Technische specificaties en procedures voor uitgifte van authenticatiemiddelen

EH1 vervalt per 1-7-2021

Met ingang van 1 juli 2021 komt het gebruik van het betrouwbaarheidsniveau eH1 te vervallen en moeten de middelen en machtigingen minimaal voldoen aan de normen van het betrouwbaarheidsniveau eH2.

2.1 Inschrijving

2.1.1 Aanvraag en registratie

LoA	Vereiste elementen	
LOA 1	1. De Deelnemers MOETEN de Gebruiksvoorwaarden Elektronische Toegangsdiensten die vastgelegd zijn in Afsprakenstelsel onderdeel maken van de voorwaarden die zij hun klanten opleggen. 2. Deelnemers MOETEN de gebruikers bekend maken met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 3. De Deelnemer MOET de Gebruiker met gebruiksvoorwaarden binden aan: a. de verplichting tot het melden van verlies, misbruik en een vermoeden van misbruik van zijn authenticatiemiddel bij de Deelnemer en; b. binden aan een verplichting om gelijktijdig een verzoek te doen tot revocatie of schorsing van zijn authenticatiemiddel. 4. De Deelnemer MOET de levensduur van het authenticatiemiddel, de procedure voor intrekking en indien van toepassing de procedure voor schorsing en vernieuwing aan de Gebruiker bekend maken. 5. Gebruiksvoorwaarden van Deelnemers moeten aan de Gebruikers ter beschikking worden gesteld 6. De identiteitsverklaring(en) die de Aanvrager aanlevert MOETEN leiden tot een unieke identificatie van de Aanvrager. De aangeleverde gegevens MOET(EN) bestaan uit meervoudige verklaringen die: a. betrekking hebben op de Aanvrager en; b. niet noodzakelijkerwijs uitsluitend bij de Aanvrager bekend zijn. c. de Identiteitsverklaring van de Aanvrager MAG alleen op LoA1 zelf-verklaard (self-asserted) zijn.	
LOA 2	Hetzelfde als LoA1 met toevoeging van: 1. Elke van de volgende kenmerken MOET worden opgevat als te gebruiken voor de meervoudige identiteitsverklaringen zoals bij LoA1 punt 6 is bedoeld: a. Naam (VERPLICHT), in combinatie met: b. Adres of; c. Geboortedatum of; d. Geboorteplaats 2. De aangeleverde identiteitsverklaring MOET zijn gebaseerd op een van de onderstaande officiële bronnen voor identificatiedoeleinden: a. Voor middelen die bedoeld zijn voor gebruik in het burgerdomein: i. Een geldig WID dat voorzien is van een BSN b. Voor overige middelen: i. een geldig Nederlands paspoort of ander nationaal paspoort dat door de Nederlandse Staat wordt erkend. ii. een geldig identiteitskaart uit een Europese Economische Ruimte (EER)-land iii. een geldig Nederlands vreemdelingendocument mits voorzien van een pasfoto. iv. een geldig rijbewijs uit een EER-land mits voorzien van pasfoto v. een geldig gekwalificeerd certificaat	

LOA 3	Hetzelfde als LoA 2 met toevoeging van: 1. Elke van de volgende kenmerken MOET worden opgevat als te gebruiken voor de meervoudige identiteitsverklaringen zoals bij LoA1 punt 6 is bedoeld: a. Naam (VERPLICHT), in combinatie met: b. Adres c. Geboortedatum (VERPLICHT voor middelen die bedoeld zijn voor het gebruik in het Burgerdomein) d. Geboorteplaats e. BSN (VERPLICHT voor middelen die bedoeld zijn voor het gebruik in het Burgerdomein) 2. Tijdens de registratie online aangeleverde verklaringen MOGEN zijn ondertekend met een niet-gekwalificeerd certificaat. 3. De identiteitsverklaring van de Gebruiker MOET worden geverifieerd aan het originele fysieke WID document. 4. Voor middelen die bedoeld zijn voor het gebruik in het Burgerdomein MOET de Deelnemer het BSN van de Gebruiker verifiëren in zijn originele fysieke WID document.	Ad 3 en 4 Voor LoA3 zijn alternatieve invullingen toegestaan zoals beschreven is in de paragraaf 2.1.2 'Eisen Identificatie op Afstand' en paragraaf 2.1.2 bij LoA3.
LOA 4	Hetzelfde als LoA 3 met toevoeging van: 1. Online aangeleverde verklaringen MOETEN zijn ondertekend met een gekwalificeerd certificaat.	

2.1.2 Bewijs en verificatie van Identiteit (natuurlijk persoon)

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	De Deelnemer moet het e-mailadres valideren als deze contactgegevens gebruikt worden als onderdeel van het registratieproces (versturen van activatiecodes, links of (one-time) passwords).	
LOA 2	LoA 1 met toevoeging van: 1. De Deelnemer moet het e-mailadres en telefoonnummer valideren als deze contactgegevens gebruikt worden als onderdeel van het registratieproces (versturen van activatiecodes, links of (one-time) passwords).	Ad 2 In Nederland is de Basisregistratie Personen (BRP) als de formele en gezaghebbende bron voor identiteitscontrole. Validatie van identificerende gegevens waarbij de HRM database van een werkgever of een werkgeversverklaring als bron wordt gebruikt MOETEN slechts betekenis hebben binnen de bedrijvencontext. Dergelijke validaties zijn vanwege de mogelijkheden tot opzettelijk misbruik door de aanvrager ongeschikt voor uitgifte van middelen die in het burgerdomein (BSN domein) en consumentendomein gebruikt kunnen worden. Deelnemers MOGEN NIET dit risico met gebruiksvoorwaarden afdekken. Het middel een MOET zodanige werking hebben dat gebruik daarvan in het burgerdomein en consumentendomein onmogelijk is gemaakt. In het geval de bankoverschrijving als een toegevoegde verificatie wordt gebruikt: De bankrekening MOET een privérekening zijn bij een bank waar de aanvrager dezelfde persoon is als de enige bankrekeninghouder en; waarvoor de financiële instelling voor het openen van de bankrekening de rekeninghouder zich conform wettelijke vereisten heeft moeten laten identificeren, op basis van een geldig identiteitsbewijs. Ad 4 Kern van deze norm is dat identificatie bij registratie of uitgifte altijd op het juiste LoA heeft plaats gevonden. Voor een gekwalificeerd certificaat heeft een identificatie op LoA4 plaats gevonden. Ten behoeve van de uitgifte van middelen voor gebruik in het burgerdomein moet altijd een verificatie van het BSN plaatsvinden aan het originele WID van de Aanvrager. Voor LoA3: Validatie van het BSN moet middels een registratie in het BSNk plaatsvinden. Ad 5c M.b.t. vereisten voor validatie van elektronische handtekening die niet op PKI zijn gebaseerd: • Een gelijke kwaliteit (equal quality) van validatie kan uitsluitend worden bereikt met een handgeschreven handtekeningen of op PKI-technologie gebaseerde handtekeningen.

2. Voor validatie van de aangeleverde identiteitsverklaringen MOET geaccepteerd worden dat een van de onderstaande bronnen een invulling zijn van een officiële neutrale en betrouwbare bron;
    a. De Nederlandse Basisadministratie Personen (BRP, voorheen bekend als GBA)
    b. De HRM-database met persoonsgegevens van medewerkers van een onderneming of rechtspersoon, indien aan voorwaarden i, ii, iii en iv wordt voldaan:
        i. De bruikbaarheid van het middel is beperkt tot die onderneming of rechtspersoon in Nederland.
        ii. Het middel en de machtigingen zijn bij dezelfde deelnemer uitgegeven.
        iii. Het BSN van de gebruiker wordt niet geregistreerd.
        iv. Het middel is niet bruikbaar in het BSN-domein en consumentendomein.
3. Slechts voor LoA 2 is het overleggen van een kopie van een identiteitsdocument geaccepteerd. In dat geval MOET de verificatie van echtheidskenmerken voor zover mogelijk worden uitgevoerd door daartoe opgeleid personeel;

4. Identificatie MAG eveneens plaatsvinden:
    a. Met een middel op LoA 2 en hoger dat door een Deelnemer in het stelsel is uitgegeven.
        i. Restrictie: Met een middel van een specifiek LoA MAG NIET zonder aanvullende validaties een Stelseldienst (middel of machtiging) met een hoger LoA worden verstrekt.
    b. Restrictie: Op basis van een middel dat niet voor gebruik in het burgerdomein is uitgegeven MAG NIET zonder aanvullende validaties een middel voor gebruik in het burgerdomein worden verstrekt.
    c. Op basis van een gekwalificeerd certificaat dat wordt gebruikt als elektronische handtekening zoals bedoeld in de Verordening (EU) nr. 910/2014.
5. Vereisten voor validatie van middelen (authenticatiemiddelen uitgegeven binnen het Stelsel) en elektronische handtekeningen:
    a. Deelnemers aan het stelsel MOETEN er op toezien dat het pseudoniem van de gebruiker wordt verstrekt middels het gebruik van het middel of;
    b. De identificerende gegevens behorende bij het uitgereikte middel worden bij de uitgever van het middel geverifieerd.
    c. De Deelnemer MOET op PKI gebaseerde elektronische handtekeningen valideren d.m.v. de certificatenketen en op basis van actuele informatie over statusintrekkingen.
    d. Niet op PKI gebaseerde handtekeningen MOETEN gevalideerd worden met een validatiemethode van gelijke kwaliteit.

LOA 3	LoA2 met toevoeging van:
	
	1. Identificatie MAG eveneens plaatsvinden met een middel op LoA 3 en hoger dat door een Deelnemer in het stelsel is uitgegeven.
	    i. Restrictie: Met een middel van een specifiek LoA MAG NIET zonder aanvullende validaties een Stelseldienst (middel of machtiging) met een hoger LoA worden verstrekt.
	    ii. Restrictie: Op basis van een middel dat niet voor gebruik in het burgerdomein is uitgegeven MAG NIET zonder aanvullende validaties een middel voor gebruik in het burgerdomein worden verstrekt.
	2. De Deelnemer MOET het fysieke adres valideren als de uitgifte van het middel face-to-face (in person) plaatsvindt op het door de aanvrager opgegeven adres voor uitgifte.
	3. De Deelnemer MOET registreren welke contactgegevens zijn gevalideerd als onderdeel van het uitgifteproces en welke gegevens slechts zijn opgeslagen als comfortinformatie als onderdeel van de algemene bedrijfsvoering.
	4. Fysieke identificatie: een fysieke ontmoeting MOET plaatsvinden tijdens de registratie of tijdens het middelenuitgifteproces.
	
	Identificatie op afstand**:** dit is als alternatief voor de fysieke ontmoeting tijdens de registratie of tijdens het middelenuitgifteproces toegestaan. Dit MOET conform de beschreven normelementen in paragraaf Eisen Identificatie op Afstand..
		Ad 1 Kern van deze norm is dat identificatie bij registratie of uitgifte altijd op het juiste LoA heeft plaats gevonden. Voor een gekwalificeerd certificaat heeft een identificatie op LoA4 plaats gevonden. Ten behoeve van de uitgifte van middelen voor gebruik in het burgerdomein moet altijd een verificatie van het BSN plaatsvinden aan het originele WID van de Aanvrager. Validatie van het BSN moet middels een registratie bij BSNk plaatsvinden.
		
		Ad 2 Validatie van het fysieke adres mag worden opgevat als:
		
		• de deelnemer controleert of het adres voor afgifte gelijk is aan het adres dat is opgegeven door de aanvrager voordat het middel wordt verzonden per aangetekende post. Deze werkwijze is slechts toegestaan in combinatie met een fysieke ontmoeting tijdens het registratieproces. Of;
		• de deelnemer controleert of het adres voor afgifte gelijk is aan het adres voor afgifte van het middel en hij identificeert de ontvanger bij uitgifte van het middel als zijnde de aanvrager. Identificatie kan in dit geval ook plaatsvinden door een besteldienst die in opdracht van de deelnemer het middel in persoon overhandigt aan de aanvrager. Deze werkwijze minimaal bedoeld voor situaties waarbij identificatie van de aanvrager in het aanvraagproces niet heeft plaatsgevonden.
		
		Ad 4 Voorbeelden van geaccepteerde face-to-face controles zijn
		
		• Controle van identiteit door daarvoor opgeleide PostNL-medewerker die het middel komt afleveren
		• Identificatie door een daarvoor opgeleide balie medewerker van de Authenticatiedienst.
		• Identificatie door de Dienstafnemer conform de wettelijke verplichting van werkgevers tot identificatie van personeel.
		    • Nota bene 1: Voor middelen die op basis van identificatie door de werkgever worden uitgegeven moet het technisch onmogelijk zijn dat deze middelen in het BSN domein en consumentendomein gebruikt kunnen worden.
		    • Nota bene 2 Mogelijke zelfverklaring moeten worden uitgesloten. Niet acceptabel is dat wettelijke vertegenwoordigers en machtigingenbeheerders over zichzelf een identiteitsverklaring afgeven.
		• De Dienstafnemer verklaart over de identiteit van de Gebruiker door de Dienstafnemer op grond van de plicht van werkgevers om medewerkers bij in diensttreden te identificeren. Mogelijke zelfverklaring moeten worden uitgesloten. Niet acceptabel is dat een wettelijke vertegenwoordiger en de machtigingenbeheerder over zichzelf een identiteitsverklaring afgeven.
		
		Indirecte vormen van face-to-face identificatie zijn niet zonder meer acceptabel:
		• Identificatie op basis van een eerder uitgegeven persoonsgebonden op hetzelfde of hoger niveau waarbij indertijd face-to-face controle heeft plaatsgevonden
		• Identificatie op basis van een banktransactie.
		
		De verificatie op basis van het resultaat van een geslaagde bankoverschrijving is slechts toegestaan als een additionele verificatie. Het is namelijk niet controleerbaar dat de aanvrager een andere persoon gemachtigd heeft voor zijn bankrekening of zijn inloggegevens heeft gedeeld met een andere persoon.
		
		Ad 5e ii Voor het introductieplateau bevat de set gegevens die aan BSNk moet worden aangeleverd minimaal uit:
		
		• het BSN van de Aanvrager
		• de geboortedatum van de Aanvrager

5. De echtheid van identiteitsbewijzen MOET geverifieerd worden door het origineel van het identiteitsbewijs te controleren op specifiek voor dat identiteitsbewijs unieke en bekende kenmerken waardoor dat document als authentiek kan worden aangemerkt.
    a. Voor validatie van de verklaringen is het tonen van een fysiek en geldig identiteitsdocument vereist.
    b. Minimaal een of meer fysieke kenmerken van de Gebruiker moeten worden geverifieerd aan het identiteitsbewijs.
    c. Verificatie van echtheidskenmerken MOET van worden uitgevoerd door daartoe opgeleid personeel en;
    d. Verificatie MOET worden uitgevoerd in het register voor gestolen of vermiste identiteitsbewijzen.
    e. Additioneel voor de uitgifte van middelen die bedoeld zijn voor het gebruik in het Burgerdomein:
        i. De Deelnemer MOET zorg dragen dat het BSN van de Aanvrager in het originele fysieke WID van de Aanvrager is geverifieerd.
        ii. De Deelnemer MOET de verplichte set gegevens ter verificatie aanleveren aan het BSNk.

