiermee kan in een netwerk dat zich, op hoofdlijnen gedraagt als het productienetwerk, worden gecontroleerd of aan alle eisen wordt voldaan.

De voorwaarden om het testnetwerk te laten functioneren, zijn als volgt:

- De staat van de preproductiecomponenten in het testnetwerk benadert zo veel mogelijk het productienetwerk.
- Een herkenningsmakelaar MAG dienstverleners via haar preproductiecomponent toegang verlenen tot AD/MR's van andere deelnemers en de simulator, mits dit niet tot overlast leidt.
- Het uitvoeren van stresstesten MAG NIET zonder toestemming vooraf van alle te raken deelnemers.
- Deelnemers MOGEN testmiddelen verschaffen aan dienstverleners die zijn aangesloten via een andere deelnemer.
- De acceptatieomgeving dient om de eigen software te testen tegen de preproductiecomponenten van andere deelnemers.
- Een deelnemer ZOU NIET MOGEN testen tegen de acceptatieomgeving van een andere deelnemer.
- Alle deelnemers en de beheerorganisatie hebben testmiddelen in bezit, voor de preproductiecomponenten in het testnetwerk, voor elke authenticatiedienst en machtigingenregister, op elk toegetreden (of nog toe te treden) betrouwbaarheidsniveau.
- Bij het deployen van een systeem in het testnetwerk dient voor een deelnemer of de beheerorganisatie helder te zijn welke build versie het systeem heeft. (Bijvoorbeeld door naamgeving, het displayen van het build nummer op de pagina of in een afgeleide (file).) Dit zodat kan worden nagegaan tegen welke versie van een systeem aan wordt getest. Bij de toetredingschecklists (Checklist simulator test en Checklist simulator test) wordt altijd aangegeven tegen welke build versies is getest.
- Acceptatiecomponenten in het testnetwerk MOETEN herkenbaar zijn aan de toevoeging (acc) in de displayname
- Preproductiecomponenten in het testnetwerk MOETEN herkenbaar zijn aan de toevoeging (preprod) in de displayname
- Voor beschikbaarheid van preproductiecomponenten in het testnetwerk wordt een inspanningsverplichting en een meldplicht van verstoringen afgesproken.
- Verzoeken van deelnemers om meer informatie betreffende een fout (op een systeem) in het testnetwerk ZOU binnen één werkdag beantwoord MOETEN worden.
- Het in bezit hebben van testmiddelen door deelnemers en dienstverleners impliceert dat deze testmiddelen ook te allen tijde kunnen werken. Dat wil zeggen dat de uitgevers van deze middelen zich hiermee verplichten een soortgelijk serviceniveau te leveren als bij productiemiddelen het geval is.
- Issues en verstoringen betreffende het testnetwerk worden gemeld in de issuetracker Mantis.
- De metadata en dienstencatalogus voor het testnetwerk zullen ad hoc verspreid worden, als de noodzaak zich aandient. Deze zullen op dezelfde manier als binnen het productienetwerk worden aangeboden aan de deelnemers.
- Een deelnemer MAG haar acceptatie- en preproductiecomponenten NIET afsluiten voor andere deelnemers.

Proces certificaatwissel

Het uitgangspunt is dat er één certificaat per deelnemer in de metadata is opgenomen. Echter, de deelnemers en de beheerorganisatie hebben de mogelijkheid om uit voorzorg meerdere certificaten op te geven. Dit maakt het netwerk minder kwetsbaar wanneer een certificaat gewisseld moet worden.

Dit proces beschrijft hoe het wisselen van certificaten verloopt.

Om het proces van het wisselen van een certificaat succesvol te laten verlopen, is het van belang dat deelnemers meerdere certificaten per deelnemer kunnen verwerken.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Aanleveren nieuwe certificaat
- 2. Verwijderen oude certificaat

Toelichting processtappen

1. Aanleveren nieuwe certificaat	
Input	Geplande certificaatwissel bij een deelnemer
Activiteit	1. De deelnemer informeert de beheerorganisatie tijdig over de geplande certificaatwissel. 2. De deelnemer levert het nieuwe metadatabestand aan bij de beheerorganisatie, voorafgaand aan moment waarop het huidige certificaat verloopt. In deze metadata is opgenomen: • de huidige public key die in gebruik is • de nieuwe public key die de deelnemer wil gaan gebruiken 1. De beheerorganisatie aggregeert en publiceert de nieuwe metadata volgens het Proces metadata, en attendeert alle deelnemers op de certificaatwissel. 2. De deelnemers MOETEN de nieuwe versie van de metadata binnen het eerstvolgende gebruikelijke Onderhoudswindow doorvoeren. 3. Na het servicewindow MAG de betreffende deelnemer het nieuwe certificaat gebruiken.
Output	Doorgevoerde metadata met oude en nieuwe certificaat
Wie?	• Beheerorganisatie, technisch beheerder • Deelnemers, technisch beheerders

2. Verwijderen oude certificaat	
Input	Doorgevoerde metadata met oude en nieuwe certificaat
Activiteit	1. Wanneer het nieuwe certificaat overal binnen het netwerk is geaccepteerd, kan het oude certificaat uit de metadata worden gehaald. De betreffende deelnemer levert nieuwe metadata aan met daarin alleen de public key van het nieuwe certificaat. 2. De beheerorganisatie aggregeert en publiceert de nieuwe metadata volgens het Proces metadata, en attendeert alle deelnemers op de certificaatwissel.
Output	Doorgevoerde metadata met enkel het nieuwe certificaat

Wie?	• Beheerorganisatie, technisch beheerder • Deelnemers, technisch beheerders

Certificaatwissel kan ook voorkomen bij certificaten die niet in de metadata zijn opgenomen. Voor de werking van Single Sign On heeft iedere eHerkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein *.eherkenning.nl. Dit gezamenlijke domein wordt beheerd door de beheerorganisatie.

De cookieservers verzenden geen berichten maar maken wel gebruik van certificaten. Wanneer deze certificaten worden gewisseld, wordt ongeveer hetzelfde proces doorlopen als bij de certificaatwissel in metadata. Dat proces verloopt dan als volgt:

- De deelnemer meldt tijdig (minimaal twee weken van te voren) bij de beheerorganisatie dat het certificaat moet worden gewisseld via de issuetracker Mantis. Hierbij vermeldt de deelnemer de huidige public key die in gebruik is, de nieuwe public key en de termijn waarop de wijziging moet plaatsvinden.
- De beheerorganisatie vervangt de public key van de betreffende deelnemer.
- De deelnemer ontvangt een bevestiging van de beheerorganisatie via Mantis wanneer de vervanging is afgerond.
- De deelnemer KAN nu het nieuwe certificaat gebruiken.

Proces change en release

Het Afsprakenstelsel eHerkenning is aan wijzigingen onderhevig. Het proces change- en releasemanagement heeft als doel te besluiten over welke wijzigingen wel of niet worden doorgevoerd en deze vervolgens door te voeren.

Doelstelling

De doelstelling van het change- en releaseproces is tweeledig:

1. Op transparante/zorgvuldig wijze besluiten over welke wijzigingen wel of niet worden doorgevoerd. Alle belanghebbenden moeten invloed kunnen hebben op de wijziging van het afsprakenstelsel.
2. De release op gestructureerde wijze inbrengen in het afsprakenstelsel en de productieversie van het netwerk.
    a. volgens de planning
    b. zonder verstoringen

Verantwoordelijkheden

De Stelselraad eHerkenning (gremium) schetst in het meerjarenplan de strategische kaders voor de inhoudelijke doorontwikkeling van het Afsprakenstelsel eHerkenning. Vervolgens neemt het Tactisch Overleg (gremium) eigenstandig een besluit over de inhoud van de releases en de implementatie. Het Tactisch Overleg dient bij het besluit rekening te houden met de door de Stelselraad gestelde kaders.

Het Operationeel Overleg (gremium) bereidt de wijzigingen voor.

De change manager van de beheerorganisatie zorgt ervoor dat de procesbeschrijving up-to-date blijft en coördineert tevens de meeste activiteiten uit vanuit de beheerorganisatie. Voor de afstemming van het change- en releaseproces is een digitale omgeving beschikbaar voor de deelnemers en de beheerorganisatie: Confluence.

Overzicht processtappen

- 1. Wijzigingsverzoeken registreren
- 2. Beoordeling wijzigingsverzoeken
- 3a. RFC opstellen
- 3b. Release samenstellen
- 3c. Besluiten over release
- 4. Implementatieplan
- 5a. Release productieversie netwerk
- 5b. Uitvoering compensatieregeling

Toelichting processtappen

1. Wijzigingsverzoeken registreren	
Input	Een wijzigingsverzoek kan door iedereen worden aangemeld. De meest voorkomende bronnen zijn dienstaanbieders, deelnemers, gebruikers en de beheerorganisatie. Een wijzigingsverzoek kan verschillende aanleidingen hebben. De drie meest voorkomende categorieën zijn: 1. Fouten: denk aan verkeerde verwijzingen of taalfouten. Het oplossen van fouten heeft geen impact op de inhoud/werking van het Afsprakenstelsel. 2. Issues: denk aan een (deel van een) functionaliteit die in de praktijk niet goed toepasbaar blijkt. Het oplossen van issues heeft impact op de inhoud/werking van het Afsprakenstelsel. 3. Usecases: denk aan nieuwe gewenste functionaliteiten. Het accepteren van een usecase heeft impact op de inhoud/werking van het Afsprakenstelsel.
Activiteit	1. Wijzigingsverzoeken worden aangemeld bij de beheerorganisatie via info@eherkenning.nl. De beheerorganisatie registreert de wijzigingsverzoeken op een verzamellijst van 'ingekomen wijzigingsverzoeken' 2. De change manager beoordeelt de wijzigingsverzoeken op deze verzamellijst periodiek op volledigheid: wat (is de fout / issue / usecase), waarom (is dit een fout / issue / usecase) en wie (is de indiener van deze fout / issue / usecase)? Het wijzigingsverzoek moet bij een usecase bovendien antwoord geven op de vraag wat de wens (nieuwe functionaliteit) oplevert en voor wie: wat is het beoogde resultaat en wie is de doelgroep? 3. De change manager doet eventueel een verzoek tot aanvullende informatie bij de indiener van het wijzigingsverzoek.
Output	Volledige actuele lijst met wijzigingsverzoeken.
Wie?	De change manager beheert de verzamellijst.

2. Beoordeling wijzigingsverzoeken	
Input	Volledige actuele lijst met wijzigingsverzoeken
Activiteit	De verzoeken op de verzamellijst worden beoordeeld door het Operationeel Overleg. Beoordelingscriteria zijn onder meer: • De wijze van inpassing in eHerkenning: is het technisch gezien mogelijk een wijziging in te passen en welke stappen zijn daar voor nodig? • De impact van de wijziging op bestaande systemen en processen • De toegevoegde waarde van de wijziging: wat levert het op en staat dit in verhouding tot de impact? • Of er een usecase is geleverd? • Of het wijzigingsverzoek past binnen de door de Stelselraad vastgestelde kaders voor doorontwikkeling? De beoordeling kan de volgende resultaten hebben: 1. Afwijzing van het wijzigingsverzoek 2. In behandeling nemen van het wijzigingsverzoek Bij afwijzing van het wijzigingsverzoek: • De change manager stelt een onderbouwing van de afwijzing op. • De change manager verplaatst het wijzigingsverzoek van de verzamellijst van 'ingekomen wijzigingsverzoeken' naar de verzamellijst van 'afgewezen wijzigingsverzoeken'. • De change manager stelt de indiener van het wijzigingsverzoek op de hoogte van de afwijzing. Bij in behandeling nemen van het wijzigingsverzoek wordt er vervolgens een Request for Change (RFC) opgesteld door het Operationeel Overleg. Het Operationeel Overleg bespreekt maandelijks wat de stand van zaken is met betrekking tot de verzamellijst van 'ingekomen wijzigingsverzoeken' en de verzamellijst van 'afgewezen wijzigingsverzoeken'.
Output	• Actuele RFC-lijst (met daarop in behandeling genomen wijzigingsverzoeken) • Actuele verzamellijst met ingekomen en afgewezen wijzigingsverzoeken • Actuele Releasekalender • Terugmelding besluiten over wijzigingsverzoeken aan indieners
Wie?	De change manager beheert de verzamellijst.

3a. RFC opstellen	
Input	Actuele RFC lijst.
Activiteit	Het Operationeel Overleg formuleert voor de wijzigingsverzoeken die in behandeling worden genomen een RFC, mede op basis van de betreffende fout, issue of use case, en eventueel ook input van een werkgroep die daartoe is ingesteld door het Tactisch Overleg. Op de RFC wordt een impactanalyse (inspanning en doorlooptijd) en een risicoanalyse uitgevoerd: • Iedere deelnemer beoordeelt de impact op de huidige systemen. Indien het een aanvullende feature betreft wordt dit als zodanig bij de RFC vermeld. • De beheerorganisatie bepaalt de impact op de simulator en andere beheerobjecten van de beheerorganisatie en voert een risicoanalyse uit De resultaten van deze impact- en risicoanalyses en de definitieve RFC wordt vervolgens door het Operationeel Overleg beoordeeld. Zij adviseren positief of negatief over de RFC. De RFC wordt vervolgens verder doorgeleid in het changeproces door de beheerorganisatie.
Output	RFC's
Wie?	• Operationeel Overleg en eventuele werkgroep stellen RFC's op • Security officer en/of jurist (indien van toepassing) toetsen RFC's • Change manager leidt RFC's door in proces

3b. Release samenstellen	
Input	RFC's
Activiteit	1. Meerdere door het Operationeel Overleg geadviseerde RFC's vormen gezamenlijk een release. Niet alle RFC's moeten direct mee in de eerstvolgende release. Het Operationeel Overleg doet een voorstel voor samenstelling van de release aan het Tactisch Overleg. Hierbij houdt het Operationeel Overleg rekening met de termijn die nodig is om de release tijdig en zorgvuldig samen te stellen. RFC's die na deze termijn worden ingediend kunnen mee in de volgende release. 2. Het Operationeel Overleg brengt advies uit over de samengestelde release. Het voorstel voor de samengestelde release wordt verder doorgeleid in het changeproces door de beheerorganisatie.
Output	Samengestelde release
Wie?	• Change manager afsprakenstelsel doet voorstel voor release en planning • Operationeel overleg geeft advies over release en planning

3c. Besluiten over release	
Input	Samengestelde release
Activiteit	1. De release, de planning en het advies van het Operationeel Overleg worden doorgeleid naar het Tactisch Overleg. Het Tactisch Overleg neemt een formeel besluit over de inhoud van de release en de planning. a. Het Tactisch Overleg dient bij het besluit rekening te houden met de door de Stelselraad gestelde kaders. 2. Indien het Tactisch Overleg een of meer goedgekeurde RFCs eerder wil laten implementeren dan in de releaseplanning mogelijk is, dan kan er besloten worden tot invoering middels een spoedprocedure. a. Bij toepassing van de spoedprocedure wordt een tussentijdse release gecreëerd die los staat van de releaseplanning. b. Deze spoedprocedure wordt gebruikt wanneer het een zeer dringende wens in de markt betreft of een dreiging/kans in de omgeving van eHerkenning waarop gereageerd moet worden.
Output	Een formeel vastgestelde release (eventueel spoedrelease)
Wie?	• Beheerorganisatie legt release voor • Tactisch overleg neemt formeel besluit over (spoed)release

4. Implementatieplan	
Input	Een formeel vastgestelde release
Activiteit	Indien de release ketenafhankelijkheden en/of compensatiedragende maatregelen bevat, stelt de beheerorganisatie een implementatieplan op. Het proces om te komen tot een concreet en duidelijk afgebakend en gezamenlijk vastgesteld implementatieplan waaraan alle betrokken partijen zijn gebonden, is als volgt: 1. De beheerorganisatie stelt een concept implementatieplan op. In het concept implementatieplan wordt een voorstel gedaan voor: a. de concrete maatregelen die de verschillende partijen moeten nemen; b. de bijbehorende deadline(s), en c. de hoogte van de compensatie bij niet naleving overeenkomstig hetgeen hierover is bepaald in de Compensatieregeling. 2. Bespreking van het concept implementatieplan in het Operationeel Overleg 3. Schriftelijke instemming van alle betrokken partijen met het concept implementatieplan, in de vorm van het ondertekenen van een kopie van het vastgestelde implementatieplan door een daartoe bevoegde vertegenwoordiger van iedere deelnemer en de beheerorganisatie. Ondertekend exemplaar moet binnen 2 weken na bespreking in het Operationeel Overleg aan de beheerorganisatie worden geleverd 4. Vaststelling van het implementatieplan door het Tactisch Overleg. 5. Archivering van alle ondertekende kopieën van het vastgestelde implementatieplan door de beheerorganisatie. Voor meer informatie over de toepasselijkheid van de compensatieregeling op het implementatieplan: zie Compensatieregeling.
Output	Goedgekeurd en door alle deelnemers en beheerorganisatie ondertekend implementatieplan.
Wie?	• De change manager stelt implementatieplan op. • Operationeel Overleg adviseert. • Bevoegde vertegenwoordigers van alle deelnemers en de beheerorganisatie ondertekenen. • Tactisch Overleg accordeert.

5a. Release productieversie netwerk	
Input	Goedgekeurd implementatieplan.
Activiteit	Na het vaststellen van de release hebben de deelnemers van eHerkenning de tijd om de release te implementeren in het productienetwerk. De deelnemers en de beheerorganisatie voeren dit uit. De implementatie bestaat uit één of meer van de volgende stappen: 1. De beheerorganisatie levert een nieuwe versie van het Afsprakenstelsel op. 2. De beheerorganisatie levert de nieuwe versie van de simulator en de testcases. 3. De beheerorganisatie levert nieuwe versies van andere beheerobjecten onder haar beheer waar nodig. 4. De beheerorganisatie levert een communicatieplan op voor communicatie rondom de nieuwe implementatie 5. De deelnemers verwerken de RFC's 6. De deelnemers doen simulatietesten 7. De beheerorganisatie en de deelnemers doen ketentesten 8. De beheerorganisatie beoordeelt de testresultaten en besluit tot definitieve go-live datum voor de nieuwe implementatie. 9. Deelnemers voeren hun acties uit het communicatieplan uit 10. Deelnemers leveren opnieuw toetredingsdocumentatie aan voor deze versie van het afsprakenstelsel (Checklist simulator test, Checklist chain test en Template zelfverklaring) 11. Deelnemers en beheerorganisatie coördineren hun activiteiten door periodieke conference calls De beheerorganisatie monitort de voortgang en rapporteert tussentijds over de voortgang aan het Tactisch Overleg.
Output	Geïmplementeerde release in productienetwerk en gepubliceerd afsprakenstelsel.
Wie?	• Deelnemers en de beheerorganisatie implementeren. • Change manager monitort en rapporteert.

5b. Uitvoering compensatieregeling	
Input	Goedgekeurd implementatieplan.
Activiteit	Aan sommige stappen in het implementatieplan zijn compensatiemaatregelen verbonden. In het implementatieplan wordt vooraf vastgesteld voor welke deadlines/mijlpalen compensatiebedragen zijn opgenomen. Wanneer een partij een dergelijke deadline overschrijdt moet hij de bijbehorende vastgestelde compensatie betalen. Het proces voor het opleggen van compensatiemaatregelen verloopt als volgt: 1. Gedurende het implementatietraject van een release houdt de beheerorganisatie bij welke partij een deadline overschrijdt en registreert welke partijen voor welke bedragen compensatieplichtig zijn. De beheerorganisatie controleert dus of elke partij zich aan zijn verplichtingen houdt. 2. Elke keer wanneer een partij een compensatieplichtige deadline overschrijdt, ontvangt hij hierover schriftelijk bericht (in de vorm van een vooraankondiging) van de beheerorganisatie, tenzij een partij een beroep doet op één van de uitzonderingen. Zie ook Compensatieregeling, Uitgangspunten compensatieregeling en Uitzonderingen hieronder 3. Aan het einde van het implementatietraject (als alle stappen van het implementatieplan succesvol zijn doorlopen en afgerond) maakt de beheerorganisatie aan ieder van de partijen schriftelijk (in de vorm van een brief) zo spoedig mogelijk bekend voor welk bedrag zij in totaal compensatieplichtig zijn en aan wie de compensatiebedragen moet worden betaald. De beheerorganisatie stelt tevens het totaaloverzicht van de te betalen en te ontvangen compensatiegelden aan alle betrokken partijen ter beschikking, alsmede het overzicht van de te verreken bedragen. 4. De partijen betalen aan elkaar binnen 30 dagen na dagtekening van het totaal overzicht de verschuldigde bedragen. De partijen zijn zelf verantwoordelijk voor het innen en betalen van de verschuldigde bedragen. 5. (Optioneel) In het geval niet wordt overgegaan tot betaling, staat het betrokken partijen vrij gebruik te maken van de klachten- en geschillencommissie dan wel een rechtszaak aanhangig te maken bij de civiele rechter, dan wel de beheerorganisatie te verzoeken overeenkomstig Nalevingsbeleid het nalevingsbeleid toe te passen.
Output	1. Vooraankondiging verschuldigd compensatiebedrag. 2. Totaal overzicht verschuldigde compensatiebedragen. 3. Betaling.
Wie?	• De Beheerorganisatie registreert de verschuldigde compensatiebedragen. • Gelet op functiescheiding binnen Logius worden de vooraankondiging en het totaaloverzicht van de verschuldigde compensatiebedragen gecontroleerd en opgesteld door Juridische Zaken / bedrijfsvoering van de beheerorganisatie. • Betaling geschiedt door bij het implementatieplan betrokken partijen.

Uitzonderingen opleggen compensatiemaatregelen

Het uitgangspunt is dat als een partij een implementatiemaatregel uit het goedgekeurde implementatieplan niet, niet goed, niet volledig of niet tijdig naleeft, zij compensatieplichting is. In de compensatieregeling worden echter twee uitzonderingssituaties onderscheiden, namelijk:

1. Het niet verschuldigd zijn van het compensatiebedrag zoals opgenomen in het goedgekeurde implementatieplan op basis van een unaniem akkoord, en
2. Het aanpassen van de deadlines van het implementatieplan op basis van een unaniem besluit.

Processtappen uitzondering I

Een partij haalt een deadline niet. Het proces voor het niet verschuldigd zijn van het bijbehorende compensatiebedrag is als volgt:

1. De partij die een bepaalde deadline zoals vastgesteld in het goedgekeurde implementatieplan niet haalt, neemt het initiatief om van alle partijen goedkeuring voor het niet betalen van het compensatiebedrag te krijgen.
2. De partij die het aangaat overlegt het bewijs van goedkeuring van alle partijen aan de beheerorganisatie. Het moet gaan om een unaniem akkoord.
3. Indien er een unaniem akkoord is van alle partijen voor het niet hoeven te betalen van het compensatiebedragen, registreert de beheerorganisatie dit in het overzicht van verschuldigde compensatiebedragen.
4. In plaats van een vooraankondiging van het te betalen compensatiebedrag (zie ook stap 5b), ontvangt de desbetreffende partij een bevestiging van de toepasselijkheid van de uitzondering van de beheerorganisatie..
5. De overige partijen ontvangen van de beheerorganisatie eveneens een bevestiging van de toepasselijkheid van de

uitzondering.
6. In het totaaloverzicht van te betalen en te ontvangen compensatiegelden dat aan het einde van het implementatietraject (als alle stappen van het implementatieplan succesvol zijn doorlopen en afgerond) door de beheerorganisatie wordt opgemaakt, wordt melding gemaakt van de bedragen die op grond van de uitzondering niet in rekening zijn gebracht.

Processtappen uitzondering II

Er is sprake van een niet tijdige levering door een partij als gevolg waarvan een keten van niet naleving ontstaat. Het proces voor het aanpassen van de deadlines van het implementatieplan is als volgt:

1. Eén van de partijen in de keten verzoekt de beheerorganisatie een inventarisatie uit te voeren bij de andere betrokken partijen over de wenselijkheid van aanpassing van het implementatieplan. Indien in de tussentijd deadlines zijn verstreken waaraan een compensatiebedrag is gekoppeld, is dit compensatiebedrag verschuldigd, tenzij door de desbetreffende partij een beroep is en/of wordt gedaan op uitzonderingsituatie I (zoals hierboven beschreven).
2. De beheerorganisatie gaat zo spoedig mogelijk na ontvangst van het verzoek over tot de gevraagde inventarisatie en zorgt voor vastlegging van de uitkomsten hiervan.
3. Indien door de beheerorganisatie wordt vastgesteld dat er een unaniem besluit is, worden partijen hiervan door de beheersorganisatie schriftelijk op de hoogte gebracht.
4. De beheerorganisatie gaat zo spoedig mogelijk over tot het opstellen van een aangepast concept implementatieplan.
5. Bespreking van het concept implementatieplan in het Operationeel Overleg.
6. Schriftelijke instemming van alle betrokken partijen met het concept van het aangepaste implementatieplan.
7. Vaststelling van het aangepaste implementatieplan in het Tactisch Overleg.

Wijzigingen buiten de release om

Indien een wijzigingsverzoek enkel en alleen betrekking heeft op een wijziging van Attribuutcatalogus of Testing, dan MAG de wijziging na beoordeling door het Operationeel Overleg direct worden doorgevoerd in het Afsprakenstelsel.

Proces contentmanagement

Voor een consistente externe communicatie is het van belang om een proces voor contentmanagement te hebben. Hiermee wordt de content van externe communicatie over eHerkenning structureel getoetst aan het afsprakenstelsel en de deelnemersovereenkomst. Bij het opstellen van nieuwe content of het wijzigen van bestaande content is dit proces van toepassing.

Doelstelling

Organiseren van consistente externe communicatie over eHerkenning. Consistent betekent in lijn met het afsprakenstelsel en de deelnemersovereenkomst.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De secretaris is ervoor verantwoordelijk dat de procesbeschrijving actueel blijft.

Uitgangspunten

Dit proces heeft betrekking op het wijzigen van de content van externe communicatiemiddelen:

- Onder een wijziging wordt verstaan een verandering in of het verwijderen van bestaande content of het opstellen van nieuwe content.
- Externe communicatiemiddelen betreft voornamelijk informatie op de website eHerkenning (www.eherkenning.nl), maar ook presentaties over eHerkenning, factsheets, nieuwsbrieven, artikelen, folders, handleidingen etc.
- De deelnemers zijn zelf verantwoordelijk voor het aanleveren van de correcte content voor hun deel in de keuzematrix en het aanbod per deelnemer op de website www.eherkenning.nl.
- Een wijziging kan een kleine of grote impact hebben.
- Een wijziging met kleine impact is bijvoorbeeld het plaatsen van een nieuwsbericht op de website, het wijzigen van links, het actualiseren van presentaties en factsheets. Het betreft hier het dagelijkse beheer van de externe communicatiemiddelen van eHerkenning.
- Een wijziging met een grote impact is bijvoorbeeld het instellen van een aanmeldportaal of de keuzematrix. Het betreft hier een wijziging met aanzienlijke impact op het merk eHerkenning, het netwerk en/of de proposities van de deelnemers. Een wijziging met een grote impact wordt door de beheerorganisatie voorgelegd aan het Tactisch Overleg.

Overzicht processtappen

- 1. Intake en beoordeling
- 2. Opstellen wijziging
- 3. Doorvoeren wijziging
- 4. Terugmelden

Toelichting processtappen

1. Intake en beoordeling

Input	Verzoek tot wijziging van externe content
Activiteit	1. Elke partij kan een verzoek tot het wijzigen van externe content indienen bij de beheerorganisatie. Dit kan per e-mail via info@eherkenning.nl. Deelnemers kunnen in plaats daarvan een verzoek indienen in Mantis. Het verzoek bestaat minimaal uit: a. de voorgestelde wijziging b. de reden voor de wijziging c. de urgentie van de wijziging 2. De beheerorganisatie beoordeelt de impact van het wijzigingsverzoek en of het in lijn is met het afsprakenstelsel en de deelnemersovereenkomst. 3. De beheerorganisatie neemt het verzoek al dan niet in behandeling. Alle wijzigingsverzoeken worden door de beheerorganisatie gearchiveerd in Mantis of in de e-mail.
Output	Eerste beoordeling verzoek tot wijziging
Wie?	Secretaris beheerorganisatie

2. Opstellen wijziging

Input	Eerste beoordeling verzoek tot wijziging
Activiteit	1. Na een eerste beoordeling formuleert de beheerorganisatie een wijzigingsvoorstel dat in lijn is met het verzoek tot wijziging, het afsprakenstelsel en de deelnemersovereenkomst. a. Bij een wijziging met kleine impact: indien er sprake is van een wijziging met kleine impact kan de communicatieadviseur het wijzigingsvoorstel zelf opstellen. Bij twijfel voorleggen aan inhoudelijke experts uit de beheerorganisatie. b. Bij een wijziging met grote impact: indien er sprake is van een wijziging die grote impact heeft op het merk of, het netwerk en/of de proposities van de deelnemers van eHerkenning, zal de beheerorganisatie het wijzigingsvoorstel voorleggen aan het Tactisch Overleg. 2. Het wijzigingsvoorstel wordt goedgekeurd. a. Bij een wijziging met grote impact op het merk of het netwerk eHerkenning, zal de beheerorganisatie het wijzigingsvoorstel ter goedkeuring voorleggen aan het Tactisch Overleg. Het goedgekeurde wijzigingsvoorstel is terug te vinden in de besluiten/vergaderstukken van het Tactisch Overleg. Deze zijn openbaar beschikbaar op www.eherkenning.nl. b. Bij een wijziging met kleine impact wordt het wijzigingsvoorstel door de beheerorganisatie goedgekeurd.
Output	Goedgekeurd wijzigingsvoorstel
Wie?	• Communicatieadviseur beheerorganisatie • Indien nodig voor opstellen, verschillende experts uit de beheerorganisatie

3. Doorvoeren wijziging

Input	Goedgekeurd wijzigingsvoorstel

Activiteit	De communicatieadviseur van de beheerorganisatie voert de wijziging door zoals besloten. • Wijzigingen die zijn doorgevoerd op de website zijn terug te vinden in het log van het Content Management Systeem (Typo3), waarmee www.eHerkenning.nl onderhouden wordt. In de praktijk vinden vrijwel alle gezamenlijke communicatie-uitingen ook plaats via de website (ook factsheets, handleidingen etc worden via de website aangeboden).
Output	Doorgevoerde wijziging.
Wie?	Communicatieadviseur beheerorganisatie

4. Terugmelden	
Input	Doorgevoerde wijziging
Activiteit	1. De beheerorganisatie doet een terugmelding aan de partij die het wijzigingsverzoek heeft gedaan. • Terugmelding aan een eHerkenning deelnemer kan via Mantis • Terugmelding aan een andere partij kan via e-mail. Alle terugmeldingen worden door de beheerorganisatie gearchiveerd in Mantis of de e-mail.
Output	Terugmelding
Wie?	Communicatieadviseur of secretaris van de beheerorganisatie

Proces distributie en publicatie van documenten

De beheerorganisatie verricht algemene communicatie activiteiten voor eHerkenning. Een van die activiteiten is het publiceren van het afsprakenstelsel eHerkenning en andere bij eHerkenning berustende informatie (dit betekent documenten met de classificatie 'eHerkenning openbaar'). De deelnemers en de beheerorganisatie gebruiken de documentatie voor het beheer van eHerkenning. Andere geïnteresseerde partijen kunnen de openbare documenten ook inzien.

Doelstelling

Publiceren van (de actuele versie van) alle documenten van het Afsprakenstelsel eHerkenning en andere bij eHerkenning berustende openbare documenten zodanig dat informatie over eHerkenning kenbaar en vindbaar is voor alle geïnteresseerde partijen. Hiermee wordt de transparantie van het beheer en de governance van eHerkenning vergroot.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De secretaris is ervoor verantwoordelijk dat de procesbeschrijving actueel blijft.

Processtappen

Input	• nieuwe versie van het afsprakenstelsel en/of; • bij eHerkenning berustende openbare documenten met betrekking tot eHerkenning
Activiteit	1. De beheerorganisatie publiceert het nieuwe afsprakenstelsel en andere openbare stukken aangaande eHerkenning in pdf formaat op de gezamenlijke digitale documentatieomgeving van eHerkenning en de website www.eherkenning.nl. 2. De deelnemers, de beheerorganisatie en sommige aangesloten overheidsdienstverleners hebben een gepersonaliseerde account met leesrechten voor de documentatieomgeving. Andere geïnteresseerde partijen kunnen via de website de openbare documentatie lezen en downloaden. 3. De openbare documentatie blijft beschikbaar op de documentatieomgeving en de website. De deelnemers, de beheerorganisatie, de overheidsdienstverleners en andere geïnteresseerden kunnen het onbeperkt raadplegen.

Output	Actief gepubliceerde openbare documenten op de website van eHerkenning en de gezamenlijke digitale documentatieomgeving van eHerkenning.
Wie?	Secretaris van de beheerorganisatie

Proces doorvoeren nieuwe dienstencatalogus

In de dienstencatalogus zijn alle diensten van aangesloten dienstverleners opgenomen die worden onderscheiden binnen eHerkenning. De beheerorganisatie beheert de geaggregeerde dienstencatalogus. Dit proces beschrijft hoe wijzigingen op de dienstencatalogus worden doorgevoerd.

Voor de publicatie van de dienstencatalogus in de testomgeving is geen formeel proces afgesproken buiten het feit dat deze op de, in het proces hieronder beschreven, URL wordt gepubliceerd. In de dienstencatalogus in de testomgeving worden de testdiensten van de simulator gepubliceerd, alsmede testomgevingen van dienstverleners indien en voor zover deze testmiddelen en -machtigingen van andere deelnemers willen gebruiken..

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Aanleveren nieuwe dienstencatalogusinformatie
- 2. Aanleveren nieuwe dienstencatalogus
- 3. Controleren en aggregeren dienstencatalogus
- 4. Nieuwe dienstencatalogus doorvoeren
- 5. Terugkoppeling onjuistheden dienstencatalogus

Toelichting processtappen

1. Aanleveren nieuwe dienstencatalogusinformatie	
Input	Wens tot registreren van nieuwe dienst of aanpassen bestaande dienst.
Activiteit	De dienstverlener levert informatie over de dienst aan bij de (primaire) eHerkenningsmakelaar. Deze informatie over de dienst MOET het volgende bevatten: 1. Of de dienst/dienstverlener al publiek beschikbaar is (op een publiek toegankelijke webpagina) voor IsPublic; 2. De precieze URL waar de dienst beschikbaar is (alleen voor diensten die al publiek beschikbaar zijn); 3. Een correcte, voor gebruikers te begrijpen beschrijving van de dienstverlener (voor OrganizationDisplayName); 4. Een correcte, voor gebruikers te begrijpen naam van de dienst (voor Servicename) en beschrijving (voor ServiceDescription); 5. Het betrouwbaarheidsniveau wat door de dienst wordt gevraagd (voor AuthnContextClassRef). Dit MOET het standaard betrouwbaarheidsniveau zijn voor de dienst, zoals in de dienstencatalogus beschreven; 6. De soorten dienstafnemer die de dienst kunnen gebruiken (incl. gebruik van het vestigingsnummer door de dienst) (voor EntityConcernedTypesAllowed); 7. Indien er een internetpagina is met uitgebreidere beschrijving van de dienst: een URL van die internetpagina (voor ServiceDescriptionURL); 8. Indien aanvullende attributen worden uitgevraagd door de dienst: het certificaat waarmee de attributen versleuteld moeten worden (voor ServiceCertificate); 9. Indien de dienst via meer dan één eHerkenningsmakelaar wordt gekoppeld aan eHerkenning: de namen en/of OINs van de verschillende alternatieve eHerkenningsmakelaars (voor AdditionalHerkenningsmakelaarID). N.B. de alternatieve eHerkenningsmakelaars leveren verder geen informatie over de dienst aan de beheerorganisatie, alleen de primaire herkenningsmakelaar;

Output	1. Aangeleverde nieuwe / gewijzigde dienstinformatie van dienstverlener 2. Geïnformeerde eHerkenningsmakelaar
Wie?	Dienstverlener

2. Aanleveren nieuwe dienstencatalogus	
Input	Aangeleverde nieuwe / gewijzigde dienstinformatie van dienstverlener
Activiteit	Deelnemers (in de rol van eHerkenningsmakelaar) vullen de door de dienstverlener geleverde informatie aan met het ServiceID, het HerkenningsmakelaarID en AdditionalHerkenningsmakelaarID en stellen de, door de dienstverlener beschikbaar gestelde, wijziging op de dienstencatalogus binnen twee werkdagen na ontvangst ter beschikking aan bij de beheerorganisatie door deze te publiceren op een URL (deze URL verwijst naar een dienstencatalogusbestand met daarin alle diensten van de klanten van deze HM).
Output	1. Beschikbare nieuwe / gewijzigde dienstencatalogusentries van deelnemer 2. Geïnformeerde collega deelnemers in het stelsel
Wie?	Technische beheerders van de deelnemers

3. Controleren en aggregeren dienstencatalogus	
Input	Aangeleverde nieuwe dienstencatalogus van deelnemer
Activiteit	• De beheerorganisatie verwerkt één keer per uur de wijzigingen in de dienstencatalogi van de deelnemende HM's door middel van een automatisch proces. • Dit proces controleert de aangeleverde dienstencatalogus wijziging(en) op conformiteit en verwijdert de handtekeningen. Als een wijziging niet door de controle komt, dan wordt de betreffende deelnemer via mail op de hoogte gebracht en worden wijzigingen van deze deelnemer niet verder verwerkt tot een correcte dienstencatalogus wordt aangeleverd. • Vervolgens aggregeert dit proces de dienstencatalogi van de verschillende deelnemers tot één nieuw bestand. • Vervolgens wordt de nieuwe dienstencatalogus gepubliceerd op een publieke URL: https://extranet.eherkenning.nl/productie_dienstencatalogus.xml. • De dienstencatalogus van de acceptatie omgeving wordt gepubliceerd op de publieke URL: https://extranet.eherkenning.nl/acceptatie_dienstencatalogus.xml • Tevens wordt de nieuwe dienstencatalogus voor productie gearchiveerd.
Output	Gepubliceerde geaggregeerde nieuwe dienstencatalogus
Wie?	Technische beheerder van de beheerorganisatie

4. Nieuwe dienstencatalogus doorvoeren	
Input	Gepubliceerde geaggregeerde nieuwe dienstencatalogus
Activiteit	De deelnemers halen de nieuwe dienstencatalogus op vanaf de publieke URL en voeren deze door in hun systeem door middel van een automatisch proces. Deelnemers moeten een gewijzigde dienstencatalogus uiterlijk twee uur na publicatie doorvoeren.
Output	Doorgevoerde nieuwe dienstencatalogus.
Wie?	• Technische beheerder beheerorganisatie • Technische beheerders deelnemers

5. Terugkoppeling onjuistheden dienstencatalogus	
Input	Feedback op dienstencatalogus entries uit de praktijk

Activiteit	1. Indien een AD of MR tijdens de uitvoering van zijn werkzaamheden constateert dat een dienstencatalogus entry onjuist is, MOET hij dat melden aan de desbetreffende eHerkenningsmakelaar (direct of via een issue in Mantis). 2. Voorbeelden van onjuiste dienstencatalogus entries zijn onder andere: • Structureel andere betrouwbaarheidsniveaus uitgevraagd dan beschreven; • Dienst ondersteunt andere dienstafnemers dan beschreven; • Dienst staat beschreven als 'IsPublic=true' maar er is geen internetpagina voor de dienst; • Beschrijving van dienst is onjuist of onbruikbaar voor het kunnen uitgeven van machtigingen. Bij meldingen aan de eHerkenningsmakelaar (direct of via Mantis) neemt deze contact op met de dienstverlener om wijzigingen te vragen van de dienstbeschrijving (keer terug naar stap 1 van dit proces).
Output	Input voor nieuw proces doorvoeren nieuwe dienstencatalogus.
Wie?	• Technische beheerder AD/MR • Technische beheerder beheerorganisatie

Proces en randvoorwaarden uitvoering penetratietesten

Procesbeschrijving en voorwaarden waaronder penetratietesten binnen het stelsel van eHerkenning worden uitgevoerd.

1. De beheerorganisatie verstrekt de opdracht tot het uitvoeren van een penetratietest aan een externe specialist. Conform het beleid voor het uitvoeren van penetratietesten wordt dit twee maal per jaar uitgevoerd.
2. Deelnemers en beheerorganisatie gaan akkoord met de uitvoering van de penetratietest en verlenen daar hun volledige medewerking aan. Indien gewenst verschaffen ze daartoe een zogenaamde vrijwaringsverklaring aan de externe specialist/uitvoerder. Een template voor deze vrijwaringsverklaring staat hier: Template vrijwaring penetratietest.
3. De externe specialist rapporteert integraal over de uitgevoerde penetratietesten aan de beheerorganisatie.
4. De beheerorganisatie zorgt ervoor dat individuele deelnemers de op hun organisatie betrekking hebbende rapport-onderdelen ontvangen.
5. De beheerorganisatie vraagt de individuele deelnemers om een reactie op het individuele rapport.
6. De beheerorganisatie rapporteert over de penetratietest aan het Tactisch overleg, waarbij individuele bevindingen zijn geanonimiseerd.
7. De beheerorganisatie archiveert het door de externe specialist opgeleverde rapport.
8. Het rapport kan, indien gewenst, ten behoeve van een stelselaudit door de stelselauditor worden geraadpleegd.

Proces incidentmanagement

In elke organisatie komen incidenten voor. Afhankelijk van het type incident en de ernst zullen passende maatregelen moeten worden getroffen. eHerkenning heeft een proces voor incidentmanagement om incidenten en calamiteiten netwerkbreed op gestructureerde wijze af te handelen.

Doelstelling

Het proces incidentmanagement heeft als doel om incidenten en calamiteiten op gestructureerde wijze afhandelen binnen het netwerk eHerkenning. Dit is aan de orde wanneer de beschikbaarheid, integriteit en/of vertrouwelijkheid van het stelsel en van de informatie daarbinnen wordt aangetast of risico op aantasting lopen.

Verantwoordelijkheden

De proceseigenaar is er verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving en dat het proces up-to-date blijft. De incidentmanager van de beheerorganisatie is eerste aanspreekpunt voor incidentmanagement. De incidentmanager van de beheerorganisatie controleert regelmatig of de contactlijst voor incidenten nog up-to-date is.

De deelnemers van eHerkenning zijn verplicht alle verstoringen, calamiteiten en beveiligingsincidenten in het netwerk z.s.m. te melden bij de beheerorganisatie. De deelnemers blijven zelf verantwoordelijk voor de oplossing van het incident/de calamiteit. De beheerorganisatie faciliteert hen en coördineert activiteiten indien nodig.

Classificatie van incidenten

Verstoring

Een verstoring is een gebeurtenis afwijkend van de verwachte standaard werking van een systeem of dienst. Dit betekent dat (onderdelen van) de dienstverlening van eHerkenning beperkt of niet beschikbaar zijn. Dit type incident heeft impact op de beschikbaarheid.

Calamiteit

Een calamiteit is een ongeplande situatie waarbij ten minste twee deelnemers zijn betrokken en waarvan verwacht wordt dat de duur van het niet beschikbaar zijn de maximale verstoringstijd van vier uur zal overschrijden. Dit betekent dat (onderdelen van) de dienstverlening van eHerkenning direct en/of ernstig hinder ondervinden.

Informatiebeveiligingsincident

Een dergelijk incident levert mogelijk impact c.q. risico op ten aanzien van de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie van eHerkenning.

Voorbeelden van informatiebeveiligingsincidenten:

- Verlies van USB stick, laptop, losse harde schijf etc. die informatie omtrent eHerkenning bevat.
- Misbruik van een eHerkenningsmiddel
- Signaleringen van hackpogingen of pogingen tot intrusion
- Fraude (of vermoeden van) door medewerker
- Signaleren van malware

Zie ook Service level

Uitvoering

Overzicht processtappen

- 1. Melding incident
- 2. Intake en beoordeling
- 3. Acties bepalen en uitvoeren
- 4. Acties monitoren
- 5. Evalueren

Toelichting processtappen

1. Melding incident	
Input	Een incident of calamiteit met betrekking tot de dienstverlening van eHerkenning doet zich voor.

Activiteit	Bij een verstoring of calamiteit 1. De betreffende deelnemer meldt de verstoring of de calamiteit in de issuetracker Mantis. Hierdoor kunnen alle deelnemers en de beheerorganisatie kennisnemen van de verstoring/calamiteit. 2. De betreffende deelnemer meldt de verstoring of de calamiteit telefonisch bij de incidentmanager van de beheerorganisatie. Bij een beveiligingsincident 1. De betreffende deelnemer meldt het beveiligingsincident telefonisch bij de incidentmanager van de beheerorganisatie. In overleg met de deelnemer kan de beheerorganisatie het beveiligingsincident alsnog in Mantis plaatsen. Hierbij wordt rekening gehouden met evt. gevoeligheden. Bij het maken van een melding in Mantis moet hiervoor het proces Meldingenbeheer gevolgd worden (zie Proces meldingenbeheer). Bij het maken van het incidentmelding in Mantis moeten de volgende gegevens worden opgenomen door de melder: a. Indien van toepassing, het laatste SAML of XACML bericht dat verstuurd werd voordat een incident optrad b. Indien van toepassing, een overzicht van de stappen die genomen moeten worden om het incident te reproduceren NB: er is een contactenlijst met telefoonnummers beschikbaar gesteld door de beheerorganisatie. Deze is te vinden op Contactlijsten.
Output	Melding van een incident of calamiteit bij de beheerorganisatie
Wie?	• Incidentmanager beheerorganisatie • Incidentmanagers van de deelnemers

2. Intake en beoordeling	
Input	Melding van een incident of calamiteit bij de beheerorganisatie
Activiteit	1. De incidentmanager van de beheerorganisatie beoordeelt voor eHerkenning: • de aard en de scope van het incident • de risico's • het mogelijk een calamiteit betreft Bij twijfel kan de incidentmanager zijn beoordeling voorleggen aan de proceseigenaar. De incidentmanager informeert zijn eigen team.
Output	Beoordeeld incident/calamiteit
Wie?	• Incidentmanager beheerorganisatie • Proceseigenaar

3. Acties bepalen en uitvoeren	
Input	Beoordeeld incident/calamiteit

Activiteit	Bij een verstoring of calamiteit: 1. De beheerorganisatie organiseert z.s.m., maar in elk geval binnen 24 uur, een telefonisch spoedoverleg met de betrokken deelnemers van eHerkenning en EZ om de calamiteit te bespreken. In dat overleg worden ten minste de volgende zaken besproken: a. Het communicatieprotocol ten aanzien van de calamiteit. Hierin wordt ook aandacht besteed aan de communicatie richting de aangesloten overheidsdienstverleners. b. De uit te voeren acties om de risico's te mitigeren en te beheersen (het te volgen proces). Bij een (beveiligings)incident: 1. De betreffende deelnemer zet acties uit om het incident z.s.m. op te lossen. 2. De beheerorganisatie coördineert indien nodig de acties en het contact met andere betrokken partijen etc. De incidentmanager is hierbij het eerste aanspreekpunt. Hij kan indien nodig het eigen team bij de beheerorganisatie inschakelen. NB: er is een contactenlijst beschikbaar gesteld die bij een calamiteit gebruikt wordt.
Output	Acties om het incident/calamiteit op te lossen
Wie?	• Incidentmanager beheerorganisatie • (Incidentmanagers van) de deelnemers • Bij calamiteit ook de leiding van de beheerorganisatie

4. Acties monitoren	
Input	Acties om het incident/calamiteit op te lossen
Activiteit	1. De incidentmanager van de beheerorganisatie wijst de melding toe aan een persoon binnen de beheerorganisatie. Hiervoor wordt Mantis gebruikt. 2. De incidentmanager van de beheerorganisatie monitort de acties die worden ondernomen om het incident of de calamiteit op te lossen. Dit betekent dat de beheerorganisatie met enige regelmaat de persoon aan wie de melding is toegewezen benadert of rechtstreeks met de betreffende deelnemer contact opneemt voor meer informatie. 3. Indien een incident/calamiteit langer dat 4 uur duurt stelt de beheerorganisatie elke 4 uur de deelnemers op de hoogte van de status. 4. Pas als het incident of de calamiteit is opgelost meldt de incidentmanager van de beheerorganisatie dit in Mantis. Hij sluit het issue en maakt het incidentrapport op basis van de input van de deelnemer.
Output	• Opgelost incident • Afgerond incidentrapport (voor template zie Template incidentrapport)
Wie?	• Incidentmanager beheerorganisatie • Incidentmanagers van de deelnemers

5. Evalueren	
Input	Incidentrapporten
Activiteit	Periodiek rapporteert de beheerorganisatie aan: 1. het Tactisch overleg over a. De aard van de incidenten b. De genomen maatregelen om de incidenten te neutraliseren c. De genomen maatregelen of voorstellen om gelijkwaardige incidenten in de toekomst te voorkomen. 2. het Security officers overleg over de bovenstaande punten, maar dan specifiek voor beveiligingsincidenten. Naar aanleiding van het evaluatierapport worden, indien mogelijk, verbeterplannen opgesteld.
Output	• Algemeen evaluatierapport • Mogelijk verbeterplannen
Wie?	Incidentmanager beheerorganisatie

Proces managementinformatie

Managementinformatie over het gebruik van het netwerk en de werking van het afsprakenstelsel wordt door middel van rapportages verzameld en verspreid. De rapportages worden o.a. gebruikt om de groei van het netwerk te monitoren op het gebied van aansluitingen, uitgifte van middelen en aantallen berichten.

Een meer uitgebreide beschrijving van de rapportage onderwerpen die in de managementrapportage aan de orde staat in Service level. Dit document beschrijft het proces voor het verzamelen , het opstellen en verspreiden van de managementrapportage.

Doelstelling

Zorgvuldig opstellen van de managementrapportage, zodat er een correct beeld bestaat van de stand van zaken in het netwerk. De managementrapportage kan tevens gebruikt worden om onregelmatigheden op te sporen.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De coördinator is ervoor verantwoordelijk dat de procesbeschrijving actueel blijft.

De deelnemers zijn verantwoordelijk voor het aanleveren van de juiste gegevens.

De beheerorganisatie is verantwoordelijk voor de verwerking van de gegevens tot een geaggregeerde rapportage. Hierbij is het van belang dat de concurrentiegevoelige informatie zoveel mogelijk verborgen blijft.

Overzicht processtappen

- 1. Aanleveren informatie
- 2. Verwerken informatie
- 3. Verspreiden informatie

Toelichting processtappen

1. Aanleveren informatie	
Input	Rapportagetool. De beheerorganisatie stelt een tool beschikbaar voor het valideren en samenvoegen van de managementinformatie.
Activiteit	1. De deelnemers verzamelen de eigen managementinformatie van de rapportageperiode (deze loopt van de eerste dag van een kalendermaand 4:00 uur tot volgende kalendermaand 4:00 uur) in xml formaat. 2. De deelnemers levert de eigen rapportage in xml formaat aan bij de beheerorganisatie, bij voorkeur zo snel mogelijk maar in ieder geval voor de 15de van elke kalendermaand. De rapportage wordt geuploadmet behulp van de rapportagetool van de beheerorganisatie. Bij het uploaden van de rapportage in xml formaat wordt een aantal gestandaardiseerde checks uitgevoerd door de rapportagetool. Zie ook Service level.
Output	Geuploade managementinformatie in xml formaat per deelnemer
Wie?	Deelnemers

2. Verwerken informatie	
Input	Managementinformatie per deelnemer
Activiteit	De beheerorganisatie verwerkt, anonimiseert en bundelt de gegevens tot een geaggregeerde rapportage. Indien de beheerorganisatie bijzonderheden heeft te melden, worden deze bijgevoegd.

Output	Geaggregeerde rapportage managementinformatie
Wie?	Secretaris van de beheerorganisatie

3. Verspreiden informatie	
Input	Geaggregeerde rapportage managementinformatie
Activiteit	1. De beheerorganisatie verzendt de geaggregeerde rapportage naar het Tactisch Overleg. 2. De beheerorganisatie gebruikt de gegevens tevens voor eventuele periodieke rapportages.
Output	Verspreiding van de geaggregeerde rapportage
Wie?	Secretaris van de beheerorganisatie

Proces meldingenbeheer

De beheerorganisatie is aanspreekpunt voor zaken met betrekking tot de ontwikkeling en implementatie van het Afsprakenstelsel eHerkenning. Mantis functioneert als portaal voor het maken van meldingen. Bij het melden van een incident moet het proces incidentmanagement als basis genomen worden.

Deelnemers gebruiken Mantis voor het aanmaken van meldingen. Bijvoorbeeld voor het melden van problemen met betrekking tot het implementeren van het afsprakenstelsel, voorstellen voor RFC's, server onderhoud, simulators, metadata en dienstencatalogus, en beveiligingsissues. De beheerorganisatie gebruikt Mantis om op meldingen te reageren.

Doelstelling

De doelstelling van het proces meldingenbeheer is enerzijds dat meldingen op de juiste manier aangemaakt worden en anderzijds dat er snel en adequate hierop gereageerd kan worden zodat ontwikkeling en implementatie voorspoedig verloopt en de productieomgeving goed functioneert.

Verantwoordelijkheden

- De technisch beheerder van de beheerorganisatie zorgt ervoor dat het beschreven proces correct wordt uitgevoerd en is eerste aanspreekpunt als het gaat om het gebruik van Mantis
- De change manager van de beheerorganisatie wordt door de technisch beheerder ingeschakeld als deze constateert dat de melding geen incident betreft.
- De deelnemers zijn verantwoordelijk voor het zorgvuldig aanmaken van meldingen en het reageren op meldingen indien nodig.

Status van een melding

De status van een melding is relevant voor gebruikers van Mantis. Elke melding start met de status "Nieuw" en moet uiteindelijk de status "Afgesloten" krijgen. Voor elk van de statussen is de betekenis de volgende.

Nieuw	De melding is ingeschoten en nog niet in behandeling genomen door de beheerorganisatie
Terugkoppeling	Er is feedback nodig. Deze status wordt in de regel door de aanmelder aan een melding gegeven als hij een melding opnieuw heeft geopend nadat deze afgesloten is geweest.
Erkend	De beheerorganisatie ziet in dat de aanmelder een terechte opmerking plaatst al is hij nog niet zeker of de al dan niet aangedragen oplossing correct is.
Bevestigd	De beheerorganisatie gaat akkoord met de genoemde oplossing – in de melding zelf of in één van de reacties – en werkt aan de implementatie van een oplossing.
Toegewezen	Melding is toegewezen aan een persoon. Deze persoon moet de melding in behandeling nemen en een nieuwe status aan de melding toewijzen. Zolang de status op "Toegewezen" blijft staan betekent dit dat de nieuwe verantwoordelijke de melding nog niet in behandeling heeft genomen.

Afgemeld	De beheerorganisatie geeft aan dat melding voldoende is behandeld.
Afgesloten	De melding is afgesloten en hoeft niet meer ingezien te worden. De aanmelder mag de melding opnieuw openen als hij meent dat de reacties niet voldoende zijn.

Overzicht processtappen

- 1. Melding aanmaken
- 2. Melding toewijzen
- 3. Melding behandelen

Toelichting processtappen

1. Melding aanmaken

Input	Een melding kan door zowel deelnemers als de beheerorganisatie worden aangemaakt. Vaak gebeurt dit door deelnemers van het stelsel, maar de beheerorganisatie kan ook zelf nieuwe meldingen aanmaken. Een persoon die een melding maakt heet een aanmelder.
Activiteit	1. Er wordt ingelogd in Mantis met de verstrekte gebruikersnaam en wachtwoord. 2. Er wordt in Mantis een project gekozen waar de melding bij past 3. Optioneel wordt er gekozen voor één van de mogelijke categorieën. Dit zijn de volgende. • Stelselbreed; als de melding voor iedereen relevant is • Beheerorganisatie; als de melding alleen relevant is voor de beheerorganisatie 4. De aanmelder geeft een korte samenvatting en omschrijft de melding met relevante details 5. De aanmelder kiest het versienummer van het afsprakenstelsel waar de melding van toepassing op is. Er mag voor n.v.t. gekozen worden als het versienummer niet relevant is. 6. De aanmelder mag de melding toewijzen aan een individu als de melding specifiek voor die persoon bedoeld is. Als de melding door verschillende personen opgepakt kan worden zou de melding niet aan een specifiek persoon toegewezen moeten worden zodat de beheerorganisatie de melding intern kan toewijzen. 7. De beheerorganisatie wordt op de hoogte gesteld van de nieuwe melding middels een automatisch verzonden e-mail. Soms geeft een melding reuring wat aanleiding kan zijn om nieuwe meldingen aan te maken. Elke melding moet apart aangemaakt worden en mag niet als reactie op een bestaande melding geplaatst worden. Als er een relatie bestaat met andere meldingen mag hier de functionaliteit van Mantis gebruikt worden om relaties aan te geven. Mantis biedt functionaliteit om de relatie met andere meldingen aan te geven nadat een melding is aangemaakt.
Output	Gerapporteerde melding
Wie?	De beheerorganisatie beheert Mantis. Deelnemers en leden van de beheerorganisatie kunnen op Mantis een melding aanmaken.

2. Melding toewijzen

Input	Een nieuwe melding op Mantis
Activiteit	1. De beheerorganisatie controleert of de melding in het juiste project binnen Mantis is geplaatst. Indien nodig verplaatst zij de melding naar het juiste project. 2. De beheerorganisatie wijst de melding toe aan een specifiek persoon. Deze persoon wordt dan verantwoordelijk voor het behandelen van deze melding en is contactpersoon voor de aanmelder van de melding.
Output	Toegewezen melding
Wie?	De technisch beheerder is verantwoordelijk voor het toewijzen van meldingen die nog aan niemand zijn toegewezen.

3. Melding behandelen	
Input	Toegewezen melding
Activiteit	Leden van de beheerorganisatie controleren regelmatig de aan hen toegewezen meldingen en meldingen die al lange tijd open staan. Ze voeren daarbij de volgende acties uit: 1. Probeer op de melding te reageren. Als dit niet mogelijk is moet de melding toegewezen worden aan een ander persoon binnen de beheerorganisatie. Zo nodig met een notitie waarom hij de melding niet kan behandelen. 2. Behandel de melding. Zet daarbij de melding op "Afgemeld" en wijs de melding toe aan een persoon die kan controleren of de melding terecht is afgemeld; bijvoorbeeld omdat het probleem is opgelost of omdat er eenvoudigweg geen actie hoeft te worden ondernomen. Deze persoon controleert of de afmelding terecht is en sluit de melding door deze de status "Gesloten" te geven. 3. Als de verantwoordelijke extra informatie nodig heeft plaatst hij een reactie op de melding. 4. Als de aanmelder niet reageert mag deze herinnerd worden door van de "Herinnering verzenden" mogelijkheid gebruik te maken. In enkele gevallen is het gewenst dat een ander persoon dan de aanmelder reageert op een melding. In dat geval wordt deze persoon op de hoogte gesteld dat hij moet reageren middels een herinnering die door de beheerorganisatie verstuurd wordt met de functionaliteit uit Mantis.
Output	Afgesloten melding
Wie?	De persoon die verantwoordelijk is gemaakt zorgt er voor dat de melding correct wordt behandeld. De beheerorganisatie ziet er op toe dat dit binnen redelijke termijn gebeurt.

Proces metadata

In het Herkenning netwerk wordt SAML metadata gebruikt voor het beschrijven van de URLs en certificaten die worden gebruikt op de verschillende koppelvlakken. Actuele metadata is van belang om twee redenen:

1. De metadata geeft weer voor welke rol en op welk betrouwbaarheidsniveau een deelnemer is toegetreden. Met andere woorden, op basis van de metadata wordt bepaald wie wat mag in het netwerk.
2. De metadata geeft weer hoe systemen van deelnemers kunnen worden benaderd en met welke certificaten deze systemen zijn te authenticeren. Hierdoor speelt de metadata een belangrijke rol in het bewaken van de integriteit en authenticiteit van de verklaringen en gegevens die door het netwerk worden geleverd.

Het in dit document beschreven proces heeft tot doel nieuwe geaggregeerde metadata op een snelle en betrouwbare manier door te voeren in de systemen van de deelnemers.

Hiervoor worden vier subprocessen doorlopen:

1. Een deelnemer biedt nieuwe metadata aan. Deze wordt door de beheerorganisatie gecontroleerd.
2. Bij goedkeuring genereert de beheerorganisatie nieuwe aggregeerde metadata. Deze metadata wordt op de afgesproken plaatsen gepubliceerd en de deelnemers worden hiervan op de hoogte gesteld.
3. Deelnemers importeren de nieuwe metadata automatisch in hun systemen vanaf de URL https://extranet.eherkenning.nl/productie_metadata.xml binnen de periode zoals die gespecificeerd is in de cacheduration in de voorgaande versie van de gepubliceerde metadata.

> Metadata wordt gebruikt voor zowel het productie- als het testnetwerk. De processen voor test en productie zijn grotendeels gelijk. Dit document beschrijft beide.

Doelstelling

De doelstelling van het metadata proces is tweeledig:

1. Waarborgen dat de geaggregeerde metadata op correcte wijze tot stand komt.
2. Waarborgen dat alle deelnemers de actuele geaggregeerde metadata in hun systemen gebruiken.

Verantwoordelijkheden

De proceseigenaar is er verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie voert de meeste activiteiten uit vanuit de beheerorganisatie en is er verantwoordelijk voor dat de procesbeschrijving actueel blijft. De juridisch coördinator van de beheerorganisatie bewaakt dat de metadata een correcte weergave is van de contractadministratie en toetredingsbesluiten.

Overzicht processtappen

- 1. Controleren en aanleveren metadata
- 2. Genereren, en publiceren geaggregeerde metadata
- 3. Doorvoeren geaggregeerde metadata

Toelichting processtappen

1. Controleren en aanleveren metadata	
Input	Een deelnemer genereert nieuwe metadata conform de technische specificaties, ondertekent deze met zijn valide digitale handtekening en controleert het resultaat met behulp van de eherkenning metadata validator (https://extranet.eherkenning.nl/metadata-validator/metadataUpload). Uiterlijk 7 dagen voor daadwerkelijk doorvoeren van de geplande wijzigingen in zijn infrastructuur stelt de deelnemer de gecontroleerde nieuwe metadata beschikbaar voor de beheerorganisatie op zijn productionele metadata (HTTPS) URL. Deelnemers publiceren hun productionele metadata op een aparte URL per rol binnen het eHerkenning netwerk. Nieuwe entities worden hierin toegevoegd met een ValidFrom datum in het beoogde onderhoudswindow waarin de wijziging moet worden doorgevoerd. Overtollige entities worden verwijderd door het toevoegen van een ValidUntil datum in het beoogde onderhoudswindow waarin de wijziging moet worden doorgevoerd. Van gewijzigde entities wordt de oude entry op genomen met een validUntil datum en de nieuwe entry met een validFrom datum. Ook hierbij liggen beide datums datum in het beoogde onderhoudswindow waarin de wijziging moet worden doorgevoerd. Daarna informeert de deelnemer de andere deelnemers en de beheerorganisatie d.m.v. een Mantis issue en een mail aan info@eherkenning.nl. Dit issue bevat minimaal: 1. Het verwachte tijdstip van doorvoeren 2. Een beschrijving van de wijzigingen 3. De URL van de nieuwe metadata
Activiteit	1. Een automatisch controle proces voert de technische controles op de, door de deelnemer gepubliceerde nieuwe, metadata uit. Deze controles bestaan uit: a. Validatie van de het metadata bestand tegen de technische specificities b. Validatie van de elektronische handtekening van de deelnemer c. Controle van de consistentie van het metadata bestand d. Controle op juridische inhoud (de rollen en betrouwbaarheidsniveaus die de deelnemer o.b.v. deze metadata claimt te mogen uitvoeren), zoals vooraf gedefinieerd door de juridisch coördinator van de beheerorganisatie. N.B. Deze controle stap wordt voor metadata van het acceptatienetwerk overgeslagen. Hier moeten (aankomende) deelnemers juist kunnen testen als onderdeel van het toetredingsproces. 2. Wanneer één van de genoemde controles geen positief resultaat heeft, wordt geen nieuwe metadata gepubliceerd op de URL van de beheerorganisatie. 3. De deelnemers worden per e-mail van het resultaat van de controle op de hoogte gebracht alleen als metadata van de deelnemer gewijzigd is om "spamming" te voorkomen. Bij fouten in de metadata die in stap 1 worden geconstateerd, worden deze via e-mail door het automatisch proces zowel naar de deelnemer als naar de beheerorganisatie verstuurd.
Output	• In behandeling genomen goedgekeurde metadata. • Terugmelding besluit.
Wie?	• Beheerorganisatie beoordeelt de metadata. • Juridisch coördinator beoordeelt de rollen en betrouwbaarheidsniveaus.

2. Genereren, en publiceren geaggregeerde metadata	
Input	Goedgekeurde metadata

Activiteit	1. Het automatisch proces genereert, na stap 1 in de voorgaande activiteit als wijziging in metadata gedetecteerd is, een nieuwe versie van het huidige geaggregeerde metadatabestand met een cacheduration van "PT1H" (één uur). Entries met een ValidUntil datum meer dan 1 maand in het verleden worden hierbij uit het metadata bestand verwijderd. 2. Deze nieuwe geconsolideerde metadata wordt door het automatisch proces gepubliceerd op de URL https://extranet.eherkenning.nl/productie_metadata.xml of https://extranet.eherkenning.nl/acceptatie_metadata.xml. Deze metadata en het moment waarop deze door het automatisch proces in productie gezet is, wordt tevens door het automatisch proces gestuurd naar info@eherkenning.nl, waarna deze informatie door de technisch beheerder op het Mantis issue wordt geplaatst en de metadata wordt gearchiveerd conform de werkbeschrijving in Confluence (https://extranet.eherkenning.nl/confluence/display/beheer/5.2.6.+Metadata+en+Dienstencatalogus).
Output	Gepubliceerde metadata
Wie?	Technisch beheerder van de beheerorganisatie voert deze stap uit

3. Doorvoeren geaggregeerde metadata	
Input	Gepubliceerde metadata
Activiteit	• De automatische processen van de deelnemers pakken de nieuwe metadata op en voeren deze door, waarbij de daadwerkelijke wijzigingen door de gebruikte ValidIUntil/ValidFrom datums pas in het onderhoudswindow daadwerkelijk actief worden. • De deelnemer die nieuwe metadata doorvoert controleert, tijdens zijn onderhoudswindow, de werking van de nieuwe metadata. Als de wijzigingen niet goed werken, dan kan de deelnemer tijdens het onderhoudswindow een nieuwe versie van de nieuwe metadata uploaden of de oude versie uploaden. Deze wordt door het automatisch proces gecontroleerd en geaggregeerd gepubliceerd op de URL https://extranet.eherkenning.nl/productie_metadata.xml of https://extranet.eherkenning.nl/acceptatie_metadata<versie>.xml (waarbij <versie> die versie van de simulator is, dus bijvoorbeeld https://extranet.eherkenning.nl/acceptatie_metadata1.5.xml voor de Simulator 1.5), waarna deze binnen een uur automatisch door de deelnemers wordt opgepakt en doorgevoerd. Zo nodig kan de technisch beheerder, bij ernstige verstoringen in het onderhoudswindow, handmatig een rollback naar de originele productionele metadata van voor de wijziging doorvoeren. • De deelnemers melden in Mantis het resultaat van de doorvoering indien relevant.
Output	Geïmplementeerde nieuwe metadata
Wie?	• Deelnemers implementeren. • Technisch beheerder monitort en rapporteert aan de deelnemers.

Proces naleving

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het netwerk voor eHerkenning. Het nalevingsbeleid is er op gericht om een correcte naleving van het afsprakenstelsel te verzekeren. Dit gebeurt zo veel mogelijk in goed onderling overleg tussen de beheerorganisatie en de betrokken deelnemer of dienstverlener. Het kan echter noodzakelijk zijn om een correcte naleving af te dwingen via het opleggen van sancties.

Doelstelling

Het proces naleving heeft als doel zorgvuldige uitvoering van het nalevingsbeleid.

Verantwoordelijkheden

De bevoegdheid tot het uitvoeren van het nalevingsbeleid is toebedeeld aan de beheerorganisatie, als uitvloeisel van de taak om het merk te beheren.

