Programma eID
Afsprakenstelsel

Introductie op 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	18
Exemplaarnummer	

Inhoud

Inleiding

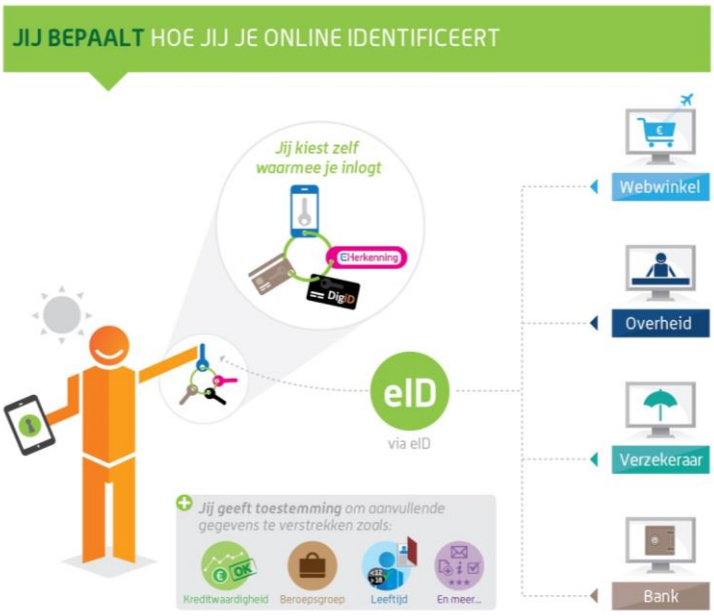
Overheden en bedrijven bieden mensen en organisaties in toenemende mate de mogelijkheid om diensten digitaal af te nemen. Ook de Nederlandse overheid en de Europese commissie stimuleren een verdergaande dienstverlening via internet. De Nederlandse overheid wil in 2017 alle transacties voor burgers en bedrijven digitaal kunnen laten verlopen.

Bij de ontwikkeling van digitale dienstverlening moet iedere organisatie een aantal vraagstukken op het terrein van geautoriseerde toegang oplossen. Het eID Stelsel is een manier om die vraagstukken te uniformeren, zodat niet iedere organisatie 'het wiel opnieuw uitvindt'. Het eID Stelsel gaat dus niet over de inhoud van de digitale diensten, maar bestaat uit een uniforme set van standaarden en afspraken voor geautoriseerde toegang tot digitale diensten.

De term 'eID' staat voor elektronische identiteit. Deze gebruik je als je bijvoorbeeld online gegevens over jezelf met een organisatie deelt.

De invoering van eID Stelsel is een ontwikkelingstraject waarbij de invulling in een samenwerking tussen overheid, markt en wetenschap tot stand moet komen. Dankzij het eID Stelsel kunnen organisaties veilig en betrouwbaar toegang geven tot hun digitale dienstverlening omdat ze met voldoende zekerheid weten 'wie er aan de andere kant van de lijn zit'. Hierbij kan het ook gaan om het aantonen dat een leeftijdsgrens is gepasseerd, maar ook dat iemand namens een bedrijf een elektronische handtekening mag zetten.

Voor de burger biedt het eID Stelsel naast veiligheid ook gebruiksgemak. Als hij een digitale dienst wil afnemen, kan hij bij organisaties die zijn aangesloten bij het eID Stelsel zelf kiezen met welk middel hij zichzelf identificeert. Zo kan hij één (of een beperkte set) middel(en) gebruiken om veilig online zaken te doen met meerdere organisaties. Wat in de fysieke wereld wordt bereikt met persoonlijk contact, kopieën van paspoorten, op papier getekende contracten en verklaringen van de Kamer van Koophandel, wordt zo ook mogelijk in de online wereld.



Met het ontwerp van het eID Stelsel wordt het volgende geregeld:

- ✓ Er komt een gestandaardiseerde manier om de authenticatie en bevoegdheid voor het afnemen van alle digitale diensten vast te stellen.
- ✓ Het gaat hierbij om persoonsgebonden digitale diensten. Dat hoeft niet altijd te betekenen dat de identiteit eenduidig vastgesteld moet worden. Het kan ook gaan om andere kenmerken van een persoon, bijvoorbeeld of de persoon ouder dan 18 jaar is, of juist kunnen aantonen dat de persoon jonger is dan 12 jaar.
- ✓ Er komt een technologie-onafhankelijk ontwerp. Hierdoor kunnen zowel bestaande als nieuwe manieren voor het vaststellen van de authenticatie en de bevoegdheid worden ingezet.

- ✓ Voor natuurlijke en niet-natuurlijke personen gelden dezelfde standaarden, met als resultaat dat het vaststellen van de authenticatie en de bevoegdheid in het burger- en het bedrijvendomein uitwisselbaar is.
- ✓ Bovendien zijn de verantwoordelijkheden van de verschillende partijen die betrokken zijn bij de levering van een digitale dienst en het vaststellen van de authenticatie en bevoegdheid van de persoon die deze dienst afneemt duidelijk beschreven. Hierbij zijn maatregelen genomen die ervoor zorgen dat de privacy gewaarborgd wordt.

Leeswijzer

- In Hoofdstuk 1 wordt de context van het eID Stelsel toegelicht aan de hand van de huidige situatie rondom toegang tot digitale dienstverlening.
- Hoofdstuk 2 beschrijft het verloop van een digitale transactie en gaat in op de randvoorwaardelijke basis, namelijk het kunnen herkennen van iemands identiteit en het vaststellen van de bijbehorende bevoegdheid.
- Hoofdstuk 3 bespreekt de vier belangrijkste ontwerpeisen voor het eID Stelsel en gaat in op welke wijze deze in het ontwerp verankerd worden.
- Hoofdstuk 4 geeft een eerste indruk van het ontwerp van het eID Stelsel, waarbij onder andere wordt ingegaan op het gebruik van verklaringen en de berekening van pseudoniemen binnen het stelsel.

1 De context van het eID Stelsel

1.1 Huidige situatie

Mensen en organisaties beschikken over een veelvoud aan authenticatiemiddelen waarmee ze online hun identiteit kunnen aangeven en transacties kunnen doen. Denk aan gebruikersnaam-wachtwoordcombinaties eventueel aangevuld met sms-code, bankpas/reader en tokens voor toegang tot de eigen bedrijfsinformatie.