	6. Met gebruik van een middel op LoA3 of gekwalificeerd certificaat kan eveneens een nieuw middel worden aangevraagd. In dit geval MOET geverifieerd worden: a. dat de aanvrager daadwerkelijk in bezit is van het middel; b. dat bij gebruik van een middel dat buiten het stelsel is uitgegeven er daadwerkelijk een identificatie op locatie heeft plaatsgevonden bij aanvraag of uitgifte van het middel, c. of dat bij gebruik van een middel dat buiten het stelsel is uitgegeven er een identificatie op afstand heeft plaatsgevonden die MOET voldoen aan de eisen van het afsprakenstelsel eTD of ETSI TS 119 461 bij aanvraag of uitgifte van het middel.	
LOA 4	LoA3 met toevoeging van: 1. Met gebruik van een middel op LoA4 of gekwalificeerd certificaat kan eveneens een nieuw middel worden aangevraagd. In dit geval MOET geverifieerd worden: a. dat de aanvrager daadwerkelijk in bezit is van het middel; b. dat bij gebruik van een middel dat buiten het stelsel is uitgegeven er daadwerkelijk een identificatie op locatie heeft plaatsgevonden bij aanvraag of uitgifte van het middel, of c. dat bij gebruik van een middel dat buiten het stelsel is uitgegeven er een identificatie op afstand heeft plaatsgevonden die MOET voldoen aan de eisen van het afsprakenstelsel eTD of ETSI TS 119 461 bij aanvraag of uitgifte van het middel.	

Eisen Identificatie op Afstand

LoA	Vereiste elementen	Toelichting en good practice
LOA 3	Op LoA3 wordt Identificatie op Afstand toegestaan, waarbij – naast de geldende vereisten inzake de identiteitsvaststelling - in elk geval moet worden voldaan aan de eisen die zijn vermeld op pagina: Eisen Identificatie op Afstand	

2.1.3 Bewijs en verificatie van identiteit (rechtspersoon)

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	• Controledoelstelling: Het machtigingenregister MOET erop toezien dat de vertegenwoordigers van de Dienstafnemer deugdelijk worden geïdentificeerd. • Controledoelstelling: Het machtigingenregister MOET erop toezien dat de Dienstafnemer of de gemachtigde Rechtspersoon deugdelijk wordt geïdentificeerd. • Controledoelstelling: Het machtigingenregister moet erop toezien dat de door de Dienstverlener aangeleverde informatie als feitelijk juist is geverifieerd. • Controledoelstelling: Het machtigingenregister MOET erop toezien dat de bevoegdheden van de vertegenwoordigers van de Dienstafnemer deugdelijk worden geverifieerd. 1. De eerste identificatie van de vertegenwoordigers van de Dienstafnemer MOET conform de vereisten voor identificatie bij uitgifte van LoA1 authenticatiemiddelen (zie paragraaf 2.1.1 en 2.1.2) worden uitgevoerd, OF conform de aangeven alternatieven in punt 4. Dit geldt in het bijzonder voor onder staande vertegenwoordigers: a. De wettelijke vertegenwoordiger(s) van de Dienstafnemer. b. De machtigingenbeheerder die door de wettelijke vertegenwoordiger geautoriseerd is en de machtigingen met betrekking tot de Dienstafnemer administreert. c. De Gevolmachtigde die door de wettelijke vertegenwoordiger geautoriseerd is namens deze te handelen. 2. Het machtigingenregister MOET de Dienstafnemer of de gemachtigde Rechtspersoon registreren. 3. Het machtigingenregister MOET de feitelijke juistheid van de door de aanvrager aangeleverde informatie verifiëren in het Handelsregister van de Kamer van Koophandel alvorens de aanvraag formeel geaccepteerd mag worden. Het volgende MOET ten minste juist zijn: a. Bedrijfsnaam en wettelijke naam van de Dienstafnemer b. Ten minste één vestigingsadres c. Identificatienummers (KvK nummer en RSIN) d. Correspondentieadres	Ad 3 Interpretatie: De gegevens die de aanvrager aandraagt moeten zijn vergeleken met de geregistreerde gegevens in het handelsregister. Van de brongegevens in het handelsregister wordt aangenomen dat zij correct zijn. Indien de deelnemer bij de controle in het handelsregister onjuistheden in de gegevens ontdekt of vermoedt bestaat er geen terug meldplicht, tenzij om een andere reden al een terug meld verplichting van toepassing was op de deelnemer. De geregistreerde vestigingsadressen in het handelsregister zijn niet altijd gelijk aan een correspondentieadres. Waar vestigingsadres en correspondentieadres samenvallen, vervalt de eis voor het verifiëren van het correspondentieadres. In het geval van rechtspersonen zonder vestigingsadres moet in elk geval het correspondentieadres gecontroleerd worden. Ad 3b en d Het vestigings- en/of correspondentieadres wordt gebruikt voor schriftelijke communicatie met de organisatie. Voor uitgifte van het token, zie paragraaf 2.2.2 Uitgifte, uitreiking en activering. Ad 3c: KvK nummer en RSIN MOETEN beide bruikbaar zijn in de Machtigingenregisters om machtigingen te registeren. Niet van toepassing op organisaties die niet beschikken over een KvK-nummer en/of RSIN. In het geval van eenmanszaken wordt ten behoeve van de belastingdienst het BSN van de wettelijke vertegenwoordiger als identificatienummer toegevoegd. Deze situatie is van toepassing vanaf niveau eH3 en wordt beschreven in paragraaf 2.1.4. Ad5 Interpretatie: Indien de dienst niet aan professionals wordt geleverd is deze norm niet van toepassing. Bedoeld worden registers zoals het BIG voor zorgprofessionals, BAR voor advocaten en KNB register voor notarissen. Advies: De opsomming is gebaseerd op de lijst van geregistreerde professionals die willen handelen vanuit of namens hun beroep te vinden in het PKI overheid Programma van eisen deel 3a bij 3.2.5-1.: a. Aangewezen door een Staatssecretaris. Niet voor alle professionals bestaat al een dergelijk register. Ad 4.c Het ANBI Register is uitsluitend digitaal bereikbaar via de beveiligde website van de Belastingdienst "opzoeken ANBI". Ad 4.c.iii het RSIN wordt in het ANBI register van de Belastingdienst vermeld in de kolom RSIN. In de situatie dat een ander nummer dan het RSIN staat vermeld kan dit alternatief niet toegepast worden. Ad 4.c.iiii Het correspondentieadres is te achterhalen via de weblink van de instelling op de ANBI pagina en de daar vermelde contactgegevens.

4. Toegestane alternatieven voor verificatie:
    a. Alternatief 1: Online verificatie in het Handelsregister van de Kamer van Koophandel of voor acceptatie van de aanvraag.
    b. Alternatief 2 (alleen voor eTD2, eTD2+): Verificatie gebaseerd op een origineel uittreksel van het Handelsregister van de Kamer van Koophandel. Op het moment dat de aanvraag geaccepteerd wordt MAG dit uit treksel niet ouder zijn dan 14 dagen (7 dagen is de wettelijk toepasselijke periode voor het aanleveren van wijzigingen in het Handelsregister van de Kamer van Koophandel).
    c. Alternatief 3:
    Verificatie gebaseerd op controle van het ANBI register. De gegevens van de organisatie die aangeleverd worden door de gebruiker MOETEN wor den gecontroleerd bij het ANBI register. Het volgende MOET ten minste juist zijn:
        i. Naam van de instelling
        ii. Vestigingsplaats
        iii. RSIN
        iv. Correspondentieadres
    d. Alternatief 4 (diplomatieke missies en internationale organisaties): Verificatie gebaseerd op controle in PROBAS. De gegevens van de organisatie die aangeleverd worden door de vertegenwoordiger MOETEN worden gecontroleerd in PROBAS. Het volgende MOET ten minste juist zijn:
        i. Voornamen vertegenwoordiger;
        ii. Achternaam vertegenwoordiger;
        iii. Geboortedatum vertegenwoordiger;
        iv. Geboorteplaats vertegenwoordiger;
        v. Bevoegdheid vertegenwoordiger;
        vi. Naam organisatie;
        vii. PROBAS-nummer van de organisatie;
        viii. Vestigings- of correspondentieadres van de organisatie.
5. Het machtigingenregister MOET de aangeleverde identiteitskenmerken verifiëren in het relevante beroepsregister in het geval de aanvrager (beroepsmatig) zich wil registreren als Dienstafnemer. Aanvaardbare bewijsbronnen voor beroepsregistratie in Nederland zijn (limitatief):
    a. Accountants Administratieconsulent;
    b. Advocaat; - Octrooigemachtigde;
    c. Registerloods;
    d. Arts (bijvoorbeeld huisartsen en medisch-specialisten zoals chirurgen en psychiaters);
    e. Tandarts; Apotheker; Verloskundige; Fysiotherapeut;
    f. Verpleegkundige;- Psychotherapeut;
    g. Gezondheidszorgpsycholoog;
    h. Notaris; Kandidaat notaris; Toegevoegd notaris;
    i. Gerechtsdeurwaarder; Waarnemend gerechtsdeurwaarder; Toegevoegd kandidaat gerechtsdeurwaarder
    j. Octrooigemachtigde;
    k. Registeraccountant;
    l. Dierenarts;
    m. Zeevarende;
    n. (Hoofd) Bewaarder; Gemandateerd bewaarder;
    o. Technisch medewerker schepen; Inspecteur Scheepsregistratie
    p. Belastingdeurwaarder; Rijksdeurwaarder.

LOA 2

Zelfde als LoA1 met toevoeging van:

1. Toegestaan als alternatief voor de verificatie van bedrijfsgegevens: Verificatie gebaseerd op een origineel uittreksel van het Handelsregister van de Kamer van Koophandel. Op het moment dat de aanvraag geaccepteerd wordt MAG dit uit treksel niet ouder zijn dan 14 dagen (7 dagen is de wettelijk toepasselijke periode voor het aanleveren van wijzigingen in het Handelsregister van de Kamer van Koophandel).
2. De aanvrager die een aanvraag indient voor een machtiging voor betrouwbaarheidsniveaus LoA2 MOET een wettelijke vertegenwoordiger van de Dienstafnemer zijn, dan wel een Gevolmachtigde.
3. Voor betrouwbaarheidsniveau LoA2 machtigingen MOET de bevoegde vertegenwoordiger geïdentificeerd worden en MOET zijn/haar identiteitsverklaring gevalideerd en geregistreerd worden conform de vereisten voor identificatie bij uitgifte van LoA2 authenticatiemiddelen (zie: paragraaf 2.1.1 en paragraaf 2.1.2) of als alternatief zijn onderstaande vereisten van toepassing op elektronische of niet-elektronische machtigingsaanvragen:
    a. Elektronisch machtigingsaanvragen:
        i. Voor elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden, MOET er een kopie van een geldig identiteitsdocument zoals genoemd onder paragraaf 2.1.1 en een kopie van een rechtsgeldig door een wettelijk vertegenwoordiger van de Dienstafnemer ondertekend formulier bij de aanvraag gevoegd worden, en de handgeschreven handtekeningen onder deze documenten MOETEN geverifieerd worden door het machtigingenregister.
        ii. Aan de hierboven opgesomde vereis ten t.a.v. de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer wordt voldaan wanneer de aanvraag elektronisch is ondertekend door de Dienstafnemer die van een Gekwalificeerde Handtekening gebruik maakt.
        iii. Alternatief: Een andere mogelijkheid is dat de registratie van de unieke kenmerken van de wettelijke vertegenwoordiger geverifieerd MOET worden op basis van het resultaat van een geslaagde bankoverschrijving van een privérekening bij een bank waar de aanvrager dezelfde persoon is als de bankrekeninghouder en waarvoor de financiële instelling bij het openen van de bankrekening de rekeninghouder deugdelijk heeft moeten identificeren, op basis van een geldig identiteitsbewijs.
    b. Niet-elektronisch machtigingsaanvragen:
        i. Voor niet-elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de

Ad 1 Betreft een toegestaan alternatief bij LoA2 punt 3

Ad 3 Toelichting: De bevoegde vertegenwoordigers zijn hier de wettelijke vertegenwoordiger(s), machtigingenbeheerder of andere Gevolmachtigde namens de wettelijke vertegenwoordiger. Het identiteitsdocument moet voorzien zijn van een handtekening zodat de vergelijking van de handtekening met de handtekening op het aanvraagformulier gemaakt kan worden.

Ad 5 Interpretatie: Van de brongegevens in registers waartegen moet worden geverifieerd wordt aangenomen dat deze correct zijn. De gegevens die in de aanvraag worden aangedragen moeten dus in overeenstemming zijn met de brongegevens in de registers.

wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. De aanvraag MOET ondertekend worden door de wettelijke vertegenwoordiger van de Dienstafnemer door middel van een handgeschreven handtekening.

ii. De aanvraag MOET worden voorzien van een kopie van een geldig identiteitsdocument. Deze handgeschreven handtekening op de kopie MOET geverifieerd worden met gebruikmaking van het machtigingenregister.

4. Een Gevolmachtigde MAG een aanvraag voor een machtiging voor betrouwbaarheidsniveaus LoA 2 indienen. Het machtigingenregister MOET de handgeschreven handtekeningen verifiëren op de Volmacht en op de kopie van het identiteitsdocument van de aanvrager (de wettelijke vertegenwoordiger van de Dienstafnemer), of op de kopie van het identiteitsdocument van de Gevolmachtigde en op het aanvraagformulier. Identificatie van de vertegenwoordiger van de Dienstafnemer MOET plaatsvinden, zoals hierboven onder punt 2 omschreven.
5. Het machtigingenregister MOET de Dienstafnemer of de gemachtigde Rechtspersoon registreren.
   a. De aangeleverde en geregistreerde kenmerken van de Dienstafnemer of de gemachtigde Rechtspersoon MOETEN uniek en feitelijk juist zijn. Identificatie MAG op openbare informatie gebaseerd zijn.
   b. Het machtigingenregister MOET de bij 5a. genoemde kenmerken ten minste verifiëren in Het Handelsregister van de Kamer van Koophandel of Beroepsregister.
6. Het machtigingenregister MOET de bevoegdheid van de aanvrager verifiëren in het Handelsregister van de Kamer van Koophandel, of, als alternatief, in aanvullende bewijsstukken, zoals statuten en mandaten. De aanvraag MOET geaccepteerd worden indien:
   a. de aanvraag is ondertekend door een volledig of zelfstandig bevoegde, of een volledig gevolmachtigde vertegenwoordiger;
   b. de aanvraag is ondertekend door minimaal twee gezamenlijk bevoegde vertegenwoordigers en de risicobeoordeling volgens punt 7 is laag;
   c. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning;
   d. de aanvraag is ondertekend door minimaal twee beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de risicobeoordeling volgens punt 7 is laag.
7. Indien de aanvraag is ondertekend door minimaal twee beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de aanvraag wordt geaccepteerd, dan MOET het machtigingenregister met betrekking tot de acceptatie en de mate van bevoegdheid van degenen die ondertekenen een risico-inschatting maken en deze bij de acceptatie van de aanvraag archiveren.