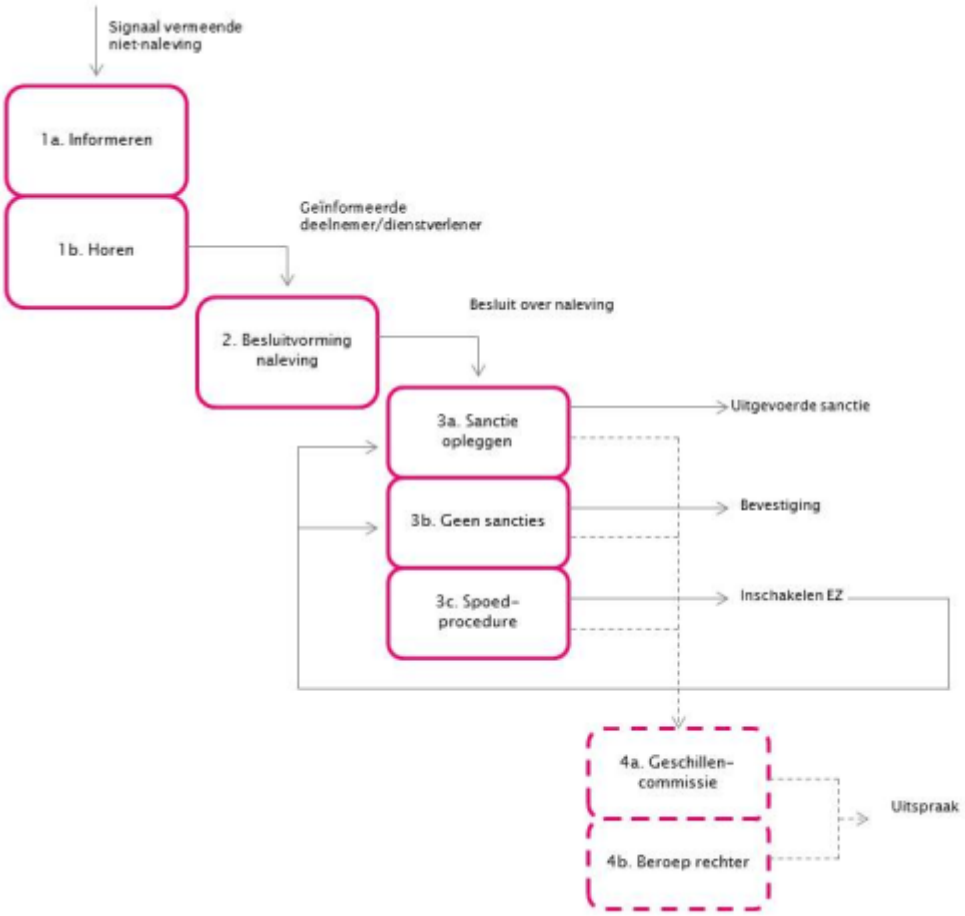
Uitgangspunt is dat de beheerorganisatie en de betrokken deelnemer/dienstverlener in eerste instantie trachten in goed onderling overleg te komen tot een oplossing van de vermeende niet-naleving.

Het opleggen van sancties kan zelfstandig door de beheerorganisatie worden afgehandeld. Bij de spoedprocedure, of bij de

sancties schorsing of beëindiging van de deelnemersovereenkomst is enkel het Ministerie van EZ bevoegd om de beslissing te nemen. Zie ook Proces uittreden.

Een specifiek onderdeel van het nalevingsbeleid is de compensatieregeling. Deze regeling is van toepassing op specifiek de naleving van het implementatieplan bij een release. De beheerorganisatie valt hier zelf ook onder. Zie ook Proces change en release.

Overzicht processtappen



- 1a. Informeren deelnemer/dienstverlener
- 1b. Horen deelnemer/dienstverlener
- 2. Besluitvorming naleving
- 3 a/b/c. Uitvoering
- 4 a/b. Optioneel: klachten en geschillencommissie en/of beroep bij de rechter

Toelichting processtappen

1a. Informeren deelnemer/dienstverlener

Input	Melding of signaal van vermeende niet-naleving van het afsprakenstelsel, waarbij het niet lukt om er in onderling overleg uit te komen. In de praktijk zal het proces naleving vaak gevoed worden door de uitvoering van andere beheerprocessen. Naar aanleiding van bijvoorbeeld het proces incidentmanagement of het proces managementinformatie rapporteren kan de beheerorganisatie signalen krijgen over vermeende niet-naleving. Voorbeelden: • een klacht • de rapportageverplichting • incidentmanagement • certificering • de resultaten van penetratietesten
Activiteit	• De beheerorganisatie signaleert op grond van verkregen informatie dat een deelnemer/dienstverlener mogelijkerwijs een of meer afspraken uit het afsprakenstelsel niet, niet tijdig of niet volledig uitvoert. • De beheerorganisatie neemt zo spoedig mogelijk contact op met de betreffende deelnemer/dienstverlener. De beheerorganisatie stelt de deelnemer/dienstverlener tevens schriftelijk zo gedetailleerd mogelijk op de hoogte van de vermeende overtreding van het afsprakenstelsel.
Output	Geïnformeerde deelnemer/dienstverlener over vermeende niet-naleving
Wie?	Beheerorganisatie Betreffende deelnemer/dienstverlener

1b. Horen deelnemer/dienstverlener	
Input	Geïnformeerde deelnemer/dienstverlener over vermeende niet-naleving
Activiteit	De deelnemer/dienstverlener wordt uitgenodigd te reageren op de mededeling van de beheerorganisatie aangaande de vermeende niet-naleving van het afsprakenstelsel. Voor informatieverstrekking zie ook het nalevingsbeleid in het [Juridisch Kader].
Output	Reactie van deelnemer/dienstverlener op vermeende niet-naleving
Wie?	Beheerorganisatie Betreffende deelnemer/dienstverlener

2. Besluitvorming naleving	
Input	Reactie van deelnemer/dienstverlener op vermeende niet-naleving

Activiteit	De beheerorganisatie beoordeelt de vermeende niet-naleving nadat de deelnemer/dienstverlener heeft gereageerd. Op basis van de beschikbare informatie beoordeelt de beheerorganisatie of er sprake is van niet-naleving. Deze beoordeling wordt door andere personen gedaan dan degene die betrokken waren bij de controle, monitoring en informatievergaring van de vermeende niet- naleving. De onder stap 1 genoemde nieuw betrokkenen bij het dossier nemen vervolgens een besluit over welke vervolgactie moet worden ondernomen in reactie op de vermeende niet-naleving. Er zijn drie opties: 1. Indien er naar de beoordeling van de beheerorganisatie sprake is van niet-naleving van het afsprakenstelsel, kan de beheerorganisatie besluiten tot het opleggen van een sanctie aan de betrokken deelnemer/dienstverlener. Voor een lijst van sancties die de beheerorganisatie kan opleggen zie het nalevingsbeleid in het [Juridisch Kader]. 2. Indien er naar de beoordeling van de beheerorganisatie geen sprake is van niet-naleving, zal de beheerorganisatie besluiten de betrokken deelnemer/dienstverlener geen sancties op te leggen. 3. Indien de beheerorganisatie van mening is dat het noodzakelijk is dat EZ wordt opgeschakeld, kan zij besluiten om EZ in te lichten en de zaak voorleggen aan en bespreken met EZ. De betrokken deelnemer/dienstverlener wordt zo snel mogelijk schriftelijk en met redenen omkleed geïnformeerd over het besluit. In het besluit wordt opgenomen welke eventuele sancties worden opgelegd, voor welke termijn en eventuele voorwaarden of voorschriften worden vermeld. Voor het opstellen van het besluit zie ook het nalevingsbeleid in het [Juridisch Kader].
Output	Besluit over de naleving
Wie?	• Beheerorganisatie of EZ • Betreffende deelnemer/dienstverlener

3 a/b/c. Uitvoering

Input	Besluit over de naleving
Activiteit	Vervolgens kan de beheerorganisatie overgaan tot het opvolgen van het besluit. • Indien is besloten is dat de beheerorganisatie zelf over gaat tot het opleggen van sancties, zal de beheerorganisatie overgaan tot het uitvoeren van de sancties, zoals opgenomen in het nalevingsbeleid in het [Juridisch Kader]. • Indien is besloten om EZ op te schakelen, zal de beheerorganisatie de zaak voorleggen aan en bespreken met EZ. EZ besluit vervolgens welke sanctie de beheerorganisatie namens haar ten uitvoer legt. • Indien is besloten dat er geen sanctie wordt opgelegd, zal de beheerorganisatie geen verdere actie ondernemen en dit besluit bevestigen.
Output	Uitgevoerd besluit
Wie?	• Beheerorganisatie • Betreffende deelnemer/dienstverlener • Indien nodig, EZ

4 a/b. Optioneel: klachten en geschillencommissie en/of beroep bij de rechter

Input	Uitgevoerd besluit
Activiteit	Tegen het besluit van de beheerorganisatie of EZ tot het al dan niet opleggen van een of meer sancties staat beroep open bij de klachten en geschillencommissie van eHerkenning en/of de bevoegde civiele rechter.
Output	Uitspraak van de klachten en geschillencommissie en/of de rechter
Wie?	• Beheerorganisatie • Betreffende deelnemer/dienstverlener • Klachten- en geschillencommissie • Rechter

Tabel doorlooptijden proces naleving

De hieronder genoemde termijnen zijn streeftermijnen en niet bindend. Het halen van de termijnen is bijvoorbeeld afhankelijk van de volledigheid van het dossier of de beschikbaarheid van andere betrokken partijen. Indien een termijn niet kan worden gehaald, worden de betrokkenen hiervan direct door de beheerorganisatie van op de hoogte gesteld. Tegelijkertijd wordt door de beheerorganisatie aangeven wat de nieuwe termijn is.

In de onderstaande tabel staat 'BO' voor beheerorganisatie.

Activiteit	Door	Tijd
1. informeren deelnemer/dienstverlener over vermeende niet-naleving	BO	1 werkdag
2. horen van de deelnemer/ dienstverlener	BO en deelnemer/dienstverlener	3 werkdagen na stap 1
3.beoordeling informatie en nemen van besluit over naleving	BO	3 werkdagen na stap 2
3a. deelnemer/dienstverlener informeren over het besluit over naleving	Deelnemer/dienstverlener	1 werkdagen na stap 3
4. Overgaan tot opvolgen besluit	BO	start 1 werkdag na ontvangst deelnemer/dienstverlener

Proces onderhoud cookieserver

Voor de werking van Single Sign On heeft iedere eHerkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein *.eherkenning.nl. De DNS van het gezamenlijke domein wordt beheerd door beheerorganisatie.

Iedere cookieserver heeft een eigen IP adres gespecificeerd door de betreffende deelnemer. Deze IP-adressen zijn door de beheerorganisatie opgenomen in de DNS van *.eherkenning.nl.

Er moet onderhoud plaatsvinden als een van de deelnemers zijn IP-adres wijzigt. In de praktijk kan dit bijvoorbeeld voorkomen wanneer er een nieuwe deelnemer toetreedt, of wanneer een deelnemer besluit zijn software over te zetten op een nieuwe machine met een ander IP-adres.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technische beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Toelichting processtappen

1. Wanneer het IP-adres van de deelnemer wijzigt, dan meldt hij dat tijdig (minimaal twee weken van te voren) via de issuetracker Mantis. Hierbij vermeldt de deelnemer in ieder geval het huidige IP-adres dat nu in gebruik is, het nieuwe IP-adres en de termijn waarop de wijziging plaats moet vinden.
2. De beheerorganisatie vervangt het IP-adres van de betreffende deelnemer in DNS van het gezamenlijke domein in afstemming met de betreffende deelnemer.
3. De deelnemer ontvangt een bevestiging van de beheerorganisatie via Mantis wanneer de vervanging is afgerond.
4. De deelnemer KAN nu het nieuwe IP-adres gebruiken.

Proces toetreden

Nieuwe partijen kunnen geïnteresseerd zijn in deelname aan het netwerk voor eHerkenning. Het toetredingsproces beschrijft de stappen die genomen moeten worden om deel te mogen nemen aan het netwerk eHerkenning en het merk eHerkenning te mogen voeren. Ook in andere situaties kan er sprake zijn van toetreding. In al die gevallen moet het toetredingsproces worden gevolgd.

Er is sprake van toetreding in de volgende situaties:

1. Een volledig nieuwe toetreder wil een of meerdere rollen in het stelsel gaan vervullen.
2. Een huidige deelnemer van eHerkenning wil zijn rol(len) in het stelsel uitbreiden met een of meerdere rollen.
3. Een huidige deelnemer van eHerkenning wil met een of meerdere betrouwbaarheidsniveaus uitbreiden op de rol(len) die hij al vervulde in het stelsel.
4. Een huidige deelnemer van eHerkenning wil zijn processen voor uitgifte van middelen of registratie van machtigingen aanpassen.
5. Een huidige deelnemer van eHerkenning wil een of meerdere optionele functionaliteiten gaan leveren (of uitbreiden) aan zijn klanten.
6. Er komt een nieuwe release van het afsprakenstelsel. Alle huidige deelnemers treden opnieuw toe tot het nieuwe afsprakenstelsel.
7. Er komt een nieuwe release van het productienetwerk (dit is een mogelijke aanvulling op het vorige punt). Alle huidige deelnemers treden opnieuw toe tot de nieuwe versie van het productienetwerk.

Het proces voor alle situaties wordt beschreven in dit document. Voor het opnieuw toetreden als deelnemer bij de implementatie van een nieuwe release, zie ook Proces change en release.

Gerelateerde onderdelen van het afsprakenstelsel:

- Toetredingseisen
- Testing
- Afspraken over verantwoordelijkheid en verantwoording

Doelstelling

De doelstelling van het toetredingsproces is als volgt:

Op zorgvuldige en gestructureerde wijze nieuwe deelnemers aansluiten op eHerkenning. Zorgvuldig betekent:

- volgens een transparant proces
- zonder verstoringen
- dat de toetreder voldoet aan het afsprakenstelsel

Verantwoordelijkheden

De coördinator toetreden is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De coördinator toetreden is er verantwoordelijk voor dat de procesbeschrijving actueel blijft en coördineert de verschillende stappen in het proces.

De externe auditor heeft de taak om de uitgifteprocessen voor middelen en machtigingen te toetsen. De externe auditor moet een gecertificeerde ISO27001 auditor of Register EDP-auditor zijn, die van de potentiële toetreder de opdracht krijgt om de uitgifteprocessen te toetsen.

De experts zijn door Logius aangesteld om de opzet van de uitgifteprocessen te toetsen. Het resultaat van deze toets wordt door de externe auditor gebruikt bij zijn toetsing. De experts zijn niet direct betrokken bij de beheerorganisatie van eHerkenning ivm functiescheiding.

De beheerorganisatie heeft de taak om de testresultaten (keten- en simulatortest) van de toetreder steekproefsgewijs te toetsen.

EZ geeft uiteindelijk toestemming voor toetreding als houder van het merkrecht van eHerkenning. Daarmee krijgt een partij het recht om aan te sluiten op het netwerk eHerkenning en onder het merk eHerkenning de propositie te voeren waarvoor hij is toegetreden.

Omdat in de toetredingsprocedure concurrentiegevoelige gegevens een rol kunnen spelen vallen alle betrokken medewerkers van de beheerorganisatie, de experts en de externe auditor onder strikte geheimhouding en wordt het betreffende deel van het archief zorgvuldig opgezet.

Processtappen

- 1. Formeel verzoek tot toetreding indienen
- 2. Benodigde documentatie leveren
- 3. Toetsing
- 4. Toestemming
- 5. Optioneel: tekenen deelnemersovereenkomst (deze stap wordt enkel doorlopen als het een volledig nieuwe toetreder

- betreft)
- 6. Aansluiting realiseren

Toelichting

1. Formeel verzoek tot toetreding indienen	
Input	Positieve intake voor toetreden met een geïnteresseerde partij
Activiteit	1. De partij maakt zich klaar voor toetreding (moet voldoen aan het afsprakenstelsel). 2. De partij dient het ingevulde formulier Template verzoek tot (uitbreiding) toetreding eHerkenning in bij de beheerorganisatie en benoemt tevens een aanspreekpunt in de eigen organisatie. 3. De beheerorganisatie beoordeelt het ingevulde formulier en bespreekt het verdere verloop van het toetredingsproces met de partij. 4. De beheerorganisatie informeert het Tactisch Overleg (gremium) over het formele verzoek tot toetreding.
Output	Formeel verzoek tot toetreding + kennisname van verloop van het toetredingsproces
Wie?	• Coördinator toetreden • Vanuit de toetreder de aangestelde contactpersoon

2. Benodigde documentatie leveren	
Input	Formeel verzoek tot toetreding
Activiteit	1. De toetredende partij levert de benodigde documentatie voor de toetsing van de toetreding indien van toepassing aan via e-mail bij de beheerorganisatie, de externe auditor en experts: • Metadata URL aanleveren en public key van het signing certificaat van zowel de acceptatie- als productiesystemen. Hiermee wordt vervolgens de metadata geautomatiseerd aangemaakt volgens het Proces metadata. Procesbeschrijving(en) van de uitgifteprocessen voor middelen en machtigingen met daaraan toegekende betrouwbaarheidsniveau(s) (indien van toepassing). Hierbij moet minimaal aangegeven zijn hoe het betrouwbaarheidsniveau kan worden toegekend. • Test-authenticatiemiddel en/of test-machtigingen (indien van toepassing) en de bijbehorende ingevulde checklists Checklist simulator test en Checklist chain test. • Een ingevulde en getekende Template zelfverklaring. Hiermee verklaart de toetreder aan het afsprakenstelsel te voldoen.
Output	Benodigde documentatie voor beoordeling toetreding
Wie?	• Coördinator toetreden • Vanuit de toetreder de aangestelde contactpersoon • De externe auditor en de experts

3. Toetsing	
Input	Benodigde documentatie voor beoordeling toetreding

Activiteit	1. toets processen (optioneel)
	• De externe auditor en de experts toetsen of de uitgifte- en registratieprocessen voor middelen en machtigingen voldoen aan de toetredingseisen, wanneer er door de toetreding sprake is van een wijziging in deze processen. Dit bestaat uit
	  • het toetsen van de procesbeschrijvingen en de daaraan toegekende betrouwbaarheidsniveaus (indien van toepassing). De aangeleverde procesbeschrijving wordt getoetst op conformiteit aan STORK en het afsprakenstelsel onderdeel Betrouwbaarheidsniveaus. De eerste toets wordt uitgevoerd door de experts. Er vindt een gesprek plaats met de experts waarin de toetreder over de beschreven processen en de belangrijkste onderdelen van de zelfverklaring wordt bevraagd. Hij krijgt dan de gelegenheid om eventuele onduidelijkheden weg te nemen.
	  • De toetreder geeft vervolgens een externe-auditor de opdracht om met het resultaat van de experts de toetsing uit te voeren. Dit kan worden gecombineerd met het uitvoeren van de ISO27001 audit.
	• Zie voor de informatiebeveiligingseisen waaraan de toetreder moet voldoen om te mogen toetreden: Afspraken over verantwoordelijkheid en verantwoording
	
	2. toets aansluiting
	• De beheerorganisatie test de zelfverklaring van de toetredende partij op twee manieren:
	  1. De simulatortest wordt uitgevoerd met de eHerkenning simulator, een instrument dat berichten verzendt en de antwoorden beoordeelt op conformiteit aan het afsprakenstelsel. De focus van deze test is conformiteit.
	  2. De ketentest vindt plaats met systemen in een apart netwerk van systemen in een eigen OTAP acceptatieomgeving. In de ketentest worden ketens van eHerkenningsmakelaar, authenticatiedienst en machtigingenregister getest, door met een gesimuleerde dienstverlener berichten te versturen naar de verschillende eHerkenningsmakelaars in het netwerk. De focus van deze test is interoperabiliteit.
	• Voor meer informatie over testen voor deelnemers, zie Testing.
	
	3. penetratietest (optioneel)
	• De toetredende partij is, wanneer hij toetreedt als nieuwe deelnemer of voor een nieuwe rol, tevens verplicht om een penetratietest te ondergaan die overeenkomt met de reguliere penetratietesten die eHerkenning uitvoert. Hiervoor kan de deelnemer aansluiten bij de halfjaarlijkse reguliere penetratietest van eHerkenning.
	• Voor meer informatie over penetratietesten, zie Proces en randvoorwaarden uitvoering penetratietesten
	
	4. rapporteren
	• De externe auditor en de experts stellen een bevindingenrapport op ten aanzien van de uitgifteprocessen. De beheerorganisatie stelt een bevindingenrapport op ten aanzien van de netwerktesten. Eventueel wordt er ook een penetratietestrapport opgeleverd.
	• Op basis van de beschikbare bevindingenrapporten geeft de beheerorganisatie een positief of negatief advies over de toetreding aan het ministerie van EZ.

Output	Advies van de beheerorganisatie aan het ministerie van EZ op basis van de aangeleverde bevindingenrapporten
Wie?	• Coördinator toetreden • Technische beheerder van de beheerorganisatie • Vanuit de toetreder de aangestelde contactpersoon • De externe auditor en de experts

4. Toestemming	
Input	Advies van de beheerorganisatie aan EZ op basis van de aangeleverde bevindingenrapporten
Activiteit	1. De beheerorganisatie legt het advies ter besluitvorming voor aan de opdrachtgever het ministerie van Economische Zaken. Het ministerie van Economische Zaken verleent uiteindelijk al dan niet toestemming voor de betreffende toetreding. 2. De toetreder wordt op de hoogte gesteld. 3. Het Tactisch Overleg wordt op de hoogte gesteld van de toetreding.
Output	Toestemming voor toetreding
Wie?	• Directie van de beheerorganisatie • Ministerie van Economische Zaken • Vanuit de toetreder de aangestelde contactpersoon

5. Optioneel: tekenen deelnemersovereenkomst (deze stap wordt enkel doorlopen als het een volledig nieuwe toetreder betreft)	
Input	Toestemming voor toetreding
Activiteit	1. De beheerorganisatie en de toetreder tekenen de deelnemersovereenkomst indien het ministerie van Economische Zaken toestemming heeft verleent voor de betreffende toetreding. 2. Na ondertekening van de deelnemersovereenkomst heeft de toetredende partij rechten en verplichtingen als deelnemer van het netwerk eHerkenning.
Output	Getekende deelnemersovereenkomst
Wie?	• Directie van de beheerorganisatie • Directie toetredende partij

6. Aansluiting realiseren	
Input	Getekende deelnemersovereenkomst of toestemming voor toetreding
Activiteit	• De toetredende partij geeft de metadata van het nieuwe productiesysteem door aan de beheerorganisatie. De beheerorganisatie verwerkt de metadata tot nieuwe metadata voor het netwerk en communiceert deze aan alle deelnemers. Nadat de deelnemers de nieuwe metadata hebben verwerkt is het nieuwe productiesysteem aangesloten op het netwerk. • Hierbij wordt het proces gevolgd zoals beschreven in Proces metadata. • De toetredende partij geeft informatie over de propositie door aan de beheerorganisatie. Dit wordt op de website van eHerkenning geplaatst.
Output	Aangesloten nieuwe deelnemer
Wie?	• Coördinator toetreden • Technisch beheerder • Vanuit de toetreder de aangestelde contactpersoon

Doorlooptijden proces toetreden

De doorlooptijden worden teruggerekend vanaf het moment van toetreding. De bij doorlooptijden genoemde mijlpalen zijn indicatief en er wordt geen rekening gehouden met extra doorlooptijd als gevolg van aanpassingen als gevolg van zaken die tijdens de gesprekken en/of testen naar voren komen. Indien gewenst zal de beheerorganisatie het proces pogen sneller te doorlopen. Hiervoor kunnen geen garanties worden afgegeven. In de tabellen wordt onder 'Toetreder' de partij die wil toetreden verstaan. 'BO' staat voor Beheerorganisatie eHerkenning.

Voor toetreden van een nieuwe partij

Activiteit	Door	Datum
Verzoek tot toetreding: inleveren toetredingsformulier bij beheerorganisatie	Toetreder	Datum x – 20 werkdagen
Toetreder komt met de externe auditor, de experts en de beheerorganisatie een datum overeen waarop de toetsing wordt gedaan	Toetreder	Datum x – 20 werkdagen
Toetreder levert metadata van de te testen acceptatiesystemen aan bij de beheerorganisatie en verstrekt (indien AD, of MR) geschikte authenticatiemiddelen en machtigingen.	Toetreder	Datum x – 20 werkdagen
Aanleveren documentatie aan externe auditor en experts en de beheerorganisatie: • Zelfverklaring • Procesbeschrijvingen (indien van toepassing)	Toetreder	Datum x – 15 werkdagen

Beoordelen opgeleverde documentatie	Externe auditor, experts	Datum x – 10 werkdagen
Toetredingsgesprek met toetreder over opgeleverde documentatie	Externe auditor, experts	Datum x – 7 werkdagen
Toetreder stuurt de beheerorganisatie de ingevulde toetredingstest checklist toe.	Toetreder	Datum x – 7 werkdagen
beheerorganisatie voert ketentest uit	Externe auditor	Datum x – 5 werkdagen
Advies verzenden aan EZ	beheerorganisatie	Datum x – 2 werkdagen
Toestemming toetreden doorEZ	EZ	Datum x
Tekenen deelnemersovereenkomst	BO en toetreder	Na datum x
Aansluiting realiseren	BO en toetreder	Na datum x

Proces uittreden

Voor geïnteresseerde partijen is er een toetredingsproces dat zij kunnen doorlopen indien zij deelnemer van eHerkenning willen worden. Uiteraard kunnen deelnemers ook uittreden. De deelnemer heeft na de uittreding geen rechten meer als deelnemer van eHerkenning. Dit betekent dat de betreffende partij het merk niet meer mag voeren en geen onderdeel meer is van het technische netwerk van eHerkenning.

1. Uittreding kan vrijwillig zijn, waarbij de deelnemer zelf aangeeft de deelnemersovereenkomst te willen beëindigen.
2. Uittreding kan ook onvrijwillig zijn. De beheerorganisatie wil dan de deelnemersovereenkomst beëindigen.

In dit document is het proces voor uittreden beschreven. Dit proces bestaat uit de juridische, technische en communicatieve stappen die moeten worden gezet voor een zorgvuldige uittreding.

Doelstelling

De doelstelling van het proces uittreding is dat een deelnemer op gestructureerde en verantwoorde wijze kan uittreden. Dit betekent:

- Zonder verstoringen
- Met minimale last voor de dienstverleners en eindgebruikers van de betreffende deelnemer

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De coördinator is ervoor verantwoordelijk dat de procesbeschrijving actueel blijft.

Uitgangspunten

Het proces uittreden gaat pas van start nadat er een besluit is genomen dat een deelnemer zal uittreden. Er zijn verschillende situaties die aanleiding kunnen geven tot uittreding. Grofweg zijn er twee soorten:

1. De deelnemer wil de overeenkomst beëindigen. Dit zal leiden tot ontbinding van de deelnemersovereenkomst. De schriftelijke opzegtermijn is volgens de deelnemersovereenkomst 2 maanden.
2. De beheerorganisatie wil de overeenkomst beëindigen. Onder bepaalde omstandigheden kan de deelnemersovereenkomst door de beheerorganisatie worden beëindigd. Zie artikel 5 van de Template

deelnemersovereenkomst en het Proces naleving.

Na het besluit tot uittreding start het proces uittreding. Dit proces is hetzelfde bij zowel vrijwillige als onvrijwillige uittreding.

Overzicht processtappen

- 1. Schriftelijke bevestiging beëindiging
- 2. Woord- en beeldmerk verwijderen
- 3. Technische uitsluiting netwerk

Processtappen uittreding

1. Schriftelijke bevestiging beëindiging	
Input	Besluit dat een deelnemer zal uittreden
Activiteit	1. In geval van vrijwillige uittreding zal de betreffende deelnemer dit melden bij de beheerorganisatie. Bij onvrijwillige uittreding zijn zowel de betreffende deelnemer als de beheerorganisatie al op de hoogte van het nalevingsbesluit. 2. De beheerorganisatie stuurt de betreffende deelnemer een formele schriftelijke bevestiging van het besluit tot beëindiging van de Deelnemersovereenkomst. Hiermee is de deelnemersovereenkomst formeel beëindigd.
Output	Een formele schriftelijke beëindiging van de deelnemersovereenkomst
Wie?	• Directie beheerorganisatie • Directie deelnemer

2. Woord- en beeldmerk verwijderen	
Input	Een formele schriftelijke beëindiging van de deelnemersovereenkomst
Activiteit	Er moet een aantal activiteiten worden uitgevoerd op het gebied van communicatie: 1. De betreffende deelnemer moet zijn contractpartijen (de eindgebruikers en aangesloten dienstverleners) binnen 24 uur informeren over de opzegging van de deelnemersovereenkomst. Deze activiteit moet terstond na het nemen van het besluit uitgevoerd worden. De contractpartijen moeten zoveel mogelijk tijd geboden krijgen om over te stappen naar een andere erkende deelnemer. 2. In overleg met de betreffende deelnemer informeert de beheerorganisatie de andere deelnemers en dienstverleners van eHerkenning over het beëindigen van de deelnemersovereenkomst met de betreffende deelnemer. 3. De betreffende deelnemer verwijdert alle verwijzingen naar eHerkenning van de eigen website (uitgezonderd oudere nieuwsberichten), inclusief het woord- en beeldmerk van eHerkenning. 4. De beheerorganisatie verwijdert alle verwijzingen naar de betreffende deelnemer van de eHerkenningswebsite (uitgezonderd oudere nieuwsberichten) en plaatst een nieuwsbericht over de beëindiging van de deelnemersovereenkomst op de eHerkenningswebsite. De betreffende deelnemer wordt tevens uit het aanmeldplatform verwijderd. 5. Indien nodig verloopt de communicatie met de pers via de persvoorlichting van EZ. 6. De beheerorganisatie informeert indien nodig externe nieuwswebsites.
Output	De betreffende deelnemer maakt geen gebruik meer van het merk eHerkenning
Wie?	• Communicatie afdeling beheerorganisatie • Communicatie afdeling deelnemer

3. Technische uitsluiting netwerk	
Input	De betreffende deelnemer maakt geen gebruik meer van het merk eHerkenning

Activiteit	Er moet een aantal technische activiteiten worden uitgevoerd: 1. De beheerorganisatie en de overige deelnemers voeren nieuwe metadata door volgens het proces zoals dat is vastgesteld in Proces metadata. Met het doorvoeren van de nieuwe metadata in het Onderhoudswindow, wordt de betreffende deelnemer technisch uit het netwerk gehaald. a. Wanneer dat noodzakelijk is kan de beheerorganisatie in overleg met de deelnemers de metadata per direct doorvoeren. Zodat uitsluiting uit het netwerk per direct geëffectueerd is. 2. De betreffende deelnemer draagt het archief inzake de dienstverlening van eHerkenning over aan de beheerorganisatie. Met behulp van een escrow service worden de archieven binnen twee maanden overgedragen aan de beheerorganisatie. Slechts wanneer er noodzaak toe is zal de beheerorganisatie het archief gebruiken. De deelnemer moet de volgende zaken aanleveren voor het archief: a. Alle loggingsbestanden in het kader van eHerkenning b. Het archief aangaande registratie van machtigingen voor eHerkenning c. De rapportage verplichtingen
Output	De betreffende deelnemer is geen onderdeel meer van het technische netwerk van eHerkenning
Wie?	• Technisch beheerder van de beheerorganisatie • Technisch beheerder van de deelnemer

Processtappen schorsing

Een resultaat van het handhavingsbeleid kan ook zijn dat een deelnemer wordt geschorst. Bij een schorsing wordt de deelnemer tijdelijk volledig afgesloten. In deze situatie worden alle stappen in het proces uittreding doorlopen zoals hierboven beschreven, met uitzondering van:

- Stap 1: schriftelijke bevestiging beëindiging. Bij een schorsing mag de deelnemer tijdelijk het merk niet meer voeren en geen onderdeel zijn van het netwerk. De deelnemersovereenkomst wordt echter niet direct ontbonden.
- Stap 3: de betreffende deelnemer hoeft geen archief te overleggen aan de beheerorganisatie. De nieuwe metadata wordt wel doorgevoerd, waardoor de geschorste deelnemer tijdelijk geen onderdeel meer is van het netwerk
- Stap 4: De beheerorganisatie krijgt van EZ de opdracht om de betreffende situatie te onderzoeken, om voorstellen te doen op welke wijze de deelnemer op korte termijn alsnog kan voldoen aan het afsprakenstelsel.
- Stap 5: Na ontvangst van de rapportage van de beheerorganisatie zal EZ een nieuw besluit nemen. Het besluit kan inhouden:
  - het opheffen van de schorsing (al dan niet onder voorwaarden),
  - het voortzetten van de schorsing (al dan niet met gewijzigde voorwaarden) of
  - overgaan tot de beëindiging van de deelnemersovereenkomst (uittreden).

Doorlooptijd proces uittreden

De hieronder genoemde termijnen zijn streeftermijnen. Indien een termijn niet kan worden gehaald, dan nemen de beheerorganisatie en de deelnemer/dienstverlener contact met elkaar op om een nieuwe termijn af te spreken. In de onderstaande tabel staat 'BO' voor beheerorganisatie.

Activiteit	Door	Tijd
Melding vrijwillige uittreding	Deelnemer	2 maanden voorafgaand aan moment van uittreding
Formele bevestiging van beëindiging deelnemersovereenkomst	BO	2 werkdagen na ontvangst
Informeren contractspartijen over uittreding	Deelnemer	Binnen 24 uur na besluit
Verwijderen beeldmerk eHerkenning van website	Deelnemer	2 werkdagen na stap 3
Plaatsen nieuwsbericht over uittreding op eHerkenningswebsite	BO	2 werkdagen na stap 3
Doorvoeren nieuwe metadata	BO en deelnemers	2 werkdagen na stap 3 proces starten
Overdracht archief	Deelnemer	2 maanden na stap 3

Proces wijziging rechtspersoon

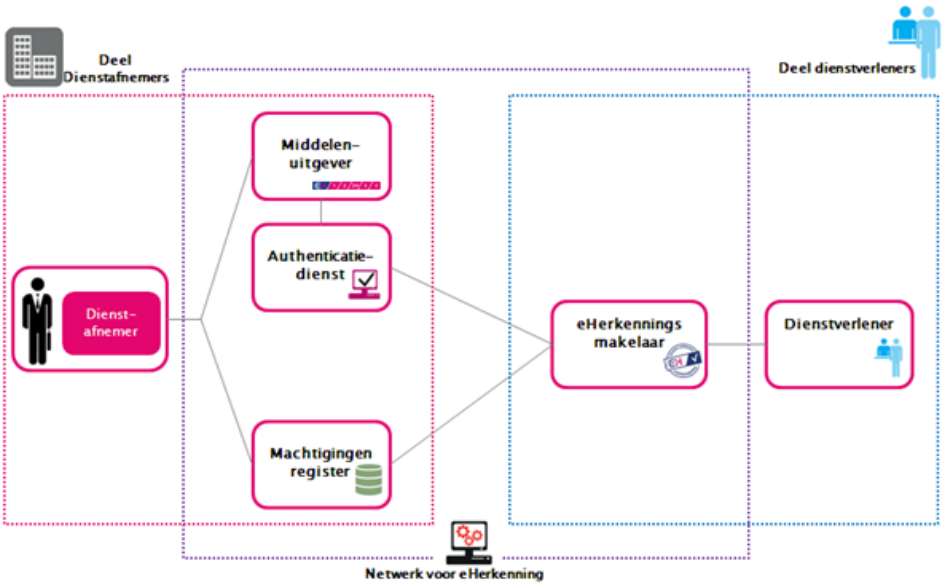
Wanneer een deelnemer de rechtspersoon wil wijzigen, maakt hij dit kenbaar aan de beheerorganisatie door middel van het formulier Template wijziging rechtspersoon deelnemer.

De deelnemer retourneert het ingevulde formulier en met bijbehorende bijlagen naar info@eherkenning.nl.

Businessmodel

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Dit document beschrijft het businessmodel voor eHerkenning. Onder het businessmodel worden verstaan de afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen die samen het netwerk voor eHerkenning invullen. Het is bedoeld voor deelnemers en dienstverleners.



Het businessmodel gaat uit van de volgende afspraken:

- De kosten voor verplichte functionaliteit worden gedeeld tussen de twee primaire doelgroepen van het netwerk voor eHerkenning: bedrijven en dienstverleners. De dienstverlener betaalt voor de dienstverlening van de eHerkenningsmakelaar, terwijl de bedrijven betalen voor de dienstverlening door de authenticatiedienst (incl. authenticatiemiddel) en het machtigingenregister.
- Deelnemers kunnen onderling afspraken maken met betrekking tot de volgende zaken:
  - Onderlinge verrekeningen.
  - Tariefstructuren.
- Onderlinge afspraken moeten altijd voldoen aan de mededingingswetten (Nma als toezichthouder).
- Tegemoetkoming in de kosten. Een voorbeeld: In de opstartfase kunnen bedrijven in de aanloop naar volwassenheid van het netwerk een tegemoetkoming krijgen vanuit de overheid voor het (stimuleren van het) gebruik van het netwerk.

Handboek huisstijl

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Dit document beschrijft de huisstijl afspraken en afspraken over marketingcommunicatie die deelnemers hebben gemaakt. Het is bedoeld voor deelnemers en dienstverleners.

De marketingcommunicatie is een onderdeel van het instrumentarium dat wordt ingezet om het merk eHerkenning te beheren. Het is van essentieel belang dat het nut, de noodzaak en de voordelen van eHerkenning op een goede wijze worden gecommuniceerd.

Succesvolle marketingcommunicatie vraagt om een duidelijke (door alle betrokken partijen geaccepteerde) marketing-communicatiestrategie, voor wat betreft boodschap, faciliteiten en publiciteit. Dit onderdeel van het afsprakenstelsel geeft de deelnemers en dienstverleners kaders voor de marketingcommunicatie over eHerkenning. De beheerorganisatie levert richtlijnen, standaard tekst- en beeldmateriaal en andere promotietools die de deelnemers en dienstverleners dienen te gebruiken.

Onderdelen van de marketingcommunicatie zijn:

1. Doel, kernboodschap en uitgangspunten
2. Richtlijnen m.b.t. publiciteit
3. De promokit en de onderdelen waaruit deze wordt samengesteld

Als bijlage is toegevoegd een document met zijn eigen opmaak dat de regels en richtlijnen voor de visuele identiteit van eHerkenning beschrijft.

Doel, kernboodschap en uitgangspunten

Het doel van de marketingcommunicatie is om potentiële afnemers van eHerkenning te overtuigen dat zij te maken hebben met een gebruiksvriendelijk en betrouwbaar product.

Daarbij zijn de volgende kernwaarden bepalend voor de basis van de brand-identity:

- Efficiënt (gemak, gebruiksvriendelijk, overzichtelijk)
- Veiligheidsgevoel (betrouwbaar)
- Netwerk (samenwerking)
- Innovatief (technisch en procedureel hoogstandje)
- Officieel (professioneel, van de overheid, serieus gevoel, zitten belangrijke bedrijven achter)

Deze waarden worden verbeeld door de beeldelementen (logo, typografie, icoon) en uitgedragen in alle teksten en uitingen (pay off, standaardteksten, website, artikelen e.d.).

Kernboodschap aan doelgroepen

De boodschap aan potentiële gebruikers - overheidsorganisaties is dat zij hun elektronische diensten voor bedrijven eenvoudig toegankelijk kunnen maken door eHerkenning af te nemen van een daartoe gecertificeerde eHerkenningsmakelaar van hun keuze. Het gehele authenticatieproces is daarmee uitbesteed aan een betrouwbaar netwerk. De overheidsorganisatie kan er zeker van zijn dat ze zaken doen met diegene die daartoe namens het bedrijf is geautoriseerd.

De kernboodschap aan overheidsorganisaties: Met eHerkenning kunt u op een efficiënte en betrouwbare manier aan bedrijven toegang verlenen tot uw elektronische diensten.

De boodschap aan potentiële gebruikers - bedrijven is dat zij zichzelf bij willekeurige overheidsorganisatie digitaal en gebruiksvriendelijk kunnen aanmelden, door (mochten zij het al niet reeds in bezit hebben) een eHerkenningsmiddel af te nemen van een daartoe gecertificeerde aanbieder van hun keuze. Het gehele authenticatieproces - en netwerk dat achter eHerkenning zit, is betrouwbaar.

De kernboodschap aan bedrijven: Met eHerkenning kunt u op eenvoudig en betrouwbaar zaken doen en gegevens uitwisselen

met de overheid.

Het is van belang dat de deelnemers uitgaan van deze boodschap om het effect van de communicatie te vergroten en het risico van verwarring en onduidelijkheid bij de ontvangers te minimaliseren.

Uitgangspunten

Naast de eerder genoemde kernboodschap, gelden ook de volgende uitgangspunten:

- Herhaling: Het gebruiksgemak dat en de betrouwbaarheid die eHerkenning biedt steeds weer voor het voetlicht brengen.
- Segmentering: doelgroepgerichte en gesegmenteerde communicatie.
- Eenduidig en uniform gebruik van benamingen en schrijfwijzen in alle communicatie-uitingen. Daartoe is onder meer een begrippenlijst beschikbaar gesteld. Deze begrippenlijst is opgenomen in het communicatiehandboek dat onderdeel is van de promokit (deze is gebaseerd op de begrippenlijst in het afsprakenstelsel).
- Ten behoeve van de professionele uitstraling en lading van het merk eHerkenning is een merkstrategie en vertaling naar merkdesign ontwikkeld. De hieruit voorkomende merkelementen (logo, steunkleuren, typografie, beeldentaal) zijn beschikbaar voor de deelnemers en dienstverleners via de promokit op de website www.eherkenning.nl .
- Communicatie- en voorlichtingsmateriaal (standaardteksten, beeldelementen, begrippenlijst e.d.) wordt zoveel mogelijk digitaal beschikbaar gesteld aan overheidsdienstverleners en deelnemers, vanwege het kostenaspect, de actualiteit, endorsement-toepassingen voor deelnemers en multi-toepasbaarheid binnen de eigen 'look and feel' en huisstijl van (overheids)organisaties. De promokit op de website www.eherkenning.nl is hiervoor ingericht.
- Voor zover de beheerorganisatie zelf communiceert, informeert zij hierover via de reguliere contactmomenten.
- Er wordt gestreefd naar maximaal hergebruik van standaardteksten en reeds ontwikkelde middelen (met daarbij oog voor doelgroepsegmentering).
- De website www.eherkenning.nl wordt ingezet als hoofdmedium en het centrale informatiepunt. De beheerorganisatie beheert de website. Op de website wordt een overzicht gegeven van alle deelnemers voor de diverse rollen, inclusief het aanbod van aanvullende features per deelnemer. Tevens wordt een link naar de website van elke deelnemer opgenomen.

Richtlijnen publiciteit

Wat betreft marketingcommunicatie ZOUDEN deelnemers en dienstverleners zich MOETEN houden aan de volgende richtlijnen:

- Ten behoeve van de eenduidigheid maken deelnemers, beheerorganisatie en dienstverleners gebruik van dezelfde beeldelementen en logo's (zoals gefaciliteerd in de promokit op de website) en passen zij dezelfde schrijfwijze en terminologie toe (zoals beschreven in het begrippenlijst van het afsprakenstelsel, onderdeel Algemene Introductie).
  - Het gebruik van het logo 'erkende aanbieder' is voorbehouden aan partijen die erkende aanbieder zijn binnen eHerkenning. Andere partijen mogen dit logo niet voeren, ook niet voor verwijzingen.
  - Het logo eHerkenning moet in de volgende situaties worden geplaatst:
    - Het logo eHerkenning moet worden geplaatst op webpagina's waar de gebruiker moet inloggen met een eHerkenningsmiddel op een portal.
    - Het logo eHerkenning moet worden geplaatst op webpagina's waarop meerdere formulieren of diensten 'met eHerkenning' worden aangeboden.

      > Het logo eHerkenning hoeft dan niet per formulier worden getoond.

    - Het logo eHerkenning hoeft niet te worden geplaatst op webpagina's waarop formulieren of diensten zowel met eHerkenning of DigiD worden aangeboden. Het logo eHerkenning hoeft dan niet per formulier/dienst te worden getoond.

      > Indien er een DigiD logo wordt getoond op de pagina of per formulier/dienst, dan moet er wel een logo eHerkenning worden geplaatst

- Deelnemers kunnen richting dienstverleners eHerkenning aanbieden en sales-activiteiten ontplooien.
- Deelnemers kunnen richting bedrijven/gebruikers eHerkenning aanbieden en sales-activiteiten ontplooien.
- Bij alle algemene, structurele uitingen over eHerkenning, van alle deelnemers, dienstverleners en de beheerorganisatie, wordt het logo of het beeldicoon van eHerkenning geplaatst/getoond. Bij incidentele uitingen, zoals nieuwsberichten, is dit niet noodzakelijk.
- Publiciteit door deelnemers zal erop gericht zijn zichzelf als deelnemer te positioneren binnen eHerkenning. Er dient altijd te worden gerefereerd aan het eHerkenningsnetwerk en de deelnemer dient zich te positioneren als 'onderdeel' van dat netwerk.

Eisen met betrekking tot de communicatie-uitingen op dialoogvensters tijdens het herkenningsproces worden beschreven in het

onderdeel Use cases.

Promokit

De beheerorganisatie verzorgt een aantal elementen die ter beschikking wordt gesteld via een promokit. De deelnemers en dienstverleners horen voor hun marketingcommunicatie gebruik te maken van de elementen en richtlijnen zoals voorzien in de promokit. Deze promokit wordt via het www.eherkenning.nl beschikbaar gesteld voor deelnemers en dienstverleners. De promokit bestaat uit de volgende onderdelen:

Communicatiehandboek

Hierin staat een draaiboek met communicatie-acties voor communicatiemedewerkers en standaardteksten voor de communicatie (zie hieronder).
Standaardteksten:

- Algemene informatie over eHerkenning (ook beschikbaar in de vorm van factsheets)
- Oproep om mee te doen aan de implementatie op website of in nieuwsbrief
- Voordelen eHerkenning
- Flyertekst eHerkenning voor afnemers/bedrijven

Manual en typografie

- Huisstijlhandboek: bevat regels en richtlijnen met betrekking tot visuele identiteit van eHerkenning
- Typografie (fonts)

Beeldelementen

- Vignetten voor betrouwbaarheidsniveaus
- Logo
- Logo met pay off, icoon en banner
- Stijlelementen

Regels en richtlijnen voor de visuele identiteit eHerkenning

Zie voor de regels en richtlijnen rondom het gebruik van het eHerkenningslogo en andere onderdelen van de visuele identiteit van eHerkenning het document Regels en richtlijnen van de visuele identiteit eHerkenning die als bijlage aan dit document is toegevoegd.

Regels en richtlijnen voor dienstverleners

Dienstverleners MOETEN zich in hun communicatieuitingen houden aan de regels en richtlijnen rondom het gebruik van het eHerkenningslogo en andere onderdelen van de visuele identiteit van eHerkenning. Deze zijn te vinden in het document Regels en richtlijnen van de visuele identiteit eHerkenning die als bijlage aan dit document is toegevoegd.

Dienstverleners ZOUDEN voor hun marketing-communicatie gebruik MOETEN maken van de elementen en richtlijnen zoals voorzien in de promokit. De promokit of delen daarvan MOGEN door de eHerkenningsmakelaar voor dit doel ter beschikking worden gesteld aan dienstverleners.

De eHerkenningsmakelaar MOET ervoor zorgdragen dat de beheerorganisatie eHerkenning beschikt over actuele contactgegevens van nieuwe en bestaande dienstverleners. De beheerorganisatie MOET deze contactgegevens gebruiken om dienstverleners het gebruiksrecht te geven voor het eHerkenningslogo. De beheerorganisatie MAG deze contactgegevens gebruiken om dienstverleners aan te spreken op onjuist gebruik van het eHerkenningslogo en andere onderdelen van de visuele identiteit. De beheerorganisatie eHerkenning MAG de contactgegevens NIET voor andere doeleinden gebruiken.

Bijlage - Regels en richtlijnen van de visuele identiteit eHerkenning

Service level

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Dit document beschrijft de service level afspraken die deelnemers hebben gemaakt die beschrijven welk service level ten minste aan hun klanten wordt bieden. Het is bedoeld voor deelnemers en dienstverleners.

Leeswijzer

- Service level definities — In dit document worden de volgende aanvullende definities gehanteerd.
  - Calamiteit — Een ongeplande situatie waarbij ten minste twee deelnemers zijn betrokken en waarvan verwacht wordt dat de duur van het niet beschikbaar zijn de maximale verstoringstijd van vier uur zal overschrijden. Veelal zullen aanzienlijke -niet vooraf te plannen- maatregelen moeten worden getroffen om de calamiteit te herstellen.
  - Gegarandeerde openstellingsduur — De periode tussen 7.00 en 24.00. Hier zijn hoge beschikbaarheidseisen van toepassing.
  - Onderhoudswindow — Het onderhoudswindow valt in de periode buiten de Gegarandeerde openstellingsduur in de nacht van zaterdag op zondag. Onderhoud vindt bij voorkeur plaats in deze periode.
  - Rapportageperiode — Een rapportageperiode loopt van de eerste dag van een kalendermaand 4:00 uur tot de eerste dag van de volgende kalendermaand 4:00 uur.
  - Verstoring — Elke gebeurtenis afwijkend van de (verwachte) standaardwerking van een systeem of dienst. Hiertoe wordt niet gerekend tijdelijke verminderde beschikbaarheid wanneer dit geen effecten voor derden heeft.
  - Werkdag — Een dag, niet zijnde een zaterdag of een zondag en niet zijnde een algemeen erkende feestdag als bedoeld in artikel 3, eerste lid, van de Algemene Termijnenwet, noch een in het tweede of krachtens het derde lid van genoemd artikel met een algemeen erkende feestdag gelijkgestelde dag.
- Beschrijving service level — Deelnemers MOETEN minimaal het beschreven Service Level leveren aan elkaar en hun gebruikers (dienstverleners, dienstafnemers, intermediaire partijen en uitvoerend natuurlijke personen).
  - Communicatie over onderhoud — Ten behoeve van het communiceren over onderhoud MOET de beheerorganisatie ruimte reserveren op de issuetracker snippet.issues. Alle deelnemers MOETEN hiertoe toegang krijgen. Ten behoeve van de uitwisseling van ervaringen rondom het Service level van het netwerk MOET de beheerorganisatie een maandelijks Operationeel Overleg (gremium) organiseren waarin de deelnemers vertegenwoordigd zijn.
  - Beschikbaarheid — Alle diensten MOETEN binnen de Gegarandeerde openstellingsduur voor 99,2% (gemeten per kalendermaand) gegarandeerd en volledig beschikbaar zijn. Hieronder worden ook verstaan de elektronische processen voor het intrekken van middelen en machtigingen.
  - Performance — Eisen rondom performance richten zich op de gebruikersbeleving.
  - Onderhoud — Elke partij MOET voor het uitvoeren van onderhoud toestemming krijgen van de beheerorganisatie. In overleg met de beheerorganisatie wordt dan het tijdstip waarop het onderhoud wordt uitgevoerd vastgesteld.
  - Ondersteuning — Deelnemers MOETEN beschikbaar zijn voor ondersteuning aan hun gebruikers en de beheerorganisatie op werkdagen tussen 9.00 en 16.30.
  - Logging — Een deelnemer MOET eerstelijns vragen o.b.v. logging (zie Eisen ten aanzien van archivering en opvraging) binnen 3 werkdagen beantwoorden.
  - Verplichtingen bij verstoringen — Elke deelnemer MOET verstoringen z.s.m. zowel in de issuetracker snippet.issues als telefonisch melden bij de incidentmanager van de beheerorganisatie.
  - Verplichtingen bij calamiteiten — Elke deelnemer MOET calamiteiten z.s.m. zowel in de issuetracker snippet.issues als telefonisch melden bij de incidentmanager van de beheerorganisatie.
  - Rapportages — Elke deelnemer MOET uiterlijk de 15e van elke kalendermaand de rapportage over de voorafgaande rapportageperiode aan de beheerorganisatie opleveren.

- Controle op service level — De controle op het Service Level zal door de beheerorganisatie worden uitgevoerd. Zij doet dit in de eerste plaats door het analyseren van de door deelnemers opgeleverde rapportages, maar ook het uitvoeren van steekproeven behoort tot de mogelijkheden. In geval van klachten van een gebruiker/bedrijf, overheidsdienstverlener of deelnemer kan een onderzoek worden ingesteld en kunnen eventueel Sancties aan de deelnemer worden opgelegd. In Proces naleving is het proces om te komen tot sancties besch

Service level definities

In dit document worden de volgende aanvullende definities gehanteerd.

- Calamiteit — Een ongeplande situatie waarbij ten minste twee deelnemers zijn betrokken en waarvan verwacht wordt dat de duur van het niet beschikbaar zijn de maximale verstoringstijd van vier uur zal overschrijden. Veelal zullen aanzienlijke -niet vooraf te plannen- maatregelen moeten worden getroffen om de calamiteit te herstellen.
- Gegarandeerde openstellingsduur — De periode tussen 7.00 en 24.00. Hier zijn hoge beschikbaarheidseisen van toepassing.
- Onderhoudswindow — Het onderhoudswindow valt in de periode buiten de Gegarandeerde openstellingsduur in de nacht van zaterdag op zondag. Onderhoud vindt bij voorkeur plaats in deze periode.
- Rapportageperiode — Een rapportageperiode loopt van de eerste dag van een kalendermaand 4:00 uur tot de eerste dag van de volgende kalendermaand 4:00 uur.
- Verstoring — Elke gebeurtenis afwijkend van de (verwachte) standaardwerking van een systeem of dienst. Hiertoe wordt niet gerekend tijdelijke verminderde beschikbaarheid wanneer dit geen effecten voor derden heeft.
- Werkdag — Een dag, niet zijnde een zaterdag of een zondag en niet zijnde een algemeen erkende feestdag als bedoeld in artikel 3, eerste lid, van de Algemene Termijnenwet, noch een in het tweede of krachtens het derde lid van genoemd artikel met een algemeen erkende feestdag gelijkgestelde dag.

Calamiteit

Een ongeplande situatie waarbij ten minste twee deelnemers zijn betrokken en waarvan verwacht wordt dat de duur van het niet beschikbaar zijn de maximale verstoringstijd van vier uur zal overschrijden. Veelal zullen aanzienlijke -niet vooraf te plannen- maatregelen moeten worden getroffen om de calamiteit te herstellen.

Gegarandeerde openstellingsduur

De periode tussen 7.00 en 24.00. Hier zijn hoge beschikbaarheidseisen van toepassing.

Onderhoudswindow

Het onderhoudswindow valt in de periode buiten de Gegarandeerde openstellingsduur in de nacht van zaterdag op zondag. Onderhoud vindt bij voorkeur plaats in deze periode.

Rapportageperiode

Een rapportageperiode loopt van de eerste dag van een kalendermaand 4:00 uur tot de eerste dag van de volgende kalendermaand 4:00 uur.

Verstoring

Elke gebeurtenis afwijkend van de (verwachte) standaardwerking van een systeem of dienst. Hiertoe wordt niet gerekend tijdelijke verminderde beschikbaarheid wanneer dit geen effecten voor derden heeft.

Werkdag

Een dag, niet zijnde een zaterdag of een zondag en niet zijnde een algemeen erkende feestdag als bedoeld in artikel 3, eerste lid, van de Algemene Termijnenwet, noch een in het tweede of krachtens het derde lid van genoemd artikel met een algemeen erkende feestdag gelijkgestelde dag.

Beschrijving service level

Deelnemers MOETEN minimaal het beschreven Service Level leveren aan elkaar en hun gebruikers (dienstverleners, dienstafnemers, intermediaire partijen en uitvoerend natuurlijke personen).

N.B. Gebruikers van het afsprakenstelsel MOGEN aanvullende Service Level eisen stellen. Deze eisen MOGEN NIET betrekking hebben zaken die niet door de betreffende deelnemer zelf te realiseren zijn zonder dat daar de betrokkenheid van andere deelnemers nodig is.

Communicatie over onderhoud

Ten behoeve van het communiceren over onderhoud MOET de beheerorganisatie ruimte reserveren op de issuetracker Mantis. Alle deelnemers MOETEN hiertoe toegang krijgen. Ten behoeve van de uitwisseling van ervaringen rondom het Service level van het netwerk MOET de beheerorganisatie een maandelijks Operationeel Overleg (gremium) organiseren waarin de deelnemers vertegenwoordigd zijn.

Ten behoeve van effectieve onderlinge communicatie is het noodzakelijk dat deelnemers elkaar op verschillende niveaus kunnen vinden. Hiertoe MOET elke deelnemer de contactgegevens van de volgende contactpersonen binnen de organisatie kenbaar maken aan de beheerorganisatie:

1. Contactgegevens directieniveau
2. Contactgegevens service management / projectleider
3. Contactgegevens service desk

Beschikbaarheid

Alle diensten MOETEN binnen de Gegarandeerde openstellingsduur voor 99,2% (gemeten per kalendermaand) gegarandeerd en volledig beschikbaar zijn. Hieronder worden ook verstaan de elektronische processen voor het intrekken van middelen en machtigingen.

Buiten de gegarandeerde openstellingsduur (tussen 0.00 en 7.00) ZOUDEN de diensten in beginsel wel volledig beschikbaar MOETEN zijn, maar hiervoor worden geen garanties afgegeven.

Performance

Eisen rondom performance richten zich op de gebruikersbeleving.

Performance wordt beschreven in termen van de tijd die een gebruiker moet wachten voordat het volgende scherm geladen is.

- 95% van de schermen MOET binnen 2 seconden worden getoond.
- 99% van de schermen MOET binnen 5 seconden worden getoond.
- Elke dienst deelnemer MOET ten minste 100 gelijktijdige berichten kunnen verwerken terwijl nog wordt voldaan aan de performance eisen.

Onderhoud

Elke partij MOET voor het uitvoeren van onderhoud toestemming krijgen van de beheerorganisatie. In overleg met de beheerorganisatie wordt dan het tijdstip waarop het onderhoud wordt uitgevoerd vastgesteld.

Planbaar onderhoud MOET worden gepland in het Onderhoudswindow en MOET minimaal 10 werkdagen van tevoren bij de

beheerorganisatie worden aangekondigd.

Incidenteel onderhoud ZOU minimaal 3 dagen van te voren bij de beheerorganisatie MOETEN worden aangekondigd.

Een ketentest (bijvoorbeeld in geval van een nieuwe implementatie of nieuwe toetreding) ZOU minimaal 10 werkdagen van tevoren bij de beheerorganisatie MOETEN worden aangekondigd. Indien toetreder dit verzuimt, kan deze geen aanspraak maken op reactietijden zoals vermeld in Logging.

In geval van wijzigingen in de onderhoudsplanning MOET de beheerorganisatie alle abonnees van de mailinglist binnen één werkdag van de inhoud van deze wijziging op de hoogte brengen.

Ondersteuning

Deelnemers MOETEN beschikbaar zijn voor ondersteuning aan hun gebruikers en de beheerorganisatie op werkdagen tussen 9.00 en 16.30.

De beheerorganisatie MOET beschikbaar zijn voor ondersteuning aan deelnemers op werkdagen tussen 9.00 en 17.00.

Logging

- Een deelnemer MOET eerstelijns vragen o.b.v. logging (zie Eisen ten aanzien van archivering en opvraging) binnen 3 werkdagen beantwoorden.
- Een deelnemer MOET tweedelijns vragen o.b.v. logging (zie Eisen ten aanzien van archivering en opvraging) binnen 10 werkdagen beantwoorden.

Verplichtingen bij verstoringen

Elke deelnemer MOET verstoringen z.s.m. zowel in de issuetracker Mantis als telefonisch melden bij de incidentmanager van de beheerorganisatie.

De beheerorganisatie MAG een gemelde verstoring aanmerken als calamiteit.

Een deelnemer MOET elke storing binnen 4 uur verhelpen.

Gedurende verstoringen MOET de beheerorganisatie minimaal elke vier uur de betrokken partijen op de hoogte stellen van de status.

Verplichtingen bij calamiteiten

Elke deelnemer MOET calamiteiten z.s.m. zowel in de issuetracker Mantis als telefonisch melden bij de incidentmanager van de beheerorganisatie.

De beheerorganisatie MAG een gemelde calamiteit aanmerken als verstoring.

Voor het geval van calamiteiten MOET elke deelnemer 24x7 een contactpersoon beschikbaar hebben. De deelnemer MOET de contactgegevens van deze persoon aan de beheerorganisatie bekend maken.

In geval van calamiteiten MOET de beheerorganisatie zo snel mogelijk, maar in elk geval binnen 24 uur, een (telefonische) bijeenkomst beleggen waarbij alle benodigde contactpersonen aanwezig MOETEN zijn.

Gedurende calamiteiten MOET de beheerorganisatie minimaal elke vier uur de betrokken partijen op de hoogte stellen van de status.

Rapportages

Elke deelnemer MOET uiterlijk de 15e van elke kalendermaand de rapportage over de voorafgaande rapportageperiode aan de beheerorganisatie opleveren.

Hiertoe MOET de deelnemer de door de beheerorganisatie beschikbaar rapportagetool gebruiken.

De eHerkenningsmakelaars MOETEN de volgende gegevens rapporteren:

- Nieuw, afgesloten en totaal aantal aangesloten dienstverleners

De middelenuitgevers MOETEN de volgende gegevens rapporteren:

- Nieuw, afgesloten en totaal aantal uitgegeven middelen

De machtigingenregisters MOETEN de volgende gegevens rapporteren:

- Het totaal aantal geregistreerde bedrijven

Tevens MOETEN alle deelnemers de volgende gegevens rapporteren:

- Aantal berichten per type bericht (gedifferentieerd naar deelnemer). Hierbij MOETEN de monitoring berichten worden uitgefilterd.

De beheerorganisatie MOET alle gerapporteerde informatie zo snel mogelijk delen met alle deelnemers en overheidsdienstverleners. Alle informatie wordt hierbij geaggregeerd zodat concurrentiegevoelige informatie zoveel mogelijk verborgen blijft.

Controle op service level

De controle op het Service Level zal door de beheerorganisatie worden uitgevoerd. Zij doet dit in de eerste plaats door het analyseren van de door deelnemers opgeleverde rapportages, maar ook het uitvoeren van steekproeven behoort tot de mogelijkheden. In geval van klachten van een gebruiker/bedrijf, overheidsdienstverlener of deelnemer kan een onderzoek worden ingesteld en kunnen eventueel Sancties aan de deelnemer worden opgelegd. In Proces naleving is het proces om te komen tot sancties beschreven.

Techniek en functionaliteit

Hier vindt u de technische documenten van het Afsprakenstelsel eHerkenning: de koppelvlakspecificaties, de use cases, testen voor dienstverleners en testen voor deelnemers. Deze documenten bevatten informatie over welke standaarden worden gehanteerd, de functionaliteit, de berichten en koppelvlakken die eHerkenning ondersteunt en de testen die worden uitgevoerd.

Deze categorie bevat de volgende onderdelen:

- Use cases — Beschrijft de functionaliteit van eHerkenning in detail.
- Interface specifications — This section describes the interface specifications for the traffic between all roles in the network. The messages are based on SAML 2.0, or XACML where applicable.
- Attribuutverstrekking — Een dienstverlener of een herkenningsmakelaar kan in een authenticatieverzoek ook een verzoek om attributen doen. De AD, MR of HM kan als attribuutverstrekker optreden. Zij mogen alleen attributen aanbieden die in dit document beschreven worden.
- Testing — This document describes the tests that (aspiring) participants must perform.

Use cases

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Beschrijft de functionaliteit van eHerkenning in detail.

Leeswijzer

- Use cases voor Gebruik
  - GUC1 Gebruiken eHerkenning als dienstafnemer — GUC1: Gebruiken eHerkenning als dienstafnemer - In deze use case wordt de identiteit van de dienstafnemer vastgesteld. De eHerkenningsmakelaar geeft hierover een verklaring af aan de dienstverlener. De uitvoerende natuurlijk persoon voert hiertoe de GUC3 Aantonen identiteit uit.
    - GUC1.2 Er wordt “met vertegenwoordiging” gespecificeerd
  - GUC2 Gebruiken eHerkenning als vertegenwoordiger — In deze use case, die een uitbreiding is op GUC1 Gebruiken eHerkenning als dienstafnemer, wordt de identiteit van de vertegenwoordigde dienstafnemer, de pseudo-identiteit van de uitvoerende natuurlijk persoon en de vertegenwoordigingsbevoegdheid van de uitvoerende natuurlijk persoon namens deze vertegenwoordigde dienstafnemer vastgesteld. De eHerkenningsmakelaar geeft een nieuwe verklaring af aan de dienstverlener. Deze verklaring is samengesteld uit de verklaringen van de authenticatiedienst en
  - GUC3 Aantonen identiteit — GUC3: Aantonen identiteit - In deze use case kiest de uitvoerende natuurlijk persoon een authenticatiedienst en identificeert zich bij die authenticatiedienst door het gebruik van een authenticatiemiddel, dat hij eerder heeft verkregen (zie Use cases voor Administratie). De authenticatiedienst authentiseert de uitvoerende natuurlijk persoon en geeft hierover een verklaring af aan de eHerkenningsmakelaar.
    - GUC3.3 Authenticatie uitvoerende natuurlijk persoon mislukt
  - GUC4 Aantonen bevoegdheid — In deze use case kiest de uitvoerende natuurlijk persoon een machtigingenregister en raadpleegt de uitvoerende natuurlijk persoon dat machtigingenregister. Het machtigingenregister stelt op basis van de eerder met GUC3 Aantonen identiteit verkregen identiteit van de uitvoerende natuurlijk persoon en een eerder geregistreerde bevoegdheid (zie Use cases voor Administratie), de identiteit van de vertegenwoordigde dienstafnemer en de pseudo-identiteit van de uitvoerende natuurlijk persoon vast en ge
    - GUC4.1 Te bevragen machtigingenregister reeds bekend
    - GUC4.2 Authenticatie voor dienst 0
    - GUC4.2 Ketenmachtiging
      - Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet (stap 4.4c alternatief)
      - Vertegenwoordigde dienstafnemer onbekend (stap 4.4 alternatief)
    - GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet
    - GUC4.2 Verschillende bevoegdheden aanwezig
  - Aanvullende eisen eHerkenningsmakelaar
  - Aanvullende eisen authenticatiedienst
  - Aanvullende eisen authenticatiedienst die SSO ondersteunt
  - Aanvullende eisen machtigingenregister
  - Aanvullende eisen machtigingenregister dat ketenmachtigingen ondersteunt
  - Use case overschrijdende alternatieve scenario's
    - Alternatief scenario attribuutverstrekking
    - Attributen niet leverbaar of niet toegestaan
    - Attribuut komt niet voor in attribuutcatalogus
    - Dienst of dienstverlener komt niet voor in dienstencatalogus
    - Soort dienstafnemer kan niet worden geleverd
    - Uitvoerende natuurlijk persoon annuleert
    - Use cases Single Sign-On
      - Geen reactie bij lezen of schrijven selectie authenticatiedienst
      - Single Log-out
- Use cases voor Administratie

- AUC1 Aansluiten dienst
- AUC2 Verkrijgen authenticatiemiddel
- AUC3 Registreren bevoegdheid
- AUC4 Registreren attribuut
- AUC5 Registreren identificerend kenmerk beroepsbeoefenaar

- Gebruikersinterface
  - Dialoogbeschrijving
  - Aanvullende eisen aan eHerkenningsmakelaarschermen
  - Toegankelijkheid

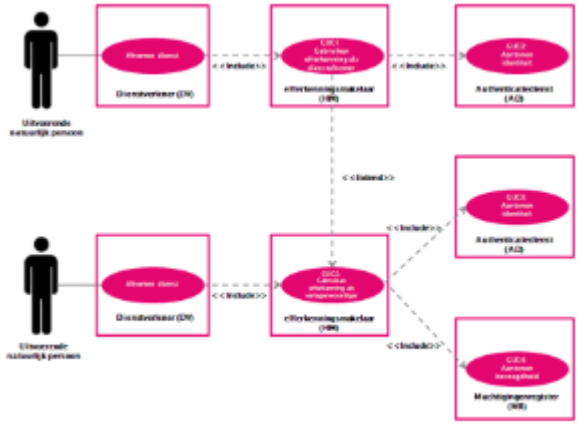
Use cases voor Gebruik

Afnemen dienst	Afnemen dienst met gebruik van eHerkenning

Het gebruik van eHerkenning is geen doel op zich. eHerkenning wordt gebruikt als bouwsteen in een business use case waarin de business actor dienstafnemer een dienst (de term "dienst" wordt hier in de breedst mogelijke zin gebruikt. Onder "dienst" worden o.a. verstaan: het verkrijgen van informatie, het indienen van een aanvraag, het aanmelden voor een nieuwsbrief, of het inloggen op een loket of portaal) afneemt van een business actor dienstverlener.