Organisaties die digitale diensten aanbieden hebben meestal een eigen eID-middel ontwikkeld waarmee toegang kan worden verkregen tot de digitale diensten. Deze organisaties hebben vaak hoge kosten om deze eID-middelen te beheren. Ook specifieke sectoren hebben voor (bijvoorbeeld) beroepsgroepen eigen digitale identificatiemiddelen ontwikkeld.

1.1.1 Zakendoen met de overheid

Binnen de overheid zijn de laatste jaren stappen gezet om eID-middelen van overheidsorganisaties te ontkoppelen. Op deze wijze kan hetzelfde eID-middel bij meerdere organisaties gebruikt worden. Voor het burgerdomein is DigiD geïntroduceerd en in het bedrijvendomein is het stelsel eHerkenning geïntroduceerd.

Met een persoonlijke DigiD (gebruikersnaam en wachtwoord, optioneel aangevuld met sms-code) kan iemand zich identificeren op websites van de overheid en van organisaties die een overheidstaak uitvoeren. Het is bij DigiD mogelijk om iemand te machtigen die namens een ander individu een transactie uitvoert. DigiD kent inmiddels ruim honderd miljoen authenticatie transacties per jaar.

Voor bedrijven die zakendoen met de overheid is eHerkenning geïntroduceerd. Ondernemers loggen in met eHerkenning op websites van de overheid, zoals burgers dat doen met hun DigiD. eHerkenning kent verschillende betrouwbaarheidsniveaus waarop de identiteit van de gebruiker kan worden vastgesteld, waarbij ook het hoogste niveau beschikbaar is.

Overheidsorganisaties geven aan in het burgerdomein behoefte te hebben aan een hoger betrouwbaarheidsniveau van eID-middelen zodat ze meer dienstverlening digitaal kunnen aanbieden en ze met meer zekerheid kunnen vaststellen wat de identiteit van de handelende persoon is. Dit mogen zowel publiek als privaat uitgegeven eID-middelen zijn. Zo wordt een fallback-optie gecreëerd voor het geval dat een eID-middel onverhoopt niet gebruikt kan worden bij een transactie. Bovendien levert het onderscheid burger/bedrijf bij een aantal organisaties en bij de handelende persoon extra administratieve lasten op, denk daarbij bijvoorbeeld aan de grote groep ZZP'ers.

Het is daarom wenselijk dat een eID-middel in beide domeinen gebruikt kan worden.

1.1.2 Zakendoen met het bedrijfsleven

Commerciële organisaties hebben er belang bij dat online zakendoen snel, gemakkelijk en veilig verloopt. Veel organisaties hebben eigen inlogprocedures en voorzieningen ingericht om een online transactie succesvol te laten verlopen. Soms wordt ook informatie hergebruikt die al online gedeeld is, bijvoorbeeld door de klant toe te staan om in te loggen met een Facebookaccount.

De huidige situatie houdt in dat organisaties veelal ieder voor zich investeren in online zakendoen en lang niet altijd over een fallback-optie beschikken als hun voorziening (tijdelijk) niet werkt. Ook zijn ze

kosten kwijt aan niet inbare facturen omdat de identiteit van hun klanten onbetrouwbaar is gebleken. Bovendien kunnen ze soms met moeite of alleen tegen hoge kosten betrouwbare aanvullende informatie over een consument verifiëren zoals kredietwaardigheid of het voldoen aan een leeftijdsgrens.

1.1.3 Zakendoen met bepaalde sectoren

Een aantal sectoren heeft zelf voorzieningen ingericht waarmee iemand kan aantonen dat hij (bijvoorbeeld) tot een bepaalde beroepsgroep behoort. De pas voor advocaten is hier een voorbeeld van, evenals de UZI-pas waarmee zorgaanbieders (zorgverleners en zorginstellingen) en indicatieorganen (CIZ en Bureaus Jeugdzorg) via de elektronische weg veilig toegang kunnen krijgen tot vertrouwelijke patiëntinformatie. Deze voorzieningen geven toegang tot specifieke informatie die voor de uitwisseling van gegevens en/of de uitvoering van een transactie of taak van belang is.

1.1.4 Situatie voor de gebruiker

Voor mensen en organisaties leidt het huidige landschap van toegangsvoorzieningen voor online zakendoen tot de noodzaak om een veelvoud aan EID-MIDDELEN te beheren. Ze moeten vaak een hele lijst aan usernames en wachtwoorden onthouden.

1.2 Nieuwe situatie

1.2.1 Pijlers eID Stelsel

Het eID Stelsel maakt het mogelijk dat mensen en organisaties digitaal zaken kunnen doen met een EID-MIDDEL van hun keuze. De basis voor het ontwerp van het stelsel is gebaseerd op drie pijlers:

1. Om vast te stellen: “Wie ben je” en “Mag je dit” wordt gebruik gemaakt van een gestandaardiseerde en uniforme invulling van de ‘bewijsstukken’. Deze bewijsstukken worden in de vorm van verklaringen voor elke digitale dienst gecreëerd.
2. De identiteit van partijen die in het stelsel eID-diensten aanbieden (bijvoorbeeld authenticatie- en machtigingsdiensten), wordt vastgesteld met een hoge mate van zekerheid. Deze partijen conformeren zich tevens aan de toezichtregels die als onderdeel van het stelsel worden geïmplementeerd.
3. De rollen en verantwoordelijkheden van betrokkenen in een keten van digitale transacties zijn helder en afzonderlijk gedefinieerd.

1.2.2 Situatie voor de gebruiker

Een gebruiker kan met één (of een beperkte set) EID-MIDDEL(en) online transacties uitvoeren, waarbij hij zelf kan aangeven of hij dat (bijvoorbeeld) als consument, beroepshalve of als bedrijf doet.

