5 Bijlage: Functionele beveiligingsspecificaties Authenticatiemiddel LoA4 en -mechanisme LoA3 en LoA4

Bijlage bij Handreiking Conformiteitstoetsing Authenticatiemiddel en -mechanisme LoA3 en LoA4

Versie	1.0
Datum	13 februari 2017
Status	**Definitief**

Wijzigingen

Versie	Datum	Toelichting
0.1	5 september 2016	Initiële opzet
0.2	12 september 2016	Initiële opzet aangepast op basis van voortschrijdend inzicht. Nadere uitwerking
0.3	19 september 2016	Opzet aangepast n.a.v. overleg met Patrick Paling en Johan van den Bosch. Nadere uitwerking.
0.4	5 oktober 2016	Figuren aangepast na overleg met Michiel Dollenkamp en zijn review commentaar verwerkt. Volledige uitwerking gemaakt. Rekening gehouden met feit dat voor het authenticatiemiddel alleen specificaties op LoA4 opgesteld moeten worden.
0.5	7 oktober 2016	Review commentaar van Patrick Paling verwerkt.
0.6	13 oktober 2016	Review commentaar van Johan van den Bosch verwerkt.
0.7	1 november 2016	Review commentaar van Eric Verheul verwerkt.
0.8	16 januari 2017	Review commentaar verwerkt van Rogier Pafort (CreAim), Finanda van der Kamp (KPN) en Eric Verheul.
0.9	2 februari 2017	Finale review

Inhoud

Wijzigingen **2**

Inhoud **3**

1 Inleiding **4**

1.1 Doelstelling en scope *4*

1.2 Indeling van dit document *4*

2 Authenticatiemiddel en authenticatiemechanisme **6**

3 Aanpak om tot functionele beveiligingsspecificaties te komen **10**

3.1 Aanpak *10*

3.2 Identificatie van assets en dreigingen *10*

4 Functionele beveiligingsspecificaties **13**

4.1 Functionele beveiligingsspecificaties voor het authenticatiemiddel (niveau Hoog/LoA4) *14*

4.2 Functionele beveiligingsspecificaties voor het Authenticatiemechanisme (niveaus Substantieel/LoA3 en Hoog/LoA4) *18*

5 Referenties **23**

1 Inleiding

1.1 Doelstelling en scope

Het Afsprakenstelsel Elektronische Toegangsdiensten (eTD) [1] is een set van standaarden, afspraken en voorzieningen voor de geautoriseerde toegang tot digitale diensten. In het Normenkader betrouwbaarheidsniveaus [2] zijn betrouwbaarheidsniveaus gedefinieerd. De betrouwbaarheidsniveaus LoA3 en LoA4 sluiten aan bij de betrouwbaarheidsniveaus Substantieel en Hoog zoals gedefinieerd in de eIDAS Verordening (EU) 910/2014 [5] en uitgewerkt in de eIDAS Uitvoeringsverordening (EU) 2015/1502 [6].

Voor toelating tot het afsprakenstelsel moeten authenticatiemiddelen op LoA4 en authenticatiemechanismen op LoA3 en LoA4 een conformiteitstoets ondergaan waarin wordt aangetoond dat voor LoA4 authenticatiemiddel en –mechanisme bestand zijn tegen attack potential high en voor LoA3 het authenticatiemechanisme bestand is tegen attack potential moderate zoals gedefinieerd in Common Criteria methode [13]. De Handreiking conformiteitstoetsing [4] geeft deelnemers aan het Afsprakenstelsel eTD en conformiteitsbeoordelaars een richtsnoer voor het uitvoeren van de conformiteitstoets. Een risicoanalyse neemt daarbij een belangrijke plaats in.

Om deelnemers te ondersteunen bij het realiseren van een betrouwbare oplossing en conformiteitsbeoordelaars bij het uitvoeren van de beoordeling, bevat dit document functionele beveiligingsspecificaties voor authenticatiemiddelen op LoA4 en authenticatiemechanismen op LoA3 en LoA4.

Deze specificaties kunnen als bron dienen bij de voorbereiding op en de uitvoering van de conformiteitstoets. Het inventariseren en uiteindelijk vaststellen van de specifieke beveiligingsspecificaties voor een oplossing is echter een taak van de deelnemer en dit dient gebaseerd te zijn op een risicoanalyse. Het geheel van benodigde beveiligingsmaatregelen hangt daarmee af van de concreet gekozen oplossing en de uitkomsten van de risicoanalyse die daarop uitgevoerd is. De beveiligingsspecificaties in dit document zijn daarmee informatief van aard, omdat immers niet alle specificaties van toepassing zijn op iedere oplossing. Sommige specificaties zijn alleen van toepassing als de oplossing gebruik maakt van een bepaalde technologie (bijv. biometrie).

Benadrukt wordt dat dit document uitsluitend in gaat op functionele beveiligingsspecificaties aan authenticatiemiddelen en –mechanismen. Procedurele en organisatorische eisen met betrekking tot uitgifte en beheer zijn onderdeel van het Normenkader Betrouwbaarheidsniveaus en worden door middel van een audit getoetst.

