Programma eID
Afsprakenstelsel

Werking van het eID Stelsel

programma eID

Versie: 1.0

Datum: 21 januari 2014

Status: Definitief

Colofon

Programma eID
Deelproject Afsprakenstelsel

Bezoekadres:
Herman Gorterstraat 5
Utrecht

Versie	1.0
Opdrachtgever	Stuurgroep eID
Bijlage(n)	
Aantal pagina's	35
Exemplaarnummer	

Referenties

[1] **eID Stelsel - Memo - PseudoIDs - v04**. Programma eID, 9 december 2013.
[2] **Beheervoorziening BSN - Aanvullende functionele specificaties.** Versie 1.5, Agentschap BPR, 2 mei 2006.
[3] **Interface Specification**. STORK document D5.8.2b, October 4, 2010.

Inhoud

Colofon—2

Referenties—4

Inhoud—5

Inleiding—7

1 Systeemdiagram eID Stelsel—9

2 De rollen van het eID Stelsel—11

2.1 Authenticatiedienst—11

2.2 SectorID-dienst—12

2.3 Machtigingsdienst—12

2.4 eID-makelaar—13

2.5 Dienstaanbieder en Dienstbemiddelaar—13

2.6 Attributendienst—14

2.7 Maskeren van gegevens—15

3 Pseudoniemen—16

3.1 Rollen en Personages—16

3.2 Stappen in het tot stand komen van een PseudoID—16

3.3 Aanvragen van een Polymorfe PseudoID: de Stelselautoriteit—17

3.4 Van Polymorf PseudoID naar Versleuteld PseudoID—19

3.5 Van Versleuteld PseudoID naar PseudoID—19

3.6 Het gebruik van SectorID's—20

3.7 Gebruik van identiteiten in een Identiteitsverklaring—22

3.8 Niet-natuurlijke personen—22

4 Omvormen van pseudoniemen—23

4.1 Gebruik van PseudoID bij Machtigingsdienst—23

4.2 Fraudebestrijding: van PseudoID terug naar Stamsleutel—25

5 De cryptografie van het stelsel—26

5.1 Stamsleutel—26

5.2 Polymorfe PseudoID—26

6 De SectorID-dienst BSN—28

6.1 Koppelen BSN op aanvraag—28

Bijlagen—29

Bijlage A Overzicht eigenschappen—29

Bijlage B Overzicht eigenschappen vs. ontwerpeisen—32

Inleiding

Deze sectie beschrijft de algemene werking van het eID Stelsel. Het benoemt de componenten en beschrijft hun interacties. Verondersteld wordt dat de lezer bekend is met de globale beschrijving van het stelsel, zoals beschreven in Sectie 1: *Introductie op het eID Stelsel*.

In de gehele tekst zijn de belangrijkste eigenschappen van de ontwerpinvulling gemarkeerd met afwijkende achtergrond en een volgnummer van het type P*nn*. Deze "Properties" zullen worden opgenomen in een afzonderlijke kruistabel met de ontwerpeisen. Deze tabel geeft daarmee inzicht in hoe de ontwerpeisen worden gerealiseerd binnen het stelsel.

Begrippen die zijn terug te vinden in de begrippenlijst van het stelsel (Sectie 5) zijn gemarkeerd met KLEIN KAPITAAL.

Deze sectie is als volgt opgebouwd.

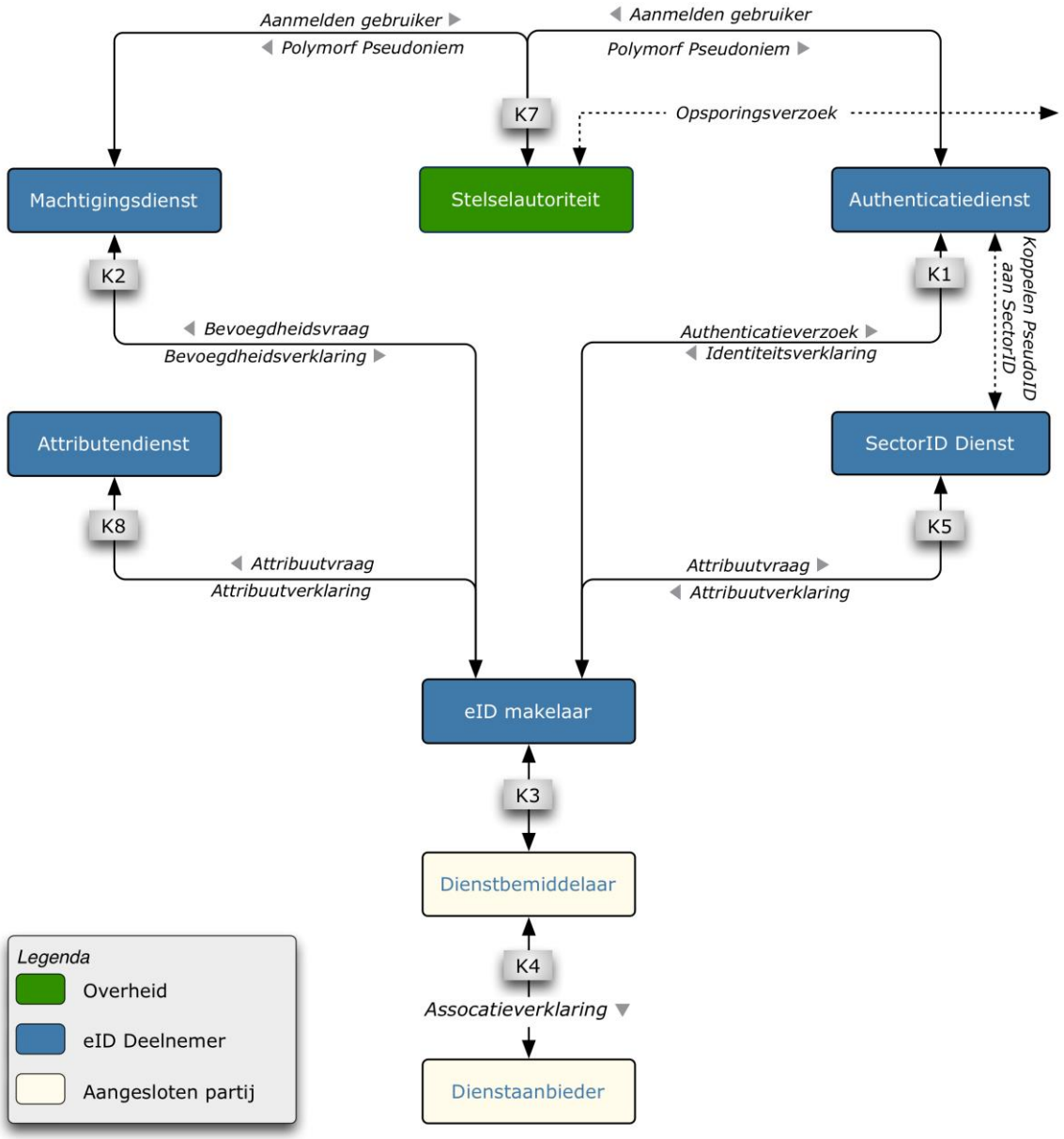
- In Hoofdstuk 1 wordt een systeemdiagram van het stelsel gepresenteerd, met daarin alle componenten van het stelsel en hun interacties.
- In Hoofdstuk 0 worden de belangrijkste eigenschappen van de componenten besproken.
- In Hoofdstuk 0 wordt een beschrijving gegeven hoe in het stelsel wordt omgegaan met pseudoniemen. Pseudoniemen vormen het fundament van het stelsel en inzicht in hun werking is essentieel voor een begrip van het stelsel als geheel. Hier wordt ook de STELSELAUTORITEIT geïntroduceerd, die een centrale rol speelt in het mechanisme van toekennen van pseudoniemen.
- Hoofdstuk 0 gaat verder in op het transformeren van pseudoniemen, noodzakelijk voor het functioneren van MACHTIGINGSDIENSTEN en voor het bestrijden van identiteitsfraude.
- Hoofdstuk 0 is gereserveerd voor een verdieping van de cryptografie van het stelsel. Dit hoofdstuk is niet essentieel voor het begrijpen van de voorgaande hoofdstukken, maar wel van belang voor bijvoorbeeld het opstellen van een privacy-impactanalyse.
- Hoofdstuk 0 beschrijft de SECTORID-DIENST BSN in wat meer detail over zowel de invulling als het gebruik. Deze SECTORID-DIENST is essentieel voor de bruikbaarheid van het stelsel voor de overheid.

1 Systeemdiagram eID Stelsel

Onderstaand diagram toont de verschillende componenten van het stelsel en de belangrijkste koppelvlakken.

De hier geschetste componenten zijn rollen. Er zijn EID-DEELNEMERS die gecertificeerd zijn en hun diensten aanbieden aan andere partijen of aan GEBRUIKERS. EID-DEELNEMERS kunnen zich specialiseren en bijvoorbeeld alleen een makelaarsdienst aanbieden, maar ze kunnen ook kiezen om meerdere rollen in te vullen en daarmee een compleet scala aan eID-diensten aan te bieden.

Deze keuzevrijheid geldt voor alle partijen. Zo kan een DIENSTAANBIEDER ervoor kiezen om zelf op te treden als DIENSTBEMIDDELAAR; voor veel kleinschalige diensten zal dit zelfs een voor de hand liggende invulling zijn. Een ander voorbeeld is een bedrijf dat zelf BEVOEGDHEIDSVERKLARINGEN afgeeft voor zijn



Figuur 1: Systeemdiagram eID Stelsel

eigen werknemers en dus optreedt als MACHTIGINGSDIENST.

P01 Het eID Stelsel is neutraal ten aanzien van partijen die een rol invullen; het formuleert alleen eisen waaraan een partij voor een bepaalde rol moet voldoen.

De uitzondering is de STELSELAUTORITEIT die een sleutelrol speelt in het beheer van de encryptie en het toezicht op het stelsel. De rol komt vooral naar voren bij het toetreden van partijen (EID-DEELNEMERS en GEBRUIKERS) tot het stelsel, en niet bij bijvoorbeeld het uitvoeren van authenticaties en bij het verstrekken van verklaringen.

P02 De rol van STELSELAUTORITEIT wordt ingevuld door de overheid.

Het stelsel is gebaseerd op het aanvragen en opstellen van verklaringen. Dit is een belangrijke eigenschap van het eID Stelsel die gestandaardiseerd gebruik in een grote verscheidenheid aan gebruikstoepassingen mogelijk maakt. Zo kan interactief (online) gebruik en system-to-system gebruik onder één noemer worden gebracht. Verklaringen worden ondertekend door de partij die ze opstelt.

P03 Een gecertificeerde EID-DEELNEMER kan verklaringen afgeven over derden (natuurlijke of niet-natuurlijke personen).

Er zijn beperkingen en voorwaarden aan verklaringen die deelnemers zelf opstellen, willen ze door andere deelnemers aan het stelsel kunnen worden geaccepteerd. Zo moet de verklaring onder meer voldoen aan de vormvereisten van het stelsel, en de verklaring moet worden ondertekend met een PKIoverheid-certificaat.

P04 Een persoon kan zelf een BEVOEGDHEIDSVERKLARING afgeven met een machtiging waarin hij als VERTEGENWOORDIGDE voorkomt.

P05 Een GEBRUIKER kan een IDENTITEITSVERKLARING of ATTRIBUUTVERKLARING afgeven over zichzelf.

2 De rollen van het eID Stelsel

In dit hoofdstuk worden de verschillende rollen binnen het eID Stelsel in meer detail besproken.

2.1 Authenticatiedienst

P06 Een Authenticatiedienst geeft Authenticatiemiddelen uit.

Om de Authenticatiemiddelen te kunnen uitgeven registreert de Authenticatiedienst zijn Gebruikers. Bij dit registratieproces wordt een koppeling gelegd tussen de identiteit van de Gebruiker in de werkelijkheid en de identiteit(en) van de Gebruiker zoals deze wordt opgenomen in het eID Stelsel. Dit wordt verder uitgewerkt in Hoofdstuk 0.

In theorie zouden de rollen van Middelenuitgever en Authenticatiedienst kunnen worden gescheiden. De ervaring heeft geleerd dat in de praktijk deze rollen altijd gecombineerd worden.

P07 Een Authenticatiedienst ontkoppelt Authenticatiemiddelen van Dienstaanbieders.

Een Middelenuitgever is verantwoordelijk voor de koppeling tussen het Authenticatiemiddel en de Authenticatiedienst. Deze koppeling blijft voor het stelsel verborgen en is daarmee onafhankelijk van de gekozen technologie van het Authenticatiemiddel. Elke Authenticatiedienst wordt via het uniforme koppelvlak K1 benaderd. Dit betekent dat nieuwe middelen kunnen worden toegevoegd en andere middelen kunnen worden ingetrokken zonder dat dit impact heeft op de Dienstbemiddelaars en Dienstaanbieders.

Het resultaat van een authenticatie is altijd een formele verklaring, ondertekend door de Authenticatiedienst.

P08 Een Authenticatiedienst levert een getekende Identiteitsverklaring. Een Identiteitsverklaring kan gericht zijn aan meerdere Ontvangende Partijen[1].

