Forum Standaardisatie

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag
96810
2509 JE Den Haag
www.logius.nl

Inlichtingen bij
B.S.J. Knubben
Senior Adviseur
M +31(0)6-21162373
bart.knubben@logius.nl

Datum
22 augustus 2013

notitie

Reactie op "Ontwerp op hoofdlijnen van de werking van het eID Stelsel NL" d.d. 7 juni 2013 (versie 0.9)

1. Achtergrond

Het Forum Standaardisatie is gevraagd om op het document "Ontwerp op hoofdlijnen van de werking van het eID Stelsel NL" d.d. 7 juni 2013 te reageren. Dit past bij de formele adviesrol die het Forum heeft bij de totstandkoming van het eID-stelsel. De scope van de adviesrol omvat koppelvlakken, standaarden en interoperabiliteit.[1]

Het document is 20 juni 2013 ontvangen. Het verzoek van het eID-stelsel was om liefst uiterlijk 19 juli een reactie te geven. De Forum-sponsoren rondom het onderwerp authenticatie&autorisatie en een aantal experts uit het netwerk van het Forum Standaardisatie is gevraagd om input te leveren. Deze notitie is opgesteld door het Bureau. Ontvangen input is erin verwerkt. De notitie is (nog) niet met het voltallige Forum gedeeld.

2. Aanpak

De volgende vragen worden in de volgende paragraaf geadresseerd.

1. Wat is de **algemene indruk**?
2. Zijn alle **actoren** en de **koppelvlakken** daartussen duidelijk?
3. Zijn de functionele **beschrijvingen van de berichten**, die op de koppelvlakken worden uitgewisseld, duidelijk?
4. Is duidelijk hoe de **privacy en beveiliging** worden gewaarborgd?
5. Zijn er nog **overige opmerkingen**?

3.1 Algemeen

Het ontwerp ziet het eID-stelsel als infrastructuur. Standaardisatie komt op veel plekken in het document als belangrijk middel terug. Deze benadering kan worden onderschreven. Het uitgangspunt dat de "invulling in overleg met overheid, markt en wetenschap tot stand moet komen" kan eveneens worden onderschreven. De ervaring rondom open standaarden leert dat juist het open totstandskomings- en beheerproces zeer bepalend is voor het succes van een standaard. Het ontwerp beschrijft het eID-stelsel op hoofdlijnen en is nog erg conceptueel van aard. Veel moet nog ingevuld en nader gedetailleerd worden, ook waar het gaat om zaken die aan koppelvlakken, standaarden en interoperabiliteit raken.

[1] Zie Forum-notities https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0416/FS-20130416.06D-Adviesrol-FS-eID-stelsel.pdf en https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0205/FS-20130205.05C-Notitie-eID-en-Forum-Standaardisatie.pdf

Het ontwerp gaat uit van verregaande federatieve opzet waarbij bedrijven en burgers met behulp van private en publieke middelen toegang kunnen krijgen tot zowel private als publieke diensten. Vanuit interoperabiliteitsperspectief is het positief dat de eID een oplossing wil bieden voor de huidige versnipperde situatie (DigiD, DigiD machtigen, eHerkenning etc.). De verregaande federatieve opzet betekent wel dat binnen het eID-stelsel een groot en divers aantal belanghebbenden actief is. Dit stelt hoge eisen aan regelgeving, governance, toezicht en beveiliging om de interoperabiliteit van en het vertrouwen in het eID-stelsel te realiseren en te behouden. Deze aspecten vallen wellicht (deels) buiten scope van het ontwerpdocument en worden waarschijnlijk elders geadresseerd.