Pas wanneer binnen deze dienst behoefte bestaat aan de herkenning van de dienstafnemer speelt eHerkenning een rol.

Use case diagram Gebruik



Het use case diagram "Gebruik", hierboven, beschrijft de twee hoofd use cases waarin de herkenning van de dienstafnemer zelf, of de herkenning van een vertegenwoordiger van de dienstafnemer binnen eHerkenning wordt geïmplementeerd en de twee sub use cases die daar een rol bij spelen.

- Afnemen dienst – In deze use case neemt de natuurlijk persoon een dienst af bij een dienstverlener. De inhoud van deze dienst wordt hier verder niet besproken. Ergens in het proces is echter behoefte aan de authenticatie van de dienstafnemer, waartoe de dienstverlener de uitvoerende natuurlijk persoon de use case "Gebruiken eHerkenning", GUC1 "Gebruiken eHerkenning als dienstafnemer" of GUC2 "Gebruiken eHerkenning als vertegenwoordiger", laat uitvoeren.

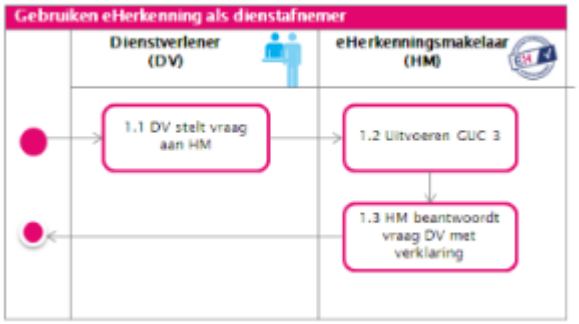
In dit hoofdstuk worden de "Gebruik" use cases in detail uitgewerkt. Voor acties waar berichten worden uitgewisseld wordt verwezen naar de betreffende bericht- en koppelvlakspecificaties.

Per use case worden verschillende alternatieve scenario's beschreven. Use case overschrijdende alternatieve scenario's worden integraal in Use case overschrijdende alternatieve scenario's beschreven. In een alternatief scenario wordt aanvullende functionaliteit, functionaliteit als gevolg van een keuze van de uitvoerende natuurlijke persoon of functionaliteit als gevolg van een uitzondering (fout) beschreven.

GUC1 Gebruiken eHerkenning als dienstafnemer

GUC1: Gebruiken eHerkenning als dienstafnemer – In deze use case wordt de identiteit van de dienstafnemer vastgesteld. De eHerkenningsmakelaar geeft hierover een verklaring af aan de dienstverlener. De uitvoerende natuurlijk persoon voert hiertoe de GUC3 Aantonen identiteit uit.

De use cases GUC1 "Gebruiken eHerkenning als dienstafnemer" wordt hieronder in een activity diagram weergegeven.



De verschillende acties voor use case GUC1 worden hier in meer detail beschreven. Voor de acties in use case GUC3 wordt verwezen naar GUC3 Aantonen identiteit.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstafnemer gebruikt zelf een dienst bij een dienstverlener die authenticatie van de dienstafnemer vereist. De dienstafnemer is daarmee tevens uitvoerende natuurlijk persoon.
1.1	Dienstverlener stelt vraag aan eHerkenningsmakelaar	De dienstverlener stuurt de uitvoerende natuurlijk persoon door naar de eHerkenningsmakelaar en stelt daarbij een vraag. Deze vraag bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst en het door de dienstverlener vereiste betrouwbaarheidsniveau van de authenticatie. In de vraag wordt expliciet een nieuwe authenticatie afgedwongen.
1.2	Uitvoeren GUC3	Het resultaat is dat de eHerkenningsmakelaar een verklaring over de authenticatie van de uitvoerende natuurlijk persoon ontvangt met een intern pseudoniem.
1.3	eHerkenningsmakelaar beantwoordt vraag van dienstverlener met verklaring	De eHerkenningsmakelaar beantwoordt de vraag van de dienstverlener. Dit antwoord bevat een verklaring die de eHerkenningsmakelaar opstelt op basis van de van de authenticatiedienst ontvangen verklaring over de authenticatie van de uitvoerende natuurlijk persoon met daarin het betrouwbaarheidsniveau van de verklaring en het specifiek pseudoniem van de dienstafnemer (is nl. gelijk aan de uitvoerende natuurlijk persoon).
	Finale staat	De dienstafnemer is geauthenticeerd en de dienstverlener heeft daar de benodigde informatie over ontvangen. De dienstafname kan worden vervolgd. Informatie over de uitvoerende natuurlijk persoon kan benut worden voor personalisatie, logging e.d.

ad stap 1.1: De vraag is als AuthnRequest in detail beschreven in Interface specifications

ad stap 1.3: Het antwoord is als Response in detail beschreven in Interface specifications

Alternatieve scenario's

Voor de use case "GUC1: Gebruiken eHerkenning als dienstafnemer" bestaan de volgende alternatieve scenario's.

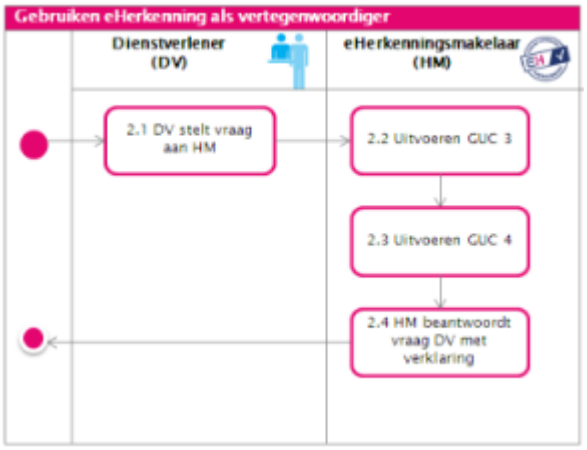
GUC1.2 Er wordt “met vertegenwoordiging” gespecificeerd

Wanneer in stap 1.2 als onderdeel van GUC3 geconstateerd wordt dat er sprake is van vertegenwoordiging wordt in plaats van met stap 1.3 de use case vervolgd als in GUC2 met stap 2.3.

GUC2 Gebruiken eHerkenning als vertegenwoordiger

In deze use case, die een uitbreiding is op GUC1 Gebruiken eHerkenning als dienstafnemer, wordt de identiteit van de vertegenwoordigde dienstafnemer, de pseudo-identiteit van de uitvoerende natuurlijk persoon en de vertegenwoordigingsbevoegdheid van de uitvoerende natuurlijk persoon namens deze vertegenwoordigde dienstafnemer vastgesteld. De eHerkenningsmakelaar geeft een nieuwe verklaring af aan de dienstverlener. Deze verklaring is samengesteld uit de verklaringen van de authenticatiedienst en het machtigingenregister. De uitvoerende natuurlijk persoon voert hiertoe de use cases GUC3 Aantonen identiteit en GUC4 Aantonen bevoegdheid uit.

De use case GUC2 "Gebruiken eHerkenning als vertegenwoordiger" is een uitbreiding op GUC1 Gebruiken eHerkenning als dienstafnemer en wordt hieronder in een activity diagram weergegeven.



De verschillende acties voor use case GUC2 worden hier in meer detail beschreven.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstafnemer laat zich voor het afnemen van een dienst vertegenwoordigen bij een dienstverlener die authenticatie van de dienstafnemer vereist. De uitvoerende natuurlijk persoon handelt als vertegenwoordiger.
2.1	Dienstverlener stelt vraag aan eHerkenningsmakelaar	Zie stap 1.1 GUC1 Gebruiken eHerkenning als dienstafnemer
2.2	Uitvoeren GUC3	Het resultaat is dat de eHerkenningsmakelaar een verklaring over de authenticatie van de uitvoerende natuurlijk persoon ontvangt met een intern pseudoniem.
2.3	Uitvoeren GUC4	Het resultaat is dat de eHerkenningsmakelaar een verklaring over de bevoegdheid van de uitvoerende natuurlijk persoon ontvangt. Indien het een ketenmachtiging betreft verifieert de eHerkenningsmakelaar de hele keten alvorens deze te gebruiken in de volgende stap.

2.4	eHerkenningsmakelaar beantwoordt vraag van dienstverlener met verklaring	De eHerkenningsmakelaar beantwoordt de vraag van de dienstverlener. Dit antwoord bevat een verklaring die de eHerkenningsmakelaar opstelt op basis van de van de authenticatiedienst en van het machtigingenregister/de machtigingenregisters ontvangen verklaringen over de authenticatie en de bevoegdheid van de uitvoerende natuurlijk persoon) met daarin het betrouwbaarheidsniveau van de verklaring, het identificerend kenmerk van de vertegenwoordigde dienstafnemer, het specifiek pseudoniem de uitvoerende natuurlijk persoon en indien relevant informatie over de ketenmachtiging. Het betrouwbaarheidsniveau is gelijk aan het laagste betrouwbaarheidsniveau van de betrouwbaarheidsniveaus van de verklaringen van de authenticatiedienst en het machtigingenregister/de machtigingenregisters.
	Finale staat	De dienstafnemer is geauthenticeerd en de dienstverlener heeft daar de benodigde informatie over ontvangen. De dienstafname kan worden vervolgd ten behoeve van de vertegenwoordigde dienstafnemer. Informatie over de uitvoerende natuurlijk persoon en zijn bevoegdheid kan benut worden voor personalisatie, logging e.d.

ad actie 2.4: Het antwoord is als Response in detail beschreven in Interface specifications DV-HM 1.7.

Druk op inloggen bij een Dienstverlener	Het scherm van de eHerkenningsmakelaar

Het scherm van de Authenticatiedienst	Terug bij de Dienstverlener

Alternatieve scenario's

Voor de use case "GUC2: Gebruiken eHerkenning als vertegenwoordiger" bestaan geen zelfstandige alternatieve scenario's.

GUC3 Aantonen identiteit

GUC3: Aantonen identiteit - In deze use case kiest de uitvoerende natuurlijk persoon een authenticatiedienst en identificeert

zich bij die authenticatiedienst door het gebruik van een authenticatiemiddel, dat hij eerder heeft verkregen (zie Use cases voor Administratie). De authenticatiedienst authentiseert de uitvoerende natuurlijk persoon en geeft hierover een verklaring af aan de eHerkenningsmakelaar.

De use case GUC3 "Gebruiken authenticatiemiddel" wordt hieronder in een activity diagram weergegeven.

De verschillende acties worden hier in meer detail beschreven.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstverlener heeft een vraag gesteld aan de eHerkenningsmakelaar.
3.1	Uitvoerende natuurlijk persoon kiest authenticatiedienst	Op de website van de eHerkenningsmakelaar kiest de uitvoerende natuurlijk persoon een authenticatiedienst uit de lijst van authenticatiediensten. De uitvoerende natuurlijk persoon kan ervoor kiezen deze keuze te bewaren. Zie Aanvullende eisen aan eHerkenningsmakelaarschermen.
3.2	eHerkenningsmakelaar stelt vraag aan authenticatiedienst	De eHerkenningsmakelaar stuurt de uitvoerende natuurlijk persoon door naar de door de uitvoerende natuurlijk persoon geselecteerde authenticatiedienst en stelt daarbij een vraag. Deze vraag bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst en het door de dienstverlener gewenste betrouwbaarheidsniveau van de authenticatie. In de vraag wordt expliciet een nieuwe authenticatie afgedwongen.
3.3	Authenticatiedienst authentiseert uitvoerende natuurlijk persoon	De uitvoerende natuurlijk persoon identificeert zich bij de authenticatiedienst door het gebruik van zijn authenticatiemiddel, waarop de authenticatiedienst de uitvoerende natuurlijk persoon authentiseert. Zie Aanvullende eisen authenticatiedienst.
3.4	Authenticatiedienst stelt rol uitvoerende natuurlijk persoon vast	De authenticatiedienst stelt vast in welke rol de uitvoerende natuurlijk persoon acteert. Mogelijke rollen zijn: • Burger/consument • Beroepsbeoefenaar • Vertegenwoordiger De authenticatiedienst bepaalt dit óf op basis van de eigen (contract-) administratie, óf door de uitvoerende natuurlijk persoon te vragen een keuze te maken. Hierbij borgt de authenticatiedienst dat de uitvoerende natuurlijk persoon uitsluitend kan acteren als burger/consument of beroepsbeoefenaar als dit door de dienstverlener voor deze dienst is toegestaan en zodanig in de dienstencatalogus is vastgelegd. Voor het vervolg van deze use case wordt er vanuit gegaan dat de uitvoerende natuurlijk persoon mag acteren en acteert als burger/consument. De andere rollen worden in alternatieve scenario's uitgewerkt.

3.5	Authenticatiedienst beantwoordt vraag van eHerkenningsmakelaar met verklaring	De authenticatiedienst beantwoordt de vraag van de eHerkenningsmakelaar. Dit antwoord bevat een verklaring over de authenticatie met daarin het betrouwbaarheidsniveau van de verklaring en het specifiek pseudoniem van de uitvoerende natuurlijk persoon. Indien de uitvoerende natuurlijk persoon in stap 3.1 heeft aangegeven zijn keuze voor de authenticatiedienst te willen bewaren dan slaat de eHerkenningsmakelaar deze nu op, zodanig dat deze instelling ook voor andere eHerkenningsmakelaars toegankelijk is.
	Finale staat	De uitvoerende natuurlijk persoon is geauthenticeerd en de eHerkenningsmakelaar heeft daar de benodigde informatie over ontvangen.

ad actie 3.2: De vraag is als AuthnRequest in detail beschreven in Interface specifications.
ad actie 3.5: Het antwoord is als Response in detail beschreven in Interface specifications.

Alternatieve scenario's

Voor de use case "GUC3: Aantonen identiteit" bestaan de volgende alternatieve scenario's.

- GUC3.3 Authenticatie uitvoerende natuurlijk persoon mislukt

GUC3.3 Authenticatie uitvoerende natuurlijk persoon mislukt

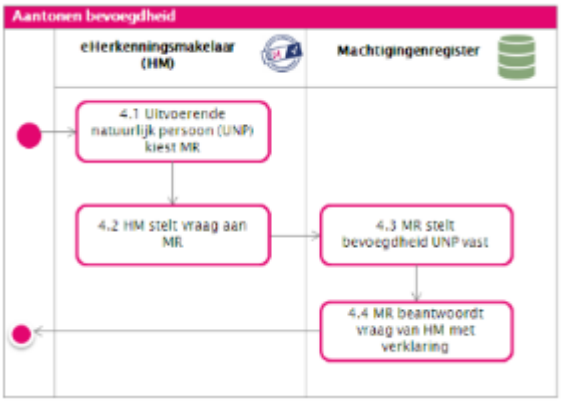
In stap 3.3 kan de authenticatie van de uitvoerende natuurlijk persoon om verschillende redenen mislukken: het authenticatiemiddel is niet van het minimaal door de dienstverlener gewenste betrouwbaarheidsniveau, het authenticatiemiddel is verlopen of ingetrokken, of de uitvoerende natuurlijk persoon gebruikt het authenticatiemiddel foutief (verkeerd wachtwoord, verkeerde kaart, et cetera). Deze situaties worden allemaal op dezelfde manier afgehandeld.

- De authenticatiedienst stelt de uitvoerende natuurlijk persoon op het scherm op de hoogte van de reden van het mislukken van de authenticatie.
- De authenticatiedienst geeft aan de uitvoerende natuurlijk persoon op het scherm een suggestie voor de vervolghandeling die de persoon naar aanleiding van de fout zou kunnen uitvoeren.
- De authenticatiedienst MAG de uitvoerende natuurlijk persoon aanbieden het opnieuw te proberen.
- De authenticatiedienst MOET de handelend natuurlijk persoon de mogelijkheid bieden te annuleren (zie Uitvoerende natuurlijk persoon annuleert).

GUC4 Aantonen bevoegdheid

In deze use case kiest de uitvoerende natuurlijk persoon een machtigingenregister en raadpleegt de uitvoerende natuurlijk persoon dat machtigingenregister. Het machtigingenregister stelt op basis van de eerder met GUC3 Aantonen identiteit verkreg en identiteit van de uitvoerende natuurlijk persoon en een eerder geregistreerde bevoegdheid (zie Use cases voor Administratie) , de identiteit van de vertegenwoordigde dienstafnemer en de pseudo-identiteit van de uitvoerende natuurlijk persoon vast en geeft hierover een verklaring af aan de eHerkenningsmakelaar.

De use case GUC4 "Aantonen bevoegdheid" wordt hieronder in een activity diagram weergegeven.



De verschillende acties voor use case GUC4 worden hier in meer detail beschreven.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstverlener heeft een vraag gesteld aan de eHerkenningsmakelaar. De uitvoerende natuurlijk persoon is geïdentificeerd door een authenticatiedienst en de eHerkenningsmakelaar heeft daarover een verklaring met een intern pseudoniem ontvangen.
4.1	Uitvoerende natuurlijk persoon kiest machtigingenregister	Op de website van de eHerkenningsmakelaar kiest de uitvoerende natuurlijk persoon een machtigingenregister uit de lijst van machtigingenregisters. Zie Aanvullende eisen eHerkenningsmakelaar
4.2	eHerkenningsmakelaar stelt vraag aan machtigingenregister	De eHerkenningsmakelaar stuurt de uitvoerende natuurlijk persoon door naar het door de uitvoerende natuurlijk persoon geselecteerde machtigingenregister en stelt daarbij een vraag. Deze vraag bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst, het door de dienstverlener gewenste betrouwbaarheidsniveau en het interne pseudoniem van de uitvoerende natuurlijk persoon.
4.3	Machtigingenregister stelt bevoegdheid uitvoerende natuurlijk persoon vast	Het machtigingenregister bepaalt op basis van het interne pseudoniem voor welke dienstafnemer de uitvoerende natuurlijk persoon bevoegd is en selecteert het specifieke pseudoniem van de uitvoerende natuurlijk persoon dat hoort bij de betreffende combinatie van dienstverlener en vertegenwoordigde dienstafnemer. Zie Aanvullende eisen machtigingenregister.
4.4	Machtigingenregister beantwoordt vraag van eHerkenningsmakelaar met verklaring	Het machtigingenregister beantwoordt de vraag van de eHerkenningsmakelaar. Dit antwoord bevat een verklaring over de bevoegdheid van de uitvoerende natuurlijk persoon met daarin het betrouwbaarheidsniveau van de verklaring, het identificerend kenmerk van de vertegenwoordigde dienstafnemer en het specifieke pseudoniem van de uitvoerende natuurlijk persoon.
	Finale staat	De bevoegdheid van de uitvoerende natuurlijk persoon namens de vertegenwoordigde dienstafnemer is aangetoond en de eHerkenningsmakelaar heeft daar de benodigde informatie over ontvangen.

ad actie 4.2: De vraag is als XACMLAuthzDecisionQuery in detail beschreven in Interface specifications HM-MR 1.7.
ad actie 4.4: Het antwoord is als XACMLAuthzDecision Response in detail beschreven in Interface specifications HM-MR 1.7.

Alternatieve scenario's

Voor de use case "GUC4: Aantonen bevoegdheid" bestaan de volgende alternatieve scenario's.

- GUC4.1 Te bevragen machtigingenregister reeds bekend
- GUC4.2 Authenticatie voor dienst 0
- GUC4.2 Ketenmachtiging
- GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet
- GUC4.2 Verschillende bevoegdheden aanwezig

GUC4.1 Te bevragen machtigingenregister reeds bekend

Indien al bekend is welk machtigingenregister geraadpleegd moet worden biedt de eHerkenningsmakelaar de uitvoerende natuurlijk persoon geen lijst van machtigingenregisters aan. Met het bekende machtigingenregister wordt stap 4.2 vervolgd. De opgave van het machtigingenregister kan afkomstig zijn uit de verklaring van de authenticatiedienst (GUC3) of uit een verklaring van een ander machtigingenregister (zie GUC4.2 Ketenmachtiging).

GUC4.2 Authenticatie voor dienst 0

Wanneer een dienstverlener een authenticatie van een uitvoerende dienstafnemer voor dienst 0 vraagt, wijzigt 4.3. Na deze stap wordt GUC4 Aantonen bevoegdheid gewoon met stap 4.4 vervolgd.

Nr.	Actie	Omschrijving

4.3	Machtigingenregister stelt bevoegdheid uitvoerende natuurlijk persoon vast	Het machtigingenregister bepaalt op basis van het interne pseudoniem voor welke uitvoerende dienstafnemer de uitvoerende natuurlijk persoon voor tenminste één dienst een bevoegdheid is geregistreerd en selecteert het specifieke pseudoniem van de uitvoerende natuurlijk persoon dat hoort bij de betreffende combinatie van dienstverlener en uitvoerende dienstafnemer. Het machtigingenregister bewaakt hierbij dat het registratieproces waarmee de bevoegdheid is vastgelegd minimaal van het door de dienstverlener vereiste betrouwbaarheidsniveau is.

GUC4.2 Ketenmachtiging

In verschillende situaties moet het machtigingenregister concluderen dat de gevonden bevoegdheid nog niet het volledige antwoord op de gevraagde bevoegdheid compleet maakt. Dit zijn de volgende situaties:

- Vertegenwoordigde dienstafnemer is in de vraag gespecificeerd en is ongelijk aan de partij die als vertegenwoordigde in de gevonden bevoegdheid voorkomt.
- Bij de gevonden bevoegdheid is een beperking vastgelegd die bepaalt dat de bevoegdheid alleen "voor derden" geldt en niet voor de in de bevoegdheid voorkomende vertegenwoordigde partij zelf. Deze derde moet dan als informatie bekend zijn in het betreffende machtigingenregister.
- Het machtigingenregister toont na bepalen van één geldige bevoegdheid (in stap 4.2 of 4.2a) een bevestigingscherm dat de optie bevat om in plaats van het bevestigen van de bevoegdheid een vertegenwoordigde dienstafnemer op te geven namens wie ditmaal toegang gevraagd wordt.

Vervolgens is het verdere verloop als volgt:

Nr.	Actie	Omschrijving
4.4	Machtigingenregister beantwoordt vraag van eHerkenningsmakelaar met verklaring en specificeert volgende machtigingenregister.	Het machtigingenregister beantwoordt de vraag van de eHerkenningsmakelaar en stuurt de uitvoerend natuurlijk persoon terug naar de eHerkenningsmakelaar. Dit antwoord bevat een verklaring over de bevoegdheid van de uitvoerende natuurlijk persoon met daarin het betrouwbaarheidsniveau van de verklaring en het specifieke pseudoniem van de uitvoerende natuurlijk persoon. Daarnaast wordt een bevoegdheidsketen meegegeven, wordt de aanduiding van het volgende machtigingenregister meegegeven. De bevoegdheidsketen bevat de specificatie van de vertegenwoordigde dienstafnemer (hetzij uit de vraag, hetzij zoals in dit machtigingenregister vastgelegd). De verklaring specificeert alleen dat het machtigingenregister voor de gevraagde schakel het bestaan van een machtiging heeft geverifieerd. Voor de rest van de bevoegdheidsketen wordt alleen informatief aangegeven hoe deze eruit ziet en waar deze geverifieerd kan worden.
4.4a	eHerkenningsmakelaar ontvangt incomplete keten.	De eHerkenningsmakelaar voert controles uit op de ontvangen verklaring en constateert dat de keten incompleet is.
4.4b	eHerkenningsmakelaar bevraagt volgend machtigingenregister.	De eHerkenningsmakelaar bevraagt het in voorgaande verklaring aangeduide machtigingenregister. De vraag daarbij bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst, het door de dienstverlener gewenste betrouwbaarheidsniveau en deze MOETEN identiek zijn aan hetgeen in de vraag bij stap 4.2 gespecificeerd was. Daarnaast bevat de vraag het identificerende kenmerk van de intermediaire partij waarvoor aan het machtigingenregister een bevoegdheid gevraagd wordt en de bevoegdheidsketen van de uitvoerend natuurlijk persoon tot aan deze intermediaire partij. De vraag bevat tevens alle andere gegevens die van het voorgaande machtigingenregister ontvangen zijn en die in de initiële vraag aan de eHerkenningsmakelaar gespecificeerd zijn.
4.4c	Machtigingenregister bepaalt machtiging aan intermediaire partij.	Het machtigingenregister bepaalt op basis van het identificerende kenmerk van de intermediaire partij of er inderdaad een bevoegdheid voor betreffende dienst is geregistreerd en controleert of deze het minimaal vereiste betrouwbaarheidsniveau heeft.
4.4d	Machtigingenregister verstrekt gevraagde verklaring aan eHerkenningsmakelaar.	Het machtigingenregister levert een verklaring met het gevraagde antwoord aan de eHerkenningsmakelaar. Dit antwoord bevat een verklaring over de bevoegdheid van de vertegenwoordigde dienstafnemer aan de in de vraag gespecificeerde intermediaire partij met daarin het betrouwbaarheidsniveau van de verklaring. Daarnaast wordt een bevoegdheidsketen meegegeven die volledig is van vertegenwoordigde dienstafnemer tot aan de intermediaire partij namens w de uitvoerende natuurlijk persoon bevoegd is.

4.4e	eHerkenningsmakelaar concludeert dat keten volledig is.	De eHerkenningsmakelaar voert controles uit op de ontvangen verklaring en constateert dat de keten compleet is (identiek aan stap 4.4a met ander resultaat).
	Finale staat	De finale staat conform use case GUC4 is bereikt met dien verstande dat daarbij nu ook informatie over een complete ketenmachtiging bij de eHerkenningsmakelaar bekend is.

Varianten bij Ketenmachtiging

Als onderdeel van de alternatieve flow voor ketenmachtiging kunnen de volgende varianten voorkomen (die hier dus als alternatieve flow binnen de alternatieve flow van GUC4.2 Ketenmachtiging beschreven worden).

Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet (stap 4.4c alternatief)

Indien geen geldige bevoegdheid gevonden wordt, of indien meerdere bevoegdheden gevonden worden zonder dat op basis van gespecificeerde vertegenwoordigde dienstafnemer bepaald kan worden welke bevoegdheid gevraagd wordt (m.a.w. er is geen eenduidig antwoord te geven) dan wordt de bevraging afgebroken met foutmelding aan de eHerkenningsmakelaar en deze geeft een foutmelding aan de uitvoerende natuurlijk persoon conform alternatief scenario GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet, met dien verstande dat de eHerkenningsmakelaar de foutmelding aan de uitvoerende natuurlijk persoon moet tonen en de afhandeling moet uitvoeren.

Vertegenwoordigde dienstafnemer onbekend (stap 4.4 alternatief)

Indien de vertegenwoordigde dienstafnemer niet is gespecificeerd in de vraag en niet aanvullend bij de gevonden bevoegdheid is opgenomen wordt de uitvoerende natuurlijk persoon gevraagd deze te specificeren. Deze vraag kan gecombineerd worden met de selectie voor het geval dat er verschillende bevoegdheden aanwezig zijn.

Dat wil zeggen dat de uitvoerende natuurlijk persoon op dit punt gevraagd wordt alle informatie aan te vullen die nodig is om de rest van de keten zonder gebruikersinteractie door eHerkenningsmakelaar middels bevraging van machtigingenregisters te laten verifiëren. De happy flow blijft de situatie waarbij al deze informatie reeds bij de bevoegdheid is vastgelegd tijdens de registratie. Belangrijk is dat alle aanvullende informatie als attribuut wordt doorgegeven en dus geen verklaring over geldigheid inhoudt, de verdere schakels van de keten MOETEN daadwerkelijk geverifieerd worden in het machtigingenregister waar ze geregistreerd zijn.

GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet

Er kunnen verschillende redenen zijn waarom een machtigingenregister geen bevoegdheid vindt die aan de vraag voldoet. Voorbeelden hiervan zijn: de geregistreerde bevoegdheid is niet van het minimaal door de dienstverlener vereiste betrouwbaarheidsniveau, de machtiging is verlopen of ingetrokken of de dienst of dienstverlener komt niet (langer) voor in de dienstencatalogus. Deze situaties worden allemaal op dezelfde manier afgehandeld.

- Het machtigingenregister stelt de uitvoerende natuurlijk persoon op het scherm op de hoogte van de reden van het mislukken van de raadpleging.
- Het machtigingenregister geeft aan de uitvoerende natuurlijk persoon op het scherm een suggestie voor de vervolghandeling die de persoon naar aanleiding van de fout zou kunnen uitvoeren.

De uitvoerende natuurlijk persoon kan annuleren (zie Uitvoerende natuurlijk persoon annuleert).

GUC4.2 Verschillende bevoegdheden aanwezig

Het is mogelijk dat voor het in de vraag gespecificeerde interne pseudoniem (van de uitvoerende natuurlijk persoon) meerdere geldige machtigingen voor dezelfde dienst gevonden worden. Denk hierbij aan situaties bij intermediairs, adviseurs met verschillende opdrachten, eigenaars van verschillende bedrijven, etc. Het is ook

mogelijk dat een uitvoerende natuurlijk persoon meer (maar niet alle) vestigingen van een dienstafnemer mag vertegenwoordigen.

Het Machtigingenregister vraagt een bevoegdheid te kiezen

I.p.v. stap 4.3 zijn dan de volgende stappen nodig. Na deze stappen wordt GUC4 gewoon met stap 4.4 vervolgd.

Nr.	Actie	Omschrijving
4.3	Machtigingenregister toont mogelijke bevoegdheden	Het machtigingenregister bepaalt op basis van het interne pseudoniem van de uitvoerende natuurlijke persoon welke mogelijke bevoegdheden bestaan en toont de bijbehorende dienstafnemers in een lijst.
4.3a	Uitvoerende natuurlijk persoon selecteert bevoegdheid	De uitvoerende natuurlijk persoon selecteert de bevoegdheid op basis waarvan hij ditmaal toegang vraagt uit de getoonde lijst.
4.3b	Machtigingenregister stelt bevoegdheid uitvoerende natuurlijk persoon vast	Het machtigingenregister bepaalt op basis van de keuze van de uitvoerende natuurlijk persoon het specifieke pseudoniem van de uitvoerende natuurlijk persoon dat hoort bij de betreffende combinatie van dienstverlener en vertegenwoordigde dienstafnemer. Zie Aanvullende eisen machtigingenregister.

Aanvullende eisen eHerkenningsmakelaar

Deze paragraaf beschrijft een aantal extra eisen aan alle eHerkenningsmakelaars:

- Een eHerkenningsmakelaar MOET na ontvangst van een verklaring van een machtigingenregister controleren of het een

incomplete keten betreft die alleen geldig is indien aanvullende schakels ook geverifieerd kunnen worden (zie ook GUC4.2 Ketenmachtiging, Werking ketenmachtigingen, Interface specifications HM-MR 1.7 chain authorization)

Aanvullende eisen authenticatiedienst

Deze paragraaf beschrijft een aantal aanvullende eisen aan de authenticatiedienst.

- De authenticatiedienst MOET bewaken dat zowel de identificatie (i.c. het gebruikte authenticatiemiddel) als het proces van de authenticatie van minimaal het door de dienstverlener gewenste betrouwbaarheidsniveau is.
- De authenticatiedienst MOET op elke getoonde web pagina de naam van dienstverlener tonen zoals die in de dienstencatalogus is opgenomen.
- De authenticatiedienst MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- De authenticatiedienst MOET alle processen inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in Betrouwbaarheidsniveaus en registratie-eisen.
- De authenticatiedienst MOET toegang hebben tot de relevante door de middelenuitgever vastgelegde informatie om tot een authenticatie van het betreffende betrouwbaarheidsniveau te komen.

Zie ook Aanvullende eisen authenticatiedienst die SSO ondersteunt

Aanvullende eisen authenticatiedienst die SSO ondersteunt

Aanvullende eisen aan authenticatiedienst die single sign-on ondersteunt

- De authenticatiedienst MOET single sign-on zodanig uitvoeren dat er geen risico's op hergebruik of afluisteren van het authenticatiemechanisme bestaan.
- De authenticatiedienst MOET zodra een vraag van een dienstverlener ontvangen wordt waarin geen verplichte authenticatie door de uitvoerende natuurlijk persoon gespecificeerd is, de optie aanbieden om ingelogd te blijven. De authenticatiedienst MAG deze optie ook bieden indien wel een verplichte authenticatie gespecificeerd is. Het is toegestaan instellingen van de handelend natuurlijk persoon aangaande het al dan niet aangemeld blijven na eerste authenticatie op een andere manier vast te leggen en toe te passen. Deze specificatie door de handelend natuurlijk persoon blijft alleen relevant indien het een vraag betreft waarbij de dienstverlener single sign-on toestaat.
- Als een uitvoerend natuurlijke persoon kiest om niet ingelogd te blijven, MOET deze keuze door de authenticatiedienst onthouden worden.
- De authenticatiedienst MOET de gebruiker middels teksten op het scherm of anderszins duidelijk maken in welke situatie de gebruiker zich bevindt (time-out van een SSO sessie, gedwongen authenticatie tijdens een bestaande SSO sessie, logout, etc.)

Aanvullende eisen machtigingenregister

Deze paragraaf beschrijft een aantal aanvullende eisen aan het machtigingenregister.

- Het machtigingenregister MOET bewaken dat het registratieproces waarmee de bevoegdheid is vastgelegd minimaal van het door de dienstverlener vereiste betrouwbaarheidsniveau is.
- Het machtigingenregister MOET op elke getoonde web pagina de naam van dienstverlener tonen zoals die in de dienstencatalogus is opgenomen.
- Het machtigingenregister MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- Het machtigingenregister MOET alle processen inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in Betrouwbaarheidsniveaus eHerkenning.
- Het machtigingenregister MOET het hoogst mogelijke betrouwbaarheidsniveau hanteren in het antwoord. Dat wil zeggen dat als er bijv. een algemene bevoegdheid is geregistreerd op een laag niveau, maar voor de betreffende dienst ook een specifieke bevoegdheid is vastgelegd op een hoger niveau dat het machtigingenregister dan het hogere niveau MOET hanteren.

Aanvullende eisen machtigingenregister dat ketenmachtigingen ondersteunt

Deze paragraaf beschrijft een aantal aanvullende eisen aan het machtigingenregister dat ketenmachtigingen ondersteunt:

- Het machtigingenregister MOET in volgende prioriteitsvolgorde de informatie aangaande de compleetheid van de keten benutten:
  - Hetgeen gespecificeerd is bij een gevonden geldige machtiging
  - Hetgeen in de vraag als specificatie is meegegeven
  - Hetgeen bij ontbreken van bovenstaande aan de uitvoerende natuurlijk persoon gevraagd is.

Use case overschrijdende alternatieve scenario's

Een aantal alternatieve scenario's heeft impact op meer dan één use case. Deze scenario's worden hier beschreven. De volgende alternatieve scenario's worden onderscheiden:

- Alternatief scenario attribuutverstrekking
- Attributen niet leverbaar of niet toegestaan
- Attribuut komt niet voor in attribuutcatalogus
- Dienst of dienstverlener komt niet voor in dienstencatalogus
- Soort dienstafnemer kan niet worden geleverd
- Uitvoerende natuurlijk persoon annuleert
- Use cases Single Sign-On

Alternatief scenario attribuutverstrekking

In stap 1.1 van GUC1 Gebruiken eHerkenning als dienstafnemer en stap 2.1 van GUC2 Gebruiken eHerkenning als vertegenwoordiger kan de dienstverlener wanneer de eHerkenningsmakelaar dit ondersteunt optioneel om aanvullende attributen vragen. Dit kan expliciet door gebruik te maken van de beschreven extensie in de Interface specifications, of impliciet door met de eHerkenningsmakelaar af te spreken dat voor een bepaalde dienst altijd een bepaalde set attributen wordt uitgevraagd. De gevraagde attributen worden opgenomen in de DV-HM SAML metadata. Een dienstverlener kan verschillende metadata profielen hanteren voor verschillende sets met uit te vragen attributen.

In stap 3.2 van GUC3 Aantonen identiteit neemt de eHerkenningsmakelaar, wanneer de dienstverlener om aanvullende attributen vraagt, de attributen die de authenticatiedienst zou kunnen leveren in de vraag op.

Na stap 3.4 van GUC3 Aantonen identiteit toont de authenticatiedienst, wanneer aanvullende attributen van de authenticatiedienst worden gevraagd en de authenticatiedienst dit ondersteunt, de beschikbare attributen en de waarden van de attributen en vraagt de uitvoerend natuurlijk persoon goedkeuring om deze attributen te verstrekken (User consent). Indien de uitvoerend natuurlijk persoon al eerder doorlopende user consent heeft gegeven dan kan deze stap achterwege worden gelaten.

In stap 3.5 van GUC3 Aantonen identiteit worden, wanneer aanvullende attributen worden gevraagd en de authenticatiedienst dit ondersteunt, in het antwoord ook de beschikbare en waarvoor de uitvoerende natuurlijk persoon user consent heeft verleend, opgenomen in versleutelde vorm.

Na stap 4.3 van GUC4 Aantonen bevoegdheid toont het machtigingenregister, wanneer aanvullende attributen van het machtigingenregister worden gevraagd en het machtigingenregister dit ondersteunt, de beschikbare attributen en de waarden van de attributen en vraagt de uitvoerend natuurlijk persoon goedkeuring om deze attributen te verstrekken (user consent). Indien de machtigingenbeheerder van de vertegenwoordigde dienstafnemer/intermediaire partij al eerder (bijvoorbeeld bij registratie van de machtiging) doorlopende user consent heeft gegeven dan kan deze stap achterwege worden gelaten.

In stap 4.4 van GUC4 Aantonen bevoegdheid worden, wanneer aanvullende attributen worden gevraagd en het machtigingenregister dit ondersteunt, in het antwoord ook de beschikbare en waarvoor uitvoerende natuurlijk persoon user consent heeft verleend, opgenomen in versleutelde vorm. Vestigingsspecifieke attributen worden alleen verstrekt indien ze als zodanig gevraagd worden.

In stap 1.3 van GUC1 Gebruiken eHerkenning als dienstafnemer en stap 2.4 van GUC2 Gebruiken eHerkenning als vertegenwoordiger worden, wanneer aanvullende attributen door de dienstverlener zijn gevraagd en deze attributen door authenticatiedienst en/of machtigingenregister zijn geleverd, deze in versleutelde vorm aan het antwoord toegevoegd.

Attributen niet leverbaar of niet toegestaan

Indien AD of MR één of meer van de gevraagde attributen, waarvan in de SAML metadata is aangegeven dat deze niet Required zijn, niet kunnen leveren (hetzij omdat zij deze gegevens niet registeren, hetzij omdat er geen User consent gegeven wordt) wordt in stap 5 van GUC3 Aantonen identiteit, respectievelijk stap 4 van GUC4 Aantonen bevoegdheid een

authenticatieverklaring afgegeven die enkel de authenticatie en gegevens die wel leverbaar zijn bevat. De Use case wordt vervolgens normaal vervolgd. In stap 3 van GUC1 Gebruiken eHerkenning als dienstafnemer of stap 4 van GUC2 Gebruiken eHerkenning als vertegenwoordiger levert de HM de gevraagde attributen die geleverd konden worden, de andere attributen worden niet meegezonden.

Indien AD of MR één of meer van de gevraagde attributen, waarvan in de metadata is aangegeven dat deze Required zijn, niet kunnen leveren (hetzij omdat zij deze gegevens niet registeren, hetzij omdat er geen user consent gegeven wordt) wordt na stap 5 van GUC3 Aantonen identiteit, respectievelijk stap 4 van GUC4 Aantonen bevoegdheid de Use case niet vervolgd en wordt het request door de HM behandeld als een functioneel ontoereikend bericht (zie Error handling).

Dienstverlener MOET er rekening mee houden dat gevraagde optionele attributen niet geleverd kunnen worden. Dit kan betekenen dat bepaalde dienstverlening niet mogelijk is.

Attribuut komt niet voor in attribuutcatalogus

Zowel de eHerkenningsmakelaar (in stap 1 van GUC1 Gebruiken eHerkenning als dienstafnemer en stap 1 van GUC2 Gebruiken eHerkenning als vertegenwoordiger) als de authenticatiedienst (in stap 2 van GUC3 Aantonen identiteit) als het machtigingenregister (in stap 2 van GUC4 Aantonen bevoegdheid) dienen te controleren of het attributen betreft die voorkomen in de attribuutcatalogus. Indien dit niet het geval is dienen zij een fout met die strekking te tonen en wordt de use case niet vervolgd.

Dienst of dienstverlener komt niet voor in dienstencatalogus

In stap 1.1 van GUC1 Gebruiken eHerkenning als dienstafnemer, stap 2.1 van GUC2 Gebruiken eHerkenning als vertegenwoordiger, stap 3.2 van GUC3 Aantonen identiteit of stap 4.2 van GUC4 Aantonen bevoegdheid kan worden geconstateerd dat de dienst of dienstverlener niet voorkomt in de door de betreffende deelnemer gehanteerde versie van de dienstencatalogus. De betreffende deelnemer MOET het proces dan afbreken met een algemene fout zoals beschreven Error handling.

Soort dienstafnemer kan niet worden geleverd

In stap 3.3 van GUC3 Aantonen identiteit kan een authenticatiedienst (en in stap 4.3 van GUC4 Aantonen bevoegdheid een machtigingenregister) vaststellen dat de voor het antwoord benodigde soort dienstafnemer niet kan worden geleverd. Dit kan bijvoorbeeld komen doordat de uitvoerende natuurlijk persoon niet behoort tot de gevraagde beroepsgroep, of doordat de authenticatiedienst of machtigingenregister niet gerechtigd is de gevraagde gegevens vast te leggen. In dat geval MOET de betreffende deelnemer het proces dan afbreken met een algemene fout zoals beschreven in de documenten Error handling.

Uitvoerende natuurlijk persoon annuleert

De uitvoerende natuurlijk persoon kan de authenticatie op elk gewenst moment annuleren.

Wanneer het annuleren plaatsvindt bij de eHerkenningsmakelaar MOET deze het proces afbreken en naar de dienstverlener antwoorden met een foutmelding die is beschreven in Error handling.

Wanneer het annuleren plaatsvindt bij de authenticatiedienst MOET deze het proces afbreken en naar de dienstverlener antwoorden met een foutmelding die is beschreven in Error handling. De eHerkenningsmakelaar MOET de uitvoerende natuurlijk persoon dan aanbieden een andere authenticatiedienst te kiezen. Indien er een selectie van een authenticatiedienst bewaard is moet deze worden genegeerd. Indien vervolgens opnieuw een authenticatiedienst geselecteerd wordt moet de vraag of deze instelling bewaard moet worden opnieuw getoond worden met default "leeg". De nieuwe keuze overschrijft de oude.

Wanneer het annuleren plaatsvindt bij het machtigingenregister MOET deze het proces afbreken en naar de dienstverlener antwoorden met een foutmelding die is beschreven in Error handling. De eHerkenningsmakelaar MOET de uitvoerende natuurlijk persoon dan aanbieden een ander machtigingenregister te kiezen.

Use cases Single Sign-On

In stap GUC1 Gebruiken eHerkenning als dienstafnemer of GUC2 Gebruiken eHerkenning als vertegenwoordiger kan de

dienstverlener in de vraag specificeren dat single sign-on is toegestaan of dat een hernieuwde authenticatie wordt afgedwongen.

> Voor diensten die betrouwbaarheidsniveau 4 vereisen is single sign-on nooit toegestaan.

In stap GUC3.3 Authenticatie uitvoerende natuurlijk persoon mislukt wordt door een authenticatiedienst die SSO ondersteunt als volgt gehandeld:

- Indien door de dienstverlener een hernieuwde authenticatie wordt afgedwongen en er al eerder een aanlog door de uitvoerende natuurlijk persoon heeft plaatsgevonden waarvan de authenticatie bewaard is gebleven, MOET de nog niet verlopen authenticatie worden beëindigd. Daarnaast MAG na succesvolle authenticatie de optie worden geboden aan de uitvoerende natuurlijk persoon om aangelogd te blijven. Indien de uitvoerende natuurlijk persoon deze optie selecteert, wordt deze bewaard en kan vanaf dat moment SSO plaatsvinden. Tevens MOET de authenticatiedienst vanaf dit moment de timer van het maximum authenticatiedienst tijdsverloop starten;
- Indien SSO is toegestaan en er al eerder een aanlog door de uitvoerende natuurlijk persoon heeft plaatsgevonden waarvan de authenticatie bewaard is en die nog niet verlopen is, wordt deze hergebruikt zonder interactie met de uitvoerende natuurlijk persoon en gaat het authenticatiedienst tijdsverloop opnieuw in;
- Indien er geen eerdere (nog) geldige authenticatie is, MAG de optie worden geboden aan de uitvoerende natuurlijk persoon om aangelogd te blijven. Indien de uitvoerende natuurlijk persoon deze optie selecteert, wordt deze bewaard en kan vanaf dat moment SSO plaatsvinden. Tevens zal de authenticatiedienst vanaf dit moment de timer van het maximum authenticatiedienst tijdsverloop starten.

Na het succesvol uitvoeren van GUC1 Gebruiken eHerkenning als dienstafnemer of GUC2 Gebruiken eHerkenning als vertegenwoordiger MOET de dienstverlener die SSO toepast lokaal de sessie bijhouden. Indien SSO wordt toegepast moet de dienstverlener een logoutfunctie aanbieden.

Varianten bij Single Sign-On

Als onderdeel van de alternatieve flow voor Single Sign-On kunnen de volgende varianten voorkomen (die hier dus als alternatieve flow binnen de alternatieve flow van Use cases Single Sign-On beschreven worden).

- Geen reactie bij lezen of schrijven selectie authenticatiedienst
- Single Log-out

Geen reactie bij lezen of schrijven selectie authenticatiedienst

Als het cookie niet gelezen kan worden, dan moet het proces doorgaan alsof er geen selectie gemaakt is. Als het cookie niet geschreven kan worden, dan moet het proces doorgaan zonder een foutmelding aan de eindgebruiker te tonen.

Single Log-out

De volgende specifieke use case (Single log-out) MOET door alle ADs en HMs ondersteund worden, ook door ADs die geen Single Sign-On ondersteunen. Zij MOGEN logoutberichten NIET afkeuren en MOETEN de melding tonen zoals beschreven in stap 2 hieronder.

Nr.	Actie	Omschrijving
	Initiële staat	Een uitvoerende natuurlijke persoon heeft op basis van één of meer eHerkenningsverklaringen toegang bij een dienstverlener en deze houden sessie lokaal bij. Mogelijk is er ook bij andere dienstverleners nog een geldige sessie aanwezig.
1	Uitvoerende natuurlijk persoon selecteert "logout" binnen de website van de dienstverlener.	De uitvoerende persoon wordt lokaal uitgelogd bij de dienstverlener conform de eisen in Single sign-on and user sessions en daarna doorgestuurd naar de eHerkenningsmakelaar met een logoutbericht (Interface specifications DV-HM 1.7#HM1.7-LogoutRequest).

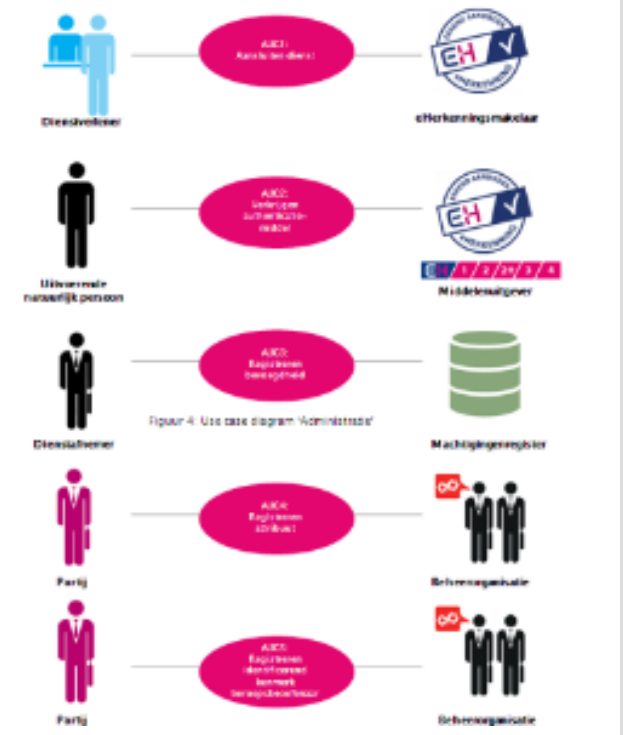
2	HM ontvangt logoutbericht en stuurt dit naar geselecteerde AD	De HM stuurt het logoutbericht door naar de AD (Interface specifications HM-AD 1.7#AD1.7-LogoutRequest). Op basis van het ontvangen bericht beëindigt de authenticatiedienst de eventueel nog geldige bewaarde authenticatie en toont daarna in browserwindow een bericht "uitgelogd bij eHerkenning" met de informatie dat het gewenst is alle browservensters te sluiten (of een andere tekst met nadere uitleg voor de gebruiker).
	Finale staat	De gebruiker heeft bij de authenticatiedienst geen geldige sessie meer, maar mogelijk nog wel bij de andere dienstverleners waarbij eerder is ingelogd. Indien de browser wordt afgesloten verdwijnen ook die sessies.

Wanneer de eHerkenningsmakelaar geen geldige authenticatiedienst vindt om het logoutbericht naar toe te sturen, dan toont de eHerkenningsmakelaar een scherm met de tekst "Uitloggen is momenteel niet mogelijk. Sluit alle [naam browser*]vensters om de beveiliging van uw informatie te waarborgen."

*naam browser bepaald op basis van browserdetectie, of alleen 'browservensters' als detectie niet mogelijk is.

Use cases voor Administratie

Use case diagram Administratie



De volgende processen onderscheiden waarin uitvoerende natuurlijke personen, dienstafnemers en dienstverleners voorbereidingen treffen voor het gebruik van eHerkenning.

- AUC1 Aansluiten dienst
- AUC2 Verkrijgen authenticatiemiddel
- AUC3 Registreren bevoegdheid
- AUC4 Registreren attribuut
- AUC5 Registreren identificerend kenmerk beroepsbeoefenaar

AUC1 Aansluiten dienst

In deze use case wordt een dienst van een dienstverlener aangesloten op eHerkenning. De invulling van deze use case is onderdeel van het competitieve domein van eHerkenning en wordt in zijn geheel overgelaten aan de eHerkenningsmakelaar. Hierbij dient een eHerkenningsmakelaar in elk geval te voldoen aan de in AUC1 Aansluiten dienst gestelde eisen.

Bij de implementatie van deze use case gelden de volgende eisen:

- De eHerkenningsmakelaar MOET een overeenkomst met de dienstverlener sluiten. Zie ook Juridisch kader. Deze overeenkomst MOET in lijn zijn met de Gebruiksvoorwaarden van eHerkenning. Zie ook Gebruiksvoorwaarden eHerkenning.
- De eHerkenningsmakelaar MOET waarborgen dat de dienstverlener het koppelvlak DV-HM zoals beschreven in Interface specifications of een gelijkwaardig koppelvlak correct heeft geïmplementeerd.
- De eHerkenningsmakelaar MOET waarborgen dat de dienst(en) van de dienstverlener, het bijbehorende betrouwbaarheidsniveau en de toegestane typen dienstafnemers correct, voorzien van een uniek nummer in een dienstencatalogus worden beschreven en dat deze dienstencatalogus wordt aangeleverd bij de beheerorganisatie. Zie Operationeel handboek en Interface specifications.

N.B. Een dienstverlener ZOU een uniek nummer voor een dienst NIET MOETEN hergebruiken voor andere diensten. Wanneer een dienstverlener een dienst of de beschrijving van een dienst wijzigt MOET de dienstverlener waarborgen dat de betekenis van de dienst gelijk blijft en daarmee geregistreerde bevoegdheden geldig blijven. In het geval dat de dienstverlener dit niet kan of wil waarborgen MOET een nieuw uniek nummer worden toegekend.

Alternatieve scenario's

Voor deze use case zijn geen alternatieve scenario's gedefinieerd.

AUC2 Verkrijgen authenticatiemiddel

In deze use case verkrijgt de uitvoerende natuurlijk persoon een voor eHerkenning geschikt authenticatiemiddel. Dit kan op verschillende manieren: Het kan zijn dat de uitvoerende natuurlijk persoon een eigen (privé) middel verkrijgt, maar het kan ook zijn dat de uitvoerende natuurlijk persoon het middel op initiatief van, of door zijn werkgever krijgt uitgereikt of dat de uitvoerende natuurlijk persoon een eerder verkregen authenticatiemiddel registreert bij een middelenuitgever voor gebruik binnen eHerkenning. Bij de registratie kan een middel worden gekoppeld aan één of meer identificerende kenmerken van beroepsbeoefenaren. De invulling van deze use case is onderdeel van het competitieve domein van eHerkenning en wordt grotendeels overgelaten aan de middelenuitgever. Hierbij dient een middelenuitgever in elk geval te voldoen aan de in AUC2 Verkrijgen authenticatiemiddel gestelde eisen.

Bij de implementatie van deze use case gelden de volgende eisen:

- De middelenuitgever MOET alle processen beschrijven en inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in document [eHerkenning - Betrouwbaarheidsniveaus]. De beschrijvingen MOETEN via de website van de middelenuitgever worden gepubliceerd.
- De middelenuitgever MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- De middelenuitgever MOET een overeenkomst met het de uitvoerende natuurlijk persoon en/of de uitvoerende dienstafnemer sluiten. Zie ook Juridisch kader.
- De middelenuitgever MOET waarborgen dat het authenticatiemiddel te gebruiken is bij ten minste één authenticatiedienst en daar uniek is te authenticeren.
- De middelenuitgever MOET waarborgen dat voor het authenticatiemiddel bevoegdheden kunnen worden geregistreerd in een machtigingenregister.

Alternatieve scenario's

Voor deze use case zijn geen alternatieve scenario's gedefinieerd.

AUC3 Registreren bevoegdheid

In deze use case legt de dienstafnemer de bevoegdheid van een uitvoerende natuurlijk persoon vast in een machtigingenregister. Deze bevoegdheid kan voortvloeien uit een machtiging of een wettelijke vertegenwoordigingsbevoegdheid (de uitvoerende natuurlijk persoon is bijv. eigenaar van een eenmanszaak). De invulling van deze use case is onderdeel van het competitieve domein van eHerkenning en wordt in zijn geheel overgelaten aan het machtigingenregister. Hierbij dient een machtigingenregister in elk geval te voldoen aan de in AUC2 Verkrijgen authenticatiemiddel gestelde eisen.

Bij de implementatie van deze use case gelden de volgende eisen:

- Het machtigingenregister MOET alle processen beschrijven en inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in document Betrouwbaarheidsniveaus en registratie-eisen. De beschrijvingen MOETEN via de website van het machtigingenregister worden gepubliceerd.
- Het machtigingenregister MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- Het machtigingenregister MOET een overeenkomst met de uitvoerende dienstafnemer sluiten. Zie ook Juridisch kader.
- Het machtigingenregister MOET bevoegdheden zo vastleggen dat voor elke dienst in de dienstencatalogus een eenduidige uitspraak is te doen over de bevoegdheid van de uitvoerende natuurlijk persoon.
- Het machtigingenregister MOET vastleggen wat het betrouwbaarheidsniveau van een vastgelegde bevoegdheid is.
- Het machtigingenregister MAG mogelijkheden bieden voor het beperken van een bevoegdheid tot een bepaalde vestiging van de uitvoerende dienstafnemer. Daarentegen MAG het machtigingenregister een beperking van de bevoegdheid tot een vestiging NIET afdwingen.
- Het machtigingenregister MOET waarborgen dat bij het vastleggen van een bevoegdheid de aanvrager voldoende geïnformeerd is over de betekenis van die bevoegdheid.
- Het machtigingenregister MOET duidelijk onderscheid maken tussen dienstverleners en diensten die live danwel in test/pilot fase zijn.
- Het machtigingenregister MOET de mogelijkheid bieden voor het registreren van een algemene bevoegdheid. Een registratie van een dergelijke bevoegdheid betekent dat de uitvoerende natuurlijk persoon alle huidige en toekomstige diensten in de dienstencatalogus mag afnemen.
- Het machtigingenregister MAG in aanvulling op de registratie van een algemene bevoegdheid ook een registratieproces voor een algemene bevoegdheid met beperkingen voor geselecteerde diensten aanbieden.
- Het registreren van machtigingen voor bedrijven en organisaties die niet in het Nederlandse handelsregister zijn ingeschreven vereist verificatie van identificatie van de dienstafnemer en vertegenwoordigingsbevoegdheid in buitenlandse handelsregisters of daarmee vergelijkbare openbare registers. Deelnemers zijn niet verplicht deze functionaliteit aan te bieden, het is een Aanvullende feature.

Alternatieve scenario's

Voor deze use case zijn geen alternatieve scenario's gedefinieerd.

AUC4 Registreren attribuut

In deze use case wordt een attribuut geregistreerd voor gebruik binnen eHerkenning. De invulling van deze use case wordt verder uitgewerkt in Proces aanpassen attribuutcatalogus en hier verder niet beschreven.

AUC5 Registreren identificerend kenmerk beroepsbeoefenaar

In deze use case wordt een identificerend kenmerk van een bepaalde groep beroepsbeoefenaren geregistreerd voor gebruik binnen eHerkenning. De invulling van deze use case wordt verder uitgewerkt in Proces aanpassen attribuutcatalogus en hier verder niet beschreven.

De "Administratie" use cases worden in hoge mate aan de respectievelijke deelnemers die de use case implementeren overgelaten. In dit hoofdstuk worden de eisen die worden gesteld aan de "Administratie" use cases in detail uitgewerkt.

Gebruikersinterface

Dit hoofdstuk beschrijft eisen die worden gesteld aan de gebruikersinterface met de uitvoerende natuurlijk persoon.

Voor eisen in dit hoofdstuk waaraan middelen en of kanalen door hun opzet niet of zeer lastig kunnen voldoen geldt de verplichting in overleg met de beheerorganisatie een acceptabele oplossing te realiseren.

Dialoogbeschrijving

Alle dialoogvensters die door partijen in het herkenningsproces worden ingezet om met de uitvoerende natuurlijk persoon te communiceren ZOUDEN MOETEN voldoen aan de volgende eisen:

- De naam van de partij die het dialoogvenster presenteert (en op dat moment een rol in het herkenningsproces vervult) wordt duidelijk getoond. Zie ook Aanvullende eisen aan eHerkenningsmakelaarschermen.
- De naam van de dienstverlener waar het herkenningsproces door is geïnitieerd of betrekking op heeft wordt duidelijk aan de uitvoerende natuurlijk persoon getoond.
- Het dialoogvenster MAG NIET informatie bevatten die niet rechtstreeks van toepassing is op, of bijdraagt aan het herkenningsproces. Reclame-uitingen of links naar andere webpagina's die buiten het herkenningsproces vallen MOGEN NIET worden opgenomen.
- Het beeldmerk van het product eHerkenning wordt getoond en wel volgens de daarvoor geldende richtlijnen. Zie document Handboek huisstijl.
- De uitvoerende natuurlijk persoon moet in staat zijn de URL en het gepresenteerde SSL certificaat te controleren. Dientengevolge MOGEN schermen NIET ingebed worden, bijvoorbeeld in een mobiele app of een (i)frame. Partijen MOETEN hierop controleren en zonodig het herkenningsproces afbreken.
- Een partij MAG naast bovengenoemde gebruik maken van haar eigen logo's en huisstijl.

Aanvullende eisen aan eHerkenningsmakelaarschermen

De eHerkenningsmakelaar MOET in het kader van gebruik aan de volgende aanvullende eisen voldoen:

- De opsomming van deelnemers in de keuzelijst van de eHerkenningsmakelaar MOET in alfabetische volgorde worden getoond volgens de naam die is opgenomen in het veld "displayname" dat is opgenomen in de metadata, ongeacht hoofd- of kleine letters. Zie Interface specifications.
- De eHerkenningsmakelaar MOET voor stap 3.1 uit GUC3 Aantonen identiteit en stap 4.1 uit GUC4 Aantonen bevoegdheid twee aparte gestandaardiseerde schermen implementeren. De beheerorganisatie stelt hiervoor templates ter beschikking (20140520 HM Schermen.zip). Het template MOET op de volgende wijze worden gevuld:
  - De naam van de dienst en dienstverlener zijn afkomstig uit de dienstencatalogus.
  - De namen van de authenticatiediensten of machtigingenregisters zijn afkomstig uit de metadata.
  - Wanneer dienst 0 (GUC4.2 Authenticatie voor dienst 0) wordt uitgevraagd, komt de dienst en het woord 'voor' ('for' in het Engelse template) te vervallen.
- Op het scherm van de eHerkenningsmakelaar wordt vermeld wat het door de dienstverlener minimaal vereiste betrouwbaarheidsniveau is.
- Het vakje "Onthoud deze keuze" is default aangevinkt, ook indien na annuleren er hernieuwde selectie plaatsvindt. Als gebruiker dit vakje uitvinkt, moet deze selectie onthouden worden door het plaatsen van een cookie. Zie Single sign-on and user sessions.

Toegankelijkheid

Alle dialoogvensters die door partijen in het herkenningsproces worden ingezet MOETEN voldoen aan de eisen die worden gesteld aan niveau 1 (" Toegankelijkheid prioriteit 1") van het Waarmerk drempelvrij.nl (www.drempelvrij.nl). Partijen MOETEN dit aantonen doormiddel van een zelfverklaring en MOGEN dit verder aantonen doormiddel van certificering.

Alle dialoogvensters die door partijen in het registratieproces van middelen worden ingezet MOETEN voldoen aan de eisen die worden gesteld aan niveau 1 ("Toegankelijkheid prioriteit 1") van het Waarmerk drempelvrij.nl. Partijen MOETEN dit aantonen doormiddel van een zelfverklaring en MOGEN dit verder aantonen doormiddel van certificering.

Alle webpagina's in het herkenningsproces MOETEN ten minste in het Nederlands als in het Engels beschikbaar zijn. De registratieprocessen MOGEN ook alleen in het Nederlands worden aangeboden.

Alle webpagina's die door partijen in het herkenningsproces worden ingezet MOETEN functioneren zonder het gebruik van client-side scripting.

Interface specifications

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

This section describes the interface specifications for the traffic between all roles in the network. The messages are based on SAML 2.0, or XACML where applicable.

Versions
Within the network, multiple versions of the interface specifications can be active at the same time. This is done to enable participants and service providers to migrate at a time of their convenience.

Currently, version 1.7 is the most recent version of the interface specifications, while 1.5 is also supported.

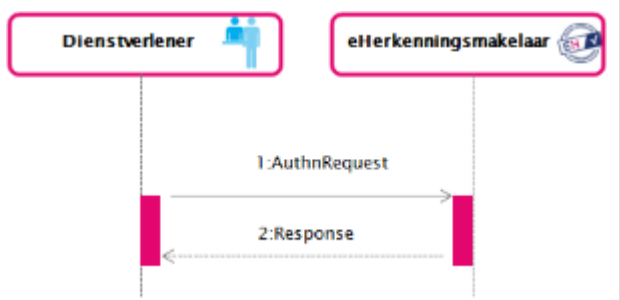
Summary

- Attributes and elements
  - EntityID
  - Level of assurance — eHerkenning distinguishes five different levels of assurance.
  - OIN format — The OIN format is used to indicate participants, service providers and specific types of service consumers and intermediaries. OIN stands for Organization Identifying Number.
    - DigiKoppeling — Logius provides this number to service providers that do not have or do not have their own KvK number. The number from the DigiKoppeling register has the prefix 00000004.
    - FI number — The FI number has the prefix 00000001 or 00000002. The number consists of 9 digits and a 3-digit suffix. For prefix 00000001, the suffix is always 000.
    - KvK nummer — The KvK number has the prefix 00000003. The number consists of the 8-digit KvK number with the suffix 0000.
    - Vestigingsnummer — The branch number has the prefix 00000006. The number consists of the 12-digit branch number.
  - Pseudonyms — In eHerkenning, an executing person may be referred to as follows:
    - Internal pseudonym — The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the acting natural person, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the
    - Specific pseudonym — The specific pseudonym can be created in two ways:
  - SAML attribute elements — This section describes the data elements that occur in messages as SAML Attribute element.
    - AuthorizationRegistryID — An SAML Attribute element with an EntityID from the MR that must be queried in the use case "raadplegen machtigingenregister" (query MR).
    - EherkenningPreferredLanguage — An URL or POST variable containing the language preference of acting natural person.

        - EntityConcernedID (SAML) — An SAML Attribute element with the identifying attribute of the acting service consumer that is represented by the acting natural person (who might be the same).
        - Representation — An SAML Attribute element with an indication whether there is an issue of representation
        - ServiceID (SAML) — An SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.
    - ServiceID — In eHerkenning, all of the services are identified by a ServiceID, a number that is unique in the context of the service provider.
    - XACML attribute elements — This chapter describes all of the XACML data elements defined for eHerkenning. SAML data elements that are defined for eHerkenning are described in SAML attribute elements.
        - ActingEntityID — An XACML Attribute element containing the specific pseudonym of the acting natural person.
        - Action-ID — An XACML Attribute element containing the action ID.
        - AssertionConsumerServiceIndex — An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the eHerkenningsmakelaar.
        - AuthenticationMeansID — An XACML Attribute element containing the internal pseudonym of the acting natural person.
        - EncryptedAttribute — An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the eHerkenning attribute catalogue (e.g. urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail).
        - EntityConcernedID (XACML) — An XACML Attribute element that matches the SAML attribute described in EntityID
        - Intermediates — A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
        - LevelOfAssurance — A XACML Attribute element containing the minimum level of assurance that is required by the service provider.
        - LevelOfAssuranceUsed — An XACML Attribute element containing the level of assurance of the registered authorization.
        - ServiceID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceID.
- Error handling — This chapter describes how errors MUST be handled in the network, in order to inform and serve both users and participants sufficiently.
- General requirements
- Information security requirements — This chapter describes the requirements that apply to the information security measures that are implemented.
    - Digital signature
    - Encryption
    - PKIoverheid
    - Secure connection
    - Synchronize system clocks
- Interface specifications DV-HM 1.7 — This page describes the messages for the interface specification between a DV (service provider) and an HM (broker).
- Interface specifications HM-AD 1.7 — This page describes the messages that are exchanged between a HM (broker) and an AD (identity provider).
- Interface specifications HM-MR 1.7 — This page describes the messages for the interface between a HM (broker) and an MR (entitlements registry).
- Interface specifications HM-MR 1.7 chain authorization — This page describes the messages for the backchannel interface between an HM (broker) and an MR (entitlements registry).
- SAML metadata — This chapter describes the metadata the participants must supply, how the Beheerorganisatie publishes the aggregated metadata, and how it is to be interpreted by the participants.
- Service catalog — This chapter describes the format and publication of the service catalog (Dienstencatalogus).
- Single sign-on and user sessions — Within certain boundaries, single sing-on and user sessions are allowed within eHerkenning. This document describes the technical requirements.

Interface specifications DV-HM 1.7

DV-HM sequence diagram



This page describes the messages for the interface specification between a DV (service provider) and an HM (broker).The interface specification described in this document is used to implement the use case GUC1 Gebruiken eHerkenning als dienstafnemer (Use eHerkenning as service consumer) and MUST (with the exception of Alternative Bindings) be implemented by every eHerkenningsmakelaar and offered to their users, the service providers. This is in order to prevent lock-in and enables middleware suppliers to write generic code that can be used by all eHerkenningsmakelaars.

In the interface described here, the use case GUC1 Gebruiken eHerkenning als dienstafnemer is populated with an SAML 2.0 AuthnRequest and Response.

The specific contents of these messages is described below. A column in a message description that starts with 'SAML:' indicates that this is a standard value within the official SAML specification. A value that starts with 'eHerkenning' indicates that the value is specific to eHerkenning.

[AuthnRequest (1)] [Response (2)] [Authentication assertion] [AttributeStatement] [LogoutRequest] [Alternative binding] [HTTP Redirect binding] [HTTP Artifact binding] [ArtifactResolve] [ArtifactResponse]

AuthnRequest (1)

This section describes regular Authentication Requests.

@ID	SAML: Unique message characteristic
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time the message was created.
@Destination	SAML: URL of the eHerkenningsmakelaar on which the message is offered. MUST match the eHerkenningsmakelaar's metadata.
@Consent	eHerkenning: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
@ForceAuthn	eHerkenning: The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the specification is missing, the AD MAY use an existing SSO session if present.
@IsPassive	eHerkenning: MAY be included. If IsPassive is included, the value MUST be 'false'.
@ProtocolBinding	SAML: MUST NOT be included if AssertionConsumerServiceIndex is used. If it is included, the value MUST be the same as urn:oasis:names:tc:SAML:2.0:bindings:http-POST binding.

