VERDONCK KLOOSTER & ASSOCIATES

FS-20120612.07A

DEFINITIEF

Startnotitie uitbreiding "Handreiking betrouwbaarheidsniveaus"

project 002303
versie 1.0
datum 5 juni 2012

Inhoudsopgave

Management samenvatting

Overheidsdienstverlening geschiedt steeds vaker langs digitale weg. Elektronische dienstverlening wordt daarbij steeds geavanceerder, niet alleen meer diensten worden elektronisch, maar ook hoogwaardiger diensten met een groter afbreukrisico. Steeds vaker gaat het daarbij om het volledige traject van een aanvraag tot aan het afgeven van een beschikking en informatie over de uitvoering van die beschikking.

Om dienstverleners te helpen bepalen welk niveau van betrouwbaarheid passend is bij de dienst die zij aanbieden is de “Handreiking betrouwbaarheidsniveaus” opgesteld. Hierin wordt een vereenvoudigde risico-analyse aangereikt waarmee dienstverleners onder hun eigen verantwoordelijkheid hun diensten kunnen inschalen.

De Handreiking betrouwbaarheidsniveaus voorziet duidelijk in een behoefte, een tweede druk van de publicatie is in gang gezet. Het College Standaardisatie heeft daarnaast reeds aangegeven dat een uitbreiding van de Handreiking wenselijk is. Deze startnotitie bepaalt daarvoor de scope en de timing. Hiervoor is een proces gevolgd in opdracht van het Forum Standaardisatie waarbij de expertgroep die de eerste handreiking begeleidde, opnieuw is betrokken.

De startnotitie gaat in op de onderwerpen die dit jaar nog opgepakt kunnen worden in een uitbreiding en biedt een ‘voorraadlijst’ voor onderwerpen die in een iets verdere toekomst aan bod kunnen komen. Daarnaast gaat de notitie kort in op relevante onderwerpen die uit het proces naar voren kwamen, maar die niet thuis horen in de uitbreiding. Nadenken over de uitbreiding heeft bevestigd dat de handreiking gericht blijft op dienstverleners in het *vaststellen van het betrouwbaarheidsniveau dat nodig is om één individuele dienst elektronisch aan te bieden*.

Ook is in dit proces een aantal overige uitgangspunten geformuleerd dat bij de doorontwikkeling van de handreiking gehanteerd zal worden:

1. De status en insteek van de handreiking blijven ongewijzigd.
2. De ontwikkeling/ uitbreiding van de handleiding is vraaggericht.
3. De handreiking moet een systematiek aanreiken en het onderwerp verhelderen.
4. De handreiking verbreedt, maar wordt niet complexer.
5. Het gaat in de Handreiking om het standaardiseren van best practices, niet om research.
6. Aandacht voor Europese ontwikkelingen.

Van een groslijst zijn de gesuggereerde onderwerpen beschouwd op de bovengenoemde afbakening, uitgangspunten en opportuniteit. De voorgestelde onderwerpen voor de eerstvolgende uitbreiding zijn:

- Het machine to machine (M2M) kanaal.
- Wilsbeschikking via de digitale handtekening.
- Machtiging.
- Retourstroom.

Behoeften die uit het proces naar voren zijn gekomen maar die niet passen binnen de inhoudelijke scope van de uitbreiding zijn:

- Duiden van het aanbod van authenticatiemiddelen.
- Onderzoek naar, en community rondom, het gebruik van de handreiking.
- Gebruiksaspecten.
- SSO en overige ketenaspecten.

1 Inleiding

Dit hoofdstuk bevat de verantwoording voor de startnotitie. Het gaat achtereenvolgens in op de aanleiding voor de startnotitie “uitbreiding handreiking betrouwbaarheidsniveaus”, de opdracht, de werkwijze en de leeswijzer.

1.1 Aanleiding

Overheidsdienstverlening geschiedt steeds vaker langs digitale weg. Elektronische dienstverlening wordt daarbij steeds geavanceerder, niet alleen meer diensten worden elektronisch, maar ook hoogwaardiger diensten met een groter afbreukrisico. Steeds vaker gaat het daarbij om het volledige traject van een aanvraag tot aan het afgeven van een beschikking en informatie over de uitvoering van die beschikking.

Waar voorheen voor eenvoudige informatiediensten een beperkt betrouwbaarheidsniveau volstond, vragen steeds geavanceerder elektronische diensten, waarvan de communicatie van persoonlijke (en daarmee privacygevoelige) gegevens een onderdeel is, er om dat ook identificatie, authenticatie en autorisatie op een hoger niveau komen te liggen om de bij de elektronische dienst passende betrouwbaarheid te borgen. Diensten waarbij hier aan gedacht kan worden zijn bijvoorbeeld het oprichten van een bedrijf, het inzenden van een voor-ingevuld belastingformulier voor je grootmoeder, of de gegevensuitwisseling tussen de Rotterdamse haven en de douane.

Op deze wijze komen diensten die kunnen volstaan met een bescheiden betrouwbaarheidsniveau te staan naast diensten waarvoor een hoger betrouwbaarheidsniveau is gewenst. Welk niveau van betrouwbaarheid een dienstverlener vraagt voor zijn diensten, is aan de betreffende organisatie zelf. Om organisaties te helpen hierin een afweging te maken, publiceerde het Forum Standaardisatie de handreiking voor overheidsorganisaties: “Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten”. Deze publicatie bedient architecten, informatiebeveiligers, juristen en bestuurders die met deze materie te maken hebben of krijgen.

