Afsprakenstelsel eHerkenning

Algemene introductie

Versie 1.7a

INHOUDSOPGAVE

COLOFON

Auteur	Status
Beheerorganisatie Afsprakenstelsel eHerkenning	Definitief
Project	**Datum**
Afsprakenstelsel eHerkenning	27 augustus 2013
Organisatie	**Classificatie**
Logius	Openbaar
Titel van het document	**Versie**
Afsprakenstelsel eHerkenning – Algemene introductie	1.7a

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
29/03/10	0.8def	T.b.v. proef- implementaties		Projectbureau
09/06/10	1.0	Losstaande algemene introductie waarin hoofdstukken 1 t/m 4 van 0.8def verwerkt zijn voor zover niet in andere delen geplaatst.	Ter goedkeuring	Projectbureau
17/06/11	1.1	RFCs verwerkt conform besluit kernteam 31 mei	Definitief	Projectbureau
11/12/11	1.2	RFCs verwerkt conform besluit kernteam 11 okt	Definitief	Projectbureau
23/12/11	1.3	RFCs verwerkt conform besluit kernteam 13 dec	Definitief	Projectbureau
28/04/12	1.4	RFCs verwerkt conform besluit kernteam 20 mrt	Definitief	Beheerorganisatie
12/07/12	1.5	RFCs verwerkt conform besluit kernteam 26 juni	Definitief	Beheerorganisatie
01/04/13	1.6	RFC0182, RFC0197, RFC0201, RFC0207 verwerkt	Definitief	Beheerorganisatie
16/05/13	1.7	RFC00188, RFC0200, RFC0204, RFC0210 verwerkt	Definitief	Beheerorganisatie
27/08/13	1.7a	RFC0226	Definitief	Beheerorganisatie

DISTRIBUTIE

Datum	Distributie	Versie
	Tactisch overleg, Gebruikersraad en publicatie op eherkenning.nl	1.7a

GOEDKEURING

Datum	Naam	Versie
27/08/13	Alle RFCs voor versie 1.7a goedgekeurd door Tactisch Overleg	1.7a

1 Inleiding

1.1 Het doel van eHerkenning

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[1]. 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] en zijn er in kader van de Overheidsbrede implementatieagenda voor dienstverlening en e-overheid (iNUP)[3] afspraken gemaakt met gemeenten en andere overheden over de implementatie.

---

1 Zie bijvoorbeeld het rapport van de commissie Wallage/Postma (2007), dat de aanzet gaf aan het Nationaal Uitvoeringsprogramma.

2 Digitale Agenda § 2.2 http://www.rijksoverheid.nl/onderwerpen/ict/documenten-en-publicaties/kamerstukken/2011/05/17/digitale-agendanl.html 17 mei 2011.

3 30 mei 2011: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/05/30/aanbiedingsbrief-overheidsbrede-implementatieagenda-voor-dienstverlening-en-e-overheid-i-nup.html

1.2 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.

1.3 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.

1.4 Proces en status van eHerkenning

1.4.1 Bij 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*[4].

4 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[5]. 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.

1.4.2 Bij 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 hebben betreffen geen inhoudelijke wijzigingen.

1.4.3 Bij 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

5 Zie voor de verdere uitwerking van de inrichting van het het beheer het document [Juridisch kader]. In 2012 is het beheer overgedragen aan Logius.

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.

1.4.4 Bij versie 1.3a

Deze versie omvat enkel correcties op de koppelvlakspecificaties welke tijdens de implementatie van versie 1.3 naar boven zijn gekomen.

1.4.5 Bij 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.

1.4.6 Bij 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.

1.4.7 Bij 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.

1.4.8 Bij versie 1.7

Deze versie bevat verschillende nieuwe functionaliteiten, te weten Single Sign On (SSO), uitgebreide attribuutverstrekking, keten machtigingen en 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.

1.5 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 (zie 1.6).

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[6] van eHerkenning te gebruiken.

1.6 Documentatieset afsprakenstelsel

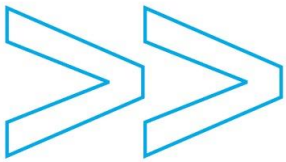
Het afsprakenstelsel eHerkenning wordt inhoudelijk compleet beschreven in totaal 15 documenten en daarnaast gebruiksvoorwaarden, deelnemersovereenkomst en normenkader. Deze versie, 1.7, is bijgewerkt met de per 24 april 2013 door het Tactisch overleg goedgekeurde wijzigingen (RFCs).