	8. Het machtigingenregister MOET in de aanvraag er schriftelijk op wijzen dat de verantwoordelijkheid ten aanzien van welke wettelijk bevoegde vertegenwoordiger zijn /hun handtekening zet(ten), bij de onderneming zelf berust.	
LOA 3	Zelfde als LoA1 en met toevoeging van: 1. Voor betrouwbaarheidsniveau LoA 3 machtigingen, MOET de bevoegde vertegenwoordiger worden geregistreerd en geïdentificeerd conform de vereisten voor identificatie bij uitgifte van LoA3 authenticatiemiddelen (zie vereisten in paragraaf 2.1.1 en 2.1.2.) of als alternatief zijn de onderstaande vereisten van toepassing: i. De vertegenwoordiger die de aanvraag voor de eerste registratie van de Dienstafnemer bij het machtigingenregister ondertekent voor betrouwbaarheidsniveau LoA3 MOET een wettelijke bevoegde vertegenwoordiger van de Dienstafnemer zijn. ii. Elektronische machtigingsaanvragen: 1. Voor elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. 2. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van ge scande kopieën van het originele aanvraagformulier die door de wettelijke vertegenwoordiger van de Dienstafnemer door middel van een hand geschreven handtekening zijn ondertekend en daarbij gevoegd de bijbehorende gesc ande kopie van het identiteitsdocument van de wettelijke vertegenwoordiger. iii. Niet-elektronisch machtigingsaanvragen: 1. Voor niet-elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van het originele aanvraagformulier en door middel van een handgeschreven handtekening ondertekend door de wettelijke vertegenwoordiger van de Dienstafnemer met de bijbehorende kopie van het identiteitsdocument van de vertegenwoordiger. 2. De handgeschreven handtekening op het aanvraagformulier MOET geverifieerd worden aan de hand van de handtekening op de kopie van het identiteitsdocument.	Ad 1 Toelichting: De bevoegde vertegenwoordigers zijn hier de wettelijke vertegenwoordiger(s) en de machtigingenbeheerders.

	3. De echtheid van identiteitsbewijzen MOET geverifieerd worden, op basis van unieke kenmerken. Er MOET gecontroleerd worden of het identiteitsbewijs (nummer) in de database als gestolen of vermist geregistreerd staat. 2. Het machtigingenregister MOET de bevoegdheid van de aanvrager verifiëren in het Handelsregister van de Kamer van Koophandel, of, als alternatief, in aanvullende bewijsstukken, zoals statuten en mandaten. De aanvraag MOET geaccepteerd worden indien: a. de aanvraag is ondertekend door een volledig of zelfstandig bevoegde, of een volledig gevolmachtigde vertegenwoordiger; b. de aanvraag is ondertekend door meer dan de helft van het totale aantal gezamenlijk bevoegde vertegenwoordigers en de risicobeoordeling volgens punt 3 is laag; c. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning; d. de aanvraag is ondertekend door meer dan de helft van het totaal aantal beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de risicobeoordeling volgens punt 3 is laag. 3. Indien de aanvraag is ondertekend door meer dan de helft van het totaal aantal beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de aanvraag wordt geaccepteerd, dan MOET het machtigingenregister met betrekking tot de acceptatie en de mate van bevoegdheid van degenen die ondertekenen een risico-inschatting maken en deze bij de acceptatie van de aanvraag archiveren. 4. Het machtigingenregister MOET in de aanvraag er schriftelijk op wijzen dat de verantwoordelijkheid ten aanzien van welke wettelijk bevoegde vertegenwoordiger zijn /hun handtekening zet(ten), bij de onderneming zelf berust.	
LOA 4	Zelfde als LoA1 en met toevoeging van: 1. Voor betrouwbaarheidsniveau LoA 4 machtigingen MOET de bevoegde vertegenwoordiger worden geregistreerd en fysiek geïdentificeerd conform de vereisten voor identificatie bij uitgifte van LoA4 authenticatiemiddelen (zie paragrafen 2.1.1 en 2.1.2). Specifiek is hierbij het volgende vereist: 2. De vertegenwoordiger die de aanvraag voor de eerste registratie van de Dienstafnemer bij het machtigingenregister ondertekent voor betrouwbaarheidsniveau LoA 4 MOET een wettelijke bevoegde vertegenwoordiger van de Dienstafnemer zijn. 3. Onderstaande uitdrukkelijke vereisten gelden specifiek voor elektronische of niet-elektronische machtigingsaanvragen: a. Voor niet-elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke	Ad 1 Toelichting: De bevoegde vertegenwoordigers zijn hier de wettelijke vertegenwoordigers. De wettelijke vertegenwoordiger moet bij de aanvraag fysiek verschijnen voor identificatie.

vertegenwoordiger van de Dienst afnemer geregistreerd worden.
   b. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van het originele aan vraagformulier en door middel van een handgeschreven handtekening ondertekend door de wettelijke vertegenwoordiger van de Dienstafnemer met de bijbehorende kopie van het identiteitsdocument van de vertegenwoordiger. De hand geschreven handtekening op het aanvraagformulier MOET geverifieerd worden aan de hand van de handtekening op de kopie van het identiteitsdocument.
   c. De echtheid van identiteitsbewijzen MOET geverifieerd worden, op basis van unieke kenmerken.
   d. Er MOET gecontroleerd worden of het identiteitsbewijs(nummer) in de database als gestolen of vermist geregistreerd staat;
   a. Elektronische machtigingsaanvragen:
      i. Voor elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van gescande kopieën van het originele aanvraagformulier en door middel van een handgeschreven handtekening ondertekend door de wettelijke vertegenwoordiger van de Dienstafnemer met de bijbehorende gescande kopie van het identiteitsdocument van de vertegenwoordiger.
   b. Niet-elektronische machtigingsaanvragen
4. Het machtigingenregister MOET de bevoegdheid van de aanvrager verifiëren in het Handelsregister van de Kamer van Koophandel, of, als alternatief, in aanvullende bewijsstukken, zoals statuten en mandaten.
   a. De aanvraag MOET geaccepteerd worden indien:
      i. de aanvraag is ondertekend door een volledig of zelfstandig bevoegde, of een volledig gevolmachtigde vertegenwoordiger;
      ii. de aanvraag is ondertekend door alle gezamenlijk bevoegde vertegenwoordigers;
      iii. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning;
      iv. de aanvraag is ondertekend door alle beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers van een publieke rechtspersoon.
   b. De aanvraag MOET worden afgewezen indien:
      i. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij NIET expliciet is aangegeven dat de vertegenwoordiger gerechtigd is

	tot het doen van een aanvraag eHerkenning;	

2.1.4 Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	Controledoelstelling: Het machtigingenregister MOET erop toezien dat de betrokkenheid van de vertegenwoordigers met de Dienstafnemer of de tussenpersoon deugdelijk is vastgesteld. 1. De betrokkenheid van de vertegenwoordiger die voor de eerste keer de diensten van het machtigingenregister aanvraagt, met de Dienstafnemer MOET geverifieerd worden door: verificatie van een concreet bedrijfsorganisatorisch kenmerk, zoals bijv. het fysieke postadres, het e-mailadres of het telefoonnummer.	
LOA 2	Hetzelfde als LoA1 en met toevoeging van: 1. Voor private rechtspersonen: a. De betrokkenheid van de aanvrager met de Dienstafnemer MOET worden geverifieerd door het Handelsregister van de Kamer van Koophandel te raadplegen. b. Het machtigingenregister MOET de aangeleverde kenmerken controleren met de geregistreerde kenmerken van de aanvrager in het Handelsregister van de Kamer van Koophandel. 2. Voor publieke rechtspersonen: De betrokkenheid van de aanvrager met de Dienstafnemer MOET worden geverifieerd volgens een van de onderstaande alternatieven: a. Controleer of de identiteitskenmerken van de aanvrager overeenstemmen met het Handelsregister van de Kamer van Koophandel en controleer bestaande beperkingen van de registratie van de machtiging, of anders b. Controleer of de geregistreerde functie in het Handelsregister van de Kamer van Koophandel overeenkomt met de functie van de aanvrager en controleer bestaande beperkingen van de registratie van de machtiging. c. De aanvrager MOET bovendien verklaren (d.m.v. een ondertekend document) dat hij /zij deze functie op het tijdstip van de aanvraag voor het machtigingenregister bekleedt, of anders d. Overeenkomstig het 'Protocol voor controle van interne mandaatbesluiten' dient de aanvrager een document in waarin verklaard wordt dat hij/zij bevoegd is namens de publieke Rechtspersoon een aanvraag te	Ad 1 Interpretatie: De gegevens die de aanvrager aandraagt moeten zijn vergeleken met de geregistreerde gegevens in het handelsregister. Van de brongegevens in de KvK register wordt aangenomen dat zij correct zijn. Indien de deelnemer bij de controle in het handelsregister onjuistheden in de gegevens van het handelsregister ontdekt of vermoedt bestaat er geen terugmeldplicht, tenzij om een andere reden al een terugmeldverplichting van toepassing was op de deelnemer. Ad 1c t/m 1f. Interpretatie (principiële afspraak): De aanvrager moet de onbeperkte bevoegdheid hebben om de organisatie te vertegenwoordigen inzake registratie bij het machtigingenregister. De geregistreerde bevoegdheden in het handelsregister kunnen verschillende soorten beperking bevatten zoals financiële beperkingen, beperkingen in type transacties of vormen van gezamenlijke bevoegdheid aangeven. Bij de beperking 'gezamenlijke bevoegdheid' kan de wilsuiting bestaan uit een door alle, in het Handelsregister opgenomen, gezamenlijk bevoegde bestuurders getekende verklaring die de vertegenwoordiger machtigt tot handelen. In het Handelsregister moet het MR de juistheid van de betreffende bestuurders verifiëren. Indien het MR de aanvraag teruglegt bij de aanvrager met het verzoek bewijs aan te leveren over de bevoegdheid van de aanvrager, kan deze bewijsvoering aangeleverd worden in de vorm van: • statuten • opgave (door organisatie bij) KvK • (intern) mandaat • instellingsbesluit(en) • aanstellingsbrief Voor het opstellen van generieke afwegingskaders kan gedacht worden aan: • de beoordeling van de beperking in relatie tot de strekking van de machtiging (dienst)* • ondertekening door meerdere in de KvK opgenomen (beperkt)bevoegd vertegenwoordigers * De Handreiking Betrouwbaarheidsniveaus van ForumStandaardisatie geeft richting aan Dienstverleners die op het Stelsel willen aansluiten bij het bepalen van het juiste LoA van hun dienst. Ad 1a Kerkgenootschappen zijn een bijzondere vorm van private organisaties zoals weergegeven in BW boek 2 artikel 2. Validatie van de bevoegdheden van de wettelijke vertegenwoordiger en zijn associatie met het Kerkgenootschap bij de KvK is niet mogelijk. Namen van bestuurders en kerkleden mogen niet worden gepubliceerd. 1. Kerkgenootschappen of hun koepelorganisatie MOETEN in zijn ingeschreven bij de Kamer van Koophandel om te kunnen worden geregistreerd bij het MR. Het MR MOET het vestigingsadres dat door de aanvrager wordt opgegeven valideren aan het vermelde vestigingsadres in het handelsregister. 2. Indien de aanvraag een stichting, vereniging of vennootschap betreft die onderdeel uitmaakt van een kerkgenootschap MOET de registratie op naam worden gesteld van- en beperkt tot die stichting, vereniging of vennootschap. De MR volgt de voor deze organisatievormen bestaande regels.

doen voor het Machtigingenregister.
   e. Publieke rechtspersonen kunnen uit meerdere onderdelen bestaan met duidelijk te onderscheiden taken. Het machtigingenregister MOET de daadwerkelijke reikwijdte van de aanvraag controleren. Als de reikwijdte beperkt is tot een bepaald organisatorenonderdeel /vestiging MOETEN de machtigingen eveneens tot dat bepaalde organisatorenonderdeel / die bepaalde vestiging beperkt zijn.
3. Het machtigingenregister MOET de onderstaande functionaliteit bieden:
   a. Registratie van een machtigingenbeheerder
   b. Registratie en beheer van bevoegdheden door de machtigingenbeheerder
4. Het Machtigingenregister registreert één of meerdere personen in de rol van Machtigingenbeheerder:

   a. De wettelijke vertegenwoordiger(s) stelt een persoon in de rol van machtigingenbeheerder aan.

   b. De Machtigingenbeheerder heeft de bevoegdheid om namens/als de wettelijke vertegenwoordiger(s) machtigingen te laten registreren bij de machtigingenregister.

   c. Indien de wettelijke vertegenwoordiger geen andere persoon in de rol van machtigingenbeheerder wenst aan te stellen, vervult de wettelijke vertegenwoordiger de rol van machtigingenbeheerder.

   d. De machtigingenbeheerder wordt, voordat hij een beheerdersmachtiging krijgt, door de machtigingendienst geïdentificeerd op een betrouwbaarheidsniveau dat op zijn minst gelijk is aan het hoogste betrouwbaarheidsniveau van de machtigingen die de wettelijke vertegenwoordiger wil kunnen laten registreren (de reikwijdte) door de machtigingenbeheerder.

   e. De reikwijdte wordt bepaald door de diensten van een beheerdersmachtiging en/of het betrouwbaarheidsniveau van een beheerdersmachtiging.

   e. Een machtigingenbeheerder heeft de bevoegdheid andere machtigenbeheerders te registreren.
5. machtigingenbeheerder heeft onderstaande bevoegheden:

3. De persoon die het Kerkgenootschap vertegenwoordigt MOET worden geïdentificeerd conform bestaande stelselregels voor de persoon van wettelijke vertegenwoordiger. Zijn bevoegdheden MOETEN worden beoordeeld conform de bestaande stelselregels.

   Additioneel slechts voor LoA2
   Alternatief 1:
4. De (wettelijke) vertegenwoordiger van het Kerkgenootschap MOET een statuut overleggen waarin de wettelijke vertegenwoordigers (bestuursleden) en hun mandaat is opgenomen en;
5. De (wettelijke) vertegenwoordiger overlegt een verklaring die is ondertekend door minimaal de bestuursleden aangevuld met kerkleden (in totaal minimaal 5) dat hij mag optreden als wettelijke vertegenwoordiger. Als alternatief voor de verklaring mag het MR additioneel bewijs accepteren zoals een banktransactie waarmee de vertegenwoordiger aantoont dat hij de beschikking heeft over een bankrekening op naam van het Kerkgenootschap aangevuld met ander bewijs, notulen en agenda's van vergaderingen waaruit de geclaimde bevoegdheid blijkt.
6. Het MR MOET de associatie van de vertegenwoordiger valideren aan de hand van het overlegde statuut en de getekende verklaring.

   Alternatief 2:
7. De koepelorganisatie van het kerkgenootschap, geregistreerd in het handelsregister, MOET met een formele brief aan de MR, het bestaan van het Kerkgenootschap en de bestuurssamenstelling bevestigen en de verantwoordelijkheid op zich voor de juistheid van deze bevestiging nemen.
8. Het MR verifieert de KvK nummer en vestigingsplaats van de koepelorganisatie aan het handelsregister.

   Alternatief 3:
9. De gebruiker levert gegevens van het kerkgenootschap die de gebruiker wil vertegenwoordigen op aan het MR.
10. Het MR controleert deze gegevens bij het ANBI register (uitsluitend digitaal bereikbaar via de beveiligde website van de Belastingdienst "opzoeken ANBI").
11. Het MR neemt contact op met de contactpersoon van het kerkgenootschap zoals deze is geregistreerd in het ANBI register. Deze contactpersoon MOET sc hriftelijk bevestigen dat de gebruiker gerechtigd is om namens het kerkgenootschap op te treden.

