# Handreiking Conformiteitstoetsing Authenticatiemiddel en -mechanisme LoA3 en LoA4

Versie 1.0

Datum 13 februari 2017

Status **Definitief**

# Wijzigingen

| Versie | Datum | Toelichting |
|---|---|---|
| 0.1 | 4 april 2016 | • Initiële opzet |
| 0.2 | 12 april 2016 | • Nieuw concept. Explicieter gemaakt dat de scope betrekking heeft op het authenticatiemiddel LoA4 (hoog) en op het authenticatie-mechanisme niveaus LoA3 en LoA4 (substantieel en hoog). |
| 0.3 | 8 augustus 2016 | • Aanpassing verwijzingen naar eisen in het nieuwe normenkader betrouwbaarheidsniveaus conform RFC 2050. |
| 1.0 | 13 februari 2017 | • Aanpassing verwijzing naar ondersteunden document functionele beveiligingsspecificaties. |

# Inhoud

# 1 Inleiding

## 1.1 Over de handreiking

Dit document bevat een handreiking voor de conformiteitstoetsing voor middelen op betrouwbaarheidsniveaus LoA 3 en LoA 4, zoals deze wordt gehanteerd binnen het Afsprakenstelsel Elektronische Toegangsdiensten.

## 1.2 Achtergrond

Het Afsprakenstelsel Elektronische Toegangsdiensten beschrijft in het Normenkader betrouwbaarheidsniveaus de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast.

De betrouwbaarheidsniveaus en de bijbehorende eisen sluiten aan bij de eIDAS-verordening (VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93) (hierna: eIDAS-verordening).

In artikel 8 van de eIDAS-verordening zijn de betrouwbaarheidsniveaus zoals die in de verordening worden onderkend (laag, substantieel en hoog) beschreven. In de eIDAS-verordening is aangegeven dat er minimale technische specificaties, normen en procedures vast zullen worden gesteld aan de hand waarvan de betrouwbaarheidsniveaus laag, substantieel en hoog worden bepaald voor de elektronische identificatiemiddelen.
Deze specificaties zijn opgenomen in de UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen (hierna: Uitvoeringsverordening).

De uitvoeringsverordening geeft nadere invulling aan de procedurele eisen en aan technische eisen voor authenticatiemiddelen en authenticatiemechanismen voor de niveaus laag, substantieel en hoog. Deze zullen worden verwerkt in het Afsprakenstelsel Elektronische Toegangsdiensten, waarbij de niveaus substantieel en hoog corresponderen met de in het afsprakenstelsel gedefinieerde niveaus LoA 3 en LoA 4).

Voor wat betreft de technische eisen die worden gesteld aan het authenticatiemiddel en authenticatiemechanismen, stelt de uitvoeringsverordening in de overwegingen dat certificatie van de IT-beveiliging op basis van internationale normen een belangrijk instrument is voor de controle of producten voldoen aan de beveiligingseisen van deze uitvoeringshandeling. Aan de wijze waarop de conformiteitstoetsing dient te worden uitgevoerd, wordt verder geen invulling gegeven.

## 1.3 Doelstelling

Het doel van dit document om de deelnemers aan het Afsprakenstelsel Elektronische Toegangsdiensten en de conformiteitsbeoordelaar een richtsnoer te bieden bij het uitvoeren van de conformiteitstoetsing van het

authenticatiemiddel op niveau LoA 4 en van de authenticatiemechanismen op de niveaus LoA 3 en LoA 4.
Deze handreiking beschrijft een proces dat de deelnemer kan volgen om aan te tonen dat aan de beveiligingseisen wordt voldaan van middelen op niveau 4 en het authenticatiemechanisme op de niveaus 3 en 4.
Ter ondersteuning bij de risicoanalyse en definiëren van specificaties/maatregelen is de bijlage 'Functionele beveiligingsspecificaties Authenticatiemiddel LoA4 en –mechanisme LoA3 en LoA4' opgesteld. Dit document is een bijlage bij de handreiking en heeft tot doel om behulpzaam te zijn in het proces van risicoanalyse bij het in kaart brengen van de relevante dreigingen, geïmplementeerde en nog te implementeren beveiligingsspecificaties.

### 1.4 Indeling van dit document

In hoofdstuk 2 wordt de scope en het object van onderzoek beschreven.
In hoofdstuk 3 wordt de aanpak voor de conformiteitstoetsing beschreven en in hoofdstuk 4 zijn de toepasselijke eisen voor de authenticatiemiddelen en -mechanismen opgenomen, afkomstig vanuit de eIDAS-verordening en de Uitvoeringsverordening, aangevuld met nadere eisen uit het Afsprakenstelsel ten aanzien van het authenticatiemiddel en -mechanisme en de conformiteitstoetsing.