Samen met de Handreiking conformiteitstoetsing geeft dit document inzicht in de wijze waarop de conformiteitstoetsing van authenticatiemiddelen en -mechanismen is ingeregeld. Dit is van belang voor de notificatie van het stelsel bij de EU ten behoeve van grensoverschrijdend gebruik.

Regelmatig moet geëvalueerd worden of het document nog actueel is. Ontwikkelingen, zowel op het gebied van oplossingen als dreigingen, kunnen ervoor zorgen dat aanpassingen nodig zijn.

1.2 Indeling van dit document

Hoofdstuk 2 geeft aan wat verstaan wordt onder authenticatiemiddel en authenticatiemechanisme.

In Hoofdstuk 3 wordt de aanpak beschreven om tot deze functionele beveiligingsspecificaties te komen en worden op generiek niveau de assets en dreigingen beschreven.

In Hoofdstuk 4 volgen de functionele beveiligingsspecificaties. Deze beveiligingsspecificaties dekken de dreigingen zoals geïdentificeerd in Hoofdstuk 3 af.

2 Authenticatiemiddel en authenticatiemechanisme

Voor het begrip authenticatiemechanisme wordt binnen de eIDAS verordening, de eIDAS uitvoeringsverordening en het Afsprakenstelsel elektronische Toegangsdiensten geen definitie gegeven. In dit document maken we gebruik van de volgende definitie[1]:
Een gedefinieerde opeenvolging van berichten tussen Gebruiker (Dienstafnemer) en Authenticatiedienst die aantoont dat de Gebruiker in het bezit is van en controle heeft over één of meer geldige authenticatiefactoren om zijn/haar identiteit vast te stellen en die aantoont aan de Gebruiker dat hij of zij communiceert met de beoogde Authenticatiedienst t.b.v. authenticatie bij een bepaalde Dienstverlener.

Volgens de IDAS Uitvoeringsverordening 1502/2015 [6] kunnen authenticatiefactoren gedefinieerd worden als:
„authenticatiefactor": een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de volgende categorieën valt:
a) „op bezit gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is;
b) „op kennis gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;
c) „inherente authenticatiefactor": een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;
De "inherente authenticatiefactor" wordt in de rest van dit document aangeduid als "authenticatiefactor biometrie".

Het authenticatiemiddel is volgens het Afsprakenstelsel eTD [1] "een set van attributen [i.e. authenticatiefactoren] (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden". Deze definitie sluit aan bij de definitie voor elektronisch identificatiemiddel uit de eIDAS Verordening [5]:"een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst".

Verder wordt conform het eIDAS guidance document [7] gebruik gemaakt van het uitgangspunt dat aangeeft dat verificatie van het authenticatiemiddel onderdeel uitmaakt van het authenticatiemechanisme bij het bepalen van de weerstand tegen aanvallen: "During assessing attack resistance, the whole authentication mechanism should be taken into account including the risks resulting from verification of the possession of the electronic identification means."

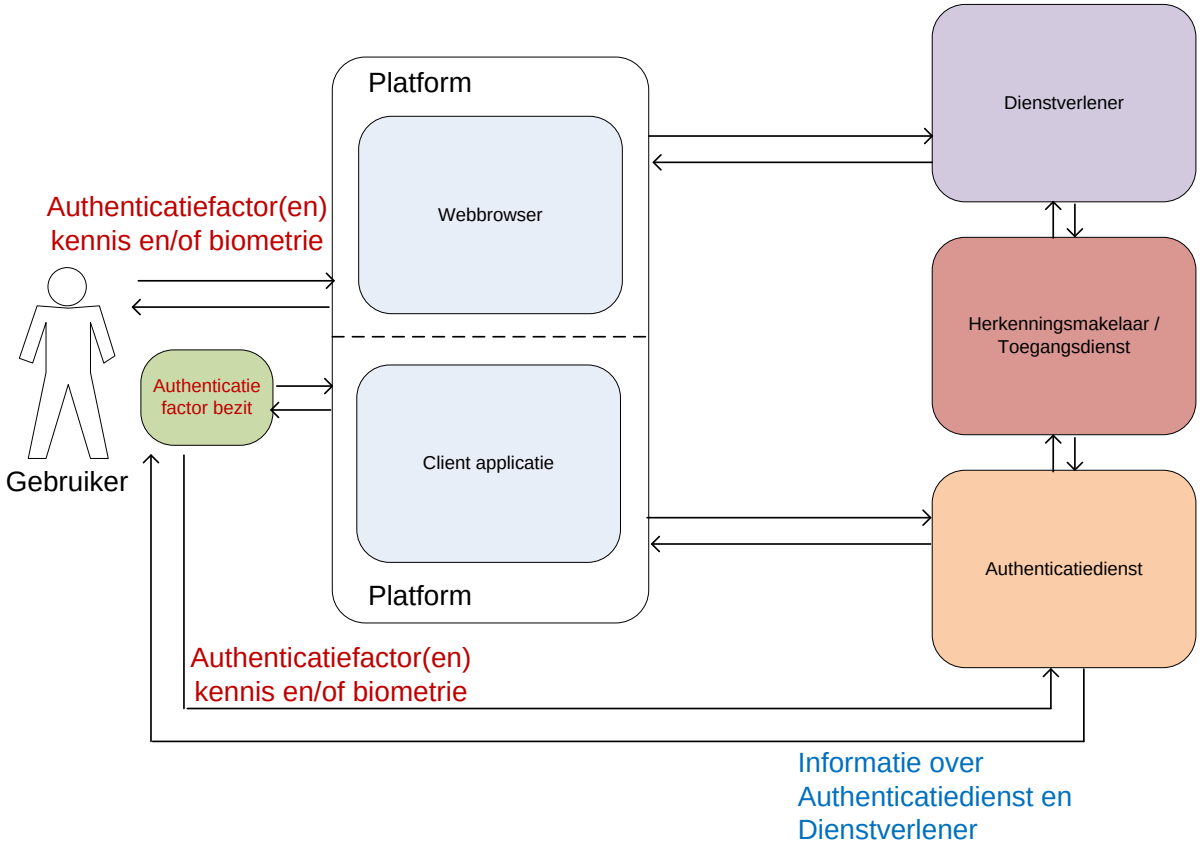
Daarnaast staat in het eIDAS guidance document [7] dat "Reasonable assumptions on the level of security of components used by, but not part of, the authentication scheme (e.g. the environment of the user, browser, smart phone, etc.) should be taken into account during the risk assessment." De Authenticatiedienst kan met de Gebruiker afspraken maken over voorwaarden waaraan de gebruikerscomponenten dienen te voldoen (zoals vereiste versie, installeren van updates en security patches, geen jailbreaking van mobiele telefoon) maar dit valt moeilijk of niet technisch af te dwingen. Daarom wordt de aanname gedaan dat deze gebruikerscomponenten onveilig kunnen zijn en dus niet op de beveiliging ervan vertrouwd kan worden. Het authenticatiemechanisme moet