Een Identiteitsverklaring bevat een pseudoniem[2]; een pseudoniem is een unieke verwijzing naar de Gebruiker in het domein van de Ontvangende Partij. Dit voorkomt dat deze partijen gegevens over dezelfde Gebruiker uitwisselen en relateren op basis van informatie die door het eID Stelsel is geleverd.

P09 Een Authenticatiedienst realiseert inzage voor de Gebruiker in het gebruik dat van zijn of haar Authenticatiemiddelen is gemaakt.

Een Authenticatiedienst houdt een audit trail bij van het gebruik dat er van de dienst wordt gemaakt. Dat is een onderdeel van de beveiliging van het eID Stelsel: als een Authenticatiemiddel vermist wordt of anderszins gecompromitteerd wordt, dan kan aan de hand van de audit trail worden vastgesteld of er misbruik van een Authenticatiemiddel is gemaakt. Dit helpt om de impact van een dergelijk incident te beperken.

Het nadeel van een audit trail is dat het gegevens zijn die iets zeggen over de diensten die een Gebruiker heeft afgenomen. Dat maakt ze privacygevoelig. Daarom geldt aanvullend:

P10 Een audit trail mag door een Authenticatiedienst uitsluitend worden gebruikt voor het geven van inzicht aan de Gebruiker welk gebruik er van zijn middelen is gemaakt.

P11 Een Authenticatiedienst kan facultatief de mogelijkheid bieden aan een Gebruiker om af te zien van het bijhouden van een audit trail.

---

[1] Ontvangende Partij is de verzamelnaam voor iedere partij die informatie uit het stelsel ontvangt. Dit kunnen dus zowel partijen binnen het stelsel zijn (eID-makelaars, Machtigingsdienst, etc.) als partijen die zijn aangesloten op het stelsel (Dienstaanbieders en Dienstbemiddelaars).

[2] In dit document wordt pseudoniem gebruikt als een algemene term. Een concrete implementatie met specifieke kenmerken wordt aangeduid als pseudo-identiteit of kortweg PseudoID. Zie Hoofdstuk 3 voor een beschrijving van de stappen waarin een PseudoID tot stand komt.

Zie ook eigenschap P41.

P12 De keuze voor een AUTHENTICATIEDIENST en voor het te gebruiken AUTHENTICATIEMIDDEL berust bij de GEBRUIKER.

2.2 SECTORID-DIENST

Het eID Stelsel is ontworpen voor het gebruik van pseudoniemen, maar het biedt daarnaast de mogelijkheid om gebruik te maken van sectorale nummers, hier SECTORID's genoemd. Een sector wordt in dit verband gedefinieerd als een groep DIENSTAANBIEDERS die gegevens uitwisselen op basis van een gemeenschappelijk identificerend nummer (zoals bijvoorbeeld het BSN). Voor burgers is de hele overheid in deze betekenis dus één sector.

P13 Een SECTORID-DIENST wordt geraadpleegd door een EID-MAKELAAR op het moment dat een DIENSTAANBIEDER aangeeft dat voor het verlenen van een bepaalde dienst een SECTORID nodig is.

Dit wordt vastgelegd in de definitie van de dienst, in een DIENSTENCATALOGUS.

Het proces van het toevoegen van een SECTORID aan een PSEUDOID verloopt globaal als volgt.

1. De EID-MAKELAAR geeft in zijn authenticatieverzoek aan de dat de IDENTITEITSVERKLARING gebruikt moet kunnen worden bij de SECTORID-DIENST.
2. De AUTHENTICATIEDIENST verstrekt een IDENTITEITSVERKLARING met een PSEUDOID die specifiek is voor de SECTORID-DIENST.
3. De EID-MAKELAAR stuurt de ontvangen IDENTITEITSVERKLARING samen met het STELSELCERTIFICAAT van de beoogde ONTVANGENDE PARTIJ (DIENSTAANBIEDER of DIENSTBEMIDDELAAR) naar de SECTORID-DIENST.
4. De SECTORID-DIENST controleert het STELSELCERTIFICAAT van de ONTVANGENDE PARTIJ. Als deze inderdaad recht heeft op de verlangde SECTORID, dan zoekt hij deze op in een conversietabel aan de hand van de PSEUDOID.
5. De SECTORID-DIENST verpakt de SECTORID in een ATTRIBUUTVERKLARING, hecht deze (onlosmakelijk) aan de ontvangen IDENTITEITSVERKLARING en stuurt het geheel terug naar de EID-MAKELAAR.

2.3 MACHTIGINGSDIENST

P14 Een MACHTIGINGSDIENST registreert een bevoegdheid van een persoon (de GEMACHTIGDE) om een bepaalde dienst of groep van diensten af te nemen namens een ander persoon (de VERTEGENWOORDIGDE).

De betrokken personen kunnen zowel natuurlijke personen als niet-natuurlijke personen zijn. Machtigingen kunnen gecombineerd worden in een keten: A machtigt B, B machtigt C – zodat uiteindelijk C de handeling namens A uitvoert.

P15 Een MACHTIGINGSDIENST kan de identiteit van een VERTEGENWOORDIGDE vaststellen aan de hand van een IDENTITEITSVERKLARING van een AUTHENTICATIEDIENST of op basis van een eigen registratieproces. In het registratieproces van de machtiging wordt ook vastgesteld dat de VERTEGENWOORDIGDE de wil heeft de machtiging tot stand te laten komen.

Het eigen registratieproces verloopt op dezelfde manier als bij een AUTHENTICATIEDIENST (zie §3.3).

Het is essentieel dat de identiteit van de GEMACHTIGDE betrouwbaar wordt vastgesteld. Daarom moet een GEMACHTIGDE een machtiging expliciet accepteren.

P16 Een machtiging is pas geldig op het moment dat hij door de GEMACHTIGDE is geaccepteerd. De MACHTIGINGSDIENST stelt de identiteit van een GEMACHTIGDE vast op het moment van acceptatie.

Machtigingen worden opgeleverd in de vorm van een verklaring.

P17 Een MACHTIGINGSDIENST levert op aanvraag een BEVOEGDHEIDSVERKLARING, waarmee een HANDELENDE PERSOON ten overstaan van een DIENSTBEMIDDELAAR of DIENSTAANBIEDER kan aantonen dat hij gemachtigd is om een dienst af te nemen namens een VERTEGENWOORDIGDE.

Dit is de meest elementaire vorm van een machtiging, te vergelijken met een machtiging zoals bij een

notaris wordt vastgelegd. Er zijn complexere vormen van machtigingen denkbaar, waarbij de bevoegdheid afhankelijk is van de aard van de transactie (bijvoorbeeld of een bedrag dat met de transactie gemoeid is een bepaalde grens niet te boven gaat). Deze vormen worden niet expliciet beschreven in het eID Stelsel; het stelsel kan ze verwerken zolang het resultaat kan worden vastgelegd in een standaard BEVOEGDHEIDSVERKLARING.

P18 De keuze bij welke MACHTIGINGSDIENST een machtiging wordt geregistreerd berust bij degene die de machtiging aanvraagt.

Een machtiging wordt vastgelegd op basis van pseudoniemen. Als een DIENSTAANBIEDER een BEVOEGDHEIDSVERKLARING op basis van een BSN of een andere SECTORID nodig heeft, dan zorgt de EID-MAKELAAR ervoor dat de benodigde ATTRIBUUTVERKLARING worden opgehaald bij de SECTORID-DIENST en aan de BEVOEGDHEIDSVERKLARING wordt gehecht. Een MACHTIGINGSDIENST doet dit nooit zelf.

2.4 EID-MAKELAAR

De interactie tussen de verschillende rollen in het stelsel is complex. Daarom is in het stelsel een afzonderlijke rol gedefinieerd die als taak heeft om de interactie in goede banen te leiden en zo de DIENSTAANBIEDERS en DIENSTBEMIDDELAARS te "ontzorgen". Deze rol is de EID-MAKELAAR.

P19 De EID-MAKELAAR vraagt aan de GEBRUIKER van welke AUTHENTICATIEDIENST hij gebruik wil maken en (indien van toepassing) waar de machtigingen van de GEBRUIKER zijn geregistreerd. Op basis van de antwoorden routeert hij de GEBRUIKER door naar de juiste voorzieningen.

P20 De EID-MAKELAAR verricht zijn werkzaamheden op basis van een contract of bewerkersovereenkomst met de DIENSTBEMIDDELAAR of DIENSTAANBIEDER. De keuze voor een bepaalde EID-MAKELAAR berust bij de DIENSTBEMIDDELAAR of DIENSTAANBIEDER.

Het is de verantwoordelijkheid van de DIENSTBEMIDDELAAR of DIENSTAANBIEDER om te zorgen voor het invullen van de rol van een EID-MAKELAAR voor het ontsluiten van zijn diensten. Ze kunnen ervoor kiezen om een contract af te sluiten met twee of meer EID-MAKELAARS omwille van de continuïteit van de dienstverlening.

In beginsel heeft de EID-MAKELAAR daarmee het recht om dezelfde gegevens te verwerken als de DIENSTAANBIEDER in wiens opdracht hij werkt. Echter, een EID-MAKELAAR kan werken in opdracht van meerdere DIENSTAANBIEDERS. Dat zou betekenen dat bij de EID-MAKELAAR een ongewenste concentratie van gegevens ontstaat. Het gebruik van versleutelde pseudoniemen (§3.4) en het maskeren van persoonsgegevens (§2.7) voorkomt dat.

2.5 DIENSTAANBIEDER en DIENSTBEMIDDELAAR

In het model van het stelsel wordt onderscheid gemaakt tussen DIENSTAANBIEDERS en DIENSTBEMIDDELAARS. Meestal zal de DIENSTAANBIEDER ook het "zichtbare" deel van de dienst tonen: het is de plaats waar de authenticatie en machtigingen van de GEBRUIKER en alle andere gegevens die nodig zijn voor het afnemen van een dienst worden opgevraagd. Het komt echter ook voor dat een andere partij de GEBRUIKER ondersteunt in het afnemen van een digitale dienst. Deze dienstverlenende partij wordt de DIENSTBEMIDDELAAR genoemd en hij biedt dan het "zichtbare" deel van de dienst aan.

P21 Een DIENSTBEMIDDELAAR bundelt de verkregen verklaringen en de bijbehorende gegevens en ondertekent het geheel. Daarmee verklaart de DIENSTBEMIDDELAAR dat alle verklaringen en gegevens bij elkaar horen (ook associëren genoemd).

De gebundelde verklaringen worden via een webservice of soortgelijke techniek (koppelvlak K4) aangeboden aan de DIENSTAANBIEDER, die na controle van de gegevens besluit of de gevraagde transactie doorgang kan vinden (autorisatiebesluit) en vervolgens de gevraagde dienst ook werkelijk uitvoert.

Een DIENSTBEMIDDELAAR kan op de volgende twee manieren gepositioneerd worden binnen het stelsel.

1. Als onderdeel van een DIENSTAANBIEDER of als bewerker namens een DIENSTAANBIEDER. De DIENSTBEMIDDELAAR heeft dezelfde rechten als de DIENSTAANBIEDER en presenteert zich ook zo aan de GEBRUI-

KER. Dat werkt doordat de DIENSTBEMIDDELAAR de beschikking heeft over het STELSELCERTIFICAAT van de DIENSTAANBIEDER.

2. Als zelfstandige verschijning binnen het EID STELSEL. De DIENSTBEMIDDELAAR doorloopt een eigen toelatingstraject en krijgt op basis daarvan een eigen STELSELCERTIFICAAT.

P22 Een DIENSTBEMIDDELAAR kan optreden als bewerker namens een DIENSTAANBIEDER of op eigen titel worden geregistreerd als EID-DEELNEMER.

Naast DIENSTAANBIEDER en DIENSTBEMIDDELAAR wordt in het stelsel ook nog het begrip DIENSTEIGENAAR gebruikt.

P23 De DIENSTEIGENAAR is de partij die beslist over onder de indeling en naamgeving van de diensten en over alle beleidsmatige aspecten die gelden voor de betreffende dienst, zoals het vereiste BETROUWBAARHEIDSNIVEAU.

Voor diensten waarvoor in het stelsel maar één DIENSTAANBIEDER is, is de DIENSTAANBIEDER tevens DIENSTEIGENAAR. Als de dienst door meerdere partijen wordt aangeboden fungeert een overkoepelend orgaan als DIENSTEIGENAAR.

2.6 ATTRIBUTENDIENST

Het eID Stelsel is in beperkte mate geschikt voor het doorgeven van attributen (anders dan de eerder genoemde SECTORID). 'Beperkt' houdt in dat het uitsluitend gaat over gegevens die met instemming van de GEBRUIKER worden verstrekt.

Attributen kunnen worden onderscheiden in:

- comfortinformatie (informatie die kan worden toegevoegd aan een IDENTITEITSVERKLARING of een BEVOEGDHEIDSVERKLARING ter wille van de herkenbaarheid);
- actuele attributen uit een welomschreven bron. De architectuur van het eID Stelsel legt geen beperkingen op aan de attributen die kunnen worden verwerkt. De eerste implementatie beperkt zich evenwel tot de set gegevens die in het kader van STORK is vastgesteld (zie ref [3]).

P24 Comfortinformatie wordt in het stelsel vastgelegd op het moment van ontlening aan een authentieke bron (bijvoorbeeld WID, STORK-verklaring, Basisregistratie, Eigen Verklaring).

