Afsprakenstelsel eHerkenning

Betrouwbaarheidsniveaus en registratie-eisen

Versie 1.7

INHOUDSOPGAVE

COLOFON

Auteur	Status
Beheerorganisatie Afsprakenstelsel eHerkenning	Definitief
Project	**Datum**
Afsprakenstelsel eHerkenning	24 april 2013
Organisatie	**Classificatie**
Logius	Openbaar
Titel van het document	**Versie**
Afsprakenstelsel eHerkenning – Betrouwbaarheidsniveaus en registratie-eisen	1.7

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
29/03/10	0.8def		Tbv proef-impl.	Projectbureau
06/09/10	1.0	§ 4.5.2 omgevormd naar los document; omzetting naar structuur STORK D2.3 en doorvoering RFCs 0004, 0005, 0024, 0028, 0029	Definitief	Projectbureau
17/12/10	1.0a	RFCs verwerkt conform besluit Kernteam 6 december	Definitief	Projectbureau
17/06/11	1.1	RFCs verwerkt conform besluit kernteam 31 mei	Definitief	Projectbureau
12/11/11	1.2	RFCs verwerkt conform besluit kernteam 11 oktober	Definitief	Projectbureau
23/12/11	1.3	RFCs verwerkt conform besluit kernteam 13 december	Definitief	Projectbureau
28/04/12	1.4	RFCs verwerkt conform besluit kernteam 20 maart	Definitief	Beheerorganisatie
12/07/12	1.5	RFCs verwerkt conform besluit kernteam 26 juni	Definitief	Beheerorganisatie
01/04/13	1.6	RFC0197, RFC0201, RFC0207 verwerkt	Definitief	Beheerorganisatie
24/04/13	1.7	RFC0188, RFC0200, RFC0204, RFC0210, RFC0211 verwerkt	Definitief	Beheerorganisatie

DISTRIBUTIE

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

GOEDKEURING

Datum	Naam	Versie
24/04/13	Alle RFCs voor versie 1.7 goedgekeurd door tactisch overleg	1.7

1 Inleiding

Dit document maakt deel uit van het afsprakenstelsel eHerkenning. Het kan niet los worden gezien van de andere documenten van het afsprakenstelsel. Voor een algemene introductie op, en een overzicht van alle documenten binnen eHerkenning wordt de lezer van dit document aangeraden eerst het document [eHerkenning – Algemene introductie] te lezen.

1.1 Doel en doelgroep van dit document

Dit document beschrijft de wijze waarop betrouwbaarheidsniveaus binnen eHerkenning gehanteerd worden, het geeft de criteria om authenticatiemiddelen en bevoegdheden te classificeren en gaat in op de wijze waarop dit aansluit op het STORK raamwerk. Het is bedoeld voor deelnemers en dienstverleners.

1.2 Leeswijzer

Het vervolg van dit document ziet er als volgt uit. Na een algemene inleiding (hoofdstuk 2) worden de betrouwbaarheidsniveaus voor authenticatiemiddelen (hoofdstuk 3) en bevoegdheden (hoofdstuk 4) afzonderlijk behandeld. Dit resulteert in een tabel die aangeeft hoe het overkoepelende betrouwbaarheidsniveau van eHerkenning is opgebouwd (hoofdstuk 5).

1.3 Begrippenlijst

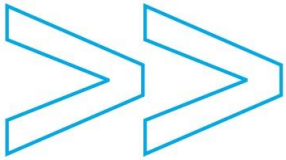
Binnen eHerkenning wordt één begrippenlijst gehanteerd. Zie de bijlage in document [eHerkenning – Algemene introductie]. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, 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.

1.4 Terminologie

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

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

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



1.5 Typografie

Alle begrippen die zijn opgenomen in de begrippenlijst worden vanaf hoofdstuk 2 de eerste keer dat ze voorkomen onderstreept genoteerd, afgezien van kopjes, delen van woorden en de benamingen van processen.

2 Betrouwbaarheidsniveaus eHerkenning

Ten behoeve van het verlenen van eHerkenningsdiensten moeten betrouwbaarheidsniveaus worden gebruikt om de mate van betrouwbaarheid aan te duiden van een authenticatie en bevoegdheidsvastlegging. Het betreft vier vastomschreven betrouwbaarheidsniveaus (zie tabel hieronder). Ieder hoger betrouwbaarheidsniveau stelt ten opzichte van het onderliggende niveau steeds verdergaande eisen aan registratie, beheer en gebruik.

Dienstverleners moeten kenbaar maken welk betrouwbaarheidsniveau minimaal vereist is voor een bepaalde dienst waarvoor zij eHerkenning toepassen. Zij mogen geen specifieke authenticatiemiddelen vereisen of uitsluiten anders dan op grond van dit betrouwbaarheidsniveau. Dit minimale betrouwbaarheidsniveau moet gelden voor het te gebruiken authenticatiemiddel en voor bevoegdheden. Daarbij moet steeds gelden dat "de zwakste schakel telt". Betrouwbaarheidsniveaus moeten downwards compatibel zijn, dat wil zeggen dat op basis van authenticatiemiddelen en bevoegdheden met een hoger betrouwbaarheidsniveau ook verklaringen verstrekt worden wanneer een lager betrouwbaarheidsniveau vereist wordt.

Ten behoeve van interoperabiliteit binnen de Europese Unie past het netwerk voor eHerkenning het STORK raamwerk voor betrouwbaarheidsniveaus toe, dat een schema van "Quality Authentication Assurance" beschrijft. Dit raamwerk definieert betrouwbaarheidsniveaus voor authenticatiemiddelen. Het raamwerk is tevens als vertrekpunt gebruikt voor de classificatie van bevoegdheden. Het afsprakenstelsel zou de verdere ontwikkeling van het raamwerk in kader van STORK 2.0 project, moeten volgen. Wanneer een nieuwe versie van het raamwerk wordt vastgesteld wordt het normale wijzigingsproces gevolgd om te beslissen over toepassing en implementatie daarvan.

In het afsprakenstelsel eHerkenning is sprake van vier betrouwbaarheidsniveaus (tijdelijk zullen er 2 versies van niveau 2 beschikbaar zijn tijdens de migratieperiode).

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

Deze overkoepelende eHerkennings-betrouwbaarheidsniveaus (EH) moeten tot stand komen door individuele beoordeling van de betrouwbaarheid van de in dit hoofdstuk gedefinieerde elementen aangaande bevoegdheden en authenticatiemiddelen. De uiteindelijke waardering van het betrouwbaarheidsniveau mag

1 Eerder is dit niveau NL genoemd, omdat het in tegenstelling tot de andere niveaus afwijkt van het STORK raamwerk. Dit niveau zal worden uitgefaseerd na publicatie van STORK versie 1.7. In deze versie zijn de specifieke eisen voor dit niveau alleen opgenomen in de samenvattende tabel in hoofdstuk 5. Zie aldaar.

niet hoger zijn dan de laagste waardering per deelaspect volgens het principe "een keten is zo sterk als de zwakste schakel". Dit geheel resulteert in de samenvattende tabel in hoofdstuk 5.

3 Betrouwbaarheidsniveaus van authenticatiemiddelen

Voor authenticatiemiddelen wordt het STORK raamwerk gevolgd. De elementen op basis waarvan de betrouwbaarheid van authenticatiemiddelen beoordeeld worden zijn in twee categorieën verdeeld: de eisen aan de registratiefase en de eisen aan de elektronische authenticatiefase.

De registratiefase bepaalt de eisen die gesteld worden wanneer een dienstafnemer wil aansluiten op eHerkenning en daartoe authenticatiemiddelen aanvraagt. Het betreft de waarborgen in het proces van registratie van de uitvoerend natuurlijk persoon tot en met de uitgifte van een authenticatiemiddel aan deze uitvoerend natuurlijk persoon. Tevens volgt het betrouwbaarheidsniveau uit de mate waarin de kwaliteit van de processen en onderliggende mechanismen zijn vastgesteld bij de partij die het authenticatiemiddel uitgeeft: aan te duiden als "de kwaliteit van de organisatie" (zoals bijvoorbeeld beschreven in ETSI TS 101 456 voor betrouwbaarheidsniveau 4). De elementen die in deze categorie beoordeeld worden zijn:

- Identificatieprocedure bij middelenuitgifte
- Proces van middelenuitgifte
- Partij die het authenticatiemiddel uitgeeft

De elektronische authenticatiefase betreft het technisch deel van de betrouwbaarheidsniveaus. Het gaat daarbij om het authenticatiemiddel zelf én de wijze waarop het tijdens het gebruik functioneert. De elementen die in deze categorie beoordeeld worden zijn:

- Type en robuustheid van het authenticatiemiddel
- Zekerheid van het authenticatiemechanisme

De maatregelen die zijn getroffen om het authenticatiemechanisme op afstand c.q. via internet ("zekerheid van het authenticatiemechanisme") betrouwbaar te laten functioneren worden beoordeeld op de bescherming tegen identiteitsdiefstal. Dit betreft:

1. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden.
2. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen.
3. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller.
4. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen.
5. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt.

Voor de gedetailleerde criteria die betrekking hebben op authenticatiemiddelen en de authenticatiedienst wordt verwezen naar de betrouwbaarheidsniveaus[2] met de corresponderende nummering in het STORK-

2 STORK spreekt van assurance levels

document[3]. In Bijlage D is per betrouwbaarheidsniveau een Nederlandstalige toelichting bij de STORK vereisten opgenomen. In geval van eventuele verschillen tussen deze bijlage en het brondocument behorende bij het raamwerk moet de brondocumentatie van het raamwerk worden toegepast.

Voor betrouwbaarheidsniveau 2 wordt onder de gebruikelijke richtlijnen voor sterke wachtwoorden tenminste die richtlijnen verstaan welke voor DigiD burger gehanteerd worden (zie Bijlage D).