1 Deze definitie is gebaseerd op de definitie voor authentication protocol uit NIST SP 800-63-1 [8]: "A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier." Maar gaat uit van authenticatiefactoren i.p.v. een token en stelt het aantonen van communicatie met de beoogde authenticatiedienst als voorwaarde.

zo ingericht worden dat ook bij compromittatie van de gebruikerscomponenten de oplossing voldoende veilig is voor het betrouwbaarheidsniveau waarvoor deze bedoeld is.

Figuur 1 illustreert dat de kennisfactoren bezit, kennis en biometrie, die samen het authenticatiemiddel kunnen vormen, worden uitgewisseld tussen de Gebruiker en de Authenticatiedienst en dat de Gebruiker betrouwbare informatie ontvangt over de Authenticatiedienst en over de Dienstverlener ten behoeve waarvan de authenticatie plaatsvindt. De gebruiker kan hierbij gebruik maken van een Client applicatie op zijn eigen platform die wel onderdeel is van het authenticatieschema maar los staat van de browser. De Client applicatie kan zich zelfs op een ander platform bevinden. De Client applicatie kan de communicatie met de gebruiker, de authenticatiefactor bezit en/of biometrische sensoren verzorgen tijdens de authenticatie en/of berichten ontvangen van de Authenticatiedienst.

De mogelijke communicatiekanalen zijn in zwart aangegeven, maar niet alle kanalen hoeven binnen een oplossing gebruikt te worden en ook de specifieke opeenvolging van berichten en de kanalen waarover die worden uitgewisseld, ligt niet vast, maar is afhankelijke van de oplossing.

