Notitie van eID over verwerking Forum-adviespunten

Ontvangen van Hans-Rob de Reus op 27-1-2014

Opmerking	Verwerkt?
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.	Op twee onderdelen: - door aan te sluiten op PEPS - als basis voor de registratie van een persoon, worden persoonsgegevens gehanteerd en niet bijvoorbeeld het BSN. Deze persoonsgegevens kunnen ook van een buitenlands (e)ID-document komen.
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.	Er is gekeken naar oplossingen van buitenlandse overheden. Met name naar Duitsland, maar ook naar oplossingen in andere landen. Voor betrouwbaarheidsniveaus volgen wij STORK (en de handreiking van het Forum) voor authenticatie. Voor machtigen en ondertekenen wachten wij nog op nieuwe handreikingen.
• Het koppelvlak met de dienstencatalogus, dat is terugkomt in paragraaf 6.2, is niet helemaal uitgewerkt.	Is nog niet beschreven
• De koppeling met (basis)registraties komt nog niet erg uitgewerkt terug. Zij zijn als leveranciers van attribuutverklaringen waarschijnlijk een belangrijke actor.	Koppelvlak attribuutverklaring wel beschreven, niet specifiek voor basisregistraties. Gevolgen voor deze basisregistraties zijn ook nog niet in beeld gebracht.
• Het koppelvlak met de "Handelende Partij" is niet uitgewerkt.	Nee, wel in storyboards. Verder met name interactie ontwerp. Eisen zijn wel geformuleerd.
o 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?	Transparantie is nu nog alleen in de vorm van ontwerpeisen. User consent komt wel al terug in de beschrijving van de werking. De koppelprocessen moeten nog worden uitgewerkt (ook o.b.v. betrouwbaarheidsniveaus) waarbij elke sector een eigen invulling kan kiezen. Op basis van het ontwerp gebaseerd op persoonsgegevens is koppeling goed uitvoerbaar. Het is niet de bedoeling dat een gebruiker een pseudoID ziet (is een technische sleutel).
o Door de federatieve opzet met een veelheid aan middelen zal standaardisatie van de gebruikersinterface (koppelvlak naar eindgebruiker) zeer relevant zijn.	Klopt, vergelijk gemaakt met Ideal, zie ook storyboards
• 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.	Niet expliciet, maar in opzet zeker mogelijk. Het nieuwe RIN is voorbeeld van een Sector invulling.
• De relatie met bestaande voorzieningen, zoals DigiD en E-	Deze voorzieningen worden

Opmerking	Verwerkt?
Herkenning, is nog niet zo sterk uitgewerkt.	gemigreerd obv eID Stelsel. Hiervoor wordt een apart migratieplan opgesteld.
De nummers van de koppelvlakken komen niet overal consistent terug (zie verschil figuren in paragraaf 4.3 op p. 19 en 20).	Punt van aandacht in laatste review
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.	Werkwijze pseudoid uitgebreid beschreven in werking stelsel
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.	Zie werking, zie story board
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.	Zie koppelvlakspecificaties
De attribuutverklaring is niet verder uitgewerkt in paragraaf 6.3.	Zie koppelvlakspecificaties
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.	Zie werking stelsel en koppelvlak spec's
De berichten voor K4 (tussen Dienstaanbieder en eID-makelaar) zijn niet nader gedefinieerd.	Zie werking stelsel en koppelvlak spec's
• De definitie van "Verklaarder" is niet duidelijk. Kan dit de ""Wat is een "Gecertificeerde Partij"?	Zie werking stelsel
• "identiteit van dienstaanbieder":	
o 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.	Zie werking stelsel en koppelvlak spec's. Koppeling met dienstencatalogus moet in volgende versie nader worden uitgewerkt.
o Hoe stellen andere partijen (eID-makelaar, Authenticatiedienst etc.) de identiteit van de dienst en dienstaanbieder betrouwbaar vast?	Zie werking stelsel en koppelvlak spec's.
o 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.	In het ontwerp zijn veel PET invullingen gemaakt. Zie ontwerp beschrijving.
• "gevraagde minimale STORK-niveau":	
o In paragraaf 6.2 staat dat dit in het dienstenregister is vastgelegd. Het is niet duidelijk hoe het koppelvlak met dit register eruit ziet.	Nog niet opgenomen Beschrijving en eisen aan dienstencatalogus in volgende versie.
• "ja/nee-waarde of een niet-natuurlijk persoon als handelende partij is toegestaan voor de dienst.":	
o Moet dit niet in het dienstenregister worden opgenomen?	Ja, moet nog worden gespecificeerd.
o "ja/nee-waarde" lijkt wat te beperkt als je ervan uit gaat dat een natuurlijk en/of niet-natuurlijk-persoon zijn toegestaan.	Klopt
T.a.v. antwoord (p.30)	