In aanvulling op het STORK raamwerk worden expliciete eisen gesteld aan de maximale doorlooptijd van het effectueren van een intrekkingsverzoek voor authenticatiemiddelen, te weten:

Eis per niveau	Doorlooptijd effectueren intrekkingsverzoek
Betrouwbaarheidsniveau 1	geen eisen
Betrouwbaarheidsniveau 2/2+	elektronisch: per direct, niet-elektronisch: 2 werkdagen
Betrouwbaarheidsniveau 3	elektronisch: per direct, niet-elektronisch: 1 werkdag
Betrouwbaarheidsniveau 4	voor middelen moet PKI-Overheid worden gevolgd

T.a.v. de doorlooptijden van uitgifteprocessen van authenticatiemiddelen en registratieprocessen van bevoegdheden worden geen eisen gesteld.

3 Document D2.3 - Quality authenticator scheme versie 1.7, paragraaf 2.3 en 2.4, te vinden op http://www.eid-stork.eu, onder STORK materials, deliverables approved/public.

4 Betrouwbaarheidsniveaus van bevoegdheden

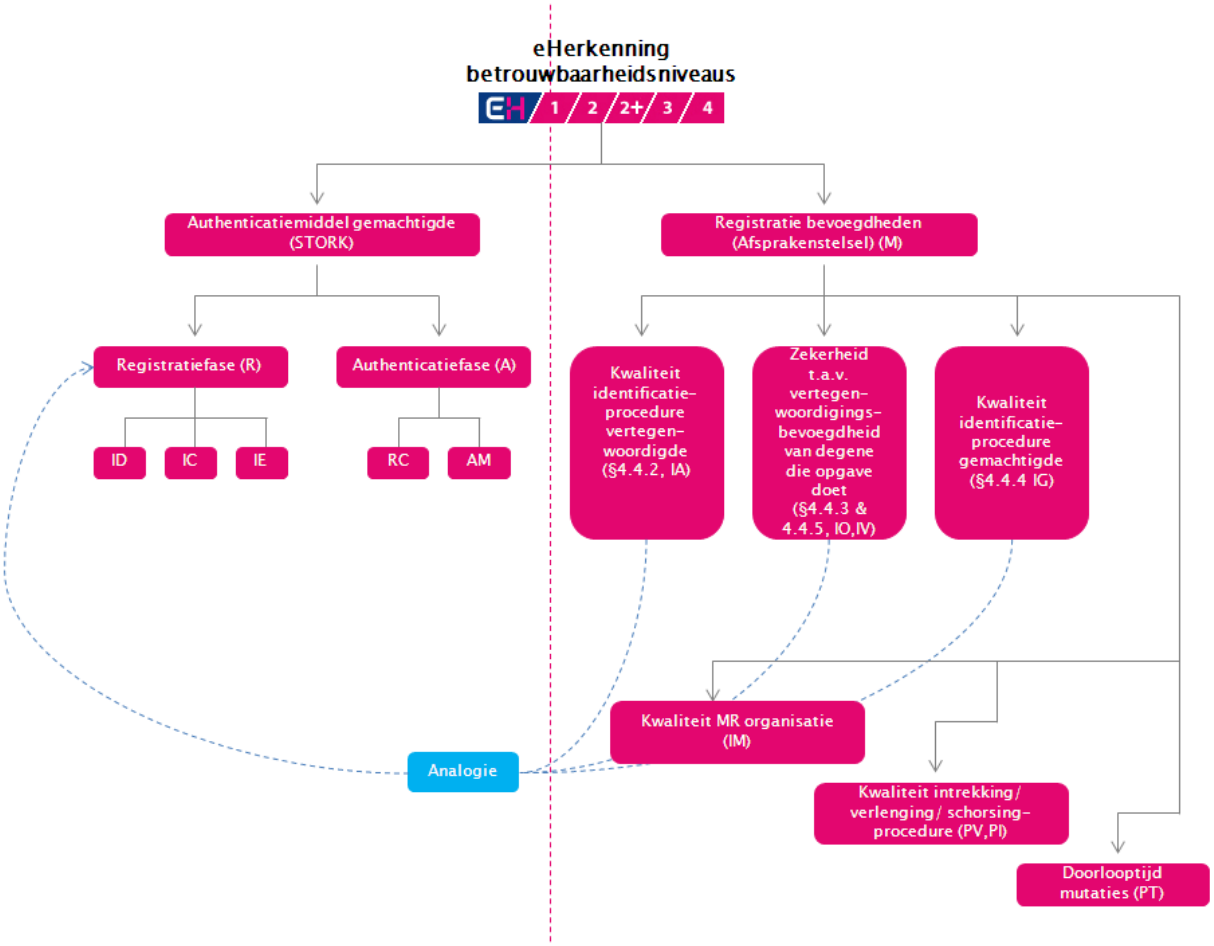
4.1 Toepassing STORK raamwerk op bevoegdheden

Onderstaand wordt uitgewerkt hoe met het STORK raamwerk als vertrekpunt de betrouwbaarheidsniveaus voor bevoegdheden moeten worden geclassificeerd. Alle te beoordelen elementen hebben betrekking op het registratieproces van bevoegdheden. Het betrouwbaarheidsniveau van bevoegdheden wordt niet afhankelijk gemaakt van de elementen die als analogie van gebruik c.q. authenticatiefase voor authenticatiemiddelen gelden. Dit omdat het afsprakenstelsel voor de technische integriteit, de ondertekening en de transportbeveiliging van de verklaringen waarmee informatie over bevoegdheden tijdens gebruik wordt gecommuniceerd in alle gevallen conform het hoogste betrouwbaarheidsniveau zijn vereist (zie [Koppelvlakspecificaties]).

De volgende elementen van de registratie van bevoegdheden worden beoordeeld:

- Kwaliteit identificatieprocedure (vertegenwoordigde) dienstafnemer(vgl. STORK IDx)
- Kwaliteit identificatieprocedure uitvoerend natuurlijk persoon (vgl. STORK IDx)
- Kwaliteit identificatieprocedure intermediaire partij, indien van toepassing (vgl. STORK IDx)
- Zekerheid omtrent vertegenwoordigingsbevoegdheid van degene die de opgave doet (vgl. STORK IDx subcriterium iii). Dit vereist beoordeling van de identificatieprocedure van deze opgever evenals beoordeling van de vertegenwoordigingsbevoegdheid namens de vertegenwoordigde.
- Kwaliteit van de organisatie die het machtigingenregister beheert (vgl. STORK IEx)
- Geldigheidsduur van bevoegdheden
- Kwaliteit van de verlengingsprocedure voor bevoegdheden
- Kwaliteit van de intrekkingsprocedure voor bevoegdheden
- Kwaliteit van de schorsingsprocedure voor bevoegdheden
- Doorlooptijd van mutaties van bevoegdheden

Onderstaande figuur toont deze elementen naast de voor authenticatiemiddelen geldende elementen van STORK.



4.2 *Het registratieproces van bevoegdheden*

Onder het registreren van bevoegdheden in een machtigingenregister wordt verstaan het vastleggen van de bevoegdheid die uit een machtiging blijkt. Wat een machtiging in juridische zin is, is toegelicht in paragraaf 3.3 van deel [Juridisch Kader]. Uitgangspunt is dat deze machtiging los van de registratie in het machtigingenregister bestaat en dat het registratieproces gaat om het correct – volgens de vereisten van een bepaald betrouwbaarheidsniveau – vastleggen van gegevens over die machtiging. Voor de betrouwbaarheid is degene die de opgave doet en de vraag of deze vertegenwoordigingsbevoegd is evenzeer belangrijk als het correct vastleggen van de gegevens over de machtiging. Dit omvat ook de situatie van een wettelijke vertegenwoordiger die zelf als uitvoerend natuurlijke persoon optreedt en dit omvat ook de bevoegdheid van de eigenaar van een éénmanszaak die zelf als uitvoerend natuurlijk persoon optreedt.

Benodigde gegevens voor het registreren van een machtiging of bevoegdheid mogen zowel elektronisch als niet-elektronisch aangeleverd worden aan het machtigingenregister. Het registreren van een bevoegdheid mag worden gedaan op basis van een ondertekend geschrift (een onderhandse akte).

Het machtigingenregister moet twee functies ondersteunen:

1. Het registreren van een beheerder.
2. Reguliere registratie van bevoegdheden (i.c. beheer van bevoegdheden) door een beheerder.

De beheerder moet hetzij zelf een volledig bevoegde wettelijke vertegenwoordiger zijn van de betreffende dienstafnemer hetzij worden geregistreerd door de wettelijke vertegenwoordiger(s). De eisen aan dit registratieproces variëren per betrouwbaarheidsniveau. Machtigingen met een betrouwbaarheidsniveau dat hoger is dan datgene waarmee een beheerder wordt geregistreerd mogen niet door die beheerder worden geregistreerd noch beheerd. Iedere dienstafnemer mag meer dan één beheerder aanmelden.

Er zijn twee methoden op basis waarvan de authenticatie van de beheerder mag worden uitgevoerd voordat de beheerder toegang krijgt tot het machtigingenregister. Ten eerste mag een machtigingenregister een eigen voorziening hebben voor authenticatie van een beheerder. Ten tweede mag een machtigingenregister gebruik maken van de authenticatiedienst van het netwerk voor eHerkenning.

Tenslotte gelden nog een aantal verdere eisen: Een deelnemer die een machtigingenregister exploiteert mag niet het beheer uitvoeren van bevoegdheden die door een dienstafnemer zijn verleend aan deze deelnemer. Naast de specificatie van de vereisten per betrouwbaarheidsniveau voor bevoegdheden, moet het machtigingenregister zorg dragen voor de betrouwbare koppeling tussen de bevoegdheid en de identificerende kenmerken. Indien het een bevoegdheid betreft die aan een authenticatiemiddel van een natuurlijk persoon gekoppeld is dan betreft dit het intern pseudoniem van de uitvoerend natuurlijk persoon. Een machtigingsverlening mag als door de gemachtigde geaccepteerd beschouwd worden zodra deze de bevoegdheid voor de eerste maal gebruikt.