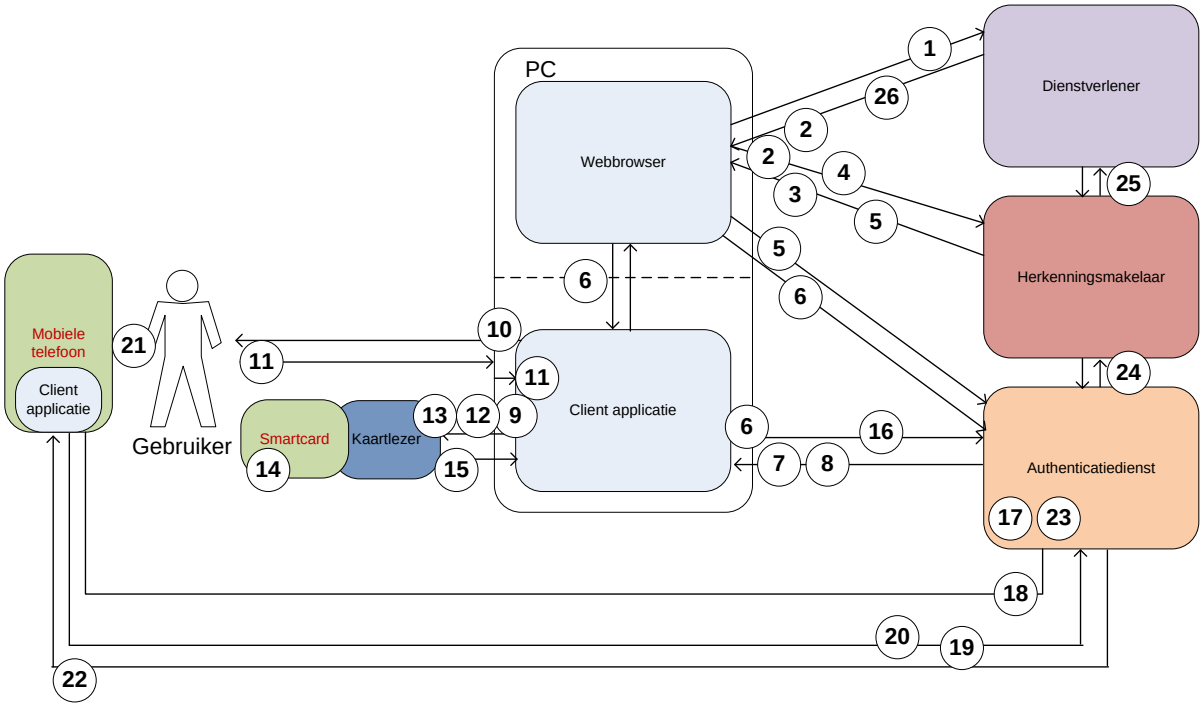


Figuur 1: Via een gedefinieerde opeenvolging van berichten (niet weergegeven in de figuur) en eventueel met gebruikmaking van een Client applicatie, applicatiefactor bezit of biometrische sensoren worden de kennisfactoren bezit, kennis, en/of biometrie uitgewisseld tussen de Gebruiker en de Authenticatiedienst en ontvangt de Gebruiker betrouwbare informatie over de Authenticatiedienst en de Dienstverlener ten behoeve waarvan de authenticatie plaatsvindt. De kanalen waarover communicatie plaats kan vinden zijn aangegeven door middel van pijlen, maar

niet alle kanalen hoeven gebruikt te worden. Ook de specifieke opeenvolging van berichten ligt niet vast, maar wordt bepaald door de specifieke oplossing.

Als hetzelfde platform gebruikt wordt om via een webbrowser met de Dienstverlener te communiceren en tevens als onderdeel van het authenticatiemiddel (bijv. authenticatiefactor bezit), zorgt dit voor een verhoogd risico waarover de Gebruiker volgens het Afsprakenstelsel elektronische Toegangsdiensten geïnformeerd moet worden.

Eén authenticatiefactor kan bestaan uit meerdere componenten. Zo kunnen in een authenticatiemechanisme bijvoorbeeld twee authenticatiefactoren bezit gebruikt worden. Dit is weergegeven in het voorbeeld in Figuur 2 waarbij gebruik gemaakt wordt van een smartcard en mobiele telefoon als authenticatiefactoren bezit. Ook zijn in Figuur 2 de berichten die worden uitgewisseld aangegeven, de volgorde waarin dat gebeurt en de kanalen waarover deze berichten worden uitgewisseld.



Figuur 2: Voorbeeld van authenticatie op basis van authenticatiefactor kennis (PIN) en authenticatiefactoren bezit (smartcard en mobiele telefoon)

1. De Gebruiker kiest via een webbrowser op zijn PC op de website van een Dienstverlener voor een actie die authenticatie vereist.
2. De Dienstverlener stuurt de Gebruiker door naar zijn Herkenningsmakelaar en geeft daarbij het minimaal vereiste betrouwbaarheidsniveau door.
3. De Herkenningsmakelaar biedt de Gebruiker de mogelijkheid zijn gewenste Authenticatiedienst te kiezen.
4. De Gebruiker kiest zijn Authenticatiedienst.
5. De Herkenningsmakelaar stuurt de Gebruiker door naar zijn Authenticatiedienst en geeft daarbij het minimaal vereiste betrouwbaarheidsniveau door en de Dienstverlener ten behoeve waarvan authenticatie plaats zal vinden.

6. De Authenticatiedienst zorgt voor het activeren van de Client applicatie op de PC van de gebruiker en het opzetten van een verbinding tussen Client applicatie en Authenticatiedienst.
7. De Authenticatiedienst toont de Gebruiker via de Client applicatie op zijn PC informatie over het inlogproces en de Dienstverlener ten behoeve waarvan de authenticatie plaats gaat vinden. Eventueel kan de Gebruiker kiezen uit verschillende inlogmethodes die minimaal het vereiste betrouwbaarheidsniveau hebben.
8. De Authenticatiedienst geeft de Client applicatie op de PC van de Gebruiker opdracht een sessie met de smartcard te starten en stuurt een challenge naar de Client applicatie.
9. De Client applicatie start een sessie met de smartcard via de aan de PC gekoppelde kaartlezer
10. De Client applicatie vraagt de Gebruiker zijn PIN in te voeren ter goedkeuring van deze stap in het authenticatieproces.
11. De Gebruiker voert zijn PIN in op het toetsenbord van zijn PC en deze wordt naar de Client applicatie op de PC gestuurd.
12. De Client applicatie stuurt de PIN via de kaartlezer naar de smartcard
13. De Client applicatie stuurt de van de Authenticatiedienst ontvangen challenge ter ondertekening naar de smartcard.
14. De smartcard ondertekent de challenge.
15. De ondertekende challenge met het bijbehorende certificaat wordt via de kaartlezer naar de Client applicatie gestuurd.
16. De Client applicatie stuurt de ondertekende challenge met het bijbehorende certificaat naar de Authenticatiedienst.
17. De Authenticatiedienst controleert de ondertekende challenge en het bijbehorende certificaat.
18. De Authenticatiedienst stuurt via een push message service (Google Cloud Messaging Service/ Apple Push Notification Service) een push bericht naar Client applicatie op de mobiele telefoon van de Gebruiker met het verzoek aan de Client applicatie om een beveiligde verbinding op te zetten met de Authenticatiedienst.
19. De Client applicatie op de mobiele telefoon zet een beveiligd kanaal op met de Authenticatiedienst.
20. De Authenticatiedienst stuurt informatie over de Authenticatiedienst en Dienstverlener ten behoeve waarvan authenticatie plaatsvindt naar de Client applicatie op de mobiele telefoon.
21. De Gebruiker bevestigt het authenticatieverzoek bij deze Authenticatiedienst ten behoeve van de genoemde Dienstverlener in de Client applicatie op zijn mobiele telefoon.
22. De Client applicatie op de mobiele telefoon stuurt de bevestiging over het beveiligde kanaal naar de Authenticatiedienst.
23. De Authenticatiedienst keurt op basis van deze bevestiging in combinatie met de eerder ontvangen en gecontroleerde ondertekende challenge en bijbehorend certificaat de authenticatie goed.
24. De Authenticatiedienst bevestigt authenticatie van de Gebruiker aan de Herkenningsmakelaar en geeft de identificerende gegevens van de Gebruiker (PI/PP) door.
25. De Herkenningsmakelaar bevestigt authenticatie van de Gebruiker aan de Dienstverlener en geeft de identificerende gegevens van de Gebruiker (PI/PP) door.
26. De Dienstverlener zet de communicatie met de Gebruiker voort.