P25 Comfortinformatie wordt alleen op verzoek van de betrokken persoon geactualiseerd door opnieuw de authentieke bron te raadplegen.

P26 Bij alle attributen wordt vastgelegd aan welke bron ze zijn ontleend en op welke datum dat is gebeurd.

Het stelsel kent geen classificatie voor de betrouwbaarheid van attributen. Het begrip "welomschreven" laat enige ruimte voor interpretatievrijheid. Basisregistraties van de overheid voldoen in ieder geval aan dit criterium. Voor andere bronnen geldt als minimale voorwaarde dat de bron zelf onderzoek doet naar de juistheid en actualiteit van de gegevens en de resultaten daarvan ter beschikking stelt aan de partijen die gebruik zouden willen maken van de gegevens. Aanvullende criteria kunnen deel uitmaken van de toetredingseisen voor het eID Stelsel.

De gegevens over de ontlening worden mee verstrekt met de attributen zelf. Het is aan de ONTVANGENDE PARTIJ om op basis van de ter beschikking gestelde gegevens te bepalen of de attributen voldoende betrouwbaar en actueel zijn voor de gevraagde dienst.

Wat betreft toegang tot attributen geldt: een ONTVANGENDE PARTIJ krijgt niet meer gegevens dan waar hij recht op heeft. Dit is in lijn met het principe van dataminimalisatie.

P27 Het eID Stelsel dwingt af[3] dat een DIENSTAANBIEDER niet meer gegevens ontvangt dan waar hij recht op heeft. Dit recht wordt vastgesteld bij het aansluiten van de die DIENSTAANBIEDER op het stelsel.

P28 De gegevens waar de DIENSTAANBIEDER volgens het autorisatiebesluit recht op heeft worden vastgelegd in de aansluitovereenkomst van de DIENSTAANBIEDER.

P29 Attributen worden uitsluitend verstrekt op basis van instemming van de GEBRUIKER. Instemming kan expliciet of impliciet worden verleend.

Impliciete toestemming wordt verondersteld voor bijvoorbeeld het verstrekken van een PSEUDOID of een SECTORID; het heeft weinig zin om nog een keer om toestemming van de GEBRUIKER daarvoor te vragen. In alle andere gevallen moet de GEBRUIKER toestemming verlenen. Dat kan eenmalig, voorafgaande aan de eigenlijke verstrekking, of op het moment dat de gegevens feitelijk worden opgevraagd. Als gebruik wordt gemaakt van voorafgaande instemming, dan moet er ook een mogelijkheid zijn om de toestemming weer in te trekken.

Daarmee wordt meteen duidelijk dat het mechanisme van een ATTRIBUTENDIENST niet dient ter vervanging van bestaande vorm van gegevensuitwisseling binnen de overheid (die plaats vinden op wettelijke gronden en meestal zonder instemming van de GEBRUIKER), maar als aanvulling.

2.7 Maskeren van gegevens

In het eID Stelsel is de functionaliteit verdeeld over meerdere partijen. Dat betekent dat alle partijen gegevens hanteren die niet direct voor hen bedoeld zijn.

P30 Persoonsgegevens die tussen partijen worden getransporteerd worden zodanig versleuteld dat alleen de ONTVANGENDE PARTIJ deze weer kan ontsleutelen.

Dit staat los van het feit dat verbindingen op transportniveau beveiligd worden; dit vormt een tweede laag van beveiliging. Gegevenstransport wordt verder beschreven in Sectie 4.

Voor identiteiten wordt het mechanisme in de volgende paragrafen beschreven, maar het geldt voor alle persoonsgegevens die in het stelsel worden getransporteerd.

[3] De details van de manier waarop deze restrictie wordt afgedwongen zijn nog niet vastgesteld. Gedacht kan worden aan vastlegging in een STELSELCERTIFICAAT dat wordt uitgereikt door de STELSELAUTORITEIT/SLEUTELBEHEER, zoals dat ook bij de Duitse NPA gebeurt.

3 Pseudoniemen

Zoals gezegd is het eID Stelsel ontworpen voor het gebruik van pseudoniemen. Dit hoofdstuk beschrijft hoe pseudoniemen tot stand komen.

3.1 Rollen en Personages

Een persoon kan in verschillende contexten verschillende rollen spelen, bijvoorbeeld betaler van belastingen, klant van een webshop of vertegenwoordiger van een bedrijf. Als een persoon aangeeft van het eID Stelsel gebruik te willen gaan maken, wordt hem of haar gevraagd te kiezen hoe hij of zij daar als Gebruiker mee om wil gaan. Hij kan ervoor kiezen om voor iedere rol een apart Authenticatiemiddel te gebruiken, desgewenst bij verschillende Authenticatiediensten, of om in iedere context hetzelfde middel te gebruiken. Evenzo kan hij ervoor kiezen meerdere middelen aan te schaffen die door elkaar gebruikt kunnen worden. Anders gezegd, de Gebruiker bepaalt zelf hoe dik zijn sleutelbos moet zijn. Binnen het stelsel zullen we voor de manier waarop de Gebruiker zich manifesteert de term Personage[4] gebruiken.

P31 Een Gebruiker kan kiezen voor meerdere Personages of voor een enkele. Aan een bepaald Personage kan hij één of meerdere Authenticatiemiddelen koppelen.

Als een Gebruiker in een bepaalde rol een dienst af wil nemen, genereert het eID Stelsel een PseudoID als representatie van het Personage van de Gebruiker bij de Dienstaanbieder. Dat gebeurt in een aantal stappen die in de volgende paragrafen zullen worden omschreven.

P32 Een PseudoID binnen het stelsel is betekenisloos. Hij is uniek voor een bepaald Personage en voor een bepaalde Dienstaanbieder.

P33 De PseudoID is onafhankelijk van het gebruikte Authenticatiemiddel en van de gebruikte Authenticatiedienst.

Deze laatste eigenschap geeft de Gebruiker keuzevrijheid, enigszins vergelijkbaar met nummerbehoud van telefoons: een telefoonabonnee kan kiezen voor één of meerdere telefoons, en als hij van telefoonmaatschappij wisselt, kan hij kiezen voor een nieuw nummer of voor behoud van zijn oude nummer.

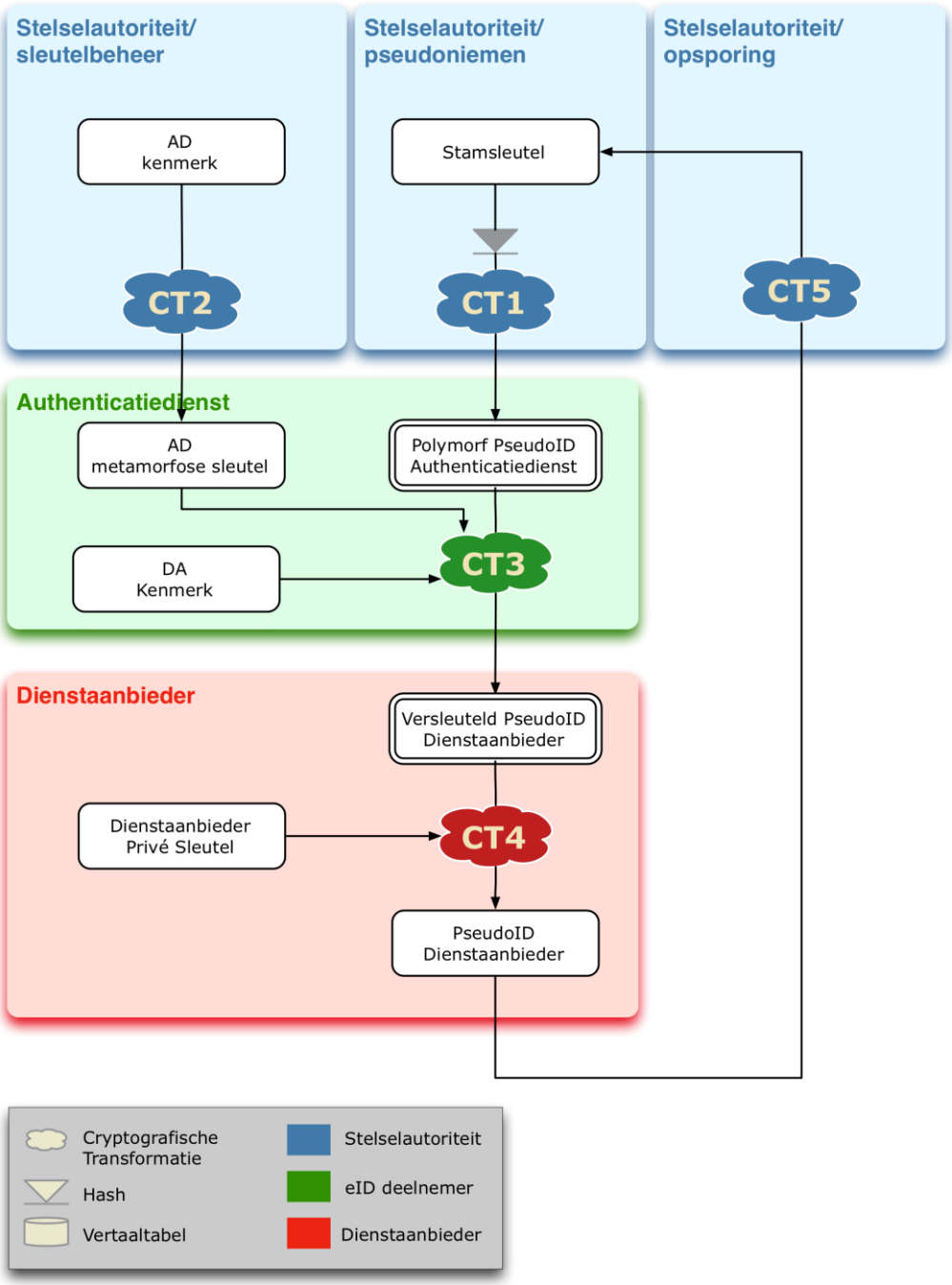
3.2 Stappen in het tot stand komen van een PseudoID

De stappen in het tot stand komen van een PseudoID zullen eerst worden toegelicht voor het eenvoudigste geval: de PseudoID die wordt gemaakt als een Gebruiker zelf inlogt bij een Dienstaanbieder (§§ 3.3 - 3.5). In §3.6 wordt toegelicht hoe het ontwerp werkt in combinatie met een SectorID-dienst. De meest uitgebreide variant treffen we aan bij Machtigingsdiensten (§4.1).

De eerste stap wordt gezet op het moment dat de Gebruiker zich meldt als (nieuwe) klant van een Authenticatiedienst. De Authenticatiedienst vraagt voor de nieuwe klant een zogenaamde Polymorfe PseudoID aan. Deze Polymorfe PseudoID is de kern van de encryptie van het stelsel. De Polymorfe PseudoID is voor iedere Authenticatiedienst verschillend; sterker nog, als een Authenticatiedienst voor dezelfde persoon de aanvraag opnieuw indient, zal het resultaat een andere Polymorfe PseudoID zijn. Toch leveren al deze verschijningsvormen na twee transformaties (de eerste bij de Authenticatiedienst, de tweede bij de Dienstaanbieder) steeds dezelfde PseudoID op. Deze PseudoID voldoet aan de eisen die in §3.1 zijn gesteld.

De wijze waarop de Polymorfe PseudoID tot stand komt en vervolgens de transformatie naar een PseudoID specifiek voor de Ontvangende Partij maakt, wordt in de volgende paragrafen beschreven.

[4] Er is nog niet vastgesteld welke regels precies gelden voor Personages, en met name hoe een Gebruiker Personages beheert. Dit zal onderwerp van onderzoek zijn in de volgende fase van de realisatie van het eID Stelsel.



Figuur 2: Genereren van PSEUDOID'S

3.3 Aanvragen van een POLYMORFE PSEUDOID: de STELSELAUTORITEIT

In deze paragraaf wordt de aanvraag van een POLYMORFE PSEUDOID voor een natuurlijke persoon beschreven. Zie voor rechtspersonen en samenwerkingsverbanden §3.8.

Een POLYMORFE PSEUDOID wordt berekend en uitgereikt door een vertrouwde centrale partij binnen het stelsel: de STELSELAUTORITEIT/PSEUDONIEMEN. De POLYMORFE PSEUDOID wordt aangevraagd door een AUTHENTICATIEDIENST op het moment dat een GEBRUIKER zich daar registreert.

P34 De POLYMORFE PSEUDOID wordt uitgereikt door de STELSELAUTORITEIT aan een AUTHENTICATIE-DIENST.

De aanvraag is gebaseerd op een beperkte set persoonsgegevens, die opgenomen zijn in een WID

(een document als bedoeld in lid 1 van de Wet op de Identificatieplicht of een daarmee gelijk te stellen buitenlands identiteitsdocument). De te gebruiken gegevens zijn geslachtsnaam, eerste voornaam, overige voorletters, geboortedatum en geboorteplaats; als één van de gegevens niet bekend is wordt een nader te bepalen standaardwaarde gebruikt. Samen vormen deze gegevens de STAMSLEUTEL. Door hiervoor niet het BSN te gebruiken worden problemen vermeden met identiteitsdocumenten waar geen BSN opstaat en met de wettelijke restricties die gelden voor het gebruik van het BSN.