# 2 Scope van de conformiteitstoetsing

## 2.1 Beschrijving van de scope

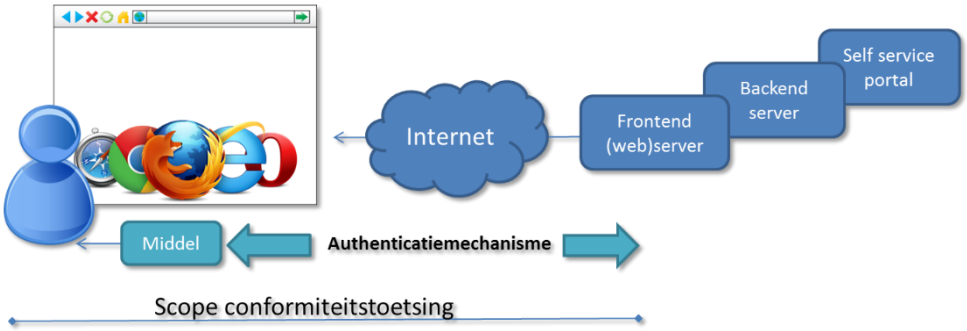
De scope van de conformiteitstoetsing betreft

- de kwaliteit van het authenticatiemiddel dat wordt gebruikt tijdens de elektronische authenticatiefase: de robuustheid van het authenticatiemiddel. Dit geldt alleen voor het niveau Hoog (LoA4).
- de kwaliteit van het authenticatiemechanisme dat wordt gebruikt tijdens de elektronische authenticatiefase: de wijze waarop het authenticatiemiddel tijdens het gebruik functioneert en de maatregelen die zijn getroffen om de kwaliteit hierbij te borgen. Dit geldt voor de niveaus Substantieel en Hoog (LoA3 en LoA4).

## 2.2 Grafische weergave van de scope

De scope van de conformiteitsbeoordeling kan als volgt grafisch worden weergegeven. Hierbij zijn opgenomen:

- De omgeving van de gebruiker: het door hem gehanteerde authenticatiemiddel (LoA4) en de webbrowser die wordt gebruikt voor de interactie met de Authenticatiedienst
- De omgeving van de Authenticatiedienst, voorzover deze relevant is voor de interactie tijdens de elektronische authenticatiefase
- Het authenticatiemechanisme: de wijze waarop het authenticatiemiddel wordt gebruikt tijdens de elektronische authenticatiefase (LoA3 en LoA4).



# 3 Aanpak conformiteitstoetsing

## 3.1 Aanpak

Hieronder wordt een aanpak beschreven voor de conformiteitstoetsing van het authenticatiemiddel op niveau LoA 4 en van het authenticatiemechanisme op de niveaus LoA3 en LoA 4.

Bij de hieronder uitgewerkte aanpak van de conformiteitstoetsing is een gedegen voorbereiding door de Beoordeelde randvoorwaardelijk. De beoordeelde is in de meeste gevallen de Deelnemer/Authenticatiedienst, danwel met medewerking van zijn toeleverancier. Bij de voorbereiding door de Beoordeelde staat de Risicoanalyse centraal, uitgevoerd in de vorm van een workshop en gericht op het Authenticatiemiddel (LoA4) en het Authenticatiemechanisme (LoA3/LoA4). Voordat de Workshop Risicoanalyse kan worden uitgevoerd dient de Beoordeelde deze voor te bereiden, zodat tijdens de workshop het benodigde materiaal ter onderbouwing voorhanden is. Nadat de Workshop is afgerond, kan de Conformiteitsbeoordelaar zijn onderzoek starten. Hierbij wordt in belangrijke mate gebruik gemaakt van de voorbereidende werkzaamheden van de Beoordeelde.

## 3.2 Voorbereiding Workshop Risicoanalyse door Beoordeelde

De risicoanalyse vindt plaats in de vorm van een workshop. De Beoordeelde voert de volgende activiteiten uit ter voorbereiding.

| nr | Handreiking | Toelichting |
|---|---|---|
| a) | Ter voorbereiding van de workshop verzamelt en documenteert een beveiligingsfunctionaris van de authenticatiedienst een of meerdere (technische) beveiliging *checklists* die aansluiten op het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3 en/of LoA4). | *Voor middelen die gebaseerd zijn op mobiele apparaten kan dit bijvoorbeeld de OWASP Mobile Apps Checklist zijn. Zie https://www.owasp.org*<br>*Daarnaast kan gebruik worden gemaakt van het document 'Functionele beveiligingsspecificaties LoA4 middelen en LoA3 en LoA4 authenticatiemechanisme'.* |
| b) | Ter voorbereiding van de workshop maken de volgende type personen een gedocumenteerde vergelijking met de checklists uit het vorige punt en onderkennen daarbij mogelijke kwetsbaarheden in de opzet van het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4):<br>1. ontwikkelaars van het middel,<br>2. de (toekomstige) beheerders van dit middel waaronder infrastructurele beheerders (netwerk, besturingssystemen) en applicatieve beheerders (applicaties, databases).<br>Deze vergelijking en de daaruit voortkomende kwetsbaarheden worden gedocumenteerd (bijvoorbeeld door de beveiligingsfunctionaris). | *Voorbeelden zijn:*<br>• *geen controle van TLS certificaten vanuit een mobiele applicatie*<br>• *een platform waarbij één applicatie de data binnen een andere applicatie kan benaderen (niet het geval bij de meeste mobiele platforms).* |
| c) | Ter voorbereiding van de workshop analyseert een beveiligingsfunctionaris van de authenticatiedienst beveiligingsincidenten of | • *Deze analyse kan gebaseerd zijn op een zoektocht op het internet maar ook op basis van een samenwerking* |