Tabel 1 geeft de onderdelen en de globale inhoud van de inhoudelijke documentatie van het afsprakenstelsel eHerkenning aan.

Tabel 1: de inhoudelijke documentatie van afsprakenstelsel eHerkenning

document	globale inhoud
Algemene introductie	Dit document; geeft op hoofdlijnen inzicht in het afsprakenstelsel en de werking van het netwerk.
Juridisch kader	Beschrijft het juridisch kader, het besturingsmodel en de controle op en monitoring van de naleving van het afsprakenstelsel.
Betrouwbaarheids-	Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd

6 Zie www.eherkenning.nl/overheden/eherkenning-voor-overheden/promokit



document	globale inhoud
niveaus	worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast.
Business model	Afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen.
Informatiebeveiliging	Beschrijft de maatregelen die genomen worden om het vertrouwen in en continuïteit van het netwerk te borgen.
Stelsel risicoanalyse	Gedetailleerde analyse naar de risico's binnen het netwerk eHerkenning.
Normenkader	Gedetailleerde uitwerking van de vereiste maatregelen voor informatiebeveiliging.
Operationeel handboek	Beschrijft de operationele processen van de beheerorganisatie.
Service level	Beschrijft de service level afspraken.
Handboek huisstijl	Richtlijn voor deelnemers ten aanzien van het gebruik van het beeldmerk en andere gezamenlijke afspraken over huisstijl die ten behoeve van de herkenbaarheid van het netwerk voor gebruikers noodzakelijk zijn.
Use cases*	Beschrijft de functionaliteit in detail
Koppelvlak DV-HM*	Technische specificatie van het koppelvlak tussen dienstverlener en eHerkenningsmakelaar.
Koppelvlak HM-AD*	Technische specificatie van het koppelvlak tussen eHerkenningsmakelaar en authenticatiedienst.
Koppelvlak HM-MR*	Technische specificatie van het koppelvlak tussen eHerkenningsmakelaar en machtigingenregister.
Testhandleiding voor dienstverleners*	Beschrijft de testen die door nieuwe dienstverleners moeten worden uitgevoerd.
Testhandleiding voor deelnemers*	Beschrijft de testen die door nieuwe deelnemers moeten worden uitgevoerd.
Gebruiksvoorwaarden	De voorwaarden waaronder dienstafnemers en uitvoerend natuurlijk personen eHerkenning mogen gebruiken en op basis waarvan zij gehouden zijn aan de zaken in het afsprakenstelsel die op hen betrekking hebben.
Deelnemers-	De overeenkomst tussen deelnemers en beheerorganisatie op basis waarvan

document	globale inhoud
overeenkomst	deelnemers gehouden zijn het afsprakenstelsel toe te passen. Deze deelnemersovereenkomst *verwijst* naar het afsprakenstelsel maar is er (strikt genomen) zelf geen onderdeel van.

*) Van deze documenten kunnen meerdere versies tegelijkertijd geldig zijn. Voor de overige documenten geldt dat enkel en alleen de laatst gepubliceerde versie geldig is.

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.

1.7 Leeswijzer

Het vervolg van dit document zit als volgt in elkaar. Eerst bekijkt hoofdstuk 2 eHerkenning vanuit het perspectief van de op het netwerk aangesloten gebruikers: de bedrijven en de dienstverleners. Wat merken die aan de "buitenkant" van hoe het afsprakenstelsel en het netwerk voor eHerkenning zich gedragen? Welke principes en uitgangspunten zitten hierachter, en welke begrippen spelen een rol? Dan wendt hoofdstuk 3 zich naar de wereld van de "deelnemers", die het netwerk voor eHerkenning mogelijk maken. Hoe werkt dit netwerk intern, welke rollen zijn daar, hoe werken ze samen, en hoe kunnen die rollen worden ingevuld? Hoofdstuk 4 bespreekt hoe op het netwerk aan te sluiten, als dienstverlener, deelnemer of dienstafnemer. Welke eisen stelt dat, wat moet daarvoor gedaan worden, welke transitiestappen zijn daarvoor nodig?

1.8 Begrippenlijst

Binnen eHerkenning wordt één begrippenlijst gehanteerd. Zie Bijlage A. Begrippenlijst. 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. Dat zelfde geldt ook andersom: waar in dit document de zelfstandige-naamwoords-vorm van een werkwoord wordt gehanteerd, heeft deze dezelfde betekenis als het gedefinieerde werkwoord.