@AssertionConsumerServiceIndex	eHerkenning: This attribute element specifies the URL to which the HM sends the response for the DV. This index refers to a URL in the service provider's metadata. In order to use this field, the HM and the DV MUST specify indices with URLs. The value of AssertionConsumerServiceIndex MUST match an index of an AssertionConsumerService element in the service provider's metadata. If neither the AssertionConsumerServiceIndex or the AssertionConsumerServiceUrl are included, the broker MUST send the response to the endpoint in the metadata that is marked with 'isDefault=true'.
@AssertionConsumerServiceURL	SAML: AssertionConsumerServiceUrl MAY be included if an AssertionConsumerServiceIndex is not included. If the AssertionConsumerServiceUrl is included, the participant MUST check whether the AssertionConsumerServiceUrl is included in the service provider's SAML metadata. If it is not included in the metadata, the participant MUST reject the message with the status code RequestDenied.
@AttributeConsumingServiceIndex	SAML: MAY contain an index that matches an AttributeConsumingService in the service provider's metadata. If the AttributeConsumingServiceIndex is not included, the participant MUST use the AttributeConsumingService that is marked with 'isDefault=true'. The AttributeConsumingService MUST contain exactly one attribute with a name that is the same as a long formatted ServiceID. ⓘ An application that cannot pass an AttributeConsumingServiceIndex can now retrieve different services and/or attribute contracts by exchanging metadata between different EntityIDs. Current applications for the 1.5 interface and earlier versions can include an AttributeConsumingService in the metadata for the different services for which the Index is the same as the short ServiceID. This enables the current systems to continue working without hindrance
@ProviderName	eHerkenning: MAY be included, but MUST be ignored by the eHerkenningsmakelaar The eHerkenningsmakelaar also uses the ProviderName element, but populates it differently.
Issuer	eHerkenning: MUST contain the EntityID of the service provider. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the service provider for the enveloped message.
Extensions	eHerkenning: Optional element If the different types of service consumers that can access a service are included in the request (this MUST be a subset of the types that are in the service catalogue), or if the additional attributes are retrieved (they MAY be a superset of what is included in the DV metadata) one RequestedAttributes element MUST be included here. The RequestedAttributes element CAN ONLY contain attributes that are contained in the attribute catalogue (see Attribuutcatalogus). These attributes MUST be included as Name of a RequestedAttribute. Other XML attributes MUST NOT be included. Other elements MUST NOT be included. An AD MAY ignore a request for additional attributes, but MUST NOT reject the whole message.
Subject	eHerkenning: MUST NOT be included

NameIDPolicy	eHerkenning: MUST NOT be included.
Conditions	eHerkenning: MUST NOT be included.
RequestedAuthnContext	eHerkenning: MUST contain an attribute Comparison='minimum' and an element AuthnContextClassRef that contains the minimum Level of assurance required by the service provider.
Scoping	eHerkenning: MUST NOT be included

Example message

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ForceAuthn="true" Destination=" " AssertionConsumerServiceIndex=" "
AttributeConsumingServiceIndex="2" ID=" " IssueInstant=" " Version="2.0"
ProviderName=" ">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
 </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
   <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
   <ds:Reference URI=" ">
    <ds:Transforms>
     <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>
                </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
 </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:KeyName>
  </ds:KeyName>
  </ds:KeyInfo>
 </ds:Signature>
 <samlp:Extensions>
    <ehsamlp:RequestedAttributes>
        <md:RequestedAttribute
Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"/>
       <md:RequestedAttribute
Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail"/>
       <md:RequestedAttribute
Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalPhone"/>
    </ehsamlp:RequestedAttributes>
 </samlp:Extensions>
 <samlp:RequestedAuthnContext Comparison="minimum">
  <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        </saml:AuthnContextClassRef>
 </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Response (2)

For chain authorizations, the identification number of the represented service consumer and the specific pseudonym of the acting natural person are included in the assertion for the HM in the same way as for single authorizations. The additional information about the chain is stored in a separate attribute.

Note: The HM will not identify the MRs from which the underlying assertions originate. Additional attributes relate to the represented service consumer or the executing natural person. There is no mechanism to include an additional attribute that relates specifically to an intermediary.

@ID	SAML: Unique message characteristic.
@InResponseTo	SAML: Unique attribute of the AuthnRequest for which this Response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time the message was created.
@Destination	SAML: URL of the service provider on which the message is offered. MUST match the service provider's metadata.
@Consent	eHerkenning: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	eHerkenning: MUST contain the EntityID of the eHerkenningsmakelaar. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the service provider for the enveloped message.
Extensions	eHerkenning: MUST NOT be included.
Status	eHerkenning: MUST contain a StatusCode element with the status of the authentication. In the event of a cancellation or error, the element MUST be populated with the value AuthnFailed. See Error handling. StatusDetail MUST NOT be included.
Assertion	eHerkenning: MUST contain an authentication assertion that contains an authorization assertion (see the next section).

Example message

› Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" "
InResponseTo=" " Version="2.0" Destination=" " IssueInstant=" ">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
   <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
   <ds:Reference URI=" ">
    <ds:Transforms>
     <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>
                </ds:DigestValue>
   </ds:Reference>
```

```
  </ds:SignedInfo>
  <ds:SignatureValue>
        </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:KeyName>
  </ds:KeyName>
  </ds:KeyInfo>
 </ds:Signature>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
        </samlp:StatusCode>
 </samlp:Status>
 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
ID=" " IssueInstant=" ">
  <saml:Issuer>
        </saml:Issuer>
  <saml:Subject>
   <saml:NameID>
            </saml:NameID>
   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData Recipient=" " NotOnOrAfter=" ">
                </saml:SubjectConfirmationData>
   </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore=" " NotOnOrAfter=" ">
   <saml:AudienceRestriction>
    <saml:Audience>
                </saml:Audience>
   </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant=" ">
   <saml:AuthnContext>
    <saml:AuthnContextClassRef>
                </saml:AuthnContextClassRef>
    <saml:AuthenticatingAuthority>
                </saml:AuthenticatingAuthority>
   </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
   <saml:Attribute Name="urn:nl:eherkenning:1.0:ServiceID">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
                </saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="urn:nl:eherkenning:1.0:EntityConcernedID">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
                </saml:AttributeValue>
   </saml:Attribute>

                                    <saml:EncryptedAttribute
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                                                <xenc:EncryptedData
mlns:xenc=http://www.w3.org/2001/04/xmlenc# Id="Encrypted_DATA_ID"
Type="http://www.w3.org/2001/04/xmlenc#Element">
```

```
                                                <xenc:EncryptionMethod
Algorithm= "http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                                                <ds:KeyInfo>
                                                      <ds:Keyname>
</ds:Keyname>
                                                </ds:KeyInfo>
                                                <xenc:CipherData>
                                                      <xenc:CipherValue>
</xenc:CipherValue>
                                                </xenc:CipherData>
                                          </xenc:EncryptedData>
                                    </saml:EncryptedAttribute>
```

```
  </saml:AttributeStatement>
 </saml:Assertion>
</samlp:Response>
```

Authentication assertion

Assertion	@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
	@ID	SAML: Unique reference to the assertion.
	@IssueInstant	SAML: Time the assertion was created.
	Issuer	eHerkenning: MUST contain the EntityID of the eHerkenningsmakelaar The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
	Signature	eHerkenning: MUST NOT be included
	Subject	eHerkenning: MUST contain a NameID element containing the specific pseudonym of the acting natural person. The NameID element MUST have a NameQualifier attribute that is populated with the EntityID for the MR. A SubjectConfirmation element that meets the Web Browser SSO profile MUST be included. Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included.
	Conditions	eHerkenning: MUST be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver. An Audience element in the AudienceRestriction element that meets the Web Browser SSO profile MUST be included. Other Audience elements MUST NOT be included. Other Conditions MUST NOT be included.
	Advice	eHerkenning: MUST NOT be included
	AuthnStatement	eHerkenning: The attribute AuthnInstant MUST contain the authentication time. The AuthnContext element MUST contain an AuthnContextClassRef element that contains the Level of assurance that was used. The AuthenticatingAuthority element MUST be populated with the EntityID of the AD that performed the authentication. Other attributes and elements MUST NOT be included. The assurance level used MUST be the lowest in the authentication assertion of the AD and the authorization assertion of the MR.
	AttributeStatement	eHerkenning: MUST contain an AttributeStatement in accordance with the following section. Other AttributeStatement elements MUST NOT be included.

AttributeStatement

Part of the authentication assertion	AttributeStatement	eHerkenning: MUST contain the attribute ServiceID (long format) and exactly one element EntityConcernedID that identifies the service consumer (contains a name that identifies the type of identification number, see Identificerende kenmerken) MAY contain the attribute IntermediateEntityID (contains a name that specifies the type of identification number, see Identificerende kenmerken). If the EntityConcernedID contains a KvK number, a second EntityConcernedID populated with the branch number (see Attribuutcatalogus) may be included. If this is included, an additional EntityConcernedID must be included, namely urn:nl:eherkenning:1.7:EntityConcernedID:SubdossierNr. This extra requirement will expire when no such numbers are provided by the Kamer van Koophandel anymore. Additional attributes that are requested by the service provider and provided by the AD and/or MR as EncryptedAttribute, MUST be included here. Other attributes MUST NOT be included.

LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied, although considering that the logout message is sent to the AD via the eHerkenningsmakelaar. Only supported, is the service provider's LogoutRequest where the acting natural person chooses to log out from the authentication.The interface for this message is described below.

@ID	SAML: Unique message characteristic
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time the message was created
@Destination	SAML: URL of the eHerkenningsmakelaar on which the message is offered.
NameID	eHerkenning: MUST contain a NameID element that contains the specific pseudonym of the acting natural person.
Issuer	eHerkenning: MUST contain the EntityID of the service provider.
Signature	eHerkenning: MUST contain the Digital signature of the service provider for the enveloped message.

Alternative binding

The following rules apply when the messages for the alternative binding are exchanged.

HTTP Redirect binding

The implementation of the HTTP Redirect binding must meet the following requirements:

- The AuthnRequest message is the same as the message described above, but MUST NOT contain a <ds:Signature> element.
- The message MUST be compressed using the DEFLATE method and in turn represented in Base-64 encoding.
- The compressed and coded message MUST be added to the URL as a query string parameter and MUST be designated as SAMLRequest.
- If RelayState data is included in the HTTP Redirect message, it must be encoded separately and added to the URL as a query string parameter and MUST be designated as RelayState. If a RelayState is not provided, the whole parameter MUST be absent in the URL.
- A digital signature MUST be calculated over the part of the URL SAMLRequest=value&RelayState=value. This digital signature MUST be generated as described in Digital signature. The digital signature MUST be included as a query string parameter. This parameter is designated as Signature.

HTTP Artifact binding

For the implementation of HTTP Artifact binding, requirements are only imposed on the ArtifactResolve and

ArtifactResponse messages.

ArtifactResolve

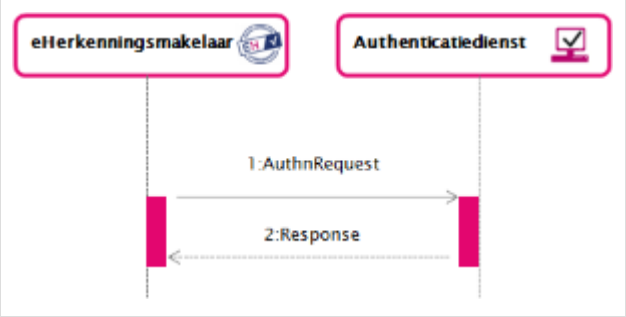
@ID	SAML: Unique message characteristic.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	eHerkenning: MUST NOT be included.
@Consent	eHerkenning: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	eHerkenning: MUST contain the EntityID of the service provider. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the service provider for the enveloped message.
Extensions	eHerkenning: MUST NOT be included.
Artifact	SAML: Contains the Artifact that was received as query parameter.

ArtifactResponse

@ID	SAML: Unique message characteristic.
@InResponseTo	SAML: Unique characteristic of the AuthnRequest for which this Response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	eHerkenning: MUST NOT be included
@Consent	eHerkenning: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	eHerkenning: MUST contain the EntityID of the eHerkenningsmakelaar. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the service provider for the enveloped message.
Extensions	eHerkenning: MUST NOT be included.
Status	eHerkenning: MUST contain a StatusCode element with the status of the authentication. In the event of a cancellation or error, the element MUST be populated with the value AuthnFailed. See also Error handling. StatusDetail MUST NOT be included.
any ##any	eHerkenning: MUST contain a Response message (see above). This message MUST NOT contain an <ds:Signature> element.

Interface specifications HM-AD 1.7

Sequence diagram HM-AD



This page describes the messages that are exchanged between a HM (broker) and an AD (identity provider).In the interface described here, the use case GUC3 Aantonen identiteit consists of an SAML 2.0 AuthnRequest and Response. The specific content of these messages is described below. Detailed information about the value of fields can be found in Attributes and elements.

A column in a message description that starts with 'SAML' indicates that this is the standard value. A value that starts with 'eHerkenning' indicates that the value is specific to eHerkenning.

[AuthnRequest (1)] [Response (2)] [Authentication assertion] [LogoutRequest]

AuthnRequest (1)

@ID	SAML: Unique message attribute
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the "Authenticatiedienst"on which the message is offered. MUST match the eHerkenningsMakelaar's metadata.
@Consent	eHerkenning: MUST NOT be included.
@ForceAuthn	The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the specification is missing, the "Authenticatiedienst" MAY use an existing SSO session if one is open.
@IsPassive	eHerkenning: MAY be included. If IsPassive is included, the value MUST be 'false'.
@ProtocolBinding	SAML: MUST NOT be included because AssertionConsumerServiceIndex is required in eHerkenning.
@AssertionConsumerServiceIndex	eHerkenning: This attribute element indicates the URL to which the response must be sent. The value of AssertionConsumerServiceIndexMUST match an index at the assertion consumer service in the eHerkenningsMakelaar's metadata.
@AssertionConsumerServiceURL	SAML: MUST NOT be included because AssertionConsumerServiceIndex is required in eHerkenning.
@AttributeConsumingServiceIndex	eHerkenning: The value MUST be '4'. Indicates that it is about the interface described in this document.
@ProviderName	eHerkenning: MUST match the OrganizationDisplayName of the service provider in the Service catalog.
Issuer	eHerkenning: MUST contain the EntityID of the eHerkenningsMakelaar. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the service provider for the enveloped message.

Extensions	eHerkenning: MUST contain the attribute ServiceID (long format). If the different types of service consumers that can access a service provided by a service provided are included in the request, or if the service provider queries additional attributes in the metadata or the request, they MUST be included here. If additional attributes are defined in the request as well as in the metadata, all the attributes MUST be included here. To this extent, one RequestedAttributes element MUST be included containing the RequestedAttribute elements in the service provider's request. The eHerkenningsMakelaar MAY only include the attributes that can and may be provided by the respective "Authenticatiedienst". See Attribuutcatalogus and SAML metadata. Other XML attributes MUST NOT be included. Other elements MUST NOT be included. An "Authenticatiedienst" MAY ignore a request for additional attributes, but MUST NOT reject the whole message.
Subject	eHerkenning: MUST NOT be included
NameIDPolicy	eHerkenning: MUST NOT be included.
Conditions	eHerkenning: MUST NOT be included.
RequestedAuthnContext	eHerkenning: MUST contain an attribute Comparison='minimum' and an element AuthnContextClassRef that contains the minimum Level of assurance required by the service provider.
Scoping	eHerkenning: MUST NOT be included

Example message

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" "
Version="2.0" IssueInstant=" " Destination=" " ForceAuthn="true"
AssertionConsumerServiceIndex=" " AttributeConsumingServiceIndex="4"
ProviderName=" ">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI=" ">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
</ds:SignatureValue>
<ds:KeyInfo>
<ds:KeyName>
</ds:KeyName>
</ds:KeyInfo>
</ds:Signature>
<samlp:Extensions>
<ehsamlp:RequestedAttributes>
<md:RequestedAttribute
Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"
IsRequired="false"/>
</ehsamlp:RequestedAttributes> </samlp:Extensions>
<samlp:RequestedAuthnContext Comparison="minimum">
<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Response (2)

@ID	SAML: Unique message characteristic.
@InResponseTo	SAML: Unique attribute of the AuthnRequest for which this Response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'
@IssueInstant	SAML: Time at which the message was created.

@Destination	SAML: URL of the eHerkenningsMakelaar on which the message is offered. MUST match the service provider's metadata.
@Consent	eHerkenning: MUST NOT be included.
Issuer	eHerkenning: MUST contain the EntityID of the "Authenticatiedienst". The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the "Authenticatiedienst" for the enveloped message.
Extensions	eHerkenning: MUST NOT be included
Status	eHerkenning: MUST be filled conform SAML 2.0 specs when the request is successfully processed. MUST be filled according to Error handling in case of an error or when the request was cancelled.
Assertion	eHerkenning: MUST contain an assertion about the authentication (see the next section).

Authentication assertion

Assertion	@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'
	@ID	SAML: Unique reference to the assertion
	@IssueInstant	SAML: Time at which the assertion was created
	Issuer	eHerkenning: MUST contain the EntityID of the "Authenticatiedienst". The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
	Signature	eHerkenning: MUST NOT be included
	Subject	eHerkenning: In the case of representation, MUST contain a NameID element containing the Internal pseudonym of the acting natural person. In the case of an acting citizen, consumer or professional, MUST contain a NameID element containing the Specific pseudonym of the acting natural person. The NameID element MUST contain the attribute NameQualifier containing the OIN format of the KvK number of the "Authenticatiedienst". A SubjectConfirmation element that meets the Web Browser SSO profile MUST be included. Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included.
	Conditions	eHerkenning: MUST be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver. An Audience element in the AudienceRestriction element that meets the Web Browser SSO profile MUST be included. Other Audience elements MUST NOT be included. Other Conditions MUST NOT be included.
	Advice	eHerkenning: MUST NOT be included

	AuthnStatement	eHerkenning: The attribute AuthnInstant MUST contain the time of authentication. The AuthnContext element MUST contain an AuthnContextClassRef element containing the level of assurance at which authentication took place and an AuthenticatingAuthority element containing the OIN format of the KvK number of the "Authenticatiedienst". In the case of proxying, AuthenticatingAuthority element MUST be populated with a unique identifying attribute for the party that carried out the authentication. Other attributes and elements MUST NOT be included.
	Optional Attribute-Statement	eHerkenning: MUST be included if StatusCode is 'Success'. MUST NOT be included otherwise. When this is included, the following requirements apply: • Representation MUST be included. See Identificerende kenmerken. • AuthorizationRegistryID MAY be included. See EntityID. • In the case of non-representation (meaning acting by a citizen, consumer or a professional) exactly one attribute that identifies the service consumer MUST be included. The attribute MUST match one of the possible service consumers that is allowed to use the service. • Additional attributes requested by the eHerkenningsMakelaar that are available and for which the acting natural person has granted user consent (during authentication or previously granted consent) MAY be included here only if the StatusCode is 'Success'. • Additional attributes MUST be included as EncryptedAttribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the attribute name in the eHerkenning attribute catalogue (e.g. urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail). • The service provider's service certificate that is included in the service catalogue MUST be used for encryption. A level of assurance is also passed for each EncryptedAttribute. • A cipher value is included in the encrypted attribute. This cipher value contains the encrypted value of the request attribute that is encrypted with the key of the DV in the service catalogue. Example for ActingPersonName › Expand source `<saml:Attribute Name= "urn:nl:eherkenning1.3:AdditionalAttribute: ActingPersonName "> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"> </saml:AttributeValue> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="eh:betrouwbaarheidsniveau"> </saml:AttributeValue> </saml:Attribute>` • Other AttributeStatement elements MUST NOT be included.

Example message › Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" "
InResponseTo=" " Version="2.0" Destination=" " IssueInstant=" " Consent=" ">
```

```
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI=" ">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
</ds:SignatureValue>
<ds:KeyInfo>
<ds:KeyName>
</ds:KeyName>
</ds:KeyInfo>
</ds:Signature>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
</samlp:StatusCode>
</samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
ID=" " IssueInstant=" ">
<saml:Issuer>
</saml:Issuer>
<saml:Subject>
<saml:NameID NameQualifier=" ">
</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData Recipient=" " NotOnOrAfter=" ">
</saml:SubjectConfirmationData>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore=" " NotOnOrAfter=" ">
<saml:AudienceRestriction>
<saml:Audience>
</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant=" ">
<saml:AuthnContext>
<saml:AuthnContextClassRef>
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
Id="_DE46C6F5E2E3111255D3A715C4760656">
```

```
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<xenc:EncryptedKey>
<xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep172mgf1p"/>
<ds:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>62355fbd1f624503c5c9677402ecca00ef1f6277</ds:KeyName>
</ds:KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>.....</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedKey>
</ds:KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>.......</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
```

```
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

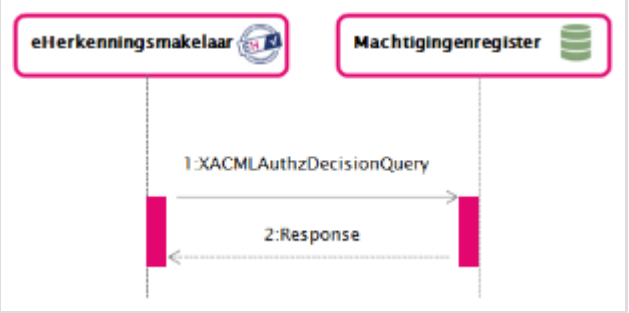
LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied on the understanding that the logout message is sent to the "Authenticatiedienst" through the eHerkennningsMakelaar. The interface for this message is described below.

@ID	SAML: Unique message attribute
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the "Authenticatiedienst" on which the message is offered.
NameID	eHerkenning: MUST contain a NameID element, this MAY NOT contain the Internal pseudonym of the acting natural person.
Issuer	eHerkenning: MUST contain the EntityID of the eHerkenningsMakelaar.
Signature	eHerkenning: MUST contain the Digital signature of the eHerkenningsMakelaar for the enveloped message.

Interface specifications HM-MR 1.7

Sequence diagram HM-MR



This page describes the messages for the interface between a HM (broker) and an MR (entitlements registry).In the interface described here, the use case GUC4 Aantonen bevoegdheid consists of an SAML 2.0 AuthnRequest and Response.

A column in a message description that starts with 'SAML:' or 'XACML:' indicates that this is the standard value. A value that starts with 'eHerkenning' indicates that the value is specific to eHerkenning.

[XACMLAuthzDecisionQuery (1)] [Response (2)] [Authorization assertion]

XACMLAuthzDecisionQuery (1)

@ID	SAML: Unique message attribute
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.

@ReturnContext		eHerkenning: The value MUST be 'true'.
@Destination		SAML: URL of the “machtigingenregister” on which the message is offered. MUST match the “machtigingenregister's” SAML metadata.
@Consent		eHerkenning: MUST NOT be included.
@InputContextOnly		eHerkenning: MUST NOT be included
Issuer		eHerkenning: MUST contain the EntityID of the eHerkenningsmakelaar. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature		eHerkenning: MUST contain the Digital signature of the eHerkenningsmakelaar for the enveloped message.
Extensions		eHerkenning: MUST contain an XACML Attribute-element with AttributeID AssertionConsumerServiceIndex.
Request	Subject	eHerkenning: MUST contain AuthenticationMeansID.
	Resource	eHerkenning: MUST contain two XACML attributes, ServiceID (long format) and LevelOfAssurance. If the different types of service consumers that can access a service provided by a service provided are included in the request, or if the service provider queries additional attributes in the metadata or the request, they MUST be included here. If additional attributes are defined in the request as well as in the metadata, all the attributes MUST be included here. The eHerkenningsmakelaar MAY only include the attributes that can and may be provided by the respective “machtigingenregister”. See Attribuutcatalogus and SAML metadata Other XML attributes MUST NOT be included. Other elements MUST NOT be included. An “machtigingenregister” MAY ignore requests for additional attributes, but MUST NOT reject the message.
	Action	eHerkenning: MUST contain the XACML attribute Action-ID.
	Environment	eHerkenning: MUST be empty.

Example message

› Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml-samlp:XACMLAuthzDecisionQuery
xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os" ID=" "
Version="2.0" IssueInstant=" " ReturnContext="true" Destination=" ">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
   <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
   <ds:Reference URI=" ">
    <ds:Transforms>
     <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>
                </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
        </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:KeyName>
  </ds:KeyName>
  </ds:KeyInfo>
 </ds:Signature>
 <extension base="samlp:RequestAbstractType">
  <attribute name="AssertionConsumerServiceIndex"
DataType="http://www.w3.org/2001/XMLSchema#unsignedShort" Issuer=" ">
   <AttributeValue>
 </AttributeValue>
  </attribute>
 </extension>
 <xacml-context:Request
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <xacml-context:Subject>
   <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:AuthenticationMeansID"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" ">
    <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
   </xacml-context:Attribute>
  </xacml-context:Subject>
  <xacml-context:Resource>
   <xacml-context:Attribute AttributeId="urn:nl:eherkenning:1.0:ServiceID"
DataType="http://www.w3.org/2001/XMLSchema#string">
    <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
   </xacml-context:Attribute>
   <xacml-context:Attribute AttributeId="urn:nl:eherkenning:1.0:LevelOfAssurance"
DataType="http://www.w3.org/2001/XMLSchema#string">
    <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
   </xacml-context:Attribute>
   <xacml-context:Attribute
AttributeId="urn:nl:eherkenning1.3:AdditionalAttribute:BusinessName"
DataType="http://www.w3.org/2001/XMLSchema#string">
    <xacml-context:AttributeValue>
    </xacml-context:AttributeValue>
   </xacml-context:Attribute>
 </xacml-context:Resource>
  <xacml-context:Action>
   <xacml-context:Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
    <xacml-context:AttributeValue>Authenticate</xacml-context:AttributeValue>
   </xacml-context:Attribute>
  </xacml-context:Action>
```

```
<xacml-context:Environment>
```

```
        </xacml-context:Environment>
 </xacml-context:Request>
</xacml-samlp:XACMLAuthzDecisionQuery>
```

Response (2)

@ID	SAML: Unique message attribute
@InResponseTo	SAML: Unique attribute of the XACMLAuthzDecisionQuery to which this Response message is the answer.
@Version	ASAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the eHerkenningsmakelaar on which the message is offered. MUST match the service provider's SAML metadata.
@Consent	eHerkenning: MUST NOT be included
Issuer	eHerkenning: MUST contain the EntityID of the "machtigingenregister". The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	eHerkenning: MUST contain the Digital signature of the "machtigingenregister" for the enveloped message.
Extensions	eHerkenning: MUST NOT be included
Status	eHerkenning: MUST be filled conform SAML 2.0 specs when the request is successfully processed. MUST be filled according to Error handling in case of an error or when the request was cancelled.
Assertion	eHerkenning: MUST contain an assertion about the authorization (see the next section).

Authorization assertion

Assertion	@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
	@ID	SAML: Unique reference to the assertion
	@IssueInstant	SAML: Time at which the assertion was created
	Issuer	eHerkenning: MUST contain the EntityID of the "machtigingenregister". The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
	Signature	eHerkenning: MUST contain the Digital signature of the "machtigingenregister" for the enveloped assertion.
	Subject	eHerkenning: MUST NOT be included
	Conditions	eHerkenning: MAY be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver. Other Conditions MUST NOT be included.
	Advice	eHerkenning: MUST NOT be included
	XACMLAuthz-Decision Statement	eHerkenning: MUST contain an SAML Statement of the type XACMLAuthzDecisionStatementType. See below.

XACMLAuthzDecision Statement	Response	Result	@ResourceID	eHerkenning: MUST NOT be included
			Decision	XACML: One of the values allowed in XACML 2.0. In the event of a cancellation or error, the element MUST be populated with the value Deny. See also Error handling.
			Obligations	Obligation urn:nl:eherkenning:1.7:RequireConfirmationFromNextMR FulfillOn=Permit AttributeAssignment urn:nl:eherkenning:1.0:AuthorizationRegistryID = <MR2> (see EntityID) eHerkenning: In the event of chain authorization, such is established by the first "machtigingenregister", which then specifies, by means of an Obligation, that the second link MUST be verified or Decision = Permit is otherwise invalid.
			Status	eHerkenning: XACML: must be filled with one of the values that are allowed according to the XACML 2.0 specifications
	Request		Subject	eHerkenning: Contains the XACMLAuthzDecisionQuery Subject element with all of the attributes stated in the request. See XACMLAuthzDecisionQuery (above). The request included in the AuthenticationMeansID MUST be deleted. If the Decision is 'Permit', the attribute ActingEntityID MUST be included. See EntityID.

			Resource	eHerkenning: MUST contain the attribute-elements contained in the resource element from the request.
				
				If the Decision is 'Permit'
				• LevelOfAssuranceUsed MUST be included. See Level of assurance
				• MUST include exactly one attribute that indentifies the service consumer (see Identificerende kenmerken).
				  • If the EntityConcernedID contains a KvK number, a second EntityConcernedID populated with the branch number (see EntityConcernedID:Vestigingsnr) MAY be included.
				  • If Obligation is included: Intermediaries (Identifier or intermediary1) must be included. See Intermediates.
				
				EncryptedAttributes MAY be included if additional attributes are requested by the eHerkenningsmakelaar and user consent was granted for these attributes by an acting natural person or the authorization manager of the represented service consumer/intermediary (during the transaction or through prior consent) and if the Decision is 'Permit'.
				
				NextAuthorizationRegistryID MAY be included. See EntityID.
				
				Other attributes MUST NOT be included.

			Action	eHerkenning: MUST be the same as the Action element in the request. See XACMLAuthzDecisionQuery (above).
			Environment	eHerkenning: MUST be empty.

Example message

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="
InResponseTo=" " Version="2.0" IssueInstant=" " Destination=" ">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    </saml:Issuer>
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
   <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
   <ds:Reference URI=" ">
    <ds:Transforms>
     <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>
                </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
        </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:KeyName>
  </ds:KeyName>
  </ds:KeyInfo>
 </ds:Signature>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success">
        </samlp:StatusCode>
 </samlp:Status>
 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
ID=" " IssueInstant=" ">
  <saml:Issuer>
        </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference URI=" ">
     <ds:Transforms>
      <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
     <ds:DigestValue>
                  </ds:DigestValue>
    </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue>
```

```
            </ds:SignatureValue>
   <ds:KeyInfo>
    <ds:KeyName>
  </ds:KeyName>
   </ds:KeyInfo>
  </ds:Signature>
  <saml:Conditions NotBefore=" " NotOnOrAfter=" ">
        </saml:Conditions>
  <saml:Statement xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
   <xacml-context:Response
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
    <xacml-context:Result>
     <xacml-context:Decision>Permit</xacml-context:Decision>
     <xacml-context:Status>
      <xacml-context:StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok">
                        </xacml-context:StatusCode>
     </xacml-context:Status>
    </xacml-context:Result>
   </xacml-context:Response>
   <xacml-context:Request
xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
    <xacml-context:Subject>
     <xacml-context:Attribute AttributeId="urn:nl:eherkenning:1.0:ActingEntityID"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=" ">
      <xacml-context:AttributeValue>
                        </xacml-context:AttributeValue>
     </xacml-context:Attribute>
    </xacml-context:Subject>
    <xacml-context:Resource>
     <xacml-context:Attribute AttributeId="urn:nl:eherkenning:1.0:ServiceID"
DataType="http://www.w3.org/2001/XMLSchema#string">
      <xacml-context:AttributeValue>
                        </xacml-context:AttributeValue>
     </xacml-context:Attribute>
     <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:LevelOfAssurance"
DataType="http://www.w3.org/2001/XMLSchema#string">
      <xacml-context:AttributeValue>
                        </xacml-context:AttributeValue>
     </xacml-context:Attribute>
     <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:LevelOfAssuranceUsed"
DataType="http://www.w3.org/2001/XMLSchema#string">
      <xacml-context:AttributeValue>
                        </xacml-context:AttributeValue>
     </xacml-context:Attribute>
     <xacml-context:Attribute
AttributeId="urn:nl:eherkenning:1.0:EntityConcernedID"
DataType="http://www.w3.org/2001/XMLSchema#string">
      <xacml-context:AttributeValue>
                        </xacml-context:AttributeValue>
     </xacml-context:Attribute>
     <xacml-context:ResourceContent>
```

```
<saml:EncryptedAttribute>
<xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
Id="_DE46C6F5E2E3111255D3A715C4760656">
 <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <xenc:EncryptedKey>
   <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
   <ds:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>62355fbd1f624503c5c9677402ecca00ef1f6277</ds:KeyName>
   </ds:KeyInfo>
   <xenc:CipherData>
    <xenc:CipherValue>.....</xenc:CipherValue>
   </xenc:CipherData>
  </xenc:EncryptedKey>
 </ds:KeyInfo>
 <xenc:CipherData>
  <xenc:CipherValue>.......</xenc:CipherValue>
 </xenc:CipherData>
</xenc:EncryptedData>
                                      </saml:EncryptedAttribute>
       </xacml-context:ResourceContent>
       </xacml-context:Resource>
    <xacml-context:Action>
     <xacml-context:Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
      <xacml-context:AttributeValue>Authenticate</xacml-context:AttributeValue>
     </xacml-context:Attribute>
    </xacml-context:Action>
    <xacml-context:Environment>
                </xacml-context:Environment>
   </xacml-context:Request>
  </saml:Statement>
 </saml:Assertion>
```

```
</samlp:Response>
```

Interface specifications HM-MR 1.7 chain authorization

This page describes the messages for the backchannel interface between an HM (broker) and an MR (entitlements registry).

In order to use chain authorization, the entire chain of the service consumer all the way to the acting natural person MUST be known by the first "machtigingenregister" (MR), the authorization where the user interaction is taking place.

eHerkenning only supports chains with one intermediary:

- User G (acting natural person) > Intermediary A > Service consumer B.

The authorization that the user may act on behalf of Intermediary A is registered as authorization with the first MR. The information that there is an authorization from Service consumer B for Intermediary, and in which MR it is stored, MUST also be known by the first MR (or retrieved at the time of authentication).

The first MR responds as follows:

- The specific pseudonym of the user in attribute urn:nl:eherkenning:1.0:ActingEntityID
- The OIN of Intermediary A in attribute urn:nl:eherkenning:1.7:Intermediates

For the purpose of scalability, this is a multi-value attribute. At this point in time Intermediaries MUST contain a maximum of one value.

The identification attribute of Service consumer B is stored in attribute urn:nl:eherkenning:1.7:EntityConcernedID:KvKnr (in the case of an KvK number, it can also be another type of identification attribute, see Identificerende kenmerken.

The HM sends this information (all above specified attributes) to the MR that is specified in the urn:nl:eHerkenning:1.7:RequireConfirmationFromNextMR element in Obligations, considering that it has registered the authorization of Service consumer B for Intermediary A. The next MR recognizes this as a claim confirmation request based on the absence of the Intermediary attribute

The mechanism and protocol to exchange information between MRs about where which authorizations are stored is outside the scope of the eHerkenning specifications. The processing of the next request is explained below.

Verification of the next chain query

If the HM receives an assertion from an MR with an obligation, the next request MUST be made. This XACMLAuthzDecisionQuery is submitted through an SOAP backchannel with an XACML query in the message body.

This query resembles the XACMLAuthzDecisionQuery as described in Interface specifications HM-MR 1.7, but differs on the following aspects:

- @Destination: SAML: URL of the "machtigingenregister" on which the message is offered. MUST match the machtigingenregister's SAML metadata. This URL is received in the response from the above "machtigingenregister" (or, if it is missing, to the acting natural person).
- Request > Subject
  - eHerkenning: MUST contain ActingEntityID.
  - MUST contain EntityConcernedID (XACML).
  - MUST contain the intermediaries attribute as received in the response to the above "machtigingenregister"

Verification of the following chain response

The respective MR issues a response that resembles the response described in Interface specifications HM-MR 1.7, but differs on the following aspects:

- Signature:
  eHerkenning: MUST contain the Digital signature of the "machtigingenregister" for the enveloped assertion.
- XACMLAuthz Decision Statement | Request | Subject

eHerkenning: Contains the XACMLAuthzDecisionQuery Subject element with all of the attributes stated in the request including the ActingEntityID and Intermediates.

General requirements

SAML Web Browser SSO Profile

The SAML Web Browser SSO Profile MUST be used for the interface described in this document. Optionally, an extension can be used for retrieving attributes.

Bindings

Different bindings can be used in SAML to transport messages between parties.

HTTP Post Binding

Every eHerkenningsMakelaar MUST implement the HTTP POST binding (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST) for the interface described in this document and offer it to their customers, the service providers. An eHerkenningsmakelaar MAY also implement the alternative binding and offer it as described in the next section.

Alternative binding

As a concession to providers, this document also describes an alternative, optional binding. This is the binding that is used for the interface between the service provider and the eHerkenningsmakelaar in pilot implementations. eHerkenningsmakelaars MAY implement and offer this binding.

The described alternative binding consists of using a combination of the HTTP Redirect (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect) and HTTP Artifact (urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact) binding, whereby the request is made by an HTTP Redirect binding and the response is returned by an HTTP Artifact binding.

The recommendations regarding the composition of a artifact (section 3.6.4 of the SAML 2.0 binding specification http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf) MUST be implemented.

Relay State

Every SAML request message MAY contain RelayState data. The response to an SAML request with RelayState data MUST also contain this RelayState data. The content of the RelayState MUST NOT exceed 80 byte and MUST be protected against changes by the party creating the RelayState.

Namespace aliases

Perhaps superfluously, it must be said that the parties are free to choose the aliases they use for the abbreviations of namespaces in tags.

HTTP Headers

The following HTTP headers MUST be used for all content that is sent to the browser of an acting natural person:

- Cache-Control with value "no-cache, no-store"
- Pragma with value "no-cache"

Optional elements and attributes

Optional elements and attributes MAY be included in the messages. These elements MUST be populated according to the specifications and MUST NOT be empty.

Versioning

Because different versions of the interface specifications (e.g. 1.1, 1.5 and 1.7) must be distinguished from each other at the interface level, message versioning MUST be used in the implemented interface. Because SAML 2.0 messages do not have a field for this and it is not desirable to use an extension in the messages, participants MUST link the URL on which SAML messages can be offered to a version of the framework in the published metadata. For example, https://www.deelnemer.nl/SAML-endpoint/v1.0/.

The same URL MUST NOT be used for two different versions of the framework. See also SAML metadata.

Language preference

In eHerkenning, the language preference of the acting natural person can be specified, so the dialogue can take place in that language. Because SAML 2.0 messages do not have a field for this and it is not desirable to use an extension in the messages, EherkenningPreferredLanguage MAY be used as query variable in the URL or provided as POST variable. See also section SAML attribute elements.

Character set and encoding

All message MUST be encoded in the Unicode UTF-8 character set.

Information security requirements

This chapter describes the requirements that apply to the information security measures that are implemented.

- Digital signature
- Encryption
- PKIoverheid
- Secure connection
- Synchronize system clocks

Digital signature

To guarantee authenticity, integrity and non-repudiation, each message described in this document MUST be provided with a digital signature from the message sender. The message recipient MUST validate all of the digital signatures in the message before processing it.

- The recipient MUST check that the message is signed with a valid digital signature that envelopes the whole message with Enveloped Signature Transform.
- The recipient MUST NOT process the message if it contains parts that are not signed with a valid digital signature.

The following requirements apply to generating digital signatures:

- The digital signature MUST envelope the whole message content with Enveloped Signature Transform http://www.w3.org/2000/09/xmldsig#enveloped-signature.
- Canonicalization MUST be carried out according to the exclusive c14n method http://www.w3.org/TR/xml-exc-c14n/
- Digests MUST be calculated with the RSA-SHA256 algorithm.
- The SignatureValue MUST be calculated with the RSA-SHA256 algorithm.
- The participant MUST sign messages with a PKIoverheid G2 certificate with a key length of at least 2048 bits. The (extended) key usage of the used certificate MUST allow use for signing.
- The service provider MUST sign messages with a PKIoverheid G1 certificate with a key length of at least 1024 bits or a PKIoverheid G2 certificate with a key length of at least 2048 bits.
- In case of signing metadata, the `<Signature>` element MUST contain only an `<X509Data>` element with an `<X509Certificate>` element.
  In all other cases, The signature MAY contain a `<KeyInfo>` element that contains a `<KeyName>`. The `<KeyName>` MUST match the `<KeyName>` stated in the metadata of the sender for the respective role. The signature MUST NOT contain other elements (such as `<X509Data>`). If a `<KeyInfo>` element is not included in the message, the metadata MUST contain at least one (1) valid certificate against which the message can be validated. If the metadata contains more than one certificate, the participant MUST validate the message against each valid certificate. The participant MAY agree with its service consumers to limit the period in which the metadata contains more than one certificate. This enables the high utilization of the system to be controlled.

Encryption

Encryption is used to guarantee confidentiality. In case encryption MAY or MUST be used, one MUST use the block encryption algorithms identified by the following URI in conjunction with the use of XML Encryption

- http://www.w3.org/2001/04/xmlenc#aes256-cbc

PKIoverheid

In order to use PKIoverheid properly, message recipients MUST meet the requirements for the receiving party described in the PKIoverheid Programma van Eisen (PKIoverheid Requirements). The following aspects are important:

- Trust the root certificate 'Staat der Nederlanden Root CA - G2', refer to http://www.pkioverheid.nl
- Know and trust all domain and CSP certificates, refer to http://www.pkioverheid.nl
- Check the PKIoverheid CRL on http://crl.pkioverheid.nl regularly

Secure connection

The following requirements apply to all connections between two systems:

- All connections MUST use or TLS.
- The WS-I basic security profile http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html advises against some cipher suites. These MUST NOT be used for TLS.
- For TLS, a participant SHOULD use a PKIoverheid G2 SSL certificate. If a PKIoverheid G2 SSL certificate is not used, a participant MUST use an EV SSL certificate with a key length of at least 2048 bits. The (extended) key usage of the used certificate MUST allow use for TLS.
- For TLS a service provider SHOULD use an EV SSL certificate with a key length of at least 2048 bits. A service provider MUST use an SSL certificate with a key length of at least 1024 bits.

The use of SSL certificates other than PKIoverheid G2 will be disallowed over time.

Synchronize system clocks

The network uses Coordinated Universal Time, i.e. UTC. All time stamps in the messages are formatted as yyyy-mm-ddThh:mm:ssZ. The T(time) and Z(zulu) are fixed values.

Each participant and service provider MUST synchronize the system with a reliable and precise time source so the system time never deviates more than 2 seconds either way.

Error handling

This chapter describes how errors MUST be handled in the network, in order to inform and serve both users and participants sufficiently.

For error handling, conformity regarding the interpretation of the status codes as used in the <Response> element is critical. Only the following top-level status codes MAY be used.

`urn:oasis:names:tc:SAML:2.0:status:Requester`

> This status code is used for errors caused by the initiator of the SAML request. For example, because an assurance level is requested which is not supported by the recipient, or because the request message has expired.

`urn:oasis:names:tc:SAML:2.0:status:Responder`

> This status code is used for errors caused by the recipient of the SAML request. For example, because of technical failure or because the recipient does not support requested (optional) functionality.

Only the following second-level status codes MAY be used

`urn:oasis:names:tc:SAML:2.0:status:AuthnFailed`

This status code is used when an user cannot be authenticated for example because invalid credentials have been provided or the cancel button has been used.

`urn:oasis:names:tc:SAML:2.0:status:RequestDenied`

This status code is used when a received request cannot be processes, for example because it has expired.

`urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported`

This status code is used when a message is correctly formatted by the requester, and understood by the recipient, but that functionality is requested which is not supported by the recipient.

Cancelling

During the process of authenticating and authorizing, a user may cancel the processes by clicking on the cancel button.

If an user cancels, the participant MUST direct the user automatically to the latest sender of a SAML request, accompanying a valid SAML response message including valid SAML status codes. An `<StatusMessage>` element MAY be included, containing for example the value "Authentication Cancelled"

Invalid formatted messages

If a participant receives an invalid formatted message, the participant MUST abort the process immediately. An invalid formatted message is one that is not formatted following the interface specifications.

The recipient MUST - if possible - notify the user that a fatal errors has occurred. The user does not have to be redirected to the requester. The recipient MUST investigate the error encountered .

Valid formatted messages which cannot become fulfilled

A participant might receive requests which cannot be handled because of functional shortcomings in the request message. For example because an invalid value for the `<Issuer>` element has been provided. When a participant receives a message which does not match the functional specifications from the afsprakenstelsel, the recipient must abort the process. The user does not have to be redirected to the requester.

A participant might receive a request to which the recipient cannot respond. for example because an assurance level is requested which the specific AD cannot offer. When a participant receives a message which it cannot process because of functional shortcomings of the participant, the recipient must abort the process. The recipient MUST direct the user automatically to initiator of the SAML request, accompanying a valid SAML response message including valid SAML status codes. The recipient must provide a description of the problem in the `<StatusMessage>` element (for example 'level not supported").

When a party receives a message that has expired, or the message was not expected at that time (unknown inresponseto) in the process, the receiving party MUST abort the process. The recipient MUST direct the user automatically to initiator of the SAML request, accompanying a valid SAML response message including valid SAML status codes. The `NotOnOrAfter` attribute determines whether or not a message has expired.

The receiver of the SAML response messages with status codes indicating the occurrence of an error - that is the initiate of the request which the responder cannot fulfill - MUST investigate the errors encountered. This receiver, MUST inform the user on this error. The receiver of this error having the HM role, MUST provide the user an alternative way to continue the process of authenticating and authorizing, by re-rendering a list with AD or MR participants. Another recipient MAY provide the user an alternative.

Single sign-on and user sessions

Within certain boundaries, single sing-on and user sessions are allowed within eHerkenning. This document describes the technical requirements.

For other requirements, see Use cases Single Sign-On.

Sessions at participants

Participants MAY maintain a session for single sign-on if the user so indicated. The following data MAY be maintained in this session:

- an eHerkenningsmakelaar maintains user preferences (selected AD and MR).
- an AD maintains the identity of the acting natural person. Based on this session, the AD MAY directly issue a new authentication assertion to the service providers making a request in which single sign-on is specified. The requirements for the maximum life span must be followed.
- an MR maintains user preferences (chosen party to represent).

The maximum life span of a session at the AD is 2 hours unless a new authentication assertion is issued in the meantime whereby the session MAY be extended to a maximum of 2 hours.

Participants MAY provide an acting natural person the option to log out.

This option has the same function as logging out from a service provider (see below). Participants and service providers must ensure that cookies are deleted after logging out or after the expiry of an authentication session, and that previously received forms that are resubmitted generate an error.

Shared domain cookies

For cookies in which the choice for an preferred AD is saved, the Identity Provider Discovery Profile is applied as follows:

- The shared domain is '*.sso.eherkenning.nl'
- The name of the cookie MUST be '_saml_idp'
- The cookie MUST have the path prefix '/'.
- The cookie is a secure cookie.
- The cookie is persistent.
- The content of the cookie consists of one or more Base-64 encoded URI values, each separated by a single space.
- Each URI value represents the unique identification number for an AD as defined in EntityID. When there is no AD related to the value stored in the cookie, the HM MUST act as if no cookie was set and MUST uncheck the checkbox stating "Bewaar selectie authenticatiedienst".

To ensure that the common domain cookies are available for all eHerkenningsmakelaars, they are sent from the browser of the acting natural person to a cookie server that belongs to the respective eHerkenningsmakelaar but placed in the shared domain. Redirects and/or a script can be used to include this information in the HTML page that is sent to the acting natural person.

If a script is used, cookie handling must be programmed in such a way that, if the cookie server does not respond, the process is continued as if a cookie value did not have to be read or written. If redirects or scripts are used, the eHerkenningsmakelaar SHOULD detect when a sent request is not being answered and the same request is being resubmitted. In that case, repeated requests must follow an alternative path without cookies. The objective of doing this is to prevent obstructing the process when cookies do not work.

See also Proces onderhoud cookieserver

Sessions at service providers

A service provider using SSO is responsible for local session management. During the session, the service provider MUST permanently offer and display a log-out option. A service provider must implement the log-out functionality as follows:

- Session cookies must be deleted and the session must be destroyed
- Submitted forms must be deleted (so that resubmitting the same form from the browser generates an error message)
- The session is then redirected to the eHerkenningsmakelaar and a logout message sent according to Interface specifications DV-HM 1.7

Attributes and elements

Within the eHerkenning interface specifications, a number of generic SAML, and specific eHerkenning attributes are defined. These form our "profile".

- EntityID
- Level of assurance — eHerkenning distinguishes five different levels of assurance.
- OIN format — The OIN format is used to indicate participants, service providers and specific types of service consumers and intermediaries. OIN stands for Organization Identifying Number.
    - DigiKoppeling — Logius provides this number to service providers that do not have or do not have

their own KvK number. The number from the DigiKoppeling register has the prefix 00000004.
    - FI number — The FI number has the prefix 00000001 or 00000002. The number consists of 9 digits and a 3-digit suffix. For prefix 00000001, the suffix is always 000.
    - KvK nummer — The KvK number has the prefix 00000003. The number consists of the 8-digit KvK number with the suffix 0000.
    - Vestigingsnummer — The branch number has the prefix 00000006. The number consists of the 12-digit branch number.
- Pseudonyms — In eHerkenning, an executing person may be referred to as follows:
    - Internal pseudonym — The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the acting natural person, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the
    - Specific pseudonym — The specific pseudonym can be created in two ways:
- SAML attribute elements — This section describes the data elements that occur in messages as SAML Attribute element.
    - AuthorizationRegistryID — An SAML Attribute element with an EntityID from the MR that must be queried in the use case "raadplegen machtigingenregister" (query MR).
    - EherkenningPreferredLanguage — An URL or POST variable containing the language preference of acting natural person.
    - EntityConcernedID (SAML) — An SAML Attribute element with the identifying attribute of the acting service consumer that is represented by the acting natural person (who might be the same).
    - Representation — An SAML Attribute element with an indication whether there is an issue of representation
    - ServiceID (SAML) — An SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.
- ServiceID — In eHerkenning, all of the services are identified by a ServiceID, a number that is unique in the context of the service provider.
- XACML attribute elements — This chapter describes all of the XACML data elements defined for eHerkenning. SAML data elements that are defined for eHerkenning are described in SAML attribute elements.
    - ActingEntityID — An XACML Attribute element containing the specific pseudonym of the acting natural person.
    - Action-ID — An XACML Attribute element containing the action ID.
    - AssertionConsumerServiceIndex — An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the eHerkenningsmakelaar.
    - AuthenticationMeansID — An XACML Attribute element containing the internal pseudonym of the acting natural person.
    - EncryptedAttribute — An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the eHerkenning attribute catalogue (e.g. urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail).
    - EntityConcernedID (XACML) — An XACML Attribute element that matches the SAML attribute described in EntityID
    - Intermediates — A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
    - LevelOfAssurance — A XACML Attribute element containing the minimum level of assurance that is required by the service provider.
    - LevelOfAssuranceUsed — An XACML Attribute element containing the level of assurance of the registered authorization.
    - ServiceID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceID.

EntityID

In eHerkenning, all of the participants' and service providers' systems are identified by a unique EntityID, which is specified in the SAML metadata.

The EntityID has the format urn:nl:eherkenning:<ROLE>:<OIN>:entities:<index> where <ROLE> can have the values DV, HM, AD or MR, <OIN> represents the OIN of the participant. The <index> is a number between 0 and 8999 that can be selected by the participant or the service provider to define different endpoints. Numbers between 9000 and 9999 are reserved for test systems.

When changes are made to the participant's system (e.g. when moving to a new version of eHerkenning) the participant MAY change a system's EntityID.

Although they look similar, EntityID's are not to be confused with ServiceID's (ServiceID). There is an n:n relationship between EntityID's and ServiceID's. One system may offer more than one service, or the other way around: more systems can offer the same service.

Level of assurance

eHerkenning distinguishes five different levels of assurance.

They map to the SAML 2.0 AuthnContextClassRef as shown below.

eHerkenning level	SAML2 AuthnContextClassRef element
1	urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
2	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
2+	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
3	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
4	urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

Other values MUST NOT be used.

Refer to Betrouwbaarheidsniveaus for legal context, and Opbouw betrouwbaarheidsniveaus eHerkenning for level of assurance in the context of STORK.

OIN format

The OIN format is used to indicate participants, service providers and specific types of service consumers and intermediaries. OIN stands for Organization Identifying Number.The OIN format is defined in DigiKoppeling. An OIN consists of the following concatenated elements:

- An 8-digit prefix that tells the register where the number is defined
- A number whose value depends on the register

eHerkenning uses FI numbers, KvK (chamber of commerce) numbers, branch numbers and numbers from the DigiKoppeling register. Numbers from international trade registers or comparable public registers can be added after a specific prefix has been published.

- DigiKoppeling — Logius provides this number to service providers that do not have or do not have their own KvK number. The number from the DigiKoppeling register has the prefix 00000004.
- FI number — The FI number has the prefix 00000001 or 00000002. The number consists of 9 digits and a 3-digit suffix. For prefix 00000001, the suffix is always 000.
- KvK nummer — The KvK number has the prefix 00000003. The number consists of the 8-digit KvK number with the suffix 0000.
- Vestigingsnummer — The branch number has the prefix 00000006. The number consists of the 12-digit branch number.

International registers

In order for international consumers in other EU member states to use eHerkenning, specific prefixes can be determined in collaboration with Logius and the Nederlandse Dienstenloket (Antwoord voor Bedrijven). A prefix is issued for each of the country's registers. If applicable, a prefix is issued for the industry level (company and legal entity) and a prefix is issued for the branch level. The eHerkenning website must inform users in the respective countries that they can use these numbers, and provide a reference to the Dutch window service and the rules for the respective country.

The rules state that the KvK number that is issued to a specific service consumer must always be used. This means that service consumers and branches of international service consumers that are registered in the Dutch trade register may not use the number with which they are registered in an international register.

If any division of the service consumer is registered in the Dutch trade register, the KvK number must be used.

DigiKoppeling

Logius provides this number to service providers that do not have or do not have their own KvK number. The number from the DigiKoppeling register has the prefix 00000004.

The number consists of 9 digits followed by 000, for example: 000000041234567890000

FI number

The FI number has the prefix 00000001 or 00000002. The number consists of 9 digits and a 3-digit suffix. For prefix 00000001, the suffix is always 000.

Example: 000000011234567890000 or 000000021234567890001

KvK nummer

The KvK number has the prefix 00000003. The number consists of the 8-digit KvK number with the suffix 0000.

For example: 000000031234567800000

Vestigingsnummer

The branch number has the prefix 00000006. The number consists of the 12-digit branch number.

For example: 000000061234567890120

Pseudonyms

In eHerkenning, an executing person may be referred to as follows:

- In the event of representation:
    1. inside the network with an Internal pseudonym issued by the AD; and
    2. inside and outside of the network with a Specific pseudonym issued by the MR
- In the event of non-representation:
    1. Inside and outside of the network with a Specific pseudonym issued by the AD

- Internal pseudonym — The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the acting natural person, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the
- Specific pseudonym — The specific pseudonym can be created in two ways:

Internal pseudonym

The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the acting natural person, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the same internal pseudonym MAY be used for the new authentication token.

The format of the internal pseudonym MUST have a hexadecimal value of 32 byte. For example, ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890

Specific pseudonym

The specific pseudonym can be created in two ways:

1. In the event of representation by an MR. It is unique for each different combination of executing natural person, represented service consumer or service provider.
    a. In the event of a chain authorization, the pseudonym is unique for each different combination of executing natural person, intermediary and service provider
2. In the event of non-representation by an AD. It is unique for every different combination of service consumer and service provider.

A specific pseudonym is preferably generated once and then stored, but it can also be generated for each request as long as it is always generated in the same way and the same value is generated for each request.

Differences in specific pseudonyms can be used by service providers to determine that the executing natural persons are different (four-eye principle). This is the reason why an MR MUST have permission to generate a new pseudonym for an existing combination of service provider, executing natural person and service consumer (or intermediary in the case of chain authorizations) from the authorization manager or legal representative of the service consumer (or the intermediary). Reasons to generate a new pseudonym can be:

- Natural person has been assigned a new job in the same company and may therefore no longer obtain access with the old pseudonym to files at service providers that are linked to the old role;
- The identity of the natural person was accidently disclosed to the service provider(s) and a new pseudonym is needed to protect/pseudonymize the identity;
- Migration to a new pseudonym is needed because the service providers merged/split.

The format of the specific pseudonym MUST have a hexadecimal value of 32 byte. For example, ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890

In the event of representation, this value is followed by an @ and hexadecimal value of 16 byte. For example, ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890@ABCDEF1234567890ABCDEF1234567890

The 32-byte value MUST be a random value This can be achieved, for example, by calculating an SHA256 hash over the following elements (in this sequence and separated by a separator):

1. The service provider's OIN (OIN format).
2. A unique (but not necessarily exclusive) identifying attribute for the executing natural person in the context of the service consumer. This attribute MAY be determined by the administrator or the creator of the pseudonym, but MAY also be the Internal pseudonym.
3. The identifying attribute for the represented service consumer (only in the event of representation without chain authorization) or for an intermediary (in the event of chain authorization).

Other methods to reach a 32-byte random value are also allowed.

The value of 16 byte MUST be an MD5 hash over the identifying attribute for the represented service consumer (or intermediary in the case of chain authorization).

> Other formats of specific pseudonyms may be in use. Users of the specific pseudonym are advised not to use (parts of) the pseudonym for other purposes than to identify the executing natural person.

SAML attribute elements

This section describes the data elements that occur in messages as SAML Attribute element.

The attributes specific to eHerkenning are identified by an urn. The urn contains the version number of the framework in which the version of the respective attribute was first included.

- AuthorizationRegistryID — An SAML Attribute element with an EntityID from the MR that must be queried in the use case "raadplegen machtigingenregister" (query MR).
- EherkenningPreferredLanguage — An URL or POST variable containing the language preference of acting natural person.
- EntityConcernedID (SAML) — An SAML Attribute element with the identifying attribute of the acting service consumer that is represented by the acting natural person (who might be the same).
- Representation — An SAML Attribute element with an indication whether there is an issue of representation
- ServiceID (SAML) — An SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.

AuthorizationRegistryID

Description	An SAML Attribute element with an EntityID from the MR that must be queried in the use case "raadplegen machtigingenregister" (query MR). This EntityID MUST exist in the metadata. See SAML metadata
Name	urn:nl:eherkenning:1.0:AuthorizationRegistryID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See EntityID
Comments	When an AuthorizationRegistryID is returned by an AD, the value of the Representation attribute MUST be TRUE.

EherkenningPreferredLanguage

Description	An URL or POST variable containing the language preference of acting natural person.
Name	EherkenningPreferredLanguage
Format	Following ISO 639-1:2002

EntityConcernedID (SAML)

Description	An SAML Attribute element with the identifying attribute of the acting service consumer that is represented by the acting natural person (who might be the same).
Name	urn:nl:eherkenning:1.7:EntityConcernedID:[Name of identifying attribute]
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See Identificerende kenmerken

Representation

Description	An SAML Attribute element with an indication whether there is an issue of representation
Name	urn:nl:eherkenning:1.7:Representation

Type	http://www.w3.org/2001/XMLSchema#boolean
AttributeValue	True or false

ServiceID (SAML)

Description	An SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.
Name	urn:nl:eherkenning:1.0:ServiceID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See ServiceID The value MUST match the value of the AttributeConsumingServiceID XML attribute in AuthnRequest.

ServiceID

In eHerkenning, all of the services are identified by a ServiceID, a number that is unique in the context of the service provider.

A service provider may provide more than one service. Users can be entitled to each individual service.

All ServiceID are registred included in the Service catalog as part of an urn in the format urn:nl:eherkenning:DV:<OIN>:services:<ServiceID> where <OIN> represents the OIN of the service provider. The urn enables unique services to be defined in eHerkenning.

Registered services MUST have a ServiceID of 1 or higher. A Portal function is specified in messages by the reserved ServiceID with value '0'. These are not included in the service catalogue.

The ServiceID is used in messages in two formats:

1. The short format. Contains only the ServiceID.
2. The long format. Contains the entire urn.

> Although they look similar, EntityID's are not to be confused with ServiceID's. There is an n:n relationship between EntityID's and ServiceID's. One system may offer more than one service, or the other way around: more systems can offer the same service.

XACML attribute elements

This chapter describes all of the XACML data elements defined for eHerkenning. SAML data elements that are defined for eHerkenning are described in SAML attribute elements.

This section describes the data elements that occur in messages as XACML Attribute element. This does not include SAML and XACML elements that strictly follow the SAML and XACML standards.

The attributes specific to eHerkenning are identified by an urn. The urn contains the version number of the framework in which the version of the respective attribute was first included.

- ActingEntityID — An XACML Attribute element containing the specific pseudonym of the acting natural person.
- Action-ID — An XACML Attribute element containing the action ID.
- AssertionConsumerServiceIndex — An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the eHerkenningsmakelaar.
- AuthenticationMeansID — An XACML Attribute element containing the internal pseudonym of the acting

natural person.

- EncryptedAttribute — An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the eHerkenning attribute catalogue (e.g. urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail).
- EntityConcernedID (XACML) — An XACML Attribute element that matches the SAML attribute described in EntityID
- Intermediates — A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
- LevelOfAssurance — A XACML Attribute element containing the minimum level of assurance that is required by the service provider.
- LevelOfAssuranceUsed — An XACML Attribute element containing the level of assurance of the registered authorization.
- ServiceID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceID.

ActingEntityID

Description	An XACML Attribute element containing the specific pseudonym of the acting natural person. The element MUST NOT contain other attributes (@) than those described here.
@AttributeID	urn:nl:eherkenning:1.0:ActingEntityID
@Datatype	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See Pseudonyms

Action-ID

Description	An XACML Attribute element containing the action ID. The element MUST NOT contain other attributes (@) than those described here.
@AttributeID	urn:oasis:names:tc:xacml:1.0:action:action-id
@Datatype	http://www.w3.org/2001/XMLSchema#string
AttributeValue	MUST contain the value 'Authenticate'

AssertionConsumerServiceIndex

Description	eHerkenning: This attribute element indicates the URL to which the response must be sent. An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the eHerkenningsmakelaar. The element MUST NOT contain other attributes (@) than those described here.
@AttributeID	urn:nl:eherkenning:1.0:AssertionConsumerServiceIndex
@Datatype	http://www.w3.org/2001/XMLSchema#unsignedShort
@Issuer	EntityID of the eHerkenningsmakelaar. See Pseudonyms
AttributeValue	0 to 99999

AuthenticationMeansID

Description	An XACML Attribute element containing the internal pseudonym of the acting natural person. The element MUST NOT contain other attributes (@) than those described here.
@AttributeID	urn:nl:eherkenning:1.0:AuthenticationMeansID
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID of the authentication service.
AttributeValue	See Pseudonyms

EncryptedAttribute

Description	An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the eHerkenning attribute catalogue (e.g. urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail). The service provider's service certificate that is included in the service catalogue MUST be used for encryption. A level of assurance is also passed for each EncryptedAttribute. A cipher value is included in the encrypted attribute. This cipher value contains the encrypted value of the request attribute that is encrypted with the key of the DV in the service catalogue.
Example	BusinessName › Expand source `<saml:Attribute Name= "urn:nl:eherkenning1.3:AdditionalAttribute:BusinessN ame"> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema- instance" xsi:type="xs:string"> </saml:AttributeValue> <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema- instance" xsi:type="eh:betrouwbaarheidsniveau"> </saml:AttributeValue> </saml:Attribute>`

EntityConcernedID (XACML)

Description	An XACML Attribute element that matches the SAML attribute described in EntityID

Intermediates

Description	A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
Name	urn:nl:eherkenning:1.7:Intermediates
Type	multi-value, with values of the type urn:nl:eherkenning:1.7:IntermediateEntityID:

AttributeValue	See Identificerende kenmerken. (the multi-value attribute contains only one value).

LevelOfAssurance

Description	A XACML Attribute element containing the minimum level of assurance that is required by the service provider. The element MUST NOT contain other attributes (@) than those described here.
@AttributeID	urn:nl:eherkenning:1.0:LevelOfAssurance
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID of the eHerkenningsmakelaar.
AttributeValue	See Level of assurance

LevelOfAssuranceUsed

Description	An XACML Attribute element containing the level of assurance of the registered authorization. If there are several registrations(authorisations) for an assertion and these registrations are established at different levels of assurance (for instance a generic authorisation at level eH1 and a specific authorisation at level eH3), the highest level of assurance MUST be used. The element MUST NOT contain other attributes (@) than those described here.
@AttributeID	urn:nl:eherkenning:1.0:LevelOfAssuranceUsed
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID of the "machtigingenregister". See EntityID
AttributeValue	See Level of assurance

ServiceID (XACML)

Description	An optional XACML Attribute element that matches the SAML attribute described in ServiceID.

SAML metadata

This chapter describes the metadata the participants must supply, how the Beheerorganisatie publishes the aggregated metadata, and how it is to be interpreted by the participants.

Participants must use SAML metadata in the eHerkenning network to describe the URLs and certificates that are used for the different interfaces. Participants supply metadata and the Beheerorganisatie validates, aggregates and publishes it according to Proces metadata.

Moreover, service providers adapting to the standard DV-HM interface specifications, MUST exchange SAML metadata with their supporting HM systems based on specifications describes in this chapter.

- Format of metadata for participants

- EntityDescriptor
- Versions
- ValidFrom and ValidUntil
- Level of assurance
- IDPSSODescriptor
- Keys for Signing
- Format of metadata for service providers
  - Attributes
  - Keys for Signing
- Format of metadata for HMs
  - Signing
- Supply of metadata by Beheerorganisatie
- XML Schema extentions

Format of metadata for participants

A participant with the role of HM, AD, or MR MUST supply metadata to the Beheerorganisatie for every system that implements the role of the participant in the network. A participant MUST NOT supply metadata for a role or functionality it has not been assigned.

This requirement is for metadata for the production network. This requirement does not apply to metadata for the acceptance network because it must also be possible to test the systems of parties that have not yet joined.

A participant that has several roles in the network MUST supply metadata for each role separately.

EntityDescriptor

The participant MUST publish SAML metadata for the Beheerorganisatie complying to the specifications defined for the namespace urn:oasis:names:tc:SAML:2.0:metadata, with one signed EntitiesDescriptor element. Signing metadata MUST meet the requirements for signing and encrypting, see Digital signature.

The EntityDescriptor element contains one or more EntityDescriptor elements.

Each EntityDescriptor element MUST contain the entityID and an additional version attribute and MUST NOT contain other SAML attributes.

The version attribute contains the version of the interface specifications on which the entity communicates. See SAML attribute elements.

Example

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
 <md:EntityDescriptor
 ID="[reference for dsig]"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 entityID="urn:nl:eherkenning:HM:9999990000010000:0001" >
 <ds:Signature>...</ds:Signature>
...
</md:EntityDescriptor>
```

The EntityDescriptor MUST contain one or more elements of the type ContactPerson containing the name, email address, and telephone number of the people that can be contacted by participants or the Beheerorganisatie in the event of an incident.

The metadata MUST contain data about one's own organization by including one element of the type Organization, which describes the name (OrganizationName), the readable name for users (OrganizationDisplayName), and the website (OrganizationURL).

The same role MAY be filled by several systems. Metadata is supplied for each of the systems. The metadata MUST contain a different EntityID in which the Organization element is the same.

Versions

When a system can send messages based on different versions of the framework, metadata MUST be supplied for each version. So, if an entity can communicate on several versions of the interface (e.g. eh:version=1.5 and eh:version=1.7), both are included in the EntitiesDescriptor as separate EntityDescriptor. These EntityDescriptor elements MAY have the same or different EntityIDs.

An eHerkenning broken MUST include separate EntityDescriptor elements in the metadata for the different logical systems that support the individual versions of the eHerkenning interfaces. So, an eHerkenningsmakelaar that can communicate on several versions of the interface (e.g. eh:version=1.5 and eh:version=1.7) will include both versions in de metadata as separate EntityDescriptor in the EntitiesDescriptor. These EntityDescriptors MAY have the same or different values for their EntityID attributes.

An AD/MR MUST inspect the values of eh:version in the metadata to determine which EntityDescriptor is to be used to communicate with an eHerkenningsmakelaar. EntityDescriptors with a version number that is different than the version of the AD/MR SHOULD be generated by the AD/MR. An AD has only one valid EntityDescriptor at a given point in time. To facilitate the transition to a new version, an AD MAY provide exactly two different EntityDescriptor elements. An EntityDescriptor element MUST contain the SAML attribute validUntil. The other EntityDescriptor element MUST contain the eHerkenning validFrom attribute (see appendix, section 11.1). The dateTime value of both fields MUST be the same. These two EntityDescriptors MAY have the same or different EntityIDs.