De publicatie blijkt in een behoefte te voorzien, er is veel belangstelling voor. In de huidige versie van de handreiking is, omwille van de eenvoud en snelheid van ontwikkelen, een aantal aspecten buiten scope gelaten:

- Machine-to-machine communicatie - De huidige handreiking is alleen gericht op diensten die via het World Wide Web worden aangeboden;
- Retourstromen - De retourstromen die ontstaan vanuit een dienstverlener richting burger of bedrijf. Hiervoor kunnen specifieke betrouwbaarheidseisen aan de orde zijn.
- Machtigingen - Situaties waarin iemand een dienst namens een andere persoon afneemt.

Bovendien is de huidige handreiking uitsluitend gericht op de 'vraagzijde': het bepalen van een geschikt betrouwbaarheidsniveau, dat een specifieke dienst vergt. De 'aanbodzijde', het bepalen van de criteria waar een authenticatiemiddel aan moet voldoen voor een bepaald betrouwbaarheidsniveau, is wel als onderwerp geïdentificeerd in de huidige handreiking, maar wordt bewust niet behandeld. Voor het aanbod is aangesloten bij de indeling in vier betrouwbaarheidsniveaus zoals die zijn gedefinieerd door het STORK programma. Een aanvullende publicatie die de aanbodzijde verder uitwerkt, is in de eerste versie van de handreiking benoemd als mogelijk vervolgwerk.

1.2 Opdracht

Vanwege de gekozen scopebeperkingen in de eerste versie van de handreiking heeft het College Standaardisatie te kennen gegeven graag een uitbreiding op de handreiking te zien voor diverse aspecten die relevant zijn voor het vaststellen van het niveau van identificatie, authenticatie en autorisatie voor betrouwbare elektronische overheidsdienstverlening. Het Forum Standaardisatie, verantwoordelijk voor het beheer en de doorontwikkeling van de publicatie, is daartoe een proces gestart en heeft opdracht gegeven aan René van den Assem (VKA) en Nathan Ducastel (HEC) om een startnotitie op te stellen.

Deze startnotitie dient duidelijkheid te verschaffen over de mogelijke onderwerpen waarmee de handreiking kan worden uitgebreid. Daarbij dient er per onderwerp duidelijk te worden gemaakt in hoeverre er behoefte aan is, wat de afhankelijkheden zijn van externe ontwikkelingen en wanneer het onderwerp naar verwachting rijp is voor opname in de handreiking. Het is overigens zo dat niet slechts één uitbreiding wordt voorzien. Het is goed mogelijk dat andere uitbreidingen volgen op het moment dat dit opportuun is, wanneer de gebruikers van de handleiding hier klaar voor zijn of/en wanneer ontwikkelingen de handleiding in betekenende mate beïnvloeden.

1.3 Werkwijze

De startnotitie is tot stand gekomen in zeer korte tijd in april en mei 2012. Hierbij zijn de volgende stappen doorlopen:

- Opstellen van een groslijst van onderwerpen waarmee de handreiking zou kunnen worden uitgebreid middels bureaustudie. Het verzamelen van kennis over relevante nationale en internationale ontwikkelingen rondom die onderwerpen.
- Opstellen van een uitbreidingsvoorstel op hoofdlijnen (powerpoint formaat).
- Bespreking van dit uitbreidingsvoorstel in een inhoudelijke werkgroep op 9 mei 2012.
- Verwerken van de reacties en het bepalen van de definitieve koers.
- Het uitwerken van deze koers in een uitgewerkte concept Startnotitie.
- Bespreking van deze startnotitie in een tweede bijeenkomst van de inhoudelijke werkgroep op 29 mei 2012.
- Verwerken van commentaren in een tweede concept Startnotitie.
- Voorleggen tweede concept in schriftelijke ronde aan de inhoudelijke werkgroep.
- Verwerken commentaren en opstellen definitieve Startnotitie voor het Forum Standaardisatie ten behoeve van de vergadering van 12 juni 2012.

Gedurende de bijeenkomst van 9 mei is gebleken dat de aanwezigen vrijwel allen de wens hadden om niet alleen de inhoudelijke onderwerpen te plannen waarmee de handreiking zou kunnen worden uitgebreid, maar om ook de activiteiten te beschouwen die rondom de handreiking moeten worden ontplooid. Denk daarbij bijvoorbeeld aan het organiseren van een platform dat gebruik van de handreiking bevordert en waar ervaringen worden uitgewisseld. Dit betrof zelfs het merendeel van de reacties.

Hoewel bovenstaande zaken van groot belang zijn, vallen ze buiten de huidige opdracht. In overleg met opdrachtgever is besloten het bereik van de startnotitie niet aan te passen. Deze startnotitie behandelt deze buiten het bereik liggende suggesties dan ook niet maar beperkt zich tot de inhoudelijke uitbreiding van de handreiking. De overige reacties zijn door stellers wel gemeld bij hun opdrachtgever, het bureau Forum Standaardisatie, ter verdere afhandeling en worden in de oplegger voor dit stuk aan het Forum Standaardisatie meegenomen.