P35 Een POLYMORFE PSEUDOID wordt afgeleid van persoonskenmerken, opgenomen in een identiteitsdocument. Daarbij wordt geen gebruik gemaakt van persoonsnummers.

Een sleutel die niet is gebaseerd op een persoonsnummer is niet gegarandeerd uniek. Voordat de STELSELAUTORITEIT een aanvraag voor een POLYMORFE PSEUDOID honoreert wordt gecontroleerd op uniciteit door de aangeleverde gegevens te controleren tegen de beheervoorziening BSN. Dit is de voorziening die ook wordt geraadpleegd bij eerste inschrijving in de GBA om dubbele inschrijvingen te voorkomen. Ook wordt gecontroleerd of een persoon al eerder is opgenomen in de administratie van de STELSELAUTORITEIT om te voorkomen dat eenzelfde persoon onder twee verschillende STAMSLEUTELS wordt ingeschreven, bijvoorbeeld door een klein verschil in de fonetische schrijfwijze van een buitenlandse naam. Hiervoor wordt gebruik gemaakt van dezelfde zoekalgoritmes die voor de beheervoorziening BSN zijn ontwikkeld.

P36 De STELSELAUTORITEIT controleert de STAMSLEUTEL bij de beheervoorziening BSN en in een eigen administratie. Daarmee voorkomt de STELSELAUTORITEIT dubbele inschrijvingen en signaleert hij niet-unieke STAMSLEUTELS.

Als de controles een eenduidig resultaat opleveren registreert de STELSELAUTORITEIT de persoonskenmerken. Het BSN wordt genegeerd.

Als de controle signaleert dat de STAMSLEUTEL niet uniek is, moeten aanvullende gegevens worden gebruikt. Een private AUTHENTICATIEDIENST beschikt daartoe niet over de nodige controlemogelijkheden. In de (zeldzame) gevallen dat deze situatie zich voordoet zal de GEBRUIKER moeten worden doorverwezen naar de gemeenteloketten die wel geëquipeerd zijn voor deze functie. Ook voor deze situatie biedt de beheervoorziening BSN in de praktijk beproefde algoritmen die uiteindelijk tot een uniek resultaat leiden. Resultaat zal zijn dat de STAMSLEUTEL wordt uitgebreid met een gegeven dat de STAMSLEUTEL alsnog uniek maakt.

P37 Als een STAMSLEUTEL niet uniek is worden aanvullende gegevens gebruikt om tot een unieke sleutel te komen. Dit proces wordt uitgevoerd door de gemeentelijke balies.

De STAMSLEUTEL wordt door de STELSELAUTORITEIT gebruikt om de POLYMORFE PSEUDOID af te leiden; dit is in Figuur 2 aangegeven als CT1 (Cryptografische Transformatie 1). De POLYMORFE PSEUDOID wordt vervolgens geleverd aan de AUTHENTICATIEDIENST.

De POLYMORFE PSEUDOID heeft de volgende eigenschappen:

P38 EEN POLYMORF PSEUDOID is randomiseerbaar (aangegeven met een dubbele lijn in Figuur 2). Dat houdt in dat er extra gegevens aan de POLYMORFE PSEUDOID kunnen worden toegevoegd zonder dat dit invloed heeft op de PSEUDOID'S die van het POLYMORFE PSEUDOID worden afgeleid.

Dit randomiseren kan op meerdere plaatsen worden toegepast, onder andere bij de STELSELAUTORITEIT zelf. Dit betekent dat als er meerdere malen een POLYMORFE PSEUDOID voor een GEBRUIKER wordt aangevraagd, het resultaat er steeds anders uit zal zien.

P39 Een POLYMORFE PSEUDOID is specifiek voor de AUTHENTICATIEDIENST die de POLYMORFE PSEUDOID heeft aangevraagd, zonder dat dit invloed heeft op de PSEUDOID'S die van de POLYMORFE PSEUDOID worden afgeleid.

Hier wordt P33 gerealiseerd: als twee AUTHENTICATIEDIENSTEN hun aanvraag voor een POLYMORFE PSEUDOID baseren op dezelfde STAMSLEUTEL, zullen ze bij één en dezelfde DIENSTAANBIEDER dezelfde PSEUDOID opleveren.

3.4 Van POLYMORF PSEUDOID naar VERSLEUTELD PSEUDOID

De AUTHENTICATIEDIENST slaat de ontvangen POLYMORFE PSEUDOID op. Als de AUTHENTICATIEDIENST gebruik maakt van een "secure device"[5] (bijvoorbeeld een geavanceerde smartcard) als AUTHENTICATIEMIDDEL, dan kan de POLYMORFE PSEUDOID op het middel zelf worden opgeslagen. AUTHENTICATIEDIENSTEN die gebruik maken van middelen die dit niet ondersteunen (zoals gebruikersnaam/wachtwoord of een eenvoudigere vorm van smartcard) slaan de POLYMORFE PSEUDOID's op in de eigen administratie.

P40 Een POLYMORFE PSEUDOID kan worden opgeslagen op een extern "secure device" of in de administratie van de AUTHENTICATIEDIENST.

Hiermee wordt de oplossing bruikbaar voor een breed scala aan AUTHENTICATIEMIDDELEN.

Een POLYMORFE PSEUDOID die is opgeslagen op een "secure device" kan bij uitlezen door het middel zelf worden gerandomiseerd. Dat betekent dat de AUTHENTICATIEDIENST de POLYMORFE PSEUDOID niet meer zal herkennen en dus de authenticatie kan uitvoeren zonder te weten over welke van zijn klanten het gaat. Dit biedt een extra niveau van privacybescherming. Het gaat evenwel ten koste van de volledigheid van de informatie in de audit trail: het is niet meer mogelijk om precies vast te leggen welk gebruik er van een kaart wordt gemaakt. De keuze is hier aan de GEBRUIKER.

P41 De informatie in een audit trail is voor een AUTHENTICATIEDIENST afhankelijk van de gebruikte techniek.

Als de GEBRUIKER zich door tussenkomst van de AUTHENTICATIEDIENST ergens wil authentiseren, berekent de AUTHENTICATIEDIENST uit de POLYMORFE PSEUDOID een VERSLEUTELDE PSEUDOID.

P42 Een AUTHENTICATIEDIENST ontvangt van de STELSELAUTORITEIT/SLEUTELBEHEER een geheime sleutel ten behoeve van het berekenen van VERSLEUTELDE PSEUDOID's.

Deze sleutel (in Figuur 2 aangeduid als METAMORFOSESLEUTEL, omdat hij de verschijningsvorm van de POLYMORFE PSEUDOID bepaalt) wordt op een zeer specifiek wijze (aangeduid als CT2) afgeleid van de identiteit van de AUTHENTICATIEDIENST.

De VERSLEUTELDE PSEUDOID wordt berekend op basis van de POLYMORFE PSEUDOID van de GEBRUIKER, het PERSONAGE dat de GEBRUIKER heeft gekozen[6], en de identiteit van de ONTVANGENDE PARTIJ. Deze omzetting is aangeduid als CT3.

Een VERSLEUTELDE PSEUDOID heeft de volgende eigenschappen.

P43 Een VERSLEUTELDE PSEUDOID is randomiseerbaar.

P44 Een VERSLEUTELDE PSEUDOID is alleen leesbaar voor de ONTVANGENDE PARTIJ.

3.5 Van VERSLEUTELD PSEUDOID naar PSEUDOID

De laatste stap in het aanmaken van de PSEUDOID wordt uitgevoerd door de ONTVANGENDE PARTIJ. Deze heeft hiertoe van de STELSELAUTORITEIT/SLEUTELBEHEER een eigen geheime sleutel ontvangen. Door deze toe te passen op het ontvangen VERSLEUTELD PSEUDOID berekent hij het feitelijk te gebruiken pseudoniem (PSEUDOID) dat het resultaat is van de authenticatie.

P45 Een PSEUDOID is persistent, uniek voor de ONTVANGENDE PARTIJ en alleen afhankelijk van de STAMSLEUTEL van de GEBRUIKER en het gekozen PERSONAGE.

Anders gezegd, het geheel van de transformaties CT1, CT2, CT3 en CT4 is zodanig dat het eindresultaat onafhankelijk is van de AUTHENTICATIEDIENST die de authenticatie uitvoert en van het

[5] Het eID Stelsel zal nader definiëren aan welke voorwaarden een "secure device" moet voldoen.

[6] Er is nog niet vastgesteld hoe de GEBRUIKER deze keuze kenbaar maakt. Een mogelijke invulling is dat het PERSONAGE wordt gekoppeld aan het middel; dat zou inhouden dat de GEBRUIKER voor ieder PERSONAGE een apart middel moet aanschaffen. Implementaties die koppelen van meerdere PERSONAGES aan één middel mogelijk maken zijn ook denkbaar. Intern in het stelsel wordt een PERSONAGE gepresenteerd door een getal met een nader te bepalen bereik.

toevoegen van random informatie aan de POLYMORFE PSEUDOID en de VERSLEUTELDE PSEUDOID.

Deze eigenschap is cruciaal; hij zorgt ervoor dat de oplossing tegelijkertijd voldoet aan alle eisen van keuzevrijheid van de GEBRUIKER, privacybescherming en onafhankelijkheid van toegepaste middelen.

3.6 Het gebruik van SECTORID's

In Hoofdstuk 0 is al aangegeven dat het eID Stelsel ook de mogelijkheid biedt voor DIENSTAANBIEDERS om gebruik te maken van SECTORID's. Het bekendste voorbeeld van een SECTORID is het BSN.

Om dit gebruik mogelijk te maken is het noodzakelijk dat er een verband word gelegd tussen PERSONAGE en een SECTORID. Dit is de taak van een SECTORID-DIENST. Daarvoor wordt niet rechtstreeks gebruik gemaakt van de POLYMORFE PSEUDOID; die is daarvoor door zijn steeds wisselende verschijningsvorm niet geschikt. In plaats daarvan wordt er gebruik gemaakt van een PSEUDOID. In feite gedraagt een SECTORID-DIENST zich op dit punt als een gewone ATTRIBUTENDIENST. Deze oplossing zorgt ervoor dat een SECTORID gebruikt kan worden in combinatie met een willekeurig AUTHENTICATIEMIDDEL van een willekeurige AUTHENTICATIEDIENST.

Het is niet wenselijk en niet nodig dat een SECTORID aan ieder PERSONAGE van een GEBRUIKER wordt gekoppeld: als een burger besluit om een bepaald PERSONAGE nooit te gebruiken voor bepaalde sector, dan kan deze link achterwege blijven. Dit geldt dus ook voor het BSN.

P46 Een SECTORID wordt uitsluitend op verzoek van de GEBRUIKER en via een expliciete koppelprocedure gekoppeld aan een PERSONAGE.

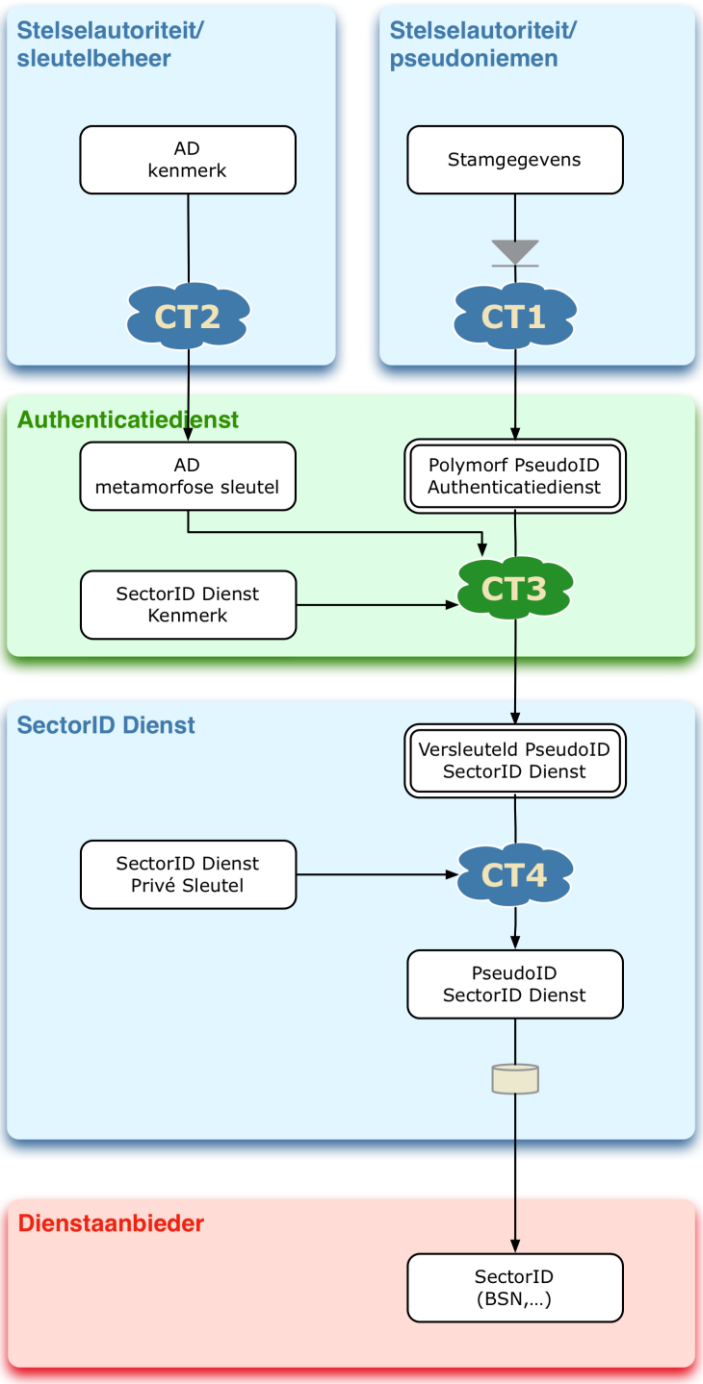
De procedure voor het maken van de koppeling hoeft niet voor alle SECTORID's hetzelfde te zijn. De procedure kan deel uitmaken van de uitgifteprocedure voor nieuwe middelen. De eisen die aan de procedure worden gesteld kunnen daarom verschillend zijn, al naar gelang het door de sector gewenste BETROUWBAARHEIDSNIVEAU (STORK-level).