| nr | Handreiking | Toelichting |
|---|---|---|
| | signalen die zich hebben voorgedaan rond soortgelijke authenticatiemiddelen en -mechanismen. Deze analyse en de daarbij onderzochte beveiligingsincidenten worden gedocumenteerd. | *verband waarin organisaties security incidenten delen.*<br>• *Ter illustratie; bij SMS gebaseerde middelen zijn de afgelopen jaren incidenten geweest rond 'SIM wissels' waarbij fraudeurs middels social engineering bij telefoonwinkels er in slaagden een SIM te registreren op andermans telefoonnummer. Dit heeft bij sommige banken geleid tot de maatregel dat zij worden geïnformeerd dat een SIM verandering is opgetreden waarbij de telefoon dan ook een periode niet kon worden gebruikt als authenticatiemiddel.*<br>• *Bij mobiele app gebaseerde middelen zullen de relevante incidenten hieromtrent moeten worden verzameld.* |
| d) | Ter voorbereiding van de workshop worden de genodigden voor de workshop van de volgende informatie voorzien:<br>• conceptuele werking van het authenticatiemiddel (LoA4) waaronder zowel de registratie en verstrekking daarvan alsmede het gebruik daarvan leidende tot een authenticatie bij een dienstverlener (authenticatiemechanisme)<br>• conceptuele werking van het authenticatiemechanisme (LoA3/LoA4), waaronder wordt verstaan het gebruik van het middel leidende tot een authenticatie bij een dienstverlener en de bijbehorende interactie<br>• de beveiligingsdoelstellingen van het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4), afgeleid van het normenkader<br>• het resultaat van de vergelijking met de relevante beveiliging checklists (zie onder 2)<br>• het resultaat van de analyse van beveiligingsincidenten of signalen die zich hebben voorgedaan rond soortgelijke middelen en mechanismen (zie onder 3) | |

## 3.3 Uitvoering Workshop Risicoanalyse door Beoordeelde

Nadat de voorbereiding is afgerond, kan de Workshop Risicoanalyse worden uitgevoerd.

| nr | Handreiking | Toelichting |
|---|---|---|
| e) | De authenticatiedienst voert, in de vorm van een workshop, een risicoanalyse uit rond het authenticatiemiddel (LoA4) en -mechanisme (LoA3/LoA4), in lijn met ISO 27005 of vergelijkbaar waarbij:<br>• op gestructureerde wijze dreigingen en | - *De verwijzing naar 'het gebruik van het middel' geeft aan dat bij de risico analyse ook de omgeving van de gebruiker moet worden meegenomen waaronder bijvoorbeeld het bestaan van malware in zijn applicatieve* |

| nr | Handreiking | Toelichting |
|---|---|---|
| | kwetsbaarheden met betrekking tot het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4) zijn geïdentificeerd.<br>• per onderscheiden dreiging en kwetsbaarheid wordt de mogelijke manifestatie beschreven in de vorm van een aanval scenario hoe een dreiging een kwetsbaarheid exploiteert en wat daarmee wordt bereikt (impact).<br>• per onderkend aanval scenario wordt de impact op de beveiligingsdoelstelling van het middel beoordeeld zoals afgeleid van het Idensys normenkader kwaliteit Substantieel/Hoog alsmede het benodigde aanvallerspotentieel om de aanval uit voeren.<br><br>De uitgevoerde risicoanalyse heeft als doelstelling te onderbouwen dat er **GEEN** *succesvol* aanvalsscenario bestaat dat:<br>• realiseert dat geheel of gedeeltelijk de beveiligingsdoelstelling van het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4) doorbreekt, bijv. dat de aanvaller in staat is het middel fysiek of logisch te kopiëren vanuit een malware geïnfecteerde applicatieve omgeving of in staat is om binnen het authenticatiemechanisme de vereiste terugkoppeling naar de gebruiker te manipuleren;<br>• uitgevoerd kan worden door een aanvaller met potentieel MODERATE ten aanzien van het authenticatiemechanisme op LoA3 (niveau Substantieel);<br>• uitgevoerd kan worden door een aanvaller met potentieel HIGH voor het authenticatiemiddel en het authenticatiemechanisme op LoA4 (niveau Hoog).<br><br>Van de risicoanalyse workshop is een gedocumenteerde verslaglegging waarin bovengenoemde punten a), b) en c) worden beschreven en waarin het ontbreken van het bovengenoemde aanvalsscenario als conclusie is opgenomen alsmede de onderbouwing daarvan. De verslaglegging is ondertekend door een representant van het management van de authenticatiedienst die ook aanwezig was bij de risicoanalyse workshop zelf (zie onder 7). | *omgeving.*<br>- *Voor schatting van het aanvalspotentieel zie onder en het bijgevoegde Excel bestand.* |
| f) | De duur van de risicoanalyse workshop bedraagt minstens een werkdag (8 uur). | |
| g) | Bij de risicoanalyse workshop zijn de volgende typen personen gedurende de workshop aanwezig:<br>• technische ontwikkelaars van het authenticatiemiddel (LoA4) en het - | |