- De geldigheid van de registratie van een bevoegdheid moet beperkt worden tot de opgegeven geldigheidsduur met een maximum van 5 jaar.
- Bij een registratie of mutatie (wijzigen, intrekken) van een bevoegdheid moet het machtigingenregister het resultaat van de registratie of mutatie (strekking, aard, duur en gemachtigde) bevestigen aan degene die de opgave gedaan heeft. Beheerders moeten steeds alle geregistreerde machtigingen kunnen inzien.

4.3 De inhoud van een bevoegdheid

Bij een registratie van een bevoegdheid moeten de volgende gegevens verstrekt worden:

1. Identificerende kenmerken van de vertegenwoordigde.
2. Identificerende kenmerken van degene(n) die de opgave van de bevoegdheid doet (de beheerder, een wettelijk vertegenwoordiger die zelf direct als beheerder optreedt of een wettelijke vertegenwoordiger die een beheerder opgeeft (op betrouwbaarheidsniveau 1 bij de score IO1 vervallen deze gegevens).
3. Identificerende kenmerken van de gemachtigde.
4. Strekking van de bevoegdheid: de afbakening van diensten en handelingen die de gemachtigde namens de vertegenwoordigde bevoegd is af te nemen of uit te voeren. De bevoegdheid kan afgebakend zijn tot een bevoegdheid 'voor derden', in het geval van een bevoegdheid verstrekt door een intermediaire partij. De bevoegdheid kan afgebakend worden naar een of meerdere vestigingen van de dienstafnemer. Deze diensten zijn gekoppeld aan de dienstencatalogus.
   N.B. Voor betrouwbaarheidsniveau EH1 is altijd sprake van een algemene bevoegdheid voor alle diensten op dat betrouwbaarheidsniveau. Ook bij registratie van een willekeurige bevoegdheid op betrouwbaarheidsniveau EH2, EH3, en EH4 geldt dat gemachtigde automatisch alle diensten op betrouwbaarheidsniveau EH1 kan afnemen.

5. Aard van de bevoegdheid: de kenmerken die van toepassing zijn op de bevoegdheid, zoals het recht van substitutie en het zelfstandig handelen conform de bevoegdheid.
   N.B. 2 Ketenmachtigingen waarbij substitutie op grond van artikel 3:64 BW niet expliciet aan vertegenwoordigde gemeld hoeft te worden zijn niet toegestaan. De machtiging aan de uitvoerende natuurlijk persoon moet bij ketenmachtigingen tenminste betrouwbaarheidsniveau EH2 hebben.
6. Ingangsdatum en geldigheidsduur van de bevoegdheid

Dit geldt zowel voor de bevoegdheid van de beheerder als voor reguliere bevoegdheden. Bij een registratie van een bevoegdheid mag een beperking van de strekking tot een of meer vestigingen van de vertegenwoordigde namens welke de bevoegdheid geldt, worden opgegeven. Voor ketenmachtigingen kan deze beperking alleen voor de vertegenwoordigde dienstafnemer worden vastgelegd en niet voor intermediaire partijen.

De ten aanzien van bevoegdheden geregistreerde gegevens mogen niet worden verstrekt anders dan voorzover en conform de in het afsprakenstelsel gespecificeerde berichten.

Aan een beheerder en bij het ontbreken van een beheerder aan alle andere gemachtigden voor dezelfde dienstafnemer mogen gegevens getoond worden die noodzakelijk zijn om aan te duiden welke gemachtigden op welke betrouwbaarheidsniveaus voor de betreffende dienstafnemer bestaan. Het is de verantwoordelijkheid van de dienstafnemer om te zorgen voor toestemming voor het gebruiken en inzien van de persoonsgegevens van de gemachtigde ten behoeve van dergelijke functies. Tijdens het aanvraagproces moet toestemming gegeven worden aan de deelnemer om voor dit doel aan anderen binnen dezelfde dienstafnemer persoonsgegevens te tonen.

In het geval van ketenmachtigingen is het machtigingsregister zelf verantwoordelijk om alle beperkingen die in het kader van gebruik van de machtiging gelden vast te leggen. Indien ketenmachtigingen over meerdere machtigingenregisters verspreid zijn kan dit betekenen dat informatie uit andere registers moet worden overgenomen of bij gebruik aan de uitvoerende natuurlijk persoon gevraagd moet worden. Dit betreft met name het machtigingsregister waarin een volgende schakel geverifieerd kan worden en de mogelijkheid om de vertegenwoordigde dienstafnemers waarvoor een machtiging in kader van een keten benut mag worden aan te duiden.

4.4 Vereisten betrouwbaarheidsaspect

De vereisten worden weergegeven op dezelfde wijze als in de STORK standaard. Per aspect volgt daaruit een bepaalde score. Deze scores zijn aangeduid met twee letters en een volgnummer. Hoe hoger de betrouwbaarheid op dat aspect, hoe hoger het nummer. Een gesloten bolletje geeft aan dat indien aan de betreffende omschrijving (regel) voldaan wordt die score (kolom) geldt. Eventuele open bolletjes daaraan voorafgaand duiden aan dat bij de hogere score ook voldaan is aan de eisen voor iedere lagere score. Indien per kolom van boven naar beneden gezocht wordt welk criterium voor betreffende score geldt dan wordt dat gevonden door de regels bij de gesloten bolletjes te nemen. Let wel: in sommige gevallen kan op twee verschillende manieren gekomen worden tot dezelfde score (zoals hieronder voor IO2 zowel b als c voldoet).

De eisen worden in paragraaf 4.4 beschreven voor de eerste registratie waarbij nog geen beheerder is aangesteld. Deze eisen gelden ook in de situatie van een eerste registratie van een wettelijke vertegenwoordiger die voor zichzelf eHerkenning aanvraagt.

In paragraaf 4.5 wordt beschreven welke alternatieven bestaan bij registratie door een eerder aangestelde beheerder of voor het geval van een wettelijke vertegenwoordiger die reeds een eHerkenningsmiddel bezit.

4.4.1 Detailvereisten

Enkele controles komen op meerdere plekken in de eisen voor. Hieronder wordt aangegeven hoe deze in detail uitgevoerd moeten worden:

[i] Verificatie in een handelsregister:

Verificatie in een handelsregister vereist dat daadwerkelijk online in een handelsregister gekeken wordt naar de actuele situatie op moment van registratie. Indien gevraagd wordt naar een al dan niet origineel of gewaarmerkt uittreksel dan dient deze inzage aanvullend gedaan te worden tenzij dit uittreksel minder dan 5 dagen oud is (de wettelijke termijn voor doorgeven wijzigingen aan Handelsregister). De verificatie moet zodanig worden uitgevoerd dat zowel de identificerende nummers, de naam (handelsnaam of statutaire naam) als één vestigingsadres overeenkomen. Het resultaat van deze toets moet voor de duur van tenminste 7 jaar worden gearchiveerd.

[ii] Validatie elektronische handtekeningen:

Het machtigingenregister moet de elektronische handtekening valideren aan de hand van de gehele certificaatketen en actuele intrekkingsinformatie of in geval van een niet PKI gebaseerde handtekening een validatie uitvoeren met vergelijkbare kwaliteit. De gegevens aangaande deze controle moeten worden gearchiveerd voor de duur van tenminste 7 jaar.

[iii] Archivering van controles:

Gegevens over de volgende controles ZOUDEN voor betrouwbaarheidsniveau 2 en hoger gearchiveerd MOETEN worden voor de duur van tenminste 7 jaar:

- Controle van natte handtekening onder een registratieformulier ten opzichte van meegezonden (afgeschermde) kopie WID-document. Hierbij ZOU tevens het documentnummer en -type MOETEN worden gearchiveerd. Let op: een afgeschermde kopie WID-document (waarbij de bijzondere persoonsgegevens, te weten, pasfoto, BSN en nationaliteit, zijn afgeschermd) MAG alleen bij niveau 3 of hoger worden gearchiveerd. Een niet-afgeschermde kopie WID-document MAG alleen bij niveau 4 worden gearchiveerd.
- Controle van ter plekke geplaatste natte handtekening ten opzichte van fysiek getoond origineel WID-document bij fysiek verschijnen. Hierbij moet tevens het documentnummer worden gearchiveerd. Een afgeschermde kopie WID-document MAG alleen bij niveau 3 of hoger worden gearchiveerd. Een niet afgeschermde kopie WID-document MAG alleen bij niveau 4 worden gearchiveerd.
- Controles in een handelsregister.
- Controles op basis van een banktransactie.
- Controles in het register van gestolen en vermiste WID-documenten.
- Validaties van elektronische handtekeningen
- Controles van authenticatie in elektronische registratieprocessen

- Formulieren of elektronische berichten waarin identificerende kenmerken ten behoeve van de registraties worden aangeleverd, inclusief alle verplichte bijlagen.

[iv] Identificatie van beroepsbeoefenaren:

Een beroepsbeoefenaar die zich als dienstafnemer wil laten vertegenwoordigen en dus een machtiging wil laten registreren moet daartoe geïdentificeerd worden met een identificerend kenmerk horend bij de beroepsgroep. Dit gebeurt door het raadplegen van een zgn. beroepsregister voor die beroepsgroep. Dit register wordt bijgehouden door een orgaan dat daartoe door de beroepsgroep is aangewezen.

Waar bovenstaande detailvereisten van toepassing zijn is dit gemarkeerd met [i], [ii], [iii] resp. [iv].

Alle deelnemers MOETEN ervoor zorgdragen dat zij die persoonsgegevens verwerken die proportioneel zijn gelet op het doel – de vaststelling en verificatie van de identiteit op verschillende betrouwbaarheidsniveaus. Deelnemers MOGEN meer of minder persoonsgegevens verwerken dan hieronder als richtlijn is opgenomen, in dat geval MOETEN zij de noodzaak hiervoor hebben vastgelegd in hun procesbeschrijving. De Deelnemer MOET zorgdragen voor verwerking van de persoonsgegevens in overeenstemming met het bepaalde in de Wet bescherming persoonsgegevens.