P47 Het in stand houden van een SECTORID-DIENST is de verantwoordelijkheid van de sector zelf.

Een belangrijk voorbeeld van een SECTORID-DIENST is de SECTORID-DIENST BSN; deze wordt beschreven in Hoofdstuk 0.

Stel nu dat een GEBRUIKER een dienst wil afnemen bij een DIENSTAANBIEDER die daarvoor een SECTORID nodig heeft. Dit feit wordt vastgelegd in de DIENSTENCATALOGUS. Het authenticatieproces verloopt in deze situatie als volgt (zie Figuur 3).

1. De AUTHENTICATIEDIENST gebruikt in CT3 niet de identiteit van de DIENSTAANBIEDER, maar de identiteit van de SECTORID-DIENST.
2. Het resultaat is een VERSLEUTELDE PSEUDOID, behorend bij het gebruikte PERSONAGE. Deze VERSLEUTELDE PSEUDOID kan alleen door de SECTORID-DIENST worden gelezen.



Figuur 3: Pseudoniemen en sectorale nummers

3. De SECTORID-DIENST past op deze VERSLEUTELDE PSEUDOID zijn eigen geheime sleutel toe en verkrijgt zo de PSEUDOID waaronder de GEBRUIKER bij hem bekend is.
4. De SECTORID-DIENST zoekt de bijbehorende SECTORID op. Deze SECTORID wordt in een ATTRIBUUTVERKLARING opgenomen. De oorspronkelijke IDENTITEITSVERKLARING wordt aan de ATTRIBUUTVERKLARING gehecht in een IDENTITEITSKETEN. Het geheel wordt vervolgens teruggegeven aan de aanvrager (de EID-MAKELAAR – zie §2.4).

Evenals een IDENTITEITSVERKLARING kan een ATTRIBUUTVERKLARING meerdere geadresseerden hebben (zie eigenschap P08).

3.7 Gebruik van identiteiten in een IDENTITEITSVERKLARING

Iedere IDENTITEITSVERKLARING bevat tenminste één VERSLEUTELDE PSEUDOID. Als hij geadresseerd is aan meerdere ONTVANGENDE PARTIJEN (zie eigenschap P08), dan bevat hij even zoveel VERSLEUTELDE PSEUDOID's. Afhankelijk van de context waarin de IDENTITEITSVERKLARING gebruikt moet worden kan hij als zelfstandige verklaring voorkomen, kan hij gehecht zijn aan een ATTRIBUUTVERKLARING (zie §3.6) of aan een BEVOEGDHEIDSVERKLARING.

Zowel attributen als identiteiten zijn kenmerken van een persoon. Een identiteit legt een eenduidig verband tussen een persoon en een verzameling gegevens over meerdere personen, zoals een klantenbestand of een registratie van beroepsbeoefenaren. Daarmee geeft de identiteit het door de HANDELENDE PERSOON beoogde gebruik van de keten van verklaringen aan. Neem als voorbeeld een advocaat die zowel een BSN als een advocatennummer (BAR-nummer) heeft. Hij zal zijn BSN gebruiken als hij als burger zaken doet met de overheid en zijn advocatennummer wanneer hij als advocaat handelt. Daarom geldt de volgende regel.

P48 Een IDENTITEITSKETEN kan per ONTVANGENDE PARTIJ slechts één identiteit (PSEUDOID of SECTORID) bevatten.

Aan een ATTRIBUUTVERKLARING is altijd een IDENTITEITSVERKLARING gehecht. In de meeste gevallen zal dat een IDENTITEITSVERKLARING zijn met twee geadresseerden: de ATTRIBUTENDIENST zelf en de ONTVANGENDE PARTIJ van de ATTRIBUUTVERKLARING. Er zijn echter ook situaties waarin de ATTRIBUTENDIENST de enige geadresseerde is. Immers, PSEUDOID's zoals hier gebruikt zijn persistent (i.e. bij ieder gebruik hetzelfde). Een persistent gegeven, hoe betekenisloos ook, stelt de ontvanger in staat om een historie op te bouwen van het gebruik van de HANDELENDE PERSOON van het stelsel. Dat is niet nodig in de situatie dat bijvoorbeeld alleen een specifiek eigenschap van de HANDELENDE PERSOON (bijvoorbeeld 'ouder dan 18?') vereist wordt. In dat geval bevat de IDENTITEITSVERKLARING alleen de VERSLEUTELDE PSEUDOID voor de ATTRIBUTENDIENST. Dat is voor de ONTVANGENDE PARTIJ verder niet leesbaar. Hij kan uit de ontvangen keten afleiden dat de identiteit deugdelijk is vastgesteld, dat de persoon in kwestie inderdaad ouder dan 18, maar niet over wie het gaat. Daarmee bevat de keten precies voldoende informatie voor de ONTVANGENDE PARTIJ.

3.8 Niet-natuurlijke personen

In het voorgaande lag de nadruk op natuurlijke personen. Bij niet-natuurlijke personen (bedrijven, stichtingen, overheden) klemmen de vraagstukken van privacy minder, maar ook daar kan afscherming van gegevens van belang zijn – bijvoorbeeld voor het beschermen van concurrentiegevoelige informatie.

P49 Uitgangspunt is dat niet-natuurlijke personen in het stelsel op dezelfde manier worden behandeld als natuurlijke personen.

Voor niet-natuurlijke personen wordt er ook gewerkt met een STAMSLEUTEL. De STAMSLEUTEL wordt samengesteld uit een indicatie van het register waar de gegevens van de niet-natuurlijke persoon zijn vastgelegd, en een uniek kenmerk van de persoon. Dat laatste kan van register tot register verschillen.

[aan te vullen in de volgende versie].

De STAMSLEUTEL wordt vervolgens gebruikt op de manier als eerder beschreven voor natuurlijke personen.

4 Omvormen van pseudoniemen

Er is een aantal situaties waarin een specifiek pseudoniem moet worden omgevormd in een ander pseudoniem om bruikbaar te zijn. Deze situaties worden in dit hoofdstuk besproken.

4.1 Gebruik van PseudoID bij Machtigingsdienst

Een Gebruiker kan bij een Machtigingsdienst meerdere machtigingen voor verschillende Dienstaanbieders vastleggen. De eis van transparantie houdt dan het volgende in.

P50 Een Gebruiker moet kunnen inloggen bij een Machtigingsdienst en al zijn machtigingen zien en beheren (zowel de machtigingen waarin hij als Vertegenwoordigde voorkomt als die waarin hij als Gemachtigde voorkomt).

In deze situatie ligt het voor de hand om de Machtigingsdienst te beschouwen als een Dienstaanbieder die de dienst "Beheer Machtigingen" verleent aan de Gebruiker. De Gebruiker wordt geauthentiseerd aan de hand van een PseudoID die specifiek is voor de Machtigingsdienst. Op het moment dat op basis van de geregistreerde machtiging een Bevoegdheidsverklaring moet worden gemaakt, dient deze persoon echter te worden aangeduid op de manier waarop de Ontvangende Partij deze persoon kent, dus met de PseudoID voor de Ontvangende Partij. Het mag voor de Ontvangende Partij immers geen verschil maken of de Vertegenwoordigde zélf inlogt of dat iemand anders dat namens hem of haar doet op basis van een machtiging. Dat kan binnen de cryptografie van het stelsel alleen als de Bevoegdheidsverklaring de Versleutelde PseudoID van de Vertegenwoordigde en de Gemachtigde bevat.

P51 Een BEVOEGDHEIDSVERKLARING bevat de DIENSTAANBIEDER-specifieke VERSLEUTELDE PSEUDOID van de GEMACHTIGDE en de VERTEGENWOORDIGDE.

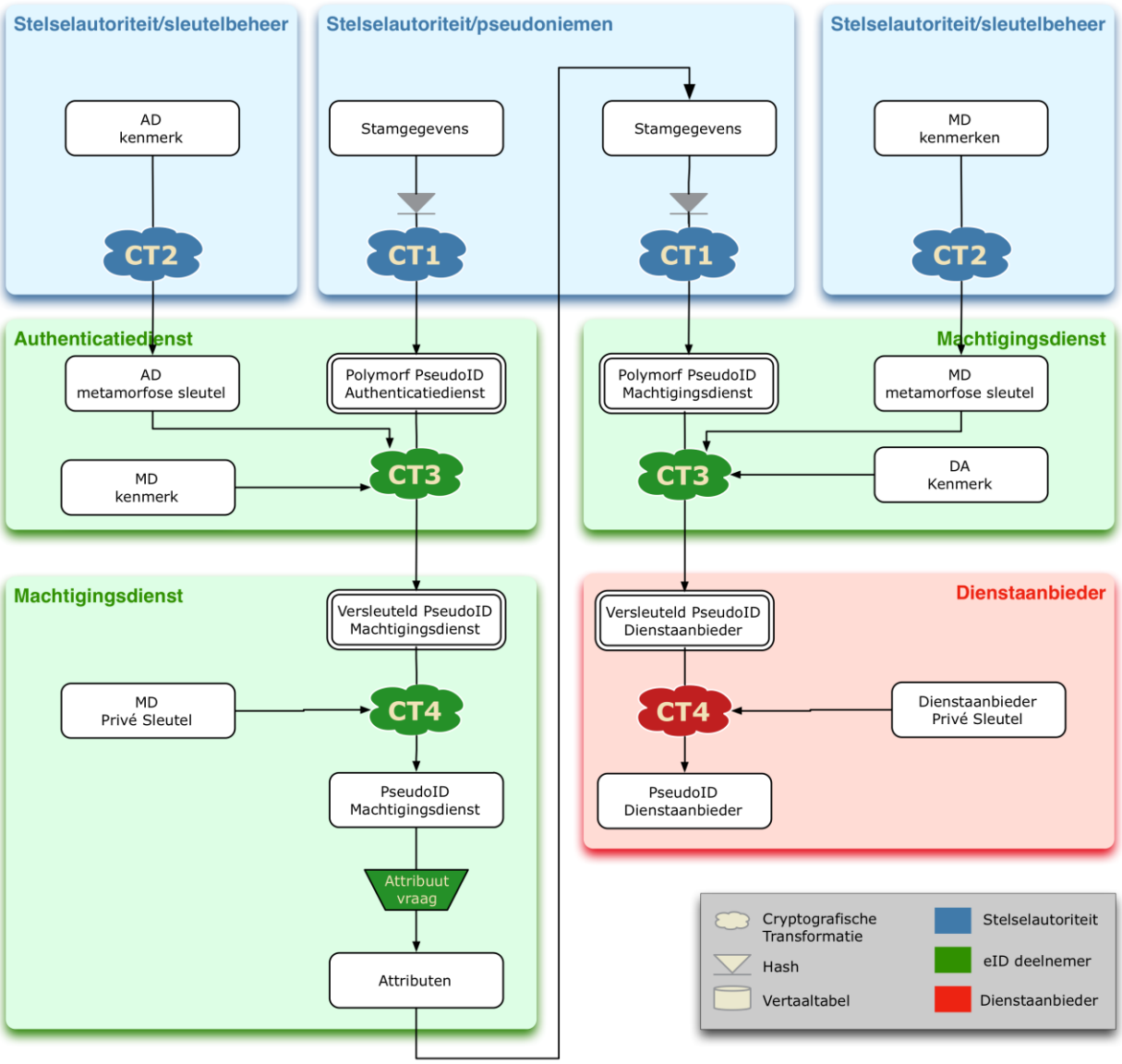
Voor de laatste GEMACHTIGDE in een keten kan dat worden gerealiseerd door de AUTHENTICATIEDIENST.

P52 Een AUTHENTICATIEDIENST levert op verzoek zowel een VERSLEUTELDE PSEUDOID voor de DIENSTAANBIEDER als voor de MACHTIGINGSDIENST.

Voor de overige GEMACHTIGDEN in een keten en voor de VERTEGENWOORDIGDE dient de MACHTIGINGSDIENST te kunnen beschikken over POLYMORFE PSEUDOID's van de betrokken personen. Deze worden door de MACHTIGINGSDIENST aangevraagd bij de STELSELAUTORITEIT/PSEUDONIEMEN als onderdeel van het registratieproces van een machtiging – zie Figuur 4. Dit hoeft alleen de eerste keer dat de GEBRUIKER een machtiging registreert; de MACHTIGINGSDIENST zal de ontvangen POLYMORFE PSEUDOID opslaan en bij een volgende gelegenheid hergebruiken.