| nr | Handreiking | Toelichting |
|---|---|---|
| | mechanisme (LoA3/LoA4);<br>• beheerders (infrastructureel, applicatief) van de authenticatiedienst die het middel in productie gaan nemen<br>• beveiligingsfunctionaris(en) van de authenticatiedienst die:<br>o zicht heeft op de technische beveiligingsmaatregelen binnen de authenticatiedienst en mogelijke zwakheden daarbij<br>o inzicht heeft in security incidenten die zich in het verleden hebben voorgedaan bij de organisatie<br>• een ervaren (helpdesk) medewerker, die zicht heeft op de wijze waarop een klant omgaat met middelen en de interactie tijdens het gebruik<br>• een (gedelegeerd) lid van het management van de authenticatiedienst die verantwoordelijkheid heeft voor informatiebeveiliging | |
| h) | De risicoanalyse workshop wordt begeleid door een persoon die aantoonbare kennis en ervaring heeft in het uitvoeren van risicoanalyses waaronder het leggen van verbanden tussen (beveiliging) techniek en bedrijfsdoelstellingen. | |
| i) | Het verslag van de risicoanalyse legt behalve de datum en de tijdspanne waarop de risicoanalyse plaatsvond ook de aanwezigen van de workshop vast. | |
| j) | Bij de risicoanalyse workshop wordt de werking van het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4), alsmede de daarop van toepassing zijnde beveiligingsdoelstellingen aan alle aanwezigen op hoofdlijnen toegelicht. | |
| k) | Op gestructureerde wijze worden de dreigingen (wie/wat) en de kwetsbaarheden (in de zin van ISO27005) rond het authenticatiemiddel (LoA4) en het -mechanisme (LOA3/LoA4) besproken. Minimaal wordt daarbij geadresseerd:<br>• incidenten die zich eerder bij de authenticatiedienst hebben voorgedaan of bij anderen<br>• kwetsbaarheden die naar voren zijn gekomen<br>• de dreigingen en kwetsbaarheden genoemd in ISO 29115 en ISO 27005<br>• kwetsbaarheden vanuit het perspectief van het ontbreken van maatregelen uit de ISO 27002 norm. | |
| l) | Op basis van de vorige stap worden tijdens de workshop mogelijke aanvalsscenario's bepaald voor het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4), i.e. mogelijke manifestaties hoe een dreiging een kwetsbaarheid exploiteert en wat daarmee wordt bereikt (impact) | |

| nr | Handreiking | Toelichting |
|---|---|---|
| m) | Per onderkend aanvalsscenario wordt tijdens de workshop:<br>• onderzocht of deze realiseert dat de beveiligingsdoelstelling van het authenticatiemiddel (LoA4) en het authenticatiemechanisme (LoA3/LoA4) geheel of gedeeltelijk wordt doorbroken, bijv. dat de aanvaller in staat is het middel fysiek of logisch te kopiëren vanuit een malware geïnfecteerde applicatieve omgeving of in staat is om binnen het authenticatiemechanisme de vereiste terugkoppeling naar de gebruiker te manipuleren;<br>• het benodigde aanvalspotentieel voor het uitvoeren van het aanvalsscenario ingeschat, in lijn met Appendix B.4 van ISO/IEC 18045 "Methodology for IT security evaluation" | *Zie bijgevoegd Excel bestand bijlage 6 met de tool voor het bepalen van het aanvalspotentieel.* |
| n) | Voor elk aanvalsscenario onderscheiden in de vorige stap worden de *succesvolle* scenario's onderkend. Dit is een aanvalsscenario:<br>- dat geheel of gedeeltelijk de beveiligingsdoelstelling van het authenticatiemiddel (LoA4)/-mechanisme (LoA3/LoA4) doorbreekt **EN**<br>- dat een aanvallerpotentieel benodigd dat lager is dan waartegen het bestand moet zijn. Dit betreft het aanvalspotentieel "High" voor het authenticatiemiddel op niveau LoA4 (niveau High) en het aanvalspotentieel "Moderate" voor authenticatiemechanismen op niveau LoA3/LoA4 (niveau substantieel en High). | *Doorbreken van het beveiligingsdoelstelling van het middel/mechanisme is bijvoorbeeld een scenario waarbij de aanvaller in staat is het middel fysiek of logisch te kopiëren vanuit een malware geïnfecteerde applicatieve omgeving of in staat is om de vereiste terugkoppeling naar de gebruiker te manipuleren. Noot: bij het authenticatiemechanisme op niveau LoA3 (niveau Substantieel) is de vereiste terugkoppeling beperkt.* |
| o) | Voor elk onderkend succesvol aanvalsscenario worden mitigerende maatregelen benoemd en beschreven en wordt gemotiveerd dat het aanvalsscenario niet meer succesvol is. Daarbij wordt ook onderzocht of de mitigerende maatregelen geen nieuwe succesvolle aanvalsscenario's introduceren. | • *Een maatregel kan bijvoorbeeld zijn dat een authenticatiemiddel App niet op bepaalde platformen beschikbaar is.* |
| p) | De mitigerende maatregelen uit de vorige stap worden gedocumenteerd in een Risk Treatment plan, inclusief een tijdsplanning van de implementatie daarvan. | |