1.4 Leeswijzer

De startnotitie bestaat naast het eerste inleidende hoofdstuk uit twee delen. Hoofdstuk twee beschrijft de inrichting van de handreiking waarbij het onderwerp van studie wordt toegelicht. Hierbij is een aanscherping aan de orde ten opzichte van de eerdere handreiking. Vervolgens wordt ingegaan op de uitgangspunten en de uitkomsten van het proces: wat kan in een volgende uitbreiding van de handreiking aan de orde komen en wat maakt daar geen onderdeel van uit. Tot slot is in hoofdstuk twee een schrijfwijzer opgenomen voor de auteur(s) van de uitbreiding van de handreiking.

Hoofdstuk drie gaat in op de onderbouwing van de keuze van de onderwerpen die in de eerstvolgende uitbreiding kunnen worden opgenomen. Werkend van breed naar smal wordt eerst een indruk gegeven van de onderwerpen die spelen rondom betrouwbaarheid en die in de werkgroep aan de orde zijn geweest. Vervolgens wordt gekomen tot een groslijst van onderwerpen die in de toekomst in de handreiking kunnen worden opgenomen omdat ze direct raken aan het vaststellen van de betrouwbaarheidsniveaus voor een dienst. Hieruit zijn de onderwerpen die voor de eerstvolgende handreiking opportuun zijn, omdat deze voldoende zijn uitgekristalliseerd, afgeleid.

2 Inrichting van de handreiking

Dit hoofdstuk geeft inzicht in de keuzes die worden gemaakt rond de uitbreiding van de handreiking betrouwbaarheidsniveaus. Deze overlappen met de inrichting van de bestaande handreiking en zijn aangevuld met nieuwe inzichten die nodig zijn om een gedegen afweging te maken wat wel en wat niet thuis hoort in de uitbreiding.

2.1 Onderwerp van studie

De bestaande handreiking is geschreven voor dienstverleners die een lichte risicoanalyse wensen uit te voeren om daarmee zicht te krijgen op het betrouwbaarheidsniveau dat nodig is voor het aanbieden van diensten langs elektronische weg.

Voor de afbakening van de uitbreiding van de handreiking is het wenselijk gebleken dit doel verder aan te scherpen. De handreiking ondersteunt dienstverleners in het *vaststellen van het betrouwbaarheidsniveau dat nodig is om één individuele dienst elektronisch aan te bieden*.

Dit betekent dat vraagstukken die zijn gerelateerd aan een stapeling van diensten, dan wel vraagstukken op organisatieniveau buiten beschouwing worden gelaten. Dit is nodig om de complexiteit te reduceren, de scope overzichtelijk te houden en daarmee de aansluiting met de doelgroep te behouden. Hiermee wordt expliciet de keuze gemaakt om interessante onderwerpen zoals dienstenaggregatie, welke toegang je krijgt in een SSO model wanneer achterliggende diensten van verschillend betrouwbaarheidsniveau uitgaan, trust frameworks, etc. in de handreiking buiten beschouwing te laten. Daarmee is niet gezegd dat hieraan geen behoefte bestaat; wel dat de handreiking niet het juiste platform is om deze onderwerpen te behandelen.

Dienstverleners blijven zelf verantwoordelijk voor het betrouwbaarheidsniveau waarmee zij een dienst elektronisch aanbieden. De handreiking is enkel een middel om daarin te ondersteunen. Het is denkbaar dat dienstverleners afwijken van de uitkomst van de inschatting van het betrouwbaarheidsniveau zoals uit de lichte risico-analyse blijkt. Daarbij onderkennen we tenminste twee smaken:

1) De uitkomst van de lichte risico-analyse komt niet overeen met de beelden van de betreffende organisatie inzake hun dienst, waarna een zware risico-analyse wordt uitgevoerd;

2) De dienstverlener vindt het betrouwbaarheidsniveau dat volgt uit de lichte risico-analyse onwenselijk (bijvoorbeeld om bedrijfsvoeringredenen) en is in staat om met mitigerende maatregelen in het dienstverleningsproces het betrouwbaarheidsniveau te corrigeren. Dit kan bijvoorbeeld optreden wanneer een dienstverlener 40 diensten aanbiedt op niveau 2 en 1 op niveau 3. De dienstverlener kan er dan voor kiezen voor alle diensten niveau 2 te vragen, mits sprake is van customer intimacy of wanneer andere mitigerende maatregelen voor handen zijn om de betrouwbaarheid van de identificatie en authenticatie te borgen.

2.2 Uitgangspunten

In deze paragraaf worden de uitgangspunten opgesomd die de doorontwikkeling van de Handreiking richting geven. Deze uitgangspunten zijn mede geformuleerd naar aanleiding van de bijeenkomsten met de inhoudelijke werkgroep.

De volgende uitgangspunten zijn geformuleerd:

7. De status en insteek van de handreiking blijven ongewijzigd.
8. De ontwikkeling/ uitbreiding van de handleiding is vraaggericht.
9. De handreiking moet een systematiek aanreiken en het onderwerp verhelderen.
10. De handreiking verbreedt, maar wordt niet complexer.
11. Het gaat in de Handreiking om het standaardiseren van best practices, niet om research.
12. Aandacht voor Europese ontwikkelingen.

Hieronder worden deze uitgangspunten kort toegelicht.