1.9 Terminologie

Ter wille van de leesbaarheid van de tekst is waar het mensen in het algemeen betreft 'hij' geschreven waar 'hij of zij' bedoeld wordt.

1.10 Typografie

Alle begrippen die zijn opgenomen in de begrippenlijst worden vanaf hoofdstuk 2 in dit document de eerste keer dat ze voorkomen onderstreept genoteerd, afgezien van kopjes, delen van woorden en de benamingen van processen en wetten. Nadat een begrip de eerste keer onderstreept voorkomt wordt het steeds exact conform definitie bedoeld in het vervolg van het gehele afsprakenstelsel.

2 Wat is eHerkenning? Het gebruikersperspectief

2.1 Inleiding

Dit hoofdstuk belicht eHerkenning vanuit het perspectief van de op het netwerk aangesloten gebruiker: de dienstverlener 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 Bijlage A. Begrippenlijst. 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.

2.2 Gedrag netwerk eHerkenning op hoofdlijnen

Het netwerk voor eHerkenning levert eHerkenningsdiensten aan gebruikers (zie Figuur 1). 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 in versie 1.7 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.

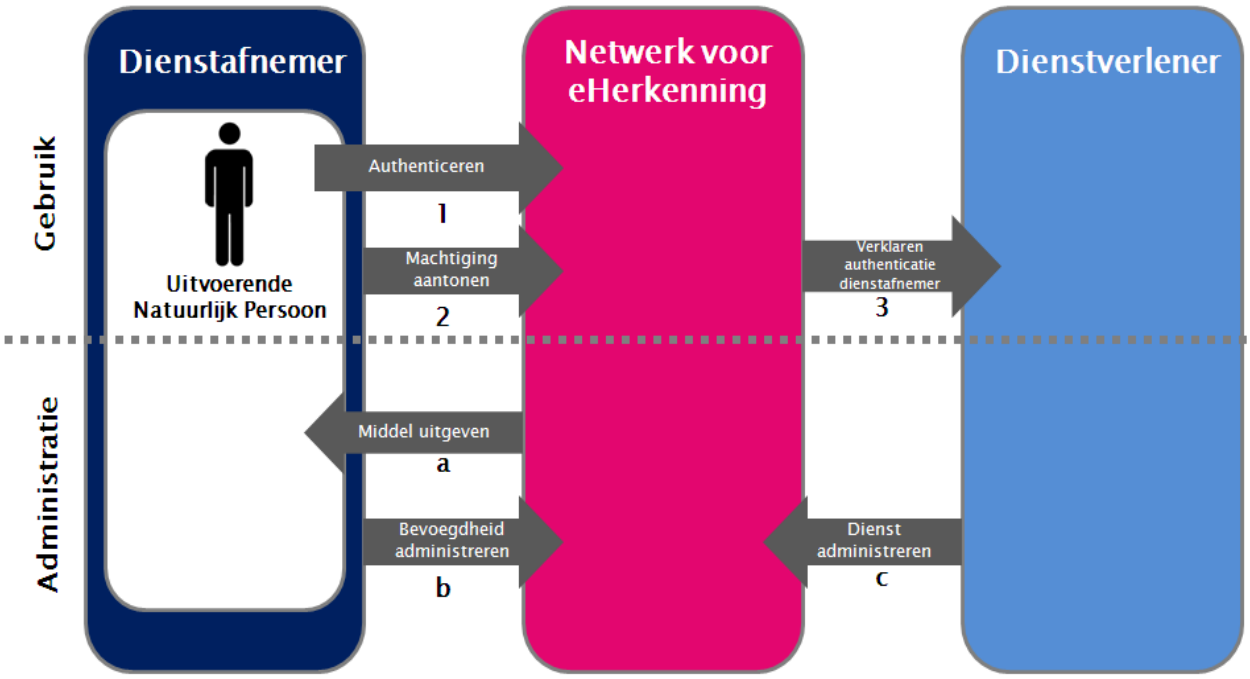
In het dagelijkse gebruik van het netwerk werken deze eHerkenningsdiensten als volgt samen (zie Figuur 1). De uitvoerend natuurlijk persoon wil een elektronische dienst afnemen bij een dienstverlener, bijvoorbeeld het doen van belastingaangifte of het aanvragen van een subsidie of vergunning. Op een 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. Hoofdstuk 4 beschrijft welke eenmalige werkzaamheden voor het aansluiten van een gebruiker nodig zijn. De hoofdstukken 2 en 3 beschrijven de *continue* werkzaamheden van gebruiker en netwerk.