Er zijn meerdere varianten van het aanvraag proces mogelijk, maar als onderdeel van het proces dienen de hier beschreven stappen zowel voor de VERTEGENWOORDIGDE als voor de GEMACHTIGDE te worden doorlopen.

Het proces begint ermee dat bijvoorbeeld de VERTEGENWOORDIGDE inlogt bij de MACHTIGINGSDIENST om een



Figuur 4: Pseudoniemen bij een MACHTIGINGSDIENST

aanvraag voor een machtiging in te dienen. In deze context is de MACHTIGINGSDIENST de DIENSTAANBIEDER, dus de AUTHENTICATIEDIENST genereert een VERSLEUTELDE PSEUDOID (CT3) die alleen gelezen kan worden door de MACHTIGINGSDIENST. Deze ontcijfert de VERSLEUTELDE PSEUDOID en verkrijgt op die manier de PSEUDOID van de VERTEGENWOORDIGDE voor zijn eigen administratie. Als onderdeel van de authenticatie vraagt de MACHTIGINGSDIENST om de attributen waaruit de STAMSLEUTEL van de GEBRUIKER is opgebouwd. Deze worden als aanvullende attributen meegeleverd in de IDENTITEITSVERKLARING. Uit hoofde van zijn rol zal de MACHTIGINGSDIENST daarvoor bij toetreding tot het stelsel autorisatie voor hebben gekregen.

De MACHTIGINGSDIENST gebruikt vervolgens deze gegevens om een eigen aanvraag voor een POLYMORFE PSEUDOID in te dienen bij de STELSELAUTORITEIT/PSEUDONIEMEN. Omdat deze gegevens al een keer eerder zijn gebruikt om een POLYMORFE PSEUDOID aan te vragen, zijn daarbij geen complicaties zoals een niet-unieke STAMSLEUTEL te verwachten. De STELSELAUTORITEIT/PSEUDONIEMEN berekent een nieuwe POLYMORFE PSEUDOID ten behoeve van de MACHTIGINGSDIENST die als onderdeel van de machtigingstriple[7] wordt opgeslagen.

P53 Een MACHTIGINGSDIENST vraagt voor het genereren van PSEUDOID's een eigen POLYMORFE PSEUDOID aan bij de STELSELAUTORITEIT/PSEUDONIEMEN.

Op het moment dat de POLYMORFE PSEUDOID is ontvangen kan de MACHTIGINGSDIENST de voor het samenstellen van de STAMSLEUTEL verkregen attributen verwijderen, voor zover ze niet als comfortinformatie deel uitmaken van de machtiging. In de praktijk zal dit betekenen dat de geboorteplaats en eventuele aanvullende gegevens geschrapt kunnen worden.

De MACHTIGINGSDIENST beschikt net als een AUTHENTICATIEDIENST over een METAMORFOSESLEUTEL. Als de machtiging wordt opgevraagd, gebruikt de MACHTIGINGSDIENST deze om uit de POLYMORFE PSEUDOID een VERSLEUTELDE PSEUDOID ten behoeve van de DIENSTAANBIEDER te genereren. De DIENSTAANBIEDER haalt bij binnenkomst van de BEVOEGDHEIDSVERKLARING zijn private sleutel over de VERSLEUTELDE PSEUDOID en verkrijgt zo de PSEUDOID van de GEBRUIKER. Op basis van de algemene eigenschappen van de cryptografie (eigenschap P45) weten we dan dat dit dezelfde PSEUDOID is als de AUTHENTICATIEDIENST voor de VERTEGENWOORDIGDE genereert wanneer de VERTEGENWOORDIGDE zelf zou inloggen bij de DIENSTAANBIEDER.

Wanneer de machtiging tot stand komt via een balieproces verloopt het feitelijk op dezelfde wijze, alleen wordt de STAMSLEUTEL van de VERTEGENWOORDIGDE dan afgeleid van de gegevens op het WID. Deze vormt dan de basis voor de aanvraag van de POLYMORFE PSEUDOID.

P54 De gegevens voor het aanvragen van een POLYMORFE PSEUDOID verkrijgt de MACHTIGINGSDIENST uit een IDENTITEITSVERKLARING of uit een eigen registratieproces.

4.2 Fraudebestrijding: van PSEUDOID terug naar STAMSLEUTEL

Er is een situatie waarin de bescherming die een PSEUDOID biedt moet kunnen worden onderbroken, namelijk wanneer ondersteuning moet worden geboden bij het opsporen van fraude. Dit kan identiteitsfraude zijn, maar ook op andere juridische gronden kan opsporing van een GEBRUIKER noodzakelijk zijn.

Als de ONTVANGENDE PARTIJ een vermoeden heeft van identiteitsfraude, dan kan hij via een daartoe bevoegde instantie een rechtshulpverzoek doen[8]. Op basis dit verzoek daarvan kan de speciale afdeling STELSELAUTORITEIT/OPSPORING een transformatie uitvoeren waarmee de PSEUDOID wordt herleid tot de achterliggende STAMSLEUTEL. In Figuur 2 (blz. 17) is dit aangeduid als CT5. Voor deze transformatie is uitvoering van een brute-force operatie op de administratie van de STELSELAUTORITEIT/PSEUDONIEMEN nodig, wat een garantie biedt dat deze weg alleen bij uitzondering gevolgd zal worden.

P55 De STELSELAUTORITEIT ondersteunt ter bestrijding van fraude de mogelijkheid om een PSEUDOID terug te herleiden tot de STAMSLEUTEL waarop de PSEUDOID was gebaseerd.

---

[7] Met de machtigingstriple worden de VERTEGENWOORDIGDE, de GEMACHTIGDE en de betrokken dienst bedoeld.

[8] Nader onderzoek moet invulling geven aan de voorwaarden waaraan een dergelijk verzoek moet voldoen.

5 De cryptografie van het stelsel

In dit hoofdstuk wordt nader ingegaan op de cryptografische principes die in de voorgaande hoofdstukken zijn gebruikt. De volledige beschrijving van de cryptografische technieken wordt in een afzonderlijk document vastgelegd.

5.1 STAMSLEUTEL

De gegevens waaruit de STAMSLEUTEL (zie §3.2) wordt opgebouwd zijn: geslachtsnaam, eerste voornaam, overige voorletters, geboortedatum en geboorteplaats.

Om problemen met spelling te voorkomen wordt gebruik gemaakt van een vereenvoudigde schrijfwijze van achternaam en voornaam, zoals ontwikkeld voor de beheervoorziening BSN (ref. [2]).

De beheervoorziening BSN wordt geraadpleegd om botsingen ("collisions": de situatie dat twee verschillende personen dezelfde STAMSLEUTEL hebben) te detecteren. Indien een botsing wordt vastgesteld wordt aan de STAMSLEUTEL een volgnummer ongelijk aan 0 toegevoegd om de STAMSLEUTEL alsnog uniek te maken; het volgnummer is 0 als er geen botsing is. De uitgevende partij zal wel nader onderzoek moeten doen om vast te stellen dat het daadwerkelijk om twee verschillende personen gaat. Dit onderzoek kan mogelijk niet door alle uitgevers van AUTHENTICATIEMIDDELen worden uitgevoerd; het is mogelijk dat de GEBRUIKER dan moet worden doorverwezen naar een gemeentelijk uitgiftepunt.

Het algoritme voor de controle van de STAMSLEUTEL is globaal als volgt.

- Indien de GEBRUIKER beschikt over een Nederlands WID (in dat geval moet hij of zij ook in de BRP zijn ingeschreven), dan wel zelf aangeeft te zijn ingeschreven in de BRP:
  1. Vraag het BSN van de GEBRUIKER op bij de beheervoorziening BSN.
  2. Indien één unieke match: rond de registratie af. Het BSN wordt genegeerd.
  3. Indien geen match: verwijs de GEBRUIKER naar de afdeling burgerzaken van zijn gemeente, dan wel een RNI-loket. De gegevens op zijn of haar WID zijn kennelijk niet in overeenstemming met de gegevens in de GBA. De gemeente is de aangewezen instelling om dit te onderzoeken en eventuele correcties door te voeren.
  4. Indien meerdere matches: stel het BSN vast op basis van aanvullende zoekgegevens. Deze procedure kan alleen worden uitgevoerd door een instantie die volledige toegang heeft tot de GBA en de beheervoorziening BSN; in de praktijk zal dit ook de gemeente zijn. Het zoekpad dat gevolgd wordt is hetzelfde als dat in de beheervoorziening BSN. Vul de STAMSLEUTEL aan met een volgnummer en registreer welke gegevens zijn gebruikt om de STAMSLEUTEL aan te vullen.
- Indien de persoon niet beschikt over een Nederlands WID en geen BSN heeft:
  1. Controleer bij de beheervoorziening BSN of de GEBRUIKER niet toch een BSN heeft.
  2. Indien geen match (de verwachte situatie): rond de registratie af. Er wordt uiteraard geen BSN gekoppeld.
  3. Indien wel een of meerdere matches: verwijs de GEBRUIKER naar een gemeentelijke balie. Er zal ondubbelzinnig moeten worden vastgesteld of de GEBRUIKER daadwerkelijk een ander persoon is dan de in de BRP gevonden mogelijke matches. Immers, er zijn toepassingen van het eID Stelsel (zoals referenda en polls) waarin dit onderscheid van wezenlijk belang is.

5.2 POLYMORFE PSEUDOID

Een POLYMORFE PSEUDOID wordt berekend door:

1. een hash te berekenen over de combinatie van STAMSLEUTEL, PERSONAGE en volgnummer;
2. deze hash te versleutelen met een geheime sleutel van de STELSELAUTORITEIT.

De sleutel van de STELSELAUTORITEIT geldt voor het hele stelsel, en dient dus uiteraard zwaar beveiligd te worden. Opslag in een HSM is hierbij een vereiste.

Het polymorfe karakter van de gegenereerde pseudoniemen (het feit dat ze zich in verschillende gedaanten kunnen manifesteren) maakt ze tot een gevoelig punt, te vergelijken met een

encryptiesleutel. AUTHENTICATIEDIENSTEN dienen daarom POLYMORFE PSEUDOID'S te bewaren in een HSM.

6 De SectorID-dienst BSN

Het BSN is een nummer dat alleen gebruikt mag worden door overheidsorganen en partijen die belast zijn met de uitvoering van een overheidstaak. Gevolg van P47 is dan:

P56 De overheid is verantwoordelijk is voor het ontwikkelen van een SectorID-dienst BSN.

Merk op dat er dus geen noodzaak is dat een Authenticatiedienst of een Machtigingsdienst het BSN gebruikt. Dat vereenvoudigt het toelaten van private partijen als Authenticatiedienst of Machtigingsdienst.

6.1 Koppelen BSN op aanvraag

Voor het vullen van de conversietabel wordt wederom gebruikt van de beheervoorziening BSN. Dit werkt als volgt.

1. De Gebruiker geeft aan dat zijn of haar middel[9] te willen gebruiken bij de overheid. Dit kan meteen bij de aanvraag van het middel, maar het proces kan ook naderhand worden doorlopen.
2. De Gebruiker wordt doorgeleid naar de SectorID-dienst BSN en doorloopt daar een normaal inlogproces. Als onderdeel van dit proces verkrijgt de SectorID-dienst de gegevens voor de Stamsleutel. Omdat het hier om een SectorID-dienst gaat is de dienst gerechtigd om deze gegevens te ontvangen.
3. De SectorID-dienst BSN vraagt bij de beheervoorziening BSN het BSN op. Deze vraag is identiek aan de vraag die de Stelselautoriteit/pseudoniemen heeft gebruikt om het uniek zijn van de Stamsleutel te verifiëren. Omdat de sleutel eerder is gebruikt zijn er verder geen complicaties te verwachten: het BSN wordt gevonden, of de Gebruiker beschikt niet over een BSN. In het laatste geval wordt de procedure afgebroken.
4. Op dat moment beschikt de SectorID-dienst BSN over de combinatie PseudoID en BSN. Deze combinatie wordt vastgelegd in de conversietabel. De gegevens van de Stamsleutel kunnen worden verwijderd.

P57 De SectorID-dienst BSN wordt gevuld op aanvraag vanuit een Authenticatiedienst middels het raadplegen van de beheervoorziening BSN.

De procedure vertoont dus grote overeenkomst met de procedure die de Machtigingsdienst volgt om een Polymorfe PseudoID aan te vragen bij de Stelselautoriteit/pseudoniemen.[10]

De verwachting is dat de procedure voor andere SectorID-diensten op dezelfde wijze kan verlopen. Voorwaarde is dat in de sector een dienst aanwezig is die ook de gegevens voor de Stamsleutel bevat. Gezien het generieke karakter van deze gegevens is dat aannemelijk.

[9] Strikt genomen wordt een Persona gekoppeld, niet een Authenticatiemiddel. Impliciete veronderstelling is hier dus dat een middel gebruikt wordt om een Persona te selecteren.

[10] Vanuit de werkgroep cryptografie is voorgesteld om in plaats van de hier geschetste procedure gebruik te maken van een polymorf versleutelde vorm van het BSN. Deze suggestie wordt nader onderzocht.