2.2.1 Status en insteek van de Handreiking ongewijzigd

Overheidsorganisaties zijn gehouden de risico's die zij ervaren op het gebied van informatiebeveiliging en privacy adequaat te beheersen. Hiertoe analyseren zij de risico's en nemen maatregelen ter beheersing van die risico's. Eén van de gebieden waarop overheidsorganisaties maatregelen moeten nemen, is het onderwerp van de Handreiking, grofweg aan te duiden als de identificatie, authenticatie en autorisatie van burgers en bedrijven. Overheidsorganisaties moeten keuzes maken of en hoe de aard van de dienst in balans is met de betrouwbaarheid van de middelen en processen voor authenticatie en autorisatie die hun klanten kunnen gebruiken.

Het bovenstaande is intrinsiek onderdeel van de eigen verantwoordelijkheid van een overheidsorganisatie. De Handreiking geeft daarbij de relevante juridische achtergrondinformatie en geeft handvatten voor een vereenvoudigde risicoanalyse. Deze positionering maakt ook duidelijk dat het moeilijk is om de Handreiking op korte tot middellange termijn een meer verplichtend karakter te geven. Hiertoe zou de Handreiking moeten evolueren naar een standaard die voor min of meer alle gevallen toepasbaar is. Dit maakt van de Handreiking en Handboek, een grote toename van omvang en complexiteit zal daarvan het gevolg zijn.
Afgezien van deze praktische aspecten is het een gezond uitgangspunt dat de risicoafweging dicht bij de bron plaatsvindt en dat organisaties dus zelf voor hun eigen risicoafwegingen verantwoordelijk blijven, wat ook spreekt voor een vrijwillig gebruik van de Handreiking.

Ook de insteek van de Handreiking blijft ongewijzigd. Dat wil zeggen, het gaat er om te bepalen wat de behoefte is aan betrouwbaarheid, vanuit de gevoeligheid van de dienst in kwestie.

2.2.2 Vraaggerichte ontwikkeling

Het onderwerp is dusdanig breed dat een veelheid van onderwerpen in de Handreiking opgenomen zou kunnen worden. Hierbij kan worden gedacht aan uiteenlopende onderwerpen als processtappen in de back office die het frauderisico mitigeren tot besturing van ketens en het hieraan gerelateerde vertrouwen in machtigingsinformatie. De verleiding is groot om al deze onderwerpen een plekje te geven. Dit zal echter tot gevolg hebben dat de Handreiking in korte tijd veel omvangrijker en complexer wordt. De Handreiking zal hiermee waarschijnlijk zijn doel voorbij schieten en organisaties zullen omwille van de (gepercipieerde) complexiteit hun eigen methodes voor risicoanalyses (blijven) hanteren. Dit leidt tot de conclusie dat de doorontwikkeling van de handreiking vraaggericht moet zijn: alleen die onderwerpen worden toegevoegd waar een relevant deel van de doelgroep in de praktijk behoefte aan heeft. De handreiking moet niet “voor de troepen uit lopen”.

2.2.3 De handreiking moet een systematiek aanreiken en het onderwerp verhelderen

In de beginfase de Handreiking gepositioneerd als een systematiek voor een vereenvoudigde risicoanalyse. Hiermee, zo is de premisse, is het te gebruiken als een alternatief voor een volledige risicoanalyse. Er is vooralsnog geen informatie die deze positionering weerlegt. Wel is duidelijk dat veel organisaties al vastgestelde risicoanalysemethoden hebben en niet snel op een alternatieve systematiek overgaan.

De handreiking moet daarom inzicht blijven geven in de (risico)factoren die bijdragen aan de inschatting van een betrouwbaarheidsniveau en het relevante juridisch kader. Ook voor die partijen die de in de handreiking bevatte systematiek niet integraal adopteren, kunnen op deze wijze hun voordeel doen met de Handreiking. Tevens moet de Handreiking relevante voorbeelden aandragen waarmee de toepassing van die criteria wordt verduidelijkt en waar organisaties hun diensten en processen ook in kunnen herkennen.

2.2.4 Verbreden, niet complexer

De huidige handreiking is geen eenvoudig stuk. Methodisch gaat het om de weging van 8 criteria. Sommige criteria vergen bovendien dat men zich verdiept in de achtergronden. Met name is dit van toepassing bij de privacy, waarbij verdieping wordt gevraagd in de systematiek voor het bepalen van de risicoklasse, zoals het College Bescherming Persoonsgegevens (CBP) die hanteert in haar publicatie AV23 (Beveiliging van Persoonsgegevens)[1].

Om nog sprake te laten zijn van een vereenvoudiging ten opzichte van de gebruikelijke risicoanalyses, en breed gebruik van de handreiking door de gestelde doelgroep mogelijk te maken, is verdere toename van de complexiteit ongewenst. Dit punt is overigens niet zozeer op harde gebruikerservaringen gebaseerd, maar eerder op basis van eerste indrukken. De handreiking hoeft overigens niet in alle gevallen een handvat te bieden.

2.2.5 Standaardiseren van best practice, geen research

Slechts die onderwerpen moeten in de handreiking worden opgenomen, die conceptueel voldoende zijn uitgewerkt en algemeen geaccepteerd worden. Alleen dan is het naar verwachting mogelijk om het aspect betrouwbaarheidsniveaus zelfstandig te beschrijven. Dat is op zijn beurt nodig om te vermijden dat de uitbreiding van de handreiking gedomineerd wordt door bredere discussies, die op andere tafels thuishoren zoals over bijvoorbeeld over een trust framework of het aanbod van authenticatiemiddelen.