    Ad 2 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:
12. het mandaatbesluit wordt door degene die opgave doet verstrekt
13. degene die opgave doet duidt aan op basis van welke in het mandaatbesluit genoemde functie hij de opgave doet
14. degene die opgave doet verklaart dat hij op moment van aanvragen daadwerkelijk in betreffende functie is aangesteld
15. het machtigingenregister MOET de betrouwbaarheid van het mandaatbesluit controleren. 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 MOET 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.
16. Het verstrekte en gecontroleerde mandaatbesluit MOET worden gearchiveerd voor de duur van tenminste 7 jaar.

Ad 3 Interpretatie: In de praktijk valt op niveau LoA 1 de rol van machtigingenbeheerder en gemachtigde samen. De beheerdersrol wordt niet aangewezen door de wettelijke vertegenwoordiger van de dienstafnemer en de machtiging kan dus ook zonder toestemming van de wettelijke vertegenwoordiger worden aangevraagd op niveau LoA 1.

Ad 4.

Een bestaande machtigingenbeheerder waarvan tussentijds de organisatie failliet of in surseance van betaling is, mag geen machtigingen registreren. Ook de wettelijk vertegenwoordiger van een vennootschap kan en mag niet meer handelen en machtigingen registreren. De curator is verantwoordelijk voor lopende contracten en hij/zij moet actie ondernemen om te voorkomen dat machtigingenbeheerders en wettelijk vertegenwoordigers machtigingen registreren. Er is geen proactieve controle van de Deelnemer nodig.

	a. De machtigingenbeheerder MAG machtigingen registreren en verlengen binnen de reikwijdte van de toegekende beheerdersmachtiging. b. De machtigingenbeheerder MAG beheerdersmachtigingen voor andere machtigenbeheerders registreren op het betrouwbaarheidsniveau waarvoor de machtigingenbeheerder gemachtigd is, of op een lager betrouwbaarheidsniveau. c. De machtigingenbeheerder MAG machtigingen voor zichtzelf registreren op het betrouwbaarheidsniveau waarvoor de machtigingenbeheerder gemachtigd is, of op een lager betrouwbaarheidsniveau. 6. Verlenging van een beheerdersmachtiging moet voldoen aan onderstaande eisen: a. Een machtigingenbeheerder MAG NIET zijn eigen beheerdersmachtiging verlengen. b. Verlenging door een wettelijk vertegenwoordiger MOET worden gedaan zoals beschreven onder Ad 4. c. Verlenging door een tweede machtigingenbeheerder MAG onder voorwaarden. De tweede machtigingenbeheerder MOET op zijn minst over een beheerdersmachtiging beschikken die een reikwijdte heeft overeenkomstig Ad 4e. 7. De machtigingenbeheerder MOET geauthenticeerd worden voor dat hij toegang tot het machtigingenregister krijgt.	De bevoegdheid van de machtigingenbeheerder bij organisaties die zijn uitgeschreven uit het handelsregister van de Kamer van Koophandel vervalt. De verantwoordelijkheid hiervoor ligt bij de wettelijk vertegenwoordiger. Er is geen proactieve controle van de Deelnemer nodig.
LOA 3	Hetzelfde als LoA2 met toevoeging van: 1. De betrokkenheid van de aanvrager bij een private rechtspersoon vereist in geval van een Kerkgenootschap additionele verificaties. 2. Indien de bedrijfsvorm een eenmanszaak is, dan gelden de volgende bepalingen: a. de volgende gegevens op het getoonde WID document moeten overeenkomen met de gegevens op het uittreksel van de Kamer van Koophandel: i) De voorletters van de eigenaar ii) De achternaam van de eigenaar iii) Geboortedatum van de eigenaar iv) Geboorteplaats van de eigenaar b. Als aan bepaling 3a is voldaan, dan MOET het BSN worden overgenomen uit het WID	Ad 1 Additioneel voor LoA3 Alternatief 1: 1. De (wettelijke) vertegenwoordiger van het kerkgenootschap MOET een door een notaris gewaarmerkt statuut overleggen waarin de wettelijke vertegenwoordigers (bestuursleden) en hun mandaat zijn opgenomen. 2. Het MR MOET het bestaan en de juistheid van het statuut verifiëren bij de betreffende notaris. Alternatief 2: 1. De (wettelijke) vertegenwoordiger van het kerkgenootschap MOET een statuut overleggen waarin de wettelijke vertegenwoordigers (bestuursleden) en hun mandaat zijn opgenomen. 2. De (wettelijke) vertegenwoordiger MOET een verklaring overleggen die is ondertekend door minimaal 5 leden dat hij mag optreden als wettelijke vertegenwoordiger. 3. De koepelorganisatie van het kerkgenootschap, geregistreerd in het handelsregister, MOET met een formele brief aan het MR het bestaan van het kerkgenootschap en de bestuurssamenstelling daarvan bevestigen. De koepelorganisatie neemt daarmee de verantwoordelijkheid op zich voor de juistheid van deze bevestiging. 4. De MR verifieert de KvK nummer en vestigingsplaats van de koepelorganisatie in het handelsregister. 5. Als alternatief voor de verklaring van de koepelorganisatie mag het MR additioneel bewijs accepteren zoals een bewijs dat de vertegenwoordiger de beschikking heeft over een bankrekening op naam van het kerkgenootschap aangevuld met notulen en agenda's van vergaderingen waaruit de geclaimde vertegenwoordigingsbevoegdheid blijkt.

	document en geregistreerd als het 'identificatienummer' van de onderneming. 3. Indien een eenmanszaak reeds gebruik maakt van de diensten van een Machtigingenregister en het BSN van de eigenaar van de eenmanszaak is nog niet bekend bij het Machtigingenregister, dan kan het BSN worden geregistreerd middels authenticatie met het eTD-identificatiemiddel van de eigenaar, of een formulier met de handschreven handtekening van de eigenaar. In beide gevallen dient een document zoals gespecificeerd onder sub a of sub b te worden aangeleverd: a. een kopie WID met zichtbaar BSN van de eigenaar van de eenmanszaak. b. een gewaarmerkt uittreksel bevolkingsregister, niet ouder dan 6 maanden, van de eigenaar van de eenmanszaak, waarop is vermeld: BSN, naam, geboorteplaats en geboortedatum.	Alternatief 3: 1. De MR MOET een bezoek afleggen aan het kerkgenootschap op het vestigingsadres dat in het handelsregister staat vermeld. 2. De MR MOET de vertegenwoordigingsbevoegdheid van de aanvrager valideren aan de hand van de geschreven verklaring van alle bestuursleden of minimaal de bestuursleden aangevuld met kerkleden (in totaal minimaal 5) én de mondelinge verklaring van minimaal 1 aanwezig mede bestuurslid. Als alternatief voor aanwezigheid van het mede bestuurslid mag het MR additioneel bewijs accepteren zoals een bewijs dat de vertegenwoordiger de beschikking heeft over een bankrekening op naam van het kerkgenootschap aangevuld met notulen en agenda's van vergaderingen waaruit de geclaimde vertegenwoordigingsbevoegdheid blijkt. 3. De aanvrager en het mede bestuurslid MOETEN zich identificeren met hun WID conform de bestaande regels voor identificatie. 4. De MR MOET de namen van de bestuursleden valideren aan het statuut aan de betreffende persoonskenmerken in het betreffende WID. 5. De MR legt alle uitgevoerde valuaties en verificaties vast t.b.v. de audit-trail. Toelichting bij punt 2: Interpretatie: Vormen van bijzondere omstandigheden zijn bijvoorbeeld 'bankroet' of 'uitstel van betaling'. Het gaat erom dat gecontroleerd wordt of er sprake is van bijzondere omstandigheden én of deze omstandigheden beperkingen meebrengen voor de vertegenwoordigingsbevoegdheid of handelingsbevoegdheid. Toelichting bij punt 3: Het BSN wordt geregistreerd als extra identificatienummer bij de identificatienummers van de onderneming die in paragraaf 2.1.3 zijn aangegeven. De belastingdienst behandelt een eenmanszaak als 'burger' en verwerkt in dat geval het BSN en niet de KvK nummer. Toelichting bij punt 3b: Deze termijn is gebaseerd op een advies van de rijksoverheid: Hoe lang is een uittreksel uit het bevolkingsregister geldig? | Rijksoverheid.nl Alternatief 4: 1. Zelfstandige onderdelen van kerkgenootschappen, dan wel parochies, MOETEN zijn ingeschreven in het handelsregister van de Kamer van Koophandel om te kunnen worden geregistreerd bij het machtigingenregister. 2. De aanvraag voor een LoA3 machtiging MOET worden ondertekend door een tekenbevoegd vertegenwoordiger van het landelijke kerkgenootschap, dan wel bisdom. 3. De koepelorganisatie van de landelijke kerkgenootschappen en bisdommen (CIO) MOET zorgdragen dat alle Machtigingenregisters eHerkenning beschikken over een gewaarmerkte lijst met identificerende kenmerken van de vertegenwoordigers die de bij 2 genoemde aanvraag mogen ondertekenen. Deze lijst bevat minimaal de volgende gegevens: a. voorna(a)m(en) en/of voorletter(s) en achternaam; b. functie; c. handtekening. 4. De koepelorganisatie van de landelijke kerkgenootschappen en bisdommen MOET zorgdragen dat: a. minstens ieder kwartaal de bij onderdeel 3 genoemde lijst wordt gecontroleerd op actualiteit; b. bij wijzigingen in de bij onderdeel 3 genoemde lijst, de Machtigingenregisters de gewijzigde lijst ontvangen. 5. De verantwoordelijkheid voor actualiteit en correctheid van de bij onderdeel 3 genoemde lijst ligt bij de volgende twee partijen: a. de koepelorganisatie van de landelijke kerkgenootschappen en bisdommen; b. de landelijke kerkgenootschappen en bisdommen. 6. Het Machtigingenregister MOET bij ontvangst van de bij onderdeel 3 genoemde lijst het waarmerk controleren. 7. De tekenbevoegd vertegenwoordiger van het landelijke kerkgenootschap, dan wel bisdom, MOET worden geïdentificeerd conform bestaande stelselregels voor de persoon van wettelijke vertegenwoordiger. Alternatief 5: 1. De eisen bij Sub 1, 3, 4, 5, 6 en 7 van Alternatief 4 zijn van toepassing. 2. De (wettelijke) vertegenwoordiger van het kerkgenootschap MOET een verklaring overleggen waarin het bestaan van het lokale kerkgenootschap wordt bevestigd en de "gedelegeerde" wettelijk vertegenwoordigers (indien

		mogelijk op functieniveau) worden benoemd die aanvragen voor eHerkenningsmiddelen en -machtigingen voor het betreffende lokale kerkgenootschap ter goedkeuring mogen ondertekenen. Deze verklaring heeft de volgende vorm: a. De verklaring staat op briefpapier van het (overkoepelende) kerkgenootschap b. Er is een referentiecode (afkorting) opgenomen welke verwijst naar het overkoepelende kerkgenootschap c. De verklaring is ondertekend door een wettelijk vertegenwoordiger van het landelijke kerkgenootschap die is opgenomen op de gewaarmerkte "Lijst CIO-kerken eHerkenning 3". Elektronische ondertekening is hierbij toegestaan d. De verklaring bevat minimaal de volgende gegevens: i. de naam en KvK nummer van het betreffende lokale kerkgenootschap ii. de naam en KvK nummer van de koepelorganisatie (landelijke kerkgenootschap) iii. de bevoegdheden van het lokale kerkgenootschap iv. de functies en/of personen binnen het lokale kerkgenootschap welke worden benoemd als "gedelegeerd" wettelijk vertegenwoordiger v. de bevoegdheden van de "gedelegeerde" wettelijke vertegenwoordigers 3. De (wettelijke) vertegenwoordiger MOET een verklaring overleggen waarin staat dat de aanvrager namens het lokale kerkgenootschap een eHerkenningsmiddel en -machtiging toegekend mag worden. Deze verklaring heeft de volgende vorm: a. De verklaring staat op briefpapier van het lokale kerkgenootschap b. Er is een verwijzing opgenomen naar de verklaring die is beschreven in Sub 2, zodat daarmee een koppeling gemaakt kan worden c. Er is een referentiecode (afkorting) opgenomen welke verwijst naar het overkoepelende kerkgenootschap d. De verklaring bevat minimaal de volgende gegevens van zowel de aanvrager van het eHerkenningsmiddel en -machtiging, de voor akkoord verklarende "gedelegeerde" wettelijk vertegenwoordiger(s), als van de verklarende kerkleden: i. Naam, adres, woonplaats (NAW gegevens) ii. Functie iii. Geboortedatum iv. Documentnummer WID v. Documenttype WID e. De verklaring is door zowel de aanvrager, de bevestigende "gedelegeerde" wettelijk vertegenwoordiger(s), als door de verklarende kerkleden ondertekend. In totaal hebben er minimaal 5 kerkleden getekend. Hierbij is het toegestaan dat de aanvrager en/of "gedelegeerd" wettelijk vertegenwoordigers ook ondertekenen als kerklid. 4. Het MR verifieert het KvK nummer en vestigingsplaats van de koepelorganisatie en het plaatselijke kerkgenootschap in het handelsregister.
LOA 4	Hetzelfde als LoA3 met toevoeging van: 1. De registratie van private rechtspersonen bij het machtigingenregister kent één beperking met betrekking tot Kerkgenootschappen.	Ad 1 De registratie van een Kerkgenootschap op LoA4 MOET door het MR worden uitgesloten vanwege het ontbreken van gezaghebbende bronnen voor het uitvoeren van validaties.

2.2 Beheer van elektronische identificatiemiddelen

2.2.1 Kenmerken en ontwerp van elektronische identificatiemiddelen

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Het authenticatiemiddel MOET tenminste een wachtwoord of PIN zijn, (a) gekozen door de gebruiker of (b) automatisch gegenereerd.	Wachtwoorden die wel voldoen aan de eisen voor sterke wachtwoorden MOGEN ook gebruikt worden op niveau LoA1.
LOA 2	Hetzelfde als LoA 1 met toevoeging van: 1. Als de authenticatiesessie een wachtwoord omvat dat in de browser van de gebruiker wordt ingevoerd dan MOET dat wachtwoord een zogenaamd ‘afgedwongen’ en ‘sterk’ wachtwoord of betreffen.	De invulling van deze norm MOET in sterkte minimaal en aantoonbaar gelijkwaardig zijn aan de good practice die is aangegeven: Het wachtwoord: • MOET ten minste 8 letters bevatten; • MOET ten minste 1 kleine letter bevatten [a-z]; • MOET ten minste 1 hoofdletter bevatten [A-Z];

		• MOET ten minste 1 cijfer bevatten [0-9];
		• MOET ten minste 1 bijzonder teken bevatten [- _ ! $ % & ' . = / \ : < > | ? @ [ ] ^ ` { } ~]
		• MAG NIET de gebruikersnaam bevatten;
		• MAG NIET gelijk zijn aan een van de 5 eerder gebruikte wachtwoorden.
		