3.2 Actoren en koppelvlakken

Internationale actoren

- Het eID-stelsel wordt gepresenteerd als "nationale infrastructuur". Dit roept de vraag op of en, zo ja, hoe rekening wordt gehouden met aansluiting op buitenlandse en Europese infrastructuren. Vanuit de Europese Unie is regelgeving aanstaande die het belang van interoperabiliteit benadrukt en die een coördinatiemechanisme introduceert om deze interoperabiliteit te bewerkstelligen ("Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt").
- Het is aan te bevelen om te leren en te kopiëren van buitenlandse overheden die vergelijkbare oplossingen al hebben gerealiseerd (zoals Zweden, Finland, Noorwegen en Estland). Op het niveau van standaarden zijn o.a. STORK en het Kantara SAML eGov profile relevante ontwikkelingen die kunnen helpen om een interfederatie met buitenlandse overheden te realiseren.

eID-actoren

- Het koppelvlak met de dienstencatalogus, dat is terugkomt in paragraaf 6.2, is niet helemaal uitgewerkt.
- De koppeling met (basis)registraties komt nog niet erg uitgewerkt terug. Zij zijn als leveranciers van attribuutverklaringen waarschijnlijk een belangrijke actor.
- Het koppelvlak met de "Handelende Partij" is niet uitgewerkt.
    - Hoe transparant is eID voor de gebruiker? Welke gegevens moet hij aanleveren en wat ziet hij terug in zijn scherm? Kan hij bijvoorbeeld zien/bepalen welke attributen worden gedeeld? Kan hij zijn verschillende pseudo-id's inzien? Is hij degene die pseudo-id's mag koppelen en ontkoppelen aan een (sectoraal) persoonsnummer?
    - Door de federatieve opzet met een veelheid aan middelen zal standaardisatie van de gebruikersinterface (koppelvlak naar eindgebruiker) zeer relevant zijn.
- Het is niet duidelijk of het eID-stelsel ook inzetbaar is voor overheidsmedewerkers die zich moeten authenticeren bij hun eigen organisatie en bij andere overheidsorganisaties. Dit is een relevante use case o.a. in het SUWI-domein.
- De relatie met bestaande voorzieningen, zoals DigiD en E-Herkenning, is nog niet zo sterk uitgewerkt.

Overig

- De nummers van de koppelvlakken komen niet overal consistent terug (zie verschil figuren in paragraaf 4.3 op p. 19 en 20).

3.3 Functionele beschrijvingen van berichten

Algemeen

- De primaire identifier tussen partijen in het eID-stelsel is de zogenoemde pseudo-ID. Vanuit privacy-perspectief is dat een verstandige keuze. Het is van belang dat dit de pseudo-id op een onomkeerbare wijze wordt berekend ('one way'), bijv. op basis van de gangbare standaard SHA-2.
- In het ontwerp staat dat de pseudo-ID persistent is (p.9 en 11). Het is niet duidelijk hoe de persistentie zicht verhoudt tot het scenario dat een dienstaanbieder geen identificerend persoonsnummer nodig heeft , maar bijv. alleen hoeft te weten of iemand ouder is dan 16. In dat geval zou de dienstaanbieder namelijk voldoende moeten hebben aan een transient (tijdelijk) pseudo-id.
- Op ieder koppelvlakken zullen (tenminste) twee berichten (vraag/antwoord) worde uitgewisseld. Nu staan in paragraaf 6.3 alleen de antwoorden te zijn beschreven. Het verdient aanbeveling om de dialoog qua berichten functioneel te beschrijven.
- De attribuutverklaring is niet verder uitgewerkt in paragraaf 6.3.
- Je zou verwachten dat in iedere verklaring de identiteit van de partijen waartussen het bericht wordt uitgewisseld terugkomt (eID-makelaar, Authenticatiedienst, Machtigingsdienst, Attribuut-leverancier). Dat lijkt nu niet het geval.
- De berichten voor K4 (tussen Dienstaanbieder en eID-makelaar) zijn niet nader gedefinieerd.