2.2.6 Aandacht voor Europese ontwikkelingen

Europa heeft elektronische identificatie over de grenzen heen als een van de belangrijke randvoorwaarden benoemt voor het functioneren van de digitale Interne Markt. Tal van Europese ontwikkelingen zijn gaande waaronder de herziening van de richtlijn elektronische handtekening, waarbij ook naar elektronische identiteiten wordt gekeken, en het zogenaamde STORK 2.0 project dat zich bezighoudt met grensoverschrijdende identificatie van bedrijven en machtigingen.

[1] http://www.cbpweb.nl/downloads_av/av23.pdf

Voor de uitbreiding van de Handreiking is het van belang de Europese ontwikkelingen op het gebied van de *Quality Authentication Assurance (QAA) levels (betrouwbaarheidsniveaus van authenticatiemiddelen)* goed te volgen. Deze zijn, na gebruik in het STORK project in (tijdelijk) beheer bij de Europese Commissie en vormen een belangrijke peiler voor (het gebruik van) de Handreiking. Wijzigingen in deze 'standaard' (zonder formeel deze status te hebben), zijn van belang. Het is waarschijnlijk dat de komende jaren wijzigingen plaatsvinden naarmate het gebruik van de QAA niveaus toeneemt. Naast het volgen van deze Europese ontwikkeling kan de ervaring die wordt opgedaan met de Handreiking ook worden teruggevoerd in het Europese circuit om zodoende de beschrijving van de QAA levels te verbeteren. Nederland heeft in het kader van eHerkenning al enkele vragen en dilemma's geconstateerd met de toepassing van de QAA niveaus en voorgelegd in Europese gremia.

2.3 Uitbreiding

Voor de aankomende uitbreiding van de handreiking heeft het College Standaardisatie een aantal onderwerpen voorgelegd. In deze paragraaf wordt kort geschetst welke uitbreiding op basis van het onderwerp van studie, de uitgangspunten en de inbreng van de inhoudelijke werkgroep opportuun zijn. Daarnaast wordt inzicht gegeven in de 'bijvangst' van het gevolgde proces, die niet direct onderdeel uitmaakt van de inhoudelijke uitbreiding van de handreiking. Het lijkt opportuun dat het Forum zich over deze onderwerpen apart buigt en een mogelijk handelingsperspectief voorstelt.

2.3.1 Onderwerpen voor de eerstvolgende release van de handreiking

De belangrijkste uitbreiding van de handreiking is gelegen in het toevoegen van een tweede kanaal van het verstrekken van diensten. De eerste handreiking ging uit van dienstverlening via het web aan burgers en bedrijven, het voorstel voor de uitbreiding is daarbij het ***machine to machine (M2M)*** kanaal toe te voegen en wel vanuit het *perspectief van betrouwbaarheidsniveau aspecten*.

Deze aanvulling komt tegemoet aan gewenste verbreding door dat deel van de dienstverlening wat zich automatisch tussen 'machines' afspeelt binnen scope te verklaren en hiermee een groot deel van de geautomatiseerde diensten/gegevensstromen tussen organisaties af te dekken. Hiermee neemt de waarde van de handreiking toe en stijgt de bruikbaarheid.

Voor beide kanalen is het vervolgens opportuun om de handreiking uit te breiden met de *betrouwbaarheidsniveau aspecten* van de onderwerpen ***wilsbeschikking via de digitale handtekening***, het digitaal ondertekenen van een bericht in aanvulling op de authenticatie, ***machtiging*** en de ***retourstroom***. Voor wat betreft de wilsbeschikking/ digitale handtekening lijkt de concept verordening die de Europese Commissie op dit gebied voorbereidt (herziening richtlijn gemeenschappelijk kader voor elektronische handtekeningen) voldoende uitgekristalliseerd om dit onderwerp op te pakken.

2.3.2 Wat buiten de boot valt

Wat opvalt is dat het proces dat is ingericht rondom de inhoudelijke uitbreiding van de handreiking veel procesmatige reacties evenals en reacties vanuit het gebruik heeft opgeleverd die niet direct geschikt zijn voor een inhoudelijke uitbreiding, maar wel van belang zijn voor het succes van de handreiking.

Om te voorkomen dat deze reacties vervliegen, omdat ze buiten scope van de inhoudelijke uitbreiding vallen, zijn ze in deze startnotitie opgenomen en wordt door de opstellers voorgesteld deze separaat in het Forum te bespreken en waar wenselijk en mogelijk te beleggen:

- *Duiden van het aanbod van authenticatiemiddelen* – Diverse partijen hebben de wens geuit dat er ook, en op korte termijn, aandacht wordt besteed aan de aanbodzijde van authenticatiemiddelen. Partijen geven aan geholpen te zijn wanneer daadwerkelijk in de markt aangeboden middelen in kaart zijn gebracht en af worden gezet tegen de criteria waaruit het betrouwbaarheidsniveau van individuele middelen blijkt. Hoewel het niet in de rede ligt dat het Forum Standaardisatie middelen gaat certificeren of verantwoordelijkheid voor een dergelijke certificering op zich zou nemen, kan het Forum Standaardisatie wel bevorderen dat er heldere criteria worden gesteld voor de classificatie van middelen en het zo mogelijk maken dat andere partijen een beoordelings-/certificeringsproces uitvoeren.