3 Aanpak om tot functionele beveiligingsspecificaties te komen

3.1 Aanpak

Voor het opstellen van de functionele beveiligingsspecificaties is de volgende aanpak gehanteerd:

- Eerst zijn de assets geïdentificeerd van Authenticatiemiddel en Authenticatiemechanisme[2]. Voor het Authenticatiemiddel wordt daarbij onderscheid gemaakt tussen de authenticatiefactoren:
  - Bezit,
  - Kennis en
  - Biometrie.

  Voor het Authenticatiemechanisme worden de componenten die een rol spelen in het authenticatiemechanisme en de communicatiekanalen daartussen in beschouwing genomen. De volgende componenten en kanalen worden apart beschouwd:
  - Authenticatiemiddel (al behandeld)
  - Authenticatiedienst
  - Client applicatie
  - Communicatie tussen Authenticatiemiddel en Client applicatie
  - Communicatie tussen Authenticatiedienst en Client applicatie
  - Communicatie tussen Authenticatiedienst en Authenticatiemiddel
- Vervolgens zijn mogelijke dreigingen m.b.t. deze assets in kaart gebracht. Als input is hierbij gebruik gemaakt van het Normenkader betrouwbaarheidsniveaus en de dreigingen zoals gedefinieerd in ISO/IEC 29115.
- Tot slot zijn in Hoofdstuk 4 de functionele beveiligingsspecificaties opgesteld die de in dit hoofdstuk geïdentificeerde dreigingen tegen gaan.

3.2 Identificatie van assets en dreigingen

Voor het Authenticatiemiddel onderkennen we de volgende assets en dreigingen.

Asset	**Dreiging**	**Dreiging nummer**
Authenticatiefactor bezit		
Authenticiteit van authenticatiefactor bezit	Kopiëren/namaken/simuleren (credential duplication)	D_1
	Aanpassen van middel, bijvoorbeeld om biometrische controle te omzeilen, retry counter uit te zetten, OTP af te geven of sleutelgebruik toe te staan zonder biometrische of kennis factor	D_2
Authenticatiefactor kennis		
Vertrouwelijkheid van authenticatiefactor kennis	Achterhalen/afluisteren/raden van kennis factor	D_3
Authenticiteit van authenticatiefactor kennis	Aanpassen van opgeslagen kennis factor	D_4
Authenticiteit van kennis factor verificatie	Aanpassen van kennis factor verificatie algoritme	D_5
Authenticatiefactor biometrie		

2 Conform het eIDAS guidance document [7] en beschreven in Hoofdstuk 2 maakt het Authenticatiemiddel onderdeel uit van het Authenticatiemechanisme. Vanwege het onderscheid dat in de eIDAS verordening en het Afsprakenstelsel eTD gemaakt wordt m.b.t. Authenticatiemiddel en –mechanisme zullen assets, dreigingen en functionele beveiligingsspecificaties toch apart behandeld worden.

Authenticiteit aangeboden biometrisch kenmerk	Look-a-like/imposter fraude/spoofing	D_6
Authenticiteit van opgeslagen biometrisch kenmerk	Aanpassen van opgeslagen biometrische factor	D_7
Authenticiteit van biometrie factor verificatie	Aanpassen van verificatie algoritme	D_8

Voor het Authenticatiemechanisme onderkennen we de volgende assets en dreigingen.