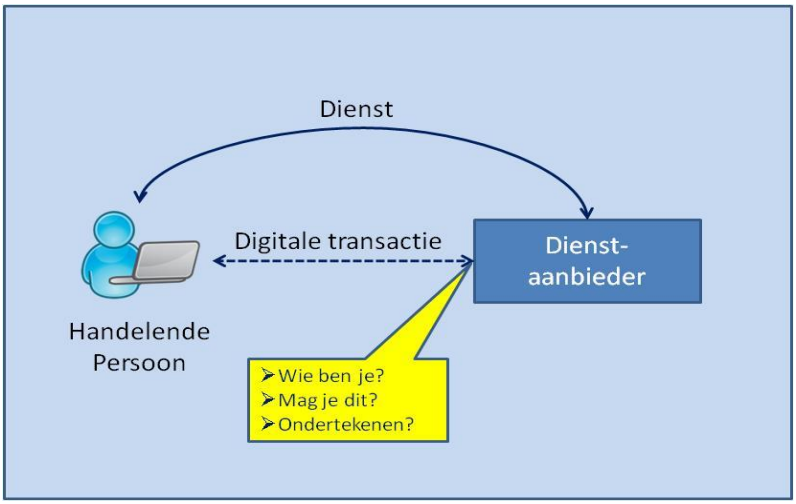
2 Een digitale transactie in het eID Stelsel

Bij een digitale transactie worden online gegevens uitgewisseld met een bepaald doel, bijvoorbeeld het invullen en indienen van een belastingaangifte, het boeken van een vakantie, of het indienen van een declaratie via het webportaal van een verzekeringsmaatschappij.

Bij de zorgvuldige totstandkoming van een transactie zijn er drie vragen van belang:

- Wie ben je?
- Mag je dit?
- Hoe wordt de transactie 'onbetwistbaar' (ondertekenen)?

In *onderstaande figuur* zijn deze vragen weergegeven, samen met een aantal sleutelbegrippen[1] bij de totstandkoming van een transactie in het eID Stelsel.



- De HANDELENDE PERSOON is de persoon die de dienst afneemt. Hij kan voor zichzelf of voor een ander handelen.
- De DIENSTAANBIEDER is de organisatie die de dienst aanbiedt.
- Een dienst is gericht op het tot stand komen van een recht, het leveren van een product of het beantwoorden van een informatievraag.
- Een digitale transactie is in het kader van een dienst de onloochenbare totstandkoming van een verrichting tussen een HANDELENDE PERSOON PARTIJ en een DIENSTAANBIEDER via een digitale weg.

2.1 Wie ben je?

Bij de vraagstelling 'wie ben je?' gaat het erom dat de DIENSTAANBIEDER kan vaststellen welke persoon zich meldt. Met andere woorden, kan de persoon zich identificeren? In de digitale wereld verloopt het herleiden van de identiteit in twee stappen:

a. Identificatie: wie ben je?
b. Authenticatie: bewijs dat maar.

[1] Een uitgebreide beschrijving van alle begrippen die binnen het eID Stelsel worden gehanteerd zijn opgenomen in Sectie 5: begrippenlijst.

Ad a. Identificatie: wie ben je?

Bij identificatie gaat het om eenduidig de ene persoon van de andere persoon te kunnen onderscheiden. In het dagelijkse leven zijn aan één natuurlijke persoon veel verschillende identificerende nummers gekoppeld. Denk aan het burgerservicenummer, het klantnummer bij de bank, het klantnummer bij een verzekeraar, het klantnummer bij een webwinkel, etc. Afhankelijk van bij welke DIENSTAANBIEDER een transactie wordt afgenomen, zal steeds een ander identificerend nummer van toepassing zijn.

Ad b. Authenticatie; bewijs dat maar

Om in het digitale verkeer de identiteit van de gebruiker te kunnen bevestigen zijn hulpmiddelen nodig. Deze hulpmiddelen worden aangeduid met de term AUTHENTICATIEMIDDELEN. Een voorbeeld van een AUTHENTICATIEMIDDEL is de gebruikersnaam-wachtwoordcombinatie van DigiD. Het proces van authentiseren wordt geleverd door een AUTHENTICATIEDIENST (bijvoorbeeld de dienst DigiD wordt geleverd door Logius). De door de AUTHENTICATIEDIENST vastgestelde (administratieve) identiteit, is vastgesteld met een bepaalde mate van betrouwbaarheid. Deze betrouwbaarheid is mede afhankelijk van het gebruikte AUTHENTICATIEMIDDEL.

2.2 Mag je dit?

Bij de beantwoording van de vraag "wie ben je" is voor de DIENSTAANBIEDER duidelijk geworden wie de persoon is die gebruik wil maken van de dienst. Voor veel diensten zal de DIENSTAANBIEDER ook de vraag stellen of de persoon wel bevoegd is om de dienst af te nemen. Kortom, de DIENSTAANBIEDER stelt de vraag 'mag je dit?'.

Het eID Stelsel standaardiseert de wijze waarop de bevoegdheidsgegevens ter beschikking worden gesteld aan de DIENSTAANBIEDER.

Een persoon kan bevoegd zijn op basis van de volgende drie situaties:

1. De persoon handelt namens zichzelf en is rechtstreeks BELANGHEBBENDE bij de gevraagde dienst. Dit is een veel voorkomende situatie: de consument die voor zichzelf een boek bestelt, de rekeninghouder die zijn eigen bankrekening via internetbankieren beheert, de belastingplichtige die zelf zijn aangifte opstelt en instuurt naar de Belastingdienst.
   In deze situatie kan het echter voorkomen dat de handelingsbevoegdheid van de persoon is ingeperkt. Voor een DIENSTAANBIEDER kan het relevant zijn om vast te kunnen stellen of de persoon handelingsbekwaam is voor de gevraagde dienst, bijvoorbeeld of de persoon minderjarig is of de persoon onder curatele is gesteld.

2. De persoon handelt niet voor zichzelf en treedt op voor een andere partij. De persoon is bevoegd gemaakt:
   - door middel van een machtiging.
   - door middel van een rechterlijke uitspraak, zodat er sprake is van een wettelijke vertegenwoordiging. Een voorbeeld hierbij is een bewindvoerder bij een faillissement.

3. De persoon handelt niet voor zichzelf en er is geen specifieke bevoegdheidsrelatie naar de BELANGHEBBENDE vastgelegd. De persoon moet dan ingeschreven zijn in een specifiek register waaraan vervolgens bevoegdheden worden ontleend. Bijvoorbeeld een persoon die is ingeschreven in het register van het notariaat, is dan als notaris bevoegd om authentieke akten op te maken. Een ander voorbeeld is de geregistreerde bevoegdheden van personen in het BIG-register (beroepen in de individuele gezondheidszorg).

2.3 Ondertekenen

Het is voor zowel de HANDELENDE PARTIJ als voor de DIENSTAANBIEDER belangrijk dat de uitgevoerde transactie onbetwistbaar is en ook nadien onbetwistbaar blijft. In de papieren wereld wordt dit meestal ingevuld door het plaatsen van een handtekening op een document.