- *Single Sign On en overige organisatieoverschrijdende aspecten* - Single Sign On is voor veel dienstverleners een belangrijk en urgent onderwerp, omdat hiermee een betere gebruikerservaring wordt gerealiseerd. Aan de handreiking te associëren aspecten betreft ondermeer de keuze van het betrouwbaarheidsniveau in geval van een cluster van onderwerpen waarvoor Single Sign On aan de orde is. Ook zijn gezamenlijke afspraken nodig over diensten en organisaties heen, bijvoorbeeld over Sign out en time-outs, maar ook over aspecten als de noodzakelijke gebruikersinteracties bij het wisselen van diensten. Verder zijn er andere organisatieoverschrijdende afspraken mogelijk die leiden tot een minimum beveiligingsniveau in de dienstverlening.

- *Onderzoek naar, en community rondom, het gebruik van de handreiking* – Het delen van ervaringen met het gebruik van de handreiking is een middel om het gebruik verder toe te laten nemen en te faciliteren, mogelijk met een verdere harmoniserende werking. Transparantie naar burgers en bedrijven over het gebruik van betrouwbaarheidsniveaus bij overheidsorganisatie leidt daarnaast tot een vertserkte positie van die burger en bedrijven. Geconstateerde verschillen in inschaling van soortgelijke diensten kunnen leiden tot verdere discussie en aanscherping van de handreiking.

- *Gebruiksaspecten* – Het perspectief van de eindgebruiker, zoals het door die eindgebruiker kunnen omgaan met het concept betrouwbaarheidsniveaus en wisseling van betrouwbaarheidsniveau in een sessie. Hierbij is bijzondere aandacht geboden voor digibeten en 55+ ers.

2.3.3 Planning

De handreiking kan rekenen op grote belangstelling in het veld. Het lijkt goed om de positieve energie die hiervan uit gaat verder te stimuleren en op relatief korte termijn te starten met het proces van de uitbreiding. Het ligt dan voor de hand de uitbreiding na instemming van het Forum aan te kondigen, interne voorbereidingen te treffen in de zomerperiode en in het derde kwartaal van 2012 een eerste bijeenkomst van de expertgroep te beleggen.

Hierbij moet rekening worden gehouden met de ontwikkelingen rondom de herziening van de richtlijn elektronische handtekening. Naar verwachting is deze na de zomer voldoende uitgekristalliseerd om zonder vertragingen in het proces te integreren.

2.4 ‘Schrijfwijzer’

In het wordingsproces van de startnotitie is een aantal duidelijke wensen naar voren gekomen voor de vorm van de uitbreiding van de handreiking:

- *Werk met use cases* – om de herkenbaarheid te borgen wordt voorgesteld te werken met een aantal use cases uit de praktijk. Daarbij zijn de volgende suggesties gedaan:
    - Neem mee wat er te leren valt uit de vergelijking van de papieren en de digitale processen. Welke problemen ontstaan wanneer papieren en digitale processen door elkaar heen lopen? Zijn er checks en balances die we in de papieren processen al lang hebben uitgevonden die in het digitale proces van toepassing kunnen zijn?
    - Wijdt één van de use cases aan machine to machine uitwisseling.
    - Stel wilsbeschikking en retourstroom centraal in een van de use cases.

- *Besteed beknopt aandacht aan wat er in de omgeving speelt* - aan werkgroepen en ontwikkelingen op het gebied van juridische aspecten, standaardisatie, organisatie, zo mogelijk met verwijzingen zodat de lezer zich verder kan informeren buiten de directe scope van de handleiding en overlap wordt voorkomen

- *Versterk de relatie met de informatiebeveiligingscommunity* - Zowel inhoudelijk met expliciete verwijzingen naar relevante standaarden (bijvoorbeeld ISO 27001) als ook procedureel door afstemming met de rijksbrede ontwikkelingen op informatiebeveiliging gebied, die onder verantwoordelijkheid van het ICCIO plaatsvinden en waaronder ook de normenkaders vallen die binnen het Rijk worden afgeleid en gehanteerd.

- *Betrek in ieder geval STORK2.0* - Betrek een vertegenwoordiger uit het relevante werkpakket (WP3) uit STORK2.0 als agendalid[2] .

[2] Let op dit moet in het proces worden geborgd en is geen onderdeel inhoudelijke uitbreiding; wel van proces beïnvloeden Europa. In de werkgroep is de afspraak gemaakt dat min EL&I (dhr Freek van Krevel) contact opneemt met STROK2.0 voor het agendalidmaatschap in de fase na de acceptatie van de startnotitie.

3 Onderbouwing

In dit hoofdstuk worden de inhoudelijke onderwerpen, waarmee de handreiking uitgebreid zou kunnen worden, verkend. Allereerst wordt een groslijst gepresenteerd van 'kandidaat' onderwerpen. Vervolgens wordt van die ontwikkelingen nagegaan:

- Past dit onderwerp in de scope van het vaststellen van het betrouwbaarheidsniveaus van één individuele dienst?
- Is er nu of later (voldoende) vraag om dit onderwerp op te nemen?
- Is het onderwerp voldoende uitgekristalliseerd om een standaard benadering te kunnen geven voor het vaststellen van het betrouwbaarheidsniveau?
- Wat zijn de relevante nationale of internationale ontwikkelingen of, indien nog niet beschikbaar, wanneer zijn die te verwachten?
- Zijn er relevante nationale of internationale ontwikkelingen die op dit onderwerp zijn te beïnvloeden?