ValidFrom and ValidUntil

An HM MUST use the ValidFrom and ValidUntil in the metadata, if present, to determine which EntityDescriptor is valid for communication with an AD. An MR has only one valid EntityDescriptor at a given point in time. To facilitate the transition to a new version, an MR MAY provide exactly two different EntityDescriptor elements. An EntityDescriptor element MUST contain the SAML attribute validUntil. The other EntityDescriptor element MUST contain the eHerkenning validFrom attribute (see appendix, section 11.1). The dateTime value of both fields MUST be the same.
These two EntityDescriptors MAY have the same or different EntityIDs.

An HM MUST inspect ValidFrom and ValidUntil in the metadata, if present, to determine which EntityDescriptor is valid for communication with an AD.

Level of assurance

An AD or MR MUST include the assurance level at which recognition requests can be processed in the EntityDescriptor in the form of an extension of the EntityDescriptor element as described in the document SAML V2.0 Identity Assurance Profiles.

Example

› Expand source

```
...
 <md:Extensions>
 <attr:EntityAttributes>
 <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="urn:oasis:names:tc:SAML:attribute:assurancecertification">
 <saml:AttributeValue>
 urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
 </saml:AttributeValue>
 </saml:Attribute>
 </attr:EntityAttributes>
 </md:Extensions>
 ...
```

Different EntityDescriptor elements MUST always be contained in a single EntitiesDescriptor element.

Example

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor
    ID="[reference for dsig]"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:Signature>...</ds:Signature>
        <md:EntityDescriptor
            entityID="urn:nl:eherkenning:AD:9999990000010000:0001"
            eh:version="1.1a" validUntil="2011-03-15T00:00:00Z">
            …
        </md:EntityDescriptor>
        <md:EntityDescriptor
            entityID="urn:nl:eherkenning:AD:9999990000010000:0001"
            eh:version="1.3" eh:validFrom="2011-03-15T00:00:00Z">
            …
        </md:EntityDescriptor>
</md:EntitiesDescriptor>
```

IDPSSODescriptor

An eHerkenningsmakelaar includes only one IDPSSODescriptor element which in turn contains a single SingleSignOnService element and no other elements.

Example

Expand source

```
...
<md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
          <md:SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://...."/>
</md:IDPSSODescriptor>
...
```

An AD or MR MUST include one IDPSSODescriptor element containing one SingleSignOnService element, and MUST NOT include any other elements. The SingleSignOnService element MUST indicate it supports the SAML POST binding with the attribute Binding, and MUST NOT contain any other attributes.

Example

Expand source

```
...
<md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAuthnRequestsSigned="true">
          <md:SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://...."/>
</md:IDPSSODescriptor>
...
```

An eHerkenningsmakelaar MUST include only one IDPSSODescriptor and only one SPSSODescriptor and MUST NOT include any other elements. The IDPSSODescriptor from the eHerkenningsmakelaar MAY contain several SingleSignOnService elements and MUST contain at least one SingleSignOnService element for which the Binding attribute has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST. The SPSSODescriptor from the eHerkenningsmakelaar MUST contain two AssertionConsumerService elements with a Binding attribute which has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST, and with indices 1 and 2 for responses from ADs and MRs and may not contain any other elements.

Example eHerkenningsmakelaar

Expand source

```
...
<md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAuthnRequestsSigned="true">
...
     <md:SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://...."/>
</md:IDPSSODescriptor>
<md:SPSSODescriptor AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://..."
index="1"/>
      <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://..."
index="2"/>
</md:SPSSODescriptor>
...
```

An IDPSSODescriptor element MUST contain the WantAuthnRequestsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes. An SPSSODescriptor element MUST contain the AuthnRequestsSigned XML attribute with value "true" and a WantAssertionsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes.

Keys for Signing

An IDPSSODesriptor or SPSSODescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing". Every KeyDescriptor element MUST contain a KeyName element and a valid G2 PKIoverheid certificate with which the participant's SAML messages can be authenticated. Note: Service providers and participants must process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.

Example

Expand source

```
...
<md:KeyDescriptor use="signing">
        <ds:KeyInfo>
              <ds:KeyName>
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>
...
```

Format of metadata for service providers

For each service, a service provider MUST supply metadata to the HM as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element. Signing metadata MUST meet the requirements for for signing and encrypting, see Digital signature.

Each EntityDescriptor element MUST contain the entityID and an additional version attribute and MUST NOT contain other SAML attributes. The version attribute contains the version of the interface specifications on which the entity communicates.

A service provider MUST include one SPSSODescriptor.

It must contain at least one AssertionConsumingService. If several AssertionConsumingService entries are included, one of these entries must be flagged as default by setting the isDefault XML attribute with value "true".

In addition, a service provider MAY include for each service offered one AttributeConsumingService element in which the service provider indicates which attributes it wants to receive for the respective service.

Attributes

Each AttributeConsumingService MUST contain exactly one attribute with the same name as ServiceID in long format (see Pseudonyms). In addition, each AttributeConsumingService MAY contain one or more RequestedAttributes that are in the eHerkenning attribute catalogue. For each requested attribute that is included, the service provider MAY use isRequired to indicate whether the attribute is required for the DV application to work properly. If isRequired is not defined, the default value 'false' is implied.

An AD/MR MAY but does not have to prompt a user during the transaction for a value based on isRequired="true". The service provider will have to take this into account during processing. Other elements MUST NOT be included.

Exaple service provider

› Expand source

```
...
<md:SPSSODescriptor AuthnRequestsSigned="true"
WantAssertionsSigned ="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
...
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://..."
index="1" isDefault='true'/>
    <md:AttributeConsumingService isDefault="true" index="1">
            <md:ServiceName xml:lang="en">Voorbeeld Dienst 1</md:ServiceName>
            <md:RequestedAttribute
Name="urn:nl:eherkenning:DV:0000000312345678000:services:0001">
                        </md:RequestedAttribute>
            <md:RequestedAttribute isRequired=”false”

Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"/>
            <md:RequestedAttribute isRequired=”true”

Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail"/>
           <md:RequestedAttribute isRequired=”false”

Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalPhone"/>
    </md:AttributeConsumingService>
    <md:AttributeConsumingService isDefault="false" index="2">
           <md:ServiceName xml:lang="en">Voorbeeld Dienst 50</md:ServiceName>
          <md:RequestedAttribute
Name="urn:nl:eherkenning:DV:0000000312345678000:services:0050">
                        </md:RequestedAttribute>
          <md:RequestedAttribute isRequired=”false”

Name="urn:nl:eherkenning1.3:AdditionalAttribute:ActingPersonName"/>
          <md:RequestedAttribute isRequired=”true”

Name="urn:nl:eherkenning1.3:AdditionalAttribute:PersonalEmail"/>
    </md:AttributeConsumingService>
</md:SPSSODescriptor>
...
```

Keys for Signing

An SPSSODescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing". Every KeyDescriptor element MUST contain a KeyName element and a valid G2 PKIoverheid certificate with which the service provider its SAML messages can be authenticated. Note: HMs must process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.

Example

Expand source

```
...
<md:KeyDescriptor use="signing">
        <ds:KeyInfo>
              <ds:KeyName>
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>
...
```

Format of metadata for HMs

A HM MUST supply metadata to the service provider as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element. Signing metadata MUST meet the requirements for signing SAML messages described Information security requirements.

Each EntityDescriptor element MUST contain the entityID and an additional version attribute and MUST NOT contain other SAML attributes. The version attribute contains the version of the interface specifications on which the entity communicates.

An eHerkenningsmakelaar MUST include only one IDPSSODescriptor and MUST NOT include any other elements. The IDPSSODescriptor from the eHerkenningsmakelaar MAY contain several SingleSignOnService elements and MUST contain at least one SingleSignOnService element for which the Binding attribute has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.

Example eHerkenningsmakelaar

Example eHerkenningsmakelaar

Expand source

```
...
<md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAuthnRequestsSigned="true">
...
     <md:SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://...."/>
</md:IDPSSODescriptor>
...
```

An IDPSSODescriptor element MUST contain the WantAuthnRequestsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes.

Signing

An IDPSSODesriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing". Every KeyDescriptor element MUST contain a KeyName element and a valid G2 PKIoverheid certificate with which the

participant's SAML messages can be authenticated. Note: Service providers must process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.

Example

Expand source

```
...
<md:KeyDescriptor use="signing">
        <ds:KeyInfo>
              <ds:KeyName>
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>
...
```

Supply of metadata by Beheerorganisatie

The Beheerorganisatie checks the participants' metadata for conformity, deletes the signatures and aggregates the metadata into one file. The aggregated metadata consists of a signed EntitiesDecriptor element with an cacheduration XML attribute with value "P7D" and an Name XML attribute with a value formatted as urn:nl:eherkenning:VERSIEAS:metadata:OMGEVING:VOLGNUMMER, whereby VERSIEAS indicates the version of the framework, OMGEVING the respective environment (P or A), and VOLGNUMMER is a sequence number that distinguishes the different versions of metadata. The signature MUST meet the requirements described in Information security requirements.

The EntitiesDescriptor element contains 3 EntitiesDescriptor elements with the names Authenticatiediensten, Machtingenregisters, and eHerkenningsmakelaars that contain the metadata from the participants in the different roles. The EntitiesDescriptor element can also contain a Dienstverleners (service providers) element that contains fictitious service providers. Each eHerkenningsmakelaar MUST process the named service providers. These service providers are named in the service catalogue and can be used by the Beheerorganisatie and for testing.
The Beheerorganisatie publishes the metadata in a fixed location. In order to maintain the privacy of the contacts' details in the metadata, the location is a non-indexed URL with server-side SSL that can only be shared with the participants.

Example

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor
ID="[reference for dsig]"
Name="urn:nl:eherkenning:1.0:metadata:P:36" cacheduration="P7D"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Signature>...</ds:Signature>
    <md:EntitiesDescriptor Name="Authenticatiediensten">
...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="Machtigingenregisters">
...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="Herkenningsmakelaars">
...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="Dienstverleners">
...
    </md:EntitiesDescriptor>
```

A participant MUST process the metadata periodically at a time that is predefined by the Beheerorganisatie. Data about the URL and the periodicity are described in Proces metadata.

A participant MUST use an automated process to process the metadata that finishes in 15 minutes. A participant MUST be able to start this automated process (e.g., manually) between the predefined periods in agreement with the Beheerorganisatie to accommodate a rollback or other changes.

XML Schema extentions

XML schema metadata extension

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:eh="urn:nl:eherkenning:1.3:metadataextensions"
    targetNamespace="urn:nl:eherkenning:1.3:metadataextensions"
    elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:attribute name="validFrom" type="xs:dateTime"/>
 <xs:attribute name="version" type="xs:string"/>
</xs:schema>
```

XML schema attribute extension

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:ehsamlp="urn:nl:eherkenning:1.3a:attributeextension"

targetNamespace="urn:nl:eherkenning:1.3a:attributeextension"
                        xmlns:xs="http://www.w3.org/2001/XMLSchema"
                        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                        elementFormDefault="qualified"
attributeFormDefault="unqualified">
     <xs:element name="RequestedAttributes">
          <xs:complexType>
               <xs:sequence>
                    <xs:element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
               </xs:sequence>
          </xs:complexType>
     </xs:element>
</xs:schema>
```

Service catalog

This chapter describes the format and publication of the service catalog (Dienstencatalogus).

Format

The service catalogue MUST have the following format:

- IssueInstant (time at which the service catalogue was created)
- NotOnOrAfter (time at which the service catalogue becomes invalid)
- Version (version of the service catalogue in the format nl:eherkenning:<version of "afsprakenstelsel eHerkenning">:<sequence number service catalogue>. E.g. nl:eherkenning:0.8def:1)
- Signature (signature from the Beheerorganisatie, eHerkenningsmakelaar or service provider for authenticity, integrity and indisputability).
- Per service provider:
  - IsPublic (attribute that indicates whether the service provider is using eHerkenning in the public domain)
  - ServiceProviderID (The service provider's OIN (government ID number)
  - OrganizationDisplayName (the name of the service provider as it MUST be displayed by participants, max 64 characters). This element MAY be included for different languages.
  - Per service:
    - IsPublic (attribute that indicates whether the service is using eHerkenning in the public domain)
    - ServiceID (a unique number between 1 and 64000 that is assigned and provided by the service provider in the format urn:nl:eherkenning:DV:<OIN>:services:<index>)
    - ServiceName (name of the service determined by the service provider, max 64 characters). This element MAY be included for different languages.
    - ServiceDescription (short description of the service determined by the service provider, max 1024 characters. MRs MAY use this text to help administrators determine the authorizations). This element MAY be included for different languages.
    - ServiceDescriptionURL (a URL of max 512 characters where a detailed description of the service can be found, determined by the service provider. MRs MAY include this link to help administrators determine the authorizations). This element MAY be included for different languages.
    - AuthnContextClassRef (assurance level that is required for the service, determined by the service provider)
    - HerkenningsmakelaarId (the OIN of the recognition broker that provides the service catalogue entry for this service)

- AdditionalHerkenningsmakelaarId (multivalue entry with the OINs for the other recognition brokers that provide this service)
- EntityConcernedTypesAllowed (multivalue entry with the different types of service consumers that are granted access to the service)
- ServiceCertificate (Service provider's PKI certificate with a public key that can be used to encrypt requested attributes).

XML schema

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:eh="urn:nl:eherkenning:dc:1.7" targetNamespace="urn:nl:eherkenning:dc:1.7"
elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="xmldsig-core-schema.xsd"/>
 <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
schemaLocation="saml-schema-assertion-2.0.xsd"/>
 <xs:import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
schemaLocation="saml-schema-metadata-2.0.xsd"/>
 <!--Elements-->
 <xs:element name="Service">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="eh:ServiceID"/>
    <xs:element ref="eh:ServiceName" maxOccurs="unbounded"/>
    <xs:element ref="eh:ServiceDescription" maxOccurs="unbounded"/>
    <xs:element ref="eh:ServiceDescriptionURL" minOccurs="0"
maxOccurs="unbounded"/>
    <xs:element ref="saml2:AuthnContextClassRef"/>
    <xs:element ref="eh:HerkenningsmakelaarId"/>
    <xs:element ref="eh:AdditionalHerkenningsmakelaarId" minOccurs="0"
maxOccurs="unbounded"/>
    <xs:element name="SSOSupport" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="eh:EntityConcernedTypesAllowed" minOccurs="0"
maxOccurs="unbounded"/>
    <xs:element ref="eh:ServiceCertificate" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute ref="eh:IsPublic" use="required"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="ServiceCatalogue">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="ds:Signature"/>
    <xs:element ref="eh:ServiceProvider" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute ref="eh:IssueInstant" use="required"/>
   <xs:attribute ref="eh:NotOnOrAfter" use="required"/>
   <xs:attribute ref="eh:Version" use="required"/>
   <xs:attribute name="ID" type="xs:string"/>
  </xs:complexType>
```

```
</xs:element>
<xs:element name="EntityConcernedTypesAllowed">
 <xs:complexType>
  <xs:simpleContent>
   <xs:extension base="xs:string"/>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
<xs:element name="ServiceDescription">
 <xs:complexType>
  <xs:simpleContent>
   <xs:restriction base="md:localizedNameType">
    <xs:maxLength value="512"/>
   </xs:restriction>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
<xs:element name="ServiceDescriptionURL">
 <xs:complexType>
  <xs:simpleContent>
   <xs:restriction base="md:localizedURIType">
    <xs:maxLength value="512"/>
   </xs:restriction>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
<xs:element name="ServiceID" type="xs:anyURI"/>
<xs:element name="ServiceName">
 <xs:complexType>
  <xs:simpleContent>
   <xs:restriction base="md:localizedNameType">
    <xs:maxLength value="64"/>
   </xs:restriction>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
<xs:element name="ServiceProvider">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="eh:ServiceProviderID"/>
   <xs:element ref="eh:OrganizationDisplayName" maxOccurs="unbounded"/>
   <xs:element ref="eh:Service" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute ref="eh:IsPublic" use="required"/>
 </xs:complexType>
</xs:element>
<xs:element name="ServiceProviderID" type="xs:anyURI"/>
<xs:element name="ServiceCertificate">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="md:KeyDescriptor"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="HerkenningsmakelaarId" type="xs:anyURI"/>
```

```
<xs:element name="AdditionalHerkenningsmakelaarId" type="xs:anyURI"/>
<xs:element name="OrganizationDisplayName">
 <xs:complexType>
  <xs:simpleContent>
   <xs:restriction base="md:localizedNameType">
    <xs:maxLength value="64"/>
   </xs:restriction>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
<!--Attributes-->
<xs:attribute name="IssueInstant" type="xs:dateTime"/>
<xs:attribute name="IsPublic" type="xs:boolean"/>
```

```
 <xs:attribute name="NotOnOrAfter" type="xs:dateTime"/>
 <xs:attribute name="Version" type="xs:anyURI"/>
</xs:schema>
```

Publication

The Beheerorganisatie publishes the service catalogue at a predetermined location. Before it is published, the service catalogue is sorted by HerkenningsmakelaarId and then by the ServiceId.

A participant MUST process the service catalogue periodically at a time that is predefined by the Beheerorganisatie. See Proces doorvoeren nieuwe dienstencatalogus.

A participant SHOULD use an automated process to process the metadata. A participant MUST be able to run this process between the predefined periods to accommodate a rollback or other changes.

Attribuutverstrekking

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Een dienstverlener of een herkenningsmakelaar kan in een authenticatieverzoek ook een verzoek om attributen doen. De AD, MR of HM kan als attribuutverstrekker optreden. Zij mogen alleen attributen aanbieden die in dit document beschreven worden.

Een deelnemer moet voor elk door te geven attribuut of identificerend kenmerk opnieuw toetreden/zijn bestaande toetreding aanpassen. Zie Proces toetreden

Verantwoordelijkheden

De AD MAG alleen attributen verstrekken die in de attribuutcatalogus gedefinieerd zijn en waarvoor bij bron AD wordt aangegeven.

De MR MAG alleen attributen verstrekken die in de attribuutcatalogus gedefinieerd zijn en waarvoor bij bron MR wordt aangegeven.

De HM MOET de ontvangen attributen doorgeven tussen AD of MR systemen en de DV.

De overige verantwoordelijkheden met betrekking tot attribuutverstrekking staan beschreven in Algemene introductie.

Gebruiken van attribuutverstrekking

De attribuutcatalogus is in eerste instantie bedoeld voor deelnemers. Zij communiceren richting hun dienstverleners welke attributen zij leveren. De attribuutcatalogus beschrijft welke attributen een attribuutverstrekker MAG leveren en op welke betrouwbaarheidsniveaus dit MAG gebeuren.

Attributen worden door een dienstverlener gevraagd aan de herkenningsmakelaar die de vraag vervolgens doorzet naar een AD of een MR. De vraag gebeurt met het <RequestedAttributes> XML element. De attributen worden aan de dienstverlener verstrekt in een <AttributeStatement> XML element. Attributen worden versleuteld opgestuurd door de deelnemers die de betreffende attributen verstrekken.

De verdere specificaties voor attribuutverstrekking zijn beschreven in Interface specifications.

Identificerende kenmerken

Dit hoofdstuk beschrijft de identificerende kenmerken binnen eHerkenning.

Deze attributen zijn niet opgenomen in de Attribuutcatalogus.

Identificerende kenmerken van dienstafnemers

Een speciaal categorie attributen zijn de identificerende kenmerken van de verschillende soorten dienstafnemers of intermediairs.

Geleverde identificerende kenmerken van dienstafnemers hebben een attribuutnaam die begint met "urn:nl:eherkenning:1.7:EntityConcernedID:".

Geleverde identificerende kenmerken van intermediairs hebben een attribuutnaam die begint met "urn:nl:eherkenning:1.7:IntermediateEntityID:".

De volgende paragrafen beschrijven de typen identificerende kenmerken van dienstafnemers en intermediairs. Indien 'Toegestaan voor ketenmachtiging?' de optie 'Nee' bevat, dan mag dit type identificerend kenmerk niet worden gebruikt voor dienstafnemers of intermediairs in een keten van machtigingen.

Identificerende kenmerken van beroepsbeoefenaren

Op verzoek van deelnemers en/of hun klanten kunnen speciale identificerende kenmerken van beroepsbeoefenaren als type dienstafnemer en/of intermediair worden opgenomen. Dergelijke identificerende kenmerken mogen alleen door deelnemers worden verstrekt als aan alle voor het betreffende kenmerk beschreven criteria wordt voldaan.

- EntityConcernedID:KvKnr — Het KvK nummer van de vertegenwoordigde dienstafnemer/intermediair of vergelijkbaar nummer
- EntityConcernedID:Pseudo — Een specifiek pseudoniem dat wordt gebruikt om een burger/consument te identificeren.
- EntityConcernedID:RSIN — Het RSIN van de vertegenwoordigde dienstafnemer/intermediair
- EntityConcernedID:SubdossierNr — Het vestigingsnummer (oude formaat) van de vertegenwoordigde dienstafnemer
- EntityConcernedID:Vestigingsnr — Het vestigingsnummer (nieuwe formaat) van de vertegenwoordigde dienstafnemer

EntityConcernedID:KvKnr

Het KvK nummer van de vertegenwoordigde dienstafnemer/intermediair of vergelijkbaar nummer

Attribuutnaam	urn:nl:eherkenning:1.7:EntityConcernedID:KvKnr urn:nl:eherkenning:1.7:IntermediateEntityID:KvKnr
Korte omschrijving	
Omschrijving	Het KvKnummer van de vertegenwoordigde dienstafnemer/intermediair of vergelijkbaar nummer
Formaat	Zie KvK nummer
Betrouwbaarheidsniveaus	n.v.t.
Bron	AD, MR
Toegestaan voor ketenmachtigingen	Ja

EntityConcernedID:Pseudo

Een specifiek pseudoniem dat wordt gebruikt om een burger/consument te identificeren.

Attribuutnaam	urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo
Korte omschrijving	
Omschrijving	Een specifiek pseudoniem dat wordt gebruikt om een burger/consument te identificeren.
Formaat	Zie OIN format
Betrouwbaarheidsniveaus	n.v.t.
Bron	AD, MR
Toegestaan voor ketenmachtigingen	Nee

EntityConcernedID:RSIN

Het RSIN van de vertegenwoordigde dienstafnemer/intermediair

Attribuutnaam	urn:nl:eherkenning:1.7:EntityConcernedID:RSIN urn:nl:eherkenning:1.7:IntermediateEntityID:RSIN
Korte omschrijving	
Omschrijving	Het RSIN van de vertegenwoordigde dienstafnemer/intermediair
Formaat	Zie FI number
Betrouwbaarheidsniveaus	n.v.t.
Bron	AD, MR
Toegestaan voor ketenmachtigingen	Ja

EntityConcernedID:SubdossierNr

Het vestigingsnummer (oude formaat) van de vertegenwoordigde dienstafnemer

Attribuutnaam	urn:nl:eherkenning:1.7:EntityConcernedID:SubdossierNr
Korte omschrijving	
Omschrijving	Het vestigingsnummer (oude formaat) van de vertegenwoordigde dienstafnemer
Formaat	Zie OIN format
Betrouwbaarheidsniveaus	n.v.t.
Bron	AD, MR
Toegestaan voor ketenmachtigingen	Nee voor intermediair, Ja voor dienstafnemer

Kamer van Koophandel heeft aangekondigd te stoppen met het leveren van dit attribuut. Doorgifte van dit attribuut is op lange termijn niet gegarandeerd.

EntityConcernedID:Vestigingsnr

Het vestigingsnummer (nieuwe formaat) van de vertegenwoordigde dienstafnemer

Attribuutnaam	urn:nl:eherkenning:1.7:EntityConcernedID:Vestigingsnr
Korte omschrijving	
Omschrijving	Het vestigingsnummer (nieuwe formaat) van de vertegenwoordigde dienstafnemer
Formaat	Zie Vestigingsnummer
Betrouwbaarheidsniveaus	n.v.t.
Bron	AD, MR
Toegestaan voor ketenmachtigingen	Nee voor intermediair, Ja voor dienstafnemer

Attribuutcatalogus

Dit onderdeel beschrijft de attributen uit de attribuutcatalogus met daarbij welk type deelnemer elk attribuut mag uitleveren.

De attribuutcatalogus is op dit moment leeg. Deelnemers kunnen via het reguliere Operationeel Overleg (gremium) voo rstellen doen voor nieuw op te nemen attributen.

Elke type deelnemer MAG alleen de attributen verstrekken die gespecificeerd zijn in de XML representatie van de attribuutcatalogus. Onderstaande geeft een beter leesbare representatie maar is niet leidend.

Kenmerken van attributen

Elk attribuut wordt beschreven met een aantal kenmerken. Elk attribuut heeft de volgende kenmerken:

Attribuutnaam	Naam die uniek is voor elk attribuut. Uit de naam van het attribuut MOET de betekenis van het attribuut zo goed mogelijk kunnen worden afgeleid.
Korte omschrijving	Korte omschrijving van het attribuut. MOET worden gebruikt in de consentvraag aan de UNP in geval van persoonsgebonden attributen.
Omschrijving	Omschrijving die de betekenis van het attribuut duidelijk MOET specificeren.
Formaat	Verwijzing naar het formaat van het attribuut. Bijvoorbeeld string of integer.
Bron	De bron waar het attribuut opgevraagd KAN worden. Mogelijke waarden zijn AD en MR, of externe registers/attribuutverstrekkers.
Betrouwbaarheidsniveau	Het betrouwbaarheidsniveau waarop een attribuut verstrekt kan worden. Een attribuut kan op verschillende betrouwbaarheidsniveaus geregistreerd worden.

Betrouwbaarheidsniveaus

Een attribuut MAG op verschillende betrouwbaarheidsniveaus verstrekt worden. Deze betrouwbaarheidsniveaus komen overeen met de betrouwbaarheidsniveaus voor authenticatie. Zie ook Betrouwbaarheidsniveaus en registratie-eisen.

EH1	Op dit niveau is sprake van zelfverklaarde, niet-gevalideerde attributen. Er is dus geen controle, hooguit op syntax.
EH2	Op dit niveau is een check gedaan op juistheid, bijvoorbeeld met behulp van de administratie van de dienstafnemer.
EH3	Op dit niveau wordt een check uitgevoerd in een betrouwbare neutrale bron zoals bank of overheid (of afgeleide)
EH4	Op dit niveau wordt een realtime check gedaan in een betrouwbaar, neutraal authentiek register (bijvoorbeeld Handelsregister, GBA).

Attribuutcatalogus in XML formaat

Deze pagina beschrijft hoe de attribuutcatalogus in XML gerepresenteerd kan worden.

Op verzoek van deelnemers en/of hun klanten kunnen speciale identificerende kenmerken van beroepsbeoefenaren worden opgenomen in de attribuutcatalogus. Dergelijke identificerende kenmerken mogen alleen door deelnemers worden verstrekt als aan alle voor het betreffende kenmerk beschreven criteria voldoet wordt.

Het XML-formaat dat in deze paragraaf beschreven is, wordt enerzijds gebruikt om de attribuutcatalogus te publiceren, anderzijds door deelnemers om nieuwe attributen voor te stellen.

Om een nieuw attribuut toe te voegen moet een stukje van een attribuutcatalogus worden aangeboden. Deze moet ook opgemaakt worden volgens de hieronder beschreven specificatie. Daarin moet alleen de toevoeging of wijziging van een attribuut opgenomen worden.

Signing gebeurt met dezelfde private key waarmee ook de metadata ondertekend wordt. Zie Digital signature.

<AttributeCatalogue>

Data element	Invulling
@eh:Version	eHerkenning: Versie van de attribuutcatalogus.
@eh:IssueInstant	eHerkenning: Tijd waarop de attribuutcatalogus is aangemaakt
Signature	eHerkenning: MOET de elektronische handtekening van de partij die de attribuutcatalogus heeft aangemaakt, over het hele bericht bevatten.
eh:Attribute	eHerkenning: Eén of meerdere elementen die een attribuut specificeren met de kenmerken uit paragraaf 2.1. De volgende paragraaf beschrijft het element.

<eh:Attribute>

Data element	Invulling
eh:Name	eHerkenning: Naam van het attribuut.
eh:Type	eHerkenning: Type van het attribuut. Bijvoorbeeld “ http://www.w3.org/2001/XMLSchema#string”
eh:Register	eHerkenning: Het type deelnemer dat het attribuut mag aanbieden. Mogelijke waarden zijn AD, MR.
eh:DescriptionShort	eHerkenning: Een beknopte omschrijving van het attribuut
eh:Description	eHerkenning: Een gedetailleerde omschrijving van het attribuut zodat de betekenis van het attribuut eenduidig geïnterpreteerd wordt.
eh:BetrouwbaarheidsniveauAvailable	eHerkenning: Element dat vaker mag worden opgenomen. Geeft het betrouwbaarheidsniveau van het attribuut. Mogelijke waarden zijn 1, 2, 3 en 4.

Aanleveren attribuutcatalogus door beheerorganisatie

De geaggregeerde XML attribuutcatalogus bestaat uit een ondertekend <AttributeCatalogue> element.

De beheerorganisatie publiceert de XML attribuutcatalogus op een vaste locatie. De locatie is een niet geïndexeerde URL met server-side SSL die alleen wordt gedeeld met de deelnemers.

Daarnaast publiceert de beheerorganisatie een nieuw Attribuutcatalogus document op Confluence en www.eherkenning.nl.

Een deelnemer MOET periodiek op een vooraf door de beheerorganisatie gekozen tijdstip, de attribuutcatalogus verwerken. Dit hoeft niet op basis van de XML representatie van de attribuutcatalogus gebeuren zolang men de kenmerken van de attributen in acht neemt.

Voorbeeld › Expand source

```
<?xml version="1.0" encoding="UTF-8"?>

<AttributeCatalogue
       eh:IssueInstant="2013-09-16T14:00:00Z"
       xmlns="urn:nl:eherkenning:ac:1.7"
       xmlns:eh="urn:nl:eherkenning:ac:1.7"
       eh:Version="nl:eherkenning:1.7:A:1">

       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
             <ds:SignedInfo>
```

```
                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                    <ds:SignatureMethod

Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
                    <ds:Reference>
                           <ds:Transforms>
                                  <ds:Transform

Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                                  <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                           </ds:Transforms>
                           <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                           <ds:DigestValue></ds:DigestValue>
                    </ds:Reference>
             </ds:SignedInfo>
             <ds:SignatureValue></ds:SignatureValue>
             <ds:KeyInfo>
                    <X509Certificate> […] </X509Certificate>
             </ds:KeyInfo>
      </ds:Signature>

      <eh:Attribute>
            <Name>urn:nl:eherkenning1.3:AdditionalAttribute:BusinessAddress</Name>
            <Type>http://www.w3.org/2001/XMLSchema#string</Type>
            <Register>MR</Register>
            <DescriptionShort xml:lang="en">Business address</DescriptionShort>
            <DescriptionShort xml:lang="nl">Correspondentieadres
bedrijf</DescriptionShort>
            <Description>Adres van de dienstafnemer, in de context van de
gebruikte bevoegdheid, multiline, geschikt voor internationale postbezorging,
mogelijk niet voor bezoek.
            </Description>
            <BetrouwbaarheidsniveauAvailable>1</BetrouwbaarheidsniveauAvailable>
            <BetrouwbaarheidsniveauAvailable>2</BetrouwbaarheidsniveauAvailable>
            <BetrouwbaarheidsniveauAvailable>3</BetrouwbaarheidsniveauAvailable>
            <BetrouwbaarheidsniveauAvailable>4</BetrouwbaarheidsniveauAvailable>
      </eh:Attribute>
      <eh:Attribute>
            <Name>urn:nl:eherkenning1.3:AdditionalAttribute:BusinessEmail</Name>
            <Type>http://www.w3.org/2001/XMLSchema#string</Type>
            <Register>MR</Register>
            <DescriptionShort xml:lang="en">Business email</DescriptionShort>
            <DescriptionShort xml:lang="nl">Bedrijfsmailadres</DescriptionShort>
            <Description>E-mailadres van de handelende natuurlijk persoon, in de
context van de gebruikte bevoegdheid.</Description>
            <BetrouwbaarheidsniveauAvailable>1</BetrouwbaarheidsniveauAvailable>
```

```
            <BetrouwbaarheidsniveauAvailable>2</BetrouwbaarheidsniveauAvailable>
      </eh:Attribute>
</AttributeCatalogue>
```

Schema

Expand source

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:eh="urn:nl:eherkenning:ac:1.7"
      targetNamespace="urn:nl:eherkenning:ac:1.7"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified">

      <xs:import
            namespace="http://www.w3.org/2000/09/xmldsig#"
            schemaLocation="xmldsig-core-schema.xsd" />

      <xs:import
            namespace="http://www.w3.org/XML/1998/namespace"
            schemaLocation="http://www.w3.org/2001/xml.xsd" />

      <!--Elements -->
      <xs:element name="Attribute">
            <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="eh:Name" />
                        <xs:element ref="eh:Type" />
                        <xs:element
                              ref="eh:Register"
                              minOccurs="1"
                              maxOccurs="unbounded" />
                        <xs:element
                              ref="eh:DescriptionShort"
                              minOccurs="1"
                              maxOccurs="unbounded" />
                        <xs:element ref="eh:Description" />
                        <xs:element
                              ref="eh:BetrouwbaarheidsniveauAvailable"
                              minOccurs="1"
                              maxOccurs="4" />
                  </xs:sequence>
            </xs:complexType>
      </xs:element>

      <xs:element name="AttributeCatalogue">
            <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="ds:Signature" />
```

```
                        <xs:element
                               ref="eh:Attribute"
                               maxOccurs="unbounded" />
                </xs:sequence>
                <xs:attribute
                        ref="eh:IssueInstant"
                        use="required" />
                <xs:attribute
                        ref="eh:Version"
                        use="required" />
        </xs:complexType>
</xs:element>

<xs:element
        name="Name"
        type="xs:anyURI" />
<xs:element
        name="Type"
        type="xs:anyURI" />

<xs:element name="Register">
        <xs:simpleType>
                <xs:restriction base="xs:string">
                        <xs:enumeration value="AD" />
                        <xs:enumeration value="MR" />
                </xs:restriction>
        </xs:simpleType>
</xs:element>

<xs:element name="DescriptionShort">
        <xs:complexType>
                <xs:simpleContent>
                        <xs:extension base="eh:shortDescriptionType">
                                <xs:attribute ref="xml:lang" />
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
</xs:element>

<xs:element name="Description" type="xs:string" />

<xs:element name="BetrouwbaarheidsniveauAvailable">
        <xs:simpleType>
                <xs:restriction base="xs:string">
                      <xs:enumeration value="1" />
                        <xs:enumeration value="2" />
                        <xs:enumeration value="3" />
                        <xs:enumeration value="4" />
                </xs:restriction>
        </xs:simpleType>
</xs:element>

<xs:attribute
        name="IssueInstant"
        type="xs:dateTime" />
```

```
<xs:attribute
      name="Version"
      type="xs:anyURI" />

<xs:simpleType name="shortDescriptionType">
      <xs:restriction base="xs:string">
            <xs:maxLength value="64" />
```

```
            </xs:restriction>
      </xs:simpleType>
</xs:schema>
```

Testing

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

This document describes the tests that (aspiring) participants must perform.

To ensure that new releases and the application process of participants go smoothly, it is required that new functionality or systems are tested thoroughly before taken into production. This document distinguishes Simulator test cases and Chain test cases. The simulator tests are executed utilizing the eHerkenning simulator, an instrument for initiating requests and validating responses. Focus on these tests is conformity with the Afsprakenstelsel. Chain tests are executed in a separate network of systems, each in its own DTAP A-environment. During the chain tests, the focus is interoperability of all participants' systems.

Test cases are formulated and a check list is available on which the participants can document the test results. The Beheerorganisatie receives a filled in checklist before an applicant may join. Based on these checklist the Beheerorganisatie shall advice on the admission and/or period of the remaining trajectory. When all tests have been properly run, the Beheerorganisatie will continue to executing tests regarding the joining of the participant. These tests are basically a check on the validity of the self-declaration. The Beheerorganisatie uses the same test cases, the same testing network and the same test tooling. Based on the outcome of these tests, it is determined whether or not technical issues are remaining which should be solved before joining.

The Beheerorganisatie shall initiate penetration tests periodically, in cooperation with the participants and executed by a specialized organization. Scope of testing shall be determined for each test individually. Before executing the penetration test, permission of the participant to be tested is always required. These tests have an independent status in relation to the other tests.

This document describes the testing procedures for (aspiring) participants in the eHerkenning network. Service providers should contact their eHerkenningsmakelaar (HM) for guidance on testing their implementation.

If an eHerkenningsMakelaar would connect a service provider to the simulator or DTAP-A environments of other participants, the Beheerorganisatie does not support this. Furthermore, the eHerkenningsMakelaar is liable for any damages or delays of other participants or Beheerorganisatie, inflicted by their service providers. During chain tests and implementations of new releases, an eHerkenningsMakelaar should make sure that other participants or Beheerorganisatie are not affected in any way by their service providers.

Continue here

- Requirements for testing
  - Acquire test means — In order to facilitate chain testing, it is necessary that all participants in the network must have authentication means and corresponding authorizations of each other.
  - Announce chain test — To be able to get support from other participants in a timely manner, it is necessary that all participants are aware when a chain test will take place.
  - Exchange metadata — Within eHerkenning, all eHerkenningsmakelaars, Authenticatiediensten and Machtigingenregisters should exchange each others metadata, so the systems can verify the origin of a request and subsequently process it.
  - Process service catalog — All systems in the network must be aware of the properties of each service, in order to process authentication requests in a correct way. For this purpose, the beheerorganisatie maintains a service catalog.
- Network monitoring
- Simulator test cases
  - Generic simulator test cases
    - Error parsing — Systems must validate messages in a number of areas. Forced errors have been built into the simulator to check whether the dependencies are also validated. If the system accepts a flagged message, the result is a fail.
      - Generating a faulty digest
      - Generating a keyname-key mismatch
    - Missing fields — Essential elements may not be missing. The message must be rejected if a

mandatory element is missing. The message must be accepted if an optional element is missing. All other behaviours result in a fail.
        - Random value swaps — These tests are part of the simulator's normal behaviour. For each message, the simulator randomly determines which type of value is used. All of the values used by the simulator must be accepted.
    - Simulator test cases eHerkenningsmakelaar
        - HMS01 Normal flow
        - HMS02 Interaction with AD
        - HMS03 AD specifies MR
        - HMS04 AD does not specify MR
        - HMS05 Interaction with MR
        - HMS06 Authentication failure
        - HMS07 Authorization failure
        - HMS08 Cancel replay
        - HMS09 ForceAuthn=false
        - HMS10 Correct displaynames
        - HMS11 Non-existent ServiceID
        - HMS12 Multiple interface specifications
        - HMS13 Level of Assurance
        - HMS14 Optional attributes
        - HMS15 Chain authorization
        - HMS16 B2C
        - HMS17 Single Sign On
        - HMS18 Logout
    - Simulator test cases Authenticatiedienst
        - ADS01 Normal flow
        - ADS02 Replay normal flow
        - ADS03 Level of Assurance too high
        - ADS04 Authentication failure
        - ADS05 Cancel authentication
        - ADS06 ForceAuthn=false
        - ADS07 Optional attributes
        - ADS08 B2C
        - ADS09 B2C not supported
        - ADS10 Logout
    - Simulator test cases Machtigingenregister
        - MRS01 Normal flow
        - MRS02 Authorization request for a level of assurance that is too high
        - MRS03 Authorization check failure
        - MRS04 Non-existent ServiceID
        - MRS05 Additional attributes
        - MRS06 Chain authorization
- Chain test cases
    - Chain test cases eHerkenningsmakelaar
        - HMC01 Normal flow
        - HMC02 Cancel normal flow
        - HMC03 Cancel normal flow with replay
        - HMC04 Check IDs
        - HMC05 Single sign on
        - HMC06 Chain authorization
        - HMC07 B2C
    - Chain test cases Authenticatiedienst
        - ADC01 Normal flow
        - ADC02 Cancel normal flow
        - ADC03 Cancel and replay
        - ADC04 Single sign on
        - ADC05 B2C
        - ADC06 Logout
    - Chain test cases Machtigingenregister
        - MRC01 Normal flow
        - MRC02 Incorrect messages
        - MRC03 Chain authorization

Requirements for testing

In order to test your systems, be sure the following requirements are met.

- Acquire test means — In order to facilitate chain testing, it is necessary that all participants in the network must have authentication means and corresponding authorizations of each other.
- Announce chain test — To be able to get support from other participants in a timely manner, it is necessary that all participants are aware when a chain test will take place.
- Exchange metadata — Within eHerkenning, all eHerkenningsmakelaars, Authenticatiediensten and Machtigingenregisters should exchange each others metadata, so the systems can verify the origin of a request and subsequently process it.
- Process service catalog — All systems in the network must be aware of the properties of each service, in order to process authentication requests in a correct way. For this purpose, the beheerorganisatie maintains a service catalog.

Acquire test means

In order to facilitate chain testing, it is necessary that all participants in the network must have authentication means and corresponding authorizations of each other.

An applicant is therefore entitled to request such information from other parties. The applicant should also supply means and authorizations to the other participants when requested.

Announce chain test

To be able to get support from other participants in a timely manner, it is necessary that all participants are aware when a chain test will take place.

It is therefore required to announce a chain test. Refer to Onderhoud for more details.

Exchange metadata

Within eHerkenning, all eHerkenningsmakelaars, Authenticatiediensten and Machtigingenregisters should exchange each others metadata, so the systems can verify the origin of a request and subsequently process it.

The beheerorganisatie has a process in place to aggregate metadata and publish one file which contains all relevant metadata. For the test environment, this also contains the metadata for all simulated entities, including the simulated Dienstverlener.

Refer to Proces metadata for the process of metadata aggregation.

Process service catalog

All systems in the network must be aware of the properties of each service, in order to process authentication requests in a correct way. For this purpose, the beheerorganisatie maintains a service catalog.

For the test network, there is a separate service catalog, which holds all services which are offered by the simulated Dienstverlener.

Network monitoring

The Beheerorganisatie does not actively monitor the network's status.

It is possible to monitor the networkstatus by executing automatic tests periodically. For this purpose, participants might purchase or develop their own tooling. Whenever the participants wish to monitor the network themselves actively, they MUST use the monitoring OIN (99999900000002) which is mentioned in the service catalog.

Simulator test cases

These tests consider the conformity with the framework by connecting participants' systems to the simulator.

The participant must run through all of the test cases for the relevant roles and levels of assurance. The results must be entered in checklist. The participant must also enter the build version of the system they are testing. Only when the Beheerorganisatie determines that simulator checks are good (also based on the documented experiences and results), certification will be considered and the tests checked using this checklist.

When the Beheerorganisatie finds discrepancies, the participant will be asked to solve them and rerun the relevant test cases. The participant must then resubmit the checklist and the process restarts.
The Beheerorganisatie is at liberty to run more tests than those described here. These tests will be run to test the conformity with SAML/XACML/WS standards and best practices in the area of IT security. Should the tests reveal that the systems are still faulty, the Beheerorganisatie will contact the participant and agree on a procedure that enables the participant to resolve the errors.

Use Checklist simulator test to submit the results.

Generic simulator test cases

These test cases are equal for all roles. Some are run automatically and even randomly. Other test cases must be selected in order to run them. The general tests can be divided into three types.

- Error parsing — Systems must validate messages in a number of areas. Forced errors have been built into the simulator to check whether the dependencies are also validated. If the system accepts a flagged message, the result is a fail.
- Missing fields — Essential elements may not be missing. The message must be rejected if a mandatory element is missing. The message must be accepted if an optional element is missing. All other behaviours result in a fail.
- Random value swaps — These tests are part of the simulator's normal behaviour. For each message, the simulator randomly determines which type of value is used. All of the values used by the simulator must be accepted.

Error parsing

Systems must validate messages in a number of areas. Forced errors have been built into the simulator to check whether the dependencies are also validated. If the system accepts a flagged message, the result is a fail.

- Generating a faulty digest
- Generating a keyname-key mismatch

Generating a faulty digest

Create a good message in the simulator for the role to be tested and click Generate message. Instead of then clicking Post request, add a character to the message. Make sure you add it in a place that can't break any other functions. This corrupts the message digest. Click Post request to send the message.

- If the message is accepted, the result is a fail.
- If the recipient does not immediately abort the process, the result is a fail.

Generating a keyname-key mismatch

Check the corresponding box to send a malformed message with a keyname-key mismatch.

- If the message is accepted, the result is a fail.
- If the recipient does not immediately abort the process, the result is a fail.

Missing fields

Essential elements may not be missing. The message must be rejected if a mandatory element is missing. The message must be accepted if an optional element is missing. All other behaviours result in a fail.

> Using the simulator, manually uncheck each of the boxes or leave them empty.

- Generate a message in which an essential element is missing. Do this for each essential element or attribute for each role to be tested. Systems must reject messages that are missing an essential element and accept messages that are missing an optional element.
- Generate a message in which an essential element is empty. Do this for each essential element or attribute for each role to be tested. Systems must reject messages with an empty element.

Random value swaps

These tests are part of the simulator's normal behaviour. For each message, the simulator randomly determines which type of value is used. All of the values used by the simulator must be accepted.

All of the rejections by the systems to be tested are a fail.

1. Boolean values are generated randomly as 0/false and 1/true.
   The simulator selects the type of value to use for each Boolean. All of the different types of values must be accepted.
2. Simulator signing certificates are swapped randomly.
   The simulator has several certificates in the metadata. The simulator selects a certificate for each message. All of the certificates that are in the simulator's metadata must be accepted
3. Two simulator government IDs (GID) are swapped randomly.
   The simulated HM/AD and MR have two GIDs in the metadata. The simulator selects a GID to use for each message. All of the GIDs that are in the simulator's metadata must be accepted.
4. Several service-provider ServiceIDs are swapped randomly.
   The simulated DV has several ServiceIDs. The simulator selects one of the service provider's ServiceIDs for each message. All of the Service IDs in the service catalogue must be accepted.

Simulator test cases eHerkenningsmakelaar

- HMS01 Normal flow
- HMS02 Interaction with AD
- HMS03 AD specifies MR
- HMS04 AD does not specify MR
- HMS05 Interaction with MR

- HMS06 Authentication failure
- HMS07 Authorization failure
- HMS08 Cancel replay
- HMS09 ForceAuthn=false
- HMS10 Correct displaynames
- HMS11 Non-existent ServiceID
- HMS12 Multiple interface specifications
- HMS13 Level of Assurance
- HMS14 Optional attributes
- HMS15 Chain authorization
- HMS16 B2C
- HMS17 Single Sign On
- HMS18 Logout

HMS01 Normal flow

Description:	The normal flow process for an HM. Makes sure the messages to and from the HM are processed correctly and comply with the "afsprakenstelsel".
Steps:	1. Generate a message for the HM to be tested from the simulated DV. 2. Check the list of ADs that is displayed by the HM. Enter the findings in the checklist.
Success:	The test is successful if all of the ADs entered in the metadata are displayed.

HMS02 Interaction with AD

Description:	Makes sure the messages to and from the HM are processed correctly and comply with the "afsprakenstelsel".
Steps:	1. Generate a message for the HM to be tested from the simulated DV. 2. Select the AD simulator from the list box for the ADs. 3. Check whether the simulator has validated the message as correct. Enter the findings in the checklist.
Success:	The test is successful if the simulator validates the message from HM as correct and indicates that there are no errors.

HMS03 AD specifies MR

Description:	Makes sure the messages to and from the HM are processed correctly and comply with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated AD for the HM. Make sure the message refers to the simulated (or other) MR by entering the correct AttributeValue in AuthorizationRegistryID. (99999900000001 in the case of the simulator) 2. The AD tells the HM which MR must be used and the HM sends the tester to the corresponding MR. Enter the findings in the checklist.
Success:	The test is successful if the HM correctly processes the message from the AD and sends the tester to the corresponding MR.

HMS04 AD does not specify MR

Description:	Makes sure the messages to and from the HM are processed correctly and comply with the "afsprakenstelsel".

Steps:	1. Generate a message from the simulated DV for the HM. 2. Select the simulated AD from the list of ADs 3. Delete (on the simulated AD) the checkmark behind saml:AttributeStatement and send a 'status:Success' message to the HM. 4. Check whether the HM is requesting to select an MR. Enter the findings in the checklist.
Success:	The test is successful if the HM correctly processes the message from the AD, generates the message that the MR is unknown and displays the list of MRs.

HMS05 Interaction with MR

Description:	Makes sure the messages to and from the HM are processed correctly and comply with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. 2. Select the simulated AD from the list. 3. Delete (on the simulated AD) the checkmark in front of saml:AttributeStatement and send a 'status:Success' message to the HM. 4. The HM indicates that the MR is unknown and displays the list of MRs. 5. Select the MR simulator from the list of MRs. 6. Send a correct 'xacml-context:Decision Permit' message from the MR simulator to the HM. 7. Check whether the HMs simulator validates the received message as correct. Enter the findings in the checklist.
Success:	The test is successful if the simulated MR correctly validates the message from the HM.

HMS06 Authentication failure

Description:	Makes sure the messages to and from the HM are processed correctly and comply with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. 2. Select the simulated AD from the list 3. Force an authentication failure by checking the 'fail' box and clicking Refresh. Send the message to the HM. 4. Check the HM to determine whether the cancellation is processed correctly and the user is given the choice to select an AD again. Enter the findings in the checklist.
Success:	The test is successful if the HM responds correctly to the 'AuthnFailed' message and informs the user in step 4 that an error has occurred (without explaining the nature of the error). The HM asks the user to select a new AD.

HMS07 Authorization failure

Description:	Makes sure the process is correct and that the messages from a DV to an HM comply with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. 2. Select the AD simulator from the list. 3. Let the AD simulator send a 'status:Success' message to the HM (containing enter the location of the MR simulator in '@Destination'). 4. Go to the simulated MR and make sure that it responds with an 'xacml-context:Decision Deny' message by replacing 'xacml-context:Decision' Permit with Deny.
Success:	The test is successful if the HM responds correctly to the message that the authorization check has failed and the simulated DV receives a correct 'AuthnFailed' message.

HMS08 Cancel replay

Description:	Makes sure the process is correct and complies with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. 2. Select a (non-simulated) AD (with cancellation function) from the list. 3. Cancel the authentication on the AD and return to the HM 4. Select new/same AD
Success:	The test is successful if the HM responds correctly to the cancellation of the authentication and lets the user select another AD (and actually sends it through).

HMS09 ForceAuthn=false

Description:	Makes sure the process is correct and complies with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. Set the ForceAuthn attribute (@ForceAuthn) to false/0. 2. Select the simulated AD. 3. Make sure the ForceAutn attribute in the message received by the simulated AD is set to false/0.
Success:	The test is successful if the HM passes the correct value in the ForceAuthn attribute.

HMS10 Correct displaynames

Description:	Makes sure the process is correct and complies with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. 2. The HM must state as service: 'eHerkenning test service would like to recognize you for test service level X', whereby X is the requested level of assurance (e.g. 2 for Eh2).
Success:	The test is successful if the HM correctly passes the information in the service catalogue in the format '<OrganizationDisplayName> would like to recognize you for <ServiceName> (1) Select the provider of your eHerkenning token Note: You need an eHerkenning token that has at least level of assurance <eR level based on AuthnContextClassRef>.'

HMS11 Non-existent ServiceID

Description:	Makes sure the process is correct and complies with the "afsprakenstelsel".
Steps:	1. Generate a message from the simulated DV for the HM. Replace the ServiceID with a nonexistent ServiceID (the attribute AttributeConsumingServiceIndex) 2. A nonexistent ServiceID is considered as an incorrectly formatted message and must be processed according to Error handling : • Abort process immediately • Inform the natural person that a fatal error has occurred. • Investigate the error and inform the sender that the error occurred. The sender must investigate the error.
Success:	The test is successful if the HM correctly processes the non-existent ServiceID.

HMS12 Multiple interface specifications

Description:	Makes sure an HM is capable of correctly supporting multiple interface specifications.
Steps:	1. Repeat the above-described test cases 01 to 11 and 13 with a different version of the interface published by the HM by using a different version of the simulator (use, for example, simulator 1.5 instead of 1.7).
Success:	The test is successful if the test cases are completed successfully.

HMS13 Level of Assurance

Description:	HM makes sure that the lowest level is used in the response to the DV (weakest link principle) for the different levels of assurance for authentication and authorization and that the level of assurance meets the DV's request.
Steps:	1. Generate a message from the simulated DV for the HM to be tested. Replace the AuthnContextClassRef with level of assurance 2. 2. Select the AD simulator from the HMs list 3. Generate a response from the AD simulator. Use level of assurance 1 in AuthnContextClassRef. 4. HM must abort the process and send an AuthnFailed message to the DV. 5. Generate a message from the simulated DV for the HM to be tested. Replace the AuthnContextClassRef with level of assurance 2. 6. Select the AD simulator from the HMs list 7. Generate a response from the AD simulator. Use level of assurance 2 in AuthnContextClassRef. 8. HM sends a message to the MR simulator 9. Generate a response from the simulated MR. Use level of assurance 1 10. HM must abort the process and send an AuthnFailed message to the DV. 11. Generate a message from the simulated DV for the HM to be tested. Replace the AuthnContextClassRef with level of assurance 2. 12. Generate a response from the AD simulator. Use level of assurance 3 in AuthnContextClassRef. 13. HM sends a message to the MR simulator 14. Generate a response from the simulated MR. Use level of assurance 4 for LevelOfAssuranceUsed 15. HM sends a response to the simulated DV. Make sure AuthnContextClassRef contains level of assurance 3
Success:	The test is successful if all of the steps and checks are completed successfully.

HMS14 Optional attributes

Description:	Test the attribute assignment functionality
Steps:	1. Generate a message for the HM to be tested from the simulated DV to request additional attributes that were assigned by both the AD and the MR. 2. Select the AD simulator from the list box for the ADs. 3. Select the MR simulator from the list of MRs. 4. Check the list of 'decoded attributes' at 'DV/Response Received' to determine whether an attribute value is returned for the requested additional attributes.
Success:	The test is successful if the additional attributes are returned.

HMS15 Chain authorization

Description:	Makes sure that chain authorization is supported correctly

Steps:	1. Generate a message for the HM to be tested from the simulated DV. 2. Select the AD simulator from the list box for the ADs. 3. Go to the MR simulator 4. Check the chain authorization box 5. HM completes the authorization process and sends a response to the simulated DV
Success:	The test is successful if the simulated DV does not return any errors

HMS16 B2C

Description:	Makes sure that B2C is correctly supported
Steps:	1. Generate a message for the HM to be tested from the simulated DV for the service with ServiceID urn:nl:eherkenning:DV:99999900000003:services:1704. In the service catalogue, the EntityConcernedTypesAllowed for this service is 'Pseudo' 2. Select the AD simulator from the HMs list box. 3. Check the 'no representation' box for the AD simulator and send a response to HM. The response from the AD simulator contains a specific pseudonym instead of the internal pseudonym, the value in the Representation attribute is false and the identifying attribute 'urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo'. 4. The HM must send a successful authorization response to the DV simulator (may not send a message to the MR) 5. Make sure the DV simulator does not return any errors 6. Generate a message for the HM to be tested from the simulated DV for the service with ServiceID urn:nl:eherkenning:DV:99999900000001:services:1701, the EntityConcernedTypesAllowed for this service is 'KvK' 7. Select the AD simulator from the HMs list box. 8. Check the 'no representation' box for the AD simulator and send a response to HM. The response from the AD simulator contains a specific pseudonym instead of the internal pseudonym, the value in the Representation attribute is false and the identifying attribute 'urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo'. 9. The HM must send an authentication failure response to the DV simulator (may not send a message to an MR) 10. Make sure the DV simulator does not return any errors
Success:	The test is successful if all of the steps are processed correctly

HMS17 Single Sign On

Description:	Makes sure that SSO is correctly supported
Steps:	1. Delete all cookies from the .sso.eherkenning.nl domain 2. Generate a message for the HM to be tested from the simulated DV. 3. The HM must display a selection list with all ADs and a checkbox 'Remember this selection' 4. Select the AD simulator and check the 'Remember this selection' box. 5. Make sure the cookie called _saml_idp en domain .sso.eherkenning.nl is created. Make sure the cookie saves the base64 encoded value of the EntityID for the AD simulator, has a path prefix of '/', and is secure. 6. Complete the login process for the simulator AD by pressing the 'Create message' button. Abort the process after returning to the DV. 7. Generate a message for the HM to be tested from the simulated DV. 8. Make sure the HM goes directly to the AD simulator without displaying the AD selection screen. 9. On the AD simulator, generate an authentication failure message. 10. HM must display the AD selection screen again
Success:	The test is successful if all of the steps are processed correctly

HMS18 Logout

Description:	Handeling of logout-messages by the HM
Steps:	1. Generate a logout message from the simulated DV for the HM. 2. Select a simulated AD from the list. 3. Verify the HM correctly sends a logout message to the AD
Success:	The test is successful if the HM correctly sends a logout message to the AD.

Simulator test cases Authenticatiedienst

- ADS01 Normal flow
- ADS02 Replay normal flow
- ADS03 Level of Assurance too high
- ADS04 Authentication failure
- ADS05 Cancel authentication
- ADS06 ForceAuthn=false
- ADS07 Optional attributes
- ADS08 B2C
- ADS09 B2C not supported
- ADS10 Logout

ADS01 Normal flow

Description:	The normal flow process for an AD. Makes sure the messages to and from an AD are processed correctly and comply with the "afsprakenstelsel".
Steps:	1. Generate a message on the simulated HM for the AD. Make sure this message has the level of assurance of the test token used. 2. Go through the authentication for AD. 3. When you return to the simulator, the simulator indicates whether the received message is validated correctly. Enter the findings in the checklist. 4. If necessary, repeat steps 1 to 3 for lower levels of assurance. These levels must deliver the same result.
Success:	If the authentication is successful, the simulator validates the response from the AD as correct.

ADS02 Replay normal flow

Description:	This test makes sure that the AD correctly processes two authentication requests made in succession by the same user. When ForceAuthn=true, the AD must process each authentication request as a new one.
Steps:	1. Generate a message on the simulated HM for the AD. Make sure this message has the level of assurance of the test token used and that ForceAuthn is set to true/1. 2. Go through the authentication for AD. 3. When you return to the simulator, step 1 and 2 (for the second time) are immediately replayed. Enter the findings in the checklist.
Success:	The AD must respond to the second authentication request in the same way that it did to the first one.

ADS03 Level of Assurance too high

Description:	Makes sure the AD correctly processes an authentication request that has a higher level than the token used.
Steps:	1. Generate a message on the simulated HM for the AD. Make sure this message has a higher level of assurance than the test token used. 2. If the AD does not directly determine that it cannot process the request (for example because it does not support the requested Level of Assurance), go through the authentication for AD. 3. The AD must indicate that the requested level cannot be met for the token used. Enter the findings in the checklist. 4. If, after the message has been displayed, a successful authentication cannot be issued at the correct level, the AD must send the user back to the HM with an AuthnFailed message. Enter the findings in the checklist.
Success:	If the authentication is successful, the AD will indicate that the token used does not meet the requested authentication level and suggest the next step the person can carry out based on the error message.

ADS04 Authentication failure

Description:	Makes sure the AD correctly processes an authentication failure.
Steps:	1. Generate a message on the simulated HM for the AD. This message must have the same level as the token used. 2. Force an authentication failure by: a. entering the wrong user name b. entering the wrong password c. providing the wrong token (wrong text message code, wrong token code) 3. Repeat until all of the applicable possibilities under 2 have been depleted. Enter the findings in the checklist. 4. If applicable, repeat 1 thru 3 for the levels that are lower than that of the token used.
Success:	The AD must reject the authentication for each case. The AD must generate a generic error message for each case (e.g. 'Your user name or password is incorrect') and must suggest the next step the person can carry out based on the error message.

ADS05 Cancel authentication

Description:	Makes sure the AD correctly processes a cancelled authentication.
Steps:	1. Generate a message on the simulated HM for the AD. 2. Click on the ADs page to cancel. 3. Make sure the cancellation is successful. Enter the findings in the checklist.
Success:	After clicking on cancel, the AD returns to the simulator. The simulator validates the received message correctly. And the message contains the status code: 'urn:oasis:names:tc:SAML:2.0:status:AuthnFailed'.

ADS06 ForceAuthn=false

Description:	Makes sure a ForceAuthn=false message is correctly processed on the AD.

Steps:	1. Generate a message on the simulated HM for the AD. Set the ForceAuthn attribute (@ForceAuthn) to false. 2. The AD asks the user to authenticate. If the AD supports SSO, select the option to remember the session. 3. Walk through the full chain of authentication and authorization. 4. Generate a new message on the simulated HM for the AD. Again, set the ForceAuthn attribute (@ForceAuthn) to false. 5. If the AD supports SSO, the AD should return a valid authentication message. If the AD does not support SSO, the AD asks the user to authenticate. 6. If authentication was required in step 2, repeat steps 1 and 2. A valid authentication message must be returned when the steps have been completed.
Success:	The AD returns a valid authentication message when ForceAuthn=false providing a valid session is running on the AD.

ADS07 Optional attributes

Description:	Optional test to test the attribute assignment functionality.
Steps:	1. Generate a message from the DV simulator for the HM simulator 2. Select the AD to be tested from the selection list on the HM simulator 3. Go through the authentication for the AD 4. Make sure the HM simulator does not return any error messages. 5. Make sure all of the ADs attributes display correctly in the list of decrypted attributes on the HM simulator.
Success:	The test is successful if the additional attributes are returned.

ADS08 B2C

Description:	Optional test to test the B2C functionality
Steps:	1. Generate a message for the HM simulator to be tested from the simulated DV, replace the attribute AttributeConsumingServiceIndex with value '20'. In the service catalogue, the EntityConcernedTypesAllowed for this service is 'Pseudo' 2. Generate a message for the AD to be tested from the simulated HM. 3. If the AD supports a pseudo identifying attribute: a. Go through the authentication process for AD b. AD sends a response to HM c. Make sure the HM simulator does not return any error messages d. Make sure the Response displays status code Success, that the AtributeStatement element is present with an urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo attribute and a Representation attribute with value 'false'
Success:	The test is successful if all of the steps are performed without errors

ADS09 B2C not supported

Description:	Optional test to test the B2C functionality

Steps:	1. Generate a message for the HM simulator to be tested from the simulated DV, replace the attribute AttributeConsumingServiceIndex with value '20'. In the service catalogue, the EntityConcernedTypesAllowed for this service is 'Pseudo' 2. Generate a message for the AD to be tested from the simulated HM. 3. If the AD does not support a pseudo identifying attribute: a. Go through the authentication process for AD b. AD sends a response to HM c. Make sure the HM simulator does not return any error messages d. Make sure the status code for the response is Success, that there is no attribute urn:nl:eherkenning:1.7:EntityConcernedID:Pseudo and that the Representation attribute has the value 'true'
Success:	The test is successful if all of the steps are performed without errors

ADS10 Logout

Description:	Handling of logout-messages by the AD
Steps:	1. Walk through the normal chain of authentication and authorizations as described in ADS01 Normal flow. 2. Generate a logout message from the simulated HM for the AD. 3. Verify the AD correctly handles the logout message
Success:	The test is successful if the AD correctly handles the logout message and removes all session cookies.

Simulator test cases Machtigingenregister

- MRS01 Normal flow
- MRS02 Authorization request for a level of assurance that is too high
- MRS03 Authorization check failure
- MRS04 Non-existent ServiceID
- MRS05 Additional attributes
- MRS06 Chain authorization

MRS01 Normal flow

Description:	The normal flow process for an MR. Makes sure the messages to and from the MR are processed correctly and are compliant.
Steps:	1. Generate a message on the simulated HM for the MR. This message must contain the test token's internal pseudonym. 2. If necessary, complete the steps on the MR for a correct authorization. 3. Check the message received by the simulator. Enter the findings in the checklist. 4. Make sure EntityConcernedSubID is populated with the new subsidiary number and that OldEntityConcernedSubID is no longer sent with it.
Success:	The simulator validates the received message as correct. The message has an 'xacml-context:Decision Permit'.
Requirements:	• The MR to be tested and the simulator must have processed the most recent acceptance metadata. • The tester must have a test authorization for the MR • The tester must have the internal pseudonym that belongs to the authorization. • The tester must have access to the eHerkenning simulator.

To create the message:

1. Populate @Issuer (ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Subject1_xacml-con

with own ADs entityID. Example for KPN AD 1.5 ACC:
CONTENT=urn:nl:eherkenning:AD:00000003341158450000:entities:0001
2. Populate AuthenticationMeansID
(ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Subject1_xacml-con
with own test user's InternalPseudonym. Example:
CONTENT=a020cf994a5babbddaa7854f715a68c0730b9ec795e94958d2f077ccd566caca
3. Populate ServiceID
(ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Resource3_xacml-c
with the service that corresponds to the authorization. Example, simulator service provider 1, test service level 1:
CONTENT=urn:nl:eherkenning:DV:99999900000001:services:1
4. Populate ServiceID
(ATTR=NAME:n_xacml-samlp:XACMLAuthzDecisionQuery0_xacml-context:Request5_xacml-context:Resource3_xacml-c
with the level that corresponds to the authorization. Example for test service level 1:
CONTENT=urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

MRS02 Authorization request for a level of assurance that is too high

Description:	Makes sure that an authorization request at a level that is too high is processed correctly.
Steps:	1. Generate a message on the simulated HM for the MR. This message must contain the test token's persistent pseudonym. This message must request a higher level of assurance than that for which the test token is registered. (xacml-context:AttributeValue) 2. If necessary, complete the steps on the MR for a correct authorization. 3. Check the message received by the simulator. Enter the findings in the checklist.
Success:	The simulator validates the received message as correct. The message received by the simulator contains 'xacml-context:Decision Deny'. The MR informs the tester of the discrepancy between the authentication level and the authorization level.

MRS03 Authorization check failure

Description:	Makes sure that a failed authorization check (nonexistent persistent pseudonym) is processed correctly.
Steps:	1. Generate a message on the simulated HM for the MR. This message must contain a nonexistent persistent pseudonym. 2. The MR must report that the authorization does not exist. 3. Check the message received by the simulator. Enter the findings in the checklist.
Success:	The simulator validates the received message as correct. The message received by the simulator contains 'xacml-context:Decision Deny'.

MRS04 Non-existent ServiceID

Description:	Makes sure a nonexistent ServiceID is processed correctly.
Steps:	1. Generate a message on the simulated HM for the MR. This message must contain a nonexistent ServiceID and an existent persistent pseudonym. 2. The MR must report that the service and/or authorization does not exist.
Success:	The MR rejects messages with a nonexistent ServiceID and includes the corresponding error message in the message to the HM.

MRS05 Additional attributes

Description:	Optional test to test the attribute assignment functionality.
Steps:	1. Generate a message for the MR to be tested from the simulated HM requesting the additional attributes assigned by the MR. 2. Send a response to the MR 3. Make sure the HM simulator does not return an error message. 4. Make sure all of the MRs attributes are displayed correctly in the list of decrypted attributes on the HM simulator.
Success:	The test is successful if the additional attributes are returned and all of the steps are completed without errors.

MRS06 Chain authorization

Description:	Optional test to test the functionality of the chain authorization.
Steps:	1. Generate a message for the MR to be tested from the simulated HM using one of the simulator's internal pseudonyms. 2. Select a chain authorization for the MR, where the second link is on the MR simulator. 3. Make sure the simulated HM did not report any errors and that it states that this is a chain authorization for which the second link is obtained from the MR simulator. 4. Generate a message for the MR simulator from the simulated HM using one of the simulator's internal pseudonyms. 5. Select the MR to test from the 'second MR in the chain' selection list and click 'Refresh' 6. Send the message to the HM simulator and make sure the simulator does not return any errors
Success:	The test is successful is all of the steps are performed without errors.

Chain test cases

In these tests, the interoperability is tested in the DTAP-A environment.

For these tests it is critical that every participant has test authentication means of every other participant, for every existing or new level of assurance (see Acquire test means).

> For this to work, a participant should know the related persistent pseudonyms.

Each test case starts with initiating an authentication request by the Simulator DV (simulated service provider), requested via the POST-binding to an eHerkenningsmakelaar.

> Use Checklist chain test to submit the results.