Deze handtekening heeft vier functies:

- vaststellen van de identiteit van de persoon die ondertekent.
- vaststellen of de persoon bevoegd is om te ondertekenen.
- vaststellen dat de persoon de inhoud van het document kent en dit wil inzenden (wilsuiting).
- de inhoud van het document onlosmakelijk en betrouwbaar binden aan de persoon.

In de digitale wereld is de behoefte aan een goede invulling van bovenstaande functies nog belangrijker. Immers, in de digitale wereld kan de schaalgrootte van mogelijke fraude enorm zijn.

In de huidige praktijk worden twee hoofdvormen van elektronisch ondertekenen onderscheiden:

- De persoon beschikt over een middel dat bij een digitale transactie gebruikt kan worden als een elektronische handtekening. De meer betrouwbare middelen zijn bijvoorbeeld gebaseerd op het toepassen van PKI-certificaten.
- Tijdens de digitale transactie krijgt de gebruiker de mogelijkheid om de digitale transactie te bevestigen. Bijvoorbeeld door een vinkje te zetten bij de tekst:
  "ik verklaar stellig en zonder voorbehoud…".

In alle gevallen is het belangrijk dat de gebruiker controle heeft op het verbinden van zijn elektronische handtekening aan de digitale transactie. De DIENSTAANBIEDER is verantwoordelijk dat de handtekening aan de juiste inhoud van de transactie wordt gekoppeld (ook wel associëren genoemd).

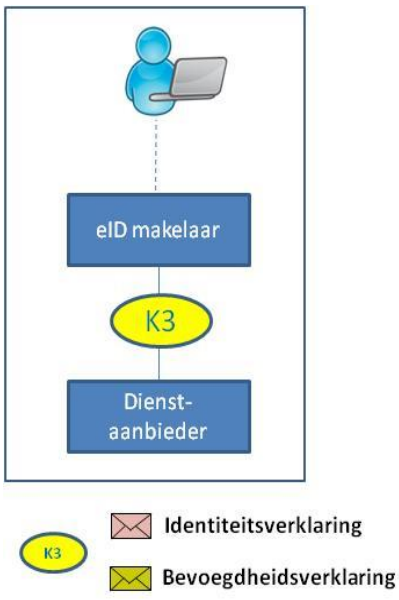
3 Ontwerpeisen

Bij de totstandkoming van het eID Stelsel zijn de volgende ontwerpeisen leidend:
1. Ontkoppelen en ontzorgen van de DIENSTAANBIEDER
2. Waarborgen privacy
3. Marktwerking mogelijk maken
4. Gebruikersgemak bevorderen
5. Toezicht en opsporing inrichten

3.1 Ontkoppelen en ontzorgen van de DIENSTAANBIEDER

Beoogde effect:
- DIENSTAANBIEDER is ontkoppeld van (technologisch) aanbod van leveranciers van AUTHENTICATIEMIDDELEN.
- Het inlogproces wordt door de DIENSTAANBIEDER als dienst afgenomen van een EID-MAKELAAR (vergelijkbaar met een iDeal-betaling).
- Dezelfde standaarden voor zowel portaaldiensten als machine-to-machinediensten

Nevenstaande figuur illustreert de ontkoppeling van het EID-MIDDEL van de DIENSTAANBIEDER. De DIENSTAANBIEDER kiest de EID-MAKELAAR waarmee de gebruiker kan inloggen. Een EID-MAKELAAR is een aparte dienst die onder andere inlogprocessen aanbiedt. Deze EID-MAKELAAR laat de EID-MIDDELEN zien waarmee de gebruiker kan inloggen. De gebruiker kan vervolgens zelf het EID-MIDDEL selecteren waarmee hij wil inloggen. Op deze wijze kan hij met hetzelfde middel terecht bij meerdere DIENSTAANBIEDERS. Via gestandaardiseerde verklaringen weet de DIENSTAANBIEDER met wie hij te maken heeft (via een IDENTITEITSVERKLARING) en wat deze gebruiker mag (via een BEVOEGDHEIDSVERKLARING). Vervolgens bepaalt de DIENSTAANBIEDER of de gebruiker de gewenste handeling mag uitvoeren. Dit is het autorisatiebesluit.



3.2 Waarborgen privacy

Beoogde effect:
- Een gebruiker kan naar elke DIENSTAANBIEDER een *andere* identiteit kenbaar maken (pseudoniem) en behoudt daarmee zijn digitale privacy.
- Een DIENSTAANBIEDER kan alleen op basis van doelbinding autorisatie aanvragen om (sommige) gegevens te kunnen ontvangen.
- De gegevens worden pas verstrekt nadat de gebruiker hiervoor toestemming heeft verleend.

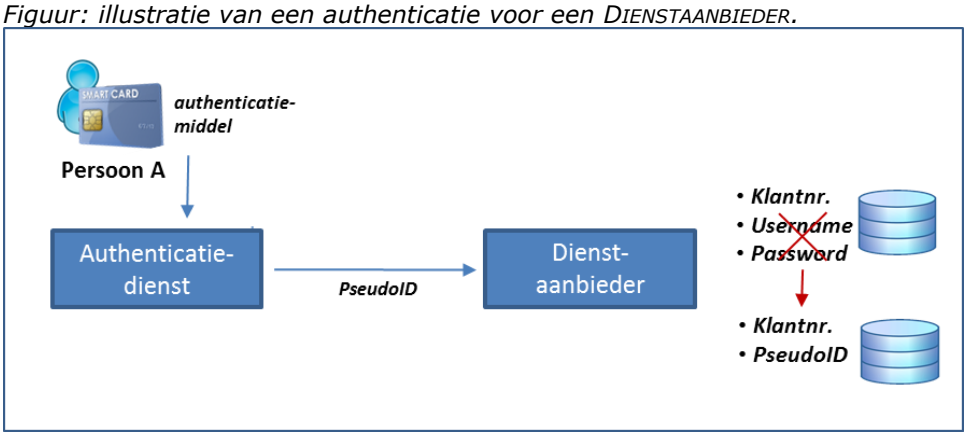
Met privacy wordt de bescherming van de persoonlijke levenssfeer bedoeld. In de digitale wereld moet iemand zelf kunnen bepalen wie welke informatie over hem krijgt en er moet voorkomen worden dat hij te maken krijgt met willekeurige of onwettige inmenging in zijn privéleven. De overheid gaat dus zorgvuldig om met persoonsgegevens; dit is verankerd in de Wet Bescherming Persoonsgegevens.