Dit leidt tot een overzicht van onderwerpen die in de eerstvolgende uitbreiding aan bod komen en onderwerpen die op een ‘voorraadlijst’ worden geplaatst. In dit hoofdstuk worden alleen de onderwerpen uitgewerkt die worden voorgesteld voor opname op korte termijn in de handreiking.

3.1 Groslijst kandidaat onderwerpen

De volgende onderwerpen zijn initieel beschouwd voor opname in de handreiking. De eerste vijf onderwerpen zijn in de eerste versie van de Handreiking bewust buiten scope gelaten, om de ontwikkeling in eerste instantie niet te ingewikkeld te maken. Het gaat steeds om de onderwerpen in relatie tot de betrouwbaarheidsniveau aspecten:

- Machine-to-machine verkeer
- Machtigingen (tussen organisaties en individuen en binnen een organisatie)
- Wilsbeschikking (e-Handtekening)
- Attribuut verstrekking
- Retour stroom (ontvangst)
- Autorisatie (binnen dienstverlener)
- Kanaalbeveiliging
- Single Sign On (SSO)
- Organisatie: Ketengovernance

3.2 Opportuniteit onderwerpen groslijst

3.2.1 Machine-to-machine en Machtigingen.

Voor machine-to-machine verkeer alsmede (keten) machtigingen geldt dat dit onderwerpen zijn die centraal staan in de huidige ontwikkeling van e-overheidsvoorzieningen en de doorontwikkeling naar één nationale infrastructuur op dit gebied. Zulks getuige de inhoud van de GOA rapportage en het A3 rapport. De behoefte

aan hogere betrouwbaarheidsniveaus is daarbij inmiddels manifest geworden. In alle ontwikkelingen rondom GOA is het gedachtegoed inmiddels ook voldoende uitgewerkt om uitwerking van het onderwerp in termen van betrouwbaarheidsniveaus mogelijk te maken. Deze onderwerpen zijn derhalve op korte termijn op te nemen in de handreiking en zijn relevant voor het inschatten van het betrouwbaarheidsniveau van één individuele dienst.

Het onderwerp machtigingen (met name de vraag welke natuurlijke persoon welke organisatie mag vertegenwoordigen) is een onderwerp dat ook in Europees verband wordt uitgewerkt (STORK, eID for legal persons en machtigingen). Hier dient derhalve de afstemming te worden gezocht, in casu het inbrengen van het Nederlandse gedachtegoed in de Europese arena.

3.2.2 Wilsbeschikking (eHandtekeningen)

Voor de elektronische handtekeningen, het digitaal ondertekenen van een bericht in aanvulling op de authenticatie, geldt dat het onderwerp uit en te na bekend is. Wel zijn er nog steeds vormen van elektronische handtekeningen waarvan de precieze status betwist is, met name waar het de vraag betreft of een bepaalde handtekening gekwalificeerd is of niet.

Rondom eHandtekeningen geldt dat er een herziening van de Europese richtlijn elektronische handtekeningen op korte termijn aan de orde is. Deze herziening neemt de vorm aan van een verordening. De herziening is zover gevorderd dat dit in de uitbreiding van de handreiking opgenomen kan worden.

3.2.3 Attribuutverstrekking

Attribuutverstrekking is een onderwerp dat van belang is voor aanvullende autorisaties, closed user groups en de communicatie van beroepskwalificaties en dergelijke. In dat opzicht is het een belangrijk onderwerp, waar ook vraag naar is. Het onderwerp staat echter nog teveel in de kinderschoenen om nu reeds opname in de Handreiking te rechtvaardigen, in eHerkenning worden hier nu de eerste ervaringen mee opgedaan.

3.2.4 Retourstromen (ontvangst)

Het onderwerp retourstromen is in de huidige handreiking buiten beschouwing gelaten. Het onderwerp is echter een essentieel onderdeel van de complete dienstverlening van grote uitvoerders. Daarom wordt voorgesteld dit onderwerp wel mee te nemen. De inhoudelijke werkgroep heeft daarbij tevens de combinatie van papieren en elektronische processen genoemd.

3.2.5 Autorisaties (binnen dienstverleners)

Autorisaties bevinden zich goeddeels in het domein van de dienstverleners, die hiervoor uiteraard wel de juiste gegevens moeten krijgen (authenticatie, machtigingen, attributen). Gegeven deze plaatsing wordt voorgesteld om autorisaties ten principale buiten scope te plaatsen.

3.2.6 Kanaalbeveiliging

De handreiking gaat uit van een bepaalde standaard ICT omgeving en daarvoor geldende beveiliging. In beginsel zou het mogelijk zijn om het betrouwbaarheidsniveau ook een bepaald niveau van bijvoorbeeld kanaalbeveiliging (beveiligd transport bijvoorbeeld) te laten dicteren. Deze aanpak achten we op dit moment echter niet opportuun, de trend in de overheid is eerder om een aantal standaard mechanismen aan te bieden en standaard beveiligingsnormen te stellen.