4.4.2 Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)

Vereisten (IA = Identificatie dienstAfnemer)	IA0	IA1	IA2
a. De opgave van de identificerende kenmerken van de dienstafnemer mogen zonder verificatie worden overgenomen.	○	●	
b. De aangeleverde gegevens moeten de vertegenwoordigde dienstafnemer uniek identificeren en mogen gebaseerd zijn op openbare gegevens. Deze gegevens moeten geverifieerd worden in een handelsregister [i] of een beroepsregister [iv]. Het adres mag hetzelfde zijn als gebruikt voor verificatie IV1. Indien de strekking van de machtiging beperkt wordt tot een vestiging dan moet ten opzichte van het HR gecontroleerd worden dat het opgegeven vestigingsnummer een actuele vestiging van de betreffende dienstafnemer betreft.	○	○	●

Voor de identificatie van de vertegenwoordigde worden geen IA3 of IA4 geformuleerd. Naar analogie van STORK geldt dat de zwaardere vormen van identificatie het aanleveren van een gegeven dat alleen bij de te identificeren persoon bekend is vereisen of het fysiek verschijnen van die persoon. Voor een bedrijf worden deze eisen toegepast op degene die opgave doet, zie volgende paragraaf.

4.4.3 Kwaliteit identificatieprocedure voor degene die de opgave doet

Degene die de opgave doet moet de dienstafnemer vertegenwoordigen. Ook kan het voorkomen dat een wettelijke vertegenwoordiger zijn eigen bevoegdheid in het machtigingenregister laat vastleggen, in dat geval zijn wettelijke vertegenwoordiger, degene die opgave doet en de gemachtigde dezelfde persoon en vindt uiteraard slechts één identificatieprocedure plaats. Uitvoering van dit aspect kan niet los gezien worden van de identificatie van het bedrijf en de zekerheid van de associatie met het bedrijf omdat deze

beide afhankelijk zijn van degene die de opgave doet. In de praktijk gaat het om de controle op een handelsregister en de aanvullende verificaties die (voor de hogere niveaus) op dezelfde gegevens worden uitgevoerd. De eisen aan de identificatie van degene die opgave doet zijn zwaarder of tenminste even zwaar als de eisen aan de identificatie van de gemachtigde, immers de gegevens van de laatste zijn afhankelijk van de betrouwbare identificatie van de eerste. Indien het dezelfde persoon betreft gelden uiteraard de zwaarste eisen uit IO en IG.

Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
a. Geen controle van de identificatie van degene die opgave doet.	●			
b. Niet elektronische opgave. Uniek identificerende kenmerken van de wettelijke vertegenwoordiger MOETEN worden vastgelegd. De opgave ZOU ondertekend MOETEN worden door de wettelijke vertegenwoordiger met diens natte handtekening en een (afgeschermde) kopie van zijn WID-document MOET worden bijgesloten. Het machtigingenregister MOET de natte handtekening controleren aan de hand van de (afgeschermde) kopie van het WID-document [iii][4]. Het machtigingenregister ZOU de (afgeschermde) kopie WID-document NIET MOETEN opslaan.	○	●		
c. Elektronische opgave (zonder reeds in bezit van eHerkenningsmiddel te zijn). Evenals (b) MOETEN uniek identificerende kenmerken van de wettelijke vertegenwoordiger worden vastgelegd. Met de opgave ZOUDEN een scan van door wettelijke vertegenwoordiger ondertekend formulier en een scan van diens (afgeschermde) WID-document MOETEN worden meegezonden. Het machtigingenregister MOET controleren dat deze twee gescande handtekeningen overeenkomen. Indien het bericht ondertekend wordt met een PKIoverheid services certificaat [ii] op naam van de tenminste op IA2 geïdentificeerde dienstafnemer dan vervangt dit verzending en controle van gescande stukken. De (afgeschermde) scan ZOU NIET MOETEN worden opgeslagen [iii].	○	●		
d. Niet elektronische opgave. Evenals (b) MOETEN uniek identificerende kenmerken van de wettelijke vertegenwoordiger worden vastgelegd en de ondertekening gecontroleerd ten opzichte van meegezonden (afgeschermde)	○	○	●	

4 Eisen aan degene die opgave doet identiek aan eisen voor middelenuitgifte ID2: i.a, ii.b, iii.b.

Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
kopie. Eén van beide volgende aanvullende controles ZOU MOETEN worden uitgevoerd[5]: • De geldigheid van het kopie WID-document MOET worden geverifieerd ten opzichte van een register van gestolen en vermiste documenten (in tegenstelling tot c mag ondertekende formulier niet door scan vervangen worden). • Een succesvolle banktransactie MOET worden uitgevoerd vanuit een bankrekening die oorspronkelijk alleen geopend kan zijn op basis van het tonen van een fysiek WID-document en waar de tennaamstelling van de bankrekening gerelateerd is aan dezelfde persoon als degene die geïdentificeerd wordt in de aangeleverde kopie van het kopie WID-document. Kopie WID-document MAG alleen in afgeschermde vorm worden opgeslagen [iii].				
e. Identificerende kenmerken als bovenstaande waarbij de wettelijke vertegenwoordiger fysiek verschijnt (of bezocht wordt) en waarbij zijn ter plekke gezette handtekening gecheckt wordt ten opzichte van zijn originele WID-document. Als alternatief mag ook een gevolmachtigde fysiek verschijnen, mits een schriftelijke ondertekende volmacht van een wettelijke vertegenwoordiger en diens kopie WID-document overlegd en gecontroleerd wordt; deze gevolmachtigde tekent ter plekke en diens handtekening wordt geverifieerd ten opzichte van zijn eigen origineel WID-document. Kopieën van WID-documenten MOGEN alleen in afgeschermde vorm worden opgeslagen [iii].	○	○	●	
f. De wettelijke vertegenwoordiger verschijnt fysiek. Evenals (b) moeten uniek identificerende kenmerken van de wettelijke vertegenwoordiger worden vastgelegd. Deze tekent ter plekke met zijn natte handtekening die geverifieerd wordt ten opzichte van zijn origineel WID-document [iii][6]. Gelet op de noodzaak voor een betrouwbare en achteraf verifieerbare controle van	○	○	○	●

5 Eisen aan degene die opgave doet identiek aan eisen voor middelenuitgifte ID3.

6 Eisen aan degene die opgave doet identiek aan eisen voor middelenuitgifte ID4.

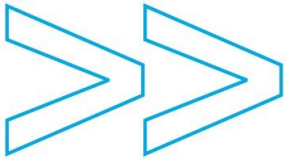
Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
de identiteit ZOU op dit niveau een kopie WID-document MOETEN worden opgeslagen, die conform STORK-eisen een handtekening en pasfoto bevat.				

4.4.4 Kwaliteit identificatieprocedure gemachtigde natuurlijk persoon

De identificatie van de gemachtigde natuurlijk persoon kan gebaseerd zijn op het feit dat aanvraag van een authenticatiemiddel in een en hetzelfde proces plaatsvindt. De vereiste bewijsstukken hoeven in dat geval slechts één keer te worden verstrekt. Het STORK niveau waarop het authenticatiemiddel mag worden uitgegeven moet tenminste even hoog te zijn als het EH-betrouwbaarheidsniveau dat aan de machtiging wordt toegekend.

Indien sprake is van gescheiden processen voor middelenuitgifte en registratie van machtigingen dan moeten vereiste bewijsstukken opnieuw worden verstrekt.

Vereisten (IG = Identificatie Gemachtigde natuurlijk persoon)	IG1	IG2	IG3	IG4
a. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 1 en MAG worden geïntegreerd in dezelfde procesgang. Alleen de volledigheid van de opgave MOET worden geverifieerd. Er vindt geen validatie plaats van de identiteit van de gemachtigde natuurlijk persoon.	●			
b. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 2 en MAG worden geïntegreerd in dezelfde procesgang. Uniek identificerende kenmerken van de gemachtigde natuurlijk persoon MOETEN worden vastgelegd. Een (afgeschermde) kopie van het WID-document van de gemachtigde ZOU MOETEN worden bijgesloten maar ZOU NIET MOETEN worden opgeslagen door machtigingenregister.	○	●		
c. Als bovenstaande (b) met elektronische verzending van gescand (afgeschermd) WID-document of waarbij de gemachtigde een persoonlijke banktransactie uitvoert waarvan de tennaamstelling overeenkomt met de identificerende kenmerken.	○	●		



Vereisten (IG = Identificatie Gemachtigde natuurlijk persoon)	IG1	IG2	IG3	IG4
d. Als bovenstaande (b) waarbij in plaats van de (afgeschermde) kopie WID dezelfde wettelijke vertegenwoordiger die de opgave doet en gecontroleerd is conform tenminste IO2 in staat voor de identificatie van de gemachtigden en de daartoe aangeleverde identificerende kenmerken. Deze wettelijke vertegenwoordiger MOET een andere persoon zijn dan de gemachtigde. Consequentie is dat de uitgifte van de middelen via deze wettelijke vertegenwoordiger MOET (zijn) verlopen opdat deze degene is die de gemachtigde fysiek identificeert. Indien het een opgave betreft aangaande reeds uitgegeven middelen dan MOET de opgave hetzij een gedeeld geheim aangaande ieder afzonderlijk middel omvatten, hetzij de volledige set van uniek makende persoonsgegevens aangaande de gemachtigde die houder is van het authenticatiemiddel bevatten. Nota bene: het gedeelde geheim MAG op meerdere manieren worden gerealiseerd, bijvoorbeeld door dit bij initiële uitgifte van middelen te verstrekken of door het in dit proces aan wettelijke vertegenwoordiger te verstrekken die het dan aan de bij hem bekende gemachtigde verstrekt waarna deze de machtiging online activeert met zijn authenticatiemiddel.	○	●		
e. Als voorgaande (d) indien de wettelijke vertegenwoordiger die de opgave doet ervoor instaat dat gecontroleerd is conform tenminste IO3. Afgeschermde kopie WID-document MAG worden opgeslagen.	○	○	●	
f. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 3 en MAG worden geïntegreerd in dezelfde procesgang. Als in (b) geldt dat uniek identificerende kenmerken van de gemachtigde MOETEN worden vastgelegd en (afgeschermde) kopie of scan van het WID-document van de gemachtigde ZOU MOETEN worden bijgesloten. De geldigheid van deze kopie MOET worden gecontroleerd ten opzichte van een register van gestolen en vermiste identiteitsdocumenten of er MOET voordat de machtiging geactiveerd wordt door de gemachtigde een succesvolle banktransactie worden uitgevoerd vanuit een bankrekening die oorspronkelijk alleen geopend kan zijn op basis van het tonen van een fysiek WID-document en waar de tenaamstelling van de bankrekening gerelateerd is aan dezelfde persoon als degene die geïdentificeerd wordt in de aangeleverde (afgeschermde) kopie van het overheidsidentiteitsdocument. Afgeschermde kopie WID-document MAG worden opgeslagen.	○	○	●	