Bijlagen

Bijlage A Overzicht eigenschappen

P01 Het eID Stelsel is neutraal ten aanzien van partijen die een rol invullen; het formuleert alleen eisen waaraan een partij voor een bepaalde rol moet voldoen. 10

P02 De rol van STELSELAUTORITEIT wordt ingevuld door de overheid. 10

P03 Een gecertificeerde EID-DEELNEMER kan verklaringen afgeven over derden (natuurlijke of niet-natuurlijke personen). 10

P04 Een persoon kan zelf een BEVOEGDHEIDSVERKLARING afgeven met een machtiging waarin hij als VERTEGENWOORDIGDE voorkomt. 10

P05 Een GEBRUIKER kan een IDENTITEITSVERKLARING of ATTRIBUUTVERKLARING afgeven over zichzelf. 10

P06 Een AUTHENTICATIEDIENST geeft AUTHENTICATIEMIDDELEN uit. 11

P07 Een AUTHENTICATIEDIENST ontkoppelt AUTHENTICATIEMIDDELEN van DIENSTAANBIEDERS. 11

P08 Een AUTHENTICATIEDIENST levert een getekende IDENTITEITSVERKLARING. Een IDENTITEITSVERKLARING kan gericht zijn aan meerdere ONTVANGENDE PARTIJEN. 11

P09 Een AUTHENTICATIEDIENST realiseert inzage voor de GEBRUIKER in het gebruik dat van zijn of haar AUTHENTICATIEMIDDELEN is gemaakt. 11

P10 Een audit trail mag door een AUTHENTICATIEDIENST uitsluitend worden gebruikt voor het geven van inzicht aan de GEBRUIKER welk gebruik er van zijn middelen is gemaakt. 11

P11 EEN AUTHENTICATIEDIENST kan facultatief de mogelijkheid bieden aan een GEBRUIKER om af te zien van het bijhouden van een audit trail. 11

P12 De keuze voor een AUTHENTICATIEDIENST en voor het te gebruiken AUTHENTICATIEMIDDEL berust bij de GEBRUIKER. 12

P13 Een SECTORID-DIENST wordt geraadpleegd door een EID-MAKELAAR op het moment dat een DIENSTAANBIEDER aangeeft dat voor het verlenen van een bepaalde dienst een SECTORID nodig is. 12

P14 Een MACHTIGINGSDIENST registreert een bevoegdheid van een persoon (de GEMACHTIGDE) om een bepaalde dienst of groep van diensten af te nemen namens een ander persoon (de VERTEGENWOORDIGDE). 12

P15 Een MACHTIGINGSDIENST kan de identiteit van een VERTEGENWOORDIGDE vaststellen aan de hand van een IDENTITEITSVERKLARING van een AUTHENTICATIEDIENST of op basis van een eigen registratieproces. In het registratieproces van de machtiging wordt ook vastgesteld dat de VERTEGENWOORDIGDE de wil heeft de machtiging tot stand te laten komen. 12

P16 Een machtiging is pas geldig op het moment dat hij door de GEMACHTIGDE is geaccepteerd. De MACHTIGINGSDIENST stelt de identiteit van een GEMACHTIGDE vast op het moment van acceptatie. 12

P17 Een MACHTIGINGSDIENST levert op aanvraag een BEVOEGDHEIDSVERKLARING, waarmee een HANDELENDE PERSOON ten overstaan van een DIENSTBEMIDDELAAR of DIENSTAANBIEDER kan aantonen dat hij gemachtigd is om een dienst af te nemen namens een VERTEGENWOORDIGDE. 12

P18 De keuze bij welke MACHTIGINGSDIENST een machtiging wordt geregistreerd berust bij degene die de machtiging aanvraagt. 13

P19 De EID-MAKELAAR vraagt aan de GEBRUIKER van welke AUTHENTICATIEDIENST hij gebruik wil maken en (indien van toepassing) waar de machtigingen van de GEBRUIKER zijn geregistreerd. Op basis van de antwoorden routeert hij de GEBRUIKER door naar de juiste voorzieningen. 13

P20 De EID-MAKELAAR verricht zijn werkzaamheden op basis van een contract of bewerkersovereenkomst met de DIENSTBEMIDDELAAR of DIENSTAANBIEDER. De keuze voor een bepaalde EID-MAKELAAR berust bij de DIENSTBEMIDDELAAR of DIENSTAANBIEDER. 13

P21 Een DIENSTBEMIDDELAAR bundelt de verkregen verklaringen en de bijbehorende gegevens en ondertekent het geheel. Daarmee verklaart de DIENSTBEMIDDELAAR dat alle verklaringen en gegevens bij elkaar horen (ook associëren genoemd). 13

P22 Een DIENSTBEMIDDELAAR kan optreden als bewerker namens een DIENSTAANBIEDER of op eigen titel worden geregistreerd als EID-DEELNEMER. 14

P23 De DIENSTEIGENAAR is de partij die beslist over onder de indeling en naamgeving van de diensten en over alle beleidsmatige aspecten die gelden voor de betreffende dienst, zoals het vereiste BETROUWBAARHEIDSNIVEAU. 14

P24 Comfortinformatie wordt in het stelsel vastgelegd op het moment van ontlening aan een authentieke bron (bijvoorbeeld WID, STORK-verklaring, Basisregistratie, Eigen Verklaring). 14

P25 Comfortinformatie wordt alleen op verzoek van de betrokken persoon geactualiseerd door opnieuw de authentieke bron te raadplegen. 14

P26 Bij alle attributen wordt vastgelegd aan welke bron ze zijn ontleend en op welke datum dat is gebeurd. 14

P27 Het eID Stelsel dwingt af dat een DIENSTAANBIEDER niet meer gegevens ontvangt dan waar hij recht op heeft. Dit recht wordt vastgesteld bij het aansluiten van de die DIENSTAANBIEDER op het stelsel. 15

P28 De gegevens waar de DIENSTAANBIEDER volgens het autorisatiebesluit recht op heeft worden vastgelegd in de aansluitovereenkomst van de DIENSTAANBIEDER. 15

P29 Attributen worden uitsluitend verstrekt op basis van instemming van de GEBRUIKER. Instemming kan expliciet of impliciet worden verleend. 15

P30 Persoonsgegevens die tussen partijen worden getransporteerd worden zodanig versleuteld dat alleen de ONTVANGENDE PARTIJ deze weer kan ontsleutelen. 15

P31 Een GEBRUIKER kan kiezen voor meerdere PERSONAGES of voor een enkele. Aan een bepaald PERSONAGE kan hij één of meerdere AUTHENTICATIEMIDDELEN koppelen. 16

P32 Een PSEUDOID binnen het stelsel is betekenisloos. Hij is uniek voor een bepaald PERSONAGE en voor een bepaalde DIENSTAANBIEDER. 16

P33 De PSEUDOID is onafhankelijk van het gebruikte AUTHENTICATIEMIDDEL en van de gebruikte AUTHENTICATIEDIENST. 16

P34 De POLYMORFE PSEUDOID wordt uitgereikt door de STELSELAUTORITEIT aan een AUTHENTICATIEDIENST. 17

P35 Een POLYMORFE PSEUDOID wordt afgeleid van persoonskenmerken, opgenomen in een identiteitsdocument. Daarbij wordt geen gebruik gemaakt van persoonsnummers. 18

P36 De STELSELAUTORITEIT controleert de STAMSLEUTEL bij de beheervoorziening BSN en in een eigen administratie. Daarmee voorkomt de STELSELAUTORITEIT dubbele inschrijvingen en signaleert hij niet-unieke STAMSLEUTELS. 18

P37 Als een STAMSLEUTEL niet uniek is worden aanvullende gegevens gebruikt om tot een

unieke sleutel te komen. Dit proces wordt uitgevoerd door de gemeentelijke balies. 18

P38 Een Polymorf PseudoID is randomiseerbaar (aangegeven met een dubbele lijn in Figuur 2). Dat houdt in dat er extra gegevens aan de Polymorfe PseudoID kunnen worden toegevoegd zonder dat dit invloed heeft op de PseudoID's die van het Polymorfe PseudoID worden afgeleid. 18

P39 Een Polymorfe PseudoID is specifiek voor de Authenticatiedienst die de Polymorfe PseudoID heeft aangevraagd, zonder dat dit invloed heeft op de PseudoID's die van de Polymorfe PseudoID worden afgeleid. 18

P40 Een Polymorfe PseudoID kan worden opgeslagen op een extern "secure device" of in de administratie van de Authenticatiedienst. 19

P41 De informatie in een audit trail is voor een Authenticatiedienst afhankelijk van de gebruikte techniek. 19

P42 Een Authenticatiedienst ontvangt van de Stelselautoriteit/sleutelbeheer een geheime sleutel ten behoeve van het berekenen van Versleutelde PseudoID's. 19

P43 Een Versleutelde PseudoID is randomiseerbaar. 19

P44 Een Versleutelde PseudoID is alleen leesbaar voor de Ontvangende Partij. 19

P45 Een PseudoID is persistent, uniek voor de Ontvangende Partij en alleen afhankelijk van de Stamsleutel van de Gebruiker en het gekozen Personage. 19

P46 Een SectorID wordt uitsluitend op verzoek van de Gebruiker en via een expliciete koppelprocedure gekoppeld aan een Personage. 20

P47 Het in stand houden van een SectorID-dienst is de verantwoordelijkheid van de sector zelf. 20

P48 Een identiteitsketen kan per Ontvangende Partij slechts één identiteit (PseudoID of SectorID) bevatten. 22

P49 Uitgangspunt is dat niet-natuurlijke personen in het stelsel op dezelfde manier worden behandeld als natuurlijke personen. 22

P50 Een Gebruiker moet kunnen inloggen bij een Machtigingsdienst en al zijn machtigingen zien en beheren (zowel de machtigingen waarin hij als Vertegenwoordigde voorkomt als die waarin hij als Gemachtigde voorkomt). 23

P51 Een Bevoegdheidsverklaring bevat de Dienstaanbieder-specifieke Versleutelde PseudoID van de Gemachtigde en de Vertegenwoordigde. 24

P52 Een Authenticatiedienst levert op verzoek zowel een Versleutelde PseudoID voor de Dienstaanbieder als voor de Machtigingsdienst. 24

P53 Een Machtigingsdienst vraagt voor het genereren van PseudoID's een eigen Polymorfe PseudoID aan bij de Stelselautoriteit/pseudoniemen. 25

P54 De gegevens voor het aanvragen van een Polymorfe PseudoID verkrijgt de Machtigingsdienst uit een Identiteitsverklaring of uit een eigen registratieproces. 25

P55 De Stelselautoriteit ondersteunt ter bestrijding van fraude de mogelijkheid om een PseudoID terug te herleiden tot de Stamsleutel waarop de PseudoID was gebaseerd. 25

P56 De overheid is verantwoordelijk is voor het ontwikkelen van een SectorID-dienst BSN. 28

P57 De SectorID-dienst BSN wordt gevuld op aanvraag vanuit een Authenticatiedienst middels het raadplegen van de beheervoorziening BSN. 28

Bijlage B Overzicht eigenschappen vs. ontwerpeisen

In deze bijlage zijn bij de verschillende ontwerpeisen (Exx) uit het document *Stakeholders, belangen en ontwerpeisen* verwijzingen opgenomen naar ontwerpeigenschappen (Pxx) uit het document *Werking van het eID Stelsel*.

E01 Ontzorgen van de DIENSTAANBIEDERS.

Verwijst naar ontwerpeigenschappen:
- P07 Een AUTHENTICATIEDIENST ontkoppelt AUTHENTICATIEMIDDELEN van DIENSTAANBIEDERS.
- P13 Een SECTORID-DIENST wordt geraadpleegd door een EID-MAKELAAR op het moment dat een DIENSTAANBIEDER aangeeft dat voor het verlenen van een bepaalde dienst een SECTORID nodig is.
- P20 De EID-MAKELAAR verricht zijn werkzaamheden op basis van een contract of bewerkersovereenkomst met de DIENSTBEMIDDELAAR of DIENSTAANBIEDER. De keuze voor een bepaalde EID-MAKELAAR berust bij de DIENSTBEMIDDELAAR of DIENSTAANBIEDER.
- P28 De gegevens waar de DIENSTAANBIEDER volgens het autorisatiebesluit recht op heeft worden vastgelegd in de aansluitovereenkomst van de DIENSTAANBIEDER.

E02 Bruikbaar voor digitaal minder vaardigen.

Verwijst naar ontwerpeigenschappen:
- P15 Een MACHTIGINGSDIENST kan de identiteit van een VERTEGENWOORDIGDE vaststellen aan de hand van een IDENTITEITSVERKLARING van een AUTHENTICATIEDIENST of op basis van een eigen registratieproces. In het registratieproces van de machtiging wordt ook vastgesteld dat de VERTEGENWOORDIGDE de wil heeft de machtiging tot stand te laten komen.
- P54 De gegevens voor het aanvragen van een POLYMORFE PSEUDOID verkrijgt de MACHTIGINGSDIENST uit een IDENTITEITSVERKLARING of uit een eigen registratieproces.

E03 Derden moeten namens een DIENSTAANBIEDER digitale diensten kunnen aanbieden.