Opmerking	Verwerkt?
Er wordt hier (nog) geen onderscheid gemaakt tussen Identiteitsverklaring van Authenticatiedienst (K1) en Identiteitsverklaring van Koppelregister (K2).	Koppelregister heet nu SectorID dienst. Deze levert een attribuutverklaring van het sectornummer. Deze wordt technisch onlosmakelijk verbonden aan de identiteitsverklaring.
In het antwoord ontbreekt het veld "Dienst-ID".	Wordt nog toegevoegd.
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	Er worden alleen functionele eisen gesteld. SAML laat dit verder vrij.
• 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.	Wordt gevolgd. Zie koppelvlakspecificaties
• Veld "Ondertekening":	
o Wordt het bericht ook versleuteld?	Het bericht alleen op transportniveau (TLS). Alle persoonsgegevens worden versleuteld (SAML Encrypted Attribute)
o Op wiens naam staat het PKI-certificaat?	Het signing certificaat staat op naam van de Issuer van de SAML Assertion (de verklaring)
• Veld "HandeldendePartij":	
o Wat is "NHP" en ("NNHP")?	Natuurlijke Handelende Persoon (geboren) Niet Natuurlijk Handelende Persoon (opgericht)
• Veld "Condities":	
o Niet geheel duidelijk wat met "tijd, doel of doelgroep" wordt bedoeld.	Zie koppelvlakspecificaties
• Veld "Comfort Informatie tbv Belanghebbende":	
o 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?	Ja, User consent en in certificaat van ontvangende partij moet hiervoor toestemming staan
o Waarom is de "samengestelde naam van de Handelende Partij" verplicht als het een Gemachtigde betreft?	Zie koppelvlakspecificaties
• Veld "Herleidbaarheid":	
o De twee opgenomen definities verschillen van elkaar.	Zie koppelvlakspecificaties
o 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.	Zie koppelvlakspecificaties. Onlosmakelijk verbonden eerder verklaringen.
K3. Bevoegdheidsverklaring (tussen eID-makelaar en Machtigingsdienst)	
T.a.v. aanroep (p.15)	
Bevoegdheidsverklaring" is enigszins misleidend, wellicht is "vertegenwoordigingsverklaring" een betere term.	Gaat om de definitie
"Identiteit van de belanghebbende": In het antwoordbericht wordt deze "Vertegenwoordigde" genoemd. Het gaat hier waarschijnlijk om identificerende gegevens, zoals BSN.	Het gaat hier om een identiteit. In de meeste gevallen een pseudo ID.
T.a.v. antwoord (p.30)	
• Zie opmerkingen over overeenkomstige velden onder "K1&2. Identiteitsverklaring".	
• Veld "BevoegdePartij"	
o Het gaat hier om een HandelendePartij die wel/niet gemachtigd om in naam van een Vertegenwoordigde een bepaalde Dienst te gebruiken.	Ja