Vereisten (IG = Identificatie Gemachtigde natuurlijk persoon)	IG1	IG2	IG3	IG4
g. MOET voldoen aan eisen gesteld voor middelenuitgifte conform STORK niveau 4 en MAG worden geïntegreerd in dezelfde procesgang. Als bovenstaande (b) waarbij de identificatie van de gemachtigde wordt overgenomen uit de opgave die de vorm heeft van een onderhandse akte, door degene die opgave doet[7] ondertekend met een authenticatiemiddel met betrouwbaarheidsniveau 4 of een natte handtekening. Kopie WID-document ZOU MOETEN worden opgeslagen.	○	○	○	●

4.4.5 Kwaliteit identificatieprocedure gemachtigde rechtspersoon

Op de identificatieprocedure van de intermediaire partij (de gemachtigde rechtspersoon) zijn dezelfde eisen van toepassing als in 4.4.2 Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer).

Vereisten (IR = Identificatie gemachtigde Rechtspersoon)	IR0	IR1	IR2
a. De opgave van de identificerende kenmerken van de intermediaire partij mogen zonder verificatie worden overgenomen.	○	●	
b. De aangeleverde gegevens moeten de intermediaire partij uniek identificeren en mogen gebaseerd zijn op openbare gegevens. Deze gegevens moeten geverifieerd worden in een handelsregister [i]. Het adres mag hetzelfde zijn als gebruikt voor verificatie IV1. De strekking van de machtiging aan een intermediaire partij kan niet beperkt wordt tot een vestiging.	○	○	●

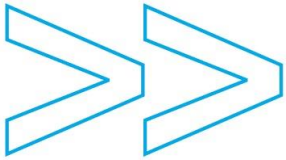
Voor de identificatie van de intermediaire partij worden geen IR3 of IR4 geformuleerd. Naar analogie van STORK geldt dat de zwaardere vormen van identificatie het aanleveren van een gegeven dat alleen bij de te identificeren persoon bekend is vereisen of het fysiek verschijnen van die persoon. Voor een bedrijf worden deze eisen toegepast op degene die opgave doet, zie vorige paragraaf.

4.4.6 Zekerheid associatie met de vertegenwoordigde dienstafnemer of intermediaire partij

Alleen in de hogere gradaties is sprake van een geverifieerde vertegenwoordigingsbevoegdheid. In de lagere gradatie is geen sprake van controle van de vertegenwoordigingsbevoegdheid van degene die de associatie goedkeurt en bestaat dus geen zekerheid over de vraag of de gemachtigde met medeweten van de wettelijke vertegenwoordigers van de dienstafnemer of intermediaire partij handelt. Dit lagere niveau is te vergelijken met “het tonen van een visitekaartje van de dienstafnemer”.

[7] De gemachtigde zelf moet zijn handtekening zetten in het kader van de middelenuitgifte, maar hoeft dus niet te tekenen voor acceptatie van de machtiging.

Vereisten (IV = "Identificatie" Vertegenwoordiging)	IV1	IV2	IV3
a. De associatie van degene die de opgave doet met de dienstafnemer moet worden geverifieerd door de opgave via een separaat kanaal te laten bevestigen aan de hand van een organisatiekenmerk (bijvoorbeeld fysieke post, e-mail of telefoon) van de dienstafnemer, waarbij dit organisatiekenmerk door een onafhankelijke en betrouwbare partij is aangedragen of geverifieerd.	●		
b. Het machtigingenregister moet aan de hand van een handelsregister controleren dat degene die namens een dienstafnemer opgave doet (de beheerder of de wettelijk vertegenwoordiger) daartoe gerechtigd is [i. iii]. • Voor opgave namens een onderneming of een privaatrechtelijke rechtspersoon moeten de identificerende kenmerken van degene die de opgave doet overeenkomen met de gegevens waarmee deze in een handelsregister als vertegenwoordiger geregistreerd is. Voor opgave namens een publiekrechtelijke rechtspersoon kan i) ofwel dezelfde overeenkomst van identificerende kenmerken gecontroleerd worden, voor zover de natuurlijk persoon die opgave doet als functionaris op naam in een handelsregister controleerbaar is; ii) ofwel gecontroleerd worden dat er een functionaris in een handelsregister geregistreerd is die overeenkomt met de functie van degene die opgave doet. In dat geval dient degene die opgave doet aanvullend zelf te verklaren dat hij op moment van aanvragen daadwerkelijk in betreffende functie is aangesteld; iii) ofwel in het geval dat de opgave niet door de wettelijke vertegenwoordiger gedaan wordt, noch door een functionaris die aanvullend in het handelsregister is geregistreerd, op basis van de controle van een intern mandaatbesluit conform het daarvoor door de beheerorganisatie eHerkenning beheerde protocol. • Voor alle controles ten opzichte van een handelsregister geldt dat naast de overeenkomst van de identificatie van de persoon gecontroleerd moet worden dat in de vertegenwoordigingsbevoegdheid geen beperkingen zijn opgenomen die de bevoegdheid om namens de dienstafnemer bevoegdheden te laten registreren doorkruisen. • Omdat publiekrechtelijke rechtspersonen kunnen bestaan uit meerdere organisatie onderdelen met zeer verschillende taken dient het machtigingenregister te controleren of de aanvraag niet in feite slechts op één van deze onderdelen betrekking heeft en derhalve zou moeten leiden tot de tot bijbehorende vestiging beperkte machtigingen.	○	●	
Als b met de uitbreiding dat het machtigingenregister bij de eerste registratie van een	○	○	●



Vereisten (IV = "Identificatie" Vertegenwoordiging)	IV1	IV2	IV3
gemachtigde moet controleren of er omstandigheden zijn waardoor er sprake is van bijzondere omstandigheden ten aanzien van de vertegenwoordigingsbevoegdheid, bijvoorbeeld een controle op faillissement of surseance van betaling. In dat geval moet via een separaat kanaal een aanvullende verificatie worden uitgevoerd bij de in een handelsregister vermelde wettelijke vertegenwoordiger, indien er meerdere vertegenwoordigers zijn wordt er een gekozen die niet in de aanvraag voorkomt. Bij wijziging van bevoegdheden van een bestaande gemachtigde kunnen deze controles achterwege blijven tenzij er bijzondere omstandigheden door de (beheerder van de) dienstafnemer bij het machtigingenregister gemeld zijn.			

Protocol voor controle van interne mandaatbesluiten.

Voor de controle van interne mandaatbesluiten die als alternatief voor controle in het handelsregister worden toegestaan geldt de volgende werkwijze:

- het mandaatbesluit wordt door degene die opgave doet verstrekt
- degene die opgave doet duidt aan op basis van welke in het mandaatbesluit genoemde functie hij de opgave doet
- degene die opgave doet verklaart dat hij op moment van aanvragen daadwerkelijk in betreffende functie is aangesteld
- het machtigingenregister controleert de betrouwbaarheid van het mandaatbesluit. Deze is voldoende als het betreffende besluit in officiële openbare overheidsbron als staatscourant of officiële openbaar gemaakte stukken van het bevoegde orgaan van de publiekrechtelijke rechtspersoon kan worden teruggevonden. Bij twijfel aan de betrouwbaarheid kan het machtigingenregister alsnog de wettelijke vertegenwoordiger vragen om zelf namens de rechtspersoon opgave te doen (indien deze niet al de opgave deed) of zelf een andere vertegenwoordiger van de rechtspersoon contacteren om deze te laten verklaren dat het mandaat geldig is.
- het verstrekte en gecontroleerde mandaatbesluit wordt gearchiveerd voor de duur van tenminste 7 jaar.

4.4.7 Kwaliteit van de organisatie die machtigingenregister beheert

Vereisten (IM = "Identificatie" Machtigingsregister)	IM1	IM2	IM3
a. Er mag sprake zijn van een vorm van overheidsinstemming of overeenkomst[8] met de overheid inzake de kwaliteit van de organisatie.	●		

8 Deze term "overeenkomst" is binnen STORK ruim geïnterpreteerd om een legio aan mogelijkheden toe te staan, waarbij de rol van de overheid kan variëren van beperkt tot nadrukkelijk.

b. Er moet sprake zijn van een vorm van overheidsinstemming of overeenkomst met de overheid inzake de kwaliteit van de organisatie. Het feit dat de partij deelnemer is van het afsprakenstelsel voorziet hierin.	○	●	
c. Er moet sprake zijn van overheidstoezicht optioneel in de vorm van accreditatie. Tevens moet voldaan worden aan de specifieke normen voor de kwaliteit van de organisatie zoals geëist voor STORK betrouwbaarheidsniveau 4 (gekwalificeerde elektronische handtekeningen).	○	○	●

4.4.8 Geldigheidsduur van bevoegdheden

Vereisten (PD = Procesaspect Duur)	PD1	PD2
a. Het machtigingenregister mag een bevoegdheid die 25 maanden niet is gebruikt intrekken. Vooraf moet aan de gemachtigde, en indien aanwezig aan de beheerder, gemeld worden dat betreffende bevoegdheid binnen een bepaalde tijd wordt ingetrokken.	●	
b. Het machtigingenregister moet een bevoegdheid die 25 maanden niet is gebruikt intrekken. Vooraf moet aan de gemachtigde, en indien aanwezig aan de beheerder, gemeld worden dat betreffende bevoegdheid binnen een bepaalde tijd wordt ingetrokken.	○	●

Verlenging, intrekking en schorsing vinden altijd plaats in situatie dat er al een registratie heeft plaatsgevonden. Ook de maximale doorlooptijd heeft daarop betrekking. Deze aspecten worden derhalve beschreven in paragraaf 4.5.