		Of;
		
		• MOET gebruikmaken van wachtwoordzinnen bestaande uit:
		  • zowel hoofdletters als kleine letters en;
		  • eventueel ook andere tekens en;
		  • minimaal een zinlengte van 20 tekens
		
		In het geval van multifactormiddelen moet de sterkte van de wachtwoordcomponent in de risicocontext worden bepaald.
		Multifactor-authenticatie is alleen op LoA3 en LoA4 en vereiste. Het Stelsel kent echter ook een variant op LoA2 (eTD 2+) waar multifactor-authenticatie een vereiste is.

LOA 3	Hetzelfde als LoA2 met toevoeging van:
	
	1. De authenticatie MOET het gebruik van minimaal twee van de volgende authenicatiefactoren omvatten:
	  a. kennis van de gebruiker,
	  b. uniek bezit van de gebruiker, of
	  c. een biometrische eigenschap van de gebruiker.
	2. Het authenticatiemiddel MOET slechts een response geven na een expliciete handeling van de Gebruiker. De handeling van de Gebruiker MOET buiten de werkingssfeer van de applicatie (o.a. browser) plaatsvinden.
	
	Implementatietermijn
	Voor punt 1 en 2 geldt:
	
	Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.
	
	De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.
		Ad 2 Toelichting:
		
		Dit betekent dat:
		
		• de Gebruiker op betrouwbare wijze informatie wordt getoond die bevestigd moet worden met een response van de Gebruiker, of;
		• de gebruiker voert zelf informatie in op middel en maakt zo deel uit maakt van de response.
		
		In deze eis bedoelde handelingen van de Gebruiker zijn bijvoorbeeld:
		
		• Het door de gebruiker invoeren van een ontvangen OTP die op een ander device dan waar het op is ontvangen wordt ingevoerd in de applicatie;
		• Het door de gebruiker invoeren van een PIN op een separate cardlezer waarmee het certificaat als authenticatiefactor wordt ingezet;
		• Het door de gebruiker presenteren en laten 'lezen' van zijn biometrische kenmerk als authenticatiefactor.
		
		Indien zowel de authenticatie-afhandeling als de inlog op het zelfde device kan plaats vinden moet de MU/AD dit risico-gedetecteerd hebben en compenserende maatregelen treffen zoals:
		
		• het de gebruikers wijzen op de risico's van het gebruik van het zelfde device voor de inlog via de browser en risico voor de ontvangst en gebruik van de informatie die nodig is voor de afhandeling van de authenticatie.
		
		Voorbeeldsituaties:
		
		• Inloggen via browser van een smartphone en ontvangst en gebruik op het zelfde toestel van een sms-code voor de afhandeling van de authenticatie.
		• Inloggen via de browser van een tablet waar ook de OTP app op staat.

LOA 4	Hetzelfde als LoA3 met toevoeging van: 1. Het correct functioneren van het authenticatiemiddel moet weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'High attacker' potentieel in de zin van Annex B van de Common Criteria (ISO 1508-3 en evaluatie norm ISO/IEC 18045).	Ad 1 Toelichting: De eis omvat de doelstellingen: • het middel MAG NIET gebruikt kunnen worden zonder expliciete actie van de gebruiker in lijn met het multi-factor gebruik; • het middel MAG NIET andere gegevens bevestigen dan wat de gebruiker verwacht; De toekomstige response van het middel MAG NIET vooraf te bepalen zijn; • Specifiek voor LoA3: Het middel MAG NIET bij eventueel klonen in combinatie met het authenticatiemechanisme bruikbaar zijn.. • Specifiek voor LoA4: Het middel MAG NIET te klonen zijn.

		De wijze waarop conformiteit met deze eis moet worden aangetoond is aangegeven in paragraaf 2.4.7 Compliance en Audit.

2.2.2 Uitgifte, uitreiking en activering

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Deelnemer MAG NIET de eenmaal uitgegeven tokens aan een andere identiteit koppelen (geen hergebruik van pseudoniemen/usernames); a. Deelnemer MOET om dit aan te tonen gedocumenteerde procedures hebben voor het gecontroleerd uitgeven van tokens, wijzigen van identificerende gegevens en het vastleggen van uitgiftes/wijzigingen (AO /IC).	
LOA 2	1. Tokens met betrouwbaarheidsniveaus 2 MOETEN met een lichte verificatie van de identificerende gegevens van de Aanvrager (bijv. naam en /of adres) worden verkregen. Onderstaande vereisten zijn in het bijzonder van toepassing: 2. Een door de uitgever van het token aangemaakte gebruikersnaam en wachtwoord MOET separaat verzonden worden met gebruikmaking van een 'buiten de bandprocedure' naar een van tevoren tijdens het registratieproces door de Aanvrager aangegeven plaats. 3. Een token dat rechtstreeks van internet is gedownload door de Aanvrager na het volgen van de registratieprocedure komt tot stand door een link door te geven naar een plaats die de Aanvrager tijdens het registratieproces heeft opgegeven; in dat geval MOET de link na 24 uur verlopen zijn. 4. De Deelnemer MOET de Gebruiker op de hoogte brengen van het procesverloop van aanvraag tot uitgifte van het middel. 5. De Deelnemer MOET de Gebruiker notificeren dat een middel op zijn naam is uitgegeven. 6. De Deelnemer MOET de Gebruiker notificeren van de uitgifte via een kanaal dat betrouwbaar is geassocieerd met de voornaam en achternaam van de gebruiker.	Ad 1 en 2: Indien het om een middel gaat dat slechts in de context van de Dienstafnemer kan worden gebruikt mag het adres waar naar het token wordt gezonden door de Dienstafnemer worden opgegeven. Ad 4, 5 en 6 Toelichting: Doelstelling van deze eisen is: • De Gebruiker wordt in staat gestelde om de naam van de Authenticatiedienst waar hij het middel heeft aangeschaft te bewaren ter herinnering voor later gebruik. • De Gebruiker wordt in staat gesteld afwijkingen in het proces van uitgifte van een middel te detecteren. • De Gebruiker wordt in staat gesteld om te vast te stellen dat er een middel terecht op zijn naam is uitgegeven. Good practice: Voorbeelden van notificaties: • Het verzenden van een bericht (email of brief) aan de Gebruiker dat bewaard kan worden ter herinnering. In het bericht is de naam van de AD waar het middel is geregistreerd opgenomen. Deze practice geeft daarnaast alleen bescherming bij een aanvraag voor een tweede middel op naam van de gebruiker. • Het gebruik van een mededeling in een terugboeking door AD/MU van een eerdere betaling door Gebruiker met een bankrekening op de opgegeven voor- en achternaam. Deze maatregel geeft enige bescherming bij toepassing voor nieuwe als bestaande Gebruikers, op voorwaarde dat de tenaamstelling van de bankrekening overeenkomt met de naam op het WID. • Het verzenden van een brief naar een adres dat is gekoppeld aan de voor en achternaam van de Gebruiker. Het adres is geverifieerd aan een origineel uittreksel uit de BPR dat de gebruiker heeft overhandigd. Ad 6: Toelichting: De betrouwbaarheid van de associatie met de voornaam een achternaam van de gebruikers neemt toe naarmate de validatie van de associatie onafhankelijker van het registratieproces uitgevoerd kan worden.
LOA 3	Het token wordt met een gemiddelde verificatie van de identificerende	Onderstaande voorbeelden verduidelijken dit type uitgifte van een token:

	gegevens van de aanvrager (bijv. naam en/of adres) verkregen.	Het token wordt per aangetekende post verzonden na voorafgaande validatie van het opgegeven adres bij een officiële identiteitsdatabase waar dit fysieke adres geregistreerd staat. Dit betekent: a) Het token wordt verzonden naar adres van de Dienstafnemer dat in het Handelsregister is opgenomen geadresseerd aan de Gebruiker, Machtigingenbeheerder of de Wettelijke vertegenwoordiger of; b) Het token wordt verzonden naar het adres van de Gebruiker zoals dit door de Dienstafnemer is opgegeven. Het risico dat het niet de bevoegde vertegenwoordiger(s) van de Dienstafnemer is die verzocht heeft om de uitgifte van het middel moet worden gemitigeerd. Acceptabele mitigerende maatregelen zijn in elk geval: i. In het geval het verzoek is gedaan door 1 wettelijke vertegenwoordiger of machtigingenbeheerder heeft verzocht om de uitgifte van het middel. Moet de Dienstafnemer van de verzending worden genotificeerd middels een brief naar het adres van de Dienstafnemer dat in het Handelsregister is opgenomen met het verzoek te reageren indien de uitgifte ongedaan gemaakt moet worden. De brief is gesteld geadresseerd aan de Machtigingenbeheerder of Wettelijke vertegenwoordiger van de Dienstafnemer. Alternatief voor een persoonlijke brief is een mail aan de in b) genoemde vertegenwoordigers op hun persoonlijke mailadres in het geverifieerde domein van de Dienstafnemer. ii. In het geval 2 wettelijke vertegenwoordigers, machtigingenbeheerders of een combinatie daarvan het verzoek hebben gedaan is de notificatie aan de dienstafnemer zoals bedoeld bij punt b) i. geen verplichting. c) Het token wordt verzonden naar het adres dat is gekoppeld aan de voor en achternaam van de Gebruiker. Het adres is geverifieerd aan een origineel uittreksel uit de BRP. Alternatieven a) en b) mogen gebruikt worden voor middelen die slechts bruikbaar zijn in de context van de Dienstafnemer. De authenticatiefactoren van het authenticatiemiddel worden gescheiden in tijd verzonden of worden via verschillende communicatiekanalen verzonden. Het is denkbaar dat voor de verzending van de verschillende authenticaticatiefactoren een combinatie van hetgeen onder a) en b) is gesteld wordt gebruikt. Indien een van de authenticatiefactoren naar het email adres van de gebruiker wordt verzonden moet dit email adres zijn geverifieerd. Opgave van het email-adres door de Dienstafnemer op een met b) vergelijkbare wijze is toegestaan mits de gebruiker juistheid van het email-adres voorafgaande aan de verzending van de authenticatiefactor heeft bevestigd. Het token is gedownload van internet nadat het verzoek om een verklaring door de aanvrager ondertekend is met een gekwalificeerde handtekening in overeenstemming met de voorwaarden van de Richtlijn elektronische handtekeningen en geverifieerd door een CSP. Onmiddellijk na de verificatie MOET het token snel aangemaakt worden door de CSP en op de browser van de aanvrager worden gedownload. Het token wordt rechtstreeks door de aanvrager gedownload na het invoeren van een persoonlijk wachtwoord dat aan de aanvrager is uitgereikt tijdens de registratie op ten minste niveau 3.
LOA 4	1. Tokens met betrouwbaarheidsniveau 4 MOETEN met een zware aanvangsverificatie van de identificerendegegevens van de Aanvrager worden verkregen. Onderstaande vereisten zijn in het bijzonder van toepassing: a. De token MOET persoonlijk aan de Aanvrager worden afgegeven, na validatie van de identiteit van de Aanvrager; of; b. de token MOET naar de Aanvrager verzonden en geactiveerd worden na validatie van diens identiteit door fysieke registratie.	

2.2.3 Schorsing, herroeping en reactivering

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2	1. De Deelnemer MOET een werkend proces hebben voor het intrekken van authenticatiemiddelen. 2. Het resultaat van het proces MOET zijn dat een ingetrokken authenticatiemiddel niet meer gebruikt kan worden in het Stelsel. 3. De Deelnemer MAG (optioneel) de mogelijkheid tot schorsing van een authenticatiemiddel aanbieden 4. De deelnemer die het authenticatiemiddel heeft verstrekt MOET het middel intrekken of schorsen ingeval: a. Een verzoek tot intrekking of schorsing is gedaan door de Gebruiker van het authenticatiemiddel; b. Een verzoek tot intrekking of schorsing is gedaan door een vertegenwoordigingsbevoegde van de Gebruiker van het authenticatiemiddel. c. Het middel blijkt te zijn gecompromitteerd; d. Het middel aantoonbaar kwetsbaar is geworden voor manipulatie of misbruik; e. De Gebruiker van het authenticatiemiddel zijn gebruiksverplichtingen niet nakomt. 5. Indien een bevoegde vertegenwoordiger van de Gebruiker verzoekt om schorsing van het middel MOET de Deelnemer aan de vertegenwoordigingsbevoegde duidelijk maken dat de Gebruiker in staat zal zijn om het middel te heractiveren als deze zijn mogelijkheden tot heractivatie in bezit behoudt. 6. De Deelnemer MOET aan kunnen tonen dat middelen die zijn ingetrokken of geschorst vanaf het moment van intrekken of schorsen niet meer gebruikt zijn. 7. De Deelnemer MOET afdoende hebben geverifieerd dat het verzoek tot intrekking of schorsing door de bevoegde vertegenwoordiger is gedaan. De Deelnemer MOET het risico afwegen dat het verzoek niet door de bevoegde vertegenwoordiger is gedaan tegen de schade voor de gebruiker die het afhandelen of het niet afhandelen van het verzoek veroorzaakt. De Deelnemer MOET de risicoafweging vastleggen. a. De risicoafweging MOET een gedocumenteerde procedure zijn waarlangs de beslissing tot stand moet komen en waaraan de uitkomst van een beslissing tot revocatie of schorsing kan worden geverifieerd of; b. De risicoafweging betreft een documentatie per gemaakte afweging die in het dossier van de gebruiker wordt opgenomen. 8. De Deelnemer MOET een het authenticatiemiddel na ontvangst door de Deelnemer van het verzoek tot intrekking of schorsing binnen een (1) werkdag hebben ingetrokken of geschorst. 9. De Deelnemer MOET bij een verzoek tot heractivering van een geschorst authenticatiemiddel dit verzoek valideren als afkomstig van de Gebruiker van het middel of zijn vertegenwoordigingsbevoegde. De wijze van validatie MOET in overeenstemming zijn met het LoA van het geschorste authenticatiemiddel: a. De Deelnemer MOET de Gebruiker of zijn vertegenwoordigingsbevoegde identificeren. b. De Deelnemer MOET verifiëren bij de geïdentificeerde Gebruiker of deze het betreffende verzoek heeft gedaan. c. Een schorsing MAG eindigen op een moment dat bij het indienden van het verzoek is overeenkomen met de verzoeker. d. De Deelnemer MOET de Gebruiker notificeren over statuswijzigingen over een communicatiekanaal dat is overeengekomen in het proces van het registratie en uitgifte van het middel.	Toelichting: Doel van deze eis is dat de gebruiker van het middel zekerheid krijgt over intrekking of schorsing van het middel als hij daar om verzoekt. Toelichting bij 3: Een vertegenwoordigingsbevoegde kan bijvoorbeeld zijn een Voogd, De Rechtbank of een Bewindvoerder. De identiteit van een Voogd of Bewindvoerder en een beslissing van de Rechtbank kan worden geverifieerd aan een onafhankelijke bron. Good practice voor het verificatie van de identiteit van de Gebruiker bij een verzoek tot intrekking en schorsing/her-activering: • Verstrekken van een code bij de uitgifte van een authenticatiemiddel aan de gebruiker die voor revocatie en schorsingen/her-activering kan worden gebruikt. Tevens wordt de Gebruiker verzocht om beveiligingsvragen te beantwoorden (zogenaamd gedeeld geheim tussen de MU/AD en Gebruiker). De verstrekte code en de antwoorden op de beveiligingsvragen geven samen afdoende zekerheid dat de gene die het verzoek doet tot revocatie en schorsing/her-activering de Gebruiker is. • Een online-dienst waarmee de gebruiker met inzet van zijn authenticatiemiddel(en) een authenticatiemiddel waarvan hij Gebruiker is kan laten intrekken, schorsen en her-activeren. • In het proces voor schorsing (indien ondersteund) MAG soepeler worden omgegaan met de authenticatie van degene die de schorsing meldt met het oog op snellere verwerking. In dat geval moet de afwijking van het normale authenticatieproces expliciet vastgelegd zijn.