Asset	**Dreiging**	**Dreiging nummer**
Authenticatiemiddel		
Zie vorige tabel		
Authenticatiedienst		
Authenticiteit van opgeslagen gegevens	Hacken van Authenticatiedienst	D_9
Vertrouwelijkheid van opgeslagen gegevens	Fysieke toegang tot systemen van Authenticatiedienst	D_10
Authenticiteit van verificatie van authenticatiemiddel en berichten		
Client applicatie		
Authenticiteit van aan Gebruiker getoonde berichten	Malware op device/ hacken van Client applicatie	D_11
Authenticiteit van door gebruiker ingevoerde informatie		
Vertrouwelijkheid van door gebruiker ingevoerde informatie		
Authenticatiemiddel – Client applicatie communicatie		
Authenticiteit van uitgewisselde informatie	Man-in-the-middle attack	D_12
	Session hijacking	D_13
	Replay attack	D_14
Vertrouwelijkheid van uitgewisselde informatie	Man-in-the-middle attack	D_12
	Session hijacking	D_13
Authenticatiedienst – Client applicatie communicatie		
Authenticiteit van uitgewisselde informatie	Man-in-the-middle attack	D_15
	Session hijacking	D_16
	Replay attack	D_17
Vertrouwelijkheid van uitgewisselde informatie	Man-in-the-middle attack	D_15
	Session hijacking	D_16
Authenticatiedienst – Authenticatiemiddel communicatie		
Authenticiteit van uitgewisselde informatie	Man-in-the-middle attack	D_18
	Session hijacking	D_19
	Replay attack	D_20
Vertrouwelijkheid van	Man-in-the-middle attack	D_18

uitgewisselde informatie	Session hijacking	D_19

4 Functionele beveiligingsspecificaties

Om de dreigingen zoals geïdentificeerd in Hoofdstuk 3 tegen te gaan worden in dit Hoofdstuk functionele beveiligingsspecificaties gedefinieerd voor het authenticatiemiddel en het authenticatiemechanisme. Merk op dat niet iedere specificatie van toepassing zal zijn op iedere oplossing aangezien oplossingen van elkaar verschillen en sommige specificaties specifiek zijn voor een bepaalde component of technologie.

4.1 Functionele beveiligingsspecificaties voor het authenticatiemiddel (niveau Hoog/LoA4)

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
1.	Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren.	eIDAS implementing regulation 2015/1502, section 2.2.1	D_1 t/m D_8 + D_11
2.	Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.	eIDAS implementing regulation 2015/1502, section 2.2.1	D_1 t/m D_8
3.	Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel (betrouwbaarheidsniveau Hoog).	eIDAS implementing regulation 2015/1502, section 2.2.1	D_1 + D_2
4.	Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.	eIDAS implementing regulation 2015/1502, section 2.2.1	D_2 t/m D_8
5.	Het authenticatiemiddel geeft slechts een response na een expliciete handeling van de gebruiker. De handeling van de gebruiker vindt buiten de werkingssfeer van de applicatie (o.a. browser) plaats. 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 het middel en maakt zo deel uit van de response. In deze specificatie 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.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.2.1	D_12 t/m D_14 + D_18 t/m D_20

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
	Als 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: 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.		
6.	Het authenticatiemiddel notificeert de gebruiker (onafhankelijk van de browser die hij gebruikt) van zijn inlogpoging bij een specifieke dienst of dienstverlener. De notificatie is gekoppeld aan het gebruik van diensten op het niveau van het middel.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_11
7.	Het authenticatiemiddel bevat een betrouwbaar (trusted) kanaal 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 bevat de mogelijkheid om de gebruiker elementen in het authenticatieverzoek te laten bevestigen. Het gaat er om dat de gebruiker via het 'trusted' kanaal hoogst betrouwbaar informatie over zijn inlog bij de dienstverlener of dienst kan worden gegeven en om hoogst betrouwbare bevestiging kan worden gevraagd van een specifiek transactiegegeven. Deze betrouwbaarheid blijft 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.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_18 t/m D_20

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
8.	Bij gebruik van het authenticatiemiddel wordt de gebruiker expliciet duidelijk gemaakt 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.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_11
9.	Het authenticatiemiddel maakt geheime opslag van sleutels, kennis factoren en/of biometrische kenmerken mogelijk en voorkomt aanpassingen aan deze opgeslagen waarden en aan algoritmes waarvan het authenticatiemiddel gebruik maakt. Mogelijke invulling: Voor Secure Element (SE) gebaseerde authenticatiemiddelen kan een Common Criteria certificering plaatsvinden volgens een geschikt Protection Profile en/of Security Target op minimaal EAL 4 aangevuld met AVA_VAN.5 and ALC_DVS.2 of een EMVCo certificering of GlobalPlatform certificering.		D_1 t/m D_8
10.	Op LoA4 dient bij gebruik van een authenticatiefactor bezit voor tenminste een deel van de authenticaties gebruik gemaakt te worden van een SE gebaseerd authenticatiemiddel. Dit wil echter niet zeggen dat voor alle authenticaties de SE gebaseerde authenticatiefactor bezit gebruikt hoeft te worden.		D_1 + D_2
11.	Na een aantal onsuccesvolle inlogpogingen blokkeert of vertraagt het authenticatiemiddel de mogelijkheid om in te loggen. Mogelijke invulling: Na 3 onsuccesvolle inlogpogingen kan de mogelijkheid om in te loggen geblokkeerd worden. Na 3 onsuccesvolle inlogpogingen kan de mogelijkheid om in te loggen met 2 seconden vertraagd worden. Bij iedere volgende onsuccesvolle inlogpoging kan een nieuwe mogelijkheid om in te loggen met nog eens 2 seconden extra vertraagd worden.		D_2 + D_4 + D_6
12.	De kennis factor is voldoende moeilijk te raden of achterhalen.		D_3