## 3.4 Uitvoering conformiteitsbeoordeling door de conformiteitsbeoordelaar

Nadat de voorbereidende werkzaamheden door de Beoordeelde zijn afgerond, kan de Conformiteitsbeoordelaar zijn onderzoek starten. Aan het uitvoeren van de Conformiteitsbeoordeling zijn nadere eisen gesteld. Deze zijn uitgewerkt in de Toepasselijke normen Afsprakenstelsel (par. 4.3, vanaf nr. 10).

| nr | Handreiking | Toelichting |
|---|---|---|

| nr | Handreiking | Toelichting |
|---|---|---|
| | Het onderzoek door de conformiteitsbeoordelaar start pas nadat het Risk Treatment plan is geïmplementeerd. | *Dit te vergelijken met een Stage 1 onderzoek (vooronderzoek) van een audit in de zin van ISO 27006.* |
| | De beoordelaar neemt kennis van de resultaten van de risicoanalyse workshop en krijgt daartoe toegang tot alle (verplicht) gedocumenteerde informatie waaronder de resultaten van de inventarisatie kwetsbaarheden en relevante beveiligingsincidenten, de onderkende (succesvolle) aanvalsscenario's en het Risk Treatment plan. In zijn rapportage maakt de conformiteitsbeoordelaar melding van eventuele hiaten in dit proces. | |
| | Indien de conformiteitsbeoordelaar meent dat het gevolgde proces onvoldoende zorgvuldig is geweest zodat mogelijk relevante aanvalsscenario's zijn gemist dan rapporteert de conformiteitsbeoordelaar dat en sluit de conformiteitsbeoordelaar zijn onderzoek. De beoordeelde dient het risicoanalyse proces dan opnieuw uit te voeren en de conformiteitsbeoordelaar dient vervolgens opnieuw kennis te nemen van de resultaten (herhaling stap 2). | |
| | De conformiteitsbeoordelaar vormt een (penetratie) testplan op basis van de (meest relevante) aanvalsscenario's die zijn onderkend vanuit de risicoanalyse en voert dit uit. | *Dit is te zien als een Stage 2 onderzoek van een audit in de zin van ISO 27006.* |
| | In zijn rapportage doet de conformiteitsbeoordelaar melding van geconstateerde afwijkingen van de conclusie van de authenticatiedienst rond het niet bestaan van succesvolle aanvalsscenario's, zoals weergegeven in de risicoanalyse workshop verslaglegging. | *[Rapportage]* |

# 4 Bijlage: Toepasselijke normen

## 4.1 Toepasselijke normen eIDAS-verordening

De volgende normen vanuit de eIDAS-verordening zijn relevant voor de conformiteitstoetsing:

| **Norm** | **Opmerking** |
|---|---|
| Artikel 8 inzake Betrouwbaarheidsniveaus van stelsels voor elektronische identificatie<br>1. Een stelsel voor elektronische identificatie dat is aangemeld krachtens artikel 9, lid 1, omschrijft betrouwbaarheidsniveaus laag, substantieel en/of hoog voor op grond van dat stelsel uitgegeven elektronische identificatiemiddelen.<br><br>*2. De betrouwbaarheidsniveaus laag, substantieel en hoog voldoen respectievelijk aan de volgende criteria:*<br><br>*a) het betrouwbaarheidsniveau laag betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een beperkte mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen;*<br><br>b) het betrouwbaarheidsniveau substantieel betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een substantiële mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen;<br><br>c) het betrouwbaarheidsniveau hoog betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een hogere mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt dan een elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te voorkomen.<br><br>3. Uiterlijk op 18 september 2015, rekening houdend met de geldende internationale normen en behoudens lid 2, stelt de Commissie bij uitvoeringshandeling minimale technische specificaties, normen en procedures vast aan de hand waarvan de betrouwbaarheidsniveaus laag, substantieel en hoog worden bepaald voor de elektronische identificatiemiddelen als bedoeld in lid 1.<br>Deze minimale technische specificaties, normen en procedures worden vastgesteld onder verwijzing naar de betrouwbaarheid en kwaliteit van de volgende elementen:<br>a) de procedure om de identiteit van de natuurlijke of rechtspersoon die om uitgifte van het elektronisch identificatiemiddel verzoekt, te bewijzen en te verifiëren;<br>b) de procedure voor de uitgifte van het aangevraagde elektronische identificatiemiddel;<br>c) het authenticatiemechanisme, door middel waarvan de natuurlijke of rechtspersoon het elektronische | Middelen op het betrouwbaarheids-niveau Laag blijven buiten de scope van de conformiteits-toetsing. |