LOA 3 4	Hetzelfde als LoA1 met toevoeging van: 1. De Deelnemer MOET een het authenticatiemiddel na ontvangst door de Deelnemer van het verzoek tot intrekking of schorsing binnen vierentwintig (24) uur hebben ingetrokken of geschorst:	

2.2.4 Verlenging en vervanging

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Betrouwbaarheidsniveau van het vernieuwingsproces MOET in elk geval gelijk zijn aan het betrouwbaarheidsniveau van eerste uitgave. 2. De levensduur van een credential voordat vernieuwing of intrekking plaatsvindt MOET gebaseerd zijn op een risicoanalyse die de kwaliteit van de onderliggende techniek en noodzaak voor 'proof of life' van de gebruiker in beschouwing neemt. Deze risicoafweging van de levensduur van het middel moet periodiek getoetst worden aan de laatste stand der techniek. 3. Een gebruiker MAG met een bestaand geldig middel vernieuwing aanvragen op hetzelfde betrouwbaarheidsniveau.	
LOA 2 3 4	LoA1 met toevoeging van: 1. De Deelnemer MOET de verwachte levensduur van een authenticatiemiddel jaarlijks vaststellen op basis van een analyse van de kenmerken en kwetsbaarheden van het middel. 2. Een Authenticatiemiddel waarvan is aangetoond dat deze kwetsbaar is geworden voor misbruik of manipulatie MOET door de Deelnemer worden ingetrokken. 3. De vastgestelde levensduur van een authenticatiemiddel MOET zijn gerelateerd aan de te verwachten technische levensduur van het middel maar ZOU niet meer MOETEN zijn dan tien (10) jaar. 4. De Gebruiker MOET minimaal elke tien (10) jaar het gehele proces identificatie tot de uitgifte van een authenticatiemiddel opnieuw doorlopen. 5. De Deelnemer MAG een authenticatiemiddel vernieuwen op basis van een bestaand en geldig authenticatiemiddel. Het vernieuwde authenticatiemiddel MOET aan de Gebruiker worden verstrekt met de zekerheid die behoort bij het LoA van het authenticatiemiddel dat wordt vernieuwd en voldaan wordt aan punt 4. 6. Voor LoA3 en LoA4 middelen die bedoeld zijn voor gebruik in het BSN domein: a. De Deelnemer MOET tenminste een maal per vijf (5) jaar vaststellen dat de Gebruiker nog in bezit is van zijn middel. Indien de Deelnemer niet kan vaststellen of de Gebruiker nog in bezit van zijn middel MOET de Deelnemer het authenticatiemiddel intrekken of schorsen. b. De Deelnemer MAG deze eis ook invullen voor ander LoA's en middelen die niet bedoeld zijn voor gebruik in het BSN domein.	Ad 3. Een authenticatiemiddel bestaat uit een technische component en procedurele component. Voor de maximale levensduur van het het middel (technisch en procedureel) is aangesloten bij de levensduur van paspoorten en gekwalificeerde certificaten. Het is vanuit optiek van het Stelsel belangrijker dat de kwetsbaarheid van de verschillende technische componenten van het middel wordt gemonitord door de AD/MU dan dat een specifieke levensduur wordt opgelegd van de technische componenten waaruit een middel kan bestaan. Ad 4. Het is altijd mogelijk dat er in de loop van de tijd fouten gemaakt worden waardoor een persoon niet of niet meer in bezit is van de juiste credentials om over een specifiek middel te mogen beschikken. Daarom is het nodig om personen periodiek opnieuw te identificeren conform het proces van de initiële uitgifte van een middel. Bij de keuze voor de termijn van 10 jaar is aangesloten bij de bestaande praktijk voor het vernieuwen van Nederlandse identiteitsbewijzen. Ad 5. Om dezelfde reden als bij 4. en omdat misbruik door derden niet is uit te sluiten van gestolen, verloren middelen of middelen van bijvoorbeeld overledenen is een extra vorm van controle voorgeschreven die eens in de 5 jaar plaatsvindt. good practice voor middelen die bedoeld zijn voor gebruik in het BSN domein op LoA3 en LoA4: • Uitvoeren van een her-registratie van het middel bij BSNk. Indien een gebruiker niet meer in leven zou zijn geeft BSNk een foutmelding. Deze toets wordt aangevuld met een toets op recent gebruik van het middel in de laatste 12 maanden. Voorbeelden van overige good practices: • Uitvoeren van een banktransactie die alleen op naam van de Gebruiker staat in combinatie met het gebruik van zijn middel. • De Gebruiker wordt telefonisch, per brief of per email verzocht zijn om binnen een vastgestelde periode (bijv. twee maanden) met zijn middel in te loggen bij zijn AD/MU en een drietal beveiligingsvragen te beantwoorden (zogenaamd gedeeld geheim tussen de MU/AD en Gebruiker) die bij de uitgifte van het middel zijn overeengekomen met de gebruiker.

2.3 Authenticatie

2.3.1 Authenticatiemechanisme

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. De gebruiker MOET in staat worden gesteld om de website/app van de authenticatiedienst en alle andere partijen in het netwerk te authenticeren. 2. De HM MOET in het keuzescherm voor de AD tonen bij welke dienst de Gebruiker gaat inloggen. 3. De AD MOET in het aanlogscherm tonen bij welke Dienstverlener de Gebruiker gaat aanloggen. 4. Optioneel: De AD/MU MAG de Gebruiker aanbieden om de notificatiemethode voor LoA4 (onder d.) toe te passen op de lagere LoA's. 5. Het authenticatiemechanisme MOET 'enige' bescherming bieden tegen ondertaande dreigingen: a. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden. b. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen. c. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller. d. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen. e. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt. f. 'Enige bescherming' MOET worden aangetoond door middel van een risicoanalyse en bijbehorende mitigerende maatregelen. 6. De Deelnemers in het Stelsel MOETEN zekerstellen dat de risico's van identiteitsfraude en misbruik van de tokens worden geanalyseerd en gemitigeerd tot het toepasselijke betrouwbaarheidsniveau.	Ad 1 Dit kan bijvoorbeeld op basis van een TLS certificaat of een digitale handtekening op basis van een vertrouwd certificaat.
LOA 2	Hetzelfde als LoA1	
LOA 3	Hetzelfde als LoA1 met toevoeging van: 1. Bij gebruik van het authenticatiemiddel MOET de Gebruiker expliciet duidelijk gemaakt worden dat hij een authenticatie in de context van een Stelselmerk uitvoert, ook wanneer zijn applicatie (o.a. de browser) of platform (o.a. PC) waarop de applicatie actief is gecorrumpeerd is. Indien het middel buiten de Stelselcontext wordt gebruik MAG een Stelselmerk NIET getoond worden.	Ad 1 Toelichting: Authenticatie onder een merk van het AS wil zeggen onder eHerkenning. Als het middel wordt gebruikt in een andere context moet het middel die notificatie achterwege laten of de andere context aangeven. Doel is om hiermee het transactierisico voor de gebruiker verminderen in het geval dat zijn applicatie/browser is gecorrumpeerd. Ad 2 Toelichting: Single Sign On voor diensten van een enkele dienstverlener op LoA3 en LoA4 is toegestaan. SSO tussen dienstverleners is slechts toegestaan op LoA1 en LoA2. Beide situaties uiteraard met handhaving van de beperking dat de LoA van het middel alleen toegang mag geven tot diensten met een zelfde LoA of een lagere LoA. Single Sign On tussen Dienstverleners moet op LoA3 en LoA4 worden beperkt. Het betrouwbaarheidsniveau wordt met SSO tussen dienstverleners te veel ondermijnd omdat de transactie kwetsbaar wordt voor Man-in-the-front en Man-in-the-browser aanvallen. Daarnaast accepteren

	2. De toegang tot diensten van elke afzonderlijke dienstverlener MOET het aanloggen met behulp van het authenticatiemiddel vereisen. 3. Het authenticatiemechanisme MOET bescherming bieden tegen de meeste van deze dreigingen: a. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden. b. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen. c. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller. d. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen. e. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt. f. Bescherming MOET worden aangetoond door een risicoanalyse en bijbehorende mitigerende maatregelen. 4. De MU/AD MOET jaarlijks het authenticatiemechanisme onderwerpen aan een risico analyse daarbij rekening houdend met (nieuwe) aanvalstechnieken en kwetsbaarheden. Dit omvat een vergelijking van de gebruikte cryptografische algoritmen en sleutellengtes met de actuele 'good practice'. Indien de analyse daar aanleiding toe geeft worden middelen aangepast en/of vervangen. 5. Het correct functioneren van het authenticatiemechanisme moet weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'moderate attacker' potentieel in de zin van Annex B van de Common Criteria (ISO 15408-3 en valuatie norm ISO/IEC 18045). Implementatietermijn Voor punt 1 en 2 geldt: Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen. De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.	Dienstverleners in formeel juridische zin een authenticatie en daarmee kan SSO tussen dienstverleners op LoA3 en LoA4 niet alleen meer een oplossing zijn voor gebruiksgemak. Ad 5 Toelichting: De wijze waarop conformiteit met deze eis moet worden aangetoond is aangegeven in paragraaf 2.4.7 Compliance en Audit.
LOA 4	LoA3 met toevoeging van: 1. Het auhenticatiemiddel MOET de Gebruiker notificeren (onafhankelijk	Toelichting: Doel van de eis is om de Gebruiker in staat te stellen een fout of inbreuk in de communicatie te herkennen en bij twijfel de informatietransactie af te breken. Het is altijd mogelijk dat de browser van de Gebruiker gecompromitteerd raakt daarom is voor LoA4 is een extra maatregel opgenomen

van de browser die hij gebruikt) van zijn inlogpoging bij een specifieke dienst of dienstverlener .
2. De notificatie MOET zijn gekoppeld aan het gebruik van diensten op het niveau van het middel.
3. De Deelnemer MAG een optie aanbieden om de notificatiedienst door de gebruiker zelf aan en uit te laten zetten voor diensten op het LoA van het middel of lager.
4. De notificatie ZOU de Gebruiker binnen een tijdsbestek MOETEN bereiken zodat de notificatie zijn beslissing om de inlog voort te zetten of af te breken kan beïnvloeden.
5. Het authenticatiemiddel MOET een betrouwbaar (trusted) kanaal bevatten ten behoeve van betrouwbare notificatie en bevestiging, ook wanneer zijn voor inlog gebruikte applicatie of het platform (o.a. PC) waarop de applicatie actief is gecorrumpeerd is. Dit kanaal MOET de mogelijkheid bevatten om de gebruiker elementen in het authenticatieverzoek te laten bevestigen.
6. De Deelnemer MOET de Gebruiker bij het aanbieden van de notificatiedienst er op attenderen dat hij als Gebruiker zelf verantwoordelijk is voor de beveiliging van zijn browser en zelf dus ook verantwoordelijk draagt voor de beslissing om in te loggen.
7. Het correct functioneren van een authenticatiemechanisme (en het authenticatiemiddel) moet weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'High attacker' potentieel in de zin van Annex B van de Common Criteria (ISO 1508-3 en evaluatie norm ISO/IEC 18045).

Implementatietermijn

Voor punt 5 geldt:

Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.

De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.

1. Implementatiedatum voor nieuwe middelen: 31 december 2018 (2 1/2 jaar na vaststelling door TB en rekening houdend met overige implementatie-inspanningen in de periode juli-dec 2016)
2. Implementatiedatum voor bestaandemiddelen: 31 december 2019 (geldigheidstermijn gekwalificeerde certificaten en rekening houdend met overige implementatie-inspanningen in de periode juli-dec 2016)
3. Periodieke evaluatie implementatiedata: Het security officers

die bij implementatie gekoppeld mag worden op het middel of op de dienst. Een voorbeeld is verzending van een SMS als een internet browser wordt gebruikt om in te loggen. Bij frequent gebruik van een middel voor diensten op lagere LoA's kan dat door de gebruiker als bezwarend worden ervaren om steeds SMS's te ontvangen, daarom mag een optie aangeboden worden om de dienst door de gebruiker zelf uit te laten zetten. Ook mag de optie worden aangeboden de de gebruiker notificatie te koppelen aan het gebruik van diensten op het LoA van het middel of lager.

Ad 5 Toelichting: Het gaat er om dat de gebruiker via het 'trusted' kanaal hoogst betrouwbaar informatie over zijn inlog bij de DV of dienst kan worden gegeven en om hoogst betrouwbare bevestiging kan worden worden gevraagd van een specifiek transactiegegeven. Deze betrouwbaarheid blijf bestaan ook al is de gebruiker slachtoffer van een aanval op zijn inlog-applicatie zoals zijn browser en de PC van de gebruiker (man-in-the-browser attack/man-in-the-front attack). Bij het nemen van maatregelen voor het betrouwbare kanaal moet dus worden uitgegaan van de idee dat de gebruikersomgeving is gecorrumpeerd.

Ad 7 Toelichting: De wijze waarop conformiteit met deze eis moet worden aangetoond is aangegeven in paragraaf 2.4.7 Compliance en Audit.

	overleg evalueert elke 6 maanden de noodzaak tot aanpassing van de implementatiedata en adviseert na consultatie van de governance om de implementatie termijn te vervroegen, te verlaten of te handhaven. De evaluatie gebeurt aan de hand van de context van Europese ontwikkelingen), Nederlandse ontwikkelingen en ontwikkeling van het risico dat de kwetsbaarheid (ontbreken van een trusted channel) wordt misbruikt.	