Figuur 1: Netwerk eHerkenning in 188context

2.3 Kernbegrippen van eHerkenning

Het netwerk voor eHerkenning (zie Figuur 1) 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 hoofdstuk 3). 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 in hoofdstuk 2.2 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 Bijlage A. Begrippenlijst).

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 versie 1.7 van eHerkenning worden ketens van maximaal twee niveaus van vertegenwoordiging ondersteund.

Het afsprakenstelsel hanteert vijf vastomschreven betrouwbaarheidsniveaus (zie Tabel 2) om 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[7]. eHerkenning bouwt voort op STORK's criteria voor authenticatiemiddelen en voegt daaraan criteria voor bevoegdheden toe. Het document [Betrouwbaarheidsniveaus en registratie-eisen] werkt dit inhoudelijk uit, gaat in op toekomstige ontwikkelingen van het raamwerk en hoe dit eHerkenning beïnvloedt.

Tabel 2: De eHerkenning betrouwbaarheidsniveaus

eHerkenning betrouwbaarheidsniveau	Omschrijving
1	Geen of minimale betrouwbaarheid
2	Beperkte betrouwbaarheid
2+	Beperkte tot redelijke betrouwbaarheid
3	Redelijke betrouwbaarheid
4	Hoge betrouwbaarheid

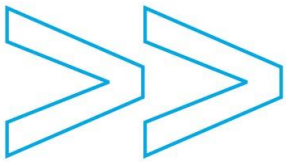
7 Generieke identificatie en authenticatie, doorontwikkeling van eerdere activiteiten in het kader van IDABC. Het raamwerk is vastgelegd in STORK deliverable D2.3 – Quality authenticator scheme, Hoofdstuk 1 (als achtergrond) en Hoofdstuk 2 (daadwerkelijke beschrijving)

2.4 Afsprakenstelsel eHerkenning en ontwerpprincipes

Leidend voor gedrag en werking van netwerk en afsprakenstelsel eHerkenning én de toekomstige ontwikkeling ervan, zijn de volgende uitgangspunten[8] 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.

8 In Bijlage C. Toepassingen uitgangspunten en randvoorwaarden is een overzicht opgenomen van de verwerking van de Uitgangspunten en Randvoorwaarden die vanuit ministerie van EZ aan eHerkenning zijn gesteld.



- 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.

3 Hoe werkt eHerkenning? Het deelnemersperspectief

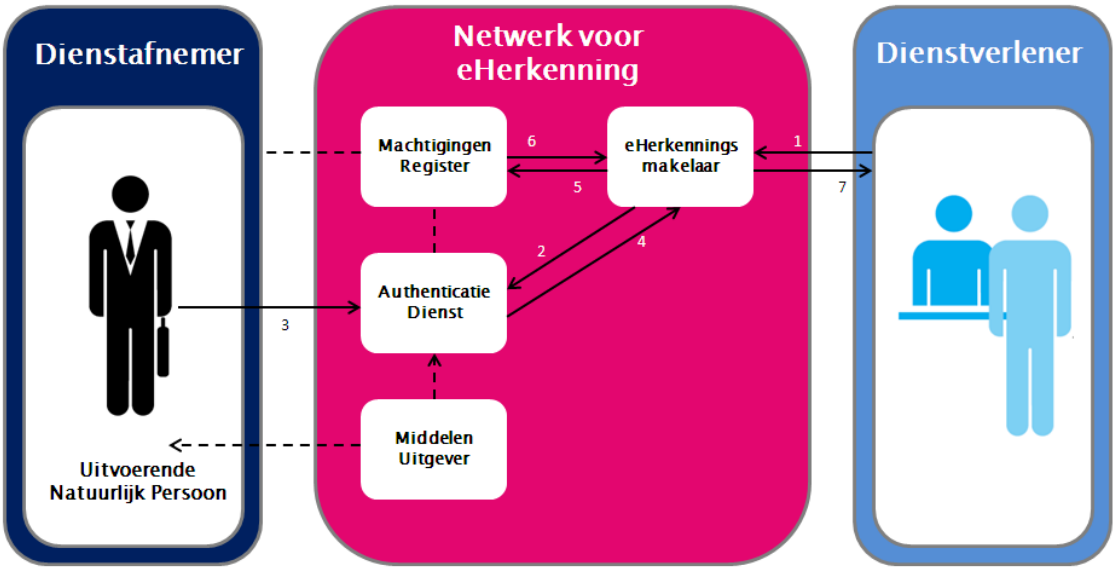
3.1 Inleiding

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 hoofdstuk 2 beschreven gedrag van het netwerk voor de aangesloten gebruikers tot stand komt? Dan wordt ingezoomd op de vier verschillende rollen die eHerkenning in versie 1.7 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 paragraaf 3.5 aan de orde.