| Norm | Opmerking |
|---|---|
| identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij;<br>d) de entiteit die het elektronische identificatiemiddel uitgeeft;<br>e) ieder ander orgaan dat betrokken is bij de uitgifte van het elektronische identificatiemiddel en<br>f) de technische en veiligheidsspecificaties van het uitgegeven elektronische identificatiemiddel.<br>Die uitvoeringsbesluiten worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld. | |

## 4.2 Toepasselijke normen Uitvoeringsverordening

De volgende normen vanuit de Uitvoeringsverordening zijn relevant voor de conformiteitstoetsing. Wij hebben omwille van de uniforme uitleg de originele Engelse tekst opgenomen.

| Norm | Opmerking |
|---|---|
| **2.2. Electronic identification means management** | |
| **2.2.1 Electronic identification means characteristics and design**<br><br><u>Substantial</u><br>1.The electronic identification means utilises at least two authentication factors from different categories.<br>2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.<br><br><u>High</u><br>Level substantial, plus:<br>1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential<br>2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others. | |
| **2.3. Authentication** | |
| **2.3.1. Authentication mechanism**<br><br><u>Low</u><br>1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.<br>2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.<br>3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.<br><br><u>Substantial</u><br>Level low, plus:<br>1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. | |

| Norm | **Opmerking** |
|---|---|
| 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.<br><br><u>High</u><br>Level substantial, plus:<br>The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms. | |
| **2.4. Management and organisation** | |
| **2.4.6. Technical controls**<br><br><u>Low</u><br>1.The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.<br>2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.<br>3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.<br>4.Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.<br>5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.<br><br><u>Substantial</u><br>Same as level low, plus:<br>Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering<br><br><u>High</u><br>Same as level substantial. | |

## 4.3 Toepasselijke normen Afsprakenstelsel

De volgende normen vanuit het Afsprakenstelsel zijn relevant voor de conformiteitstoetsing. Er kunnen verschillen optreden tussen de hier opgenomen normtekst en de gepubliceerde tekst van het Afspraken. De gepubliceerde tekst van het Afsprakenstelsel is altijd leidend en geldig.

| nr. | Ref eIDAS | Ref AS | Generieke eisen middelen LoA3 | Generieke eisen middelen LoA4 | Toelichting |
|---|---|---|---|---|---|
| 1 | § 2.3.1 | Par. 2.3.1 onder LoA1 punt 3<br><br>LoA4 punten 1 t/m 4 | De AD MOET in het aanlogscherm tonen bij welke Dienstverlener de Gebruiker gaat aanloggen. | Idem en<br>1. Het auhenticatiemiddel MOET de Gebruiker notificeren (onafhankelijk van de browser die hij gebruikt) van zijn inlogpoging bij een specifieke dienst of dienstverlener .<br>2. De notificatie MOET zijn gekoppeld aan het gebruik van diensten op het niveau van het middel.<br>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.<br>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. | **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 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 verschillende het LoA van het middel of lager. |
| 2 | § 2.3.1 | Par. 2.3.1 onder LoA3 punt 2 | De toegang tot diensten van elke afzonderlijke dienstverlener MOET het aanloggen met behulp van het authenticatiemiddel vereisen. | Idem | ***Toelichting**:* Single Sign On voor diensten van een enkele dienstverlener op LoA3 en LoA4 is toegestaan. SSO tussen dienstverleners is slechts toegestaan op |

| nr. | Ref eIDAS | Ref AS | Generieke eisen middelen LoA3 | Generieke eisen middelen LoA4 | Toelichting |
|---|---|---|---|---|---|
| | | | | | 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 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. |
| 3 | § 2.3.1 | Par. 2.3.1 onder LoA 3 punt 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. | Idem | ***Toelichting**:* Authenticatie onder een merk van het AS wil zeggen onder Idensys respectievelijk 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. |
| 4 | § 2.3.1 | Par. 2.2.1 onder LoA3 | 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 | Idem | ***Toelichting:*** Dit betekent dat:<br>• de Gebruiker op betrouwbare wijze informatie wordt getoond die bevestigd moet worden met een response van de Gebruiker, of; |