In het ontwerp voor het eID Stelsel wordt met pseudo-identiteiten (PSEUDOID) gewerkt. Een PSEUDOID is een nummer dat de afnemer van een dienst identificeert en dat door een AUTHENTICATIEDIENST aan

een DIENSTAANBIEDER wordt verstrekt. Binnen het domein van alle AUTHENTICATIEDIENSTEN is elke PSEUDOID uniek en is gekoppeld aan één bepaalde DIENSTAANBIEDER. Elke DIENSTAANBIEDER ontvangt een PSEUDOID dat speciaal aan hem is gericht. Hierdoor kunnen verschillende DIENSTAANBIEDERS de ontvangen PSEUDOID's van eenzelfde persoon niet vergelijken. Deze PSEUDOID's zijn persistent: iedere volgende authenticatie ten behoeve van dezelfde DIENSTAANBIEDER levert dezelfde PSEUDOID op.

Zoals hierboven beschreven levert elke authenticatie een DIENSTAANBIEDER-specifieke PSEUDOID op. De DIENSTAANBIEDER zal echter in veel gevallen dat PSEUDOID willen koppelen aan het administratieve nummer waaronder de persoon bij de DIENSTAANBIEDER bekend staat (het eigen interne klantnummer). De gebruiker moet daarvoor toestemming geven en zet met zijn AUTHENTICATIEMIDDEL een eenmalig koppelproces in gang.

Figuur: illustratie van een authenticatie voor een DIENSTAANBIEDER.

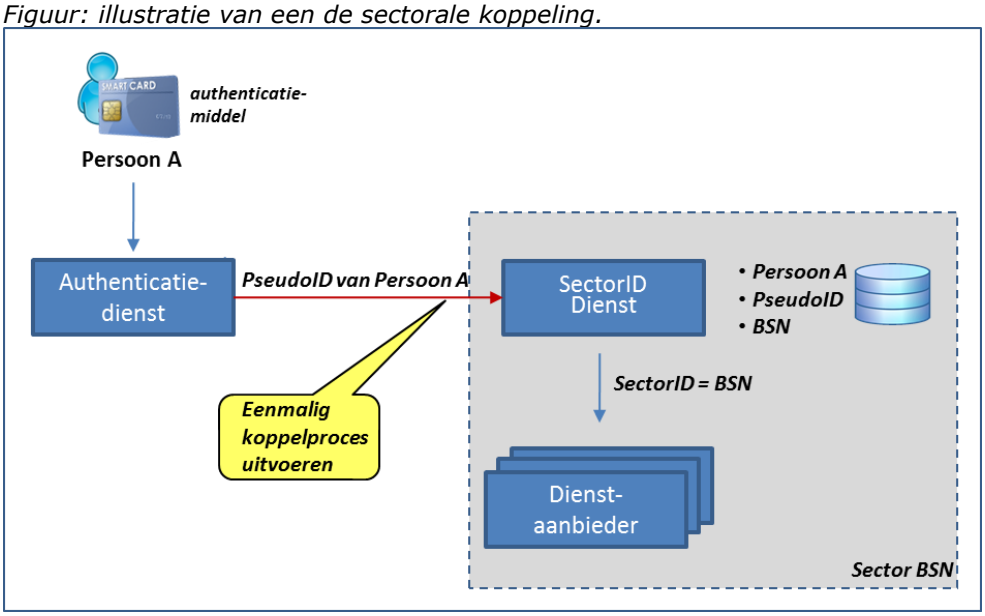


Sectoren

Er is in Nederland een aantal sectoren waarin meerdere DIENSTAANBIEDERS onderling gebruik maken van hetzelfde identificerende nummer van een persoon. Binnen een dergelijke sector bestaat een register waarin het sectorale nummer van de persoon is opgenomen. In dit geval moet de authenticatie niet een DIENSTAANBIEDER-specifieke PSEUDOID opleveren, maar een sector-specifieke PSEUDOID.

Per sector wordt een koppelregister ingericht. Hierin wordt, na toestemming van de gebruiker, de koppeling door de sector zelf geregistreerd tussen het PSEUDOID en het sectorale nummer.

Figuur: illustratie van een de sectorale koppeling.



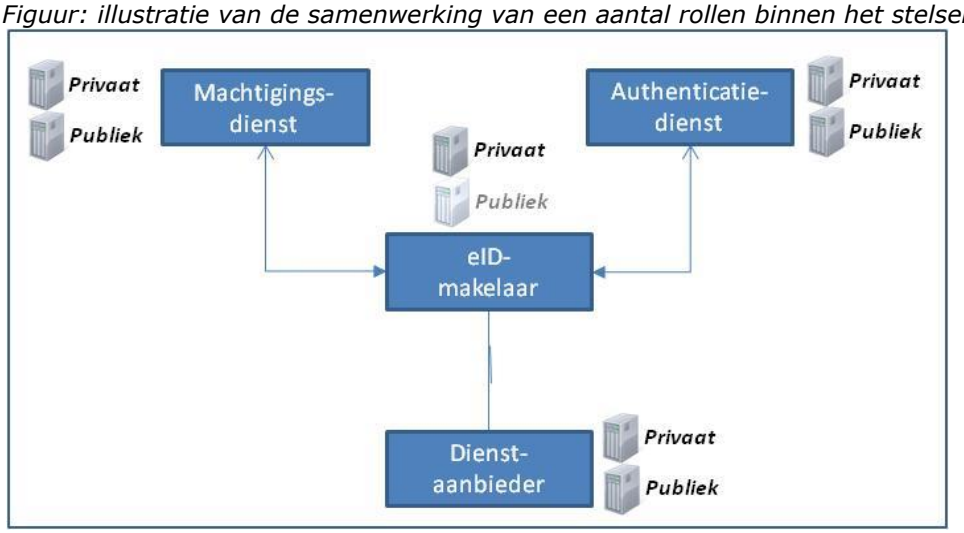
3.3 Marktwerking mogelijk maken

Beoogde effect:

- EID-MIDDELEN bruikbaar maken in alle domeinen en sectoren die zijn aangesloten op het eID Stelsel.
- Geen onderscheid maken tussen private en publieke invulling, maar dezelfde standaarden en toezicht voor beide domeinen.
- Fallback eenvoudiger te realiseren, zowel voor gebruiker als voor DIENSTAANBIEDER.
- Hergebruik van AUTHENTICATIEMIDDELEN mogelijk maken.