2.4 Beheer en organisatie

2.4.1 Algemene bepalingen

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Partijen die deelnemen in het Stelsel MOETEN het toetredingsproces hebben doorlopen dat is vastgelegd in het Afsprakenstelsel. Het is van belang dat de Deelnemer identificeerbaar is en kan voldoen aan zijn verplichtingen. Daarvoor MOET de Deelnemer bij toetreding en daarna voldoen aan de volgende vereisten: a. De Deelnemer drijft een onderneming en MOET als zodanig zijn ingeschreven in het Nederlandse Handelsregister. De Deelnemer MOET binnen het Stelsel uitsluitend een geregistreerde handelsnaam hanteren. b. De Deelnemer MAG NIET in staat van faillissement verkeren, aan hem MAG NIET een surseance van betaling zijn verleend en voor hem MAG NIET een schuldsaneringsregeling van toepassing zijn. Ook MAG NIET ten aanzien van de deelnemer een faillissement zijn aangevraagd en de Deelnemer MAG NIET zijn gestopt met het betalen van zijn schulden. c. Als combinaties van deelnemers willen toetreden dan is dat mogelijk. In dat geval dienen alle deelnemers te voldoen aan de toetredingseisen. 2. Binnen het afsprakenstelsel MOET iedere deelnemer aansprakelijk zijn voor zijn eigen handelen en/of nalaten voor de rol die hij vervult. Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. De deelnemers MOGEN NIET afwijken van deze algemene regels. 3. De beheerorganisatie MOET door de Deelnemer op de hoogte worden gesteld van de mate waarin de Deelnemer onafhankelijk kan opereren. De Deelnemer MOET minimaal informatie verstrekken over: a. De buitenlandse stakeholders in de Deelnemer of moedermaatschappij van de deelnemer;De mate waarin stakeholders in de Deelnemer of moedermaatschappij van deelnemer zeggenschap hebben over de procesgang binnen de Deelnemer; b. de scheiding van processen en verantwoordelijkheden tussen de Authenticatiedienst en de overige onderdelen van de organisatie, in het	Ad 1 Het Afsprakenstelsel Elektronische Toegangsdiensten is een publiek private samenwerking onder vigerend Nederlands Recht. Alle verplichtingen die een deelnemer aangaat bij toetredingen zijn vastgelegd in het Juridisch kader. De specifieke vereisten m.b.t privacybescherming en informatiebeveiliging zijn opgenomen in het Privacybeleid respectievelijk het B eleid voor informatiebeveiliging. Het proces voor toetreding is vastgelegd in het Operationeel Handboek, Proces toetreden. Onderdeel van dit proces is een toetsing door de Toezichthouder van de relevante processen, procedures en uitgevoerde technische tests. Ad 2 Hoe deze algemene regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval. De deelnemer kan zijn aansprakelijkheid beperken in de overeenkomst die hij sluit met een dienstafnemer of met een dienstverlener. Daarbij blijft hij gebonden aan de algemene regels van het Nederlandse recht inzake aansprakelijkheid en schadevergoeding. Ad 3 De aansprakelijkheidsregels zijn opgenomen in het Juridisch kader Ad 4 Deze eIDAS eis overlapt de eis met betrekking tot sub-contractanten in 2.4.5. Zowel het Juridisch kader en vooral het Gemeenschappelijk normenkader informatiebeveiliging bevatten voor deze eis relevante specificaties.

	geval de Authenticatiedienst onderdeel is van een grotere organisatie. c. Daar waar de onafhankelijkheid of betrouwbaarheid van de deelnemer in twijfel is MAG de Toezichthouder van het Stelsel nadere eisen stellen aan de deelnemer om het voldoen aan wettelijke eisen te waarborgen en imagoschade voor het Stelsel te voorkomen. 4. Alle Deelnemers MOETEN voldoen aan de stelseleisen inzake de naleving van verplichtingen bij uitbesteding of gezamenlijk uitvoeren van activiteiten. a. De Deelnemers zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden. b. Als een combinatie onder een gemeenschappelijke naam als 'een organisatie' diensten wil verrichten geldt de eis dat: i. De leden van de combinatie vanaf de start van deelname hoofdelijk aansprakelijk MOETEN zijn voor de volledige en correcte nakoming van alle juridische verbintenissen die in het kader van het Stelsel zijn aangegaan. ii. Alle combinanten MOETEN individueel voldoen aan de toetredingseisen. Bij wijziging in de samenstelling van de combinatie MOET de toetredingsprocedure door nieuwe leden van de combinatie opnieuw worden doorlopen.	
LOA 2 3 4	LoA1 met toevoeging van: 1. Deelnemer MOET in het bezit te zijn van een aansprakelijkheidsverzekering die dekkend is voor aansprakelijkheidseisen die kunnen voortvloeien uit het opereren als onderdeel van het Stelsel. 2. Deelnemer MOET beschikken over een continuïteitsplan/exitplan dat in werking treedt op het moment dat deelnemer niet meer aan zijn Stelselverplichtingen kan voldoen of wenst te voldoen. Het continuïteitsplan/exitplan MOET ten minste waarborgen treffen voor het ondersteunen van de bestaande klanten van de deelnemer voor de periode die is afgesproken in contracten met deze klanten. 3. Als de Deelnemer niet beschikt over een aansprakelijkheidsverzekering MOET een deelnemer op andere wijze afdoende aantonen dat eventuele aansprakelijkheidsclaims kunnen worden gedekt (bijvoorbeeld uit eigen middelen).	

2.4.2 Gepubliceerde mededelingen en informatie voor de gebruikers

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Het Afsprakenstelsel MOET openbaar toegankelijk	Ad 1 De bedoelde vereisten voor zijn vastgelegd in de het Operationeel handboek en de Gebruiksvoorwaarden Elektronische Toegangsdiensten. Daarnaast betreft het de naleving van algemene wettelijke verplichtingen inzake gebruiksvoorwaarden en privacy. Specifiek stelselvereisten voor privacybescherming zijn opgenomen in het Privacybeleid van het stelsel.

	gepubliceerd zijn. Deelnemers MOETEN de stelselvereisten inzake publicatie van dienstbeschrijvingen en gebruiksvoorwaarden naleven.	
LOA 2 3 4	Zelfde als LoA1 met toevoeging van: 1. De Deelnemer MOET de Gebruiker online inzicht bieden in: a. de gegevens die over hem zijn vastgelegd ten behoeve van de uitgifte van een authenticatiemiddel of registratie van een machtiging; b. de authenticatiemiddelen die op zijn naam zijn uitgegeven en indien van toepassing door hem afgegeven machtigingen; c. de transacties die met middelen op zijn naam zijn uitgevoerd (datum, tijd, dienstverlener, dienst). 2. Indien een persoon claimt niet meer over zijn middel te beschikken of claimt dat ten onrechte op zijn naam een middel is uitgegeven MOET de Deelnemer fysiek inzicht geven in de gegevens genoemd onder 2a. 3. De Deelnemer MOET en allen tijde op afdoende wijze vaststellen dat inzage in de gegevens genoemd onder 2a. wordt verstrekt aan de juiste persoon. a. In alle gevallen MOET de Deelnemer een persoon die toegang tot de gegevens vraagt fysiek of online identificeren als ware het de Gebruiker.	Ad 1 Doel van deze eis: De Gebruiker wordt in staat gesteld om anomalieën in het gebruik van zijn middel te ontdekken en met deze informatie in contact te treden met een dienstverlener. De persoon op wiens naam ten onrechte een middel is uitgegeven wordt in staat gesteld registraties op zijn naam en de transacties die met het middel op zijn naam gedaan in te zien. good practice: De Deelnemer geeft zich rekenschap van het feit dat het gaat om toegang tot persoonsgegevens de zin van de AVG. Verwacht mag worden dat de maatregelen die de Deelnemer treft voor bescherming van de toegang tot de transactiegegevens altijd gerelateerd is het LoA van de middel van de Gebruiker. Ad 3 Toelichting bij 3a: Hier is uitgegaan van de situatie dat een fraudeur gebruik heeft gemaakt van identificerende kenmerken van de persoon die claimt dat ten onrechte een middel op zijn naam is uitgereikt. De identificerende kenmerken van de claimant moeten dus overeenkomen met de identificerende kenmerken die zijn gebruikt bij de registratie en uitgifte van het middel. Dat betekent dat de claimant zich kan identificeren als ware hij de daadwerkelijke gebruiker. Een deelnemer mag hier niet van af wijken omdat het risico bestaat dat persoonsgegevens ten onrechte ter inzage worden gegeven. In het geval de identificerende kenmerken niet overeenkomen is een andere juridische basis nodig om de gegevens te verstrekken zoals in het kader van formele opsporing of gerechtelijk bevel.

	b. De Deelnemer MOET de Gebruiker toegang verstrekken tot de gegevens op minimaal hetzelfde LoA als het LoA van het middel dat aan de Gebruiker is uitgereikt.	

2.4.3 Beheer van informatiebeveiliging

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2 3 4	1. De Deelnemers en de Beheerorganisatie MOETEN een systeem voor het management van informatiebeveiliging inrichten waarin minimaal hun dienstverlening voor het Stelsel MOET zijn ondergebracht. Het managementsysteem MOET zijn ingericht conform de ISO/IEC 27001:2013 standaard en MOET zijn gecertificeerd of de Deelnemer en de Beheerorganisatie MOETEN beschikken over een Third Party Mededeling met gelijkwaardige conformiteitsverklaring (TPM) van een onafhankelijke Register EDP auditorgelijkwaardige. Hierna wordt kortweg gesproken over een TPM. De toetsing van opzet, bestaan en werking van geïmplementeerde controls en implementatie van de stelselafspraken over de technische invulling maken onderdeel uit van het certificaat of de TPM (inclusief conformiteitsverklaring). 2. De Deelnemer in het Stelsel MOET het risico's op identiteitsfraude onderkennen en in het ontwerp en implementatie van processen voor middelenuitgifte mitigeren. a. De Deelnemer MOET in de risicoanalyse in het kader van de ISO 27001 certificering het procesontwerp van de processen voor registratie en uitgifte van middelen hebben geadresseerd. b. De Deelnemers en Beheerorganisatie MOETEN de op risico gebaseerde beslissingen t.a.v. het ontwerp en de implementatie van mitigerende beheersmaatregelen vastleggen. c. De Deelnemer in het Stelsel MOET iedere afwijking van de vereisten voor de implementatie van risico-verlagende beheersmaatregelen toelichten en vastleggen. d. De Deelnemers in het Stelsel MOETEN erop toezien dat procesgerelateerde gebeurtenissen herleidbaar zijn. Deelnemers MOETEN de procesvoorvallen registreren, wanneer deze betrekking hebben op: de aanvraag van een token het resultaat van de toegepaste verificaties en validaties aanvaarding en weigering van aanvragen.	Ad 1 Dit is een eis die aan alle Deelnemers en Beheerorganisaties wordt gesteld als onderdeel van de basisbeveiliging van het Stelsel.

2.4.4 Bijhouden van de administratie

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2 3 4	1. Algemene vereisten voor registratie en archivering;De invulling van deze norm voor record keeping MOET de volgende doelstellingen ondersteunen: a. Het voldoen aan wettelijke verplichtingen; b. Dispute resolution in geval van (fraude) claims; c. Het vastleggen van adequate audit trails. 2. Deelnemers aan het Stelsel MOETEN toezien op naleving van het toepasselijke belasting- en privacyrecht. 3. De Deelnemer in het Stelsel MOET kopieën van identiteitsbewijzen archiveren conform de onderstaande eisen: a. Het type identiteitsbewijs en het documentnummer van het identiteitsbewijs MOET geregistreerd en gearchiveerd worden. b. Persoonsgegevens zoals een foto, het Burger Service Nummer (BSN) en de nationaliteit MOETEN bij archivering en opslag conform de AVG verwerkt worden. 4. Op LoA3 en LoA4 MOET de deelnemer de registraties en logging zodanig vastleggen dat deze kunnen worden gebruikt voor bewijsvoering in geval van fraudeonderzoek of claims van misbruik. Het is toegestaan om gevoeliger gegevens vast te leggen als die het doel dienen om te bewijzen dat een middel zorgvuldig is uitgegeven en gebruikt. 5. Specifieke vereisten voor registratie en archivering: De deelnemer aan het Stelsel MOET een log bijhouden van alle uitgevoerde verificaties en validaties. Het betreft minimaal de: a. validaties van inschrijvingen in het Handelsregister van de Kamer van Koophandel. b. validaties van handgeschreven handtekeningen	Interpretatie: Ad1 Archivering van verificaties en validaties bedoeld voor de opbouw van audittrails is ten behoeve van: • de opsporing en bestrijding van frauduleuze informatietransacties; • de bescherming van de Gebruiker bij misbruik van zijn (digitale) identiteit. De Deelnemer legt de overwegingen voor de vastleggingen in het kader van archivering vast. De Deelnemer specificeert de vastleggingen in het kader van archivering. Ad 3 Persoonsgegevens zoals een foto, het Burger Service Nummer (BSN) en de nationaliteit MOETEN bij archivering en opslag blijvend onleesbaar zijn gemaakt. Deelnemers zijn voor al hun stelselactiviteiten zelf verantwoordelijk voor de naleving van de wettelijke vereisten uit de Algemene verordening gegevensbescherming (AVG).

	c. validaties van een identiteit door bankoverschrijving d. validaties van elektronische handtekeningen e. validaties van authenticaties in het elektronische registratieproces f. elektronische berichten met een identiteitsverklaring van de Aanvrager ter registratie, waaronder de verplichte bijlage. g. controles van (interne) Machtigingen 6. Archivering van verificaties en validaties is verplicht: a. gedurende de geldigheidsduur van uitgegeven middelen en; b. tot 7 jaar na intrekking of verlopen van het middel. 7. Met het oog op de betrouwbare elektronische communicatie MOETEN de deelnemers voldoen aan volgende eisen ten aanzien van archivering: a. Elke Deelnemer MOET gearchiveerde gegevens beveiligd opslaan zodat zij niet toegankelijk zijn voor onbevoegden. Elke Deelnemer MOET alle door haar ondertekende en alle door haar ontvangen ondertekende berichten 7 jaar archiveren. Na deze periode MOETEN ten minste de persoonsgegevens in deze berichten vernietigd worden. Een Deelnemer MAG NIET persoonsgegevens afkomstig van berichten of bewijsstukken langer bewaren dan noodzakelijk voor het doel waarvoor ze worden verwerkt (conform Wet Bescherming Persoonsgegevens).	Indien een deelnemer afwijkt van de hetgeen in de toelichting is aangegeven is deze afwijking voor de auditor slechts acceptabel als: • de afwijking is gedocumenteerd en formeel is geaccepteerd door het bevoegde managementniveau van de Deelnemer. • De deelnemer een expliciete afweging heeft gemaakt in het kader van de wet bescherming persoonsgegevens t.a.v. het doel van de opslag en de risico's die dit met zich mee brengt voor personen. De Deelnemer blijft te allen tijde zelf verantwoordelijk voor de inhoud van de gemaakte afweging. Het oordeel van de auditor over naleving van deze norm heeft geen enkele betekenis als verweer indien de Deelnemer door de bevoegde instanties in het kader van de AVG ter verantwoording wordt geroepen. Ad 4 en 5 Toelichting: Afwijken van deze norm is slechts acceptabel indien de noodzaak kan worden aangetoond door de Deelnemer.

2.4.5 Faciliteiten en personeel

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2 3 4	1. De Deelnemer in het Stelsel MAG bij het vervullen van zijn rol (mede) gebruik maken van andere marktpartijen, onderaannemers of samenwerken met partijen waarmee een ander verband bestaat. In dat geval hoeven deze andere partijen niet toe te treden tot het afsprakenstelsel. Essentieel is het uitgangspunt dat alleen toegetreden Deelnemers diensten in het Stelsel verrichten. Bij inschakeling van derde partijen geldt de eis dat: a. De Deelnemer aansprakelijk MOET zijn voor de nakoming van alle verplichtingen in de leveringsketen. De Deelnemer MOET de diensten op eigen naam uit te voeren. b. De Deelnemer de Beheerorganisatie in staat stelt om de naleving van de Stelselafspraken door de Deelnemer op grond van het nalevingsbeleid te monitoren en controleren. 2. De Deelnemer dient het voor de te leveren diensten gebruik te maken van op afdoende opgeleid personeel.	Ad 1 Toelichting: Voor het doorgeven van verplichtingen aan onderaannemers etc. volgt de Deelnemer de vereisten uit het Privacybeleid van het Stelsel en het Gemeenschappelijk Normenkader Informatiebeveiliging. Ad 2 Verondersteld wordt dat de implementatie van de eis grotendeels wordt afgedekt door de ISO 27001 certificatie van de deelnemer en dat de deelnemer het daar waar het gaat om het competenties voor het uitvoeren van verificaties in het identificatieproces dit specifiek maakt (zie paragraaf 2.1.2 en 2.1.3).