Overigens: om rollen te vervullen in het netwerk dient de deelnemer daarop aangesloten te zijn. Hoofdstuk 4 beschrijft welke *eenmalige* werkzaamheden voor het aansluiten van een deelnemer in één of meer rollen nodig zijn. Dit hoofdstuk (3) beschrijft de *continue* werkzaamheden van de rollen.

3.2 Werking van netwerk eHerkenning op hoofdlijnen

De werking van het netwerk eHerkenning is op hoofdlijnen als volgt. Zoals in hoofdstuk 2.2 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 in Figuur 2 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.



Gebruik:

1. Authenticatievraag stellen
2. Kiezen authenticatiedienst
3. Identificeren m.b.v. authenticatiemiddel
4. Bevestigen identiteit uitvoerende natuurlijk persoon
5. Opvragen bevoegdheid, eventueel selecteren vertegenwoordigd bedrijf
6. Verklaren bevoegdheid uitvoerende natuurlijk persoon
7. Verklaren authenticatie dienstafnemer, incl. specifiek pseudoniem uitvoerende natuurlijk persoon op betrouwbaarheidsniveau.

Figuur 2: 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 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.

Tabel 3: Dienstencatalogus – vb

dienst	vereist betrouwbaarheidsniveau
A	niveau 2
B	niveau 3
C	niveau 4

Zie Tabel 3 voor een kleine (zeer vereenvoudigde) voorbeeldinvulling van de dienstencatalogus op een bepaald moment.

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 4 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 Elimam.

Tabel 4: Middelenadministratie – vb

intern pseudoniem	authenticatiemiddel		betrouwbaarheidsniveau
	middeltype	middel-ID	
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. **Error! Reference source not found.** 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

Tabel 5: Machtigingenregister – vb

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

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.

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.

3.3 Deelnemers: rollen en verantwoordelijkheden

Zoals in hoofdstuk 3.3 en Figuur 2 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, voorzover deze verplicht zijn voor alle deelnemers. Voor toetredingseisen wordt verwezen naar het document [Juridisch kader] en voor details over de functionaliteit naar [deel Use Cases].

3.3.1 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.

3.3.2 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 het deel Use Cases.

3.3.3 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 het deel betrouwbaarheidsniveaus.

3.3.4 Verantwoordelijkheden eHerkenningsmakelaar

Een eHerkenningsmakelaar moet aan dienstverleners een gestandaardiseerd koppelvlak leveren waarover eHerkenningsdiensten kunnen worden geïnitieerd en gevraagde verklaringen kunnen worden geleverd. Een eHerkenningsmakelaar moet voor authenticatiediensten en machtigingenregisters tenminste de twee meest recente gestandaardiseerde koppelvlakken ondersteunen zolang dit voor migratie noodzakelijk is.

Een eHerkenningsmakelaar moet 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.

Een eHerkenningsmakelaar moet 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.

Een eHerkenningsmakelaar moet 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.

Een eHerkenningsmakelaar moet 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.

Een eHerkenningsmakelaar moet SSO ondersteunen en daartoe vragen met SSO doorgeven aan een authenticatiedienst en logoutberichten verwerken en doorsturen naar de authenticatiedienst.

3.4 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 hoofdstuk 4 en document [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.

3.5 Werking aanvullende features

3.5.1 Werking aanvullende feature: 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.

3.5.1.1 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.

3.5.1.2 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).

3.5.1.3 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).

3.5.1.4 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.

3.5.2 Werking aanvullende feature: ketenmachtigingen

De vereisten voor het leveren van eHerkenningsdiensten gebaseerd op ketenmachtigingen moeten door eHerkenningsmakelaars als verplichte functionaliteit worden ondersteund (zie § 3.3.4), 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.

3.5.2.1 Verantwoordelijkheden machtigingenregister met ketenmachtigingen

Een machtigingenregister dat ketenmachtigingen kan ondersteunen vult dezelfde verantwoordelijkheden in als een standaard machtigingenregister (zie § 3.3.3) 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[9]. 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 koppelvlakbeschrijving HM – MR).

3.5.3 Werking aanvullende feature: 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.

[9] Bij uitbreiding naar meer schakels moeten de controles aangaande kennisgeving bij substitutie hier worden toegevoegd.

3.5.3.1 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.