4.5 Situatie van herhaalde registratie

In deze paragraaf wordt beschreven welke alternatieven bestaan bij registratie door een eerder aangestelde beheerder of voor het geval van een wettelijke vertegenwoordiger die reeds een eHerkenningsmiddel bezit. Naast een eHerkenningsmiddel MOET voor de beheerder een machtiging te zijn geregistreerd voor de beheerbevoegdheid. Voor de leesbaarheid wordt verder gesproken over beheerder en daarbij wordt eveneens een wettelijke vertegenwoordiger bedoeld die zelf over een eHerkenningsmiddel beschikt en de benodigde bevoegdheid heeft.

De beheerder kan ook niet-elektronisch werken. In dat geval ondertekent de beheerder steeds met natte handtekening en ZOU deze steeds ten opzichte van zijn eerder gearchiveerde handtekening MOETEN worden geverifieerd.

4.5.1 *Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)*

Bij elektronische opgave wordt de identificatie van de vertegenwoordigde afgeleid uit de machtiging die voor de beheerder bij diens authenticatiemiddel is geregistreerd. Deze machtiging moet tenminste hetzelfde betrouwbaarheidsniveau hebben als datgene wat ermee opgegeven wordt.

Vereisten (IA = Identificatie dienstAfnemer)	IA0	IA1	IA2
a. Vertegenwoordigde geïdentificeerd op basis van machtiging van beheerder op betrouwbaarheidsniveau EH1.	○	●	
b. Voor een niet-elektronische beheerder conform § 4.4.2.b	○	○	●
Vertegenwoordigde geïdentificeerd op basis van machtiging van beheerder op betrouwbaarheidsniveau EH2 of hoger. Indien de strekking van de machtiging beperkt wordt tot een vestiging dan moet volledige controle conform b plaats vinden, tenzij het een beheerder betreft waarvan vastligt dat deze enkel beheerrechten heeft voor betreffende vestiging.	○	○	●

4.5.2 *Kwaliteit identificatieprocedure van degene die de opgave doet*

Deze kwaliteit wordt direct bepaald door het EH-betrouwbaarheidsniveau van de beheerder.

Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
a. Beheerder met EH-betrouwbaarheidsniveau 1.	●			
b. Voor een niet-elektronische beheerder conform § 4.4.3.b. Aangezien het (afgeschrmde) kopie WID-document al eerder gecontroleerd is door het machtigingenregister, hoeft het niet opnieuw meegezonden te worden mits het machtigingenregister de beheerder op andere wijze kan verifiëren.	○	●		
c. Beheerder met EH-betrouwbaarheidsniveau 2.	○	●		
d. Voor een niet-elektronische beheerder conform § 4.4.3.d. Eén van beide verificaties van de afgeschermde kopie WID, hetzij ten opzichte van een register van gestolen en vermiste documenten, hetzij ten opzichte van een persoonlijke banktransactie MOET worden herhaald voor deze beheerder. Zolang de afgeschermde kopie WID-document die al in bezit van het machtigingenregister is nog niet verlopen is, hoeft het niet opnieuw meegezonden te worden.	○	○	●	
e. Beheerder met EH-betrouwbaarheidsniveau 3.	○	○	●	

Vereisten (IO = Identificatie Opgever)	IO1	IO2	IO3	IO4
f. Beheerder met EH-betrouwbaarheidsniveau 4 die de opgave met elektronische handtekening ondertekent.	○	○	○	●

De aspecten identificatieprocedure gemachtigde, zekerheid associatie, kwaliteit van de organisatie en geldigheidsduur zijn identiek aan situatie bij initiële opgave.

4.5.3 Kwaliteit van de verlengingsprocedure voor bevoegdheden

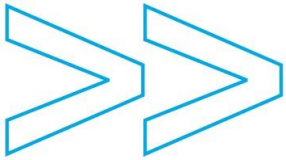
De eisen voor verlenging dienen gelijk te zijn aan de eisen voor eerste vastleggen van een bevoegdheid. Verleningen dienen altijd bevestigd te worden aan de beheerder, indien aanwezig.

Vereisten (PV = Procesaspect Verlenging)	PV1	PV2	PV3	PV4
a. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO1 en IV1.	●			
b. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO2 en IV2. De machtiging waarop de verlenging betrekking heeft wordt geïdentificeerd conform IA2 en uniek identificerende kenmerken van de gemachtigde.	○	●		
c. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO3 en IV2. De machtiging waarop de verlenging betrekking heeft wordt geïdentificeerd conform IA2 en uniek identificerende kenmerken van de gemachtigde.	○	○	●	
d. Degene die opgave doet van verlenging wordt geïdentificeerd in een proces dat tenminste voldoet aan IO4 en IV2. De machtiging waarop de verlenging betrekking heeft wordt geïdentificeerd conform IA2 en uniek identificerende kenmerken van de gemachtigde.	○	○	○	●

4.5.4 Kwaliteit van de intrekkingsprocedure voor bevoegdheden

Van de volgende partijen mogen intrekkingsverzoeken geaccepteerd worden: alle wettelijke vertegenwoordigers inclusief een curator, de gemachtigde zelf, de beheerder van de dienstafnemer of op last van de rechtbank.

Vereisten (PI = Procesaspect Intrekking)	PI1	PI2	Pi3	PI4
a. Het intrekkingsverzoek dient schriftelijk, per e-mail of na authenticatie op betrouwbaarheidsniveau 1 te gebeuren door één van bovengenoemde partijen. Er worden geen eisen gesteld aan doorlooptijd van intrekking van	●			



Vereisten (PI = Procesaspect Intrekking)	PI1	PI2	Pi3	PI4
authenticatiemiddelen en bevoegdheden.				
b. Een intrekkingsverzoek mag alleen geaccepteerd worden mits de opgever geïdentificeerd kan worden conform de eisen van tenminste IO2. Intrekking van authenticatiemiddelen en bevoegdheden moet door deelnemers als volgt uitgevoerd worden: • indien de elektronische procedure gevolgd wordt per direct en • indien het verzoek niet elektronisch wordt gedaan binnen 1 werkdag na ontvangst van het intrekkingsverzoek.	○	●		
c. Tenminste als bovenstaande waarbij de opgever geïdentificeerd kan worden conform de eisen van tenminste IO3.	○	○	●	
d. Tenminste als bovenstaande waarbij echter voor de intrekking van authenticatiemiddelen PKIoverheid gevolgd moet worden.	○	○	○	●

4.5.5 Kwaliteit van de schorsingsprocedure voor bevoegdheden

Indien schorsing (tijdelijke intrekking) wordt ondersteund, MOET aan deze minimale eisen worden voldaan:

1. Opdracht tot schorsing moet zijn gedaan door één van de volgende partijen: wettelijke vertegenwoordiger inclusief een curator, beheerder van de dienstafnemer, de gemachtigde zelf of op last van de rechtbank en voldaan aan dezelfde eisen als voor een intrekking.
2. Ongedaan maken van een schorsing moet plaatsvinden door een beheerder op het betreffende betrouwbaarheidsniveau of conform de eisen voor verlenging.

4.5.6 Doorlooptijd van mutaties van bevoegdheden

Vereisten (PT = Procesaspect doorloopTijd)	PT1	PT2
a. Mutaties moeten zo snel mogelijk verwerkt worden.	●	
b. Elektronisch ingediende mutaties, inclusief intrekking van een bevoegdheid, moeten per direct verwerkt worden. Niet-elektronische mutaties moeten binnen twee werkdagen na ontvangst bij de deelnemer van het verzoek verwerkt zijn.	○	●

4.6 Synthese betrouwbaarheidsniveau van bevoegdheden

Bovenstaande criteria zijn geformuleerd in termen van vertegenwoordigde – gemachtigde. Dit kan toegepast worden op meerdere situaties:

- Een wettelijke vertegenwoordiger wordt geregistreerd met zijn bevoegdheid de dienstafnemer te vertegenwoordigen.
- Een wettelijke vertegenwoordiger geeft de bevoegdheid op van een uitvoerend natuurlijk persoon.
- Een wettelijke vertegenwoordiger geeft een beheerder op.
- Een beheerder doet opgave van een machtiging voor een andere gemachtigde.

In alle gevallen komt het overkoepelende betrouwbaarheidsniveau voor machtigingen zoals dat binnen eHerkenning geldt tot stand op basis van onderstaande tabel.

Criterium (betrouwbaarheid Machtiging)	M1	M2	M3	M4
Kwaliteit identificatieprocedure vertegenwoordigde (dienstafnemer)	IA1	IA2	IA2	IA2
Kwaliteit identificatieprocedure van degene die opgave doet	IO1	IO2	OI3	IO4
Kwaliteit identificatieprocedure gemachtigde natuurlijk persoon	IG1	IG2	IG3	IG4
Kwaliteit identificatieprocedure gemachtigde rechtspersoon	IR1	IR2	IR2	IR2
Zekerheid omtrent de associatie van degene die de opgave doet met de dienstafnemer	IV1	IV2	IV3	IV3
Kwaliteit van de organisatie die het machtigingenregister beheert	IM1	IM2	IM2	IM3
Geldigheidsduur bevoegdheden	PD1	PD2	PD2	PD2
Kwaliteit verlengingsprocedure	PV1	PV2	PV3	PV4
Kwaliteit intrekkingsprocedure (evenals schorsing)	PI1	PI2	PI3	PI4
Doorlooptijd van mutaties	PT1	PT2	PT2	PT2

De score op het aspect machtiging (aangeduid met M en volgnummer) wordt vervolgens gecombineerd met de score van het authenticatiemiddel om tot een eHerkennings-betrouwbaarheidsniveau te komen. Voor deze laatste stap zie de volgende paragraaf.