<u>K1&2. Identiteitsverklaring (tussen Dienstaanbieder en Authenticatiedienst óf Sectoraal koppelregister)</u>

T.a.v. aanroep (p.15)

- De definitie van "Verklaarder" is niet duidelijk. Kan dit de "'Wat is een "Gecertificeerde Partij"?
- "identiteit van dienstaanbieder":
    - Er wordt geen unieke identifier van de dienst meegegeven (Dienst-ID). Dat lijkt een hiaat. In deze identifier kan ook de identiteit van de dienstaanbieder worden opgenomen.
    - Hoe stellen andere partijen (eID-makelaar, Authenticatiedienst etc.) de identiteit van de dienst en dienstaanbieder betrouwbaar vast?
    - Andere partijen in het stelsel (eID-makelaar, Authenticatiedienst, Machtigingsdienst, Attribuut-leverancier) weten wanneer een gebruiker een bepaalde dienst gebruikt. Vanuit privacy-perspectief is dat onwenselijk, tenzij hiertegen maatregelen worden genomen.
- "gevraagde minimale STORK-niveau":
    - In paragraaf 6.2 staat dat dit in het dienstenregister is vastgelegd. Het is niet duidelijk hoe het koppelvlak met dit register eruit ziet.
- "ja/nee-waarde of een niet-natuurlijk persoon als handelende partij is toegestaan voor de dienst.":
    - Moet dit niet in het dienstenregister worden opgenomen?
    - "ja/nee-waarde" lijkt wat te beperkt als je ervan uit gaat dat een natuurlijk en/of niet-natuurlijk-persoon zijn toegestaan.

T.a.v. antwoord (p.30)

- Er wordt hier (nog) geen onderscheid gemaakt tussen Identiteitsverklaring van Authenticatiedienst (K1) en Identiteitsverklaring van Koppelregister (K2).
- In het antwoord ontbreekt het veld "Dienst-ID".

- Veld "VerklaringID": Hiervoor kan een hashwaarde over bepaalde gegevens worden gebruikt. Bijv. o.b.v. de standaad SHA-2 die op de lijst met gangbare standaarden van het Forum Standaardisatie staat.
- Veld "Uitgiftemoment": Op de lijst met gangbare standaarden van het Forum Standaardisatie opgenomen de standaard ISO 8601 voor de notatie van datum en tijd opgenomen.
- Veld "Ondertekening":
    - Wordt het bericht ook versleuteld?
    - Op wiens naam staat het PKI-certificaat?
- Veld "HandeldendePartij":
    - Wat is "NHP" en ("NNHP")?
- Veld "Condities":
    - Niet geheel duidelijk wat met "tijd, doel of doelgroep" wordt bedoeld.
- Veld "Comfort Informatie tbv Belanghebbende":
    - Dit lijken attributen te zijn, waarvan het niet altijd nodig/toegestaan is om deze uit te wisselen. Moeten ze in het ontwerp niet als zodanig terugkomen?
    - Waarom is de "samengestelde naam van de Handelende Partij" verplicht als het een Gemachtigde betreft?
- Veld "Herleidbaarheid":
    - De twee opgenomen definities verschillen van elkaar.
    - Het is niet geheel duidelijk wat de betekenis is van dit veld. Het lijkt erop dat het bedoeld is om de "Bevoegdheidsketen" vast te leggen.

K3. Bevoegdheidsverklaring (tussen eID-makelaar en Machtigingsdienst)

T.a.v. aanroep (p.15)

- Bevoegdheidsverklaring" is enigszins misleidend, wellicht is "vertegenwoordigingsverklaring" een betere term.
- "Identiteit van de belanghebbende": In het antwoordbericht wordt deze "Vertegenwoordigde" genoemd. Het gaat hier waarschijnlijk om identificerende gegevens, zoals BSN.