4 Hoe aansluiten op eHerkenning?

4.1 Inleiding

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 paragraaf 4.4 toegelicht.

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

4.2 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.

4.2.1 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 op www.eHerkenning.nl openbaar[10].

"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.

4.2.1.1 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

10 Zie www.eherkenning.nl/bedrijven/aanvragen/aanbieders

uitgeeft en beheert toe te treden als deelnemer aan eHerkenning (zie 4.4), 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.

4.2.2 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[11].

4.2.3 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.

11 Dit is hetzelfde overzicht als voor middelenuitgevers, de deelnemers maken zelf de gecombineerde proposities inzake authenticatiemiddelen en machtigingen inzichtelijk.

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 document [Informatiebeveiliging].

4.3 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 document [Koppelvlak HM-DV] is het koppelvlak tussen dienstverlener en eHerkenningsmakelaar technisch beschreven en de specificatie van de dienstencatalogus uitgewerkt.

Na aansluiting op eHerkenning worden (overheids)dienstverleners in de besturing van het afsprakenstelsel betrokken via de stelselraad eHerkenning.

4.3.1 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.

4.4 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 hoofdstuk 3.3 werden deze eisen per rol beschreven. De juridische kant van de benodigde samenwerking en de toetredingseisen worden toegelicht in deel Juridisch kader. Het toetredingsproces wordt uitgewerkt in het document [Operationeel Handboek]

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

4.5 Aansluiten op aanvullende features

4.5.1 Aansluiten op aanvullende feature: 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.

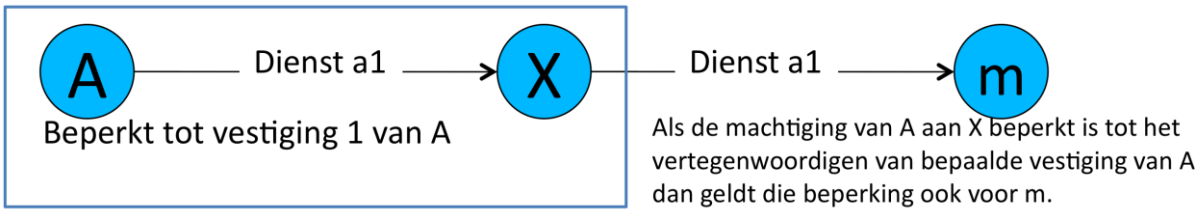
Het is niet toegestaan aan uitvoerend natuurlijk personen of wettelijke vertegenwoordigers vooraf globaal toestemming te vragen voor verstrekken van alle mogelijke attributen. De user consent dient specifiek te zijn voor een bepaald attribuut en mag beperkt zijn tot een bepaalde machtiging. Nadat de 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 paragraaf "Doorlooptijd van mutaties van bevoegdheden" van deel [Betrouwbaarheidsniveaus en registratie-eisen].

4.5.2 Aansluiten op aanvullende feature: 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 § 4.2.

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. Zie Figuur 3.



Figuur 3: Beperking op vestigingsnummer bij ketenmachtiging

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 A. Begrippenlijst

Term	Definitie
Aanvullende feature	Een in het afsprakenstelsel 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.
	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.
	Eigen definitie conform Richtsnoeren CBP
Afspraken-stelsel	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.
	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.
Attribuut-catalogus	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.
	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.
	Analoog aan KPMG[12], Modinis[13], opdrachtformulering Vraagstuk eHerkenning bedrijven en instellingen d.d. 10-1-2008, NTP Authorisation Policy (AP) v1.1. Definitie is tevens analoog aan PKIoverheid[14] alwaar opgemerkt wordt: "In de Wet EH wordt de term "Authentificatie"

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

Term	Definitie
	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."
Authenticatie-verklaring	Een verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een authenticatie die heeft plaatsgevonden in de context van een bepaalde handeling of dienst.
	Eigen definitie
Authenticatie-dienst	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.
Authenticatie-middel	Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.
	Analoog aan KPMG
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.
	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
	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	Zie dienstafnemer
	Eigen definitie

Term	Definitie
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.
	Eigen definitie
Beheer-organisatie	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 vastgestelde nalevingsbeleid.
	Eigen definitie
Beroeps-beoefenaar	Een natuurlijk persoon die een gereglementeerd beroep uitoefent conform EU richtlijn 2005/36/EG (http://ec.europa.eu/internal_market/qualifications/policy_developments/legislation_en.htm)
	Gebaseerd op EU Richtlijn 2005/36/EG
Betrouwbaar-heidsniveau	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).
	Vertaald uit engels van STORK "assurance level" en aangepast aan terminologie afsprakenstelsel[15]
Bevoegdheid	Het recht van een persoon om een handeling te verrichten.
	Eigen definitie
BSN	*Burgerservicenummer*: Persoonlijke identificatie van de Nederlandse overheid voor natuurlijke personen.
	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

15 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.