Verwijst naar ontwerpeigenschappen:
- P21 Een DIENSTBEMIDDELAAR bundelt de verkregen verklaringen en de bijbehorende gegevens en ondertekent het geheel. Daarmee verklaart de DIENSTBEMIDDELAAR dat alle verklaringen en gegevens bij elkaar horen (ook associëren genoemd).
- P22 Een DIENSTBEMIDDELAAR kan optreden als bewerker namens een DIENSTAANBIEDER of op eigen titel worden geregistreerd als EID-DEELNEMER.

E04 Opheffen domeinscheiding burgers / bedrijven.

Verwijst naar ontwerpeigenschappen:
- P31 Een GEBRUIKER kan kiezen voor meerdere PERSONAGES of voor een enkele. Aan een bepaald personage kan hij één of meerdere middelen koppelen.
- P49 Uitgangspunt is dat niet-natuurlijke personen in het stelsel op dezelfde manier worden behandeld als natuurlijke personen.

E05 Sectoren met eigen nummers moeten ondersteund kunnen worden.

Verwijst naar ontwerpeigenschappen:
- P13 Een SECTORID-DIENST wordt geraadpleegd door een EID-MAKELAAR op het moment dat een DIENSTAANBIEDER aangeeft dat voor het verlenen van een bepaalde dienst een SECTORID nodig is.
- P47 Het in stand houden van een SECTORID-DIENST is de verantwoordelijkheid van de sector zelf.
- P56 De overheid is verantwoordelijk is voor het ontwikkelen van een SECTORID-DIENST BSN.
- P57 De SECTORID-DIENST BSN wordt gevuld op aanvraag vanuit een AUTHENTICATIEDIENST middels raadplegen van de beheervoorziening BSN.

E11 Multimiddelenstrategie.

Verwijst naar ontwerpeigenschappen:
- P31 Een GEBRUIKER kan kiezen voor meerdere PERSONAGES of voor een enkele. Aan een bepaald PERSONAGE kan hij één of meerdere AUTHENTICATIEMIDDELEN koppelen.
- P33 De PSEUDOID is onafhankelijk van het gebruikte AUTHENTICATIEMIDDEL en van de gebruikte AUTHENTICATIEDIENST.

E13 Zorg ervoor dat alle partijen gelijke kansen hebben.

Verwijst naar ontwerpeigenschappen:
- P01 Het eID Stelsel is neutraal ten aanzien van partijen die een rol invullen; het formuleert alleen eisen waaraan een partij voor een bepaalde rol moet voldoen.
- P03 Een gecertificeerde EID-DEELNEMER kan verklaringen afgeven over derden (natuurlijke of niet-natuurlijke personen).

E21 Wees laagdrempelig, gebruikersvriendelijk en consistent voor betrokkenen.

Verwijst naar ontwerpeigenschappen:
- P04 Een persoon kan zelf een BEVOEGDHEIDSVERKLARING afgeven met een machtiging waarin hij als VERTEGENWOORDIGDE voorkomt.
- P05 Een GEBRUIKER kan een IDENTITEITSVERKLARING of ATTRIBUUTVERKLARING afgeven over zichzelf.
- P12 De keuze voor een AUTHENTICATIEDIENST en voor het te gebruiken AUTHENTICATIEMIDDEL berust bij de GEBRUIKER.
- P18 De keuze bij welke MACHTIGINGSDIENST een machtiging wordt geregistreerd berust bij degene die de machtiging aanvraagt.
- P19 De EID-MAKELAAR vraagt aan de GEBRUIKER van welke AUTHENTICATIEDIENST hij gebruik wil maken en (indien van toepassing) waar de machtigingen van de GEBRUIKER zijn geregistreerd. Op basis van de antwoorden routeert hij de GEBRUIKER door naar de juiste voorzieningen.
- P50 Een GEBRUIKER moet kunnen inloggen bij een MACHTIGINGSDIENST en al zijn machtigingen zien en beheren (zowel de machtigingen waarin hij als VERTEGENWOORDIGDE voorkomt als die waarin hij als GEMACHTIGDE voorkomt).

E22 BELANGHEBBENDE kan zelf machtigingen en activiteiten achteraf controleren.

Verwijst naar ontwerpeigenschappen:
- P09 Een AUTHENTICATIEDIENST realiseert inzage voor de GEBRUIKER in het gebruik dat van zijn of haar AUTHENTICATIEMIDDELEN is gemaakt.
- P10 Een audit trail mag door een AUTHENTICATIEDIENST uitsluitend worden gebruikt voor het geven van inzicht aan de GEBRUIKER welk gebruik er van zijn middelen is gemaakt.
- P11 Een AUTHENTICATIEDIENST kan facultatief de mogelijkheid bieden aan een GEBRUIKER om af te zien van het bijhouden van een audit trail.

E23 GEBRUIKERS houden de controle over machtigingen en gegevens.

Verwijst naar ontwerpeigenschappen:
- P16 Een machtiging is pas geldig op het moment dat hij door de GEMACHTIGDE is geaccepteerd. De MACHTIGINGSDIENST stelt de identiteit van een GEMACHTIGDE vast op het moment van acceptatie.
- P25 Comfortinformatie wordt alleen op verzoek van de betrokken persoon geactualiseerd door opnieuw de authentieke bron te raadplegen.
- P29 Attributen worden uitsluitend verstrekt op basis van instemming van de GEBRUIKER. Instemming kan expliciet of impliciet worden verleend.
- P46 Een SECTORID wordt uitsluitend op verzoek van de GEBRUIKER en via een expliciete koppelprocedure gekoppeld aan een PERSONAGE.

E24 Keuzevrijheid in aanschaf en gebruik.

Verwijst naar ontwerpeigenschap:
- P31 Een GEBRUIKER kan kiezen voor meerdere PERSONAGES of voor een enkele. Aan een bepaald PERSONAGE kan hij één of meerdere AUTHENTICATIEMIDDELEN koppelen.

E31 Bescherming privacy betrokkenen.

Verwijst naar ontwerpeigenschappen:
- P30 Persoonsgegevens die tussen partijen worden getransporteerd worden zodanig versleuteld dat alleen de ONTVANGENDE PARTIJ deze weer kan ontsleutelen.
- P32 Een PSEUDOID binnen het stelsel is betekenisloos. Hij is uniek voor een bepaald PERSONAGE en voor een bepaalde DIENSTAANBIEDER.
- P33 De PSEUDOID is onafhankelijk van het gebruikte AUTHENTICATIEMIDDEL en van de gebruikte AUTHENTICATIEDIENST.

• P38 Een POLYMORFE PSEUDOID is randomiseerbaar. Dat houdt in dat er extra gegevens aan de POLYMORFE PSEUDOID kunnen worden toegevoegd zonder dat dit invloed heeft op de PSEUDOID'S die van de POLYMORFE PSEUDOID worden afgeleid.
• P43 Een VERSLEUTELDE PSEUDOID is randomiseerbaar.
• P45 Een PSEUDOID is persistent, uniek voor de ONTVANGENDE PARTIJ en alleen afhankelijk van de STAMSLEUTEL van de GEBRUIKER en het gekozen PERSONAGE.

E32 Een eID-DEELNEMER krijgt niet meer gegevens dan strikt noodzakelijk is voor het uitvoeren van zijn taak.

Verwijst naar ontwerpeigenschappen:
• P27 Het eID Stelsel dwingt af dat een DIENSTAANBIEDER niet meer gegevens ontvangt dan waar hij recht op heeft. Dit recht wordt vastgesteld bij het aansluiten van de die DIENSTAANBIEDER op het stelsel.
• P28 De gegevens waar de DIENSTAANBIEDER volgens het autorisatiebesluit recht op heeft worden vastgelegd in de aansluitovereenkomst van de DIENSTAANBIEDER.
• P30 Persoonsgegevens die tussen partijen worden getransporteerd worden zodanig versleuteld dat alleen de bedoelde ONTVANGENDE PARTIJ deze weer kan ontsleutelen.
• P39 Een POLYMORFE PSEUDOID is specifiek voor de AUTHENTICATIEDIENST die de POLYMORFE PSEUDOID heeft aangevraagd, zonder dat dit invloed heeft op de PSEUDOID'S die van de POLYMORFE PSEUDOID worden afgeleid.
• P44 Een VERSLEUTELDE PSEUDOID is alleen leesbaar voor de ONTVANGENDE PARTIJ.
• P48 Een IDENTITEITSKETEN kan per ONTVANGENDE PARTIJ slechts één identiteit (PSEUDOID of SECTORID) bevatten.
• P51 Een BEVOEGDHEIDSVERKLARING bevat het DIENSTAANBIEDER-specifieke VERSLEUTELDE PSEUDOID van de GEMACHTIGDE en de VERTEGENWOORDIGDE.
• P52 Een AUTHENTICATIEDIENST levert op verzoek zowel een VERSLEUTELDE PSEUDOID voor de DIENSTAANBIEDER als voor de MACHTIGINGSDIENST.
• P53 Een MACHTIGINGSDIENST vraagt voor het genereren van PSEUDOID'S een eigen POLYMORFE PSEUDOID aan bij de STELSELAUTORITEIT /PSEUDONIEMEN.

E33 DIENSTAANBIEDER (en andere deelnemende partijen) kunnen verantwoording afleggen.

Verwijst naar ontwerpeigenschappen:
• P10 Een audit trail mag door een AUTHENTICATIEDIENST uitsluitend worden gebruikt voor het geven van inzicht aan de GEBRUIKER welk gebruik er van zijn middelen is gemaakt.
• P11 Een AUTHENTICATIEDIENST kan facultatief de mogelijkheid bieden aan een GEBRUIKER om af te zien van het bijhouden van een audit trail.
• P41 De informatie in een audit trail is voor een AUTHENTICATIEDIENST afhankelijk van de gebruikte techniek.

E41 Zorg voor robuustheid, flexibiliteit en veerkracht in het ontwerp.

Verwijst naar ontwerpeigenschappen:
• P01 Het eID Stelsel is neutraal ten aanzien van partijen die een rol invullen; het formuleert alleen eisen waaraan een partij voor een bepaalde rol moet voldoen.
• P02 De rol van STELSELAUTORITEIT wordt ingevuld door de overheid.
• P06 Een AUTHENTICATIEDIENST geeft AUTHENTICATIEMIDDELEN uit.
• P08 Een AUTHENTICATIEDIENST levert een getekende IDENTITEITSVERKLARING. Een IDENTITEITSVERKLARING kan gericht zijn aan meerdere ONTVANGENDE PARTIJEN.
• P14 Een MACHTIGINGSDIENST registreert een bevoegdheid van een persoon (de GEMACHTIGDE) om een bepaalde dienst of groep van diensten af te nemen namens een ander persoon (de VERTEGENWOORDIGDE).
• P17 Een MACHTIGINGSDIENST levert op aanvraag een BEVOEGDHEIDSVERKLARING, waarmee een HANDELENDE PERSOON ten overstaan van een DIENSTBEMIDDELAAR of DIENSTAANBIEDER kan aantonen dat hij gemachtigd is om een dienst af te nemen namens een VERTEGENWOORDIGDE.
• P21 Een DIENSTBEMIDDELAAR bundelt de verkregen verklaringen en de bijbehorende gegevens en ondertekent het geheel. Daarmee verklaart de DIENSTBEMIDDELAAR dat alle verklaringen en gegevens bij elkaar horen (ook associëren genoemd).
• P23 De DIENSTEIGENAAR is de partij die beslist over onder de indeling en naamgeving van de diensten en over alle beleidsmatige aspecten die gelden voor de betreffende dienst, zoals het vereiste BETROUWBAARHEIDSNIVEAU.

• P24 Comfortinformatie wordt in het stelsel vastgelegd op het moment van ontlening aan een authentieke bron (bijvoorbeeld WID, STORK-verklaring, Basisregistratie, Eigen Verklaring).
• P26 Bij alle attributen wordt vastgelegd aan welke bron ze zijn ontleend en op welke datum dat is gebeurd.
• P35 Een POLYMORFE PSEUDOID wordt afgeleid van persoonskenmerken, opgenomen in een identiteitsdocument. Daarbij wordt geen gebruik gemaakt van persoonsnummers.
• P37 Als een STAMSLEUTEL niet uniek is worden aanvullende gegevens gebruikt om tot een unieke sleutel te komen. Dit proces wordt uitgevoerd door de gemeentelijke balies.
• P40 Een POLYMORFE PSEUDOID kan worden opgeslagen op een extern "secure device" of in de administratie van de AUTHENTICATIEDIENST.
• P42 Een AUTHENTICATIEDIENST ontvangt van de STELSELAUTORITEIT /SLEUTELBEHEER een geheime sleutel ten behoeve van het berekenen van VERSLEUTELDE PSEUDOID'S.

E51 Misbruik kan eenvoudig ontdekt en opgespoord worden.

Verwijst naar ontwerpeigenschappen:
• P34 De POLYMORFE PSEUDOID wordt uitgereikt door de STELSELAUTORITEIT aan een AUTHENTICATIEDIENST.
• P36 De STELSELAUTORITEIT controleert de STAMSLEUTEL bij de beheervoorziening BSN en in een eigen administratie. Daarmee voorkomt de STELSELAUTORITEIT dubbele inschrijvingen en signaleert hij niet-unieke STAMSLEUTELS.
• P55 De STELSELAUTORITEIT ondersteunt ter bestrijding van fraude de mogelijkheid om een PSEUDOID terug te herleiden tot de STAMSLEUTEL waarop de PSEUDOID was gebaseerd.