T.a.v. antwoord (p.30)

- *Zie* opmerkingen *over overeenkomstige velden onder "K1&2. Identiteitsverklaring".*
- Veld "BevoegdePartij"
    - Het gaat hier om een HandelendePartij die wel/niet gemachtigd om in naam van een Vertegenwoordigde een bepaalde Dienst te gebruiken.
    - Het lijkt handiger om dit veld "HandelendePartij" te noemen en een los veld (attribuut) "Machtiging" met als veldwaarden "Ja/Nee" op te nemen.
    - De Machtigingsdienst ontvangt nu het sectorale persoonsnummer van zowel de "Bevoegde Partij" als de "Vertegenwoordigde ". Zou je dit net als bij de "Dienstaanbieder" ook met pseudo-id's kunnen doen?
- Veld "Bevoegdheid":
    - Dit lijkt een overbodig veld. De omvang van de machtiging betreft de dienst. Zoals onder "K1&2 Identiteitsverklaring" is aangegeven moet wel de "Dienst-ID" zijn opgenomen.
- Er lijkt geen rekening gehouden met het stapelen van Bevoegdheidsverklaringen ("doormachtigen"). Is dat een bewuste keuze?

K5. Associatieverklaring (tussen Dienstverlener en Dienstaanbieder)

T.a.v. aanroep (p. 23)

- De aanroep vindt plaats door het "Transactiebericht". In de definitie van het "Transactiebericht" staat echter dat deze de "Associatieverklaring" bevat. Dit lijkt zich niet goed tot elkaar te verhouden.

T.a.v. antwoord (p.23 en 32)

- Op p.23 staat onder antwoord "resultaatbericht". Dit moet waarschijnlijk de "Associatieverklaring" zijn.
- *Zie* opmerkingen *over overeenkomstige velden onder "K1&2. Identiteitsverklaring".*
- "Bevoegdheidsketen": Hoe verhoudt dit zich tot het veld "Herleidbaarheid" in de andere Verklaringen?
- De identiteit van de Dienstverlener (en/of zijn IntermediaireDienst-ID) en de Dienstaanbieder (en/of Dienst-ID) ontbreken in het bericht.

3.4 Beveiliging en privacy

- Bepaalde partijen, zoals de authenticatiedienstaanbieder,de makelaar en het (sectoraal) koppelregister kunnen veel persoonsgebonden informatie over het gebruik van diensten vastleggen en mogelijk misbruiken. Het is niet duidelijk welke (technische en organisatorische) maatregelen zijn genomen om dit te voorkomen.
- Het pseudo-id is een persoonsgegeven en mag dus niet zomaar uitgewisseld worden tussen sectorale dienstaanbieders. Goed om dit expliciet te laten terugkomen.
- Een Dienstaanbieder (en eID-makelaar) mag uiteraard niet zomaar bij alle attributen van een persoon. In het ontwerp komt deze autorisatie van de Dienstaanbieder niet terug. De HandelendePartij kan in het geven toestemming voor het leveren van attributen ook een rol in spelen.
- Op p.17 staat privacy hotaspot risico genoemd, maar niet duidelijk wordt hoe het moet worden vermeden (moet er wellicht staan "één eID-makelaar" (...) moet worden vermeden"?). Is wel van belang, zeker je nu je je zoveel moeite getroost met de pseudo-identiteiten.

3.5 Overige opmerkingen

- "Single Sign On" komt niet terug.
- "Step Up Authentication", wat bijvoorbeeld voor ondertekening relevant kan zijn, komt niet terug in het ontwerp.
- In het ontwerp is uitgegaan van centrale attribuut-leveranciers. Daarnaast kan een Dienstaanbieder uiteraard ook zelf (buiten eID-stelsel om) toegang hebben tot attribuut-informatie. Attribuut-informatie kan eventueel ook bij de gebruiker zijn vastgelegd, bijv. op een kaart. Het is niet geheel duidelijk of het ontwerp hierin voorziet.
- Pseudo-identiteiten maken het complex (en het is al complex met de verschillende middelleveranciers, intermediairs etc), dus:
    - manage deze complexiteit goed (hoe doe je pseudonummerportabiliteit precies: goed, goedkoop en AL vriendelijk)
    - hoe zorg je ervoor dat de pseudonummers uniek zijn (er geen dubbele worden gegenereerd)
      beschrijf pseudonummerfunctionaliteit zo dat het niet perse het middel is dat het genereert (die indruk ontstaat op p.11), maar ook de dienst kan zijn (op p.12 staat dat goed). Simpeler middelen (zoals DigiD) kunnen 'via de dienst' zo ook pseudonummerfunctionaliteit bieden.
    - hou het gebruiksvriendelijk: hou de complexiteit weg bij de