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
	Mogelijke invulling: Van een PIN kan vereist worden dat deze uit minimaal 4 cijfers bestaat en dat de verschillen tussen opvolgende cijfers niet gelijk. Van een wachtwoord kan vereist worden dat dit ten minste 8 letters, ten minste 1 kleine letter [a-z], ten minste 1 hoofdletter [A-Z], ten minste 1 cijfer [0-9] en ten minste 1 bijzonder teken [- _ ! $ % & ' . = / \ : < > | ? @ [ ] ^ ` { } ~] bevat en dat het niet de gebruikersnaam bevat of gelijk is aan een van de 5 eerder gebruikte wachtwoorden. Van een wachtwoord kan vereist worden dat het gebruik maakt van wachtwoordzinnen die bestaan uit zowel hoofdletters als kleine letters en eventueel ook andere tekens en minimaal een zinlengte van 20 tekens.		
13.	De biometrische verificatie vindt met voldoende betrouwbaarheid plaats. De False Acceptance Rate (FAR) en kwaliteit van het opgeslagen template zijn van belang voor de betrouwbaarheid. Daarnaast vindt liveness detectie plaats. Mogelijke invulling: De FAR kan bepaald worden zoals gedefinieerd in ISO/IEC 19795-5 en ligt bij voorkeur beneden 0.3%. De quality indicator van een opgeslagen template kan gedefinieerd worden zoals in ISO/IEC 29794-1 en berekend volgens een geschikt algoritme en heeft bij voorkeur een waarde groter dan 75 (op een schaal van 100). Het biometrisch verificatie mechanisme kan gecertificeerd worden volgens het Biometric Verification Mechanisms Protection Profile BVMPP. Bij biometrische verificatie kan presentation attack detection uitgevoerd worden zoals beschreven in ISO/IEC 30107-1. Dit kan bestaan uit detectie d.m.v. data capture (o.a. artefact detection, liveness detectie, non-conformance detectie) en detectie d.m.v. system-level		D_6

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
	monitoring (bijv. failed attempt detection counter). Zodra ISO/IEC 30107-3 beschikbaar komt met "principles and methods for performance assesment of presentation attack detection algorithms or mechanisms" kan hiervan gebruik gemaakt worden om de betrouwbaarheid van de presentation attack detection te bepalen en ligt deze bij voorkeur boven een nader aan te geven waarde. In geval gebruik gemaakt wordt van vingerafdrukherkenning kan het biometric spoof detection system gecertificeerd zijn volgens het Fingerprint Spoof Detection Protection Profile FSDPP.		

4.2 Functionele beveiligingsspecificaties voor het Authenticatiemechanisme (niveaus Substantieel/LoA3 en Hoog/LoA4)

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
Authenticatiemechanisme algemeen			
14.	De gebruiker wordt in staat gesteld om de website/app van de authenticatiedienst en alle andere partijen in het netwerk te authentiseren. Dit kan bijvoorbeeld op basis van een TLS/SSL certificaat of een elektronische handtekening op basis van een vertrouwd certificaat.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_12 t/m D_14 + D_15 t/m D_17 + D_18 t/m D_20
15.	Bij gebruik van het authenticatiemiddel wordt de gebruiker expliciet duidelijk gemaakt 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.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_11

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
16.	Alleen LoA4: de authenticatiedienst 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.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_11 + D_15 t/m D_17 + D_18 t/m D_20
17.	Alleen LoA4: 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. Mogelijke invulling: Dit tijdsbestek kan beperkt worden tot minder dan 5 seconden.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_11 + D_15 t/m D_17 + D_18 t/m D_20
18.	Informatie (berichten) uitgewisseld over verschillende kanalen voor dezelfde authenticatie sessie wordt op een betrouwbare manier gelinkt. Mogelijke invulling: Aan de berichten wordt een niet-voorspelbare sessie identifier toegevoegd.		D_12 t/m D_20
Authenticatiemiddel			
Zie voorgaande tabel			
Authenticatiedienst			
19.	De authenticatiedienst toont in het aanlogscherm bij welke dienstverlener de gebruiker gaat aanloggen.	Afsprakenstelsel eTD, Normenkader betrouwbaarheidsniveaus, Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.3.1	D_12 t/m D_20
20.	De Authenticatiedienst implementeert beveiligingsmaatregelen tegen hacking. Mogelijke invulling:		D_9