5 Opbouw betrouwbaarheidsniveaus eHerkenning

Het betrouwbaarheidsniveau zoals dat in eHerkenning geldt, komt tot stand door twee losstaande classificaties met elkaar te combineren, namelijk:

de classificatie van het authenticatiemiddel van de gemachtigde (zoals behandeld in hoofdstuk 3) en de classificatie van de betrouwbaarheid van de bevoegdheid zoals behandeld in hoofdstuk 4.

Dit is weergegeven in onderstaande tabel. Ter vergelijking zijn de STORK betrouwbaarheidsniveaus vermeld.

RESULTAAT: Betrouwbaarheids-niveau eHerkenning	Betrouwbaarheidsniveau authenticatiemiddel van de betreffende gemachtigde	Classificatie t.a.v. bevoegdheden[9]	Betrouwbaarheidsniveau eHerkenning van degene die de opgave doet (in geval van elektronisch proces)
EH1	STORK 1	M1	EH1
EH2	STORK 2	M2	EH2
EH2+	STORK 3 cfm versie 1.7[10]	M2[11]	EH2+
EH3	STORK 3	M3	EH3
EH4	STORK 4	M4	EH4

De laatste kolom betreft alleen de situaties waarin bevoegdheden via een elektronisch proces worden opgegeven. In die gevallen geldt de “zwakste schakel telt” regel en is derhalve voor een bepaald betrouwbaarheidsniveau een opgave door iemand die minimaal zelf gemachtigd is op dat niveau vereist.

Betrouwbaarheidsniveaus worden bepaald tijdens de registratie. Tijdens het gebruik wordt gecontroleerd op het voldoen aan het gevraagde betrouwbaarheidsniveau. Het is niet toegestaan voor een authenticatiedienst om Single Sign On toe te passen als betrouwbaarheidsniveau 4 vereist wordt.

9 In het geval van een keten van bevoegdheden geldt voor de classificatie van de gehele transactie de schakel in de keten met de laagste betrouwbaarheid.

10 In STORK versie 1,7 zijn de eisen van het niveau dat specifiek was voor eHerkenning versie 1.4 en eerder geaccepteerd als STORK 3.

11 In de wijziging van versie 1.4 naar 1.5 zijn bij invoering van EH2 tevens aanscherpingen doorgevoerd aan EH3. Hierdoor zijn de eisen voor bevoegdheden M3 vanaf versie 1.5 zwaarder dan deze in 1.4 waren voor EH3. De eisen van M2 vanaf versie 1.5 zijn op enkele nieuwe alternatieven na gelijk aan die van M2 in versie 14 en dus ook geldend voor EH2+, echter met dien verstande dat de zwakste schakel redenering moet worden toegepast en dat waar in deze M2 eisen een STORK 2 middel vereist wordt voor EH2+ een middel dat voldoet aan het specifieke niveau vereist wordt. Daarmee is verzekerd dat de eisen voor het uit te faseren niveau EH2+ ongewijzigd zijn ten opzichte van versie 1.4.

6 Toepassing betrouwbaarheidsniveaus op aanvullende features

6.1 Registratieeisen attributen (additionele feature)

Indien een middelenuitgever of machtigingenregister attributen verstrekt dan leidt dit tot de volgende aanvullende registratieverplichtingen.

Per verstrekbaar attribuut wordt de naam conform de attribuutcatalogus vastgesteld en welk betrouwbaarheidsniveau het betreffende gegeven heeft.

Indien het gegevens betreft die verplicht geregistreerd worden in het kader van uitgifte van middelen (zie Bijlage D) en/of registratie van machtigingen (als gespecificeerd in § 4.3 punt 1, 3 en 4) MOETEN deze minimaal gecontroleerd zijn conform het betrouwbaarheidsniveau van betreffende registratie en MOGEN op dat betrouwbaarheidsniveau worden geregistreerd conform de beschrijving in document [Attribuutcatalogus]. Overige attributen MOGEN alleen gevraagd worden voor latere verstrekking indien deze in de attribuutcatalogus gespecificeerd zijn. Deze attributen MOGEN alleen geregistreerd worden conform de daar bepaalde registratie-eisen. Voor deze attributen geldt dat de registrerende deelnemer onweerlegbaar MOET kunnen aantonen dat deze attributen verstrekt zijn exact overeenkomstig opgave door de uitvoerend natuurlijk persoon, respectievelijk beheerder of wettelijke vertegenwoordiger of dat deze gegevens tijdens de authenticatie zijn gevalideerd in een neutraal en betrouwbaar register.

De doorlooptijd van mutaties MAG NIET langer zijn dan die welke geldt voor mutaties van machtigingen op betreffende betrouwbaarheidsniveau als vermeld in § 4.5.6 van document [Betrouwbaarheidsniveaus en registratie-eisen].

Iedere keer dat een uitvoerend natuurlijk persoon, beheerder of wettelijke vertegenwoordiger user consent voor verstrekking verleent MOET dit geregistreerd worden. User consent voor verstrekking van persoonsgegevens door de AD MAG NIET gevraagd worden in een dialoogvorm waarbij de defaultwaarde het geven van toestemming voor alle mogelijke persoonsgegevens inhoudt. User consent voor verstrekking van gegevens over de vertegenwoordigde dienstafnemer/intermediaire partij door de MR MAG gevraagd worden in een dialoogvorm waarbij de defaultwaarde het geven van toestemming voor alle mogelijke bedrijfsgegevens inhoudt.

Verzoeken om user consent MOETEN specifiek zijn en aan te duiden ten behoeve van welke dienstverlener en dienst de gegevens worden verstrekt. De geldigheid van een geregistreerde user consent MOET beperkt zijn tot maximaal de geldigheidsduur die conform § 4.4.8 geldt voor machtigingen op het betreffende betrouwbaarheidsniveau.

User consent MOET te allen tijde kunnen worden ingetrokken op basis van online verzoek door de uitvoerend natuurlijk persoon, beheerder of wettelijke vertegenwoordiger of MOET op het moment van de authenticatietransactie zichtbaar zijn en op dat moment kunnen worden ingetrokken.

De houder van een authenticatiemiddel respectievelijk de wettelijk vertegenwoordiger / machtigingenbeheerder MOET steeds op het betreffende betrouwbaarheidsniveau elektronisch inzage kunnen krijgen, correcties en verwijderingen kunnen aanvragen van alle over hem respectievelijk over de

vertegenwoordigde dienstafnemer/intermediaire partij geregistreerde (persoons)gegevens inclusief of er doorlopende user consent voor verstrekking gegeven is.

6.2 Gebruikersgedefinieerde attributen

Bij authenticatiedienst en machtigingenregisters worden alleen die attributen vastgelegd die zijn gedefinieerd in document [Attribuutcatalogus]. Andere, gebruikersgedefinieerde, attri- buten MOGEN NIET worden gebruikt.

Bijlage D.

Deze bijlage beschrijft per betrouwbaarheidsniveau de kenmerken van de verschillende betrouwbaarheidsniveaus in STORK. Voor de gedetailleerde criteria die betrekking hebben op authenticatiemiddelen en de authenticatiedienst wordt verwezen naar het brondocument van het STORK raamwerk[12]. In gevallen van eventuele verschillen tussen deze bijlage en het brondocument behorende bij het raamwerk moet de brondocumentatie van het raamwerk worden toegepast.

Betrouwbaarheidsniveau 1

Betrouwbaarheidsniveau 1 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten zekerheid van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst.

Registratiefase	**Elektronische authenticatiefase**
Identificatieprocedure	**Type en robuustheid authenticatiemiddel**
a. De registratie heeft tenminste met de volgende kenmerken vergelijkbare eigenschappen. Identificatie mag plaatsvinden zonder fysieke verschijning. Identificatie (niet noodzakelijk uniek) moet plaatsvinden aan de hand van een enkel kenmerk dat ook bij anderen bekend kan zijn. Validatie moet plaatsvinden aan de hand van een e-mailadres.	Het authenticatiemiddel moet tenminste een wachtwoord of PIN zijn, (a) gekozen door de uitvoerend natuurlijk persoon of (b) automatisch gegenereerd zonder eisen aan de sterkte van het wachtwoord of PIN.
Proces van middelenuitgifte	**Zekerheid van het authenticatiemechanisme**
b. Middelenuitgifte mag plaatsvinden zonder enige vorm van verificatie van de identiteit van de uitvoerend natuurlijk persoon.	Het authenticatiemechanisme geeft geen of nauwelijks bescherming tegen de dreigingen uit hoofdstuk 3 van het deel 4. Betrouwbaarheidsniveaus (1-factor authenticatie).
Partij die het authenticatiemiddel uitgeeft	
c. Er is geen sprake van toezicht op of accreditatie van de middelenuitgever.	

12 Document D2.3 - Quality authenticator scheme, paragraaf 2.3 en 2.4, te vinden op http://www.eid-stork.eu, onder STORK materials, deliverables approved/public.

Betrouwbaarheidsniveau 2

Betrouwbaarheidsniveau 2 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten zekerheid van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst.