| nr. | Ref eIDAS | Ref AS | Generieke eisen middelen LoA3 | Generieke eisen middelen LoA4 | Toelichting |
|---|---|---|---|---|---|
| | | | applicatie (o.a. browser) plaatsvinden. | | • de gebruiker voert zelf informatie in op middel en maakt zo deel uit maakt van de response.<br>In deze eis bedoelde handelingen van de Gebruiker zijn bijvoorbeeld:<br>• 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;<br>• Het door de gebruiker invoeren van een PIN op een separate cardlezer waarmee het certificaat als authenticatiefactor wordt ingezet;<br>• Het door de gebruiker presenteren en laten 'lezen' van zijn biometrische kenmerk als authenticatiefactor.<br>Als de zowel 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:<br>• 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.<br>Voorbeeldsituaties:<br>• Inloggen via browser van een smartphone en ontvangst en gebruik op het zelfde toestel van een sms-code voor de afhandeling van de authenticatie. |

| nr. | Ref eIDAS | Ref AS | Generieke eisen middelen LoA3 | Generieke eisen middelen LoA4 | Toelichting |
|---|---|---|---|---|---|
| | | | | | • Inloggen via de browser van een tablet waar ook de OTP app op staat. |
| | §2.2.1 | Par 2.2.1 onder LoA4 | n.v.t. | 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). | ***Toelichting***: De eis omvat de doelstellingen:<br>• het authenticatie-middel MAG NIET gebruikt kunnen worden zonder expliciete actie van de gebruiker in lijn met het multi-factor gebruik;<br>• het authenticatie-middel MAG NIET andere gegevens bevestigen dan wat de gebruiker verwacht; De toekomstige response van het middel MAG NIET vooraf te bepalen zijn;<br>• Specifiek voor LoA3: Het middel MAG NIET bij eventueel klonen in combinatie met het authenticatiemechanisme bruikbaar zijn..<br>• Specifiek voor LoA4: Het middel MAG NIET te klonen zijn. |
| | | Par 3.2.1 onder LoA4 punt 5 | n.v.t. | 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. | ***Toelichting***: De eis omvat de doelstellingen:<br>het authenticatie-middel MAG NIET gebruikt kunnen worden zonder expliciete actie van de gebruiker in lijn met het multi-factor gebruik;<br>het authenticatie-middel MAG NIET andere gegevens bevestigen dan wat de gebruiker verwacht; De toekomstige response van het middel MAG NIET vooraf te bepalen zijn;<br>Specifiek voor LoA3: Het middel MAG NIET bij eventueel klonen in combinatie met het |

| nr. | Ref eIDAS | Ref AS | Generieke eisen middelen LoA3 | Generieke eisen middelen LoA4 | Toelichting |
|---|---|---|---|---|---|
| | | | | | authenticatiemechanisme bruikbaar zijn.. Specifiek voor LoA4: Het middel MAG NIET te klonen zijn. |
| 5 | § 2.2.1 | Par. 2.2.1 onder LoA 3 punt 1 | De authenticatie MOET het gebruik van minimaal twee van de volgende authenticatiefactoren omvatten:<br>• kennis van de gebruiker,<br>• uniek bezit van de gebruiker, of<br>• een biometrische eigenschap van de gebruiker. | Idem | |
| 6 | § 2.2.1 | Par 2.2.1 onder LoA2 punt 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. | Idem | ***Toelichting:*** In het geval van multifactormiddelen moet de sterkte van de wachtwoordcomponent in de risicocontext worden bepaald. |
| 8 | § 2.3.1 | Par. 2.3.1 onder LoA3 punt 5 respectievelijk LoA4 punt 7 | Het correct functioneren van het authenticatiemeachanisme 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). | Het correct functioneren van een authenticatiemechanisme 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 evaluatie norm (ISO/IEC 18045). | ***Toelichting:*** *Dit omvat de doelstellingen:*<br>1. *het authenticatie-middel MAG NIET niet gebruikt kunnen worden zonder bewuste actie van de gebruiker in lijn met het multi-factor gebruik;*<br>2. *het authenticatie-middel MAG NIET andere gegevens bevestigen dan wat de gebruiker verwacht; * toekomstige response van het middel MAG NIET vooraf te bepalen zijn;*<br>3. *het middel MAG NIET te klonen zijn.* |
| 9 | § 3.2.1 | Par 3.2.1 onder LoA3 punt 4 | De MU/AD MOET jaarlijks het authenticatiemechanisme onderwerpen aan een risico analyse daarbij rekening houdend met (nieuwe) | Idem | |

| nr. | Ref eIDAS | Ref AS | Generieke eisen middelen LoA3 | Generieke eisen middelen LoA4 | Toelichting |
|---|---|---|---|---|---|
| | | | 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. | | |