2.4.6 Technische controles (technical controls)

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Deelnemers in het Stelsel MOETEN voldoen aan de specificaties voor berichtenuitwisseling zoals is vastgelegd in het Afsprakenstelsel. 2. De bescherming van (persoons-)gegevens MOET expliciet worden meegenomen als een aspect van de risicoanalyse in het kader van de verplichte ISO27001 certificatie van Deelnemers. 3. Verbindingen MOETEN gebruik maken van TLS conform de vereisten uit de koppelvlakspecificaties. 4. Deelnemer moet conform de geldende stand der techniek 'secret information' beschermen en de genomen maatregelen documenteren. 5. Het Stelsel waarborgt dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken.	Ad 1 en 3 Het Afsprakenstelsel bevat meerdere specificaties waaronder de specificaties van interfaces en berichten en communicatiekanalen. Alle Deelnemers hebben zich bij toetreding tot het stelsel verplicht deze specificaties te implementeren. Ad 2 Toelichting: Deelnemers zijn voor al hun stelselactiviteiten zelf verantwoordelijk voor de naleving van de wettelijke vereisten uit de Wet Bescherming Persoonsgegevens. Alleen op LoA3 en LoA4 wordt in het Afsprakenstelsel aantoonbaarheid vereist van risicoafweging t.a.v. bescherming van persoonsgegevens in de veronderstelling dat op deze LoAs bijzondere maatregelen noodzakelijk zullen zijn. Ad 4 'Secret information' omvat persistente wachtwoorden, PINs en (geheime) sleutelmateriaal dat benodigd is voor de authenticatie. Niet bedoeld worden hier eenmalige wachtwoorden (OTPs).

		Ad 5 De vereisten voor het duurzaam handhaven van de veiligheid is vastgelegd in het Beleid voor informatiebeveiliging en de uitwerking daarvan in het Gemeenschappelijk normenkader informatiebeveiliging.
LOA 2	Zelfde als LoA1 plus 1. De deelnemer MOET risico-beperkende maatregelen nemen voor de dreiging dat een medewerker met valse voorwendselen een authenticatiemiddel creëert op naam van een fictief persoon, of op naam van een bestaand persoon zonder dat deze daarom heeft verzocht. 2. Alle digitale persoonsgegevens en andere gevoelige gegevens MOETEN met cryptografie zijn beschermd tijdens transport. 3. Alle digitale persoonsgegevens en andere gevoelige gegevens in ruste MOETEN met cryptografie zijn beschermd als: i) deze data vanaf het internet te benaderen is ii) deze data op draagbare /verwijderbare media staat. 4. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, MOET zijn beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is.	Ad 2 en 3 Alle 'persoonsgegevens' en 'andere gevoelige gegevens' omvat naast persistente wachtwoorden, PINs en (geheim) sleutelmateriaal dat benodigd is voor de authenticatie ook alle herleidbare persoonsgegevens. Het omvat niet het pseudoniem. Ad 3 Als toegang tot de systemen of media op eenvoudige wijze verkregen kan worden dan dient via cryptografie dit risico beperkt te worden. Betreft bijvoorbeeld een database server die rechtstreeks met een client vanaf het Internet te benaderen is. Is niet van toepassing op een database server die in een beveiligde zone staat waar enkel andere (interne) systemen zoals applicatie servers bij kunnen komen. Met draagbare/verwijderbare media wordt bedoeld: Laptops, usb-sticks, harddisks etc. Is niet van toepassing als deze media in beveiligde ruimtes, zoals een datacenter, zijn geplaatst. Ad 4 Verondersteld wordt dat met de verplichte ISO27001 certificatie voldaan wordt aan deze eis.
LOA 3	Zelfde als LoA2 punten 2 en 3 en met toevoeging van: 1. De deelnemer MOET risico-beperkende maatregelen nemen voor de dreiging dat een medewerker met valse voorwendselen een authenticatiemiddel creëert op naam van een fictief persoon, of op naam van een bestaand persoon zonder dat deze daarom heeft verzocht. De Deelnemer MOET zijn maatregelen baseren op een analyse van de risico's in het registratie en uitgifte proces ten aanzien van de genoemde dreiging. 2. Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt MOET zijn beschermd tegen ongeoorloofde manipulatie.	Ad 1 Toelichting: Voorkomen wordt dat één en dezelfde medewerker zonder enige vorm van controle, toezicht of functiescheiding in staat is om de registratie van een gebruiker te doen en vervolgens een authenticatiemiddel kan creëren en uitreiken.Dat het onwaarschijnlijk wordt gemaakt dat technisch beheerders ongezien rechtstreeks ingrijpen op databases om daarmee een werkend authenticatiemiddel te creëren. Dat betekent dat ofwel de technisch beheerder deze handeling niet kan verrichten ofwel dat een dergelijke handeling van de beheerder vrijwel direct wordt gesignaleerd en onder de aandacht van het management wordt gebracht. Ad 2 Verondersteld wordt dat met de verplichte ISO27001 certificatie voldaan wordt aan deze eis.
LOA 4	Hetzelfde als LoA 2 punten 2 en 3 en LoA3 punt 2 en met toevoeging van: 1. De deelnemer MOET risicobeperkende maatregelen nemen voor de dreiging dat een medewerker met valse voorwendselen een authenticatiemiddel creëert op naam van een fictief persoon, of op naam van een bestaand persoon zonder dat deze daarom heeft verzocht. De Deelnemer MOET maatregelen nemen die functiescheiding handhaven tussen medewerkers die de uitgifte van het authenticatiemiddel controleren en medewerkers die de uitgifte van het authentictiemiddel goedkeuren. Deze eis is ontleent aan het Programma van Eisen PKIoverheid v4.3, deel 3 – basiseisen, eis-nummer 5.2.4-pkio77 en onderliggende ETSI eisen. Van registratie- en uitgifteprocessen voor LoA4 authenticatiemiddelen die zijn gebaseerd op een gekwalificeerd certificaat mag worden verondersteld dat die aan deze eis voldoen.	Ad 1 Toelichting: Voorkomen wordt dat één en dezelfde medewerker zonder enige vorm van controle, toezicht of functiescheiding in staat is om de registratie van een gebruiker te doen en vervolgens een authenticatiemiddel kan creëren en uitreiken. Dat het onwaarschijnlijk wordt gemaakt dat technisch beheerders ongezien rechtstreeks ingrijpen op databases om daarmee een werkend authenticatiemiddel te creëren. Dat betekent dat ofwel de technisch beheerder deze handeling niet kan verrichten ofwel dat een dergelijke handeling van de beheerder vrijwel direct wordt gesignaleerd en onder de aandacht van het management wordt gebracht.

2.4.7 Compliance en audit

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2	1. De Deelnemer MOET bij toetreding tot het Stelsel zijn processen voor uitgifte van middelen en de technische beschrijving van de middelen en het authenticatiemechanisme ter beoordeling aanbieden aan de Toezichthouder en de externe conformiteitsbeoordelaar. Als toegetreden partij MOET de Deelnemer bij wijziging van zijn processen deze opnieuw aanbieden ter beoordeling door de Toezichthouder.	Ad 1 en 2 Toelichting: • De wijze waarop deelnemers processen aan de Toezichthouder aanbieden volgt de betreffende vereisten uit het Operationeel handboek van het stelsel. • De eisen aan de conformiteitsbeoordelaar, de uit te voeren toetsen en conformiteitsrapportage zijn beschreven in de Handreiking Conformiteitstoetsing

	2. De Deelnemer MOET bij essentiële wijziging in processen of de gebruikte technologie van authenticatiemechanisme of authenticatiemiddel opnieuw zijn processen en technische documentatie ter beoordeling aanbieden aan de Toezichthouder en de conformiteitsbeoordelaar. 3. De deelnemer moet zijn dienstverlening aantoonbaar binnen de scope van de verplichte ISO 27001 certificatie hebben gebracht.	authenticatiemiddel en mechanisme. (zie ook resp. par 2.2.1 en 3.2.1). • In het kader van het Toezicht op het Stelsel vinden periodieke nalevingscontroles plaats door de toezichthouder. Ad 3 Toelichting: In het kader van ISO 27001 certificatie vinden periodieke interne audits plaats die de voor de dienst relevante processen raken.
LOA 3 4	Zelfde als LoA1 met toevoeging van: 1. De MU/AD moet ten behoeve van de conformiteitsbeoordeling en het toezicht een actueel overzicht kunnen opleveren van de aan het authenticatiemiddel en autenticatiemechanisme, uitgevoerde wijzigingen, met daarbij een beschrijving van de impact op de conformiteit aan de gestelde eisen. 2. Bij de conformiteitsbeoordeling wordt onderscheid gemaakt tussen verschillende typen onderzoek, te weten: een initieel onderzoek, een herhalingsonderzoek en een heronderzoek. a. Een initieel onderzoek is een eerste beoordeling over de volledige scope van het object van onderzoek op basis van de gestelde eisen; b. Een herhalingsonderzoek vindt uitsluitend plaats bij uitgevoerde wijzigingen aan het object van onderzoek die van invloed (kunnen) zijn op de conformiteit aan de gestelde eisen. De scope is beperkt tot de wijzigingen aan het object van onderzoek; c. Een heronderzoek vindt minimaal binnen drie jaar na uitgifte van de rapportage initieel onderzoek plaats over de volledige scope van het object van onderzoek. 3. De conformiteitsbeoordelaar die de conformiteitsbeoordeling uitvoert: a. Heeft aantoonbaar ruime ervaring met het uitvoeren van technische beoordelingsopdrachten van authenticatiemiddelen of vergelijkbare objecten van onderzoek; b. Zal voor de opdracht personeel inzetten met ruime ervaring en de voor de beoordeling benodigde competenties; c. Is bij het uitvoeren van de beoordeling en in haar oordeelsvorming geheel onafhankelijk van haar opdrachtgever en de MU/AD; d. Heeft een intern kwaliteitssysteem en/of vaktechnische richtlijnen en procedures voor het uitvoeren van beoordelingsopdrachten, met inbegrip van registratie van ondersteunend bewijs, rapportering aan opdrachtgever en aan derden en – waar nodig - interne (peer) review; e. Verstrekt toestemming dat toezichthouder op elk moment, binnen 7 jaar na het uitbrengen van de rapportage van conformiteitsbeoordelaar inzage kan vorderen in de rapportage en in het bijbehorende dossier waarin het ondersteunend bewijs is vastgelegd; f. Levert voorafgaand aan de opdrachtverstrekking aan de opdrachtgever of de MU/AD een formele verklaring op waarin conformiteit aan sub a tot en met sub e op het moment van opdrachtverstrekking en gedurende de conformiteitsbeoordeling verklaard en onderbouwd wordt; g. Een testlaboratorium ingevolge ISO 17025 voor de scope "testing of information technology products" wordt vermoed aan sub b tot en met sub d te voldoen. h. De conformiteitsbeoordelaar beschikt over een bedrijfs- of beroepsaansprakelijkheidsverzekering. 4. Een onderzoek van de conformiteitsbeoordelaar wordt zodanig gepland en uitgevoerd dat een redelijke mate van zekerheid kan worden verkregen dat het object van onderzoek op het in de rapportage aangegeven moment aan de gestelde eisen voldoet. 5. De rapportage van de conformiteitsbeoordelaar bevat minimaal: a. De doelstelling van de opdracht, een beschrijving van het object van onderzoek (uniek identificerend, met datum en versienummer), de eisen op basis waarvan het object van onderzoek is beoordeeld en het plan van aanpak met de gevolgde stappen en de gehanteerde onderzoeksmethoden en aanvalstechnieken; b. Het eindoordeel over de mate waarin het object op het aangegeven moment aan de gestelde eisen voldoet, met onderbouwing; c. Belangrijkste bevindingen en aanbevelingen;	Ad 1 t/m 5 Toelichting: Ten behoeve van de voorbereiding op de conformiteitsbeoordeling is een 'Handreiking voorbereiding Conformiteitsbeoordeling' beschikbaar. Ad 3 Toelichting bij sub g: Indien van een conformiteitsbeoordelaar zoals bedoeld in sub g gebruik wordt gemaakt blijven sub a, e, f en h wel onverkort van toepassing. Ad 6 Toelichting: Dit artikel beschrijft de situatie dat de autor tot een positieve verklaring komt. Het is bij het afgeven van conformteitverklaringen een gangbare auditpraktijk dat er niet wordt gewerkt met vooraf bepaalde termijnen genoemd (bijvoorbeeld 3 maanden voor een kritieke afwijking). Een realistische oplostijd is namelijk afhankelijk van de activiteit die moet worden uitgevoerd (fundamentele systeemontwikkeling kost bijvoorbeeld meer tijd dan een aanpassing instellingen van applicaties en hardware). Daarom gaat vereist het vaststellen van deadlines maatwerk. Aangezien er een positieve auditor tot een positieve verklaring is gekomen zal de auditor de juiste uitvoering van het verbeterplan pas bij de volgende controle nagaan. De toezichthouder zal daarom geheel naar eigen inzicht de uitvoering van het verbeterplan controleren. Ad 7 Toelichting: Dit artikel beschrijft de situatie waarin de auditor tot een negatieve verklaring komt. Het rapport met de negatieve verklaring is formeel en definitief en wordt door de deelnemer aan de toezichthouder gezonden. Het is aan de Toezichthouder om al dan niet consequenties aan de negatieve verklaring van de auditor te verbinden. Het ligt daarom voor de hand dat de Deelnemer de Toezichthouder op de hoogte houdt van de afspraken die hij maakt met de auditor over de wijze waarop de oplossing en her-boordeling plaats gaat vinden.

d. Detailbevindingen, met vermelding van referenties naar het geregistreerde bewijs over de conformiteit aan de betreffende eis.

6. Opdrachtgever MOET op basis van de rapportage een verbeterplan op te stellen voor de geconstateerde afwijkingen, met daarin minimaal een oorzaakanalyse, adequate corrigerende maatregelen voor de geconstateerde afwijkingen en een oplostermijn en deadline. De gespecificeerde oplostermijn staat nadrukkelijk in verhouding tot de classificatie van de afwijking en de benodigde middelen om deze op te lossen. De termijnen voor het opstellen van het verbeterplan en de oplossingen zijn ter beoordeling aan de autitor. De opdrachtgever MOET het door de auditor geaccepteerde verbeterplan aan de toezichthouder ter beschikking te stellen.
7. Indien de conformiteitsbeoordelaar in de rapportage oordeelt dat het object van onderzoek - op het in de rapportage aangegeven moment- niet of slechts gedeeltelijk aan de gestelde eisen voldoet, MOET Opdrachtgever in overleg te treden met de conformiteitsbeoordelaar om een herbeoordeling uit te laten voeren van de corrigerende maatregelen als uitbreiding van de uitgevoerde conformiteitsbeoordeling, danwel een hernieuwd initieel onderzoek te laten uitvoeren door een conformiteitsbeoordelaar. De conformiteitsbeoordelaar kan daarbij eisen dat het verbeterplan vooraf ter beoordeling en goedkeuring wordt voorgelegd.

Implementatietermijn

Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.

De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.