De architectuur van het stelsel wordt zo opgesteld dat er duidelijke, afgebakende rollen in het stelsel te onderscheiden zijn. Iedere rol kan zowel privaat als publiek ingevuld worden, waarbij het uitgangspunt geldt dat dit waar mogelijk privaat gebeurt. Iedere organisatie die aantoonbaar aan de afspraken van het eID Stelsel voldoet en toegelaten wordt tot het stelsel kan meerdere rollen vervullen en aanbieder worden van de bijbehorende diensten.

Figuur: illustratie van de samenwerking van een aantal rollen binnen het stelsel.



3.4 Gebruikersgemak bevorderen

Beoogde effect:

- De gebruiker kiest zelf hoeveel AUTHENTICATIEMIDDELEN hij wil gebruiken en voor welke diensten.
- Overstappen moet makkelijk kunnen op basis van eigen keuze, bijvoorbeeld:_:
  - nieuw middel, dan zelfde PSEUDOID;
  - tweede middel, dan zelfde PSEUDOID;
  - veranderen van AUTHENTICATIEDIENST, dan zelfde PSEUDOID.
- Het recht om vergeten te worden moet ook gehonoreerd kunnen worden. Dat houdt in: een AUTHENTICATIEMIDDEL niet meer willen gebruiken en bijvoorbeeld een andere aanschaffen.

Zolang de gebruiker hetzelfde AUTHENTICATIEMIDDEL gebruikt, wordt steeds dezelfde PSEUDOID gebruikt en blijft de koppeling met het 'klantnummer' van de DIENSTAANBIEDER in het koppelregister in tact. In de praktijk zullen echter veel gebruikssituaties voorkomen waarbij de gebruiker een ander AUTHENTICATIEMIDDEL gaat gebruiken. Bijvoorbeeld:

- ✓ Mijn middel is verlopen, ik krijg een nieuwe. Dan wil ik met mijn nieuwe middel nog steeds bij mijn bestaande klantaccount kunnen inloggen.
- ✓ Ik wil met een tweede middel kunnen inloggen bij een bestaand klantaccount.
- ✓ Ik stap over naar een andere AUTHENTICATIEDIENST en krijg daar een nieuw middel. Met dat nieuwe middel wil ik nog steeds kunnen inloggen bij een bestaand klantaccount.

Bovenstaande is als beeld te vergelijken met het nummerbehoud bij abonnementen van mobiele telefoons. De houder kan ervoor kiezen om bij wijziging van provider het mobiele nummer te behouden. Dezelfde werkwijze wordt ook ondersteund in het eID Stelsel. De houder van een middel moet zelf de keuze kunnen maken om aan een AUTHENTICATIEDIENST te verzoeken dat een nieuw middel dezelfde PSEUDOID'S genereert. De PSEUDOID'S zijn dan niet afhankelijk van het specifieke middel, maar zijn persistent gemaakt op persoonsniveau. Het voordeel hierbij is dat bij een nieuw middel de bestaande koppelingen bij diverse DIENSTAANBIEDERS intact blijven.

Om persoonlijke redenen (bijvoorbeeld privacy) kan een gebruiker ervoor kiezen om bij een nieuw AUTHENTICATIEMIDDEL juist wel nieuwe PSEUDOID'S te genereren. Om zijn bestaande klantaccount bij een DIENSTAANBIEDER dan te behouden, zal er wel een nieuwe koppeling tot stand moeten komen.

3.5 Opsporing en toezicht inrichten

Beoogde effect:

- Het toezicht op het eID Stelsel is ingericht.
- Fraude kan worden opgespoord.

Toezicht moet ervoor zorgen dat misbruik en falen van het eID Stelsel zoveel mogelijk wordt voorkomen. Wanneer een incident optreedt dan moet snel en adequaat kunnen worden ingegrepen.

Indien fraude is geconstateerd dan is het ondanks alle privacymaatregelen mogelijk dat een opsporingsdienst de identiteit van de betrokken personen kan opsporen. Dit moet uiteraard alleen mogelijk zijn op basis van een wettelijke verankering.

De drie ontwerpeisen:

- gebruikersgemak bevorderen,
- privacy garanderen, en
- toezicht en opsporing inrichten

zijn vanuit hun aard conflicterende eisen. Bij veel gebruikersgemak kan de privacy moeilijker worden gegarandeerd. Bij veel privacy bevorderende maatregelen is opsporing en toezicht weer moeilijker. Daarom wordt in het ontwerp van het eID Stelsel steeds een weloverwogen afweging gemaakt tussen deze drie ontwerpeisen.

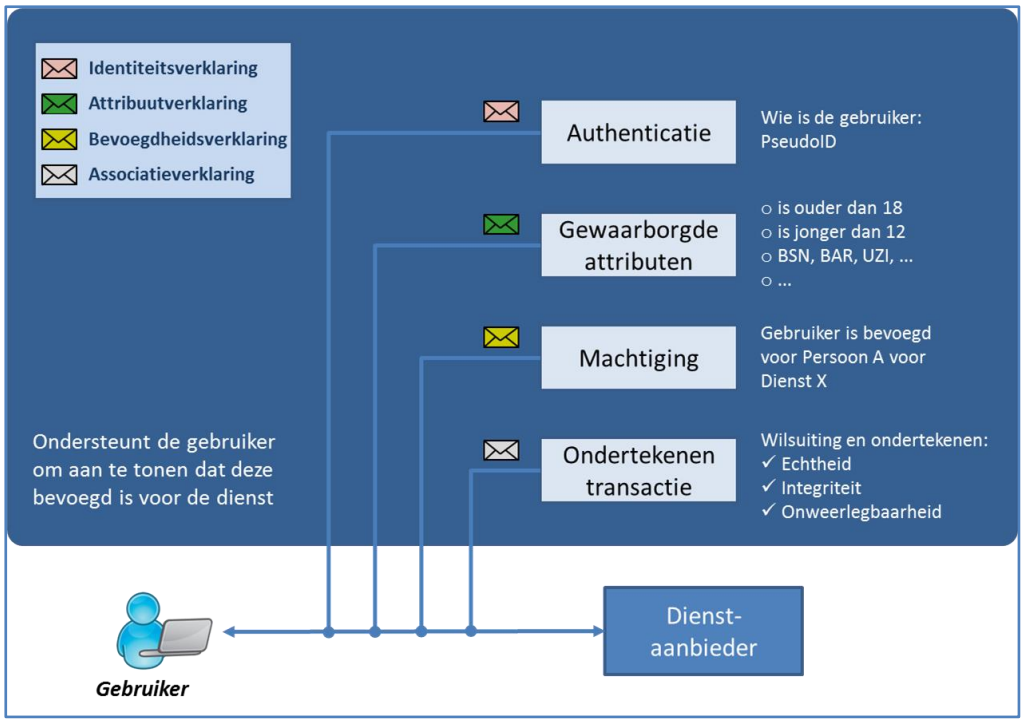
4 Basisinvulling van het eID Stelsel

In Hoofdstuk 3 werden de belangrijkste ontwerpeisen beschreven. In dit hoofdstuk wordt een eerste indruk gegeven van het ontwerp van het eID Stelsel.