Term	Definitie
	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).
	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.
	Eigen definitie
Data-minimalisatie	Het zodanig inrichten van een gegevensverwerking dat er zo weinig mogelijk identificerende gegevens bekend hoeven te zijn bij zo weinig mogelijk partijen.
	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.
	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: o.a. gebaseerd op Hrw 2007 en BW deel 3, artikel 15d en BAO artikel 47 lid 1.
Diensten-	Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle

Term	Definitie
catalogus	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.
	Eigen definitie
Dienstverlener	Een partij die elektronische diensten aanbiedt aan dienstafnemers waarvoor eHerkenningsdiensten voorwaardelijk zijn. Dit kan zowel een overheidsdienstverlener als een private dienstverlener zijn.
	Eigen definitie specifiek voor de context van het afsprakenstelsel.
eHerkenning	Onder eHerkenning wordt elektronische herkenning verstaan; zie bij herkenning
	Eigen definitie specifiek voor de context van het afsprakenstelsel
eHerkennings-makelaar	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 (?) ondertekendiensten.
	Eigen definitie
eHerkennings-netwerk	Synoniem voor Netwerk (voor eHerkenning)
	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.
	Eigen definitie specifiek voor de context van het afsprakenstelsel
Geïnformeerde uitdrukkelijke toestemming	Zie User consent.
	Zie User consent
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

Term	Definitie
	voorkomen van niet ingezetenen als gemachtigde. Zo kan ook een buitenlandse natuurlijke persoon gemachtigde zijn.
	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.
	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.
	Eigen definitie
Herkenning	In deze context wordt onder 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.
	Eigen definitie specifiek voor de context van het afsprakenstelsel. Generalisatie van de begrippen authenticatie, bevoegdheid en wilsuiting.
eHerkennings-diensten	Diensten voor herkenning, te weten: authenticatie, controle van bevoegdheden, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.
	Eigen definitie specifiek voor de context van het afsprakenstelsel.
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.
	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.
	Eigen definitie
Identificerend	Een identificerend kenmerk dat bestaat uit cijfers

Term	Definitie
nummer	
	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.
	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.
	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.
	Eigen definitie.
Intern pseudoniem	Pseudoniem dat gedurende een langere periode toegepast wordt en enkel binnen eHerkenning gebruikt wordt zonder een specifiek werkingsdomein.
	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
	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. De Klachten- en geschillencommissie is ingesteld door het Ministerie van EZ, op voordracht van de Stelselraad.
	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 levert het afsprakenstelsel de specificaties (a), het netwerk verzorgt de implementaties (b). Synoniem met Engelse term 'interface'.

Term	Definitie
	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.
	Eigen definitie gebaseerd op Modinis
Machtigingen-register	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 uitvoerend natuurlijk persoon verstrekken van machtigingsverklaringen).
	Eigen definitie
Machtigings-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 machtigingenregister ten behoeve van een bepaalde handeling of dienst.
	Eigen definitie
Middelen-uitgever	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.
	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.
	Eigen definitie overeenkomstig Catalogus Nieuw Handelsregister
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 bedrijven, inclusief de benodigde voorzieningen voor beheer conform het

Term	Definitie
	afsprakenstelsel.
	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.
	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.
	Handelsregisterwet 2007
Onderteken-dienst	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. Scope: In versie 1.7 is de rol ondertekendienst nog niet uitgewerkt maar wordt deze waar relevant wel benoemd.
	Eigen definitie
Overheids-dienstverlener	Een dienstverlener die onderdeel van de Nederlandse overheid is. Voorzover zaken zowel overheidsdienstverleners als private dienstverleners kunnen betreffen wordt gesproken van "dienstverleners".
	Eigen definitie
Partij	Een persoon of samenwerkingsverband die in de context van eHerkenning 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.
	Gebaseerd op Identified Entity (STORK glossary[16]) Party, Principal en System Entity (SAML glossary) en Identifiable Entity (Modinis) en vervolgens specifiek gemaakt voor eHerkenning.
Persoon	Hetzij een natuurlijk persoon hetzij een rechtspersoon.