Chain test cases eHerkenningsmakelaar

- HMC01 Normal flow
- HMC02 Cancel normal flow
- HMC03 Cancel normal flow with replay
- HMC04 Check IDs
- HMC05 Single sign on
- HMC06 Chain authorization
- HMC07 B2C

HMC01 Normal flow

Description:	The processing of normal messages by the HM. Check the correct processing and interoperability between HM and other systems within the network.
Steps:	1. Generate a message for the HM to be tested, utilizing the Simulator DV. Start with the highest level of assurance of the related means. 2. Pick an AD of the list presented by the HM. When only an MR should be tested, one should choose for the Simulator AD. 3. Authenticate at the chosen AD with the provided means. In case of the chosen AD being the Simulator AD, set the location of the MR in the @Destination attribute field. 4. Proceed to the MR related to the testing means. 5. If relevant, complete the required steps at the MR 6. Check if the Simulator DV validates the response and note observations in the checklist 7. If relevant, repeat steps 1 thru 6 for authentication means having an lower level of assurance 8. Repeat steps 1 thru 7 for every AD and MR.
Success:	This test is successful when all AD and MR systems (optionally having a testing means relationship) provide the expected results.

HMC02 Cancel normal flow

Description:	Processing the standard messages for an HM, in case of cancelling authentication by an user. Check the correct processing and interoperability between HM and AD systems in the network.
Steps:	1. Initiate a request for the HM with the simulator DV. 2. Pick an AD in the list rendered by the HM 3. Cancel authentication by pressing the Cancel button at the AD. 4. Check whether or not the HM processes canceling correctly and that the user is again offered the possibility to pick an AD. Note the observations in the checklist. 5. For each AD, repeat steps 1 thru 4
Success:	This test is successful when all AD and MR systems provide the expected results.

HMC03 Cancel normal flow with replay

Description:	Processing the standard messages for an HM, in case of cancelling authentication by an user. Check the correct processing and interoperability between HM and AD systems in the network.
Steps:	1. Initiate a request for the HM with the simulator DV. 2. Pick an AD in the list rendered by the HM 3. Cancel authentication by pressing the Cancel button at the AD. 4. Check whether or not the HM processes canceling correctly and that the user is again offered the possibility to pick an AD. Note observations in the checklist. 5. Select again the same AD as in step 2, in the list rendered by the HM. 6. Complete authentication at the AD. 7. Check whether or not the HM processes the successful authentication correctly, and that the user is forwarded. Note observations in the checklist. 8. Repeat step 1 thru 4 for every AD.
Success:	This test is successful when all AD and MR systems provide the expected results.

HMC04 Check IDs

Description:	Processing standard messages for the HM

Steps:	1. Initiate a request for the HM with the simulator DV. 2. Walk through the full chain of authentication and authorization chain. 3. Check in the response received by the Simulator DV whether the attribute NameQualifier contains the EntityID of the used MR, and whether the AuthenticatingAuthority contains the EntityID of the chosen AD. 4. Repeat steps 1 to 3 for every AD and MR combination
Success:	The test is successful when the HM supplies the different EntityID values correctly.

HMC05 Single sign on

Description:	Processing messages in the SSO flow by the HM (Single sign-on and user sessions)	
Steps:	1. Clear all stored cookies for the domain .sso.eherkenning.nl 2. Initiate a request for the HM with the simulator DV. Set @ForceAuthn to false. 3. The HM must present a list with al ADs and a checkbox stating "Bewaar selectie authenticatiedienst" 4. Pick an AD and check the checkbox. 5. Continue to the AD, check “houd mij ingelogd” and continue walking through the full chain of authentication and authorization. 6. Verify that the HM has set a cookie named _saml_idp on domain .sso.eherkenning.nl. Check this cookie holds a base64-encoded value of the EntityID of the chosen AD, the path prefix "/" and that it is a secure cookie. 7. Initiate another request for the HM with the simulator DV. Set @ForceAuthn to false. 8. Verify that the HM does not present a list with ADs and automatically redirects to the one selected earlier. 9. Verify that the AD does not request to authenticate again. 10. Check in the message, received by the simulated DV, the attributes NameQualifier, this attribute should contain the EntityID of the used MR, and the AuthenticatingAuthority, this should contain the EntityID of the used AD. 11. Repeat steps 1 thru 11 for every AD.	
Success:	This test is a success when the HM passes all EntityID's correctly	

HMC06 Chain authorization

Description:	The processing of chain authorizations for an HM (Interface specifications HM-MR 1.7 chain authorization)
Steps:	1. Initiate a request for the HM with the simulated DV. 2. Walk through the authentication at the AD (may be the simulated AD). Use a pseudonym that has a chain authorization registration at the MR. 3. Walk through the chain authorization process 4. Check in the response received by the Simulated DV whether the attribute NameQualifier contains the EntityID of the used MR, whether the AuthenticatingAuthority contains the EntityID of the chosen AD, and whether IntermediateEntityID contains the OIN of the intermediate party that exist in the chain authorization. 5. For each MR that supports chain authorizations, repeat step 1 thru 4
Success:	The test is successful if the HM correctly facilitates the process of chain authorization.

HMC07 B2C

Description:	Processing messages part of the flows that result from B2C use cases for an HM.

Steps:	1. Initiate a request for the HM with the simulator DV. 2. Go through the authentication at the AD, and use a testing means of authentication for professionals when it considers representation. 3. Check in the response received by the Simulator DV whether the attribute NameQualifier contains the EntityID of the used MR, whether the AuthenticatingAuthority contains the EntityID of the chosen AD, and whether EntityConcernedID refers to the service consumer. 4. For every AD supporting B2C, repeat steps 1 thru 3.
Success:	The test is successful when the HM processes through the flow correctly.

Chain test cases Authenticatiedienst

- ADC01 Normal flow
- ADC02 Cancel normal flow
- ADC03 Cancel and replay
- ADC04 Single sign on
- ADC05 B2C
- ADC06 Logout

ADC01 Normal flow

Description:	The normal flow through an AD. Does the AD correctly process requests from the different HMs and do the HMs react correctly on messages received from the AD.
Steps:	1. Generate a message for one of the HMs from the simulated DV, start with the highest level of assurance for which the AD is certified (saml:AuthnContextClassRef). 2. Select The AD to be tested from the list that is presented by the HM. 3. Check if the AD reacts and authenticates correctly. 4. Check if the HM redirects the user correctly to the MR that is registrered with the authentication means or if the user is requested to select the MR (if no MR is registered). Note the findings in the checklist. 5. Repeat steps 1 thru 4 for every relevant level of assurance. 6. Repeat steps 1 thru 5 for every HM.
Success:	The test is successful if all HMs produce the expected result in combination with the AD to be tested.

ADC02 Cancel normal flow

Description:	The normal flow processing by the AD. Does the AD process requests from the different HMs correctly and do the HMs act correctly on messages they receive from the AD.
Steps:	1. Generate a message to one of the HMs from the simulated DV. 2. Choose The AD to be tested from the list of ADs and proceed to this AD. 3. Cancel the authentication at the AD by clicking on the button Annuleren (Cancel). 4. Check if the HM correctly processes the AuthnFailed message and if the user can make a new AD selection. Make a note of the findings in the checklist. 5. Repeat steps 1 thru 4 for every HM in the network.
Success:	The test is successful when all HMs show the expected result, in combination with the AD to be tested.

ADC03 Cancel and replay

Description:	The normal flow processing by an AD. Does the AD process requests from the different HMs correctly and do the different HMs react correctly on messages from the AD
Steps:	1. Generate a message for one of the HMs from the simulated DV. 2. Choose The AD to be tested from the list of ADs and proceed to this AD. 3. Cancel the authentication at the AD by clicking on the button Annuleren (Cancel) 4. Check if the HM correctly processes the AuthnFailed message and if the user can make a new AD selection. 5. Select the same AD as at step 2 and check if the flow is processed exactly as normal (ADC01 Normal flow). Make a note of the findings in the checklist. 6. Repeat steps 1 thru 5 for every HM in the network.
Success:	This test is succesful when the AD to be tested shows the same behaviour during the replay of a user and a new user. During this test, all HMs in combination with the AD should produce the expected result.

ADC04 Single sign on

Description:	The SSO (Single sign-on and user sessions) flow processing by an AD
Steps:	1. Generate a message for an HM from the simulated DV. 2. Choose The AD to be tested from the list of ADs produced by the HM. 3. Proces a complete authentication and authorization chain.. 4. Generate a message for The AD to be tested from the simulated DV within 10 minutes. Make sure @IsPassive is true and @ForceAuthn is false. 5. Choose The AD to be tested at the HM. 6. Proces a complete authentication and authorization chain. 7. Generate a message for The AD to be tested from the simulated DV within 10 minutes. Make sure @IsPassive is false and @ForceAuthn is false. 8. Choose The AD to be tested at the HM 9. Proces a complete authentication and authorization chain (if the AD supports SSO, then the authentication should be handled without user interaction) 10. Check if the simulated DV receives a message with the attributes NameQualifier, which must contain the EntityID of the involved MR, and AuthenticatingAuthority, which must contain the EntityID of the involved AD. 11. Repeat steps 1 thru 10 for every HM.
Success:	The test is successful when all HM, in combination with the to be tested AD, produce the expected result.

ADC05 B2C

Description:	The processing of the B2C use case flow for an AD
Steps:	1. Generate a message for an HM from the simulated DV. 2. Go through the authentication proces at the to be tested AD, and use an authentication means for a beroepsbeoefenaar (person with a specific profession, i.e lawyers, doctors or registered accountants) without representation. 3. Check if the simulated DV receives a response message, containing the attributes NameQualifier, which contains the EntityID of the AD, and the attribute AuthenticatingAuthority, which contains the EntityID of the involved AD, and the attribute EntityConcernedID, which identifies the Dienstafnemer (service consumer). 4. Repeat steps 1 thru 3 for every HM that supports B2C.
Success:	The test is successful when all HMs, in combination with the AD to be tested, produce the expected result.

ADC06 Logout

Description:	Handeling logout messages by the AD
Steps:	1. Walk through the normal chain of authentication and authorizations as described in ADC01 Normal flow. 2. Generate a logout message from the simulated DV for the selected HM. 3. Select the AD to be tested from the list presented by the HM 4. Verify the AD correctly handles the logout message 5. Repeat the steps above for every HM
Success:	The test is successful if the AD correctly handles the logout message and removes all session cookies.

Chain test cases Machtigingenregister

- MRC01 Normal flow
- MRC02 Incorrect messages
- MRC03 Chain authorization

MRC01 Normal flow

Description:	The normal flow processing for an MR. Check correct processing and interoperability between the MR and other systems in the network.
Steps:	1. Generate a message for The HM to be tested from the simulated DV, start with the highest level of assurance of the used authentication means. 2. Select on the HM the AD to which the used authentication means belongs or use the simulated AD. 3. Finish the authentication successfully. In case you are using the simulated AD, fill in the location of the MR at "@Destination" and the persistent pseudonym at "..saml:NameID". 4. Continue at the MR that belongs with the authentication means in-use. 5. Finish all the steps necessary at the MR for a correct authorization. 6. Check if the simulated DV receives a correct message and make a note of the findings in the checklist. 7. Repeat steps 1 thru 6 also for the lower level of assurances 8. Repeat steps 1 thru 7 also for the other HMs in the network..
Success:	The test is successful when all HMs deliver the expected result in combinatie with the to be tested MR.

MRC02 Incorrect messages

Description:	Check the correct processing of incorrect messages.
Steps:	1. Generate a message at the simulated DV with a level of assurance that is too low for the requested means (authorization). 2. Select the simulated AD at the HM. 3. Finish the authentication successfully. In case you are using the simulated AD, fill in the location of the MR at "@Destination" and the persistent pseudonym at "..saml:NameID". 4. Continue at the MR that belongs with the authentication means in-use. 5. Finish, if necessary, the steps at the MR for correct authorization. 6. Check if the simulated DV receives a correct message (status:deny) and make a note of the findings in the checklist. 7. Repeat steps 1 thru 6 for all HMs in the network
Success:	The test is successful if the to be tested MR refuses levels of assurance that are too low, and does so in combination with every HM.

MRC03 Chain authorization

Description:	The chain authorization (Interface specifications HM-MR 1.7 chain authorization) flow for an MR
Steps:	1. Generate a message for an HM from the simulated DV. 2. Go through the authentication using one of the ADs (or the simulated AD). Use a pseudonym with a registered chain authorization at the MR. 3. Go through the chain authorization process. 4. Check if the simulated DV receives a message with the attributes NameQualifier, containing the EntityID or the used MR, AuthenticatingAuthority, containing the EntityID of the used AD, and IntermediateEntityID, containing the OIN of the intermediate party in the chain authorization. 5. Repeat steps 1 thru 4 for all HMs
Success:	This test is successful if the MR correctly processes the chain authorization in combination with the HM.

Beveiliging

Hier vindt u de documenten over de beveiliging van het Afsprakenstelsel eHerkenning: het informatiebeveiligingsbeleid, de stelselrisicoanalyse, het normenkader en de betrouwbaarheidsniveaus. Deze documenten bevatten informatie over de normen ten aanzien van veiligheid en de maatregelen die worden genomen om het vertrouwen en de continuïteit in het netwerk te borgen.

Deze categorie bevat de volgende onderdelen:

- Betrouwbaarheidsniveaus en registratie-eisen — Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast. Het gaat in op de wijze waarop dit aansluit op het STORK raamwerk. Het is bedoeld voor deelnemers en dienstverleners.
- Informatiebeveiliging en privacy — In het netwerk voor eHerkenning wordt informatie verwerkt die vertegenwoordigers van dienstafnemers toegang geeft tot diensten van dienstverleners. Informatiebeveiliging is essentieel voor de continuïteit van het stelsel en moet daarom worden beschouwd als integraal onderdeel van de bedrijfsvoering van de deelnemers in het netwerk en de beheerorganisatie van het netwerk.
- Normenkader Stelselaudit
- Stelsel risicoanalyse
- Gemeenschappelijk normenkader informatiebeveiliging eHerkenning — Gedetailleerde uitwerking van de vereiste maatregelen voor informatiebeveiliging.

Betrouwbaarheidsniveaus en registratie-eisen

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast. Het gaat in op de wijze waarop dit aansluit op het STORK raamwerk. Het is bedoeld voor deelnemers en dienstverleners.

Leeswijzer

- Betrouwbaarheidsniveaus eHerkenning — Ten behoeve van het verlenen van eHerkenningsdiensten moeten betrouwbaarheidsniveaus worden gebruikt om de mate van betrouwbaarheid aan te duiden van een authenticatie en bevoegdheidsvastlegging. Het betreft vier vastomschreven betrouwbaarheidsniveaus. Ieder hoger betrouwbaarheidsniveau stelt ten opzichte van het onderliggende niveau steeds verdergaande eisen aan registratie, beheer en gebruik.
- Betrouwbaarheidsniveaus van authenticatiemiddelen — Voor authenticatiemiddelen wordt het STORK raamwerk gevolgd. De elementen op basis waarvan de betrouwbaarheid van authenticatiemiddelen beoordeeld worden zijn in twee categorieën verdeeld: de eisen aan de registratiefase en de eisen aan de elektronische authenticatiefase.
- Intrekkingsverzoeken — In aanvulling op het STORK raamwerk worden expliciete eisen gesteld aan de maximale doorlooptijd van het effectueren van een intrekkingsverzoek voor authenticatiemiddelen
- Betrouwbaarheidsniveaus van bevoegdheden
- Opbouw betrouwbaarheidsniveaus eHerkenning
- Toepassing betrouwbaarheidsniveaus op aanvullende features
- STORK niveaus — Voor de gedetailleerde criteria die betrekking hebben op authenticatiemiddelen en de authenticatiedienst wordt verwezen naar het brondocument van het STORK raamwerk (document D2.3 - Quality authenticator scheme, paragraaf 2.3 en 2.4, te vinden op https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577 https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577).

Betrouwbaarheidsniveaus eHerkenning

Ten behoeve van het verlenen van eHerkenningsdiensten moeten betrouwbaarheidsniveaus worden gebruikt om de mate van betrouwbaarheid aan te duiden van een authenticatie en bevoegdheidsvastlegging. Het betreft vier vastomschreven betrouwbaarheidsniveaus. Ieder hoger betrouwbaarheidsniveau stelt ten opzichte van het onderliggende niveau steeds verdergaande eisen aan registratie, beheer en gebruik.

Dienstverleners moeten kenbaar maken welk betrouwbaarheidsniveau minimaal vereist is voor een bepaalde dienst waarvoor zij eHerkenning toepassen. Zij mogen geen specifieke authenticatiemiddelen vereisen of uitsluiten anders dan op grond van dit betrouwbaarheidsniveau. Dit minimale betrouwbaarheidsniveau moet gelden voor het te gebruiken authenticatiemiddel en voor bevoegdheden. Daarbij moet steeds gelden dat "de zwakste schakel telt". Betrouwbaarheidsniveaus moeten downwards compatibel zijn, dat wil zeggen dat op basis van authenticatiemiddelen en bevoegdheden met een hoger betrouwbaarheidsniveau ook verklaringen verstrekt worden wanneer een lager betrouwbaarheidsniveau vereist wordt.

Ten behoeve van interoperabiliteit binnen de Europese Unie past het netwerk voor eHerkenning het STORK raamwerk voor betrouwbaarheidsniveaus toe, dat een schema van "Quality Authentication Assurance" beschrijft. Dit raamwerk definieert betrouwbaarheidsniveaus voor authenticatiemiddelen. Het raamwerk is tevens als vertrekpunt gebruikt voor de classificatie van bevoegdheden. Het afsprakenstelsel zou de verdere ontwikkeling van het raamwerk in kader van STORK 2.0 project, moeten volgen. Wanneer een nieuwe versie van het raamwerk wordt vastgesteld wordt het normale wijzigingsproces gevolgd om te beslissen over toepassing en implementatie daarvan.

In het afsprakenstelsel eHerkenning is sprake van vier betrouwbaarheidsniveaus (tijdelijk zullen er 2 versies van niveau 2 beschikbaar zijn tijdens de migratieperiode).

Betrouwbaarheidsniveaus eHerkenning	Omschrijving

1	Geen of minimale betrouwbaarheid
2	Beperkte betrouwbaarheid
2+[1]	Beperkte tot redelijke betrouwbaarheid
3	Redelijke betrouwbaarheid
4	Hoge betrouwbaarheid

Deze overkoepelende eHerkennings-betrouwbaarheidsniveaus (EH) moeten tot stand komen door individuele beoordeling van de betrouwbaarheid van de in dit hoofdstuk gedefinieerde elementen aangaande bevoegdheden en authenticatiemiddelen. De uiteindelijke waardering van het betrouwbaarheidsniveau mag niet hoger zijn dan de laagste waardering per deelaspect volgens het principe "een keten is zo sterk als de zwakste schakel". Dit geheel resulteert in de samenvattende tabel in Opbouw betrouwbaarheidsniveaus eHerkenning.

Voetnoten:

1. Eerder is dit niveau NL genoemd, omdat het in tegenstelling tot de andere niveaus afwijkt van het STORK raamwerk. Dit niveau zal worden uitgefaseerd na publicatie van STORK versie 1.7. In deze versie zijn de specifieke eisen voor dit niveau alleen opgenomen in de samenvattende tabel in Opbouw betrouwbaarheidsniveaus eHerkenning.

Betrouwbaarheidsniveaus van authenticatiemiddelen

Voor authenticatiemiddelen wordt het STORK raamwerk gevolgd. De elementen op basis waarvan de betrouwbaarheid van authenticatiemiddelen beoordeeld worden zijn in twee categorieën verdeeld: de eisen aan de registratiefase en de eisen aan de elektronische authenticatiefase.

De registratiefase bepaalt de eisen die gesteld worden wanneer een dienstafnemer wil aansluiten op eHerkenning en daartoe authenticatiemiddelen aanvraagt. Het betreft de waarborgen in het proces van registratie van de uitvoerend natuurlijk persoon tot en met de uitgifte van een authenticatiemiddel aan deze uitvoerend natuurlijk persoon. Tevens volgt het betrouwbaarheidsniveau uit de mate waarin de kwaliteit van de processen en onderliggende mechanismen zijn vastgesteld bij de partij die het authenticatiemiddel uitgeeft: aan te duiden als "de kwaliteit van de organisatie" (zoals bijvoorbeeld beschreven in ETSI TS 101 456 voor betrouwbaarheidsniveau 4). De elementen die in deze categorie beoordeeld worden zijn:

- Identificatieprocedure bij middelenuitgifte
- Proces van middelenuitgifte
- Partij die het authenticatiemiddel uitgeeft

De elektronische authenticatiefase betreft het technisch deel van de betrouwbaarheidsniveaus. Het gaat daarbij om het authenticatiemiddel zelf én de wijze waarop het tijdens het gebruik functioneert. De elementen die in deze categorie beoordeeld worden zijn:

- Type en robuustheid van het authenticatiemiddel
- Zekerheid van het authenticatiemechanisme

De maatregelen die zijn getroffen om het authenticatiemechanisme op afstand c.q. via internet ("zekerheid van het authenticatiemechanisme") betrouwbaar te laten functioneren worden beoordeeld op de bescherming tegen identiteitsdiefstal. Dit betreft:

1. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden.
2. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen.
3. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller.
4. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen.
5. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt.

Voor de gedetailleerde criteria die betrekking hebben op authenticatiemiddelen en de authenticatiedienst wordt verwezen naar de betrouwbaarheidsniveaus (STORK spreekt van assurance levels) met de corresponderende nummering in het STORK-document (Document D2.3 - Quality authenticator scheme versie 1.7, paragraaf 2.3 en 2.4, te vinden op

http://www.eid-stork.eu, onder STORK materials, deliverables approved/public). In STORK niveaus is per betrouwbaarheidsniveau een Nederlandstalige toelichting bij de STORK vereisten opgenomen. In geval van eventuele verschillen tussen deze bijlage en het brondocument behorende bij het raamwerk moet de brondocumentatie van het raamwerk worden toegepast.

Voor betrouwbaarheidsniveau 2 wordt onder de gebruikelijke richtlijnen voor sterke wachtwoorden tenminste die richtlijnen verstaan welke voor DigiD burger gehanteerd worden (zie STORK niveaus).

Intrekkingsverzoeken

In aanvulling op het STORK raamwerk worden expliciete eisen gesteld aan de maximale doorlooptijd van het effectueren van een intrekkingsverzoek voor authenticatiemiddelen

, te weten:

Eis per niveau	Doorlooptijd effectueren intrekkingsverzoek
Betrouwbaarheidsniveau 1	geen eisen
Betrouwbaarheidsniveau 2/2+	elektronisch: per direct, niet-elektronisch: 2 werkdagen
Betrouwbaarheidsniveau 3	elektronisch: per direct, niet-elektronisch: 1 werkdag
Betrouwbaarheidsniveau 4	voor middelen moet PKI-Overheid worden gevolgd

T.a.v. de doorlooptijden van uitgifteprocessen van authenticatiemiddelen en registratieprocessen van bevoegdheden worden geen eisen gesteld.

Betrouwbaarheidsniveaus van bevoegdheden

- Toepassing STORK raamwerk op bevoegdheden — Onderstaand wordt uitgewerkt hoe met het STORK raamwerk als vertrekpunt de betrouwbaarheidsniveaus voor bevoegdheden moeten worden geclassificeerd.
- Het registratieproces van bevoegdheden — Onder het registreren van bevoegdheden in een machtigingenregister wordt verstaan het vastleggen van de bevoegdheid die uit een machtiging blijkt.
- De inhoud van een bevoegdheid — Bij een registratie van een bevoegdheid moeten de volgende gegevens verstrekt worden
- Detailvereisten — Enkele controles komen op meerdere plekken in de eisen voor. Hieronder wordt aangegeven hoe deze in detail uitgevoerd moeten worden
    - _i_ Verificatie in een handelsregister — Verificatie in een handelsregister vereist dat daadwerkelijk online in een handelsregister gekeken wordt naar de actuele situatie op moment van registratie. Indien gevraagd wordt naar een al dan niet origineel of gewaarmerkt uittreksel dan dient deze inzage aanvullend gedaan te worden tenzij dit uittreksel minder dan 5 dagen oud is (de wettelijke termijn voor doorgeven wijzigingen aan Handelsregister).
    - _ii_ Validatie elektronische handtekeningen — Het machtigingenregister moet de elektronische handtekening valideren aan de hand van de gehele certificaatketen en actuele intrekkingsinformatie of in geval van een niet PKI gebaseerde handtekening een validatie uitvoeren met vergelijkbare kwaliteit.
    - _iii_ Archivering van controles — Gegevens over de volgende controles ZOUDEN voor betrouwbaarheidsniveau 2 en hoger gearchiveerd MOETEN worden
    - _iv_ Identificatie van beroepsbeoefenaren — Een beroepsbeoefenaar die zich als dienstafnemer wil laten vertegenwoordigen en dus een machtiging wil laten registreren moet daartoe geïdentificeerd worden met een identificerend kenmerk horend bij de beroepsgroep. Dit gebeurt door het raadplegen van een zgn. beroepsregister voor die beroepsgroep.
- Vereisten betrouwbaarheidsaspect eerste registratie — De eisen worden hier beschreven voor de eerste registratie waarbij nog geen beheerder is aangesteld. Deze eisen gelden ook in de situatie van een eerste registratie van een wettelijke vertegenwoordiger die voor zichzelf eHerkenning aanvraagt.
    - IA - Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)
    - IO - Kwaliteit identificatieprocedure voor degene die de opgave doet
    - IG - Kwaliteit identificatieprocedure gemachtigde natuurlijk persoon

    - IR – Kwaliteit identificatieprocedure gemachtigde rechtspersoon
    - IV – Zekerheid associatie met de vertegenwoordigde dienstafnemer of intermediaire partij
    - IM – Kwaliteit van de organisatie die machtigingenregister beheert
    - PD – Geldigheidsduur van bevoegdheden
- Vereisten betrouwbaarheidsaspect herhaalde registratie — In deze paragraaf wordt beschreven welke alternatieven bestaan bij registratie door een eerder aangestelde beheerder of voor het geval van een wettelijke vertegenwoordiger die reeds een eHerkenningsmiddel bezit. Naast een eHerkenningsmiddel MOET voor de beheerder een machtiging te zijn geregistreerd voor de beheerbevoegdheid. Voor de leesbaarheid wordt verder gesproken over beheerder en daarbij wordt eveneens een wettelijke vertegenwoordiger bedoeld die zelf over een eHerkenningsmiddel beschikt
    - IA – Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer) (herhaalde registratie)
    - IO – Kwaliteit identificatieprocedure van degene die de opgave doet (herhaalde registratie)
    - PV – Kwaliteit van de verlengingsprocedure voor bevoegdheden (herhaalde registratie)
    - PI – Kwaliteit van de intrekkingsprocedure voor bevoegdheden (herhaalde registratie)
    - Kwaliteit van de schorsingsprocedure voor bevoegdheden (herhaalde registratie)
    - PR – Doorlooptijd van mutaties van bevoegdheden (herhaalde registratie)
- M – Synthese betrouwbaarheidsniveau van bevoegdheden
- Scoring

Toepassing STORK raamwerk op bevoegdheden

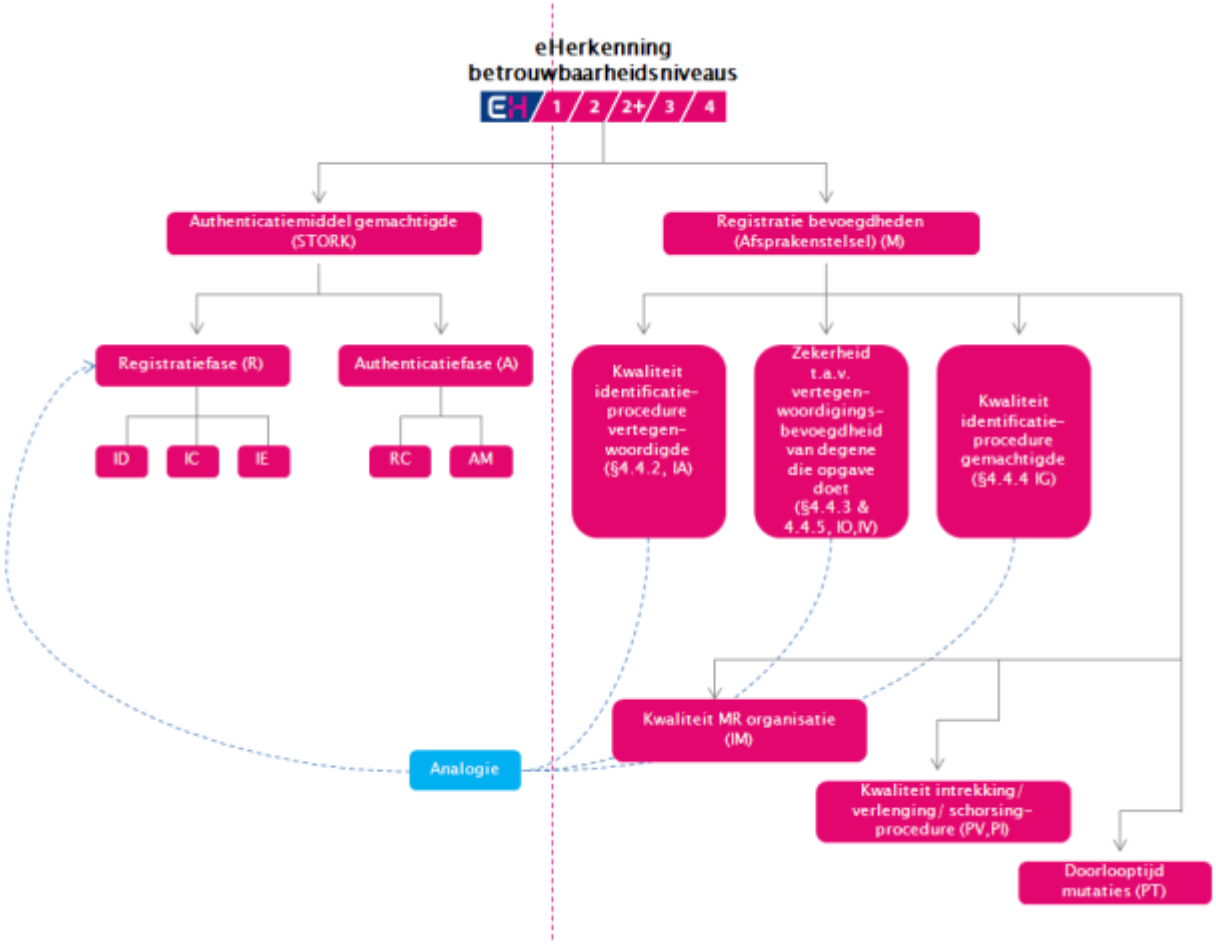
Onderstaand wordt uitgewerkt hoe met het STORK raamwerk als vertrekpunt de betrouwbaarheidsniveaus voor bevoegdheden moeten worden geclassificeerd.

Alle te beoordelen elementen hebben betrekking op het registratieproces van bevoegdheden. Het betrouwbaarheidsniveau van bevoegdheden wordt niet afhankelijk gemaakt van de elementen die als analogie van gebruik c.q. authenticatiefase voor authenticatiemiddelen gelden. Dit omdat het afsprakenstelsel voor de technische integriteit, de ondertekening en de transportbeveiliging van de verklaringen waarmee informatie over bevoegdheden tijdens gebruik wordt gecommuniceerd in alle gevallen conform het hoogste betrouwbaarheidsniveau zijn vereist (zie Interface specifications).

De volgende elementen van de registratie van bevoegdheden worden beoordeeld:

- Kwaliteit identificatieprocedure (vertegenwoordigde) dienstafnemer(vgl. STORK IDx)
- Kwaliteit identificatieprocedure uitvoerend natuurlijk persoon (vgl. STORK IDx)
- Kwaliteit identificatieprocedure intermediaire partij, indien van toepassing (vgl. STORK IDx)
- Zekerheid omtrent vertegenwoordigingsbevoegdheid van degene die de opgave doet (vgl. STORK IDx subcriterium iii). Dit vereist beoordeling van de identificatieprocedure van deze opgever evenals beoordeling van de vertegenwoordigingsbevoegdheid namens de vertegenwoordigde.
- Kwaliteit van de organisatie die het machtigingenregister beheert (vgl. STORK IEx)
- Geldigheidsduur van bevoegdheden
- Kwaliteit van de verlengingsprocedure voor bevoegdheden
- Kwaliteit van de intrekkingsprocedure voor bevoegdheden
- Kwaliteit van de schorsingsprocedure voor bevoegdheden
- Doorlooptijd van mutaties van bevoegdheden

Onderstaande figuur toont deze elementen naast de voor authenticatiemiddelen geldende elementen van STORK.



Het registratieproces van bevoegdheden

Onder het registreren van bevoegdheden in een machtigingenregister wordt verstaan het vastleggen van de bevoegdheid die uit een machtiging blijkt.

Wat een machtiging in juridische zin is, is toegelicht in Vertegenwoordiging, volmacht en machtiging. Uitgangspunt is dat deze machtiging los van de registratie in het machtigingenregister bestaat en dat het registratieproces gaat om het correct – volgens de vereisten van een bepaald betrouwbaarheidsniveau – vastleggen van gegevens over die machtiging. Voor de betrouwbaarheid is degene die de opgave doet en de vraag of deze vertegenwoordigingsbevoegd is evenzeer belangrijk als het correct vastleggen van de gegevens over de machtiging. Dit omvat ook de situatie van een wettelijke vertegenwoordiger die zelf als uitvoerend natuurlijke persoon optreedt en dit omvat ook de bevoegdheid van de eigenaar van een éénmanszaak die zelf als uitvoerend natuurlijk persoon optreedt.

Benodigde gegevens voor het registreren van een machtiging of bevoegdheid mogen zowel elektronisch als niet-elektronisch aangeleverd worden aan het machtigingenregister. Het registreren van een bevoegdheid mag worden gedaan op basis van een ondertekend geschrift (een onderhandse akte).

Het machtigingenregister moet twee functies ondersteunen:

1. Het registreren van een beheerder.
2. Reguliere registratie van bevoegdheden (i.c. beheer van bevoegdheden) door een beheerder.

De beheerder moet hetzij zelf een volledig bevoegde wettelijke vertegenwoordiger zijn van de betreffende dienstafnemer hetzij worden geregistreerd door de wettelijke vertegenwoordiger(s). De eisen aan dit registratieproces variëren per betrouwbaarheidsniveau. Machtigingen met een betrouwbaarheidsniveau dat hoger is dan datgene waarmee een beheerder wordt geregistreerd mogen niet door die beheerder worden geregistreerd noch beheerd. Iedere dienstafnemer mag meer dan één beheerder aanmelden.

Er zijn twee methoden op basis waarvan de authenticatie van de beheerder mag worden uitgevoerd voordat de beheerder

toegang krijgt tot het machtigingenregister. Ten eerste mag een machtigingenregister een eigen voorziening hebben voor authenticatie van een beheerder. Ten tweede mag een machtigingenregister gebruik maken van de authenticatiedienst van het netwerk voor eHerkenning.

Tenslotte gelden nog een aantal verdere eisen: Een deelnemer die een machtigingenregister exploiteert mag niet het beheer uitvoeren van bevoegdheden die door een dienstafnemer zijn verleend aan deze deelnemer. Naast de specificatie van de vereisten per betrouwbaarheidsniveau voor bevoegdheden, moet het machtigingenregister zorg dragen voor de betrouwbare koppeling tussen de bevoegdheid en de identificerende kenmerken. Indien het een bevoegdheid betreft die aan een authenticatiemiddel van een natuurlijk persoon gekoppeld is dan betreft dit het intern pseudoniem van de uitvoerend natuurlijk persoon. Een machtigingsverlening mag als door de gemachtigde geaccepteerd beschouwd worden zodra deze de bevoegdheid voor de eerste maal gebruikt.

- De geldigheid van de registratie van een bevoegdheid moet beperkt worden tot de opgegeven geldigheidsduur met een maximum van 5 jaar.
- Bij een registratie of mutatie (wijzigen, intrekken) van een bevoegdheid moet het machtigingenregister het resultaat van de registratie of mutatie (strekking, aard, duur en gemachtigde) bevestigen aan degene die de opgave gedaan heeft. Beheerders moeten steeds alle geregistreerde machtigingen kunnen inzien.

De inhoud van een bevoegdheid

Bij een registratie van een bevoegdheid moeten de volgende gegevens verstrekt worden

:

1. Identificerende kenmerken van de vertegenwoordigde.
2. Identificerende kenmerken van degene(/n) die de opgave van de bevoegdheid doet (de beheerder, een wettelijk vertegenwoordiger die zelf direct als beheerder optreedt of een wettelijke vertegenwoordiger die een beheerder opgeeft (op betrouwbaarheidsniveau 1 bij de score IO1 vervallen deze gegevens).
3. Identificerende kenmerken van de gemachtigde.
4. Strekking van de bevoegdheid: de afbakening van diensten en handelingen die de gemachtigde namens de vertegenwoordigde bevoegd is af te nemen of uit te voeren. De bevoegdheid kan afgebakend zijn tot een bevoegdheid 'voor derden', in het geval van een bevoegdheid verstrekt door een intermediaire partij. De bevoegdheid kan afgebakend worden naar een of meerdere vestigingen van de dienstafnemer. Deze diensten zijn gekoppeld aan de dienstencatalogus.

   > Voor betrouwbaarheidsniveau EH1 is altijd sprake van een algemene bevoegdheid voor alle diensten op dat betrouwbaarheidsniveau. Ook bij registratie van een willekeurige bevoegdheid op betrouwbaarheidsniveau EH2, EH3, en EH4 geldt dat gemachtigde automatisch alle diensten op betrouwbaarheidsniveau EH1 kan afnemen.

5. Aard van de bevoegdheid: de kenmerken die van toepassing zijn op de bevoegdheid, zoals het recht van substitutie en het zelfstandig handelen conform de bevoegdheid.

   > Ketenmachtigingen waarbij substitutie op grond van artikel 3:64 BW niet expliciet aan vertegenwoordigde gemeld hoeft te worden zijn niet toegestaan. De machtiging aan de uitvoerende natuurlijk persoon moet bij ketenmachtigingen tenminste betrouwbaarheidsniveau EH2 hebben.

6. Ingangsdatum en geldigheidsduur van de bevoegdheid

Dit geldt zowel voor de bevoegdheid van de beheerder als voor reguliere bevoegdheden. Bij een registratie van een bevoegdheid mag een beperking van de strekking tot een of meer vestigingen van de vertegenwoordigde namens welke de bevoegdheid geldt, worden opgegeven. Voor ketenmachtigingen kan deze beperking alleen voor de vertegenwoordigde dienstafnemer worden vastgelegd en niet voor intermediaire partijen.

De ten aanzien van bevoegdheden geregistreerde gegevens mogen niet worden verstrekt anders dan voor zover en conform de in het afsprakenstelsel gespecificeerde berichten.

Aan een beheerder en bij het ontbreken van een beheerder aan alle andere gemachtigden voor dezelfde dienstafnemer mogen gegevens getoond worden die noodzakelijk zijn om aan te duiden welke gemachtigden op welke betrouwbaarheidsniveaus voor de betreffende dienstafnemer bestaan. Het is de verantwoordelijkheid van de dienstafnemer om te zorgen voor toestemming voor het gebruiken en inzien van de persoonsgegevens van de gemachtigde ten behoeve van dergelijke functies. Tijdens het aanvraagproces moet toestemming gegeven worden aan de deelnemer om voor dit doel aan anderen binnen dezelfde dienstafnemer persoonsgegevens te tonen.

In het geval van ketenmachtigingen is het machtigingsregister zelf verantwoordelijk om alle beperkingen die in het kader van gebruik van de machtiging gelden vast te leggen. Indien ketenmachtigingen over meerdere machtigingenregisters verspreid zijn

kan dit betekenen dat informatie uit andere registers moet worden overgenomen of bij gebruik aan de uitvoerende natuurlijk persoon gevraagd moet worden. Dit betreft met name het machtigingsregister waarin een volgende schakel geverifieerd kan worden en de mogelijkheid om de vertegenwoordigde dienstafnemers waarvoor een machtiging in kader van een keten benut mag worden aan te duiden.

Detailvereisten

Enkele controles komen op meerdere plekken in de eisen voor. Hieronder wordt aangegeven hoe deze in detail uitgevoerd moeten worden

:

- _i_ Verificatie in een handelsregister — Verificatie in een handelsregister vereist dat daadwerkelijk online in een handelsregister gekeken wordt naar de actuele situatie op moment van registratie. Indien gevraagd wordt naar een al dan niet origineel of gewaarmerkt uittreksel dan dient deze inzage aanvullend gedaan te worden tenzij dit uittreksel minder dan 5 dagen oud is (de wettelijke termijn voor doorgeven wijzigingen aan Handelsregister).
- _ii_ Validatie elektronische handtekeningen — Het machtigingenregister moet de elektronische handtekening valideren aan de hand van de gehele certificaatketen en actuele intrekkingsinformatie of in geval van een niet PKI gebaseerde handtekening een validatie uitvoeren met vergelijkbare kwaliteit.
- _iii_ Archivering van controles — Gegevens over de volgende controles ZOUDEN voor betrouwbaarheidsniveau 2 en hoger gearchiveerd MOETEN worden
- _iv_ Identificatie van beroepsbeoefenaren — Een beroepsbeoefenaar die zich als dienstafnemer wil laten vertegenwoordigen en dus een machtiging wil laten registreren moet daartoe geïdentificeerd worden met een identificerend kenmerk horend bij de beroepsgroep. Dit gebeurt door het raadplegen van een zgn. beroepsregister voor die beroepsgroep.

Alle deelnemers MOETEN ervoor zorgdragen dat zij die persoonsgegevens verwerken die proportioneel zijn gelet op het doel - de vaststelling en verificatie van de identiteit op verschillende betrouwbaarheidsniveaus. Deelnemers MOGEN meer of minder persoonsgegevens verwerken dan hieronder als richtlijn is opgenomen, in dat geval MOETEN zij de noodzaak hiervoor hebben vastgelegd in hun procesbeschrijving. De Deelnemer MOET zorgdragen voor verwerking van de persoonsgegevens in overeenstemming met het bepaalde in de Wet bescherming persoonsgegevens.

_i_ Verificatie in een handelsregister

Verificatie in een handelsregister vereist dat daadwerkelijk online in een handelsregister gekeken wordt naar de actuele situatie op moment van registratie. Indien gevraagd wordt naar een al dan niet origineel of gewaarmerkt uittreksel dan dient deze inzage aanvullend gedaan te worden tenzij dit uittreksel minder dan 5 dagen oud is (de wettelijke termijn voor doorgeven wijzigingen aan Handelsregister).De verificatie moet zodanig worden uitgevoerd dat zowel de identificerende nummers, de naam (handelsnaam of statutaire naam) als één vestigingsadres overeenkomen. Het resultaat van deze toets moet voor de duur van tenminste 7 jaar worden gearchiveerd.

_ii_ Validatie elektronische handtekeningen

Het machtigingenregister moet de elektronische handtekening valideren aan de hand van de gehele certificaatketen en actuele intrekkingsinformatie of in geval van een niet PKI gebaseerde handtekening een validatie uitvoeren met vergelijkbare kwaliteit.De gegevens aangaande deze controle moeten worden gearchiveerd voor de duur van tenminste 7 jaar.

iii Archivering van controles

Gegevens over de volgende controles ZOUDEN voor betrouwbaarheidsniveau 2 en hoger gearchiveerd MOETEN wordenvoor de duur van tenminste 7 jaar:

- Controle van natte handtekening onder een registratieformulier ten opzichte van meegezonden (afgeschermde) kopie WID-document. Hierbij ZOU tevens het documentnummer en -type MOETEN worden gearchiveerd.
- Controle van ter plekke geplaatste natte handtekening ten opzichte van fysiek getoond origineel WID-document bij fysiek verschijnen. Hierbij moet tevens het documentnummer worden gearchiveerd.
- Controles in een handelsregister.

- Controles op basis van een banktransactie.
- Controles in het register van gestolen en vermiste WID-documenten.
- Validaties van elektronische handtekeningen
- Controles van authenticatie in elektronische registratieprocessen
- Formulieren of elektronische berichten waarin identificerende kenmerken ten behoeve van de registraties worden aangeleverd, inclusief alle verplichte bijlagen.

> Let op
> Een afgeschermde kopie WID-document (waarbij de bijzondere persoonsgegevens, te weten, pasfoto, BSN en nationaliteit, zijn afgeschermd) MAG alleen bij niveau 3 of hoger worden gearchiveerd. Een niet-afgeschermde kopie WID-document MAG alleen bij niveau 4 worden gearchiveerd.

_iv_ Identificatie van beroepsbeoefenaren

Een beroepsbeoefenaar die zich als dienstafnemer wil laten vertegenwoordigen en dus een machtiging wil laten registreren moet daartoe geïdentificeerd worden met een identificerend kenmerk horend bij de beroepsgroep. Dit gebeurt door het raadplegen van een zgn. beroepsregister voor die beroepsgroep.Dit register wordt bijgehouden door een orgaan dat daartoe door de beroepsgroep is aangewezen.

Vereisten betrouwbaarheidsaspect eerste registratie

De eisen worden hier beschreven voor de eerste registratie waarbij nog geen beheerder is aangesteld. Deze eisen gelden ook in de situatie van een eerste registratie van een wettelijke vertegenwoordiger die voor zichzelf eHerkenning aanvraagt.

In Vereisten betrouwbaarheidsaspect herhaalde registratie wordt beschreven welke alternatieven bestaan bij registratie door een eerder aangestelde beheerder of voor het geval van een wettelijke vertegenwoordiger die reeds een eHerkenningsmiddel bezit.

IA - Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)

Vereisten (IA = Identificatie dienstAfnemer)	IA0	IA1	IA2
a. De opgave van de identificerende kenmerken van de dienstafnemer mogen zonder verificatie worden overgenomen.	O	X	
b. De aangeleverde gegevens moeten de vertegenwoordigde dienstafnemer uniek identificeren en mogen gebaseerd zijn op openbare gegevens. Deze gegevens moeten geverifieerd worden in een handelsregister (_i_ Verificatie in een handelsregister) of een beroepsregister (_iv_ Identificatie van beroepsbeoefenaren). Het adres mag hetzelfde zijn als gebruikt voor verificatie IV1. Indien de strekking van de machtiging beperkt wordt tot een vestiging dan moet ten opzichte van het HR gecontroleerd worden dat het opgegeven vestigingsnummer een actuele vestiging van de betreffende dienstafnemer betreft.	O	O	X

Voor de identificatie van de vertegenwoordigde worden geen IA3 of IA4 geformuleerd. Naar analogie van STORK geldt dat de zwaardere vormen van identificatie het aanleveren van een gegeven dat alleen bij de te identificeren persoon bekend is vereisen of het fysiek verschijnen van die persoon. Voor een bedrijf worden deze eisen toegepast op degene die opgave doet, zie IO - Kwaliteit identificatieprocedure voor degene die de opgave doet.

IO - Kwaliteit identificatieprocedure voor degene die de opgave doet

Degene die de opgave doet moet de dienstafnemer vertegenwoordigen. Ook kan het voorkomen dat een wettelijke vertegenwoordiger zijn eigen bevoegdheid in het machtigingenregister laat vastleggen, in dat geval zijn wettelijke vertegenwoordiger, degene die opgave doet en de gemachtigde dezelfde persoon en vindt uiteraard slechts één identificatieprocedure plaats. Uitvoering van dit aspect kan niet los gezien worden van de identificatie van het bedrijf en de zekerheid van de associatie met het bedrijf omdat deze beide afhankelijk zijn van degene die de opgave doet. In de praktijk gaat het om de controle op een handelsregister en de aanvullende verificaties die (voor de hogere niveaus) op dezelfde

gegevens worden uitgevoerd. De eisen aan de identificatie van degene die opgave doet zijn zwaarder of tenminste even zwaar als de eisen aan de identificatie van de gemachtigde, immers de gegevens van de laatste zijn afhankelijk van de betrouwbare identificatie van de eerste. Indien het dezelfde persoon betreft gelden uiteraard de zwaarste eisen uit IO en IG.

Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
a. Geen controle van de identificatie van degene die opgave doet.	X			
b. Niet elektronische opgave. Uniek identificerende kenmerken van de wettelijke vertegenwoordiger MOETEN worden vastgelegd. De opgave ZOU ondertekend MOETEN worden door de wettelijke vertegenwoordiger met diens natte handtekening en een (afgeschermde) kopie van zijn WID-document MOET worden bijgesloten. Het machtigingenregister MOET de natte handtekening controleren aan de hand van de (afgeschermde) kopie van het WID-document (_iii_ Archivering van controles) (Eisen aan degene die opgave doet identiek aan eisen voor middelenuitgifte ID2: i.a, ii.b, iii.b.). Het machtigingenregister ZOU de (afgeschermde) kopie WID-document NIET MOETEN opslaan.	O	X		
c. Elektronische opgave (zonder reeds in bezit van eHerkenningsmiddel te zijn). Evenals (b) MOETEN uniek identificerende kenmerken van de wettelijke vertegenwoordiger worden vastgelegd. Met de opgave ZOUDEN een scan van door wettelijke vertegenwoordiger ondertekend formulier en een scan van diens (afgeschermde) WID-document MOETEN worden meegezonden. Het machtigingenregister MOET controleren dat deze twee gescande handtekeningen overeenkomen. Indien het bericht ondertekend wordt met een PKIoverheid services certificaat (_ii_ Validatie elektronische handtekeningen) op naam van de tenminste op IA2 geïdentificeerde dienstafnemer dan vervangt dit verzending en controle van gescande stukken. De (afgeschermde) scan ZOU NIET MOETEN worden opgeslagen (_iii_ Archivering van controles).	O	X		
d. Niet elektronische opgave. Evenals (b) MOETEN uniek identificerende kenmerken van de wettelijke vertegenwoordiger worden vastgelegd en de ondertekening gecontroleerd ten opzichte van meegezonden (afgeschermde) kopie. Eén van beide volgende aanvullende controles ZOU MOETEN worden uitgevoerd (Eisen aan degene die opgave doet identiek aan eisen voor middelenuitgifte ID3): • De geldigheid van het kopie WID-document MOET worden geverifieerd ten opzichte van een register van gestolen en vermiste documenten (in tegenstelling tot c mag ondertekende formulier niet door scan vervangen worden). • Een succesvolle banktransactie MOET worden uitgevoerd vanuit een bankrekening die oorspronkelijk alleen geopend kan zijn op basis van het tonen van een fysiek WID-document en waar de tennaamstelling van de bankrekening gerelateerd is aan dezelfde persoon als degene die geïdentificeerd wordt in de aangeleverde kopie van het kopie WID-document. Kopie WID-document MAG alleen in afgeschermde vorm worden opgeslagen (_iii_ Archivering van controles).	O	O	X	
e. Identificerende kenmerken als bovenstaande waarbij de wettelijke vertegenwoordiger fysiek verschijnt (of bezocht wordt) en waarbij zijn ter plekke gezette handtekening gecheckt wordt ten opzichte van zijn originele WID-document. Als alternatief mag ook een gevolmachtigde fysiek verschijnen, mits een schriftelijke ondertekende volmacht van een wettelijke vertegenwoordiger en diens kopie WID-document overlegd en gecontroleerd wordt; deze gevolmachtigde tekent ter plekke en diens handtekening wordt geverifieerd ten opzichte van zijn eigen origineel WID-document. Kopieën van WID-documenten MOGEN alleen in afgeschermde vorm worden opgeslagen (zie _iii_ Archivering van controles).	O	O	X	
f. De wettelijke vertegenwoordiger verschijnt fysiek. Evenals (b) moeten uniek identificerende kenmerken van de wettelijke vertegenwoordiger worden vastgelegd. Deze tekent ter plekke met zijn natte handtekening die geverifieerd wordt ten opzichte van zijn origineel WID-document (_iii_ Archivering van controles) (Eisen aan degene die opgave doet identiek aan eisen voor middelenuitgifte ID4) Gelet op de noodzaak voor een betrouwbare en achteraf verifieerbare controle van de identiteit ZOU op dit niveau een kopie WID-document MOETEN worden opgeslagen, die conform STORK-eisen een handtekening en pasfoto bevat.	O	O	O	X

IG - Kwaliteit identificatieprocedure gemachtigde natuurlijk persoon

De identificatie van de gemachtigde natuurlijk persoon kan gebaseerd zijn op het feit dat aanvraag van een authenticatiemiddel in een en hetzelfde proces plaatsvindt. De vereiste bewijsstukken hoeven in dat geval slechts één keer te worden verstrekt. Het STORK niveau waarop het authenticatiemiddel mag worden uitgegeven moet tenminste even hoog te zijn als het EH-betrouwbaarheidsniveau dat aan de machtiging wordt toegekend.

Indien sprake is van gescheiden processen voor middelenuitgifte en registratie van machtigingen dan moeten vereiste bewijsstukken opnieuw worden verstrekt.

Vereisten (IG = Identificatie Gemachtigde natuurlijk persoon)	IG1	IG2	IG3	IG4
a. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 1 en MAG worden geïntegreerd in dezelfde procesgang. Alleen de volledigheid van de opgave MOET worden geverifieerd. Er vindt geen validatie plaats van de identiteit van de gemachtigde natuurlijk persoon.	X			
b. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 2 en MAG worden geïntegreerd in dezelfde procesgang. Uniek identificerende kenmerken van de gemachtigde natuurlijk persoon MOETEN worden vastgelegd. Een (afgeschermde) kopie van het WID-document van de gemachtigde ZOU MOETEN worden bijgesloten maar ZOU NIET MOETEN worden opgeslagen door machtigingenregister.	O	X		
c. Als bovenstaande (b) met elektronische verzending van gescand (afgeschermd) WID-document of waarbij de gemachtigde een persoonlijke banktransactie uitvoert waarvan de tennaamstelling overeenkomt met de identificerende kenmerken.	O	X		
d. Als bovenstaande (b) waarbij in plaats van de (afgeschermde) kopie WID dezelfde wettelijke vertegenwoordiger die de opgave doet en gecontroleerd is conform tenminste IO2 in staat voor de identificatie van de gemachtigden en de daartoe aangeleverde identificerende kenmerken. Deze wettelijke vertegenwoordiger MOET een andere persoon zijn dan de gemachtigde. Consequentie is dat de uitgifte van de middelen via deze wettelijke vertegenwoordiger MOET (zijn) verlopen opdat deze degene is die de gemachtigde fysiek identificeert. Indien het een opgave betreft aangaande reeds uitgegeven middelen dan MOET de opgave hetzij een gedeeld geheim aangaande ieder afzonderlijk middel omvatten, hetzij de volledige set van uniek makende persoonsgegevens aangaande de gemachtigde die houder is van het authenticatiemiddel bevatten. Nota bene: het gedeelde geheim MAG op meerdere manieren worden gerealiseerd, bijvoorbeeld door dit bij initie?le uitgifte van middelen te verstrekken of door het in dit proces aan wettelijke vertegenwoordiger te verstrekken die het dan aan de bij hem bekende gemachtigde verstrekt waarna deze de machtiging online activeert met zijn authenticatiemiddel.	O	X		
e. Als voorgaande (d) indien de wettelijke vertegenwoordiger die de opgave doet ervoor instaat dat gecontroleerd is conform tenminste IO3. Afgeschermde kopie WID-document MAG worden opgeslagen.	O	O	X	
f. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 3 en MAG worden geïntegreerd in dezelfde procesgang. Als in (b) geldt dat uniek identificerende kenmerken van de gemachtigde MOETEN worden vastgelegd en (afgeschermde) kopie of scan van het WID-document van de gemachtigde ZOU MOETEN worden bijgesloten. De geldigheid van deze kopie MOET worden gecontroleerd ten opzichte van een register van gestolen en vermiste identiteitsdocumenten of er MOET voordat de machtiging geactiveerd wordt door de gemachtigde een succesvolle banktransactie worden uitgevoerd vanuit een bankrekening die oorspronkelijk alleen geopend kan zijn op basis van het tonen van een fysiek WID-document en waar de tenaamstelling van de bankrekening gerelateerd is aan dezelfde persoon als degene die geïdentificeerd wordt in de aangeleverde (afgeschermde) kopie van het overheidsidentiteitsdocument. Afgeschermde kopie WID-document MAG worden opgeslagen.	O	O	X	
g. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 4 en MAG worden geïntegreerd in dezelfde procesgang. Als bovenstaande (b) waarbij de identificatie van de gemachtigde wordt overgenomen uit de opgave die de vorm heeft van een onderhandse akte, door degene die opgave doet (De gemachtigde zelf moet zijn handtekening zetten in het kader van de middelenuitgifte, maar hoeft dus niet te tekenen voor acceptatie van de machtiging) ondertekend met een authenticatiemiddel met betrouwbaarheidsniveau 4 of een natte handtekening. Kopie WID-document ZOU MOETEN worden opgeslagen.	O	O	O	X

IR – Kwaliteit identificatieprocedure gemachtigde rechtspersoon

Op de identificatieprocedure van de intermediaire partij (de gemachtigde rechtspersoon) zijn dezelfde eisen van toepassing als in IA – Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer).

Vereisten (IR = Identificatie gemachtigde Rechtspersoon)	IR0	IR1	IR2
a. De opgave van de identificerende kenmerken van de intermediaire partij mogen zonder verificatie worden overgenomen.	O	X	
b. De aangeleverde gegevens moeten de intermediaire partij uniek identificeren en mogen gebaseerd zijn op openbare gegevens. Deze gegevens moeten geverifieerd worden in een handelsregister (_i_ Verificatie in een handelsregister). Het adres mag hetzelfde zijn als gebruikt voor verificatie IV1. De strekking van de machtiging aan een intermediaire partij kan niet beperkt wordt tot een vestiging.	O	O	X

Voor de identificatie van de intermediaire partij worden geen IR3 of IR4 geformuleerd. Naar analogie van STORK geldt dat de zwaardere vormen van identificatie het aanleveren van een gegeven dat alleen bij de te identificeren persoon bekend is vereisen of het fysiek verschijnen van die persoon. Voor een bedrijf worden deze eisen toegepast op degene die opgave doet, zie vorige paragraaf.

IV – Zekerheid associatie met de vertegenwoordigde dienstafnemer of intermediaire partij

Alleen in de hogere gradaties is sprake van een geverifieerde vertegenwoordigingsbevoegdheid. In de lagere gradatie is geen sprake van controle van de vertegenwoordigingsbevoegdheid van degene die de associatie goedkeurt en bestaat dus geen zekerheid over de vraag of de gemachtigde met medeweten van de wettelijke vertegenwoordigers van de dienstafnemer of intermediaire partij handelt. Dit lagere niveau is te vergelijken met "het tonen van een visitekaartje van de dienstafnemer".

Vereisten (IV = "Identificatie" Vertegenwoordiging)	IV1	IV2	IV3
a. De associatie van degene die de opgave doet met de dienstafnemer moet worden geverifieerd door de opgave via een separaat kanaal te laten bevestigen aan de hand van een organisatiekenmerk (bijvoorbeeld fysieke post, e-mail of telefoon) van de dienstafnemer, waarbij dit organisatiekenmerk door een onafhankelijke en betrouwbare partij is aangedragen of geverifieerd.	X		
b. Het machtigingenregister moet aan de hand van een handelsregister controleren dat degene die namens een dienstafnemer opgave doet (de beheerder of de wettelijk vertegenwoordiger) daartoe gerechtigd is (_i_ Verificatie in een handelsregister en _iii_ Archivering van controles). • Voor opgave namens een onderneming of een privaatrechtelijke rechtspersoon moeten de identificerende kenmerken van degene die de opgave doet overeenkomen met de gegevens waarmee deze in een handelsregister als vertegenwoordiger geregistreerd is. Voor opgave namens een publiekrechtelijke rechtspersoon kan i) ofwel dezelfde overeenkomst van identificerende kenmerken gecontroleerd worden, voor zover de natuurlijk persoon die opgave doet als functionaris op naam in een handelsregister controleerbaar is; ii) ofwel gecontroleerd worden dat er een functionaris in een handelsregister geregistreerd is die overeenkomt met de functie van degene die opgave doet. In dat geval dient degene die opgave doet aanvullend zelf te verklaren dat hij op moment van aanvragen daadwerkelijk in betreffende functie is aangesteld; iii) ofwel in het geval dat de opgave niet door de wettelijke vertegenwoordiger gedaan wordt, noch door een functionaris die aanvullend in het handelsregister is geregistreerd, op basis van de controle van een intern mandaatbesluit conform het daarvoor door de beheerorganisatie eHerkenning beheerde protocol. • Voor alle controles ten opzichte van een handelsregister geldt dat naast de overeenkomst van de identificatie van de persoon gecontroleerd moet worden dat in de vertegenwoordigingsbevoegdheid geen beperkingen zijn opgenomen die de bevoegdheid om namens de dienstafnemer bevoegdheden te laten registreren doorkruisen. • Omdat publiekrechtelijke rechtspersonen kunnen bestaan uit meerdere organisatie onderdelen met zeer verschillende taken dient het machtigingenregister te controleren of de aanvraag niet in feite slechts op één van deze onderdelen betrekking heeft en derhalve zou moeten leiden tot de tot bijbehorende vestiging beperkte machtigingen.	O	X	

Als b met de uitbreiding dat het machtigingenregister bij de eerste registratie van een gemachtigde moet controleren of er omstandigheden zijn waardoor er sprake is van bijzondere omstandigheden ten aanzien van de vertegenwoordigingsbevoegdheid, bijvoorbeeld een controle op faillissement of surseance van betaling. In dat geval moet via een separaat kanaal een aanvullende verificatie worden uitgevoerd bij de in een handelsregister vermelde wettelijke vertegenwoordiger, indien er meerdere vertegenwoordigers zijn wordt er een gekozen die niet in de aanvraag voorkomt. Bij wijziging van bevoegdheden van een bestaande gemachtigde kunnen deze controles achterwege blijven tenzij er bijzondere omstandigheden door de (beheerder van de) dienstafnemer bij het machtigingenregister gemeld zijn.	O	O	X

Protocol voor controle van interne mandaatbesluiten

Voor de controle van interne mandaatbesluiten die als alternatief voor controle in het handelsregister worden toegestaan geldt de volgende werkwijze:

- het mandaatbesluit wordt door degene die opgave doet verstrekt
- degene die opgave doet duidt aan op basis van welke in het mandaatbesluit genoemde functie hij de opgave doet
- degene die opgave doet verklaart dat hij op moment van aanvragen daadwerkelijk in betreffende functie is aangesteld
- het machtigingenregister controleert de betrouwbaarheid van het mandaatbesluit. Deze is voldoende als het betreffende besluit in officiële openbare overheidsbron als staatscourant of officiële openbaar gemaakte stukken van het bevoegde orgaan van de publiekrechtelijke rechtspersoon kan worden teruggevonden. Bij twijfel aan de betrouwbaarheid kan het machtigingenregister alsnog de wettelijke vertegenwoordiger vragen om zelf namens de rechtspersoon opgave te doen (indien deze niet al de opgave deed) of zelf een andere vertegenwoordiger van de rechtspersoon contacteren om deze te laten verklaren dat het mandaat geldig is.
- het verstrekte en gecontroleerde mandaatbesluit wordt gearchiveerd voor de duur van tenminste 7 jaar.

IM – Kwaliteit van de organisatie die machtigingenregister beheert

Vereisten (IM = "Identificatie" Machtigingsregister)	IM1	IM2	IM3
a. Er mag sprake zijn van een vorm van overheidsinstemming of overeenkomst[1] met de overheid inzake de kwaliteit van de organisatie.	X		
b. Er moet sprake zijn van een vorm van overheidsinstemming of overeenkomst met de overheid inzake de kwaliteit van de organisatie. Het feit dat de partij deelnemer is van het afsprakenstelsel voorziet hierin.	O	O	
c. Er moet sprake zijn van overheidstoezicht optioneel in de vorm van accreditatie. Tevens moet voldaan worden aan de specifieke normen voor de kwaliteit van de organisatie zoals geëist voor STORK betrouwbaarheidsniveau 4 (gekwalificeerde elektronische handtekeningen).	O	O	X

Voetnoten:

1. Deze term "overeenkomst" is binnen STORK ruim geïnterpreteerd om een legio aan mogelijkheden toe te staan, waarbij de rol van de overheid kan variëren van beperkt tot nadrukkelijk

PD – Geldigheidsduur van bevoegdheden

Vereisten (PD = Procesaspect Duur)	PD1	PD2
a. Het machtigingenregister mag een bevoegdheid die 25 maanden niet is gebruikt intrekken. Vooraf moet aan de gemachtigde, en indien aanwezig aan de beheerder, gemeld worden dat betreffende bevoegdheid binnen een bepaalde tijd wordt ingetrokken.	X	
b. Het machtigingenregister moet een bevoegdheid die 25 maanden niet is gebruikt intrekken. Vooraf moet aan de gemachtigde, en indien aanwezig aan de beheerder, gemeld worden dat betreffende bevoegdheid binnen een bepaalde tijd wordt ingetrokken.	O	X

Verlenging, intrekking en schorsing vinden altijd plaats in situatie dat er al een registratie heeft plaatsgevonden. Ook de maximale doorlooptijd heeft daarop betrekking. Deze aspecten worden derhalve beschreven in Vereisten betrouwbaarheidsaspect herhaalde registratie.

Vereisten betrouwbaarheidsaspect herhaalde registratie

In deze paragraaf wordt beschreven welke alternatieven bestaan bij registratie door een eerder aangestelde beheerder of voor het geval van een wettelijke vertegenwoordiger die reeds een eHerkenningsmiddel bezit. Naast een eHerkenningsmiddel MOET voor de beheerder een machtiging te zijn geregistreerd voor de beheerbevoegdheid. Voor de leesbaarheid wordt verder gesproken over beheerder en daarbij wordt eveneens een wettelijke vertegenwoordiger bedoeld die zelf over een eHerkenningsmiddel beschikt en de benodigde bevoegdheid heeft.

De beheerder kan ook niet-elektronisch werken. In dat geval ondertekent de beheerder steeds met natte handtekening en ZOU deze steeds ten opzichte van zijn eerder gearchiveerde handtekening MOETEN worden geverifieerd.

IA - Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer) (herhaalde registratie)

Bij elektronische opgave wordt de identificatie van de vertegenwoordigde afgeleid uit de machtiging die voor de beheerder bij diens authenticatiemiddel is geregistreerd. Deze machtiging moet tenminste hetzelfde betrouwbaarheidsniveau hebben als datgene wat ermee opgegeven wordt.

Vereisten (IA = Identificatie dienstAfnemer)	IA0	IA1	IA2
a. Vertegenwoordigde geïdentificeerd op basis van machtiging van beheerder op betrouwbaarheidsniveau EH1.	O	X	
b. Voor een niet-elektronische beheerder conform b van IA - Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)	O	O	X
Vertegenwoordigde geïdentificeerd op basis van machtiging van beheerder op betrouwbaarheidsniveau EH2 of hoger. Indien de strekking van de machtiging beperkt wordt tot een vestiging dan moet volledige controle conform b plaats vinden, tenzij het een beheerder betreft waarvan vastligt dat deze enkel beheerrechten heeft voor betreffende vestiging.	O	O	X

IO - Kwaliteit identificatieprocedure van degene die de opgave doet (herhaalde registratie)

Deze kwaliteit wordt direct bepaald door het EH-betrouwbaarheidsniveau van de beheerder.

Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
a. Beheerder met EH-betrouwbaarheidsniveau 1.	X			
b. Voor een niet-elektronische beheerder conform b van IO - Kwaliteit identificatieprocedure voor degene die de opgave doet. Aangezien het (afgeschermde) kopie WID-document al eerder gecontroleerd is door het machtigingenregister, hoeft het niet opnieuw meegezonden te worden mits het machtigingenregister de beheerder op andere wijze kan verifiëren.	O	X		
c. Beheerder met EH-betrouwbaarheidsniveau 2.	O	X		
d. Voor een niet-elektronische beheerder conform d van IO - Kwaliteit identificatieprocedure voor degene die de opgave doet. Eén van beide verificaties van de afgeschermde kopie WID, hetzij ten opzichte van een register van gestolen en vermiste documenten, hetzij ten opzichte van een persoonlijke banktransactie MOET worden herhaald voor deze beheerder. Zolang de afgeschermde kopie WID-document die al in bezit van het machtigingenregister is nog niet verlopen is, hoeft het niet opnieuw meegezonden te worden.	X	O	X	
e. Beheerder met EH-betrouwbaarheidsniveau 3.	O	O	X	
f. Beheerder met EH-betrouwbaarheidsniveau 4 die de opgave met elektronische handtekening ondertekent.	O	O	O	X

De aspecten identificatieprocedure gemachtigde, zekerheid associatie, kwaliteit van de organisatie en geldigheidsduur zijn identiek aan situatie bij initiële opgave.