- In de eerste paragraaf staat een overzicht met de belangrijkste componenten van het stelsel.
- In de tweede paragraaf staat beschreven hoe de identificerende verwijzing naar een persoon is vormgegeven. Deze verwijzing wordt de PSEUDOID genoemd.

4.1 De componenten van het eID Stelsel

In onderstaande figuur zijn de componenten van het eID Stelsel weergegeven.



Toelichting bij bovenstaande figuur:
De GEBRUIKER die online zaken wil doen met een DIENSTAANBIEDER, doet dat via het eID Stelsel op de volgende wijze.

- In het inlogscherm kiest hij de AUTHENTICATIEDIENST die zijn authenticatie kan doen. Hij authentiseert zich en de AUTHENTICATIEDIENST levert vervolgens een IDENTITEITSVERKLARING aan de DIENSTAANBIEDER met daarin de PSEUDOID van de GEBRUIKER, specifiek gericht aan de DIENSTAANBIEDER.
- Aanvullend kan er informatie verstrekt worden die toegang tot specifieke digitale diensten mogelijk maakt. Denk aan het voldoen aan een leeftijdsgrens of het handelen namens iemand anders. Deze informatie ontvangt de DIENSTAANBIEDER via een ATTRIBUUTVERKLARING en/of een BEVOEGDHEIDSVERKLARING. De GEBRUIKER moet hier wel expliciet toestemming voor geven.
- Tot slot kan de GEBRUIKER de transactie bevestigen via een online handtekening waarmee hij (digitaal) instemt met de inhoud van de transactie. Deze ondertekening wordt opgenomen in een ASSOCIATIEVERKLARING.

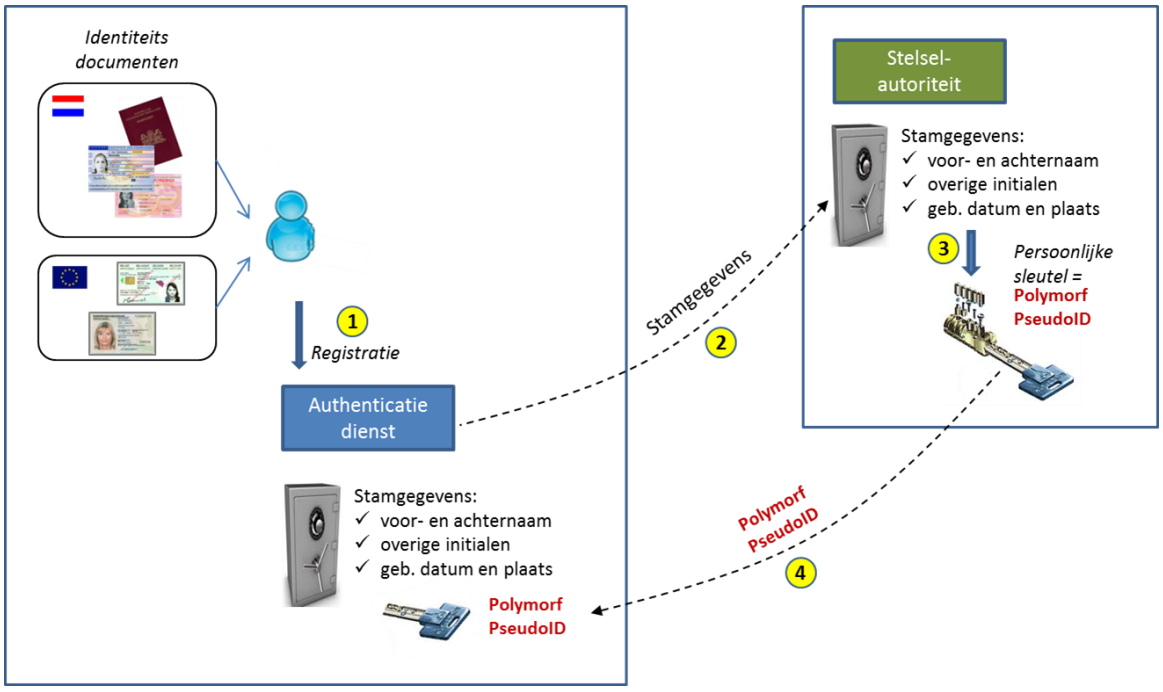
4.2 Berekening van een PSEUDOID

In Hoofdstuk 3 is de ontwerpeis 'waarborgen privacy' geïntroduceerd. Als ontwerpinvulling is daarbij het gebruik van zogenaamde PSEUDOID'S beschreven. Deze invulling is fundamenteel voor de gehele werking van stelsel. Zonder al te veel in de details te treden, wordt in deze paragraaf de essentie beschreven. Dat wordt in twee stappen toegelicht:

- In de eerste stap wordt het initiële proces beschreven waarbij een GEBRUIKER wordt opgenomen in het stelsel door een AUTHENTICATIEDIENST. Het resultaat is dat de GEBRUIKER daarna beschikt over een AUTHENTICATIEMIDDEL.
- In de tweede stap wordt het gebruik van het AUTHENTICATIEMIDDEL uitgelegd: het verstrekken van een PSEUDOID aan een DIENSTAANBIEDER.