16 STORK Glossary and Acronyms v6.0

Term	Definitie
	Nota bene: samenwerkingsverbanden zijn verbanden van personen maar zelf geen persoon.
	Generalisatie van de definities natuurlijk persoon en rechtspersoon. Nota bene: www.stelselcatalogus.nl is niet consistent ten aanzien van de vraag of het begrip persoon tevens samenwerkingsverbanden omvat, derhalve is dit in deze begrippenlijst expliciet gemaakt. *Nog checken of deze bewering klopt: persoon is synoniem met rechtssubject, namelijk altijd drager van rechten en verplichtingen*
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.
	PKIoverheid
Privépersoon	Een natuurlijk persoon, echter uitsluitend voor situaties en dienstafnames bij niet-overheidsdienstverleners c.q. In B2C diensten.
	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.
	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.
	Definitie conform Catalogus Basisregistraties
Rol	Één 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.
	Eigen definitie specifiek voor het afsprakenstelsel

Term	Definitie
Service provider	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.
	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 wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel, waardoor een authenticatie van een uitvoerend natuurlijk persoon wordt hergebruikt, waardoor deze utvoerend natuurlijk persoon niet opnieuw hoeft in te loggen.
	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 in wiens context het gebruikt wordt, een dienstafnemerspecifiek pseudoniem is steeds hetzelfde voor de context van één dienstafnemer etc.
	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.
	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.
	Eigen definitie
Uitvoerend natuurlijk persoon	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 betreft dit handelen het afnemen van een dienst bij een dienstverlener.
	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

Term	Definitie
	verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.
	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 koppelvlakspecificaties is beschreven.
	Eigen definitie
Vertegenwoor-digde	De partij die de vertegenwoordiger de bevoegdheid heeft verleend om in naam van eerstgenoemde te handelen.
	Artikel 3:60 lid 1 BW; Analoog aan AP1.1. Zie definitie vertegenwoordiging
Vertegenwoor-digde dienst-afnemer	Dienstafnemer die niet zelf handelt maar zich laat vertegenwoordigen. De vertegenwoordigde dienstafnemer is de eerste partij in een keten van machtigingen.
	Eigen definitie
Vertegenwoor-diger	De partij die bevoegd is om een andere partij (de vertegenwoordigde) te vertegenwoordigen in het verrichten van handelingen met derden.
	Zie definitie vertegenwoordiging
Vertegenwoor-diging (vertegen-woordigen)	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) 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.
	Conform juridische toets prof. A. Mohr
Vestiging	Een vestiging is een onderdeel van een dienstafnemer met een afbakening die in een handelsregister is opgenomen.

Term	Definitie
	Eigen definitie
Wettelijke vertegenwoor-diging	Een vertegenwoordiging 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.
	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.
	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 die de wilsuiting afgeeft op ieder moment nadien geauthenticeerd kan worden.
	Eigen definitie
ZZP-er	Zelfstandige Zonder Personeel. 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.
	Eigen definitie

839

Bijlage B. 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 C. Toepassingen uitgangspunten en randvoorwaarden

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel versie 1.7
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 (§ 3.2 en § 3.3) 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 in versie 1.7 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 § 4.2 en voorbeelden zijn gegeven in het deel 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 (§ 3.3), waaronder deze twee en beschrijft verantwoordelijkheden, functies en eisen uitgesplitst naar deze rollen (§ 4.4). Wat betreft de betrouwbaarheidsniveaus wordt onderscheid gemaakt tussen de toepassing van het Europese STORK raamwerk voor authenticatiemiddelen (zie bijlage D) 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 B.

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel versie 1.7
5. Rollen, rechten en verantwoordelijkheden van partijen moeten nauwkeurig worden beschreven in het afsprakenstelsel.	Deze beschrijving is te vinden in § 3.3. Op basis van de procesbeschrijvingen in deel Operationeel Handboek is vastgelegd welke functionaliteit de verschillende rollen in detail leveren. De verantwoordelijkheden aangaande de beheerorganisatie zijn uitgewerkt in deel 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 versie 1.7 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

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel versie 1.7
	basis van specifieke toestemming van de betrokken natuurlijk persoon – uitgebreidere persoonsgegevens kan leveren. Deze uitbreiding is in 1.7 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 (§ 3.3) 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.

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel versie 1.7
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 eHerkenning voor Bedrijven 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 versie 1.7 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 (§ 3.3).
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	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.

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel versie 1.7
bescherming persoonsgegevens.	
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 B 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

Uitgangspunten en randvoorwaarden	Verwerking in afsprakenstelsel versie 1.7
	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.)

896