Opmerking	Verwerkt?
o Het lijkt handiger om dit veld "HandelendePartij" te noemen en een los veld (attribuut) "Machtiging" met als veldwaarden "Ja/Nee" op te nemen.	Nu in Engels
o 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?	Ja, is aangepast
• Veld "Bevoegdheid":	
o 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.	Zie koppelvakspecificaties
• Er lijkt geen rekening gehouden met het stapelen van Bevoegdheidsverklaringen ("doormachtigen"). Is dat een bewuste keuze?	Doormachtigen kan. Zie koppelvakspecificaties
K5. Associatieverklaring (tussen Dienstverlener en Dienstaanbieder)	Deze verklaring wordt (met bijbehorend koppelvlak) nog verder uitgewerkt.
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.	In werking stelsel nu duidelijker beschreven
Zie opmerkingen over overeenkomstige velden onder "K1&2. Identiteitsverklaring".	
"Bevoegdheidsketen": Hoe verhoudt dit zich tot het veld "Herleidbaarheid" in de andere Verklaringen?	Zie koppelvakspecificaties
De identiteit van de Dienstverlener (en/of zijn IntermediaireDienst-ID) en de Dienstaanbieder (en/of Dienst-ID) ontbreken in het bericht.	Zie koppelvakspecificaties
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.	Zie werking stelsel en eerdere opmerkingen. Hotspots zijn zoveel als mogelijk beperkt
Het pseudo-id is een persoonsgegeven en mag dus niet zomaar uitgewisseld worden tussen sectorale dienstaanbieders. Goed om dit expliciet te laten terugkomen.	Hier is user consent op van toepassing.
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.	Nu wel beschreven in werking stelsel
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.	In nieuwe beschrijving moet dit duidelijk zijn
3.5 Overige opmerkingen	
• "Single Sign On" komt niet terug.	Komt terug in volgende versie
• "Step Up Authentication", wat bijvoorbeeld voor ondertekening relevant kan zijn, komt niet terug in het ontwerp.	Ondertekenen moet nog verder worden uitgewerkt

Opmerking	Verwerkt?
• 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.	Klopt, is voorzien
• Pseudo-identiteiten maken het complex (en het is al complex met de verschillende middelleveranciers, intermediairs etc), dus:	
o manage deze complexiteit goed (hoe doe je pseudonummerportabiliteit precies: goed, goedkoop en AL vriendelijk)	Voorstel is om dit samen met marktpartijen concreet te maken in de POC's.
o hoe zorg je ervoor dat de pseudonummers uniek zijn (er geen dubbele worden gegenereerd)	Zie werking stelsel
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.	Pseudoniemen is uitgebreid beschreven in werking stelsel
o 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).	Gebruikersgemak is een ontwerpeis. Ook keuzevrijheid
• 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?	Zie werking stelsel en storyboards
• Wellicht noemen (p.8 of p.10) dat binnen de overheid t.a.v. burgers met het BSN nummer gewerkt zal worden (geen sectornummers).	Wordt terloops duidelijk, maar gaat over implementatie. Het stelsel zelf is breder dan alleen overheid.
• 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)	Dienstencatalogus en toegangsbeleid zijn idd belangrijke punten die nog verder uitgewerkt moeten worden.
• 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.	Nieuwe begrippenlijst opgeleverd
• Wellicht handig om alle nader gedefinieerde termen in het document te markeren. Het lijkt ook slim om qua terminologie zoveel mogelijk aan te sluiten bij bestaande begrippenkaders bijv. van de genoemde Europese (concept-)Verordening, van eHerkenning en/of van standaarden zoals ISO10181-3, SAML en XACML.	Is gedaan met small caps Ook een Engelse term toegevoegd. Koppelvlak spec's in het Engels
• Identificatie, authenticatie en autorisatie kunnen nog wat strakker worden gedefinieerd en gehanteerd. Hieronder een voorzet:	Zie nieuwe begrippenlijst
Identificatie ('Wie bent u?' --> 'Ik ben mr X.')	
Je naam en/of andere persoonsattributen (zoals woonplaats en	Zie beschrijving: werking stelsel en

Opmerking	Verwerkt?
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.	introductie eID