Registratiefase	**Elektronische authenticatiefase**
Identificatieprocedure	**Type en robuustheid authenticatiemiddel**
a. De registratie heeft tenminste met de volgende kenmerken vergelijkbare eigenschappen. Identificatie mag online plaatsvinden zonder fysieke verschijning (i.a). Unieke identificatie moet plaatsvinden aan de hand van meerdere kenmerken die ook bij anderen bekend kunnen zijn (ii.b). Validatie moet plaatsvinden door te vergelijken met een neutrale en betrouwbare derde zoals een bank, verzekeraar of overheidsinstantie (iii.b).	Het authenticatiemiddel moet tenminste zijn: Wachtwoord op PIN gebaseerd token dat hetzij door de houder gekozen is, hetzij gegenereerd maar in beide gevallen voldoet aan gebruikelijke richtlijnen voor sterke wachtwoorden of PINcodes (voldoende lang, verschillende karakters, niet herbruikbaar, etc.) en daarom niet kwetsbaar voor raden of woordenboek aanvallen (RC2).
Proces van middelenuitgifte	**Zekerheid van het authenticatiemechanisme**
b. Middelenuitgifte moet plaatsvinden aan de hand van lichte mate van zekerstelling van de identiteit van de uitvoerend natuurlijk persoon (bijvoorbeeld verzending van gebruikersnaam en wachtwoord in twee losse zendingen waarvan tenminste één per gewone post naar het adres van de houder zoals dat bekend is in een officiële overheidsdatabase (werkwijze van DigiD Burger basis) of download van het authenticatiemiddel van een eenmalige link die naar door de houder opgegeven e-mailadres verzonden wordt) (IC2).	Het authenticatiemechanisme is een veilig mechanisme dat enige bescherming biedt tegen de dreigingen uit hoofdstuk 3 van het deel Betrouwbaarheidsniveaus (1-factor authenticatie) (AM2).
Partij die het authenticatiemiddel uitgeeft	
c. Er moet sprake zijn van toezicht of accreditatie onder verantwoordelijkheid van de overheid. Het feit dat de partij deelnemer is van het afsprakenstelsel voorziet hierin (IE2).	

Gebruikelijke richtlijnen voor sterke wachtwoorden

Voor deze richtlijnen gelden de op enige moment voor DigiD burger basis geldende richtlijnen als minimum. Deze worden overgenomen, met uitzondering van de beperking van lengte tot maximaal 32 tekens. Momenteel zijn deze[13]:

- Het wachtwoord moet bestaan uit minimaal 8 tekens
- Bevat minimaal 1 kleine letter [a-z]
- Bevat minimaal 1 hoofdletter [A-Z]
- Bevat minimaal 1 cijfer [0-9]
- Bevat minimaal 1 bijzonder teken: [- _ ! $ % & ' . = / \ : < > | ? @ [ ] ^ ` { } ~]
- Mag niet uw gebruikersnaam bevatten
- Het wachtwoord mag niet gelijk zijn aan een van de laatste 5 wachtwoorden.

Betrouwbaarheidsniveau 3

Betrouwbaarheidsniveau 3 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten **zekerheid** van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst.

Registratiefase	Elektronische authenticatiefase
Identificatieprocedure (ID)	**Type en robuustheid authenticatiemiddel (RC)**
a. Twee varianten van de identificatieprocedure zijn toegestaan (i.b + tenminste ii.b + tenminste iii.c of i.a + tenminste ii.c + tenminste iii.d), met de volgende combinaties van kenmerken. 1. Er moet (initiële) fysieke verschijning plaats vinden op enig moment in het registratie en uitgifteproces (i.b). Unieke identificatie moet plaatsvinden aan de hand van meerdere kenmerken die ook bij anderen bekend kunnen zijn (ii.b). Validatie moet plaatsvinden aan de hand van een elektronische handtekening die niet gebaseerd hoeft te zijn op een gekwalificeerd certificaat óf door een van de	Het authenticatiemiddel is tenminste: • een soft certificaat (al of niet gekwalificeerd conform de Richtlijn Elektronische handtekeningen), • een one-time password token of een certificaat op een hardware token (niet noodzakelijk conform de Richtlijn Elektronische handtekeningen).

13 (http://www.digid.nl/vraag-en-antwoord/?nodeid=2426). De beperking van de lengte tot 32 tekens wordt niet overgenomen.

ondergenoemde methoden (tenminste iii.c). 2. Identificatie mag online plaatsvinden zonder fysieke verschijning (i.a). Unieke identificatie moet plaatsvinden aan de hand van in een of ander officieel register verifieerbare kenmerken die uitsluitend bij de uitvoerend natuurlijk persoon bekend zijn (ii.c). Validatie moet plaatsvinden aan de hand van een van de ondergenoemde methoden (tenminste iii.d).	
Proces van middelenuitgifte (IC)	**Zekerheid van het authenticatiemechanisme (AM)**
b. Middelenuitgifte moet plaatsvinden aan de hand van redelijke mate van zekerstelling van de identiteit van de uitvoerend natuurlijk persoon (bijvoorbeeld aan de hand van een aangetekende brief aan een gevalideerd adres, identificatie met een gekwalificeerd certificaat of downloaden aan de hand van een fysiek verkregen wachtwoord).	Het authenticatiemechanisme moet een veilig mechanisme zijn dat bescherming geeft tegen de meeste van de dreigingen uit hoofdstuk 3 van het deel Betrouwbaarheidsniveaus (2-factor authenticatie).
Partij die het authenticatiemiddel uitgeeft (IE)	
c. Er moet sprake zijn van toezicht of accreditatie onder verantwoordelijkheid van de overheid. Het feit dat de partij deelnemer is van het afsprakenstelsel voorziet hierin.	

Validatiemethoden toegelaten in de identificatieprocedure op niveau 3 (ID, iii)

Onderstaande methoden moeten gelezen worden als opeenvolgend steeds betrouwbaarder

d (tussengevoegd in STORK v1.7). De validatie vereist een verklaring van een werkgever van de aanvrager gebaseerd op een overeenkomst tussen werkgever en middelenuitgever waarin de werkgever verklaart dat hij de validatie van het fysieke en officieel WID-document, heeft uitgevoerd bij indiensttreding. Deze validatiemethode MAG NIET worden toegepast indien de werkgever dezelfde persoon is als degene die geïdentificeerd wordt.

e (tussengevoegd in STORK v1.7). De validatie vereist het aanleveren van een fotokopie of scan van een WID-document. De geldigheid van deze kopie MOET worden gecontroleerd ten opzichte van een register van gestolen en vermiste identiteitsdocumenten. De kopie ZOU alleen in afgeschermde vorm MOETEN worden opgeslagen.

f. (tussengevoegd in STORK v1.7). De validatie vereist het aanleveren van een fotokopie of scan van een WID-document. Vervolgens moet een succesvolle banktransactie worden uitgevoerd vanuit een

bankrekening die oorspronkelijk alleen geopend kan zijn op basis van het tonen van een fysiek en officieel WID-document en waar de bankrekening gerelateerd is aan dezelfde persoon als degene die geïdentificeerd wordt in de aangeleverde kopie WID-document. De kopie ZOU alleen in afgeschermde vorm MOETEN worden opgeslagen.

g. (minimum in STORK tot aan v1.7 en tevens het minimum voor niveau 4). De validatie vereist het tonen van een fysieke (geen kopie) en officieel WID-document[14]. Een kopie van dit WID-document ZOU alleen in afgeschermde vorm MOETEN worden opgeslagen.

h. De validatie vereist dat de aangeleverde gegevens ondertekend zijn met een elektronische handtekening die geverifieerd wordt bij een certificatiedienstverlener (CSP) voordat het authenticatiemiddel wordt uitgereikt.

Betrouwbaarheidsniveau 4

Betrouwbaarheidsniveau 4 kent voor authenticatiemiddelen de criteria zoals weergegeven in onderstaande tabel. De aspecten **zekerheid** van het authenticatiemechanisme en partij die het authenticatiemiddel uitgeeft, gelden ook voor de authenticatiedienst. PKIoverheid wordt beschouwd als een invulling van betrouwbaarheidsniveau 4.

Registratiefase	**Elektronische authenticatiefase**
Identificatieprocedure	**Type en robuustheid authenticatiemiddel**
a. De registratie heeft tenminste met de volgende kenmerken vergelijkbare eigenschappen. Bij registratie en/of uitgifte moet sprake zijn van een (initiële) fysieke verschijning. Unieke identificatie moet plaatsvinden aan de hand van verifieerbare kenmerken die uitsluitend bij de uitvoerend natuurlijk persoon bekend zijn. Validatie moet plaatsvinden aan de hand van het tonen van een officieel identiteitsdocument of door een certification service provider geverifieerde elektronische handtekening.	Het authenticatiemiddel moet tenminste een gekwalificeerd certificaat zijn gebaseerd op een veilig middel zoals bedoeld in de Richtlijn Elektronische handtekeningen.

[14] In ieder geval valt hieronder een service van de middelenuitgever waarbij een medewerker van de middelenuitgever naar de uitvoerend natuurlijk persoon toe gaat. Een mogelijke alternatieve interpretatie is dat de uitvoerend natuurlijk persoon zijn originele officiële identiteitsdocument opstuurt of meegeeft aan iemand anders. Er is nog geen praktijkervaring of uitspraak ten aanzien van de acceptatie hiervan binnen STORK.

Proces van middelenuitgifte	Zekerheid van het authenticatiemechanisme
b. Middelenuitgifte moet plaatsvinden aan de hand van een sterke mate van zekerstelling van de identiteit van de uitvoerend natuurlijk persoon (bijvoorbeeld verstrekking of activatie na fysieke identiteitsvaststelling)	Het authenticatiemechanisme moet erkend zijn als veilig mechanisme dat beschermt tegen de dreigingen uit hoofdstuk 3 van het deel 4. Betrouwbaarheidsniveaus vergelijkbaar met Common Criteria EAL 4+ (2-factor authenticatie).
Partij die het authenticatiemiddel uitgeeft	
c. Er is sprake van verplicht toezicht en optionele vrijwillige accreditatie zoals bedoeld in de Richtlijn Elektronische handtekeningen.	

496