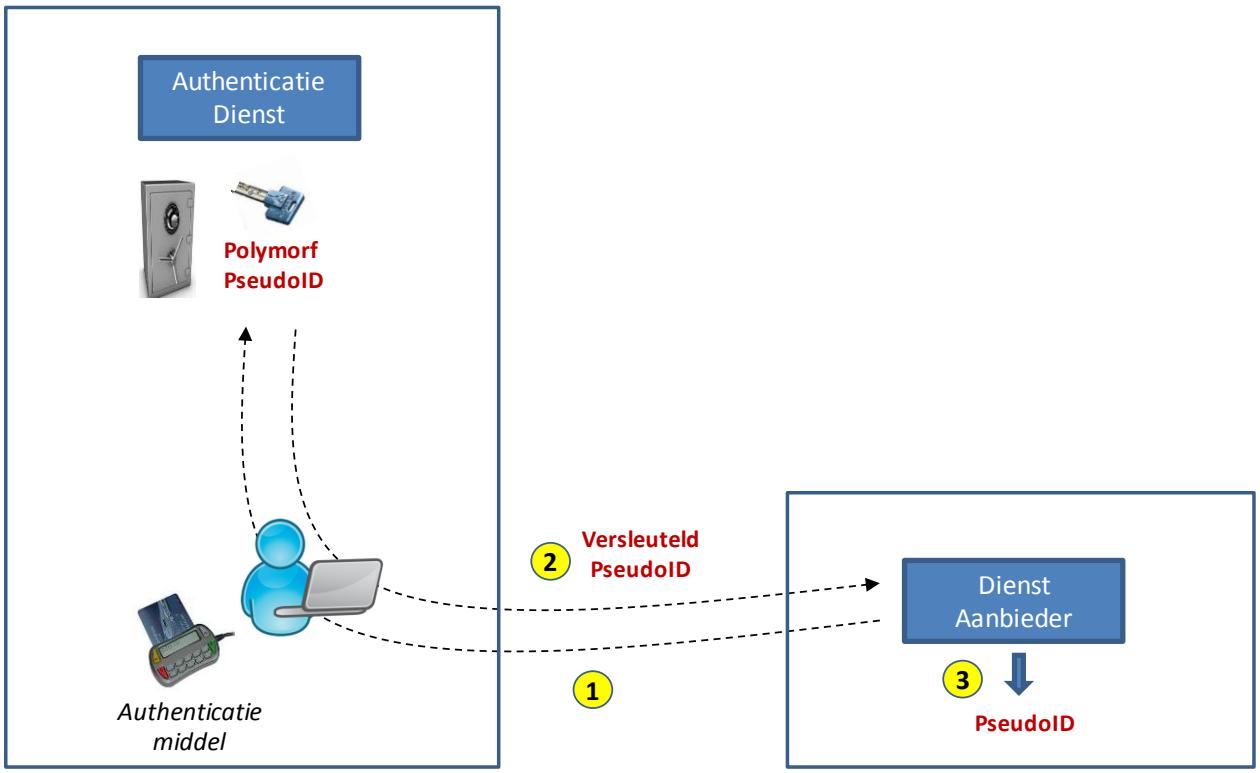
Stap 1: Inschrijving van een persoon bij een AUTHENTICATIEDIENST.

Als basis voor het registreren van de persoonskenmerken en daarmee de identiteit van de persoon, wordt een identiteitsdocument gebruikt. Voor elke persoon wordt een vaste set aan persoonsgegevens vastgelegd, in de figuur hieronder aangeduid met de term 'stamgegevens'. Deze stamgegevens vormen de basis voor de unieke sleutel van de persoon. De STELSELAUTORITEIT past een cryptografisch algoritme toe om op basis van onder andere de stamgegevens een unieke persoonsgebonden geanonimiseerde sleutel te berekenen, de zogenaamde POLYMORFE PSEUDOID.



1. Registratie van de persoon bij een AUTHENTICATIEDIENST.
2. AUTHENTICATIEDIENST verstuurt de stamgegevens van de persoon aan de STELSELAUTORITEIT.
3. De STELSELAUTORITEIT berekent op basis van de stamgegevens een persoonlijke sleutel van de persoon, aangeduid met de term POLYMORFE PSEUDOID.
4. De AUTHENTICATIEDIENST registreert de POLYMORFE PSEUDOID . De POLYFORME PSEUDOID is nu de persoonlijke sleutel van de GEBRUIKER om bij DIENSTAANBIEDER de verschillende (DIENSTAANBIEDER-specifieke) PSEUDOID'S te berekenen.

Stap 2: Gebruik van een AUTHENTICATIEMIDDEL bij een DIENSTAANBIEDER.
In de vorige stap heeft de GEBRUIKER bij de AUTHENTICATIEDIENST de beschikking over zijn POLYMORFE PSEUDOID. Vervolgens wil de GEBRUIKER inloggen bij een bepaalde DIENSTAANBIEDER. In het ontwerp is afgesproken dat een GEBRUIKER voor elke DIENSTAANBIEDER een andere PSEUDOID gebruikt. Die afspraak wordt in deze stap gerealiseerd. De POLYMORFE PSEUDOID wordt cryptografisch gecombineerd met een identificerend kenmerk van de DIENSTAANBIEDER. Het resultaat is een PSEUDOID die DIENSTAANBIEDER-specifiek is.



1. De GEBRUIKER wil inloggen bij een DIENSTAANBIEDER. De DIENSTAANBIEDER levert aan de AUTHENTICATIEDIENST zijn STELSELCERTIFICAAT (met daarin de naam en identiteit van de DIENSTAANBIEDER) en vraagt om een IDENTITEITSVERKLARING met daarin een voor de DIENSTAANBIEDER leesbare PSEUDOID van de GEBRUIKER. De GEBRUIKER voert vervolgens een authenticatiesessie uit bij de AUTHENTICATIEDIENST.

2. De AUTHENTICATIEDIENST herkent de GEBRUIKER op basis van deze authenticatiesessie en raadpleegt de persoonlijke sleutel van de GEBRUIKER (de POLYMORF PSEUDOID). De AUTHENTICATIEDIENST berekent op basis daarvan en op basis van de identiteit van de DIENSTAANBIEDER de PSEUDOID, die daarmee DIENSTAANBIEDER-specifiek wordt. Deze PSEUDOID wordt nog extra versleuteld, zodat alleen de DIENSTAANBIEDER deze kan lezen. Tijdens het transport heet deze dan de VERSLEUTELDE PSEUDOID.

3. DE DIENSTAANBIEDER ontvangt de VERSLEUTELDE PSEUDOID en ontsleutelt deze, zodat voor hem de PSEUDOID leesbaar wordt.