PV – Kwaliteit van de verlengingsprocedure voor bevoegdheden (herhaalde registratie)

De eisen voor verlenging dienen gelijk te zijn aan de eisen voor eerste vastleggen van een bevoegdheid. Verleningen dienen altijd bevestigd te worden aan de beheerder, indien aanwezig.

Vereisten (PV = Procesaspect Verlenging)	PV1	PV2	PV3	PV4
a. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO1 en IV1.	X			
b. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO2 en IV2. De machtiging waarop de verlenging betrekking heeft wordt geïdentificeerd conform IA2 en uniek identificerende kenmerken van de gemachtigde.	O	X		
c. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO3 en IV2. De machtiging waarop de verlenging betrekking heeft wordt geïdentificeerd conform IA2 en uniek identificerende kenmerken van de gemachtigde.	O	O	X	
d. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO4 en IV2. De machtiging waarop de verlenging betrekking heeft wordt geïdentificeerd conform IA2 en uniek identificerende kenmerken van de gemachtigde.	O	O	O	X

PI – Kwaliteit van de intrekkingsprocedure voor bevoegdheden (herhaalde registratie)

Van de volgende partijen mogen intrekkingsverzoeken geaccepteerd worden: alle wettelijke vertegenwoordigers inclusief een curator, de gemachtigde zelf, de beheerder van de dienstafnemer of op last van de rechtbank.

Vereisten (PI = Procesaspect Intrekking)	PI1	PI2	PI3	PI4
a. Het intrekkingsverzoek dient schriftelijk, per e-mail of na authenticatie op betrouwbaarheidsniveau 1 te gebeuren door één van bovengenoemde partijen. Er worden geen eisen gesteld aan doorlooptijd van intrekking van authenticatiemiddelen en bevoegdheden.	X			
b. Een intrekkingsverzoek mag alleen geaccepteerd worden mits de opgever geïdentificeerd kan worden conform de eisen van tenminste IO2. Intrekking van authenticatiemiddelen en bevoegdheden moet door deelnemers als volgt uitgevoerd worden: • indien de elektronische procedure gevolgd wordt per direct en • indien het verzoek niet elektronisch wordt gedaan binnen 1 werkdag na ontvangst van het intrekkingsverzoek.	O	X		
c. Tenminste als bovenstaande waarbij de opgever geïdentificeerd kan worden conform de eisen van tenminste IO3.	O	O	X	
d. Tenminste als bovenstaande waarbij echter voor de intrekking van authenticatiemiddelen PKIoverheid gevolgd moet worden.	O	O	O	X

Kwaliteit van de schorsingsprocedure voor bevoegdheden (herhaalde registratie)

Indien schorsing (tijdelijke intrekking) wordt ondersteund, MOET aan deze minimale eisen worden voldaan:

1. Opdracht tot schorsing moet zijn gedaan door één van de volgende partijen: wettelijke vertegenwoordiger inclusief een curator, beheerder van de dienstafnemer, de gemachtigde zelf of op last van de rechtbank en voldaan aan dezelfde eisen als voor een intrekking.
2. Ongedaan maken van een schorsing moet plaatsvinden door een beheerder op het betreffende betrouwbaarheidsniveau of conform de eisen voor verlenging.

PR – Doorlooptijd van mutaties van bevoegdheden (herhaalde registratie)

Vereisten (PT = Procesaspect doorloopTijd)	PT1	PT2
a. Mutaties moeten zo snel mogelijk verwerkt worden.	X	
b. Elektronisch ingediende mutaties, inclusief intrekking van een bevoegdheid, moeten per direct verwerkt worden. Niet-elektronische mutaties moeten binnen twee werkdagen na ontvangst bij de deelnemer van het verzoek verwerkt zijn.	O	X

M – Synthese betrouwbaarheidsniveau van bevoegdheden

Bovenstaande criteria zijn geformuleerd in termen van vertegenwoordigde –gemachtigde. Dit kan toegepast worden op meerdere situaties:

- Een wettelijke vertegenwoordiger wordt geregistreerd met zijn bevoegdheid de dienstafnemer te vertegenwoordigen.
- Een wettelijke vertegenwoordiger geeft de bevoegdheid op van een uitvoerend natuurlijk persoon.
- Een wettelijke vertegenwoordiger geeft een beheerder op.
- Een beheerder doet opgave van een machtiging voor een andere gemachtigde.

In alle gevallen komt het overkoepelende betrouwbaarheidsniveau voor machtigingen zoals dat binnen eHerkenning geldt tot stand op basis van onderstaande tabel:

Criterium (betrouwbaarheid Machtiging)	M1	M2	M3	M4
Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)	IA1	IA2	IA2	IA2
Kwaliteit identificatieprocedure van degene die opgave doet	IO1	IO2	OI3	IO4
Kwaliteit identificatieprocedure gemachtigde natuurlijk persoon	IG1	IG2	IG3	IG4
Kwaliteit identificatieprocedure gemachtigde rechtspersoon	IR1	IR2	IR2	IR2
Zekerheid omtrent de associatie van degene die de opgave doet met de dienstafnemer	IV1	IV2	IV3	IV3
Kwaliteit van de organisatie die het machtigingenregister beheert	IM1	IM2	IM2	IM3
Geldigheidsduur bevoegdheden	PD1	PD2	PD2	PD2
Kwaliteit verlengingsprocedure	PV1	PV2	PV3	PV4
Kwaliteit intrekkingsprocedure (evenals schorsing)	PI1	PI2	PI3	PI4
Doorlooptijd van mutaties	PT1	PT2	PT2	PT2

De score op het aspect machtiging (aangeduid met M en volgnummer) wordt vervolgens gecombineerd met de score van het authenticatiemiddel om tot een eHerkennings-betrouwbaarheidsniveau te komen. Voor deze laatste stap zie Opbouw betrouwbaarheidsniveaus eHerkenning.

Scoring

De vereisten worden weergegeven op dezelfde wijze als in de STORK standaard. Per aspect volgt daaruit een bepaalde score.

Deze scores zijn aangeduid met twee letters en een volgnummer. Hoe hoger de betrouwbaarheid op dat aspect, hoe hoger het nummer. Een X geeft aan dat indien aan de betreffende omschrijving (regel) voldaan wordt die score (kolom) geldt. Eventuele open bolletjes daaraan voorafgaand duiden aan dat bij de hogere score ook voldaan is aan de eisen voor iedere lagere score. Indien per kolom van boven naar beneden gezocht wordt welk criterium voor betreffende score geldt dan wordt dat gevonden door de regels bij de X te nemen.

In sommige gevallen kan op twee verschillende manieren gekomen worden tot dezelfde score (zoals bij IO - Kwaliteit identificatieprocedure voor degene die de opgave doet, waar zowel b als c voldoet).

Opbouw betrouwbaarheidsniveaus eHerkenning

Het betrouwbaarheidsniveau zoals dat in eHerkenning geldt, komt tot stand door twee losstaande classificaties met elkaar te combineren, namelijk:

1. de classificatie van het authenticatiemiddel van de gemachtigde (Betrouwbaarheidsniveaus van authenticatiemiddelen), en
2. de classificatie van de betrouwbaarheid van de bevoegdheid (Betrouwbaarheidsniveaus van bevoegdheden).

Dit is weergegeven in onderstaande tabel. Ter vergelijking zijn de STORK betrouwbaarheidsniveaus vermeld.

RESULTAAT: Betrouwbaarheidsniveau eHerkenning	Betrouwbaarheidsniveau authenticatiemiddel van de betreffende gemachtigde	Classificatie t.a.v. bevoegdheden (zie 1)	Betrouwbaarheidsniveau eHerkenning van degene die de opgave doet (in geval van elektronisch proces)
EH1	STORK 1	M1	EH1
EH2	STORK 2	M2	EH2
EH2+	STORK 3 cfm versie 1.7 (zie 2)	M2 (zie 3)	EH2+
EH3	STORK 3	M3	EH3
EH4	STORK 4	M4	EH4

De laatste kolom betreft alleen de situaties waarin bevoegdheden via een elektronisch proces worden opgegeven. In die gevallen geldt de "zwakste schakel telt" regel en is derhalve voor een bepaald betrouwbaarheidsniveau een opgave door iemand die minimaal zelf gemachtigd is op dat niveau vereist.

Betrouwbaarheidsniveaus worden bepaald tijdens de registratie. Tijdens het gebruik wordt gecontroleerd op het voldoen aan het gevraagde betrouwbaarheidsniveau. Het is niet toegestaan voor een authenticatiedienst om Single Sign On (Single sign-on and user sessions) toe te passen als betrouwbaarheidsniveau 4 vereist wordt.

Voetnoten:

1. In het geval van een keten van bevoegdheden geldt voor de classificatie van de gehele transactie de schakel in de keten met de laagste betrouwbaarheid.
2. In STORK versie 1.7 zijn de eisen van het niveau dat specifiek was voor eHerkenning versie 1.4 en eerder geaccepteerd als STORK 3.
3. In de wijziging van versie 1.4 naar 1.5 zijn bij invoering van EH2 tevens aanscherpingen doorgevoerd aan EH3. Hierdoor zijn de eisen voor bevoegdheden M3 vanaf versie 1.5 zwaarder dan deze in 1.4 waren voor EH3. De eisen van M2 vanaf versie 1.5 zijn op enkele nieuwe alternatieven na gelijk aan die van M2 in versie 14 en dus ook geldend voor EH2+, echter met dien verstande dat de zwakste schakel redenering moet worden toegepast en dat waar in deze M2 eisen een STORK 2 middel vereist wordt voor EH2+ een middel dat voldoet aan het specifieke niveau vereist wordt. Daarmee is verzekerd dat de eisen voor het uit te faseren niveau EH2+ ongewijzigd zijn ten opzichte van versie 1.4.

Toepassing betrouwbaarheidsniveaus op aanvullende features

Registratie-eisen attributen

Indien een middelenuitgever of machtigingenregister attributen verstrekt (Attribuutverstrekking) dan leidt dit tot de volgende aanvullende registratieverplichtingen.

Per verstrekbaar attribuut wordt de naam conform de Attribuutcatalogus vastgesteld en welk betrouwbaarheidsniveau het

betreffende gegeven heeft.

Indien het gegevens betreft die verplicht geregistreerd worden in het kader van uitgifte van middelen (zie STORK niveaus) en/of registratie van machtigingen (als gespecificeerd in punt 1, 3 en 4 van De inhoud van een bevoegdheid) MOETEN deze minimaal gecontroleerd zijn conform het betrouwbaarheidsniveau van betreffende registratie en MOGEN op dat betrouwbaarheidsniveau worden geregistreerd conform de beschrijving in Attribuutcatalogus. Overige attributen MOGEN alleen gevraagd worden voor latere verstrekking indien deze in de attribuutcatalogus gespecificeerd zijn. Deze attributen MOGEN alleen geregistreerd worden conform de daar bepaalde registratie-eisen. Voor deze attributen geldt dat de registrerende deelnemer onweerlegbaar MOET kunnen aantonen dat deze attributen verstrekt zijn exact overeenkomstig opgave door de uitvoerend natuurlijk persoon, respectievelijk beheerder of wettelijke vertegenwoordiger of dat deze gegevens tijdens de authenticatie zijn gevalideerd in een neutraal en betrouwbaar register.

De doorlooptijd van mutaties MAG NIET langer zijn dan die welke geldt voor mutaties van machtigingen op betreffende betrouwbaarheidsniveau als vermeld in BR456 Doorlooptijd van mutaties van bevoegdheden (PT).

Iedere keer dat een uitvoerend natuurlijk persoon, beheerder of wettelijke vertegenwoordiger user consent voor verstrekking verleent MOET dit geregistreerd worden. User consent voor verstrekking van persoonsgegevens door de AD MAG NIET gevraagd worden in een dialoogvorm waarbij de defaultwaarde het geven van toestemming voor alle mogelijke persoonsgegevens inhoudt. User consent voor verstrekking van gegevens over de vertegenwoordigde dienstafnemer/intermediaire partij door de MR MAG gevraagd worden in een dialoogvorm waarbij de defaultwaarde het geven van toestemming voor alle mogelijke bedrijfsgegevens inhoudt.

Verzoeken om user consent MOETEN specifiek zijn en aan te duiden ten behoeve van welke dienstverlener en dienst de gegevens worden verstrekt. De geldigheid van een geregistreerde user consent MOET beperkt zijn tot maximaal de geldigheidsduur die conform PD - Geldigheidsduur van bevoegdheden geldt voor machtigingen op het betreffende betrouwbaarheidsniveau.

User consent MOET te allen tijde kunnen worden ingetrokken op basis van online verzoek door de uitvoerend natuurlijk persoon, beheerder of wettelijke vertegenwoordiger of MOET op het moment van de authenticatietransactie zichtbaar zijn en op dat moment kunnen worden ingetrokken.

De houder van een authenticatiemiddel respectievelijk de wettelijk vertegenwoordiger/machtigingenbeheerder MOET steeds op het betreffende betrouwbaarheidsniveau elektronisch inzage kunnen krijgen, correcties en verwijderingen kunnen aanvragen van alle over hem respectievelijk over de vertegenwoordigde dienstafnemer/intermediaire partij geregistreerde (persoons)gegevens inclusief of er doorlopende user consent voor verstrekking gegeven is.

Gebruikersgedefinieerde attributen

Bij authenticatiedienst en machtigingenregisters worden alleen die attributen vastgelegd die zijn gedefinieerd in Attribuutcatalogus. Andere, gebruikersgedefinieerde, attributen MOGEN NIET worden gebruikt.

STORK niveaus

Dit onderdeel beschrijft per betrouwbaarheidsniveau de kenmerken van de verschillende betrouwbaarheidsniveaus in STORK. Voor de gedetailleerde criteria die betrekking hebben op authenticatiemiddelen en de authenticatiedienst wordt verwezen naar het brondocument van het STORK raamwerk (document D2.3 - Quality authenticator scheme, paragraaf 2.3 en 2.4, te vinden op https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577).

In gevallen van eventuele verschillen tussen deze bijlage en het brondocument behorende bij het raamwerk moet de brondocumentatie van het raamwerk worden toegepast.

- Betrouwbaarheidsniveau 1 — Het authenticatiemiddel moet tenminste een wachtwoord of PIN zijn, (a) gekozen door de uitvoerend natuurlijk persoon of (b) automatisch gegenereerd zonder eisen aan de sterkte van het wachtwoord of PIN.
- Betrouwbaarheidsniveau 2 — Het authenticatiemiddel moet tenminste zijn: Wachtwoord op PIN gebaseerd token dat hetzij door de houder gekozen is, hetzij gegenereerd maar in beide gevallen voldoet aan gebruikelijke richtlijnen voor sterke wachtwoorden of PINcodes (voldoende lang, verschillende karakters, niet herbruikbaar, etc.) en daarom niet kwetsbaar voor raden of woordenboek aanvallen
- Betrouwbaarheidsniveau 3 — Het authenticatiemiddel is tenminste:
- Betrouwbaarheidsniveau 4 — Het authenticatiemiddel moet tenminste een gekwalificeerd certificaat zijn gebaseerd op een veilig middel zoals bedoeld in de Richtlijn Elektronische handtekeningen.

Betrouwbaarheidsniveau 1

Betrouwbaarheidsniveau 1 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten zekerheid van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst.

Registratiefase	Elektronische authenticatiefase
Identificatieprocedure	Type en robuustheid authenticatiemiddel
a. De registratie heeft tenminste met de volgende kenmerken vergelijkbare eigenschappen. Identificatie mag plaatsvinden zonder fysieke verschijning. Identificatie (niet noodzakelijk uniek) moet plaatsvinden aan de hand van een enkel kenmerk dat ook bij anderen bekend kan zijn. Validatie moet plaatsvinden aan de hand van een e-mailadres.	Het authenticatiemiddel moet tenminste een wachtwoord of PIN zijn, (a) gekozen door de uitvoerend natuurlijk persoon of (b) automatisch gegenereerd zonder eisen aan de sterkte van het wachtwoord of PIN.
Proces van middelenuitgifte	Zekerheid van het authenticatiemechanisme
b. Middelenuitgifte mag plaatsvinden zonder enige vorm van verificatie van de identiteit van de uitvoerend natuurlijk persoon.	Het authenticatiemechanisme geeft geen of nauwelijks bescherming tegen de dreigingen uit hoofdstuk 3 van het deel 4. Betrouwbaarheidsniveaus (1-factor authenticatie).
Partij die het authenticatiemiddel uitgeeft	
c. Er is geen sprake van toezicht op of accreditatie van de middelenuitgever.	

Betrouwbaarheidsniveau 2

Betrouwbaarheidsniveau 2 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten zekerheid van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst.

Registratiefase	Elektronische authenticatiefase
Identificatieprocedure	Type en robuustheid authenticatiemiddel
a. De registratie heeft tenminste met de volgende kenmerken vergelijkbare eigenschappen. Identificatie mag online plaatsvinden zonder fysieke verschijning (i.a). Unieke identificatie moet plaatsvinden aan de hand van meerdere kenmerken die ook bij anderen bekend kunnen zijn (ii.b). Validatie moet plaatsvinden door te vergelijken met een neutrale en betrouwbare derde zoals een bank, verzekeraar of overheidsinstantie (iii.b).	Het authenticatiemiddel moet tenminste zijn: Wachtwoord op PIN gebaseerd token dat hetzij door de houder gekozen is, hetzij gegenereerd maar in beide gevallen voldoet aan gebruikelijke richtlijnen voor sterke wachtwoorden of PINcodes (voldoende lang, verschillende karakters, niet herbruikbaar, etc.) en daarom niet kwetsbaar voor raden of woordenboek aanvallen (RC2).
Proces van middelenuitgifte	Zekerheid van het authenticatiemechanisme
b. Middelenuitgifte moet plaatsvinden aan de hand van lichte mate van zekerstelling van de identiteit van de uitvoerend natuurlijk persoon (bijvoorbeeld verzending van gebruikersnaam en wachtwoord in twee losse zendingen waarvan tenminste één per gewone post naar het adres van de houder zoals dat bekend is in een officiële overheidsdatabase (werkwijze van DigiD Burger basis) of download van het authenticatiemiddel van een eenmalige link die naar door de houder opgegeven e-mailadres verzonden wordt) (IC2).	Het authenticatiemechanisme is een veilig mechanisme dat enige bescherming biedt tegen de dreigingen uit hoofdstuk 3 van het deel Betrouwbaarheidsniveaus (1-factor authenticatie) (AM2).
Partij die het authenticatiemiddel uitgeeft	

c. Er moet sprake zijn van toezicht of accreditatie onder verantwoordelijkheid van de overheid. Het feit dat de partij deelnemer is van het afsprakenstelsel voorziet hierin (IE2).	

Gebruikelijke richtlijnen voor sterke wachtwoorden

Voor deze richtlijnen gelden de op enige moment voor DigiD burger basis geldende richtlijnen als minimum. Deze worden overgenomen, met uitzondering van de beperking van lengte tot maximaal 32 tekens.

Momenteel zijn deze richtlijnen:

- Het wachtwoord moet bestaan uit minimaal 8 tekens
- Bevat minimaal 1 kleine letter [a-z]
- Bevat minimaal 1 hoofdletter [A-Z]
- Bevat minimaal 1 cijfer [0-9]
- Bevat minimaal 1 bijzonder teken: [- _ ! $ % & ' . = / \ : < > | ? @ [ ] ^ ` { } ~]
- Mag niet uw gebruikersnaam bevatten
- Het wachtwoord mag niet gelijk zijn aan een van de laatste 5 wachtwoorden.

Betrouwbaarheidsniveau 3

Betrouwbaarheidsniveau 3 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten zekerheid van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst.

Registratiefase	Elektronische authenticatiefase
Identificatieprocedure (ID)	Type en robuustheid authenticatiemiddel (RC)
a. Twee varianten van de identificatieprocedure zijn toegestaan (i.b + tenminste ii.b + tenminste iii.c of i.a + tenminste ii.c + tenminste iii.d), met de volgende combinaties van kenmerken. 1. Er moet (initiële) fysieke verschijning plaats vinden op enig moment in het registratie en uitgifteproces (i.b). Unieke identificatie moet plaatsvinden aan de hand van meerdere kenmerken die ook bij anderen bekend kunnen zijn (ii.b). Validatie moet plaatsvinden aan de hand van een elektronische handtekening die niet gebaseerd hoeft te zijn op een gekwalificeerd certificaat óf door een van de ondergenoemde methoden (tenminste iii.c). 2. Identificatie mag online plaatsvinden zonder fysieke verschijning (i.a). Unieke identificatie moet plaatsvinden aan de hand van in een of ander officieel register verifieerbare kenmerken die uitsluitend bij de uitvoerend natuurlijk persoon bekend zijn (ii.c). Validatie moet plaatsvinden aan de hand van een van de ondergenoemde methoden (tenminste iii.d).	Het authenticatiemiddel is tenminste: • een soft certificaat (al of niet gekwalificeerd conform de Richtlijn Elektronische handtekeningen), • een one-time password token of een certificaat op een hardware token (niet noodzakelijk conform de Richtlijn Elektronische handtekeningen).
Proces van middelenuitgifte (IC)	Zekerheid van het authenticatiemechanisme (AM)
b. Middelenuitgifte moet plaatsvinden aan de hand van redelijke mate van zekerstelling van de identiteit van de uitvoerend natuurlijk persoon (bijvoorbeeld aan de hand van een aangetekende brief aan een gevalideerd adres, identificatie met een gekwalificeerd certificaat of downloaden aan de hand van een fysiek verkregen wachtwoord).	Het authenticatiemechanisme moet een veilig mechanisme zijn dat bescherming geeft tegen de meeste van de dreigingen uit hoofdstuk 3 van het deel Betrouwbaarheidsniveaus (2-factor authenticatie).
Partij die het authenticatiemiddel uitgeeft (IE)	
c. Er moet sprake zijn van toezicht of accreditatie onder verantwoordelijkheid van de overheid. Het feit dat de partij deelnemer is van het afsprakenstelsel voorziet hierin.	

Validatiemethoden toegelaten in de identificatieprocedure op niveau 3 (ID, iii)

Onderstaande methoden moeten gelezen worden als opeenvolgend steeds betrouwbaarder

d (tussengevoegd in STORK v1.7). De validatie vereist een verklaring van een werkgever van de aanvrager gebaseerd op een overeenkomst tussen werkgever en middelenuitgever waarin de werkgever verklaart dat hij de validatie van het fysieke en officieel WID-document, heeft uitgevoerd bij indiensttreding. Deze validatiemethode MAG NIET worden toegepast indien de werkgever dezelfde persoon is als degene die geïdentificeerd wordt.

e (tussengevoegd in STORK v1.7). De validatie vereist het aanleveren van een fotokopie of scan van een WID-document. De geldigheid van deze kopie MOET worden gecontroleerd ten opzichte van een register van gestolen en vermiste identiteitsdocumenten. De kopie ZOU alleen in afgeschermde vorm MOETEN worden opgeslagen.

f. (tussengevoegd in STORK v1.7). De validatie vereist het aanleveren van een fotokopie of scan van een WID-document. Vervolgens moet een succesvolle banktransactie worden uitgevoerd vanuit een bankrekening die oorspronkelijk alleen geopend kan zijn op basis van het tonen van een fysiek en officieel WID-document en waar de bankrekening gerelateerd is aan dezelfde persoon als degene die geïdentificeerd wordt in de aangeleverde kopie WID-document. De kopie ZOU alleen in afgeschermde vorm MOETEN worden opgeslagen.

g. (minimum in STORK tot aan v1.7 en tevens het minimum voor niveau 4). De validatie vereist het tonen van een fysieke (geen kopie) en officieel WID-document (In ieder geval valt hieronder een service van de middelenuitgever waarbij een medewerker van de middelenuitgever naar de uitvoerend natuurlijk persoon toe gaat. Een mogelijke alternatieve interpretatie is dat de uitvoerend natuurlijk persoon zijn originele officiële identiteitsdocument opstuurt of meegeeft aan iemand anders. Er is nog geen praktijkervaring of uitspraak ten aanzien van de acceptatie hiervan binnen STORK). Een kopie van dit WID-document ZOU alleen in afgeschermde vorm MOETEN worden opgeslagen.

h. De validatie vereist dat de aangeleverde gegevens ondertekend zijn met een elektronische handtekening die geverifieerd wordt bij een certificatiedienstverlener (CSP) voordat het authenticatiemiddel wordt uitgereikt.

Betrouwbaarheidsniveau 4

Betrouwbaarheidsniveau 4 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten zekerheid van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst. PKIoverheid wordt beschouwd als een invulling van betrouwbaarheidsniveau 4.

Registratiefase	Elektronische authenticatiefase
Identificatieprocedure	Type en robuustheid authenticatiemiddel
a. De registratie heeft tenminste met de volgende kenmerken vergelijkbare eigenschappen. Bij registratie en/of uitgifte moet sprake zijn van een (initiële) fysieke verschijning. Unieke identificatie moet plaatsvinden aan de hand van verifieerbare kenmerken die uitsluitend bij de uitvoerend natuurlijk persoon bekend zijn. Validatie moet plaatsvinden aan de hand van het tonen van een officieel identiteitsdocument of door een certification service provider geverifieerde elektronische handtekening.	Het authenticatiemiddel moet tenminste een gekwalificeerd certificaat zijn gebaseerd op een veilig middel zoals bedoeld in de Richtlijn Elektronische handtekeningen. PKIoverheid wordt beschouwd als een invulling van betrouwbaarheidsniveau 4.
Proces van middelenuitgifte	Zekerheid van het authenticatiemechanisme
b. Middelenuitgifte moet plaatsvinden aan de hand van een sterke mate van zekerstelling van de identiteit van de uitvoerend natuurlijk persoon (bijvoorbeeld verstrekking of activatie na fysieke identiteitsvaststelling)	Het authenticatiemechanisme moet erkend zijn als veilig mechanisme dat beschermt tegen de dreigingen uit hoofdstuk 3 van het deel 4. Betrouwbaarheidsniveaus vergelijkbaar met Common Criteria EAL 4+ (2-factor authenticatie).
Partij die het authenticatiemiddel uitgeeft	
c. Er is sprake van verplicht toezicht en optionele vrijwillige accreditatie zoals bedoeld in de Richtlijn Elektronische handtekeningen.	

Informatiebeveiliging en privacy

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

In het netwerk voor eHerkenning wordt informatie verwerkt die vertegenwoordigers van dienstafnemers toegang geeft tot diensten van dienstverleners. Informatiebeveiliging is essentieel voor de continuïteit van het stelsel en moet daarom worden beschouwd als integraal onderdeel van de bedrijfsvoering van de deelnemers in het netwerk en de beheerorganisatie van het netwerk.

Het netwerk voor eHerkenning is in essentie een 'makelaar van vertrouwen' tussen dienstafnemers en dienstverleners. Het vertrouwen van dienstverleners en dienstafnemers in het netwerk voor eHerkenning is essentieel voor het zakelijke succes ervan en wordt op twee manieren bereikt:

1. Organisatorisch en administratief door contracten en formele toetsing zoals certificatie en Third Party Mededelingen.
2. Gebruikerservaringen met de ongestoorde en veilige werking van de technische infrastructuur.

In het netwerk voor eHerkenning worden vertrouwelijke gegevens zoals identificerende persoonsgegevens, gegevens over het gebruik van diensten verwerkt. Er bestaat een wettelijke verplichting van dienstverleners, dienstafnemers, deelnemers en beheerorganisatie om dergelijke gegevens aantoonbaar afdoende te beschermen. Daarnaast wordt het netwerk in de praktijk een onmisbare schakel in de dienstverlening aan dienstafnemers. Naarmate er meer dienstverleners en meer dienstafnemers op het netwerk voor eHerkenning aangesloten worden, zal het belang van de continue werking van het netwerk toenemen en worden dus hogere eisen gesteld aan ongestoorde beschikbaarheid van de onderdelen van het netwerk.

Daarom MOET op het niveau van het stelsel verantwoording kunnen worden afgelegd over de status van de informatiebeveiliging aan de gebruikers van het stelsel en de deelnemers aan het stelsel. Deelnemers en beheerorganisatie MOETEN daarom afdoende beveiligingsmaatregelen treffen om een betrouwbare werking te garanderen.

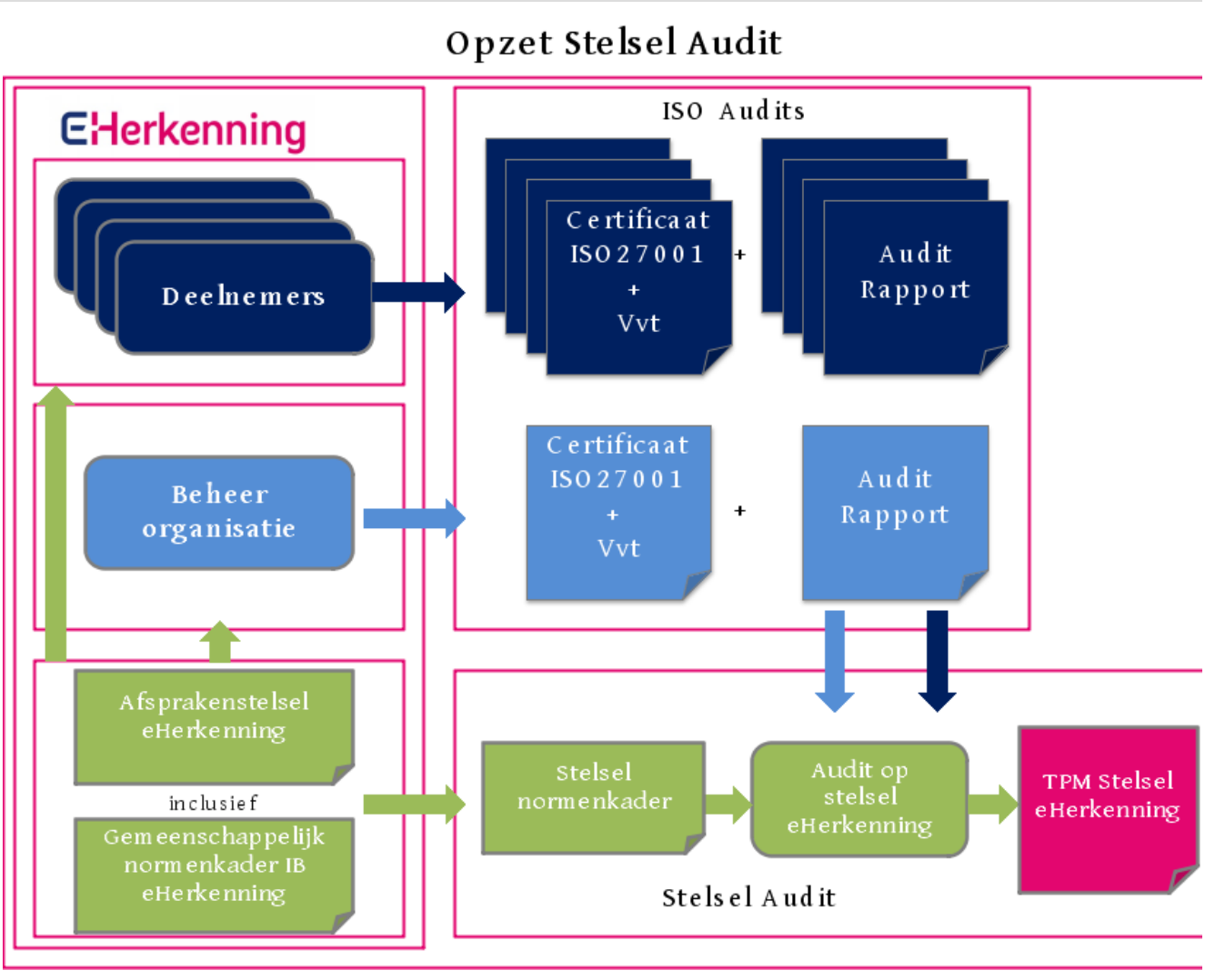
Afspraken over verantwoordelijkheid en verantwoording

1. De beheerorganisatie MOET de verantwoordelijkheid nemen voor het management van de informatiebeveiliging op het niveau van het stelsel voor eHerkenning en de externe verantwoording daarover. De beheerorganisatie MOET daartoe een Third Party Mededeling (TPM) laten afgeven over de opzet, het bestaan en de werking van de informatiebeveiliging van het stelsel eHerkenning. Voor de TPM wordt o.a. gebruikt gemaakt van de auditdossiers over de verantwoording die de deelnemers en de beheerorganisatie afleggen (zie 2).
2. Iedere deelnemer aan het stelsel en de beheerorganisatie van het stelsel MOETEN de verantwoordelijkheid nemen voor de beveiliging en controle van de eigen systemen die gebruikt worden in eHerkenning. De deelnemers en de beheerorganisatie MOETEN een systeem voor het management van informatiebeveiliging inrichten waarin minimaal hun dienstverlening voor eHerkenning MOET zijn ondergebracht. Het managementsysteem MOET zijn ingericht conform de ISO/IEC 27001 standaard en ZOU formeel MOETEN zijn gecertificeerd. Als alternatief MAG de deelnemer en de beheerorganisatie beschikken over een TPM (inclusief conformiteitsverklaring) die door een onafhankelijke Register EDP auditor is bevestigd. Hierna wordt kortweg gesproken over een TPM.
   De toetsing van opzet, bestaan en werking van geïmplementeerde controls en implementatie van de stelselafspraken over de technische invulling maken onderdeel uit van het certificaat of de TPM (inclusief conformiteitsverklaring).
3. Deelnemers die voor het eerst willen toetreden en de genoemde certificaten of TPM's nog niet kunnen overleggen MOETEN om te worden toegelaten:
   a. zelf verklaren dat zij aan de materiële eisen van ISO 27001 (inclusief het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning) voldoen, alsmede aan de gestelde eisen voor de dienstverlening van de betrouwbaarheidsniveaus die geleverd gaan worden.
   b. voorbereidingen in gang hebben gezet voor de ISO 27001 certificatie en/of een TPM van het managementsysteem voor informatiebeveiliging, zoals bedoeld in ISO 27001, alsook de specifieke eisen die zijn gesteld aan de betrouwbaarheidsniveaus van de te leveren diensten.
   c. een risicoanalyse overleggen die op de eHerkenningsdiensten betrekking heeft (en de Stelselrisicoanalyse als input heeft) met daarin aangegeven de reeds genomen, nog te nemen maatregelen en de restrisico's.
   d. een GAP-analyse overleggen waarin ten opzichte van het Gemeenschappelijke Normenkader Informatiebeveiliging is aangegeven welke maatregelen reeds zijn geïmplementeerd en welke maatregelen nog moeten worden geïmplementeerd.
4. Met ingang van 1 december 2012 geldt dat nieuwe deelnemers binnen een half jaar na hun initiële toetreding de

certificaten en/of TPM's (tevens o.b.v. het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning) MOETEN overleggen of hebben overlegd.

5. Aanpassingen in het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning moeten aantoonbaar in de audit van het certificaat zijn gereviewd door de auditor.
6. Op de toepasselijke jaarlijkse momenten MOETEN door de deelnemers aan de Beheerorganisatie de volgende bewijsstukken worden overlegd:
    a. Het ISO 27001 certificaat of TPM.
    b. Een door de auditor bevestigde verklaring dat de scope van het certificaat de dienstverlening t.b.v. eHerkenning omvat (de scopeverklaring wordt meestal op het afgegeven certificaat vermeld)
    c. De Verklaring van Toepasselijkheid (VvT) behorende bij het ISO 27001 certificaat of TPM .
7. De deelnemer MOET de Beheerorganisatie inzage geven in het auditrapport ISO 27001 certificaat en indien van toepassing Corrective Action Plan(s).
8. De Stelselauditor MOET op verzoek van de Beheerorganisatie inzage worden gegeven in de voor het netwerk relevante auditdossiers. De deelnemers MOETEN daarover afspraken maken met hun eigen onafhankelijke auditors.

Opbouw stelselverantwoording



Maatregelen voor informatiebeveiliging

Maatregelen voor informatiebeveiliging MOETEN betrekking hebben op organisatie, processen en gebruikte technologie die voor het stelsel van eHerkenning wordt ingezet door de deelnemers en de beheerorganisatie.

1. De deelnemer in het stelsel beveiligt en controleert zijn eigen systemen die hij gebruikt voor eHerkenning overeenkomstig de rol die hij vervult in het netwerk. De deelnemer MOET daarvoor de toepasselijke controls implementeren uit de norm ISO/IEC 27001/27002 en maatregelen implementeren conform het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning en dit document.
2. De beheerorganisatie beveiligt en controleert haar eigen systemen die zij gebruikt voor eHerkenning en MOET daarvoor de toepasselijke controls implementeren uit de norm ISO/IEC 27001/27002 en maatregelen implementeren conform het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning.
3. De beheerorganisatie MOET een beveiligingsplan voor het netwerk voor eHerkenning opstellen waarin de samenhang van de informatiebeveiliging binnen het netwerk is geborgd. Onderdeel van dit plan MOET o.a. de inrichting zijn van:
    a. een proces voor het melden en afhandelen van beveiligingsincidenten;
    b. een proces voor de juiste classificatie op betrouwbaarheidsniveaus conform document Betrouwbaarheidsniveaus en registratie-eisen;
    c. een proces voor de uitvoering van impactanalyses van wijzigingen in netwerk voor eHerkenning op de samenhang van de informatiebeveiliging van het netwerk;
    d. een proces voor het faciliteren en/of coördineren van (ook forensische) onderzoeken naar de toedracht en oorzaken van beveiligingsincidenten (waaronder ook fraude) en bewijs van informatietransacties;
    e. een proces voor het minimaal jaarlijks evalueren van de getroffen beveiligingsmaatregelen in het netwerk en het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning;
    f. een proces voor het uitvoeren van periodieke beveiligingstests (o.a. penetratietests) van het netwerk;
    g. een proces voor het uitvoeren van een beveiligingstest (w.o. penetratietests) op de systemen van een potentiële deelnemer voorafgaande aan de acceptatie als deelnemer;
    h. een gemeenschappelijke classificatie van de in het netwerk verwerkte gegevens inclusief de classificatie van persoonsgegevens conform de aanwijzingen van het College Bescherming Persoonsgegeven (AV23 of opvolger daarvan);
    i. een proces voor afstemming en besluitvorming over de eisen aan de inrichting van de audit trail bij de deelnemers.
4. Het bovengenoemde beveiligingsplan voor het netwerk KAN in verschillende iteraties worden ontwikkeld, bijvoorbeeld proces voor proces. Het plan wordt vastgesteld door het tactisch beheer overleg van eHerkenning. De deelnemers MOETEN aan de opstelling en de implementatie van het netwerkbreed beveiligingsplan actief meewerken, ongeacht of het maatregelen betreft in het gezamenlijke verantwoordelijkheidsdomein van het netwerk of maatregelen in het verantwoordelijkheidsdomein van de individuele deelnemer. Deelnemers MOETEN zich conformeren aan het gestelde in het beveiligingsplan.
5. De deelnemer MOET zijn verbindingen beveiligen en berichten ondertekenen conform de specificaties in de koppelvlakbeschrijvingen (Digital signature).
6. De te nemen beveiligingsmaatregelen MOETEN worden bepaald aan de hand van een risicoanalyse. De Stelsel risicoanalyse MOET als input meegenomen worden in de risicoanalyses van deelnemers en beheerorganisatie.
7. De deelnemers MOETEN aan de aansluiting van een dienstverlener of dienstafnemer de eis stellen dat de dienstverlener of dienstafnemer verantwoordelijkheid neemt voor de informatiebeveiliging van de eigen systemen van de dienstverlener of dienstafnemer.
8. Indien deelnemers voldoen aan de voorgaande afspraken 1 t/m 7, dan MOGEN deelnemers bij interconnectie NIET om aanvullende zekerheden omtrent de beveiliging van een andere deelnemer vragen bij het gezamenlijk vormgeven van dienstverlening in het kader van het netwerk.
9. De beheerorganisatie MOET het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning en de Stelsel risicoanalyse opstellen en beheren:
10. Het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning MOET generieke beveiligingseisen bevatten die voor elke rol in het netwerk van toepassing zijn. De generieke eisen omvatten minimaal de beveiligingseisen aan koppelvlakken, berichten en verbindingen en het beheer daarvan en de inrichting van het management voor informatiebeveiliging.
11. Het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning ZOU naast de generieke eisen ook specifieke eisen MOETEN stellen die verschillen per rol in het netwerk.
12. Het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning ZOU onderscheid MOETEN maken naar toepasselijkheid voor de verschillende betrouwbaarheidsniveaus van de aan te bieden eHerkenningsdiensten.

Beheer Stelselrisicoanalyse en Gemeenschappelijk Normenkader Informatiebeveiliging

De beheerorganisatie MOET de Stelsel risicoanalyse en het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning onderhouden:

1. Tenminste jaarlijks of bij gebeurtenissen met een grotere impact op het netwerk MOET de Stelsel risicoanalyse worden herijkt om te bezien of beoordeling van de gedefinieerde stelselrisico's nog actueel is, of risico's kunnen vervallen of nieuwe risico's moeten worden toegevoerd en gemitigeerd.
2. Tenminste jaarlijks of bij gebeurtenissen met een grotere impact op het netwerk MOET het gemeenschappelijke

normenkader MOETEN worden herijkt met medeneming van de resultaten van de herijkte Stelselrisicoanalyse.
3. De herijkingen van de Stelselrisicoanalyse en het normenkader MOETEN door de beheerorganisatie worden geïnitieerd en ZOUDEN minimaal MOETEN worden uitgevoerd met een representatieve vertegenwoordiging vanuit de deelnemers.
4. De beheerorganisatie MOET er zorg voor dragen dat de vaststelling van de herijkte Stelselrisicoanalyse en het herijkte normenkader het wijzigingsproces van het stelsel doorloopt. Herijkte Stelselrisicoanalyse en normenkader worden door de beheerorganisatie ingebracht in het Tactisch Overleg ter vaststelling en het Tactisch Overleg besluit tevens over de datum waarop de herijkte risicoanalyse en het herijkte normenkader van kracht is.
5. De beheerorganisatie MOET er voor zorgdragen dat de herijkte risicoanalyse en het herijkte normenkader voor de vastgestelde datum formeel ter beschikking komen van de deelnemers en van formele kandidaat-deelnemers.
6. De beheerorganisatie MOET een controleplan opstellen voor alle activiteiten die nodig zijn om het beheer van de stelselrisicoanalyse, het gemeenschappelijk normenkader en de stelselaudit uit te voeren.
7. De beheerorganisatie MOET het versiebeheer van de Stelselrisicoanalyse en het normenkader voeren. Dit betekent eveneens dat de beheerorganisatie per deelnemer MOET bijhouden welke versie van het normenkader van toepassing was bij de audits in het kader van de certificering.

Implementatie Gemeenschappelijk Normenkader Informatiebeveiliging en certificatie

Het gemeenschappelijke normenkader is opgesteld op basis van de analyse van de risico's die voor het stelsel als geheel relevant zijn. Dit betekent ook dat alleen die maatregelen (normen) zijn geselecteerd die van betekenis zijn op het niveau van het stelsel en dus voor elke deelnemer.

Deelnemers en beheerorganisatie MOETEN om voor certificatie of TPM in aanmerking te komen individueel een risicoanalyse uitvoeren en MOETEN daarbij onder meer de Stelselrisicoanalyse als input gebruiken.

Op basis van de individuele risicoanalyse (Plan-fase van het ISMS zie de bijlage) selecteren de deelnemers beheersmaatregelen uit de Appendix van de norm IEC/ISO 27001:2005 of formuleren deze maatregelen eventueel zelf. De geselecteerde maatregelen nemen zij op in de Verklaring van Toepasselijkheid (VvT). Iedere deelnemer beargumenteert individueel zijn keuze voor maatregelen of uitsluiting van maatregelen.

Op stelselniveau is in het kader van het programma eHerkenning onder verantwoordelijkheid van de (tijdelijke) Beheerorganisatie en vertegenwoordigers van deelnemers een risicoanalyse uitgevoerd op de gemeenschappelijke processen en objecten van het Netwerk voor eHerkenning. Mede op basis van deze risicoanalyse zijn ten behoeve van de informatiebeveiliging van eHerkenning als geheel de minimaal te nemen beheersmaatregelen geselecteerd uit de Appendix van de ISO 27001:2005 norm. De geselecteerde beheersmaatregelen zijn opgenomen in het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning.

De beheersmaatregelen uit dit Gemeenschappelijk normenkader informatiebeveiliging eHerkenning MOETEN door deelnemers (afhankelijk van hun rol(len) in het stelsel) in hun individuele VvT worden opgenomen.

Er zijn twee typen maatregelen:

1. Het eerste is een verplichte maatregel die NIET MAG ontbreken in de VvT. Voor dit type maatregel zijn er op stelselniveau reeds uitwerkingen vastgesteld zoals koppelvlakspecificaties, operationeel handboek en procedure- en procesbeschrijvingen.
2. Het tweede type is een maatregel die de deelnemer of beheerorganisatie vanuit zijn rol ZOU MOETEN nemen en waarvan met dus mag verwachten dat deze in de VvT is opgenomen. De deelnemer MAG echter de beheersmaatregel 'niet van toepassing' verklaren maar in dat geval MOET deze uitsluiting met argumenten zijn omkleed.

De gemeenschappelijke maatregelen MOETEN dus op de VvT van de deelnemers herkenbaar voorkomen (geselecteerd of beargumenteerd niet geselecteerd).

Het Gemeenschappelijke normenkader en Stelselrisicoanalyse worden tenminste jaarlijks geëvalueerd en zo nodig bijgesteld. Dit betekent ook dat:

1. een deelnemer bij toetreding tot het Netwerk voor eHerkenning contractueel de verplichting tot certificatie op zich neemt en dus de op dat moment geldende versie van het normenkader MOET gebruiken.
2. een redelijke termijn in acht genomen ZOU MOETEN worden om de bestaande deelnemers de gelegenheid te geven de bijstellingen uit het normenkader te implementeren. Deze termijn wordt gesteld op 3 maanden na vaststelling van de bijstelling tenzij het tactisch beheer overleg anders besluit.

Eisen ten aanzien van archivering en opvraging

Vanuit het oogpunt van een betrouwbare elektronische communicatie en vanuit het oogpunt van informatiebeveiliging en betrouwbaarheid van het netwerk voor eHerkenning, gelden de volgende eisen ten aanzien van archivering.

- Elke deelnemer MOET alle door haar ondertekende en alle door haar ontvangen ondertekende berichten minimaal 7 jaar archiveren. Na deze periode ZOUDEN ten minste de in deze berichten voorkomende persoonsgegevens vernietigd MOETEN worden.
- Authenticatiediensten MOETEN tevens een referentie naar het gebruikte middel opslaan, zodat de audit trail naar de uitvoerend natuurlijk persoon sluitend wordt.
- Machtigingenregisters MOETEN tevens een referentie naar de geregistreerde bevoegdheid waarop de verklaring van bevoegdheid berust opslaan, zodat de audit trail naar de vertegenwoordigde dienstafnemer sluitend wordt.
- Middelenuitgevers en Machtigingenregisters ZOUDEN tevens bewijsstukken die zijn gebruikt bij uitgifte/registratie van middelen of machtigingen 7 jaar MOETEN archiveren zodat de audittrail naar handelend natuurlijk persoon of machtigingenbeheerder sluitend wordt.
- Een deelnemer MAG NIET persoonsgegevens afkomstig van berichten of bewijsstukken langer bewaren dan noodzakelijk voor het doel waarvoor ze worden verwerkt (conform Wet Bescherming Persoonsgegevens).
- Elke deelnemer MOET gearchiveerde gegevens beveiligd opslaan zodat zij niet toegankelijk zijn voor onbevoegden.
- Elke deelnemer MOET een verzoek waarbij gearchiveerde gegevens worden opgevraagd honoreren in de volgende gevallen:
  - Wanneer er beroep is ingesteld tegen een bestuursrechtelijk besluit dat de dienstverlener heeft genomen op basis van gegevens die zijn verkregen middels een eHerkenningsdienst en de dienstverlener deze bewijsstukken nodig heeft in het kader van de beroepsprocedure moeten de gegevens worden verstrekt aan zowel betreffende dienstverlener als dienstafnemer of de uitvoerend natuurlijk persoon die het beroep heeft ingesteld.
  - Op vordering van een bevoegde opsporingsinstantie, een inlichtingen- of veiligheidsdienst of een bevoegde toezichthouder moeten de gegevens aan betreffende instantie worden verstrekt.
  - Op verzoek van de beheerorganisatie. Bijv. omdat elders in de keten informatie verloren is gegaan en met als doel dat het informatiegat wordt hersteld.
- Een partij ZOU een verzoek voor het vrijgeven van gearchiveerde informatie in beginsel MOETEN indienen bij de betreffende deelnemer. Een dienstverlener ZOU een dergelijk verzoek in beginsel MOETEN indienen bij haar eHerkenningsmakelaar. In geval van geschillen, of bij onvoldoende medewerking MAG een partij een verzoek indienen bij de beheerorganisatie, die vervolgens de coördinatie op zich MOET nemen.

Logging

- Elke deelnemer MOET het volledige HTTP bericht van binnenkomende communicatie als gevolg van eHerkenning loggen. Elke deelnemer MOET alle uitgaande SAML en XACML berichten loggen.
- Elke deelnemer MOET logging beveiligd opslaan en MOET deze alleen toegankelijk maken voor bevoegde personen. Een deelnemer MAG logging NIET verwijderen binnen de verplichte bewaartermijn.
- Elke deelnemer MOET logging kunnen inzetten ten behoeve van foutopsporing.

Uitzondering op de loggingvereisten vormen cookieservers. Deze MOGEN NIET logging toepassen om gebruikers te volgen.

Op basis van logging MOET de deelnemer in staat zijn om vragen te beantwoorden. Er is een onderscheid in eerstelijns en tweedelijns vragen.

Eerstelijns vragen

Elke deelnemer MOET met behulp van logging over elke periode vragen over transacties kunnen beantwoorden waarin één van de volgende criteria, of een combinatie ervan, zijn opgenomen:

1. OIN per rol deelnemer
2. OIN dienstafnemer
3. OIN intermediaire partij (indien van toepassing)
4. OIN van dienstverlener
5. Dienst uit dienstencatalogus
6. Intern pseudoniem van een uitvoerend natuurlijk persoon
7. Extern pseudoniem van een uitvoerend natuurlijk persoon
8. Betrouwbaarheidsniveau

Daarnaast MOET de deelnemer op basis van logging inzicht kunnen geven in het totaal aantal geslaagde transacties en het totaal aantal foutieve transacties in een periode.

Tweedelijns vragen

Elke deelnemer MOET op verzoek van een daarvoor bevoegde instantie een (gearchiveerd) ondertekend verzonden of ontvangen bericht aan de instantie beschikbaar stellen. Tevens MOET een deelnemer op verzoek van een daarvoor bevoegde instantie de persoonsgegevens (van een houder van een authenticatiemiddel of betrokkene bij een machtiging) beschikbaar stellen aan de instantie.

Eisen aan de classificatie van informatie

Deze paragraaf beschrijft de nadere specificatie van de norm A.7.2 Classificatie van informatie (A7.1.1 en A.7.2.2) in de ISO 27001:2005. Doelstelling van de norm is: bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

Reikwijdte

Deze uitwerking van de norm heeft betrekking op gegevens die binnen eHerkenning (deelnemers en beheerorganisatie inclusief 'bestuurlijke opdrachtgever') worden gegenereerd, uitgewisseld en opgeslagen. De uitwerking van de norm is niet bedoeld als classificatie van systemen of netwerkcomponenten. Een normering van de classificatie van eHerkenning-systemen heeft geen toegevoegde waarde vanwege het ontbreken van generieke typering van systeemcomponenten van eHerkenning. De individuele deelnemers zijn vrij in de wijze waarop zij hun infrastructurele omgevingen concreet inrichten en moeten in staat blijven hun eigen classificatiemethodiek te volgen.

Classificatie en maatregelen

De classificatie is niet gekoppeld aan een generieke set maatregelen. De te classificeren informatie betreft uiteenlopende typen gegevens op uiteenlopende gegevensdragers. De concretisering van maatregelen MOET door de individuele deelnemers en beheerorganisatie worden gedefinieerd op basis van de Stelselrisicoanalyse en de eigen risicoanalyses. De voorbeelden van geclassificeerde gegevens dienen als input voor individuele risicoanalyses.

De classificatie

In tabel 1 is de classificatie van informatie binnen eHerkenning beschreven. De tabel legt met voorbeelden uit hoe de classificatie moet worden begrepen. Tabel 2 geeft een lijst van voorbeelden die als referentie dienen voor de classificatie van de overige en nieuwe eHerkenningsinformatie.

Tabel 1: Classificatie van informatie binnen eHerkenning

Classificatie	eHerkenning Intern	eHerkenning Gevoelig	eHerkenning Publiek/Openbaar
Uitleg	• Informatie die door alle direct betrokkenen bij eHerkenning wordt uitgewisseld. • De informatie is niet bedoeld voor anderen maar als onverhoopt deze informatie met derden wordt gedeeld treedt er geen substantiële financiële schade of imago schade op.	• Informatie die extra bescherming nodig heeft. • Openbaring aan niet bevoegden brengt substantiële schade toe aan het Netwerk voor eHerkenning; financieel, imago gerelateerd of anderszins.	• Alle informatie over eHerkenning bedoeld voor (potentiële) klanten of breder publiek.
Voorbeeld	• Agenda's en vergaderverslagen • Mails (tenzij expliciet is aangegeven dat deze vertrouwelijk zijn) • Dienstencatalogus • Meta Data	• Contractgegevens • Testgegevens • Klantenregistratie • MU en MR • Logbestanden	• De Stelsel documentatie • Informatie over de aanbieders van eHerkenningsdiensten op de website van eHerkenning • Factsheets etc.
Referentie	• Vertrouwelijkheid is laag • WBP/AV 23 Maatregelniveau: • Baseline • WBP Risicoklasse 1	• Vertrouwelijkheid is Midden/Hoog • WBP/AV 23 Maatregelniveau: • Baseline + Specifiek • WBP Risicoklasse 2	• Vertrouwelijkheid is n.v.t. • NB: er worden wel eisen gesteld aan de juistheid en beschikbaarheid van deze informatie

Tabel 2: Referentietabel met voorbeelden van geclassificeerde gegevens binnen eHerkenning

	Referentietabel met gegevens binnen eHerkenning (niet uitputtend)	Classificatie

1	Logbestanden van berichten-/transactieverkeer	Gevoelig WBP Risicoklasse 2
2	Contractgegevens	Gevoelig
3	Registraties MU en MR	Gevoelig WBP Risicoklasse 2
4	Metadata	Intern*)
5	Dienstencatalogus	Intern[1]
6	Testgegevens	Gevoelig
7	Auditrapporten	Gevoelig
8	Informatie betreffende de toetreding van deelnemers exclusief het advies aan het 'tactisch beheer overleg'.	Gevoelig
9	Berichten (verkeer)	Gevoelig
10	SLA rapportages van individuele deelnemers	Gevoelig
11	Generieke managementrapportages	Intern
12	Vergaderverslagen tactisch beheer overleg, gebruikersraad etc.	Intern
13	Beveiligingsincidenten-registratie	Gevoelig
14	Generieke beveiligingsrapportage (trends)	Intern
15	Het afsprakenstelsel voor eHerkenning	Publiek
16	Informatie op de website eHerkenning	Publiek
17	RFC's	Intern/Gevoelig[2]
18	Rapporten van security-audits of penetratietesten	Gevoelig

Voetnoten

1. Betreft slechts het aspect vertrouwelijkheid. Er zal wel sprake zijn van extra maatregelen i.v.m. eisen aan de integriteit van de gegevens.
2. Per RFC dient de mate van gevoeligheid te worden vastgesteld en de consequenties voor de behandeling van de RFC in de wijzigingsprocedure.

Eisen aan screening van medewerkers

Deze paragraaf bevat de nadere specificatie van de norm A.8.1.2 Screening in de ISO 27001:2005. Deze norm is opgenomen in het Gemeenschappelijk normenkader informatiebeveiliging eHerkenning en MOET worden nagevolgd door deelnemers en beheerorganisatie.

Doel en reikwijdte van screening

Doel van de screening is om te voorkomen dat door de beheerorganisatie of deelnemers medewerkers worden aangenomen die door hun gedrag de integriteit en betrouwbaarheid van eHerkenning in gevaar brengen.

Het kan gaan om (potentiële of reeds in dienst zijnde) medewerkers die met voorbedachte rade dan wel onder druk van andere personen de integriteit en betrouwbaarheid van de organisatie moedwillig zouden willen schenden, of medewerkers die door een gebrek aan kennis en inzicht de integriteit en betrouwbaarheid zullen schenden.

Bij integriteit en betrouwbaarheid gaat het zowel om het handelen in overeenstemming met algemeen aanvaarde maatschappelijke normen en waarden, (wettelijke) richtlijnen en procedures als het nakomen van afspraken en toezeggingen aan klanten, medewerkers, leveranciers en andere belanghebbenden.

De maatregel heeft betrekking op al het vaste en tijdelijke personeel dat werkzaamheden uitvoert binnen de scope van eHerkenning.

Procedure

Inleiding

Deze paragraaf beschrijft op welke wijze deelnemers en de beheerorganisatie screening MOETEN toepassen. Het doel van de procedure is om binnen eHerkenning tot een gemeenschappelijk – minimaal – niveau van screening te komen.

Het staat deelnemers en de BO overigens vrij om, bijvoorbeeld naar aanleiding van de eigen risicoanalyse, een strenger screening-regime dan in deze procedure is beschreven toe te passen.

De wijze en diepgang van de screening MOET zijn gerelateerd aan de bevoegdheden en taakstelling van de betreffende medewerker. Zo mag worden verwacht dat de screening voor een systeembeheerder met speciale bevoegdheden ten aanzien van systeemprogrammatuur strenger zal zijn dan voor een ondersteunende stafmedewerker.

Basisniveau van screening

Het basisniveau van screening voor alle personeel, bestaat uit:

- het controleren van de juistheid van de identiteit (WID-document);
- controleren van de juistheid van gegevens in het curriculum vitae en met name van opleidingsgegevens;
- controleren van relevante referenties.

Vast personeel t.b.v. eHerkenning

- Medewerkers die met activiteiten voor eHerkenning zijn belast MOETEN een Verklaring Omtrent Gedrag (VOG) aanvragen c.q. overleggen in relatie tot de omgang van gegevens waarbij integriteit en vertrouwelijkheid van belang zijn. Het gaat hierbij in ieder geval om de paragrafen 11, 12 en 13.
- De (originele of digitale kopie) VOG MOET worden opgenomen in het personeelsdossier of digitale registratie.
- In het geval een zwaardere screening dan VOG aantoonbaar al reeds heeft plaatsgevonden en nog steeds geldig is, KAN de deelnemer of beheerorganisatie besluiten om de VOG achterwege te laten. Zwaarder dan een VOG zijn bijvoorbeeld: veiligheidsonderzoek door de AIVD (A, B of C onderzoek) of de MIVD, antecedentenonderzoek door een erkend onderzoeksbureau.

Ingehuurd personeel

Deze beheersmaatregel is ook van toepassing op van externe leveranciers ingehuurd personeel. De eisen die aan ingehuurd personeel worden gesteld worden MOETEN van hetzelfde niveau zijn als de eisen aan het vaste personeel.

In het contract met de leverancier MOET zijn opgenomen:

- welke verantwoordelijkheden deze heeft ten aanzien van het screeningproces en;
- de verplichting daarover om direct de opdrachtgever te informeren als de screening van een in te zetten of ingezette medewerker niet (volledig) heeft plaatsgevonden of tot een negatief resultaat heeft geleid.

Verantwoordelijkheden

De organisatie (deelnemer, beheerorganisatie) MOET een functionaris aanwijzen die verantwoordelijk is voor het laten uitvoeren van dit proces. In veel gevallen ligt deze verantwoordelijkheid bij een security officer of een risk manager.

- De werkgever MOET de (a.s.) medewerker verzoeken om een VOG aan te vragen.
- In de aanvraag MOET de werkgever aangeven wat de aard van het werk is dat de medewerker gaat uitvoeren (refereren aan paragraaf 11, 12 en 13).
- De werkgever heeft expliciet beleid geformuleerd dat er zorg voor MOET dragen dat gedurende het dienstverband van de medewerker de integriteit en betrouwbaarheid aantoonbaar geborgd is.

Frequentie

Het screeningsproces MOET worden doorlopen voor elk personeelslid (vast of ingehuurd):

- Bij indiensttreding.

- Ingeval van een bestaand dienstverband als de screening nog niet heeft plaatsgevonden.
- Bij verandering van functie of werkgebied van een medewerker als de nieuwe werkzaamheden meer omvatten of in hoge mate afwijken van de vroegere werkzaamheden.

Beleid en doel penetratietesten

Organisaties hebben diverse, zowel technische als organisatorische, maatregelen genomen om te voorkomen dat niet-geautoriseerden zich toegang kunnen verschaffen tot hun informatie en informatiesystemen.

Om te toetsen of het stelsel van maatregelen dat genomen is daadwerkelijk effectief en adequaat is, wordt bij de deelnemers van eHerkenning en bij de Beheerorganisatie periodiek, in beginsel twee maal per jaar, een zogenaamde penetratietest uitgevoerd. Deze test wordt uitgevoerd door een externe specialist.

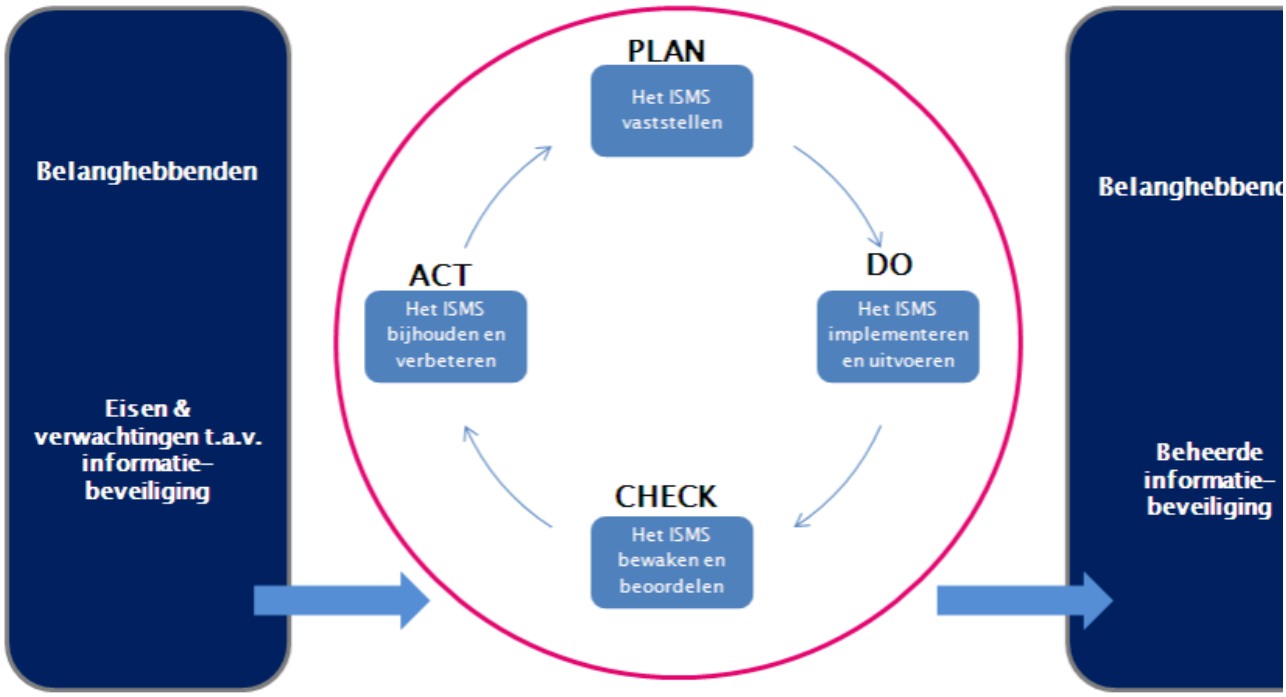
Een dergelijke controle kan nuttig zijn om zwakke plekken in het systeem te ontdekken en om te controleren hoe doeltreffend de beheersmaatregelen zijn bij het voorkómen van onbevoegde toegang als gevolg van deze zwakke plekken.

Penetratietesten geven een momentopname van een systeem in een bepaalde toestand op een bepaald tijdstip. De momentopname blijft beperkt tot die delen van het systeem die werkelijk zijn getest tijdens de penetratiepoging(en). De penetratietest vormt daarmee een aanvulling op de risicoanalyses en de audits.

Bijlage - Toelichting ISO 27001 certificatie

De organisatie die zijn IB (Informatiebeveiliging) wil inrichten en wil laten certificeren tegen de ISO/IEC 27001 norm moet een "gedocumenteerd Information Security Management System (ISMS) vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren binnen het kader van de bedrijfsactiviteiten en -risico's van de organisatie. Het proces dat in het kader van deze norm wordt gehanteerd, is gebaseerd op het PDCA-model zoals in de figuur hierna is weergegeven in de norm" (zie 4.1 Algemene eisen in het normdocument NEN-ISO/IEC 27001:2005).

Activiteiten in de PDCA cyclus van het ISMS



IB41 Toelichting op het ISMS en de PDCA-cyclus

In de hoofdstukken 4 t/m 8 van het ISO normdocument staat gedetailleerd en normatief beschreven wat een organisatie moet doen om een werkend ISMS te implementeren. Op deze plaat volstaan met een beknopte samenvatting op van de PDCA-cyclus.

Het systematisch doorlopen van deze PDCA-cyclus "dwingt" de organisatie als het ware tot het verbeteren van de Informatiebeveiliging. De uitgevoerde risicoanalyses en de in de VvT opgenomen beheersmaatregelen vormen de basis voor een ISMS van goede kwaliteit.

Activiteiten in de Plan-fase:

- Beschrijf de scope van het ISMS in termen van processen, systemen en organisatie.
- Voer een risico-analyse uit op deze scope en bepaal of en hoe de bepaalde risico's worden behandeld.
- Selecteer waar de van toepassing zijn de maatregelen uit de Appendix van de norm of beschrijf eigen specifieke maatregelen.
- Stel een Verklaring van Toepasselijkheid op.
- Verkrijg goedkeuring van het verantwoordelijk management en stel het ISMS vast.

Activiteiten in de Do-fase:

- Implementeer het plan voor risico-behandeling ofwel voer de geselecteerde maatregelen in, zorg dat deze gaan werken en beheerd worden.
- Richt de bijbehorende organisatie in, definieer rollen en verantwoordelijkheden.

Activiteiten in de Check-fase

- Controleer en beoordeel de werking van het ISMS.
- Beoordeel hierbij vooral of de gedachte risico's ook daadwerkelijk beheerst worden.
- Laat interne audits, reviews en controles uitvoeren.
- Beheer documentatie en registraties.

Activiteiten in de Act-fase

- Identificeer mogelijke verbeteringen en maak het mogelijk dat er corrigerende of preventieve maatregelen genomen worden die bewerkstelligen dat de beheersdoelstellingen worden bereikt.

Normenkader Stelselaudit

20141021Normenkader Stelselaudit eHerkenning 1.3.pdf

Stelsel risicoanalyse

Colofon			Document	
Versie afsprakenstelsel	1.8c		Auteur	Beheerorganisatie eHerkenning
Datum vaststelling	29-10-2014		Organisatie	Logius
Datum publicatie	30-10-2014		Classificatie	Openbaar

Achtergrond

Voor het eerst is begin 2010 door een werkgroep van deelnemers een meer techniek georiënteerde risicoanalyse op het Netwerk voor eHerkenning uitgevoerd. De risicoanalyse uit 2010 is in maart en april 2011 in een werkgroep van deelnemers en stelselexperts herijkt. Het resultaat van de herijking is dat er stelselrisico's zijn weggenomen door nadere specificaties van het stelsel, risico's door praktijkervaring na de implementaties minder relevant blijken en een aantal risico's zijn toegevoegd.

Doel en uitgangspunten voor de risicoanalyse

- De stelselrisicoanalyse is als basis gebruikt voor het opstellen van het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning ten behoeve van de stelselverantwoording en de ISO 27001 certificering van deelnemers.
- De deelnemers worden geacht deze risicoanalyse ook te gebruiken als input voor hun eigen risicoanalyses in het kader van de verplichte ISO 27001 certificering.
- De beheerorganisatie wordt geacht de stelselrisicoanalyse te gebruiken als input voor de risicoanalyses op haar beheerprocessen, dit in het kader van de stelselverantwoording.
- De risicoanalyse wordt tenminste jaarlijks herijkt.