eindgebruiker als deze dat wil (niet iedereen wil elke nieuwe OV kaart opnieuw activeren voor automatisch opladen, ov-fiets etc.; luie gebruiker moet ook bediend worden).

- Nog niet duidelijk wordt hoe de koppeltabellen gevuld worden voor met name bestaande klanten (p.9, 10 en 19). Hoe doe je dat goed, goedkoop en AL vriendelijk. Hoe voorkom je dat je dezelfde gebruiker meerdere keren voor gaat komen? Ga je dat bijvoorbeeld met attribuut vergelijking doen (voorletters+achternaam+geb. datum+geb. plaats etc), of anders?
- Wellicht noemen (p.8 of p.10) dat binnen de overheid t.a.v. burgers met het BSN nummer gewerkt zal worden (geen sectornummers).
- Op p12 staat de authenticatiedienst die een bedrijfsgebonden middel aan een medewerker verstrekt registreert welke bevoegdheden deze medewerker heeft. Aandachtspunt is de wijze waarop de diensten daarbij beschreven worden. Bij overheden, maar nog moeilijker bij private partijen. Daarbij komt nog de uitdaging van evt. gewenste hierarchiën hierin (al mijn belastingzaken, cq. iemand is bevoegd kantoorartikelen te kopen)
- Het is goed dat in het document begrippen worden gedefinieerd. Niet alle begrippen zijn echter eenduidig gedefinieerd en worden ook niet altijd consequent toegepast. Bijv. onderscheid "dienst" en "transactie" niet geheel helder en beide begrippen niet consistent gebruikt. Ook bijv. worden "handelende partij'" en "gebruiker" door elkaar gebruikt.
- Wellicht handig om alle nader gedefinieerde termen in het document te markeren. Het lijkt ook slim om qua terminologie te kiezen voor een bestaand begrippenkader bijv. van de genoemde Europese (concept-)Verordening, van eHerkenning en/of van standaarden zoals ISO10181-3, SAML en XACML.
- Identificatie, authenticatie en autorisatie kunnen nog wat strakker worden gedefinieerd en gehanteerd. Hieronder een voorzet:

Identificatie *('Wie bent u?' --> 'Ik ben mr X.')*
Je naam en/of andere persoonsattributen (zoals woonplaats en geboortedatum) aan een ander bekend maken.

Authenticatie *('Kunt u aantonen dat u mr X bent?' --> 'ja, zie dit bewijs.')*
Het identificeren staven mbv een middel ('iets dat je weet (bijv. wachtwoord), hebt (bijv. paspoort) en/of bent (bijv. iris-scan)'). Voor de sterkte van een authenticatiemiddel is de inrichting van het proces van uitgifte, gebruik en intrekking bepalend. Een authenticatiemiddel kan afgeleid zijn van een ander sterker middel (bijv. bankpas van paspoort).

Autorisatie *('Is mr X bevoegd?' --> 'ja,mr X is ouder dan 18 jaar, dus mag hij dienst Z gebruiken' of 'ja, mr X staat te boek als vertegenwoordigervan onderneming Y, dus mag hij dienst Z gebruiken')*
Iemand na betrouwbare authenticatie op basis van iemands persoonsattributen (toegangs-)rechten geven. De persoonsattributen (bijv. woonplaats, geboortedatum, vertegenwoordigingsbevoegdheid) kunnen worden opgevraagd uit registers of uitgelezen van het authenticatiemiddel. De bevoegdheid kan ex ante of ex post (d.w.z. voor of na de rechtshandeling) worden gevalideerd.