3.2.7 Single Sign On en ketengovernance

Het onderwerp Single-Sign-On is onvermijdelijk verbonden aan identificatie en authenticatie. Echter gezien de focus van de uitbreiding van de handreiking op het vaststellen van het betrouwbaarheidsniveau dat nodig is voor het vaststellen van één individuele dienst, valt dit onderwerp nu buiten scope. Dit zelfde geldt voor het onderwerp ketenbesturing, dat zich bezighoudt met de (organisatie)vraagstukken die ontstaan in het gebruik van elektronische authenticatiemiddelen voor het aanbieden van elektronische diensten in ketens en over processen heen. Daarnaast is het maar zeer de vraag of dit onderwerp voldoende is uitgekristalliseerd om de vertaling te maken naar de praktische verwerking in het vaststellen van betrouwbaarheidsniveaus.

3.3 Selectie voor de uitbreiding van de handreiking

3.3.1 Geselecteerde onderwerpen

Op basis van het voorgaande wordt voorgesteld met de volgende onderwerpen in de eerstvolgende uitbreiding aan de slag te gaan:

- Machine 2 machine.
- Machtiging.
- Wilsuiting/ elektronische handtekening.
- Retourstoom.

3.3.2 De inhoudelijke voorraadlijst

De duiding hierboven houdt in dat een aantal onderwerpen wel interessant is voor een uitbreiding van de handreiking maar op dit moment nog niet opportuun worden geacht. Deze onderwerpen komen op de voorraadlijst voor een eventuele latere uitbreiding. Het gaat dan om:

- Attributen.
- Ketengovernance.
- SSO.
- Eventueel: kanaalbeveiliging (afhankelijk van de ontwikkeling).

Bijlage A details geselecteerde onderwerpen

Machine to Machine (M2M)

- Wat is het?
  - End-to-end authenticatie van een geautomatiseerde entiteit (machine, applicatie,service)
  - (Keten van) machtiging(en) van de geautomatiseerde entiteit c.q. de houderorganisatie onder wiens verantwoordelijkheid deze geautomatiseerde entiteit functioneert
  - Logging, toezicht, governance in ketens
- Wat is het niet?
  - Wilsuiting van (bestuurder van) een organisatie
- Urgentie dienstverlening
  - Speelt nu. Dit is een kernonderdeel van de wijze waarop de uitvoerders geautomatiseerde stromen verwerken.
- Aspecten betrouwbaarheid aanbod
  - Binding van authenticatiemiddel aan geautomatiseerde entiteit
  - Binding van authenticatiemiddel aan houderorganisatie
  - Sterkte van mechanisme van authenticatiemiddel
  - Betrouwbaarheid van administratie van machtigingen (zie machtigingen)
  - Sterkte zwarte / witte lijst mechanisme
- Aspecten betrouwbaarheid vraag (dienstverlening)
  - Aanvullende feedbackloops oid ter vermindering risico. (Nu in de sfeer van correctiefactoren)
- Aannames over omgeving (referentiescenario)
  - Closed User Group met overheidsorganisaties en ‘erkend’ bedrijfsleven → well behaved toepassingen op eindpunten, bekende beheerder
  - Machines hebben zelf adequate fysieke en logische toegangsbeveiliging
  - Standaard model voor logging, toezicht, governance
- Afhankelijkheden
  - Onderwerp is inhoudelijk verkend in het GOA traject, wordt momenteel uitgewerkt binnen eHerkenning
  - Er is geen directe relatie met STORK
  - Er zijn mogelijk wel verbanden met internationale sectorale ontwikkelingen

Machtiging inclusief retourstroom

- Wat is het?
  - Machtigingen (voor goed gedefinieerde diensten) van een machtigende persoon (natuurlijke of niet-natuurlijke persoon) naar een gemachtigde persoon
  - Machtigingsketens
- Wat is het niet?
  - Autorisatie in het domein van de dienstverlener
- Urgentie dienstverlening
  - Is direct gewenst als uitvloeisel van GOA/A3. Voorzieningen voor te treffen in allerhande e-

overheids diensten en -voorzieningen

- Aspecten betrouwbaarheid aanbod
  - Sterkte authenticatie gemachtigde
  - Sterkte registratieproces machtigingen
  - Feedback actualiteit machtigingen
- Aspecten betrouwbaarheid vraag
  - Wie mag machtigingen administreren. High trust / low trust aspecten.
- Aannames over omgeving
  - …
- Afhankelijkheden
  - Wordt uitgewerkt ihkv eHerkenning, hoofdroute traject
  - Gaat ook spelen in STORK 2

Wilsuiting/ eHandtekening

- Wat is het?
  - Handtekeningdiensten
  - Notariaat. Bewijzen, bewaren.
- Wat is het niet?
  - Urgentie dienstverlening
  - Is wel behoefte aan. Urgentie niet geheel duidelijk.
  - Aspecten betrouwbaarheid aanbod
  - Vormgeving handtekeningdienst, WYSIWYS aspecten
  - Afhankelijkheid van procedurele aspecten, sole control aspecten
- Aspecten betrouwbaarheid vraag
  - Juridische behoefte
- Aannames over omgeving
  - …
- Afhankelijkheden
- Herziening Richtlijn