Opbouw van de analyse

In de initiële risicoanalyse van 2010 is alleen de impact opgenomen van optreden van een dreiging en de inschatting van de kans weggelaten omdat er op dat moment nog nauwelijks praktijkervaring met het netwerk was. In de afgelopen jaren is er echter voldoende ervaring en kennis opgebouwd om daar een eerste inschatting van te doen. De hoogte van het (rest)risico is veelal sterk afhankelijk van de kwaliteit van genomen maatregelen door deelnemers en beheerorganisatie. Er is van uitgegaan dat de hoogte van het risico afhankelijk is van:

- Het ontbreken van specificaties of afspraken op stelselniveau;
- Het niet nemen van maatregelen door een enkele individuele deelnemer waardoor ernstige netwerkbrede effecten kunnen ontstaan.

De mate van impact van het optreden van een dreiging is als volgt ingeschaald:

- Hoog = Gevolgen zijn zeer bedreigend voor het functioneren van het stelsel eHerkenning en/of zijn gebruikers.
- Midden = Gevolgen zijn zeer negatief voor het functioneren van het Netwerk voor eHerkenning en/of enkele individuele gebruikers.
- Laag = Gevolgen zijn negatief voor het functioneren van het Netwerk voor eHerkenning.

De hoogte van de kans wordt als volgt verdeeld:

- Hoog = komt tenminste eenmaal per maand of vaker voor binnen het stelsel eHerkenning.
- Midden = komt enkele malen per jaar tot maximaal eenmaal per maand voor binnen het stelsel.
- Laag = komt een tot enkele keren per jaar voor binnen het stelsel.

Risicomatrix

In de onderstaande tabel is de referentie opgenomen voor de beoordeling van hoogte van het risico.

Kans / Impact	Hoog	Midden	Laag
Hoog	H	H	M
Midden	H	M	L
Laag	M	L	L

De mate van risico is opgebouwd uit de impact door het optreden van een dreiging en de kans dat deze dreiging zich manifesteert.

Leeswijzer

- Algemene risico's
- Risico's van de Beheerorganisatie
- Risico's van de Herkenningsmakelaar
- Risico's voor de Authenticatiedienst
- Risico's voor het Machtigingenregister
- Risico's in de relatie DV-HM
- Risico's in de relatie HM-AD
- Risico's in de relatie HM-MR

Algemene risico's

Nr	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Netwerkrollen worden verstoord door een Denial-of-Service attack Toelichting: het manifest worden van deze dreiging leidt tot het niet functioneren van een deel van het netwerk voor eHerkenning. De impact op het stelsel hangt af van het aantal partijen dat er per rol beschikbaar is. Oorzaken kunnen zijn: 1. extern: een aanval op een frontend-applicatie 2. intern: een fout in de configuratie bij een deelnemer waardoor een niet beheerste berichtenstroom wordt gegenereerd.	M	a. H b. L	H L	Ad a. Periodieke penetratietest. Afgesproken is dat tweemaal per jaar een penetratietest zal worden uitgevoerd door een externe partij op de eHerkenning systemen van de deelnemers en van de BO. Ad a. Inrichten van monitoring op pogingen van onbevoegden om binnen te dringen op de systemen (security incident en event monitoring en intrusion detection). Ad b: Testen door de BO bij entree van een kandidaat-deelnemer in het Netwerk of bij nieuwe implementaties. Inrichten van configuratiemanagement door de deelnemers.
2.	Verlies van berichten Toelichting: het manifest worden van deze dreiging leidt tot het niet correct afhandelen van één of meerdere individuele herkenningsvragen. De impact is daarmee gering.	L	L	L	Is gemitigeerd in de ontwerpspecificaties van het Netwerk. Een verloren bericht wordt opnieuw aangeboden.
3.	Afgifte van onvolledige antwoorden Toelichting: het manifest worden van deze dreiging leidt tot het niet correct afhandelen van één of meerdere individuele herkenningsvragen. De impact is daarmee gering.	L	L	L	Is gemitigeerd in de ontwerpspecificaties van het Netwerk. Onvolledige berichten worden niet geaccepteerd.

4.	Logging/tracing-gegevens zijn onvoldoende bruikbaar voor het nagaan van een volledige herkenningsvraag Toelichting: in geval van een geschil of problem-solving zal mogelijk gebruik gemaakt moeten worden van logging/tracing-gegevens van een volledige herkenningsvraag. Indien een deel van de keten niet beschikbaar is of inhoudelijk onvoldoende betrouwbaar is, kan dit leiden tot een beperkte tot zeer ernstige complicatie van een geschilafhandeling of een veel langer problem-solving proces.	M	L	L	In het (technisch) ontwerp van het stelsel is deze dreiging gemitigeerd. Maatregelen: • Beheer en beveiliging van de integriteit van logging en tracing gegevens. • Test van de implementaties bij toetreding. Deelnemers zijn zelf verantwoordelijk voor het beheer van de logging/tracing van (transactie)gegevens die binnen hun eigen domein worden vastgelegd.
5.	Verkeerde vertaling van de berichten Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegevens dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. De gevolgen zijn niet beperkt tot één deelnemer. waardoor dit tot een hoge imagoschade voor het gehele netwerk kan resulteren.	H	L	M	Maatregel: • Uitvoeren van testen bij de entree van een kandidaat- deelnemer in het Netwerk of bij nieuwe implementaties. • Inrichten van configuratiemanagement door de deelnemers.
6.	Besmetting van het netwerk door gebruikers Toelichting: een dienstverlener of dienstafnemer kan onvoldoende beveiligingsmaatregelen hebben getroffen om te voorkomen dat een besmetting met virussen, wormen etc. wordt overgedragen aan het netwerk. In theorie zou dit tot gevolg kunnen hebben dat het netwerk niet meer of niet meer volledig functioneert. Tevens kan hierdoor een imagoprobleem ontstaan.	H	M	H	In de aansluitvoorwaarden wordt van gebruikers verwacht (niet afgedwongen) dat zij hun informatiebeveiliging in voldoende mate op orde hebben. Deelnemers zijn zelf verantwoordelijk voor hun eigen informatiebeveiliging en hebben anti-virus software geïnstalleerd. Er zijn afspraken omtrent incidentmanagement, waardoor relevante partijen adequaat geïnformeerd worden over een mogelijke besmetting met malware.

7.	Repeterende incidenten of beschikbaarheidproblemen bij een of meerdere partijen of rollen Toelichting: Het vertrouwen van gebruikers in het gehele netwerk voor eHerkenning komt in het geding als een en meerdere deelnemers frequent beveiligings- of beschikbaarheidproblemen hebben. Doorgaans wordt een ervaring van niet beschikbaarheid binnen een half jaar 'vergeten'; herhaling binnen die periode leidt doorgaans tot verlies aan vertrouwen.	M	M	M	Er zijn (status medium 2012) voldoende redundant ingevulde rollen om de continuïteit van het Netwerk te borgen. Er zijn echter (nog) geen afspraken gemaakt over het (tijdelijk) overnemen van activiteiten indien een rol bij een deelnemer, bijvoorbeeld een HM, niet meer beschikbaar is. In het kader van ISO certificering en bedrijfscontinuiteit gaan deelnemers na in hoeverre maatregelen genomen moeten worden om continuiteit te borgen. Er is een incidentmanagement procedure afgesproken waardoor monitoring van incidenten in het stelsel plaatsvindt.
8.	Niet of niet tijdig melden van beveiligingsincidenten of kwetsbaarheden en oplossingen door deelnemers en beheerorganisatie. Toelichting: Indien deelnemers en beheerorganisatie niet tijdig incidenten melden wordt een mogelijk door de beheerorganisatie te coördineren actie steeds omvangrijker. Wanneer niet op basis van onderling vertrouwen binnen het netwerk incidenten en oplossingen worden gedeeld is dit negatief voor de performance op netwerkniveau.	H	H	H	Er is een incidentmanagement procedure afgesproken. Hierbinnen is ruimte om bepaalde gevoelige incidenten discreet te behandelen. Incidenten en incidentmanagement worden periodiek besproken in het security officers overleg. Informatie over kwetsbaarheden vanuit het NCSC wordt door de beheerorganisatie doorgegeven aan deelnemers.

9.	Niet of niet tijdig melden van beveiligingsincidenten door dienstverleners of dienstafnemers Toelichting: Diensverleners en dienstafnemers kunnen het netwerk onbedoeld besmetten met malware. Het niet tijdig melden van besmettingen leidt tot een verhoogde kans dat de besmetting door het netwerk heen verspreidt .	H	L	M	De systemen in het Netwerk zijn gescheiden van de systemen van de dienstverleners en dienstafnemers. Alleen berichten die voldoen aan de specificaties worden geaccepteerd. Het Netwerk is niet aansprakelijk indien de besmetting door systemen van dienstverleners en dienstafnemers het gebruik van eHerkenning onmogelijk maken. Op stelselniveau worden geen gegevens bijgehouden omtrent incidenten in relatie tot eHerkenning bij dienstafnemers of dienstverleners. Meer in de "awareness"-zin wordt er in de gebruikersvoorwaarden c.q. aansluitvoorwaarden aandacht gevraagd voor informatiebeveiliging. Voor gemeenten, als gebruiker van DigiD, is de verplichting vanuit het Rijk opgelegd om periodiek een audit op de informatiebeveiliging te laten uitvoeren.
10.	Een middel of machtiging wordt op een te hoog betrouwbaarheidsniveau geclassificeerd. Toelichting: te hoog geclassificeerde middelen of machtigingen kunnen leiden tot misbruik van diensten van dienstverleners of ongeldigheid van informatietransacties tussen dienstverleners en dienstafnemers. Op die manier zouden diensten afgenomen kunnen worden waarvoor de dienstafnemer zich onvoldoende geauthenticeerd heeft.	H	L	M	Het afsprakenstelsel bevat afspraken en procedures voor het classificeren van middelen en machtigingen.
11.	Webapplicaties van beheerorganisatie en deelnemers zijn kwetsbaar. Toelichting: Bij de bouw van webapplicaties is het vanzelfsprekend dat de bouwer zonder expliciete opdracht de applicatie standaard test op kwetsbaarheden. Niet testen kan leiden tot kwetsbaarheden die kunnen worden misbruikt. Misbruik ondermijnt het vertrouwen in het Netwerk voor eHerkenning.	H	M	H	Applicaties van deelnemers worden verplicht voor opname in het Netwerk getest. Periodiek worden door de beheerorganisatie penetratietesten in het Netwerk georganiseerd. Afgesproken is om tweemaal per jaar penetratietesten uit te laten voeren bij deelnemers en BO. Wellicht ten overvloede: uitgesloten hiervan zijn de 'browser-lekken' die bij gebruikers (dienstverleners en dienstafnemers) kunnen voorkomen.

Risico's van de Beheerorganisatie

De BO heeft een eigen risicoanalyse uitgevoerd op de processen en onderdelen (assets) waar zij direct verantwoordelijk voor is. Voor enkele specifieke assets werken de processen uitsluitend indien zowel deelnemers als de BO hun deel op orde hebben. In deze risicoanalyse worden de dreigingen en risico's geanalyseerd en maatregelen geformuleerd ten aanzien van:

- metadata
- dienstencatalogi
- testfaciliteiten
- incidentmanagement
- documentatie met betrekking tot het Afsprakenstelsel

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	De meta-data is onjuist, onvolledig of niet aktueel. Toelichting: Onjuiste of niet tijdige wijzigingen kunnen leiden tot het schaden van de werking van eHerkenning of evt. het toelaten van een ongewenste berichten tot het netwerk.	H	M	H	De (gezamenlijke) procedure voor het komen tot een aktueel en integer metadatabestand is beschreven in het Operationeel Handboek. De BO heeft tevens een werkbeschrijving gemaakt om te komen tot een geaggregeerd metadatabestand.
2.	De trusted party list van deelnemers op het netwerk van eHerkenning die opgenomen is in het metadatabestand, is onjuist, onvolledig of niet aktueel. Toelichting: Onjuiste of niet tijdige wijzigingen kunnen leiden tot het schaden van de werking van eHerkenning of het toelaten van een ongewenste partij tot het netwerk.	H	M	H	Door het opnemen van de certificaatnummers van de toegestane partijen (deelnemers) (ook wel genoemd "whitelist") is het in principe uitgesloten dat onbevoegde partijen zich op het eHerkenningsnetwerk begeven. In de werkbeschrijving bij de BO is aangegeven op welke wijze de controles hierop moeten plaatsvinden.
3.	Proces voor melding en afhandeling van beveiligingsincidenten werkt niet adequaat. Toelichting: Afhankelijk van het type incident kan het niet goed werken van het incidentmanagement proces het netwerk operationeel schaden.	M	M	M	Het incidentmanagement proces is beschreven en afgesproken. Dit omvat de afspraak over de verplichting tot het melden van beveiligingsincidenten door deelnemers. Het incidentmanagement proces is beschreven in het Operationeel Handboek. Periodiek wordt hierover gerapporteerd aan het Bestuur nadat de geaggregeerde rapportage is besproken in het security officers overleg.
4.	De door DV's aangeleverde gegevens omtrent dienstencatalogi wordt foutief verwerkt. Toelichting: Foutief verwerken kan bewust en onbewust. Bij foutieve gegevens bestaat het risico dat niet geautoriseerde personen toegang krijgen tot door DV aangeboden diensten of dat geautoriseerde personen geen diensten kunnen afnemen. Nieuwe versie van dienstencatalogus wordt te laat gepubliceerd. Hierdoor bestaat het risico dat door DV aangeboden dienst(en) niet via eHerkenning kunnen worden geleverd.	M	M	M	Bij de BO is een procedure opgesteld om fouten in de Dienstencatalogus te minimaliseren. Basis wordt gevormd door de deelnemers die de gegevens van dienstverleners krijgen aangereikt. Daar zal de eerste controle moeten plaatsvinden. Beschikbare procedure moet strikt gevolgd worden, in dit geval vooral met betrekking tot de afgesproken tijdlijn.

5.	De beheerorganisatie beschikt over onvoldoende kennis en ervaring met betrekking tot informatiebeveiliging en risicomanagement. Toelichting: Onvoldoende kennis en ervaring kan leiden tot inschattingsfouten bij incidentbehandeling of onvoldoende kwaliteit van de beveiligingstesten. In beide gevallen kan het imago van eHerkenning geschaad worden.	M	M	M	De beheerorganisatie beschikt overexpertise met betrekking tot informatiebeveiliging Door capaciteitsmanagement en gedocumenteerde bedieningsprocessen is kennis beschikbaar en overdraagbaar. Er zijn rollen gedefinieerd en ingevuld voor autorisatie manager, securitymanager, riskmanager, incidentmanager en changemanager.
6.	Testgereedschap wordt misbruikt. Toelichting: Het testgereedschap is publiek beschikbaar. Beschikbaar wordt gesteld: - de simulatortool	M	L	L	Deze testtools zijn in feite publiek beschikbaar op de extranet website. De BO beheert de software. De testtools zelf worden, na een change, getest door de BO.
7.	Testomgeving is onvoldoende gedocumenteerd. Toelichting: Zonder documentatie zijn testwerkzaamheden onvoldoende overdraagbaar en kan een gebrek aan kennis van testgereedschap en omgeving leiden tot verstoringen in het Netwerk.	H	M	H	De BO heeft een bedieningsprocedure gemaakt voor het beheren van de .
8.	Documentatie van het Netwerk voor eHerkenning is niet integer of volledig. Toelichting: Te weinig zekerheid over de juistheid en volledigheid van de gedocumenteerde afspraken in het stelsel voor eHerkenning kan leiden tot verstoringen (issues over technisch aspecten) of juridische discussie over o.a. aansprakelijkheden	H	M	H	Er is een changemanagement procedure ingericht die moet borgen dat de documentatie van het Afsprakenstelsel juist en volledig beschikbaar wordt gesteld aan de deelnemers. Alle changes worden, binnen deze procedure, besproken met (vertegenwoordigers van) deelnemers.
9.	Documentatie van het Netwerk voor eHerkenning is niet toegankelijk. Toelichting: Langdurige onbeschikbaarheid van het archief is belemmerend voor de processen van de beheerorganisatie en kan bijvoorbeeld leiden tot vertragingen bij kandiaten voor toetreding.	M	M	M	De documenten uit het Afsprakenstelsel zijn in principe "openbaar". Ten behoeve van de deelnemers heeft de BO de geldende documentatie online beschikbaar gesteld aan hiertoe geautoriseerde (vertegenwoordigers van) deelnemers. De documentatie in het AS is eveneens opgenomen op de website www.eherkenning.nl .
10.	Fouten bij DNS beheer cookieserver Toelichting: De gemeenschappelijke cookieserver is nodig voor de SSO functionaliteit bij de Herkenningsmakelaar.	L	M	L	Het proces voor het beheer van de cookieserver is beschreven in Proces onderhoud cookieserver. Oplossingen testen en periodiek monitoren. Risico ligt ook bij de deelnemers.

Risico's van de Herkenningsmakelaar

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen

1.	Er wordt een verkeerde combinatie van authenticatie en machtiging op een vraag van de dienstverlener samengesteld. Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren. Het verspreidingsgebied van de fout zal echter beperkt zijn.	H	L	M	De kans dat een verkeerde combinatie zich voordoet wordt als Laag geclassificeerd. De oorzaak kan liggen in het onjuist invoeren van gegevens in de authenticatie of machtigingstabellen. Maatregel ligt in de sfeer van inputvalidatie. Iedere deelnemer is verantwoordelijk voor het juist registreren van gegevens.
2.	Ten onrechte niet doorgeven van berichten. Toelichting: in dit geval is er sprake van een denial of service voor één of meerdere dienstafnemers. De oorzaak kan liggen in een al of niet bewust veroorzaakte technische fout in de dienstverlening. Gevolg kan zijn dat een deel van de dienstverlening niet beschikbaar is.	H	M	H	Diverse maatregelen: zoals inputvalidatie bij het opnemen van machtigings- en authenticatiegegevens alsmede het testen van het netwerkverkeer.
3.	Bewust zelfstandig genereren van berichten als antwoord op een vraag van de dienstverlener zonder dat de achterliggende authenticatie en machtiging zijn aangevraagd. Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren.	M	L	L	De technische specificaties van het berichtenverkeer maakt het optreden van de deze dreiging onwaarschijnlijk. De kans op een onbewust genereren van een bericht bijvoorbeeld als gevolg van een foutieve beheerhandeling is groter maar de impact zal dan in de meeste gevallen klein zijn.
4.	Teruggeven van een te hoog betrouwbaarheidsniveau. Toelichting: betrouwbaarheidsniveaus zijn in hoge mate bepalend voor het gestelde vertrouwen in het netwerk. Fouten in het gebruik van betrouwbaarheidsniveaus, al of niet opzettelijk, zijn direct gerelateerd aan de kern van de dienstverlening in het afsprakenstelsel. Dit kan grote imagoschade opleveren voor het gehele netwerk en de deelnemers.	H	M	H	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging. Maatregelen worden gevonden in configuratiemanagement, inputvalidatie en testen.

5.	Foutief gegenereerde berichten. Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegevens dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. De gevolgen zullen primair een klein verspreidingsgebied kennen, echter deze dreiging raakt wel de kern van de dienstverlening van het gehele netwerk en de deelnemers.	H	M	H	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging. Maatregelen worden gevonden in configuratiemanagement en testen.
6.	verwijderd igv RFC192				
7.	Deelnemer wordt ten onrechte vertrouwd. Toelichting: deze dreiging is van toepassing op het moment dat een deelnemer op niet-legitieme wijze toegang verkrijgt tot het netwerk of op legitieme wijze ten onrechte tot het netwerk wordt toegelaten. Het vertrouwen in het afsprakenstelsel is gebaseerd op het niet voorkomen van een dergelijke situatie. Deze dreiging betreft daarmee het fundament van het afsprakenstelsel.	H	M na:L	H na: M	Een fout in de tabellen is de oorzaak van het optreden van deze dreiging. Testbatterij is ingericht om o.a. bij toetreding fouten in de tabellen te reduceren. NB De kans dat deze dreiging optreedt is gedurende het toetredingsproces Hoog omdat dit een wijzigingsmoment is. In het afsprakenstelsel is een toetredingsproces beschreven. Onderdeel hiervan is een toetsing door een externe auditor. Na toetreding is de kans dat deze dreiging optreedt Laag en vooral afhankelijk van een juist tabellenbeheer (inputvalidatie).
8.	verwijderd igv RFC192				
9.	verwijderd igv RFC192				
10.	verwijderd igv RFC192				
11.	Ongeautoriseerd ophalen van machtigingen Toelichting: Het manifest worden van deze dreiging, door het opvragen van een machtigingsbewijs zonder voorafgaande authenticatie, geeft een onbevoegd persoon inzicht in een specifieke machtiging. Deze informatie zou als input gebruikt kunnen worden voor het opbouwen van een malafide handeling.	L	L	L	Dreiging zou op kunnen treden indien een deelnemer ten onrechte is vertrouwd (zie 7).
12.	verwijderd igv RFC192				

13.	Denial-of-Service attack op de Herkenningsmakelaar via een gecompromitteerde dienstverlener Toelichting: het manifest worden van deze dreiging leidt tot het niet functioneren van een deel of het geheel van het netwerk voor eHerkenning. De impact hangt af van het aantal partijen dat er voor de rol van herkenningsmakelaar beschikbaar is. De gevolgen zullen merkbaar zijn voor alle dienstverleners die bij de betreffende herkenningsmakelaar zijn aangesloten.	M	L	L	De dienstverlener heeft geen belang bij het offline brengen van de HM en verplicht zich volgens contract zijn netwerk afdoende te beschermen. De inschatting van de lage kans van optreden is ingegeven door het uitgangspunt dat de HM zijn verkeer afdoende monitort om tijdig actie te kunnen ondernemen.

Risico's voor de Authenticatiedienst

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Er wordt een verkeerde combinatie van authenticatie en machtiging op een vraag van de dienstverlener samengesteld. Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren. Het verspreidingsgebied van de fout zal echter beperkt zijn.	M	M	M	De oorzaak kan liggen in het onjuist invoeren van gegevens in de authenticatie of machtigingstabellen. Maatregel ligt in de sfeer van inputvalidatie.
2.	Ten onrechte niet doorgeven van berichten. Toelichting: in dit geval is er sprake van een denial of service voor één of meerdere dienstafnemers. De oorzaak kan liggen in een al of niet bewust veroorzaakte technische fout in de dienstverlening.	H	M	H	Diverse maatregelen: zoals inputvalidatie bij het opnemen van machtigings- en authenticatiegegevens alsmede het testen van het netwerkverkeer.
3.	Bewust zelfstandig genereren van berichten als antwoord op een vraag van de dienstverlener zonder dat de achterliggende authenticatie en machtiging zijn aangevraagd. Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren.	H	L	M	De technische specificaties van het berichtenverkeer maakt het optreden van de deze dreiging onwaarschijnlijk. De kans op een onbewust genereren van een bericht bijvoorbeeld als gevolg van een foutieve beheerhandeling is groter maar de impact zal dan in de meeste gevallen klein zijn. Waardoor dit risico maximaal op laag tot midden zal scoren.

4.	Teruggeven van een te hoog betrouwbaarheidsniveau. Toelichting: betrouwbaarheidsniveaus zijn in hoge mate bepalend voor het gestelde vertrouwen in het netwerk. Fouten in het gebruik van betrouwbaarheidsniveaus, al of niet opzettelijk, zijn direct gerelateerd aan de kern van de dienstverlening in het afsprakenstelsel. Dit kan grote imagoschade opleveren voor het gehele netwerk en de deelnemers.	H	L	M	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging.
5.	Foutief gegenereerde berichten. Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. De gevolgen zullen primair een klein verspreidingsgebied kennen, echter deze dreiging raakt wel de kern van de dienstverlening van het gehele netwerk en de deelnemers zal resulteren.	H	L	M	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging.
6.	verwijderd igv RFC192				
7.	Deelnemer wordt ten onrechte vertrouwd. Toelichting: deze dreiging is van toepassing op het moment dat een deelnemer op niet-legitieme wijze toegang verkrijgt tot het netwerk of op legitieme wijze ten onrechte tot het netwerk wordt toegelaten. Het vertrouwen in het afsprakenstelsel is gebaseerd op het niet voorkomen van een dergelijke situatie. Deze dreiging betreft daarmee het fundament van het afsprakenstelsel.	H	H na:L	H na:M	Een fout in de metadata is de oorzaak van het optreden van deze dreiging. Testbatterij is ingericht om o.a. bij toetreding fouten in de tabellen te reduceren. NB De kans dat deze dreiging optreedt is gedurende het toetredingsproces Hoog omdat dit een wijzigingsmoment is. In het afsprakenstelsel is een toetredingsproces beschreven. Onderdeel hiervan is een toetsing door een onafhankelijke auditor. Na toetreding is de kans dat deze dreiging optreedt Laag en vooral afhankelijk van een juist tabellenbeheer (inputvalidatie).

8.	Deelnemer wordt ten onrechte niet vertrouwd Toelichting: deze dreiging is van toepassing op het moment dat een beoogde deelnemer ten onrechte niet tot het netwerk wordt toegelaten of uitgesloten wordt. Dit levert irritatie op bij de deelnemer en mogelijk bij de klant van de deelnemer, maar geeft uiting aan een groot belang van het toetredingsproces. De impact geldt dus voor een enkele partij.	L	H na:L	M na:L	Idem
9.	verwijderd igv RFC192				
10.	verwijderd igv RFC192				
11.	Ongeautoriseerd ophalen van machtigingen Toelichting: Het manifest worden van deze dreiging, door het opvragen van een machtigingsbewijs zonder voorafgaande authenticatie, geeft een onbevoegd persoon inzicht in een specifieke machtiging. Deze informatie zou als input gebruikt kunnen worden voor het opbouwen van een malafide handeling.	L	L	L	Dreiging zou op kunnen treden indien een deelnemer ten onrechte is vertrouwd (zie 7).
12.	verwijderd igv RFC192				
13.	Denial-of-Service attack via een gecompromitteerde dienstverlener Toelichting: het manifest worden van deze dreiging leidt tot het niet functioneren van een deel of het geheel van het netwerk voor eHerkenning. De impact hangt af van het aantal partijen dat er voor de rol van AD beschikbaar is. De gevolgen zullen merkbaar zijn voor alle dienstverleners die bij de betreffende herkenningsmakelaar zijn aangesloten.	M	L	L	De dienstverlener heeft geen belang bij het offline brengen van de AD en verplicht zich volgens contract zijn netwerk afdoende te beschermen. De inschatting van de lage kans van optreden is ingegeven door het uitgangspunt dat de HM zijn verkeer afdoende monitort om tijdig actie te kunnen ondernemen.

Risico's voor het Machtigingenregister

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Onjuist invoeren van machtigingsgegevens Toelichting: bij optreden van deze dreiging wordt ten onrechte structureel de toegang tot een dienst van een dienstverlener toegewezen of geweigerd. Bij onjuiste toewijzing kan sprake zijn van significante impact, indien het een hoog betrouwbaarheidsniveau betreft. Daarnaast heeft het manifest worden van deze dreiging een negatief effect op het imago van het netwerk voor eHerkenning gezien de relevantie van machtigingen voor het netwerk. Het effect zal betrekking hebben op individuele gevallen.	M*)	L	L*)	*) impact en hoogte van het risico is afhankelijk van het van toepassing zijnde betrouwbaarheidsniveau. Maatregel: inputvalidatie

2.	Ten onrechte afgeven van berichten Toelichting: bij optreden van deze dreiging wordt ten onrechte eenmalig of structureel de toegang tot een dienst van een dienstverlener toegewezen. Er kan sprake zijn van significante impact, indien het een hoog betrouwbaarheidsniveau betreft. Daarnaast heeft het manifest worden van deze dreiging een negatief effect op het imago van het netwerk voor eHerkenning gezien de relevantie van machtigingen voor het netwerk. De impact blijft beperkt tot individuele gevallen.	H	M	H	Oorzaak kan liggen in foutieve gegevens in de machtigingentabel. Zie onder 1.
3.	Ten onrechte negatief beantwoorden van machtigingsvragen Toelichting: bij optreden van deze dreiging wordt ten onrechte structureel de toegang tot een dienst van een dienstverlener geweigerd. Dit zal leiden tot irritatie in individuele gevallen.	L	L	L	Oorzaak kan liggen in foutieve gegevens in de machtigingentabel. Zie nr. 1
4.	Onjuiste koppeling van machtigingsvraag en bericht Toelichting: bij optreden van deze dreiging wordt toegang tot een onbedoelde dienst van een mogelijk andere dienstverlener toegewezen. Het manifest worden van deze dreiging kan bij bekend worden een zeer negatief effect op het imago van het netwerk voor eHerkenning omdat dienstverleners er van op aan moeten kunnen dat alleen de juiste geauthenticeerden toegang tot de dienstverlening hebben. De impact blijft beperkt tot individuele gevallen.	M	M	M	Deze dreiging is een variant op dreiging 2. Oorzaak kan liggen in foutieve gegevens in de machtigingentabel. Zie nr. 1
5.	verwijderd igv RFC192				
6.	verwijderd igv RFC192				
7.	verwijderd igv RFC192				
8.	Foutief importeren/exporteren van machtigingen (bij overgang naar ander MR) Toelichting: het manifest worden van deze dreiging leidt tot een aantasting van het imago (betrouwbaarheid) van het betreffende (nieuwe) machtigingregister door machtigingsvragen die ten onrechte worden toegewezen of afgewezen. Dit geldt voor het gehele verzorgingsgebied van het machtigingregister. De impact kan afhankelijk zijn van het zekerheidsniveau. De uitstraling op het imago van het gehele netwerk is afhankelijk van de grootte van het verzorgingsgebied van het machtigingregister.	L	L	L	Dienstafnemers zijn zelf verantwoordelijk voor de controle van de juistheid van machtigingen.
9.	Ongeautoriseerde toegang tot MR (opzettelijk) Toelichting: deze dreiging betreft het ten onrechte toegang krijgen tot het MR waardoor de vastgelegde machtigingen gecorrumpeerd kunnen worden. Het manifest worden van deze dreiging leidt tot een aantasting van de betrouwbaarheid van het machtigingregister door machtigingsvragen die ten onrechte worden toegewezen (of evt. afgewezen). Dit geldt potentieel voor het gehele verzorgingsgebied van het machtigingregister. Daarnaast is de impact afhankelijk van het betrouwbaarheidsniveau. De uitstraling op het imago van het gehele netwerk is afhankelijk van de grootte van het verzorgingsgebied van het machtigingregister.	M	M	M	Indien er sprake is van online toegang door een dienstafnemer tot zijn machtigingen zal een dienstafnemer (juridisch) op zijn verantwoordelijkheid gewezen moeten worden op de noodzaak vertrouwelijk om te gaan met toegangsgegevens of middelen. Dit kan onderdeel zijn van het contract tussen dienstafnemer en deelnemer.

10.	Registratie bij een machtigingsregister is onvolledig of onjuist Toelichting: registratie van een nieuwe dienstafnemer bij een machtigingenregister, inclusief de houder van de hoogste machtiging. Fouten in dit proces kunnen leiden tot het ten onrechte verkrijgen van diensten bij dienstverleners.	M	M	M	Maatregel: inputvalidatie Registratie moet conform de procesbeschrijvingen en eisen gesteld aan de verschillende betrouwbaarheidsniveaus.
11.	verwijderd igv RFC192				
12.	verwijderd igv RFC192				

Risico's in de relatie DV-HM

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Commerciële competitie kan leiden tot stellen van lage informatiebeveiligingseisen aan dienstverleners. Toelichting: het stellen van lage informatiebeveiligingseisen aan dienstverleners vergroot de kans op aantasting van de betrouwbaarheid van het netwerk voor eHerkenning (zie de betreffende dreiging in de paragraaf over de herkenningsmakelaar). Vraag is of dit wel een dreiging is. De eisen aan het koppelvlak zijn uniform. De gebruikersvoorwaarden zijn ook uniform. Verder dan dat kun je in feite als deelnemer niet gaan.	M	L	L	Eisen aan het koppelvlak tussen HM en Dienstverlener zijn beschreven evenals de vrijheidsgraden daarin. Aansluitingen worden getest.
2.	verwijderd igv RFC192				
3.	De dienstverlener heeft onvoldoende beveiligingsmaatregelen getroffen: Toelichting: vergroot de kans op aantasting van de betrouwbaarheid van het netwerk voor eHerkenning (zie de betreffende dreiging in de paragraaf over de herkenningsmakelaar). De dienstverlener kan bijvoorbeeld een stroom aan berichten in het netwerk genereren.	M	L	L	Eisen aan het koppelvlak tussen HM en Dienstverlener is beschreven evenals de vrijheidsgraden daarin. Aansluitingen worden getest.
4.	HM is niet in staat technische fouten van de dienstverlener te herkennen en te mitigeren: Toelichting: vergroot de kans op aantasting van de betrouwbaarheid van het netwerk voor eHerkenning.	M	M	M	Impact hang sterk af van de aard van de dienst en de dienstverlener en het bijbehorende betrouwbaarheidsniveau.
5.	verwijderd igv RFC192				

Risico's in de relatie HM-AD

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	verwijderd igv RFC192				
2.	[LEEG]				Geen additionele dreigingen anders dan al genoemd onder SR10 Algemene Risico's.

Risico's in de relatie HM-MR

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	verwijderd igv RFC192				
2.	verwijderd igv RFC192				
3.	verwijderd igv RFC192				

Gemeenschappelijk normenkader informatiebeveiliging eHerkenning

Gedetailleerde uitwerking van de vereiste maatregelen voor informatiebeveiliging.

Gemeenschappelijk Normenkader Informatiebeveiliging eHerkenning versie 1.8a.pdf

Templates en formulieren

Onderstaande documenten kunnen worden opgeslagen als PDF of als Word document voor verdere verwerking. Klik hiervoor rechtsboven op Tools > Export to PDF of Tools > Export to Word.

- Checklist chain test
- Checklist simulator test
- Template deelnemersovereenkomst — De overeenkomst tussen deelnemers en beheerorganisatie op basis waarvan deelnemers gehouden zijn het afsprakenstelsel toe te passen. Deze deelnemersovereenkomst verwijst naar het afsprakenstelsel maar is er (strikt genomen) zelf geen onderdeel van.
- Template incidentrapport
- Template verzoek tot (uitbreiding) toetreding eHerkenning
- Template vrijwaring penetratietest
- Template wijziging rechtspersoon deelnemer
- Template zelfverklaring

Checklist chain test

Checklist chain test

Test date:	_____ / _____ / _____
Build version:	_____
Tester:	_____
Signature:	

eHerkenningsmakelaar

Test	Result Connectis | CreAim | Digidentity | KPN | QuoVadis | Zetsolutions	Comment
HMC01 Normal flow HMC02 Cancel normal flow HMC03 Cancel normal flow with replay HMC04 Check IDs HMC05 Single sign on HMC06 Chain authorization HMC07 B2C		

Authenticatiedienst

Test	Result Connectis | CreAim | Digidentity | Gemnet | iWelcome | KPN	Comment

ADC01 Normal flow ADC02 Cancel normal flow ADC03 Cancel and replay ADC04 Single sign on ADC05 B2C ADC06 Logout		

Machtigingenregister

Test	Result Connectis | CreAim | Digidentity | Gemnet | iWelcome | KPN	Comment
MRC01 Normal flow MRC02 Incorrect messages MRC03 Chain authorization		

Checklist simulator test

Simulator test cases

Test date:	_____ / _____ / _____
Build version:	_____
Tester:	_____
Signature:	

eHerkenningsmakelaar

Test	Result	Comment
HM – Keyname-Key Mismatch A		
HM – Keyname-Key Mismatch B		
HM – Wrong digest		
HM – Missing fields		
@IssueInstant		
@ID		
@AssertionConsumerServiceIndex		
@AttributeConsumingServiceIndex		
@IsPassive		
@ProtocolBinding		
@Consent		
- Issuer		
- RequestedAuthnContext		
- AuthnContextClassRef		
HM – Empty fields		
@IssueInstant		
@ID		
@AssertionConsumerServiceIndex		
@AttributeConsumingServiceIndex		
- Issuer		
@Comparison		
- AuthnContextClassRef		

HMS01 Normal flow		
HMS02 Interaction with AD		
HMS03 AD specifies MR		
HMS04 AD does not specify MR		
HMS05 Interaction with MR		
HMS06 Authentication failure		
HMS07 Authorization failure		
HMS08 Cancel replay		
HMS09 ForceAuthn=false		
HMS10 Correct displaynames		
HMS11 Non-existent ServiceID		
HMS12 Multiple interface specifications		
HMS13 Level of Assurance		
HMS14 Optional attributes		
HMS15 Chain authorization		
HMS16 B2C		
HMS17 Single Sign On		
HMS18 Logout		

Authenticatiedienst

Test	Result	Comment

AD – Keyname-Key Mismatch A		
AD – Keyname-Key Mismatch B		
AD – Wrong digest		
AD – Missing fields		
@ProviderName		
@IssueInstant		
@ID		
@AssertionConsumerServiceIndex		
@AttributeConsumingServiceIndex		
- Issuer		
- RequestedAuthnContext		
- AuthnContextClassRef		
AD – Empty fields		
@ProviderName		
@IssueInstant		
@ID		
@AssertionConsumerServiceIndex		
@AttributeConsumingServiceIndex		
- Issuer		
@Comparison		
- AuthnContextClassRef		
AD – Random value swaps		

ADS01 Normal flow ADS02 Replay normal flow ADS03 Level of Assurance too high ADS04 Authentication failure ADS05 Cancel authentication ADS06 ForceAuthn=false ADS07 Optional attributes ADS08 B2C ADS09 B2C not supported ADS10 Logout		

Machtigingenregister

Test	Result	Comment
MR – Keyname-Key Mismatch A MR – Keyname-Key Mismatch B MR – Wrong digest MR – Missing fields @IssueInstant @ID – Issuer – Extensions – xacml-context:Attribute (1) – xacml-context:AttributeValue – xacml-context:Request – xacml-context:Subject – xacml-context:Attribute (2) – xacml-context:AttributeValue – xacml-context:Resource		

- xacml-context:Attribute (3)
- xacml-context:AttributeValue
- xacml-context:Attribute (4)
- xacml-context:AttributeValue
- xacml-context:Action
- xacml-context:Attribute
- xacml-context:AttributeValue
- xacml-context:Environment
MR - Empty fields
@IssueInstant
@ID
- Issuer
- Extensions
- xacml-context:Attribute (1)
- xacml-context:AttributeValue
- xacml-context:Request
- xacml-context:Subject
- xacml-context:Attribute (2)
- xacml-context:AttributeValue
- xacml-context:Resource
- xacml-context:Attribute (3)
- xacml-context:AttributeValue
- xacml-context:Attribute (4)
- xacml-context:AttributeValue
- xacml-context:Action
- xacml-context:Attribute
- xacml-context:AttributeValue
- xacml-context:Environment
MR - Random value swaps

MRS01 Normal flow MRS02 Authorization request for a level of assurance that is too high MRS03 Authorization check failure MRS04 Non-existent ServiceID MRS05 Additional attributes MRS06 Chain authorization		

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Template deelnemersovereenkomst

s eHerkenning - Deelnemersovereenkomst 1.8 TC.docx

Edit Document

Afsprakenstelsel eHerkenning

Deelnemersovereenkomst

Versie 1.8

Partijen

De Staat der Nederlanden, te dezen vertegenwoordigd door de minister van Binnenlandse Zaken en Koninkrijksrelaties, voor deze de directeur Logius, de heer S.B. Luitjens,

Verder te noemen: beheerorganisatie en

<Naam deelnemer> gevestigd te <adres>, te dezen vertegenwoordigd door <naam> , voor deze <functie>, <naam>,

verder te noemen: deelnemer,

Overwegende dat

I. dienstverleners in toenemende mate langs elektronische weg diensten wensen te verlenen aan dienstafnemers;

II. een betrouwbare herkenning van de dienstafnemer daarbij noodzakelijk is;

III. in deze behoefte wordt voorzien door middel van het netwerk voor eHerkenning;

IV. in het netwerk voor eHerkenning vijf rollen worden onderscheiden, te weten de middelenuitgever, de authenticatiedienst, de ondertekendienst, het machtigingenregister en de herkenningsmakelaar;

V. in het netwerk voor eHerkenning de positie van dienstverlener wordt onderscheiden;

VI. de deelnemer herkenningsdiensten wenst te verlenen en wenst te worden toegelaten tot het netwerk voor eHerkenning om één of meer rollen te vervullen;

VII. het deelnemers alleen wordt toegestaan een rol in het netwerk voor eHerkenning te vervullen indien zij de toetredingsprocedure met goed gevolg hebben doorlopen en onderhavige overeenkomst met de beheerorganisatie hebben gesloten;

VIII. in het afsprakenstelsel is vastgelegd aan welke verplichtingen de deelnemer dient te voldoen voor de desbetreffende rol;

IX. de beheerorganisatie optreedt als beheer- en toezichtorganisatie;

X. de deelnemer en de beheerorganisatie hun afspraken in deze Deelnemersovereenkomst hebben vastgelegd.

Verklaren te zijn overeengekomen als volgt

Artikel 1. Definities

1.1 Alle onderstreepte begrippen die in deze Deelnemersovereenkomst zijn opgenomen, hebben de betekenis, zoals opgenomen in het afsprakenstelsel. De begrippen worden slechts de eerste keer dat zij in de Deelnemersovereenkomst voorkomen, onderstreept. Alle definities kunnen zowel in enkel- als meervoud gehanteerd worden.

Artikel 2. Voorwerp van de Deelnemersovereenkomst

2.1 De deelnemer verkrijgt hierbij het recht binnen het netwerk voor eHerkenning voor eigen rekening en risico herkenningsdiensten aan te bieden en de rol(len) te vervullen waarvoor hij de toetredingsprocedure met goed gevolg heeft doorlopen.

2.2 De deelnemer is gehouden alle verplichtingen onverkort na te komen die op grond van deze Deelnemersovereenkomst, het afsprakenstelsel , de Gebruiksvoorwaarden en alle overige bindende regelingen in het kader van eHerkenning op enig moment voor zijn rol zijn vastgesteld en in werking zijn getreden.

2.3 De deelnemer is op de hoogte van en erkent de taak van de beheerorganisatie , zoals vastgelegd in het Instellingsbesluit.

2.4 De beheerorganisatie is gerechtigd om aan anderen dan de deelnemer toestemming te geven één of meer rollen in het netwerk voor eHerkenning te vervullen.

2.5 Het is de deelnemer niet toegestaan ook andere rollen en/of andere betrouwbaarheidsniveaus te vervullen zonder opnieuw de toetredingsprocedure te doorlopen.

2.6 De beheerorganisatie zal zich inspannen de op haar rustende verplichtingen naar beste vermogen na te komen, met inachtneming van de belangen van alle betrokken partijen.

2.7 Deze Deelnemersovereenkomst bestaat uit de volgende documenten:

a) dit document;
b) het afsprakenstelsel zoals formeel op enig moment is vastgesteld en van toepassing is op en in werking getreden is voor een bepaalde rol;
c) de Gebruiksvoorwaarden.

2.8 Bij strijdigheden tussen de in het vorige lid genoemde documenten, prevaleert het eerder genoemde document boven het later genoemde document.

2.9 Een bepaling in de Deelnemersovereenkomst die strijdig is met het afsprakenstelsel en/of het geldende recht, laat de overige bepalingen van de Deelnemersovereenkomst onverlet.

Artikel 3. Gebruiksrecht voor het voeren van het Merk

3.1 Onder het Merk wordt verstaan: het (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan de beheerorganisatie in het kader van eHerkenning in opdracht van het ministerie van Economische Zaken, Landbouw en Innovatie het merkenrecht uitoefent.

3.2 De beheerorganisatie verleent hierbij aan de deelnemer het niet-exclusieve en niet-overdraagbare recht om, gedurende de looptijd van de Deelnemersovereenkomst, het Merk te gebruiken in verband met het uitvoeren van eHerkenningsdiensten en het vervullen van de overeengekomen rol(len), in overeenstemming met deze Deelnemersovereenkomst en de daaruit voortvloeiende voorschriften.

3.3 De deelnemer is niet bevoegd derden toestemming te geven het Merk te gebruiken.

3.4 De deelnemer zal niets doen dan wel nalaten waardoor de rechten van de beheerorganisatie en/of het ministerie van Economische Zaken, Landbouw en Innovatie ten aanzien van het Merk kunnen worden aangetast en/of de door de beheerorganisatie ter zake van het Merk en/of opgebouwde goodwill negatief zou kunnen beïnvloeden.

Artikel 4. Aanvang, looptijd en duur van de Deelnemersovereenkomst

4.1 De Deelnemersovereenkomst treedt in werking op 1 oktober 2012 en eindigt van rechtswege op 1 januari 2014.

Artikel 5. Beëindiging van de Deelnemersovereenkomst

5.1 De deelnemer is te allen tijde gerechtigd de Deelnemersovereenkomst tussentijds schriftelijk te beëindigen met inachtneming van een opzegtermijn van 2 kalendermaanden.

5.2 De beheerorganisatie kan de Deelnemersovereenkomst in de navolgende situaties beëindigen:

- Op basis van het nalevingsbeleid indien de deelnemer enige verplichting uit de Deelnemersovereenkomst of het afsprakenstelsel niet nakomt en hem de sanctie van beëindiging van de Deelnemersovereenkomst door het ministerie van Economische Zaken, Landbouw en Innovatie wordt opgelegd;
- Het ministerie van Economische Zaken, Landbouw en Innovatie de opdracht aan de beheerorganisatie intrekt om op te treden als beheerorganisatie binnen het stelsel van eHerkenning;
- De klachten- en geschillencommissie hiertoe adviseert naar aanleiding van een klacht of geschil;
- De deelnemer de belang en schaadt van het netwerk voor eHerkenning waaronder de reputatie van het Merk;
- De deelnemer failliet is verklaard of aan hem surseance van betaling is verleend;
- De beheerorganisatie besluit haar activiteiten te staken.

5.3 Na beëindiging van de Deelnemersovereenkomst zal de deelnemer direct alle activiteiten en uitingen in het kader van het vervullen van de betreffende rol(len) staken, dan wel zo snel mogelijk staken als toelaatbaar is. De deelnemer zal alle medewerking verlenen om de continuïteit van de herkenningsdienstverlening zeker te stellen, onder meer door mee te werken aan overdracht van de herkenningsdienstverlening aan een andere deelnemer.

Artikel 6. Aansprakelijkheid deelnemers jegens derden en beheerorganisatie

6.1 De deelnemer aanvaardt door ondertekening van deze Deelnemersovereenkomst aansprakelijkheid voor het eigen handelen en/of nalaten binnen de rol die de deelnemer vervult. De deelnemer aanvaardt deze aansprakelijkheid ook in die situaties waarbij dit handelen en/of nalaten schade veroorzaakt aan andere deelnemers en/of bedrijven en/of dienstverleners en/of de beheerorganisatie. Bedrijven, dienstverleners, andere deelnemers en de beheerorganisatie kunnen zich jegens de deelnemer onmiddellijk en direct op deze aansprakelijkheid beroepen.

6.2 In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

6.3 De deelnemer vrijwaart de beheerorganisatie voor vorderingen van derden, uit welke hoofde dan ook, ten gevolge van het gebruik van de herkenningsdiensten.

Artikel 7. Overige bepalingen

7.1 De beheerorganisatie is bevoegd te (doen) onderzoeken of deelnemer de afspraken van het afsprakenstelsel naleeft en/of deelnemer voldoet aan de eisen en voorwaarden die aan zijn rol worden gesteld in het afsprakenstelsel. De deelnemer verleent hieraan zijn medewerking.

7.2 Verplichtingen uit deze Deelnemersovereenkomst die naar hun aard bedoeld zijn om ook na afloop van deze Deelnemersovereenkomst voort te duren, behouden hun werking na afloop van deze Deelnemersovereenkomst.

7.3 Op deze overeenkomst is Nederlands recht van toepassing.

Aldus overeengekomen in tweevoud,

Namens de beheerorganisatie , Naam: S.B. Luitjens Functie: Directeur Logius Datum: Plaats: 's-Gravenhage	Namens de deelnemer, Naam: Functie: Datum: Plaats:
	<Naam deelnemer>

Template incidentrapport

Incidentrapport

Incidentnummer:	In te vullen door de beheerorganisatie
Korte beschrijving	
Auteur(s)	
Datum:	
Versie	

Samenvatting

Datum/tijdstip/periode incident	
Melder bij BO	
Manier van melden bij BO	Mantis <issue nr vermelden> of e-mail aan info@eherkenning.nl (datum, tijd en afzender vermelden)
Behandeling beperken tot BO	Ja/nee Ja = communicatie over incident beperken tussen deelnemer en BO Nee = mag gedeeld worden via Mantis en besproken worden in overleg met andere deelnemers
Type incident	Beschikbaarheid/vertrouwelijkheid/integriteit; onbewust/bewust veroorzaakt Opties verwijderen die niet van toepassing zijn op het incident
Beveiligingsincident	Ja/nee
Non-conformiteit SLA-afspraken	In te vullen door beheersorganisatie
Impact	Hoog/medium/laag
Prioriteit	Hoog/medium/laag
Status	Open/closed
Oorzaak	Korte omschrijving van de oorzaak van het incident
Lognummer	In te vullen door beheerorganisatie
Datum en tijdstip afmelding	In te vullen door beheerorganisatie

Omschrijving

Beschrijf hier de oorzaak van het incident

Geef de mate van zekerheid aan dat dit inderdaad de oorzaak is

Geef aan of er een kans op herhaling bestaat

Mogelijke gevolgen

Beschrijf de gevolgen op het afsprakenstelsel

Maatregelen

Beschrijf de maatregelen die getroffen zijn om de gevolgen te beperken cq herhaling van het incident te voorkomen. Geef aan of deze maatregelen al actief zijn, of anders wanneer deze, naar verwachting, kunnen worden geïmplementeerd.

Template verzoek tot (uitbreiding) toetreding eHerkenning

Dit verzoek tot toetreding stelt (potentiële) deelnemers van eHerkenning in staat zich aan te melden voor (uitbreiding van) deelname aan het netwerk voor eHerkenning. Dit ingevulde formulier vormt een onderdeel van het toetredingsproces voor eHerkenning, zoals beschreven in de meest actuele versie van het Afsprakenstelsel eHerkenning, onderdeel Operationeel handboek.

Bedrijf

Naam:	_____
Handelsnaam:	_____
KvK nummer:	_____

Contactpersoon

Naam:	_____
Functie:	_____
E-mailadres:	_____
Telefoonnummer:	_____

Huidige rollen

Bovengenoemd bedrijf is op datum van ondertekening toegetreden tot het netwerk voor eHerkenning in de volgende rollen en voor de volgende betrouwbaarheidsniveaus:

	eH1	eH2	eH2+	eH3	eH4
eHerkenningsmakelaar			O		
Middelenuitgever	O	O	O	O	O
Authenticatiedienst	O	O	O	O	O
Machtigingenregister	O	O	O	O	O

Huidige optionele functionaliteit

Bovengenoemd bedrijf levert op datum van ondertekening de volgende optionele functionaliteit:

	Herkennings makelaar	Middelen uitgever	Authenticatie dienst	Machtigingen register
B2C		O	O	
Beroepsbeoefenaren		O	O	
Gevalideerde attributen		O	O	O
Single Sign On			O	
Ketenmachtigingen				O
Machtigingen voor beroepsbeoefenaren				O

Nieuwe rollen

Ondergetekende verklaart dat bovengenoemd bedrijf voornemens is het in het afsprakenstelsel beschreven toetredingsproces te doorlopen voor de volgende rollen en voor de volgende betrouwbaarheidsniveaus:

	eH1	eH2	eH2+	eH3	eH4
eHerkenningsmakelaar			O		
Middelenuitgever	O	O	O	O	O
Authenticatiedienst	O	O	O	O	O
Machtigingenregister	O	O	O	O	O

Nieuwe optionele functionaliteit

Ondergetekende verklaart dat bovengenoemd bedrijf voornemens is het in het afsprakenstelsel beschreven toetredingsproces te doorlopen voor de volgende optionele functionaliteit:

	Herkennings makelaar	Middelen uitgever	Authenticatie dienst	Machtigingen register
B2C		O	O	
Beroepsbeoefenaren		O	O	
Gevalideerde attributen		O	O	O
Single Sign On			O	
Ketenmachtigingen				O
Machtigingen voor beroepsbeoefenaren				O

N.B. Bij dit verzoek dient voor elk van de aangekruiste betrouwbaarheidsniveaus een (proces)beschrijving te worden overlegd die volgens de kandidaat een classificatie op het betreffende betrouwbaarheidsniveau rechtvaardigt. Tevens moet voor elke (proces)beschrijving een URL worden verschaft waar deze (proces)beschrijving beschikbaar is gemaakt voor gebruikers.

Systemen

Ondergetekende verklaart de systemen van de kandidaat succesvol te hebben getest met de door de beheerorganisatie ter beschikking gestelde testsimulator. De door ondergetekende eerder aangeleverde metadata kan door de beheerorganisatie worden gebruikt om de systemen (steekproefsgewijs) te testen.

Testfaciliteiten

Wanneer de kandidaat toetreding vraagt als middelenuitgever moeten bij dit verzoek ten minste twee testauthenticatiemiddelen met de bijbehorende (door de authenticatiedienst te gebruiken) pseudoniemen worden overlegd die door de beheerorganisatie gebruikt kunnen worden om de implementatie te testen.

Wanneer de kandidaat toetreding vraagt als machtigingenregister moeten voor alle geleverde testauthenticatiemiddelen testmachtigingen worden geregistreerd, voor de in de dienstencatalogus beschreven testdienstverlener. De geregistreerde machtinginformatie (inclusief de specifieke pseudoniemen) moet worden overlegd.

Conformiteit

Ondergetekende dient de Template zelfverklaring voor bovengenoemd bedrijf te controleren op juistheid voor de nieuwe situatie (uitbreiding rollen) en eventuele aanpassingen (visueel onderscheidend) door te voeren, en waar nodig een nieuwe ondertekende Zelfverklaring aan te leveren aan de beheerorganisatie

Ondertekening

Ondergetekende verzoekt de beheerorganisatie op basis van de door invulling van dit formulier verschafte informatie en de bijgevoegde bijlagen bovengenoemd bedrijf toe te laten treden als deelnemer van het afsprakenstelsel eHerkenning voor de

hierboven aangekruiste rollen, betrouwbaarheidsniveaus en optionele functionaliteit.

Datum:	_____
Plaats:	_____
Naam:	_____
Handtekening:	_____

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Template vrijwaring penetratietest

u eHerkenning – Template Vrijwaringsverklaring Penetratietest 1.8 TC.docx

Edit Document

Afsprakenstelsel eHerkenning

Bijlage: Template Vrijwaringsverklaring Penetratietest

Versie 1.8

Overeenkomst inzake een regeling van aansprakelijkheid met betrekking tot een penetratietest

De ondergetekenden:

1. De Staat der Nederlanden, gevestigd te Den Haag, hierbij rechtsgeldig vertegenwoordigd door de heer S.B. Luitjens, directeur Logius,

hierna te noemen De Opdrachtgever ,

en

2. < Naam uitvoerder > gevestigd te < plaats >, hierbij rechtsgeldig vertegenwoordigd door de heer/mevrouw < naam/functie >,

hierna te noemen: De Uitvoerder ,

en

3. < Naam onderzochte partij > gevestigd te < plaats >, hierbij rechtsgeldig vertegenwoordigd door de heer/mevrouw < naam/functie >,

hierna te noemen: De Onderzochte Partij ,

Overwegende dat

1. het beheer van het Afsprakenstelsel eHerkenning is ondergebracht bij de Opdrachtgever;
2. de Opdrachtgever in het kader van informatiebeveiliging van de Onderzochte Partij een zogenaamde penetratietest wenst uit te laten voeren bij de Onderzochte Partij;
3. de Uitvoerder bereid is deze penetratietest bij de Onderzochte Partij uit te voeren ;
4. de penetratietest alleen kan geschieden met toestemming van de Onderzochte Partij;
5. de in het kader van de penetratietest door de Uitvoerder te verrichten werkzaamheden mogelijkerwijs schade tot gevolg zouden kunnen hebben;
6. de Uitvoerder ten aanzien van de aansprakelijkheid voor deze schade van de Onderzochte Partij een vrijwaring wenst;
7. partijen hun afspraken in verband met de penetratietest in deze overeenkomst wensen te regelen.

Zijn het volgende overeengekomen:

Artikel 1 Toestemming en vrijwaring

1. De Onderzochte Partij geeft de Uitvoerder hierbij toestemming tot het uitvoeren van een penetratietest voor zover deze ziet op:
   a. een TYPE ONDERZOEK (NB: grey box of black box, white box etc) waarbij de Uitvoerder beschikt over alle relevante informatie nodig voor het goed kunnen uitvoeren van de penetratietest (indien nodig aanpassen) ;
   b. een infrastructuurscan waarbij onder meer wordt gezocht naar mogelijke toegangen in de productie omgeving van de Onderzochte Partij;
   c. een penetratietest waarbij onder meer gezocht wordt naar de top 10 kwetsbaarheden zoals beschreven door OWASP op de productie omgeving van de Onderzochte Partij;
   d. een functionele test waarbij onder meer de berichtenuitwisseling en de inhoud van de berichten wordt gemanipuleerd op de acceptatie omgeving van de Onderzochte Partij.
2. Gezien de in lid 1 omschreven reikwijdte van de penetratietest, zullen de werkzaamheden van de Uitvoerder niet zien op Denial of Service-attacks, social engineering-attacks of mysteryguest bezoeken , en garandeert de Uitvoerder dat er geen schade zal worden aangericht buiten de in artikel 1 lid 1 omschreven reikwijdte en zal de Uitvoerder alleen gegevens vastleggen of verwerken als dat voor bewijsvoering van genoemde penetratietest nodig is.
3. De Onderzochte Partij is zich ervan bewust dat de werkzaamheden van de Uitvoerder zijn gericht op het identificeren van kwetsbaarheden in de beveiliging van het geautomatiseerde werk en de gegevens die aan de Onderzochte Partij toebehoren, met het oogmerk om doeltreffende maatregelen te kunnen treffen ten aanzien van deze kwetsbaarheden.
4. Onverminderd het bepaalde in artikel 2 is de Uitvoerder niet aansprakelijk voor schade die ontstaat als gevolg van diens werkzaamheden, voor zover deze werkzaamheden vallen binnen de reikwijdte van de penetratietest zoals omschreven in artikel 1 lid 1. De Onderzochte Partij vrijwaart de Uitvoerder van aansprakelijkheden dienaangaande, met name ingeval van maar niet beperkt tot de situatie waarin een derde zich direct of indirect beroept op de artikelen 161sexies, 161septies, 351, 351bis, 138a en 138b van het Wetboek van Strafrecht. De vrijwaring omvat dat:
   - de Onderzochte Partij afziet van schadeaanspraken ten aanzien van de Uitvoerder;
   - de Onderzochte Partij de Uitvoerder bijstaat indien hij aansprakelijk wordt gesteld door een derde. Zij zal in dat geval de schade van de Uitvoerder, inclusief eventuele proceskosten, vergoeden mits de Uitvoerder de Onderzochte Partij hiervan prompt op de hoogte stelt, voorts zal zij in een voorkomend geval en voor

zover de Onderzochte Partij daarover beschikt bewijs leveren ten gunste van de Uitvoerder, tenzij Onderzochte Partij wenst dat de procedure aan haar wordt overgelaten en Uitvoerder Onderzochte partij daartoe alle nodige medewerking verleent.

Artikel 2 Geen vrijwaring voor wanprestatie

1. De in artikel 1 genoemde vrijwaring ziet niet op schade die is ontstaan door een toerekenbare tekortkoming bij het uitvoeren van deze Overeenkomst c.q. de penetratietest door de Uitvoerder dan wel bij opzet, bewuste roekeloosheid, ernstige verwijtbaarheid of een beroepsfout bij Uitvoerder.

Artikel 3 Bewerkersovereenkomst

1. Bij de uitvoering van de penetratietest zal de Uitvoerder het verwerken van persoonsgegevens vermijden. Dit kan echter niet worden uitgesloten door de Uitvoerder.
2. De Onderzochte Partij is de verantwoordelijke voor de gegevensverwerking in de zin van de Wet bescherming persoonsgegevens.
3. De Uitvoerder verbindt zich om in het kader van de verwerking van persoonsgegevens, de Wet bescherming persoonsgegevens na te leven en onder meer de persoonsgegevens van de Onderzochte Partij als bewerker in de zin van de Wet bescherming persoonsgegevens behoorlijk en zorgvuldig te verwerken. In dit kader zal Uitvoerder de persoonsgegevens slechts in opdracht van Onderzochte Partij verwerken en deze adequaat beveiligen en technische en organisatorische maatregelen treffen tegen enige vorm van onrechtmatige verwerking. Tevens zal Uitvoerder Onderzochte Partij in staat stellen toe te zien op naleving van de verplichting tot adequate beveiliging en mogelijke beveiligingsincidenten onverwijld aan Onderzochte Partij melden.
4. De Uitvoerder zal te allen tijde op eerste verzoek van de Onderzochte Partij onmiddellijk alle van de Onderzochte Partij afkomstige en/of in opdracht van de Onderzochte Partij verwerkte gegevens met betrekking tot deze overeenkomst aan de Onderzochte Partij ter hand stellen.
5. De Uitvoerder zal te allen tijde op eerste verzoek van de Onderzochte Partij onmiddellijk alle afschriften en kopieën van de Onderzochte Partijen afkomstige en/of in opdracht van de Onderzochte Partij verwerkte gegevens met betrekking tot de Onderzochte Partij vernietigen.

Artikel 4 Beschikbaar stellen en eigendom van onderzoekresultaten

1. De resultaten van de penetratietest worden door de Uitvoerder, na afstemming van de concept rapportage door de Opdrachtgever met de Onderzochte Partij en de Uitvoerder, ter beschikking gesteld aan de Opdrachtgever.

Artikel 5 Uitvoer ing van de pen etratietest

1. De Opdrachtgever zal de Onderzochte Partij vooraf informeren over de periode waarin de penetratietest zal plaatsvinden. Dit zal geschieden door het aanmaken van een “Ma n tis issue”. De Uitvoerder zal pas van start gaan met het uitvoeren van de penetratietest na instemming van de Onderzochte Partij. De Uitvoerder zal zich buiten de door Opdrachtgever aangekondigde periode onthouden van onderzoeken bij de Onderzochte Partij.
2. De Uitvoerder zal de Onderzochte Partij benaderen vanaf een IP nummer dat wordt gecommuniceerd in het onder Artikel 5 lid 1 genoemde “Mantis issue”.
3. De Uitvoerder zal een contactpersoon aanwijzen waarmee de Onderzochte Partij altijd en onmiddellijk contact kan opnemen. Deze gegevens zullen worden opgenomen in het “Mantis issue” zoals beschreven in Artikel 5 lid 1.
4. Op eerste verzoek van de Onderzochte Partij aan de contactpersoon van de Uitvoerder zal de Uitvoerder de uitvoering van de penetratietest onmiddellijk staken. De onderzochte Partij doet dit verzoek aan Uitvoerder niet eerder dan nadat dit, met redenen omkleed, is afgestemd met de Opdrachtgever en Opdrachtgever hiermee heeft ingestemd.
5. De Uitvoerder verklaart dat hij bij het uitvoeren van de penetratietest als een zorgvuldige en vakbekwame dienstverlener te werk zal gaan. Dit betekent onder meer dat de Uitvoerder gebruik zal maken van gekwalificeerd personeel en enkel geschikte middelen ter uitvoering van de penetratietest zal inzetten.

Artikel 6 Looptijd

1. De afspraken vervat in deze overeenkomst zien enkel op het uitvoeren van een penetratietest zoals beschreven in artikel 1 lid 1 in de periode lopende van [begin pentest periode] tot en met [gepland einde pentest periode], dan wel tot het moment dat de uitvoering door de Uitvoerder wordt gestaakt zoals genoemd in artikel 5 lid 4 indien dit moment eerder is dan de voornoemde lopende periode.

Artikel 7 Toepasselijk recht en geschillen

1. Op deze overeenkomst en alle daaruit voortvloeiende gevolgen is Nederlands recht van toepassing. Geschillen inzake deze overeenkomst en de uitvoering daarvan worden voorgelegd aan de bevoegde rechter te Den Haag.

Aldus overeengekomen en in drievoud ondertekend,

Namens Opdrachtgever,

Naam :
Datum :
Plaats :

Namens Uitvoerder,

Naam : FUNCTIE ONDERTEKENAAR
Datum : DATUM VAN ONDERTEKENING
Plaats : PLAATS VAN ONDERTEKENING

Logius
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Namens Onderzochte Partij,

Naam : FUNCTIE ONDERTEKENAAR
Datum : DATUM VAN ONDERTEKENING
Plaats : PLAATS VAN ONDERTEKENING

Template wijziging rechtspersoon deelnemer

Wijziging rechtspersoon deelnemer

De deelnemer verklaart door ondertekening van dit formulier dat:

- de rechtspersoon waaraan de onderneming van de deelnemer toebehoort, wijzigt;
- de deelnemer de Beheerorganisatie verzoekt de deelnemersovereenkomst op naam te zetten van de nieuwe rechtspersoon;
- de organisatie en bedrijfsprocessen van de deelnemer, zoals daarvan tijdens de toetredingsprocedure verslag van is gedaan en zoals daarvan testen hebben plaatsgevonden, niet zijn gewijzigd;
- hij in het kader van de nieuwe rechtspersoon onveranderd conform het Afsprakenstelsel zal handelen.

(1) Huidige rechtspersoon

Naam	_____
KvK nummer	_____

(2) Nieuwe rechtspersoon

Naam	_____
KvK nummer	_____

(3) Contactpersoon

Naam	_____
E-mailadres	_____
Telefoonnummer	_____

(4) Rollen en/of betrouwbaarheidsniveaus

Ondergetekende verklaart dat de deelnemer het toetredingproces heeft doorlopen voor de volgende rollen en voor de volgende betrouwbaarheidsniveaus:

	eH1	eH2	eH2+	eH3	eH4
eHerkenningsmakelaar			O		
Middelenuitgever	O	O	O	O	O
Authenticatiedienst	O	O	O	O	O
Machtigingenregister	O	O	O	O	O

(5) Verplichting ten aanzien van testen en conformiteit

De ondergetekende verklaart op grond van de reeds doorlopen toetredingsprocedure:

- onverminderd zijn medewerking te verlenen aan penetratietesten van de systemen;
- onverminderd zal handelen conform het afsprakenstelsel zoals dat op enig moment formeel is vastgesteld.

(6) Ondertekening

Datum:	_____

Plaats:	_____
Naam:	_____
Handtekening:	_____

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.

Bijgevoegd:

O Kopie uittreksel handelsregister (liefst ingescand/elektronisch exemplaar)

O Kopie volmacht (liefst ingescand/elektronisch exemplaar)

Template zelfverklaring

Dit document dient als zelfverklaring van een aankomende of bestaande deelnemer waarmee wordt aangegeven dat wordt voldaan aan de eisen uit Afsprakenstelsel eHerkenning. Nieuwe toetreders dienen dit document te overleggen als onderdeel van de toetredingsprocedure. Het document vormt gezamenlijk met het Template verzoek tot (uitbreiding) toetreding eHerkenning en procesbeschrijvingen (afhankelijk van de rol(len) waarvoor de toetredingsprocedure wordt doorlopen) input voor het toetredingsgesprek. Tevens dient het document door bestaande deelnemers te worden overlegd wanneer wordt overgegaan op een nieuwe versie van het afsprakenstelsel.

Naast deze zelfverklaring zijn er in het Afsprakenstelsel eHerkenning certificeringen voorgeschreven die in een separaat proces worden gevalideerd.

Zelfverklaring

Ondergetekende verklaart hierbij voor alle rollen, betrouwbaarheidsniveaus en optionele functionaliteiten waarvoor de toetredingsprocedure is/wordt doorlopen, te voldoen aan de vereisten in de volgende delen van het Afsprakenstelsel eHerkenning:

- Algemene introductie
- Gebruiksvoorwaarden eHerkenning
- Juridisch kader
- Businessmodel
- Informatiebeveiliging en privacy
- Operationeel handboek
- Handboek huisstijl
- Service level
- Use cases
- Interface specifications
- Betrouwbaarheidsniveaus en registratie-eisen

Ondertekening

Datum:	_____
Plaats:	_____
Naam:	_____
Handtekening:	_____

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.