| | Ref eIDAS | Ref AS | Eisen conformiteitsbeoordeling middelen LoA3 | Eisen conformiteitsbeoordeling middelen LoA4 | Opmerking |
|---|---|---|---|---|---|
| 10 | § 2.4.7 | Par 2.4.7 onder LoA3 punt 1 | De MU/AD moet 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. | Idem | ***Opmerking****: maak bijvoorbeeld onderscheid tussen major changes, minor changes en maintenance.* |
| 11 | § 2.4.7 | Par 2.4.7 onder LoA3 punt 2 | Bij de conformiteitsbeoordeling wordt onderscheid gemaakt tussen verschillende typen onderzoek, te weten: een initieel onderzoek, een herhalingsonderzoek en een heronderzoek. | Idem | ***Toelichting***:<br><br>***Op LoA3***: De MU/AD toont conformiteit van het authenticatiemechanisme aan de gestelde eisen aan door het overleggen van een rapportage van een |

| | Ref eIDAS | Ref AS | Eisen conformiteitsbeoordeling middelen LoA3 | Eisen conformiteitsbeoordeling middelen LoA4 | Opmerking |
|---|---|---|---|---|---|
| | | | a. Een initieel onderzoek is een eerste beoordeling over de volledige scope van het object van onderzoek op basis van de gestelde eisen.<br>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.<br>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. | | conformiteitsbeoordelaar.<br><br>***Op LoA4***: De MU/AD toont conformiteit van het authenticatiemechanisme en het authenticatiemiddel aan de gestelde eisen aan door het overleggen van een rapportage van een conformiteitsbeoordelaar. |
| 12 | § 2.4.7 | Par. 2.4.7 onder LoA3 punt 3 | De conformiteitsbeoordelaar die de conformiteitsbeoordeling uitvoert:<br><br>a. heeft aantoonbaar ruime ervaring met het uitvoeren van technische beoordelingsopdrachten van authenticatiemiddelen, -mechanismen of vergelijkbare objecten van onderzoek.<br>b. zal voor de opdracht personeel inzetten met ruime ervaring en de voor de beoordeling benodigde competenties<br>c. is bij het uitvoeren van de beoordeling en in haar oordeelsvorming geheel onafhankelijk van haar opdrachtgever en de MU/AD<br>d. heeft een intern kwaliteitssysteem en/of vaktechnische richtlijnen en | Idem | ***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. |

| | Ref eIDAS | Ref AS | Eisen conformiteitsbeoordeling middelen LoA3 | Eisen conformiteitsbeoordeling middelen LoA4 | Opmerking |
|---|---|---|---|---|---|
| | | | 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.<br>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.<br>f. levert voorafgaand aan de opdrachtverstrekking aan de opdrachtgever of de MU/AD een formele verklaring op waarin conformiteit aan sub 1 tot en met sub 5 op het moment van opdrachtverstrekking en gedurende de conformiteitsbeoordeling verklaard en onderbouwd wordt.<br>g. Een testlaboratorium ingevolge ISO 17025 voor de scope "testing of information technology products" wordt vermoed aan sub 2 tot en met sub 4 te voldoen.<br>h. De conformiteitsbeoordeelaar beschikt over een bedrijfs- of beroepsaansprakelijkheidsverzeke-ring. | | |
| 13 | § 2.4.7 | Par. 2.4.7 onder LoA3 punt 4 | Een onderzoek van de conformiteitsbeoordelaar wordt zodanig gepland en uitgevoerd dat een redelijke mate van zekerheid kan worden verkregen dat het object van | Idem | |

| | Ref eIDAS | Ref AS | Eisen conformiteitsbeoordeling middelen LoA3 | Eisen conformiteitsbeoordeling middelen LoA4 | Opmerking |
|---|---|---|---|---|---|
| | | | onderzoek op het in de rapportage aangegeven moment aan de gestelde eisen voldoet. | | |
| 14 | § 2.4.7 | Par 2.4.7 onder LoA3 punt 5 | De rapportage van de conformiteitsbeoordelaar bevat minimaal:<br><br>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.<br>b. Het eindoordeel over de mate waarin het object op het aangegeven moment aan de gestelde eisen voldoet, met onderbouwing.<br>c. Belangrijkste bevindingen en aanbevelingen.<br>d. Detailbevindingen, met vermelding van referenties naar het geregistreerde bewijs over de conformiteit aan de betreffende eis. | Idem | |

# 5 Bijlage: Functionele beveiligingsspecificaties authenticatiemiddel LoA4 en –mechanisme LoA3 en LoA4

Deze bijlage is in een separaat document op genomen met een gelijknamige titel.
De bijlage betreft een hulpmiddel bij de risicoanalyse en opstellen van beveiligingsspecificaties.
Deze beveiligingsspecificaties zijn input voor de auditor die de conformiteitstoets uitvoert.

# 6 Bijlage: Tool voor het bepalen van het aanvalspotentieel.

De tool is behulpzaam bij het berekenen van het aanvalspotentieel zoals is aangegeven in paragraaf 3.3 stap m).

Het betreffende Excelbestand is hieronder ingevoegd.

20170213 Bijlage Aanvalspotentieel toc