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
	De inrichting voldoet aan en is gecertificeerd volgens ISO 27001.		
21.	De systemen van de Authenticatiedienst bevinden zich in een beveiligde ruimte en zijn alleen fysiek toegankelijk voor geautoriseerde personen. De aanwezigheid van personen in de ruimte wordt geregistreerd. Mogelijk invulling: De inrichting voldoet aan en is gecertificeerd volgens ISO 27001.		D_10
22.	Logische toegang tot de systemen van de Authenticatiedienst is voorbehouden aan geautoriseerde personen. Hun acties worden op individuele basis gelogd. Mogelijke invulling: De inrichting voldoet aan en is gecertificeerd volgens ISO 27001.		D_9 + D_10
23.	De Authenticatiedienst controleert dat het Authenticatiemiddel niet ingetrokken is. Mogelijke invulling: De Authenticatiedienst raadpleegt de Middelenuitgever over de status of zijn eigen register als de Authenticatiedienst tevens Middelenuitgever is.		D_1 t/m D_8
24.	Na een aantal onsuccesvolle inlogpogingen blokkeert of vertraagt de Authenticatiedienst de mogelijkheid om in te loggen. Mogelijke invulling: Na 3 onsuccesvolle inlogpogingen kan de mogelijkheid om in te loggen geblokkeerd worden. Na 3 onsuccesvolle inlogpogingen kan de mogelijkheid om in te loggen met 2 seconden vertraagd worden. Bij iedere volgende onsuccesvolle inlogpoging kan een nieuwe mogelijkheid om in te loggen met nog eens 2 seconden extra vertraagd worden.		D_1 t/m D_8

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
25.	De Authenticatiedienst genereert per sessie een unieke challenge en accepteer voor deze sessie uitsluitend de response op deze challenge. Mogelijke invulling: De Authenticatiedienst houdt per sessie de verzonden challenge bij. Een getekende challenge die niet overeenkomt met de challenge verzonden in dezelfde sessie, wordt niet geaccepteerd.		D_15 t/m D_20
Client applicatie			
26.	Op basis van de gebruikersinterface is de gebruiker gemakkelijk in staat vast te stellen of gebruik gemaakt wordt van de Client applicatie of van de browser. Mogelijke invulling: De Client applicatie gebruikersinterface verschilt duidelijk van die van de browser.		D_11
27.	De Client applicatie accepteert alleen berichten van een geauthentiseerde Authenticatiedienst waarvan de gegevens in de Client applicatie zijn vastgelegd en alleen via een betrouwbaar kanaal. Mogelijke invulling: Voor authenticatie van de Authenticatiedienst en het beveiligd kanaal kan gebruik gemaakt worden van TLS waarbij voldaan wordt aan de specificaties beschreven voor secure connection in het Afsprakenstelsel eTD of van gelijkwaardige beveiliging. De Client applicatie kan de certificaten die geaccepteerd worden beperken tot uitsluitend de certificaten van de eigen Authenticatiedienst.		D_15 t/m D_17
Communicatie tussen Authenticatiemiddel en Client applicatie			
28.	Elektronische communicatie tussen het Authenticatiemiddel en de Client applicatie is beveiligd tegen ongeautoriseerd wijzigen. Mogelijke invulling: De elektronische communicatie kan beveiligd zijn tegen ongeautoriseerd wijzigen door een geavanceerde elektronische handtekening of op een gelijkwaardige manier.		D_12 t/m D_14

Nr.	Specificatie	Gebaseerd op	Dreiging(en) die tegen gegaan wordt/worden
Communicatie tussen Authenticatiedienst en Client applicatie			
29.	Informatie uitwisseling tussen Client applicatie en Authenticatiedienst vindt plaats via een beveiligd kanaal dat zorgt voor confidentialiteit, authenticiteit en replay beveiliging. Mogelijke invulling: Het beveiligd kanaal kan gebruik maken van TLS waarbij voldaan wordt aan de specificaties beschreven voor secure connection in het Afsprakenstelsel eTD of van gelijkwaardige beveiliging.		D_15 t/m D_17
Communicatie tussen Authenticatiedienst en Authenticatiemiddel			
30.	Informatie uitwisseling tussen Authenticatiedienst en Authenticatiemiddel vindt plaats via een beveiligd kanaal dat zorgt voor confidentialiteit, authenticiteit en replay beveiliging. Mogelijke invulling: Het beveiligd kanaal kan gebruik maken van TLS waarbij voldaan wordt aan de specificaties beschreven voor secure connection in het Afsprakenstelsel eTD of van gelijkwaardige beveiliging.		D_18 t/m D_20
31.	Indien communicatie tussen Authenticatiedienst en Authenticatiemiddel plaatsvindt over een minder beveiligd kanaal bevat deze communicatie geen transactie informatie en is de communicatie beschermd tegen replay en guessing. De eigenlijke informatie uitwisseling vindt plaats over een beveiligd kanaal.		D_18 t/m D_20

5 Referenties

1. Afsprakenstelsel Elektronische Toegangsdiensten, versie 1.10c van 30 september 2016, https://afsprakenstelsel.etoegang.nl/display/as/Startpagina
2. Normenkader betrouwbaarheidsniveaus, versie 1.10c van 30 september 2016, https://afsprakenstelsel.etoegang.nl/display/as/Normenkader+betrouwbaarheidsniveaus
3. Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen
4. Handreiking Conformiteitstoetsing Authenticatiemiddel en –mechanisme LoA3 en LoA4, versie 1.0 van 13 februari 2017.
5. 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/EGISO/IEC 29115
6. 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 overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt
7. Guidance for the application of the levels of assurance which support the eIDAS Regulation, https://www.viestintavirasto.fi/attachments/suositukset/LOA_Guidance.pdf.
8. NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 2011.
9. ISO/IEC 29115 Information technology – Security techniques – Entity authentication assurance framework, first edition, 2013-04-01
10. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1, Revision 4, CCMB-2012-09-0001, https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
11. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-0002, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
12. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB–2012–09–003, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf
13. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-0004, https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf