Ontwerp op hoofdlijnen van de werking van het eID Stelsel NL

Den Haag, 28 oktober 2013

Inhoudsopgave

Versienummer

07 juni 2013	Conceptversie
28 oktober 2013	In lijn gebracht met nota "Afwegingskader publieke diensten in het eID-stelsel" d.d. 19 september 2013

1 Inleiding

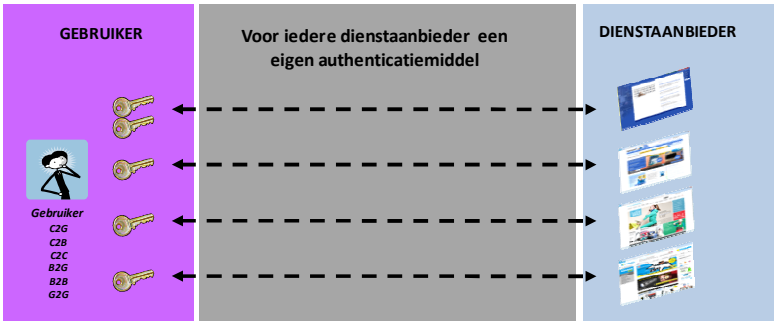
In dit document is een ontwerp op hoofdlijnen toegelicht voor de eerste fase van een nationale infrastructuur voor identificatie, authenticatie en vaststellen bevoegdheid voor het maatschappelijk verkeer via internet: het eID Stelsel NL.

Nu een steeds groter deel van het maatschappelijk verkeer via internet verloopt hebben burgers, bedrijven en de dienstaanbieders er belang bij laagdrempelig en met voldoende zekerheid te kunnen vaststellen wie er 'aan de andere kant van de lijn zit'. Daarnaast is van belang dat digitale transacties rechtsgeldig zijn en dat duidelijk is wat iemand mag: bij dat laatste kan het gaan om het aantonen dat een leeftijdsgrens is gepasseerd, maar ook dat iemand namens een bedrijf een elektronische handtekening mag zetten. Wat in de fysieke wereld wordt bereikt met persoonlijk contact, kopieën van paspoorten, op papier getekende contracten en verklaringen van de Kamer van Koophandel, moet ook mogelijk zijn in de online wereld.

De invoering van het eID Stelsel is een ontwikkelingstraject waarbij de invulling in overleg met overheid, markt en wetenschap tot stand moet komen. In dit document wordt de eerste basis beschreven voor deinhoudelijke invulling van het eID Stelsel NL. Centraal in dit ontwerp staan de rollen en verantwoordelijkheden van betrokkenen in een keten van digitale transacties en de (digitaal te leveren) verklaringen die de dienstaanbieders nodig hebben om deze rollen en verantwoordelijkheden te kunnen verifiëren.

Met het ontwerp van het eID stelsel worden de volgende resultaten beoogd:
- ✓ Gestandaardiseerde authenticatie en autorisatie invullingen voor alle transacties die via het digitale kanaal tot stand komen.
- ✓ Duidelijk op welke wijze privacy borging in het ontwerp is opgenomen.
- ✓ Zelfde gestandaardiseerde invulling voor natuurlijk en niet-natuurlijke personen, met als resultaat dat de invulling van authenticatie en machtigingen in het burger- en het bedrijven domein uitwisselbaar is.
- ✓ De standaard invulling moet onafhankelijk zijn van de verschillende technologieën die gebruikt worden bij de diverse soorten authenticatiemiddelen en invullingen van machtigingsregisters.
- ✓ Duidelijk en onderscheiden verantwoordelijkheden van de verschillende rollen van personen en partijen betrokken bij de totstandkoming van een digitale transactie.
- ✓ In de huidige praktijk van digitale dienstverlening is sprake van een grote diversiteit in de wijze waarop authenticatie en het vaststellen van de bevoegdheid is ingevuld. Het ontwerp biedt de mogelijkheid dat bestaande invullingen hergebruikt kunnen worden volgens dezelfde standaarden, zodat die bestaande invullingen uitwisselbaar worden.

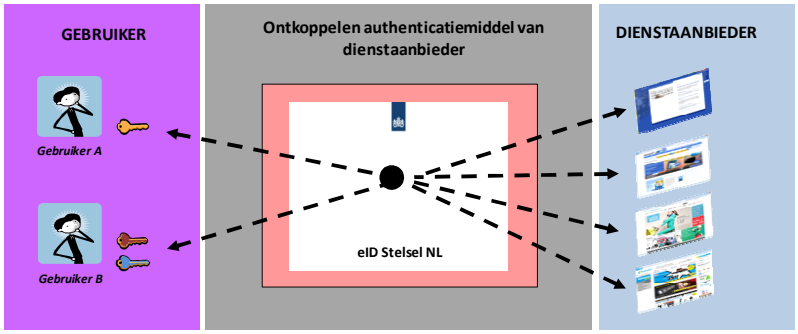
Als het bijvoorbeeld gaat om de invulling van authenticatie (wie ben je) dan is te zien dat veel dienstaanbieders nog zelf de authenticatie voor de gebruikers van hun diensten regelen. Dat is niet alleen deels het geval binnen de overheid. Maar ook op het terrein van webwinkels wordt de veelheid aan gebruikersnamen en wachtwoorden door consumenten als een probleem ervaren.



Binnen de overheid zijn de laatste jaren stappen gezet om het authenticatiemiddel te ontkoppelen van de dienstaanbieder. Voor het burgerdomein is DigiD geïntroduceerd en in het bedrijvendomein is het stelsel eHerkenning geïntroduceerd. Echter dit zijn nog steeds

gescheiden domeinen. De volgende stap is om publieke- en private authenticatiediensten onder te brengen in één stelsel, zodat de gebruiker en de dienstaanbieder zelf een eigen keuze kan maken in het authenticatiemiddel dat het beste bij zijn situatie past. En dat die gebruiker dan met het authenticatiemiddel van zijn keuze bij zoveel mogelijk dienstaanbieders terecht kan.

Dit uniforme stelsel wordt aangeduid met de naam eID Stelsel NL. Dit document beschrijft de onderdelen van het stelsel benodigd voor digitale dienstverlening, zodat op basis hiervan de resultaten van een uitgevoerde authenticatie en de vaststelling van de bevoegdheid worden gestandaardiseerd.



De basis voor het beschrijven van de werking van het stelsel is gebaseerd op drie pijlers:

- Definiëring van de rollen en verantwoordelijkheden van betrokkenen in een keten van digitale transacties.
- De gestandaardiseerde en uniforme invulling van de 'bewijsstukken' die nodig zijn om vast te kunnen stellen "wie ben je?" en "mag je dit?". Deze bewijsstukken worden in de vorm van verklaringen bij elke transactie gebruikt.
- 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. Toezichtregels voor bijvoorbeeld authenticatie zijn gebaseerd op het Europese STORK-model[1].

In hoofdstuk 2 wordt de context van het stelsel toegelicht. De eerste begrippen worden geïntroduceerd. Vervolgens wordt in hoofdstuk 3 ingegaan op de randvoorwaardelijke basis, namelijk het kunnen herkennen van iemands identiteit.

In de huidige praktijk van digitale transacties via internet zijn twee modellen gangbaar:

a. In het eerste model biedt de dienstaanbieder de transacties aan via een eigen webportaal. Voorbeelden zijn de portalen voor internetbankieren, de webwinkels en meer algemeen de diverse Mijnxxx portalen. In het eID stelsel wordt de ondersteuning van dit model aangeduid met de term het Portaal Model.
b. In het tweede model worden de transacties van de dienstaanbieder zonder directe menselijke tussenkomst door een applicatie-applicatie koppeling tot stand gebracht. Bijvoorbeeld een softwarepakket voor het opmaken van een aangifte Vennootschapsbelasting zendt deze aangifte geautomatiseerd in via Digipoort. In dit model stelt de dienstaanbieder geen webportaal (a), maar een webservice ter beschikking aan de afnemers van de transactie. In het eID stelsel wordt de ondersteuning van dit model aangeduid met de term het Webservice Model.

In hoofdstuk 4 wordt het Portaal model beschreven en in hoofdstuk 5 het Webservice model. In hoofdstuk 6 worden nog een aantal aanvullende onderwerpen geïntroduceerd. Deze onderwerpen, zoals bijvoorbeeld de opzet van een Dienstencatalogus, zijn nodig voor een juiste werking van het stelsel.

[1] www.eid-stork.eu

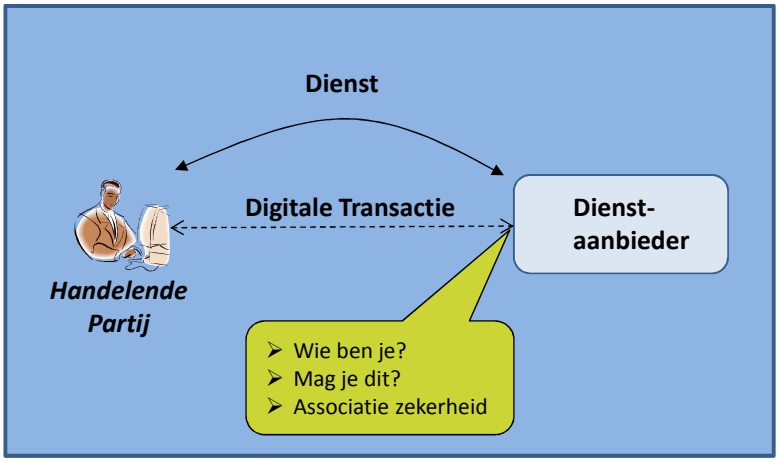
2 Context van het eID Stelsel NL

Dienstaanbieders (overheden en bedrijven) bieden natuurlijke- en niet-natuurlijke personen (burgers, consumenten, bedrijven en organisaties) in toenemende mate de mogelijkheid om hun diensten digitaal af te nemen. Ook de Nederlandse overheid en de Europese commissie stimuleren een verdergaande dienstverlening via internet, bijvoorbeeld het streven van de Nederlandse overheid om in 2017 alle transactiesvoor burgers en bedrijven digitaal beschikbaar te hebben.

Voor het aanbieden van digitale transacties zal elke dienstaanbieder een aantal vraagstukken op het terrein van geautoriseerde toegang moeten oplossen. Het eID stelsel is een ontwerp om die vraagstukken te uniformeren, zodat niet elke dienstaanbieder 'het wiel opnieuw' uitvindt. Het eID stelsel gaat dus niet over de inhoud van de digitale transacties, maar om een uniforme set van standaarden en afspraken voor geautoriseerde toegang tot digitale transacties.

In de context van het eID stelsel gaat het in principe om transacties die persoonsgebonden zijn. Dat hoeft niet altijd betekenen dat de identiteit eenduidig vastgesteld moet worden, maar het kan ook gaan om andere kenmerken van een persoon, bijvoorbeeld is de persoon ouder dan 16 jaar.

De basis van het ontwerp van het stelsel is het benoemen en eenduidig definiëren van een aantal begrippen. In onderstaande figuur zijn een aantal sleutelbegrippen weergegeven, met daaronder in tabelweergave de definitie.



Begrip	Toelichting
Persoon	Een natuurlijke- of niet-natuurlijke persoon. Een persoon is drager van rechten en plichten.
Handelende partij	Eenhandelende partij is een persoon (natuurlijk of niet-natuurlijk) die handelingen verricht, dan wel verantwoordelijkheid neemt voor de handelingen ten behoeve van het tot stand komen van een digitale transactie met een dienstaanbieder, als onderdeel van een dienst. Van een handelende partij moet de bevoegdheid worden vastgesteld. Deze bevoegdheid kan gebaseerd zijn op basis van de volgende invullingen: • De handelende partij handelt voor zichzelf als de belanghebbende. Een belanghebbende is degene wiens belang rechtstreeks bij de dienst is betrokken. In deze situatie is wel relevant of de handelende partij voor de gevraagde transactie handelingsbekwaam is. • De handelende partij handelt niet voor zichzelf, maar is specifiek voor die belanghebbende bevoegd vanwege het bestaan van een wettelijke

	vertegenwoordiging (zoals bestuurders van rechtspersonen, eigenaren van eenmanszaken en curatoren) of vanwege een door de belanghebbende verstrekte volmacht (een privaatrechtelijke volmacht op basis van artikel 3:60 BW of een bestuursrechtelijke machtiging op basis van artikel 2:1 Awb). • De handelende partij handelt niet voor zichzelf, maar is bevoegd vanwege de uitoefening van een in een register geregistreerde persoonsrol, bijvoorbeeld de persoon is ingeschreven in het BIG register.
Dienstaanbieder	Een dienstaanbieder is een persoon (orgaan) dat kenbaar heeft gemaakt dat het elektronisch bereikbaar is voor burgers en bedrijven, zodat zij als handelende partij in staat worden gesteld om digitale transacties in het kader van een dienst te kunnen uitvoeren.
Dienst	Een dienst is gericht op: • het tot stand komen van een rechtsbetrekking (het nemen van een besluit of een overeenkomst). • het leveren van een product. • het beantwoorden van een informatievraag. De dienst wordt gedefinieerd en aangeboden door een dienstaanbieder, die bepaalt welke eisen worden gesteld om de dienst te mogen afnemen. Deze eisen zijn: a. Het minimale STORK-betrouwbaarheidsniveau waarmee de handelende partij moet worden geauthenticeerd. b. Met welke mate van betrouwbaarheid de handelende partij wordt gebonden aan de inhoud van de transactie. c. Welk type identiteit is toegestaan (bijvoorbeeld alleen een RSIN-nummer of ook een KvK-nummer). d. Of het voor de dienst is toegestaan dat de handelende partij een niet-natuurlijke persoon mag zijn.
Digitale Transactie	In het kader van een dienst de onloochenbare totstandkoming van een verrichting tussen een handelende partij en een dienstaanbieder via een digitale weg.

Bij de zorgvuldige totstandkoming van een transactie zal de dienstaanbieder de volgende vraagstukken moeten invullen:

Wie ben je?
Bij het beantwoorden van deze vraag spelen twee begrippen een rol: identificatie en authenticatie. Bij identificatie en authenticatie gaat het erom dat voor de dienstaanbieder bekend wordt welke partij (natuurlijke of niet-natuurlijke persoon) gebruik wil maken van de dienst.

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-wachtwoord combinatie van DigiD. Het proces waarin een authenticatiemiddel als hulpmiddel voor identificatie wordt gebruikt, wordt aangeduid met de term authenticatie. Het proces van authenticeren wordt ondersteund door een authenticatiedienst (bijvoorbeeld de dienst DigiD in beheer bij 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. Zo heeft DigiD met gebruikmaking van een aanvullende SMS-code een hogere betrouwbaarheid, dan alleen de gebruikersnaam en wachtwoord combinatie.

In Europees verband is een standaard ontwikkeld om vergelijkbare betrouwbaarheidsniveaus eenduidig te beschrijven, genaamd de STORK-normering. Het moge duidelijk zijn dat een authenticatiedienst zelf hoogst betrouwbaar moet zijn, omdat een dienstaanbieder 'blind' op de

diensten van de authenticatiedienst moet kunnen vertrouwen. Dit vertrouwen wordt getoetst op basis van regelgeving en toezicht daarop.

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 dienst-aanbieder 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'. Op basis van bevoegdheids informatie over die persoon zal de dienstaanbieder een autorisatiebesluit nemen: krijgt de persoon wel of geen toegang. Het eID stelsel standaardiseert de wijze waarop aanvullende 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 belanghebbend bij de gevraagde dienst. Dit is een veel voorkomende situatie: de consument die voor zichzelf een boek bestelt, de rekening-houder 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 is de persoon minderjarig of is de persoon onder curatele is gesteld.

2. In deze situatie handelt de persoon niet voor zichzelf maar treedt op voor een andere belang-hebbende partij. De persoon is bevoegd gemaakt op basis van een vastgelegde specifieke bevoegdheidsrelatie tussen de persoon en de belanghebbende. Deze bevoegdheidsrelatie kan gebaseerd zijn op twee invullingen:

   - De bevoegdheid is vastgelegd door middel van een volmacht. Juridisch mag een volmacht vormvrij worden vastgelegd. Echter vormvrije volmachten lenen zich niet om via geautomati-seerde wijze de bevoegdheid te kunnen vaststellen. Dit staat een verdere uitbreiding van de gewenste dienstverlening via internet in de weg. Hiervoor is nodig een verdere ontwikkeling van digitale machtigingsregisters, zoals DigiD Machtigen en eHerkenning. De totstandkoming van de registratie van een machtiging is weliswaar vormvrij, maar moet voldoen aan normering vergelijkbaar met het STORK-model. De inhoud van een machtiging en de wijze waarop een machtigingsregister bevraagd kan worden, worden in het eID Stelsel gestandaardiseerd. Een machtigingsregister wordt beheerd door een machtigingsdienst. Een machtigingsdienst mag een verklaring afgeven, waarin is opgenomen dat een gemachtigde partij bevoegd is om te handelen namens een belanghebbende voor een bepaalde dienst. Op basis van deze verklaring kan dan de dienstaanbieder vaststellen of de handelende partij bevoegd is. Net als een authenticatiedienst moet ook het gestelde vertrouwen in een machtigingsdienst hoog zijn. Ook hiervoor is regelgeving en toezicht vereist.

   - De bevoegdheid is gebaseerd op een rechtelijke uitspraak, zodat er sprake is van een wettelijke vertegenwoordiging. Bijvoorbeeld een bewindvoerder bij faillissement. Op dit moment zijn registraties van wettelijke vertegenwoordiging nog niet (alle) geautomatiseerd raadpleegbaar.

3. Ook in deze situatie handelt de persoon niet voor zichzelf. Het verschil met situatie 2 is dat er geen specifieke bevoegdheidsrelatie naar de belanghebbende is vastgelegd, maar de persoon is ingeschreven in een specifiek register en aan deze inschrijving worden bevoegdheden 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).

Associatie zekerheid van de transactie

Het is voor zowel de handelende partij als voor de dienstaanbieder belangrijk dat de uitgevoerde transactie onbetwistbaaris en ook nadien onbetwistbaarblijft.In de papieren wereld wordt dit meestal ingevuld door het plaatsen van een handtekening op een document. Deze handtekening heeft drie functies:

- Met een handtekening kan iemands identiteit worden vastgesteld.
- Het dient ter vaststelling van de wil van de desbetreffende persoon met betrekking tot de inhoud van het document.
- De inhoud van het document wordt onlosmakelijk en integer aan de persoon gebonden.

In de digitale wereld is de behoefte aan een goede invulling van bovenstaande functies minstens zo belangrijk, wellicht nog van groter belang. Immers in de digitale wereld is de schaalgrootte van mogelijke fraude potentieel omvangrijk. Er zijn op dit moment diverse mogelijkheden als invulling van een elektronisch handtekening. De wet op de elektronische handtekeningen stelt: de elektronische handtekening moet voldoende betrouwbaar zijn, gelet op het doel waarvoor de elektronische gegevens worden gebruikt en op alle overige omstandigheden van het geval.

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 met cryptografische versleuteling. In de wet op de elektronische handtekeningen zijn dergelijke middelen beschreven.
- In het proces bij de dienstaanbieder 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…". Een andere mogelijkheid is dat gebruik wordt gemaakt van een aparte elektronische ondertekendienst.

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 geassocieerd. De wijze waarop dit gebeurd kan met verschillende invullingen. Net als dat bij authenticatie verschillende betrouwbaarheids niveaus worden onderkend, is dit ook het geval bij het associëren van de persoon aan de transactie.De toepassing van een gekwalificeerde elektronische handtekening levert een sterkere associatie op, dan het zetten van een 'vinkje'.De aard van de transactie zal veelal bepalen met welke mate van zekerheid de associatie moet worden ingevuld.

In de volgende hoofdstukken worden de drie vraagstukken: wie ben je, mag je dit en associatie zekerheid nader ingevuld.

3 Identificatie en authenticatiemiddelen

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: zeggen wie je bent.
b. Authenticatie: bewijzen die je zegt dat je bent.

Ad a. Identificatie
Bij identificatie gaat het om eenduidig de ene persoon van de andere persoon te kunnen onderscheiden. In theorie kunnen daar kenmerken zoals naam en geboortedatum voor gebruikt worden. In het eID stelsel wordt de voorkeur gegeven aan het gebruik van identificerende administratieve nummers; dit voorkomt dat het uitwisselen van de identiteit meteen ook het uitwisselen van persoonskenmerken impliceert. Een uniek administratief nummer garandeert dat de aanduiding identificerend is. In het dagelijkse leven zijn aan één natuurlijke persoon veel verschillende identificerende nummers gekoppeld. Denk aan burgerservicenummer, klantnummer bij de bank, klantnummer bij een verzekeraar, klantnummer bij een webwinkel, etc. Afhankelijk bij welke dienstaanbieder een transactie wordt afgenomen, zal steeds ander identificerende nummer van toepassing zijn.

Ad b. Authenticatie
Om als persoon via digitale weg te bewijzen wie je bent, wordteen hulpmiddelgebruikt. Dit hulpmiddel wordt aangeduid met de term authenticatiemiddel. Voorbeelden zijn een gebruikersnaam en wachtwoord combinatie of een bankpasje. Authenticatie is dan het proces waarin de persoon het authenticatiemiddel gebruikt om zijn identificatie claim te staven. In de huidige praktijk is het vaak zo dat een bepaald authenticatiemiddel specifiek bruikbaar is voor maar één dienstaanbieder, omdat dat authenticatiemiddel hard gekoppeld is aan één identificerend nummer en dat het authenticatiemiddel veelal is verstrekt door de dienstaanbieder zelf. Hiermee ontstaat voor de gebruiker een zogenaamde digitale sleutelbos.Het ontwerp van het eID stelsel moet het mogelijk maken dat deze digitale sleutelbos niet wordt opgedrongen, maar dat de 'sleutelbos' door de gebruiker zelf kan worden samengesteld.In de strategische verkenning van het eID stelsel is hierover het volgende opgenomen:

- ✓ Groeiende behoefte aan veilige(re) elektronische dienstverlening in private en publieke sector
- ✓ Hoog betrouwbare authenticatiemiddelen cruciaal
- ✓ Klantvriendelijk (geen digitale sleutelbos)
- ✓ Verminderen kwetsbaarheid van voorzieningen
- ✓ Scheiding burger/bedrijf niet altijd gewenst
- ✓ Privacy voldoende geborgd

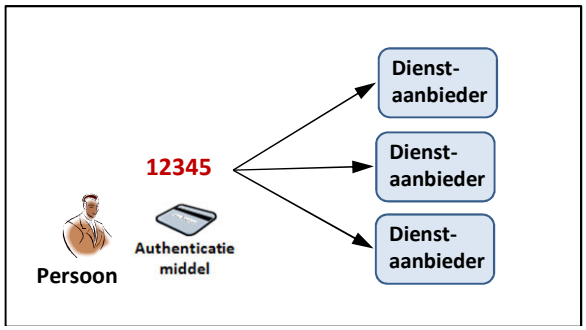
EN

- ✓ Burger en bedrijf hebben keuzevrijheid

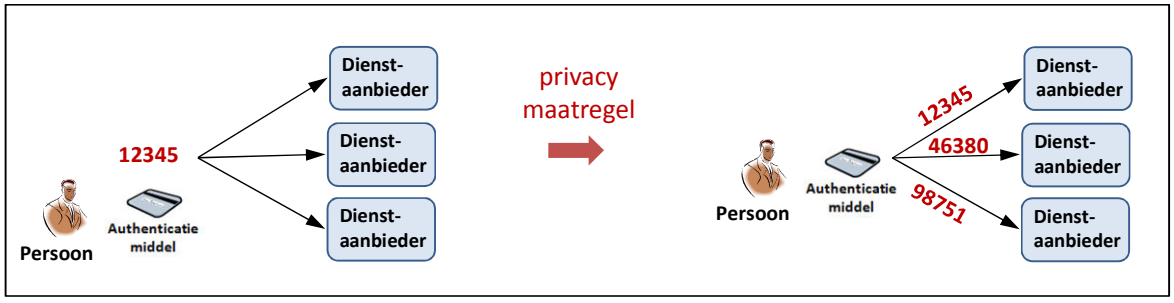
Het ontwerp en de daarop gebaseerde werking van het eID stelsel moet bovenstaande mogelijk maken.

Ontkoppeling authenticatiemiddel van dienstaanbieder

De eerste stap in het ontwerp is het ontkoppelen van het authenticatiemiddel van de dienstaanbieder. Daarbij moet het tevens mogelijk zijn om met één authenticatiemiddel terecht te kunnen bij meerdere dienstaanbieders.

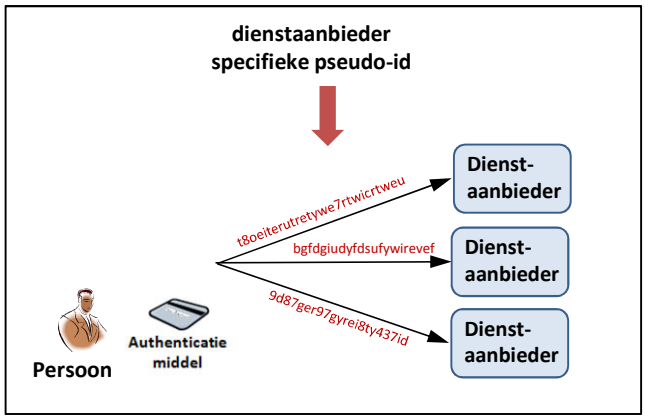


In bovenstaande figuur is weergegeven dat een gebruiker met één authenticatiemiddel terecht kan bij meerdere dienstaanbieders. In het voorbeeld verstrekt het authenticatiemiddel steeds hetzelfde identificerende nummer, namelijk '12345'. Dat is een eenvoudig ontwerp. Echter als er voor die dienstaanbieders geen wettelijke grondslag is om onderling informatie over dezelfde persoon uit te wisselen, dan wordt mogelijk de privacy van de persoon in kwestie geschaad. Het is dan nodig dat het authenticatiemiddel naar elke dienstaanbieder een ander identificerend nummer verstrekt. Vanwege de beoogde privacy borging is de eerste ontwerp maatregel dat een authenticatiemiddel verschillende identificerende nummers oplevert naar verschillende dienstaanbieders.



Een tweede maatregel is het ontkoppelen van de specifieke inrichting van de dienstaanbieder van de inrichting van de authenticatiediensten. Hiermee wordt bedoeld dat dienstaanbieders een eigen invulling kiezen van het administratieve identificerende nummer van 'de klant'. Het BSN, een klantnummer bij een bank, een klantnummer bij een webshop zijn voorbeelden van specifiek door de dienstaanbieder gekozen nummers. In het eID stelsel wordt als ontwerp principe gehanteerd dat de dienstaanbieder specifieke inrichting 'verborgen' blijft in het domein van de dienstaanbieder. De authenticatiediensten hebben op deze wijze geen beheerlast om bijvoorbeeld kopie bestanden aan te leggen van die klantnummers.

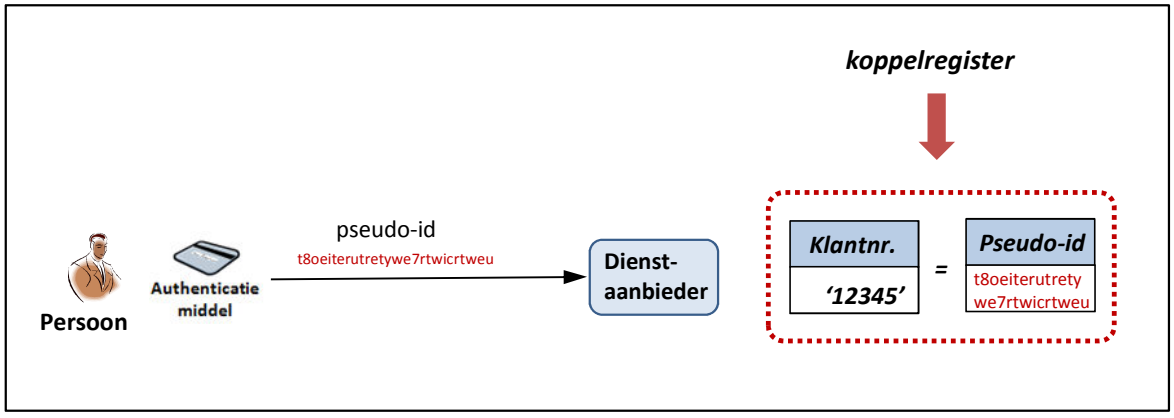
De authenticatiediensten standaardiseren op het verstrekken van een pseudo identificerend nummer (pseudo-id) aan een dienstaanbieder. Binnen het domein van alle authenticatiediensten is elke pseudo-id uniek en gekoppeld aan één bepaalde dienstaanbieder. Dit wordt aangeduid met de term dienstaanbieder specifieke pseudo-id. Deze pseudo-id's zijn persistent: iedere volgende authenticatie ten behoeve van dezelfde dienstaanbieder levert dezelfde pseudo-id op.



In het eID stelsel worden de pseudo-id's op basis van een rekenkundig voorschrift gegenereerd.

Koppelen pseudo-id met klantnummer van de dienstaanbieder

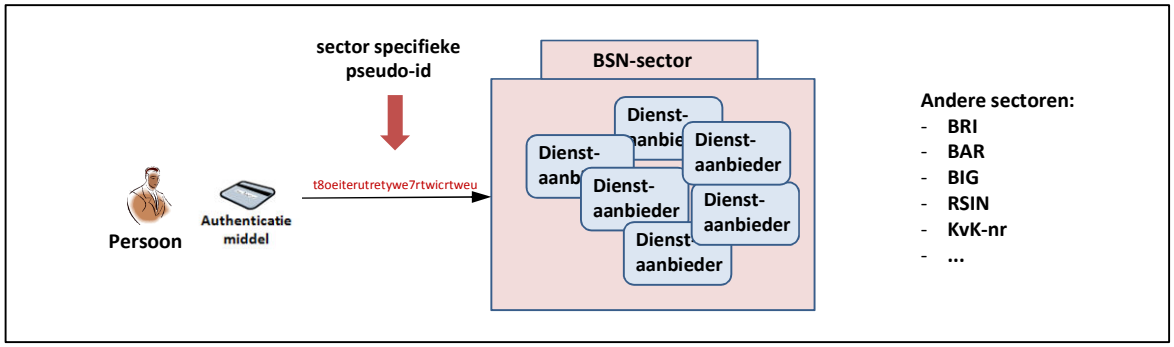
Conform de ontwerp principes van het eID stelsel levert elke authenticatie een dienstaanbieder specifieke pseudo-id op. De dienstaanbieder zal echter in veel gevallen dat pseudo-id willen koppelen aan het administratieve nummer waaronder de persoon bij de dienstaanbieder bekend staat (het eigen interne klantnummer). De eerste keer dat een nieuw pseudo-id aan een dienstaanbieder wordt verstrekt, zal ereenmalig een koppelproces doorlopen moeten worden. Het resultaat wordt vastgelegd in een zogenaamd koppelregister.



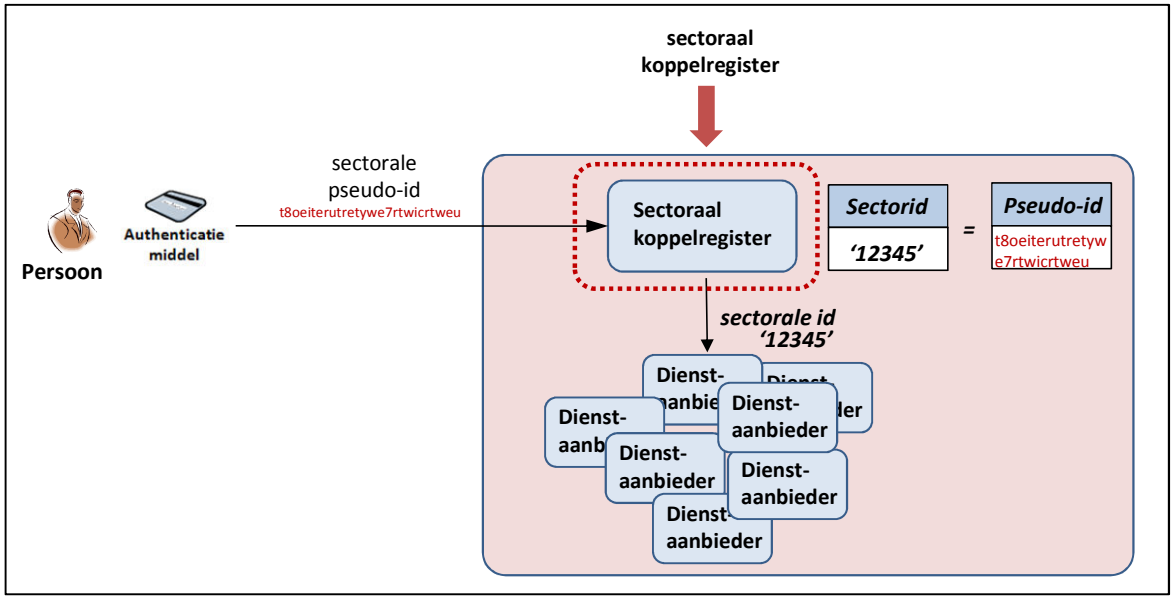
Het koppelproces kan via verschillende invullingen verlopen met daarbij verschillendeinvulling van betrouwbaarheid niveaus, analoog aan het normenmodel van STORK.

Het sector model: meerdere dienstaanbieders gebruiken hetzelfde identificerende nummer

Er zijn in Nederland een aantal sectoren waarin meerdere dienstaanbieders onderling gebruik maken van hetzelfde identificerende nummer van een persoon. Binnen een dergelijk sector bestaat een register waarin het sectorale nummer van de persoon is opgenomen. In dit geval moet de authenticatie niet een dienstaanbieder specifieke pseudo-id opleveren, maar een sector specifieke pseudo-id.



Per sector wordt een sectoraal koppelregister ingericht. In dit register wordt de koppeling geregistreerd tussen de pseudo-id en het sectorale nummer. De verantwoordelijkheid daarvoor ligt bij de sector zelf, inclusief het inrichten van het proces voor het koppelen van authenticatiemiddelen aan de identiteit binnen de sector. De wijze waarop deze koppeling tot stand komt en met welke verificatie controles, bepaalt de mate van betrouwbaarheid van de koppeling. In het eID Stelsel wordt een met Stork vergelijkbaar normenmodel voor het kwalificeren van het koppelproces opgesteld.



Persistentie en overdraagbaarheid van de pseudo-identiteit

Het eID stelsel ontwikkelt voorschriften op basis waarvan een authenticatiedienst een pseudo-id per dienstaanbieder of sector genereert. Het uitgangspunt is dat de authenticatiedienst ervoor zorgt dat het authenticatiemiddel van een persoon naar dezelfde dienstaanbieder of sector steeds dezelfde pseudo-id genereert, de pseudo-id dient persistent te zijn.

Zolang de gebruiker hetzelfde authenticatiemiddel gebruikt, wordt steeds dezelfde pseudo-id gebruikt en blijft de koppeling met het 'klantnummer' van de dienstaanbieder in het koppelregister intact. In de praktijk zullen echter veel gebruikssituaties voorkomen, waarbij de gebruiker een ander authenticatiemiddel gaat gebruiken. Bijvoorbeeld:

- ✓ Mijn authenticatiemiddel 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 authenticatiemiddel (naast mijn eerste) kunnen inloggen bij een bestaand klantaccount.
- ✓ Ik stap over naar een andere authenticatiedienst en krijg dan een nieuw authenticatiemiddel. Met dat nieuwe middel wil ik nog steeds kunnen inloggen bij een bestaand klantaccount.

Bovenstaande is als beeld te vergelijken met het nummerbehoud bij mobiele telefoon abonnementen.De houder kan ervoor kiezen om bij wijziging van provider het mobiele nummer te behouden. Deze zelfde lijn wordt ook ondersteund in het eID stelsel. De houder van een authenticatiemiddel moet zelf de keuze kunnen maken om aan een authenticatiedienst te verzoeken dat een nieuw authenticatiemiddel dezelfde pseudo-id's genereert. De pseudo-id's zijn dan niet afhankelijk van het specifieke authenticatiemiddel, maar zijn dan persistent gemaakt op persoonsniveau. Het voordeel hierbij is dat bij een nieuw authenticatiemiddel de bestaande koppelingen in de diverse koppelregisters intact blijven.

Om persoonsgebonden redenen (bijvoorbeeld privacy), kan een gebruiker ervoor kiezen om bij een nieuw authenticatiemiddel juist wel nieuwe pseudo-id's te genereren. Om zijn bestaande 'klantaccount' bij een dienstaanbieder dan te behouden, zal er wel een nieuwe koppeling tot stand moeten komen.

Er zijn meerdere invullingen mogelijk voor het realiseren van 'nummerbehoud'. Deze invulling wordt verder door de authenticatiediensten bepaald.

Bedrijfsgebonden authenticatiemiddelen

Een bedrijfsgebonden authenticatiemiddel wordt vooral toegepast in de situatie dat een medewerker van een bedrijf, namens dat bedrijf, een digitale transactie wil uitvoeren. De authenticatiedienst die het bedrijfsgebonden middel aan de medewerker heeft verstrekt, registreert welke bevoegdheden deze medewerker voor dat bedrijf heeft. Het gebruik van een bedrijfsgebonden authenticatiemiddel resulteert inzowel identificerende gegevens van het bedrijf als van de medewerker. De authenticatie-dienst beoordeeld tijdens het gebruik of het authenticatiemiddel mag worden gebruikt voor de gevraagde dienst (soms wel aangeduid met het controleren van een verticale machtiging binnen het bedrijf).

Definities

Begrip	**Toelichting**
Sector	Een groep van dienstaanbieders die onderling gebruik maken van hetzelfde identificerende administratieve nummer van een persoon.
Sectoraal nummer	Persoonsgebonden nummer dat gedeeld wordt in de gegevensuitwisseling tussen meerdere dienstaanbieders binnen een bepaalde sector. Voorbeelden: het BSN voor gebruik binnen de overheid en het BAR nummer dat gebruikt wordt voor het identificeren van advocaten.
Pseudo-id	Een door een authenticatiedienst gegenereerd betekenisloos identificerend nummer van een persoon.
Koppelregister	In dit register wordt de pseudo-id van een persoon gekoppeld aan het administratieve nummer waaronder de persoon bekend is bij de dienstaanbieder.
Sectoraal Koppelregister	In dit register wordt de pseudo-id van een persoon gekoppeld aan het sectorale nummer van die persoon.

4 Het Portaal model

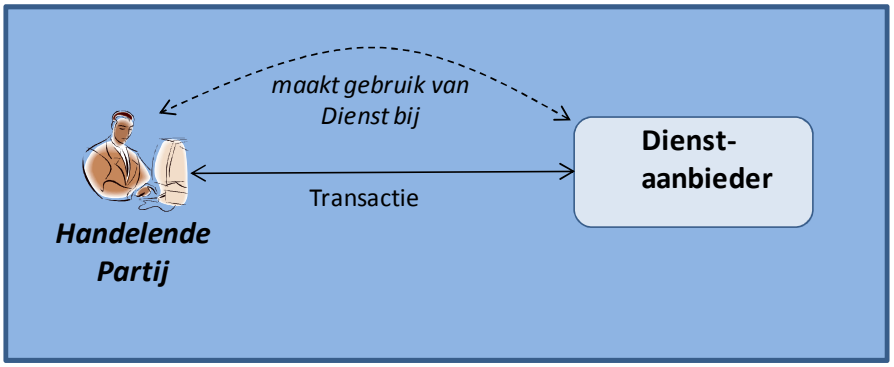
In dit hoofdstuk wordt het Portaal model beschreven. HetPortaal model beschrijft de veel voorkomende situatie dat een dienstaanbieder haar diensten via een ICT-voorziening (web portaal of software pakket) rechtstreeks zelf aanbiedt aan gebruikers. De dienstaanbieder zal de beslissing nemen of de gebruiker wel of niet geautoriseerd wordt (toegang krijgt) tot de gevraagde transactie. De kernbijdrage van het eID Stelsel is dat een dienstaanbieder niet meer zelf allerlei voorzieningen voor authenticatie en bevoegdheden hoeft in te richten, maar dat die dienstaanbieder het autorisatiebesluit kan baseren op basis van gestandaardiseerde berichten afkomstig van partijen die zich bekwamen in authenticatie- en machtigingsdiensten.

4.1 Eerste invulling van het Portaal Model

Kenmerkend voor het model van het eID-stelsel is dat precies wordt geduid wat de verschillende actoren zijn, die een rol spelen bij de totstandkoming van een digitale transactie. Elke rol van een actor wordt ingevuld door een persoon. Deze persoon is aanspreekbaar op zijn rechten en plichten die horen bij de betreffende rol.

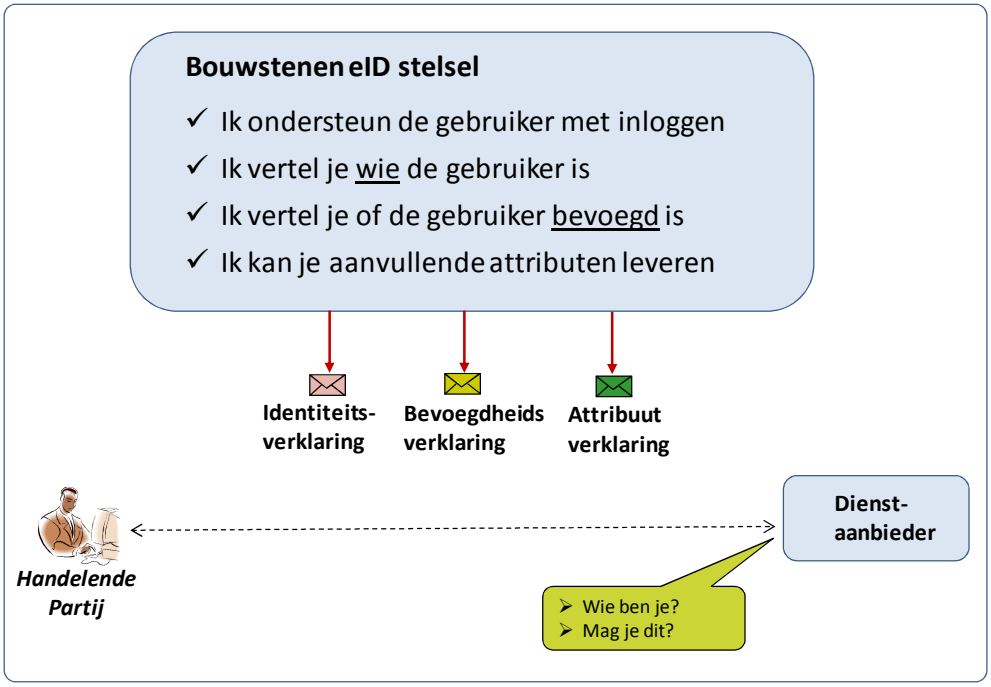
Het model van het eID-stelsel gaat over de totstandkoming van een dienst tussen een persoon en een dienstaanbieder, waarbij die dienst wordt afgenomen door middel van één of meerdere digitale transacties. Bijvoorbeeld een belastingplichtige is gehouden om de dienst Inkomstenbelasting met de dienstaanbieder Belastingdienst te regelen. De Belastingdienst stelt hiervoor meerdere digitale transacties ter beschikking, bijvoorbeeld het aanvragen van uitstel, het ophalen van een vooringevulde aangifte en het insturen van een ondertekende aangifte.

In de totstandkoming van een digitale transactie staan drie begrippen centraal: de Handelende partij die door middel van een transactie een Dienst afneemt bij een Dienstaanbieder. Hierbij zijn handelende partij en dienstaanbieder actoren en is het begrip dienst datgene wat hen bindt.



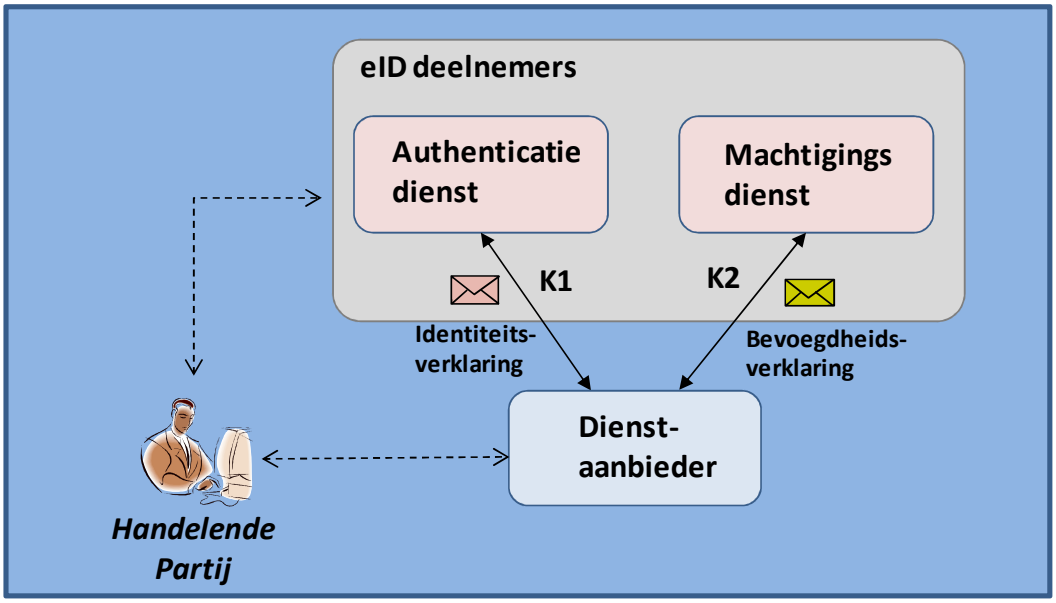
De dienstaanbieder wil kunnen vaststellen wie de handelende partij is en of deze voor de gevraagde dienst bevoegd is. De dienstaanbieder heeft ervoor gekozen om voor het beantwoorden van die vragen gebruik te maken van partijen die specifieke eID-diensten aanbieden. Deze partijen worden aangeduid met de aanduiding eID-deelnemer. De dienstaanbieder kiest er dus voor om die vraagstukken niet meer geheel 'in eigen huis' te organiseren, het ontzorgen van de dienstaanbieder. De dienstaanbieder blijft wel zelf verantwoordelijk om op basis van de aangeleverde resultaten van de eID-deelnemer te beslissen of de handelende partij toegang krijgt tot de dienst (het autorisatie besluit).

Het ontzorgen gebeurd door een aantal functies onder te brengen in het stelsel. In de onderstaande figuur zijn de vier belangrijkste ontzorg-functies van het eid stelsel benoemd.



De functies leveren gestandaardiseerde resultaten op naar de dienstaanbieder, zogenaamde verklaringen.De wijze waarop een functie wordt geïmplementeerd is aan de specifieke eid-deelnemer en worden als een dienst ontsloten. Voor het beantwoorden van de vraag 'wie ben je' wordt een authenticatiedienst onderkend. Voor het beantwoorden van de vraag 'mag je dit', wordt een eID-deelnemer van het type machtigingsdienst onderkend.

In onderstaand schema is weergeven op welke gestandaardiseerde wijze een dienstaanbieder gebruik kan maken van een authenticatie- en/of een machtigingsdienst.



Begrip	**Toelichting**
eID-deelnemer	Een eID-deelnemer is een organisatie die specifieke diensten aanbiedt op het terrein van authenticatie en het bepalen van de bevoegdheid. Elke eID-deelnemer is gebonden aan de standaarden en afspraken van het eID Stelsel. Tevens is elke eID-deelnemer onderhevig aan toezicht en handhaving.
Authenticatiedienst	Een authenticatiedienst is een eID-deelnemer en heeft als specifieke dienst het vaststellen van de identiteit van de handelende partij. De authenticatiedienst hanteert daarbij voor elke persoon een bestendige unieke persoonsaanduiding. Ter ondersteuning van het identificatie-proces stelt de authenticatiedienst een persoonsgebonden authenti-catiemiddel beschikbaar. Voor de invulling van het authenticatiemiddel kan een authenticatiedienst eigen technologie inzetten, bijvoorbeeld smartcard-technologie of het gebruik van mobiele telefoons. Ook de specifieke invulling van de authenticatiedialoog met de gebruiker wordt door de authenticatiedienst bepaald.
Identiteitsverklaring	Een identiteitsverklaring is een gestandaardiseerde verklaring waarin een identificerende eigenschap van de handelende partijis opgenomen. Voorbeelden zijn: BSN=123456789, KvK nr.=12345678, pseudo-identiteit = 1234567890ABCDEF.
Attribuutverklaring	Niet alle diensten van dienstaanbieders vereisen een eenduidige identificatie van de handelende partij, maar alleen of aanvullend een bepaalde eigenschap van de persoon. Bijvoorbeeld of de persoon ouder dan 18 jaar is. Ook een bepaalde persoonsrol wordt beschouwd als een attribuut van die persoon, bijvoorbeeld of de persoon advocaat is of dat de persoon erkend keurmeester is. Deze eigenschappen van een persoon worden aangeduid als attributen. De attributen worden verstrekt door een partij die voor die attributen verantwoordelijk is voor de juiste registratie van die attributen. Deze partij is een eID-deelnemer en verstrekt de attributen in de vorm van een attribuutverklaring. Alhoewel een identificerende eigenschap van een persoon ook een attribuut is, is er in dit model voor gekozen om de attribuutverklaring te onderscheiden van de identiteitsverklaring.
Koppelvlak K1	Een gestandaardiseerde communicatie interface voor de aanroep en het antwoord van een authenticatiedienst. Aanroep: - Identiteit van de dienstaanbieder - Het door de dienstaanbieder gevraagde minimaleSTORK-niveau voor authenticatie en een ja/nee waarde of een niet-natuurlijke persoonals handelende partij is toegestaan voor die dienst. Antwoord: - Identiteitsverklaring
Machtigingsdienst	Een machtigingsdienst is een eID-deelnemer en is de beheerder van een machtigingsregister. In een machtigingenregister worden op basis van een verstrekte volmacht de bevoegdhedenvan een gemachtigde persoon vastgelegd. Deze gemachtigde mag dan binnen de grenzen van de geregistreerde machtiging namens de belanghebbende digitaletransacties uitvoeren. De beheerder van het machtigingsregister moet erop toezien dat de machtigingen op een juiste wijze tot stand komen.
Bevoegdheids-verklaring	Een gestandaardiseerde verklaring waaruit blijkt dat één persoon een andere persoon mag vertegenwoordigen voor een bepaalde dienst. Voorbeelden zijn: KPMG mag de aangifte Omzetbelasting van Philips doen, BSN123456789 mag dienst X namens KvK12345678.
Koppelvlak K2	Een gestandaardiseerde communicatie interface voor de aanroep en het antwoord van een machtigigsdienst. Aanroep: - Identiteit van de dienstaanbieder - Identiteitsverklaring van de handelende partij - Identiteit van de belanghebbende - De door de handelende partij gevraagde dienst (of transactie) Antwoord: - Bevoegdheidsverklaring

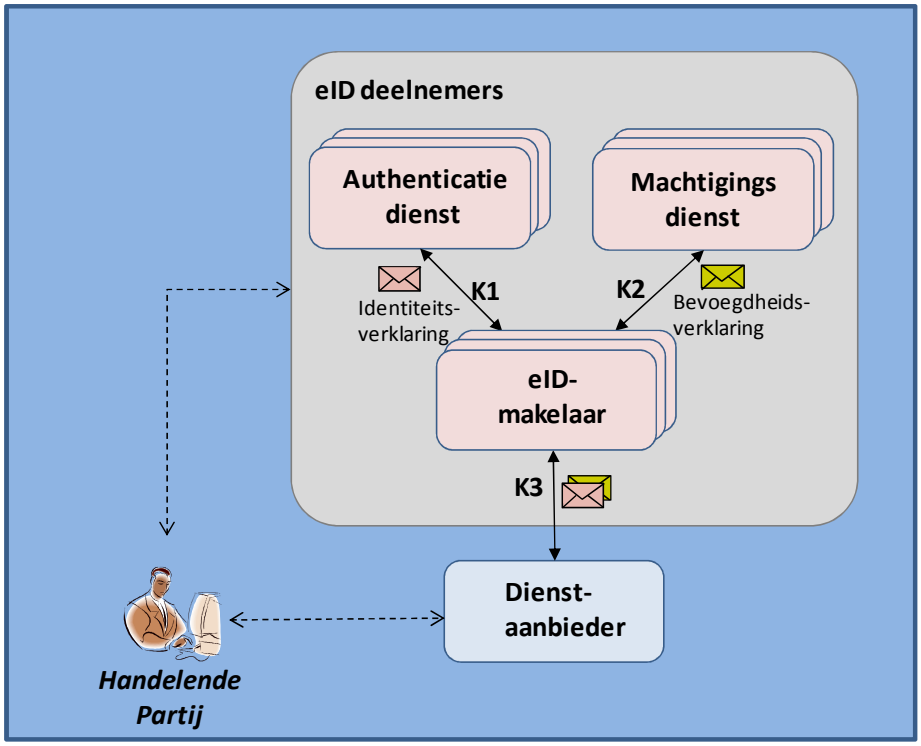
Elke identiteits- en bevoegdheidsverklaring wordt afgegeven door een verklaarder. De identiteit van de verklaarder moet met een hoogst mogelijke betrouwbaarheid worden vastgesteld. Dit niveau wordt gerealiseerd met behulp van het PKI-certificaat van de degene die de verklaring heeft opgesteld. Alleen als de handelende partij zelf in het bezit is van een PKI-certificaat, mag deze de identiteitsverklaring in eigen beheer afgeven.

4.2 Ontzorgen van de dienstaanbieder en de eID-deelnemer

Het ligt voor de hand dat er meerdere authenticatie- en machtigingsdiensten beschikbaar komen. Het is de taak van de dienstaanbieder om de handelende partij te ondersteunen om bijvoorbeeld bij de juiste authenticatiedienst 'terecht' te komen. Het is voor een dienstaanbieder dan beter om het leiden van de handelende partij naar de juiste authenticatiedienst via een gestandaardiseerde component in te vullen. In het eID Stelsel wordt dit mogelijk gemaakt door de component aangeduid met de term eID-makelaar.

Deze eID-makelaar functie heeft ook voor de eID-deelnemers een toegevoegde waarde. Het is bijvoorbeeld voor een authenticatiedienst niet aantrekkelijk om afzonderlijke koppelingen aan te leggen met een veelheid aan dienstaanbieders. Als voorbeeld kan het iDeal-model genoemd worden: in dat model zijn er slechts een beperkt aantal partijen die de makelaarsfunctie vervullen tussen de webwinkels en de banken.

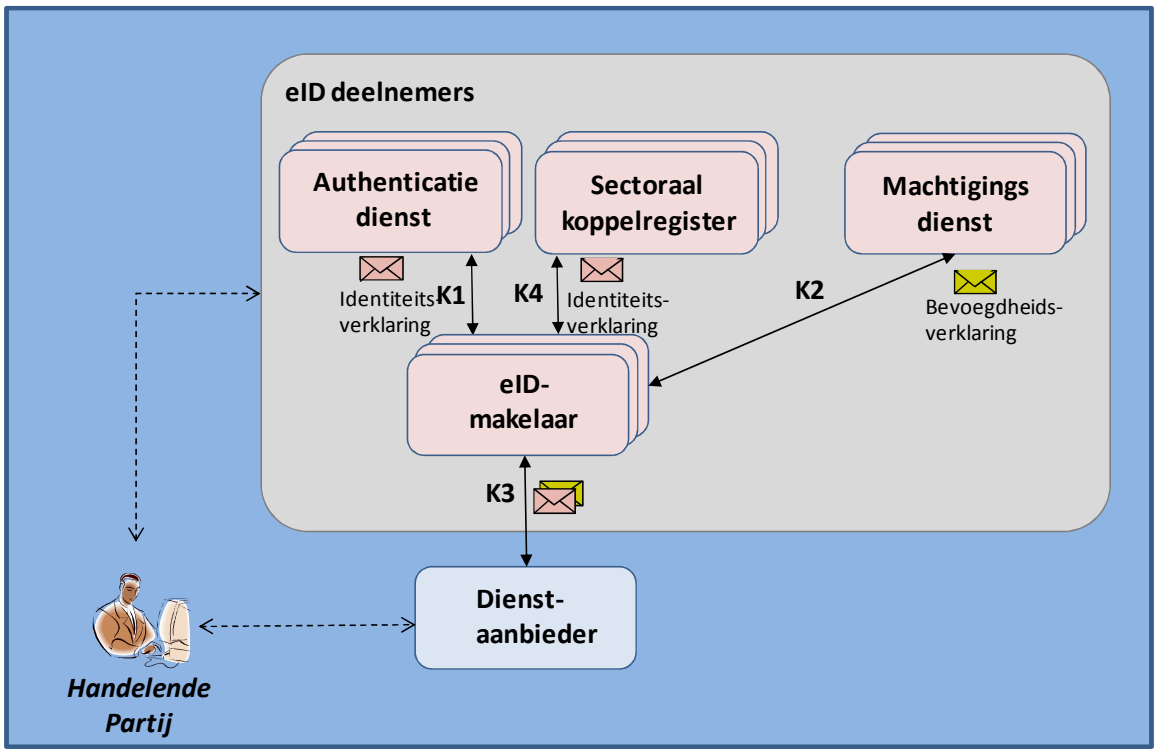
In onderstaand schema is de uitbreiding met de eID-makelaar weergegeven. Tevens is aangegeven dat de communicatie tussen eID-makelaar en dienstaanbieder door middel van een gestandaar-diseerd koppelvlak K3 wordt ingevuld.



Begrip	**Toelichting**
eID-makelaar	De eID-makelaar is een "single point of entry" van een dienstaanbieder naar eID-dienstverleners: - De eID-makelaar voert de dialoog met de handelende partij voor het selecteren van de gewenste authenticatiedienst. - De eID-makelaar voert de dialoog met de handelende partij voor het 'vinden' van het juiste machtigingsregister. De eID-makelaar controleert of alle benodigde verklaringen voor de gevraagde dienst beschikbaar zijn (de bevoegdheidsketen) en levert via een gestandaardiseerd koppelvlak de resultaten van de authenticatie- en machtigingsbevragingen terug aan de dienstaanbieder.
Bevoegdheidsketen	Een bevoegdheidsketen representeert een verifieerbare *keten van verklaringen* over identiteit en bevoegdheden zodanig dat de dienstaanbieder een autorisatiebesluit kan nemen voor het verstrekken van de gevraagde dienst. Alle schakels in een bevoegdheidsketen samen geven antwoord op de vraag "wie ben je?" en "mag je dit?".
Koppelvlak K3	Een gestandaardiseerde communicatie interface voor de aanroep en het antwoord van een eID-makelaar. Aanroep: - Identiteit van de dienstaanbieder in het geval de eID-makelaar een autonome voorziening is - Identiteit van de belanghebbende - De door de handelende partij gevraagde dienst (of transactie) Antwoord: - Bevoegdheidsketen, de verzamelde identiteits- en bevoegdheidsverklaringen.

4.3 Gebruik van sectorale pseudo-identiteiten

In hoofdstuk 3 is het gebruik van pseudo-id's en sectoren toegelicht. In dit hoofdstuk wordt die invulling geoperationaliseerd. De werking is in onderstaand schema weergegeven.



Als een persoon een authenticatiemiddel gebruikt, wordt door de authenticatiedienst de identiteitsverklaring geleverd. In deze identiteitsverklaring is de sectorale pseudo-id opgenomen. De betreffende dienstaanbieder kent echter alleen het sectorale nummer van de persoon. De eID-makelaar verstuurt daarom aan het sectoraal koppelregister de ontvangen identiteitsverklaring met het verzoek het bijbehorende sectorale nummer aan te leveren. Het sectorale koppelregister verstrekt, na controle of de persoon nog geldig is binnen de sector, een nieuwe identiteitsverklaring waarin het sectorale nummer is opgenomen.

Begrip	**Toelichting**
Koppelvlak K4	Een gestandaardiseerde communicatie interface voor de aanroep en het antwoord van een sectoraal koppelregister. Aanroep: - Identiteitsverklaring op basis van pseudoID, specifiek voor de sector; Antwoord: - Identiteitsverklaring op basis van sectoraal nummer (bijvoorbeeld BSN).

Procesverloop beschrijving hoe het inloggen bij het portaal model verloopt.

Het verkrijgen van online toegang bij een dienstaanbieder vindt plaats in vier stappen:

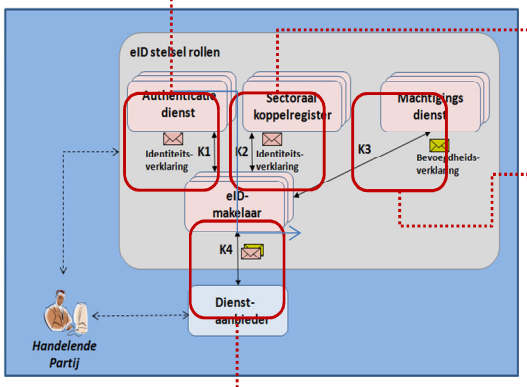
1. Authenticatie
   De gebruiker gebruikt een authenticatiemiddel en verstrekt daarmee de pseudo-id.

2. Identiteit koppeling
   De pseudo-id wordt omgewisseld naar het voor de dienstaanbieder herkenbare 'klantnummer'.

3. Controleren bevoegdheid
   In deze optionele stap wordt de juiste bevoegdheden gecontroleerd.

4. Autorisatiebesluit
   Uiteindelijk is het de verantwoordelijkheid van de dienstaanbieder of de gebruiker daadwerkelijk toegang krijgt tot de gevraagde dienst. De dienstaanbieder neemt deze beslissing mede op de door deelnemers van het eID stelsel aangeleverde verklaringen.

Procesverloop inloggen bij een webportaal



Authenticatie

1. Gebruiker surft naar dienstaanbieder en klikt op inloggen.
2. eID makelaar neemt het over van de dienstaanbieder en ondersteunt de gebruiker bij het inloggen en voor het ophalen van de bevoegdheid.
3. Gebruiker geeft aan welk authenticatiemiddel gebruikt wordt (vergelijkbaar met een iDeal-keuze).
4. eID makelaar routeert de gebruiker naar de juiste authenticatiedienst.
5. Gebruiker voert authenticatie uit -> resultaat is een identiteitsverklaring welke via koppelvlak K1 wordt doorgegeven aan de eID makelaar.

Identiteit koppeling

6. De ontvangen pseudo-id wordt omgezet naar een voor de dienstaanbieder herkenbare (sector) identiteit -> resultaat is een nieuwe identiteitsverklaring welke via koppelvlak K2 wordt doorgegeven aan de eID makelaar.

Controleren bevoegdheid

7. eID makelaar vraagt of de gebruiker voor zichzelf komt of voor een ander, in geval dat laatste dan wordt gevraagd bij welke machtigingsdienst de machtiging is geregistreerd.
8. eID makelaar verzoekt machtigingsdienst om bewijs van bevoegdheid aan te leveren -> resultaat is een bevoegdheidsverklaring welke via koppelvlak K3 wordt doorgegeven aan de eID makelaar.

Autorisatiebesluit

9. eID makelaar controleert of de bevoegdheidsketen volledig is en levert de ontvangen verklaringen op aan d dienstaanbieder via koppelvlak K4
10. Op basis van de ontvangen verklaringen kan de dienstaanbieder een autorisatiebesluit nemen.

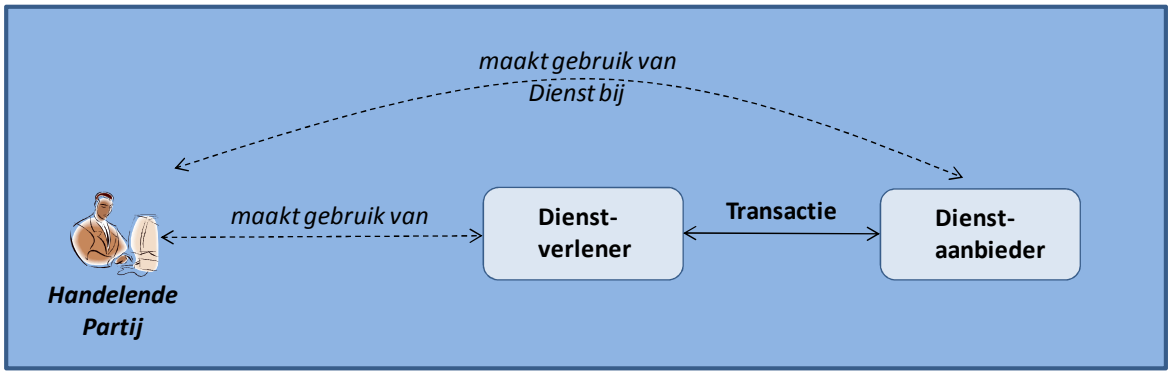
5 Het Webservice Model

5.1 De dienstverlener als intermediair tussen handelende partij en dienstaanbieder

Het Portaal model is beschreven vanuit het perspectief dat een dienstaanbieder rechtstreeks de handelende partij ondersteunt voor het realiseren van een dienst. Er zijn echter situaties dat die dienstaanbieder niet meer zelf de diensten rechtstreeks aanbiedt, maar dat een andere intermediaire persoon de handelende partij ondersteunt. Bijvoorbeeld een intermediaire partij biedt een web portaal aan waarmee door een bedrijf een aangifte omzetbelasting kan worden opgemaakt. Via dat portaal verstuurt het bedrijf vervolgens de aangifte omzetbelasting naar de dienstaanbieder Belastingdienst. Een ander voorbeeld is dat een handelende partij gebruik maakt van een softwarepakket en vanuit dat softwarepakket wordt informatie uitgewisseld met een (overheid)dienstaanbieder.

In bovenstaande situaties is te zien dat er in het tot stand komen van transacties in het kader van een dienst tussen handelende partij en dienstaanbieder een aanvullende persoonsrol is ontstaan. Deze persoonsrol wordt in het model aangeduid met de term dienstverlener. Dit is een uitbreiding op het Portaal model en wordt aangeduid als het Webservice model van het eID stelsel.

De dienstverlener communiceert 'onder water' met de dienstaanbieder via een applicatie-naar-applicatie invulling.

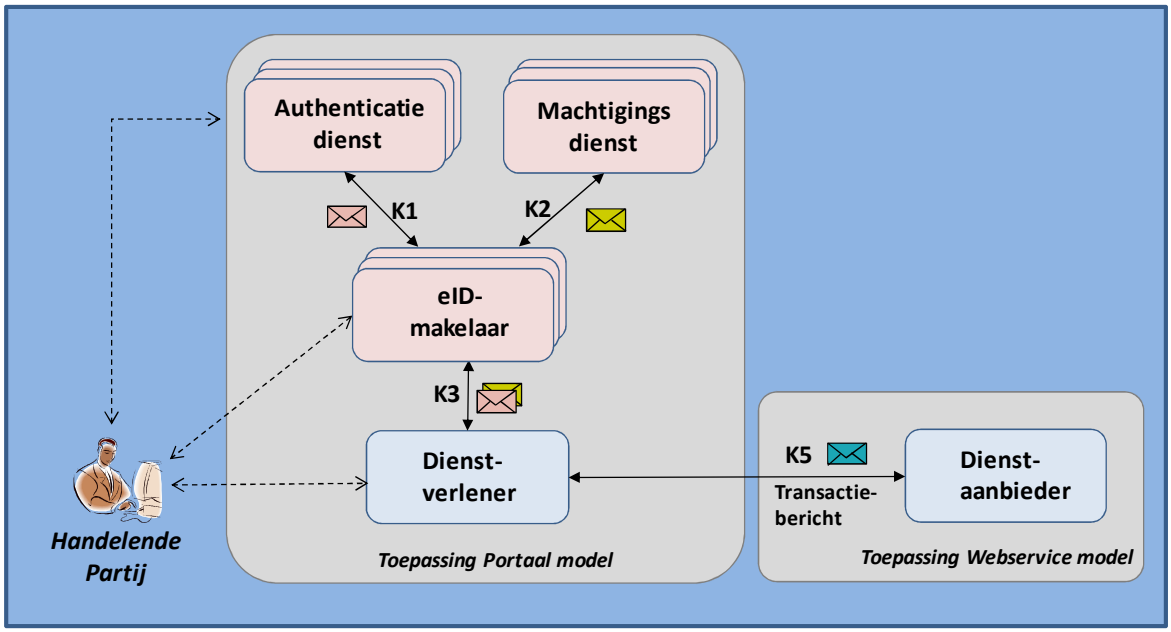


Net als in het Portaal model stelt de dienstaanbieder de eisen ten aanzien van authenticatie en de benodigde bevoegdheid. Immers de dienstaanbieder blijft ook in het Webservice model eigenaar van de dienst. De dienstaanbieder bepaalt of de handelende partij, weliswaar via tussenkomst van een dienstverlener,geautoriseerd wordt voor de gevraagde transactie bij de dienstaanbieder. Conform het Portaal model baseert de dienstaanbieder het autorisatiebesluit op de aangeleverde identiteits- en bevoegdheidsverklaringen. Deze verklaringen worden nu niet via een eID-makelaar aangeleverd, maar worden door de dienstverlener aangeleverd. De dienst-verlener stelt voor de dienstaanbieder een transactiebericht samen. In het transactiebericht zijn naast de inhoudelijke gegevens bestemd voor de dienst, tevens de benodigde identiteits- en bevoegdheidsverklaringen gevoegd.

Voordat de dienstverlener het transactiebericht kan opstellen, zal de dienstverlener eerst moeten zorgen dat de identiteits- en bevoegdheidsverklaringen met behulp van de handelende partij beschikbaar komen. De wijze waarop de dienstverlener dit realiseert is geheel volgens het Portaal model van het eID Stelsel.

5.2 Invulling van het Webservice Model

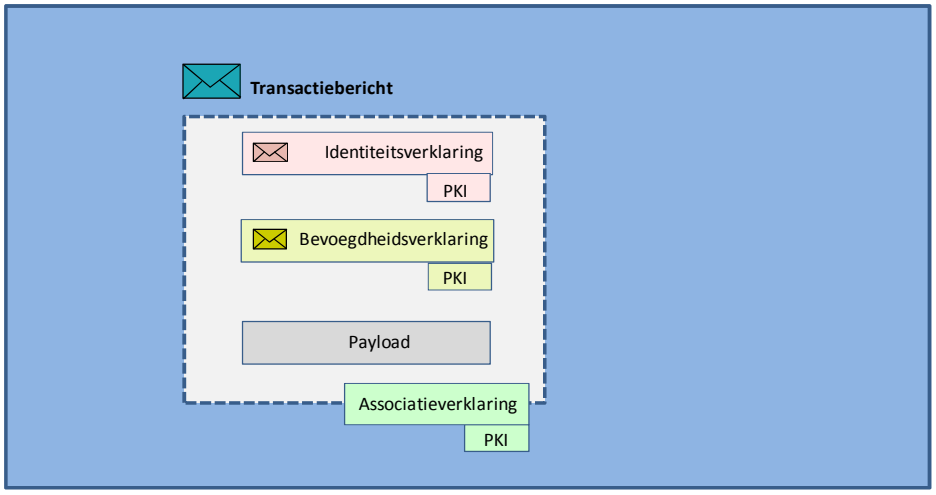
In onderstaand schema wordt de invulling van het Webservice model weergegeven.



Begrip	Toelichting
Dienstverlener	Dedienstverlener is verantwoordelijk voor de juiste totstandkoming van het transactiebericht dat wordt verstrekt aan de dienstaanbieder. De verantwoordelijkheid betreft het samenstellen en controleren van de keten van verklaringen benodigd voor de transactie en het op een betrouwbare wijze verbinden van deze keten aan de inhoud van de transactie. De dienstverlener geeft over de keten de associatieverklaring af. De dienstverlener draagt overigens anders dan de consistentie en integriteit geen inhoudelijke verantwoordelijkheid voor de geassocieerde verklaringen. Het samenstellen en controleren vindt plaats door middel van een ICT-voorziening waarmee de transactie tussen de dienstverlener en dienstaanbieder wordt afgehandeld.
Transactiebericht	Naast de inhoud van het bericht (de payload) zijn onderstaande eID-elementen op een standaardwijze opgenomen in elk transactiebericht. - Identiteitsverklaring van de Handelende Partij - Bevoegdheidsverklaring(en) van de Handelende Partij - Associatieverklaring
Associatieverklaring	Het doel van de associatieverklaring is om de verschillende andere verklaringen te bundelen en deze samenstelling niet meer wijzigbaar te maken. Dit voorkomt misbruik van de andere verklaringen. De associatieverklaring wordt opgesteld door de dienstverlener die de verschillende verklaringen verzamelt. In de verklaring wordt aangegeven met welke mate van betrouwbaarheid de associatie heeft plaatsgevonden (de associatie zekerheid).
Koppelvlak K5	Een gestandaardiseerde communicatie interface voor de applicatie service aanroep en het antwoord van een dienstaanbieder met betrekking tot authenticatie- en autorisatie informatie. Aanroep: - transactiebericht Antwoord: - resultaatbericht

5.3 Het transactiebericht nader beschouwd

Op dit moment komen er in de samenleving vele variaties voor in de wijze waarop de invulling van authenticatie en bevoegdheid via een transactiebericht wordt uitgewisseld. De kracht van de eID stelsel standaard voor het transactiebericht is dat deze standaard toepasbaar is op de vele verschijningsvormen die nu zijn ontstaan. De standaard geeft een impuls aan vereenvoudiging en hergebruik van de standaard voor de diverse berichtstromen, waarbij deze nu veelal een eigen invulling hebben.



6 Aanvullende onderwerpen eID stelsel

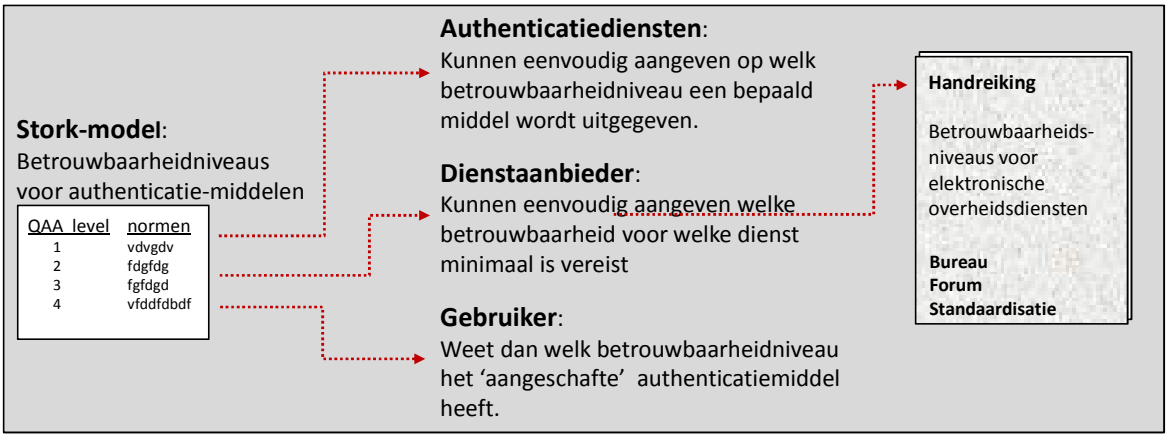
6.1 Gebruik van kwalificatiemodellen als basis voor Toezicht

Het eID stelsel is erop gericht om standaarden te ontwikkelen voor authenticatie en autorisatie, als basis voor digitale transacties. Een dienstaanbieder die ervoor kiest om diensten via internet toegankelijk te maken, dient ervoor te zorgen dat die diensten op een voldoende beveiligde en betrouwbare wijze toegankelijk zijn. Voor elke dienst zal de dienstaanbieder de volgende aspecten van de digitale transactie moeten beoordelen:

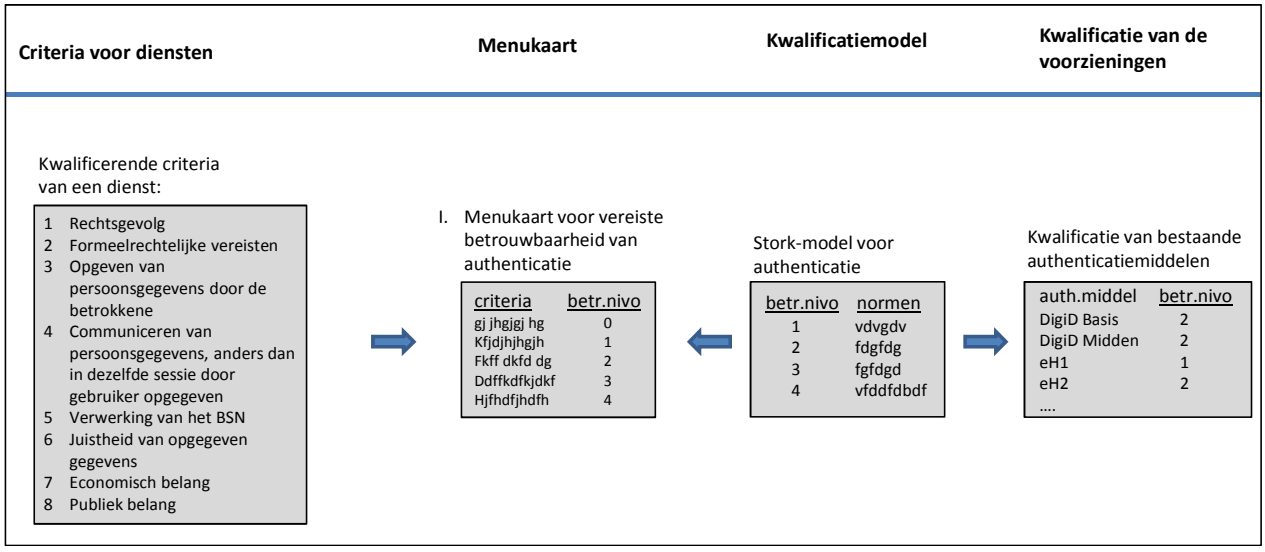
1. Wat is het vereiste betrouwbaarheidsniveau waarmee de identiteit van de handelende partij moet worden vastgesteld.
2. Is het toegestaan dat de dienst niet door de belanghebbende zelf, maar door een gemachtigde (anders dan een wettelijke vertegenwoordiger) wordt afgenomen. Indien dat zo is, met welke mate van betrouwbaarheid moet dan, naast de identiteit, tevens de bevoegdheid van die gemachtigde worden vastgesteld.
3. In het geval de handelende partij gegevens inzendt naar de dienstaanbieder moet worden bepaald met welk betrouwbaarheidsniveau de integriteit van de inhoud van het bericht of elektronisch geschrift gewaarborgd wordt. Naast technische integriteit wordt hier vooral bedoeld de bevestiging door de ondertekenaar (wilsuiting) dat dit inderdaad de gegevens zijn die hij bedoelde in te sturen. Daarmee wordt tevens bereikt dat de inhoud van het bericht of elektronisch geschrift onloochenbaar aan de ondertekenaar is gekoppeld. Voorgaande onderwerpen worden gebundeld in het begrip 'de associatie zekerheid' van een transactie.

Voor elke digitale dienst zal de dienstaanbieder de bovenstaande beoordeling moeten maken. Om de dienstaanbieder hierbij een handvat te geven, is door het Bureau Forum Standaardisatie een Handreiking Betrouwbaarheidsniveaus opgesteld. Deze handreiking levert een praktische uitleg op welke wijze de dienstaanbieder een dienst kan kwalificeren in termen van het gewenste betrouwbaarheidsniveau van identificatie en authenticatie. Deze handreiking zorgt daarmee voor meer uniformiteit in de kwalificatie van alle overheidsdiensten.

Op basis van een uitgewerkte 'menukaart' kan de dienstaanbieder een dienst kwalificeren op het vereiste authenticatieniveau. De basis van deze uitwerking is de toepassing van het kwalificatiemodel voor authenticatie, genaamd het STORK-model. Op basis van een aantal kwalificerende criteria is een model opgesteld waarmee authenticatiemiddelen ten opzichte van elkaar gewogen kunnen worden.



In de handreiking is voor het onderdeel authenticatie een raamwerk ontwikkeld voor het kunnen beoordelen van een dienst om zo het gewenste betrouwbaarheidsniveau vast te stellen. In onderstaand schema zijn de onderdelen weergegeven.



Het model bestaat uit de volgende onderdelen:

a. Criteria voor diensten: een indeling in criteria die een bepaalde eigenschap van een dienst beschrijven. De aanname daarbij is dat elke criterium een bepaalde invloed heeft op het gewenste betrouwbaarheidsniveau. Bijvoorbeeld het criterium rechtsgevolg: elektronische handelingen met aanzienlijke rechtsgevolgen vereisen een hogere betrouwbaarheid dan handelingen met beperkte rechtsgevolgen.
b. Kwalificatiemodel: een kwalificatiemodel van authenticatiemiddelen, in dit geval ingevuld door het Stork-model. Dit model beschrijft de verschillende betrouwbaarheidsniveaus die voor authenticatiemiddelen zijn te onderkennen.
c. Menukaart: vervolgens worden de modellen van a en b samengebracht tot een praktische invulling in de vorm van een menukaart. Op basis van de menukaart kan een dienstaanbieder relatief eenvoudig zijn diensten kwalificeren. Daarbij geldt als aandachtspunt dat in gevallen waarin formeelrechterlijke eisen ontbreken, de aanbieders in het veld van de rechtspleging en juridische beroepen erop moeten kunnen vertrouwen dat de rechter geen van de menukaart afwijkend oordeel zal hebben over de betrouwbaarheid van de elektronische geschriften die hem door tussenkomst van de dienstaanbieders wordt voorgelegd.
d. Kwalificatie van de beschikbare voorzieningen: het Stork-model uit b kan ook gebruikt worden om bestaande authenticatiemiddelen, zoals DigiD Basis en eHerkenning, te kwalificeren.

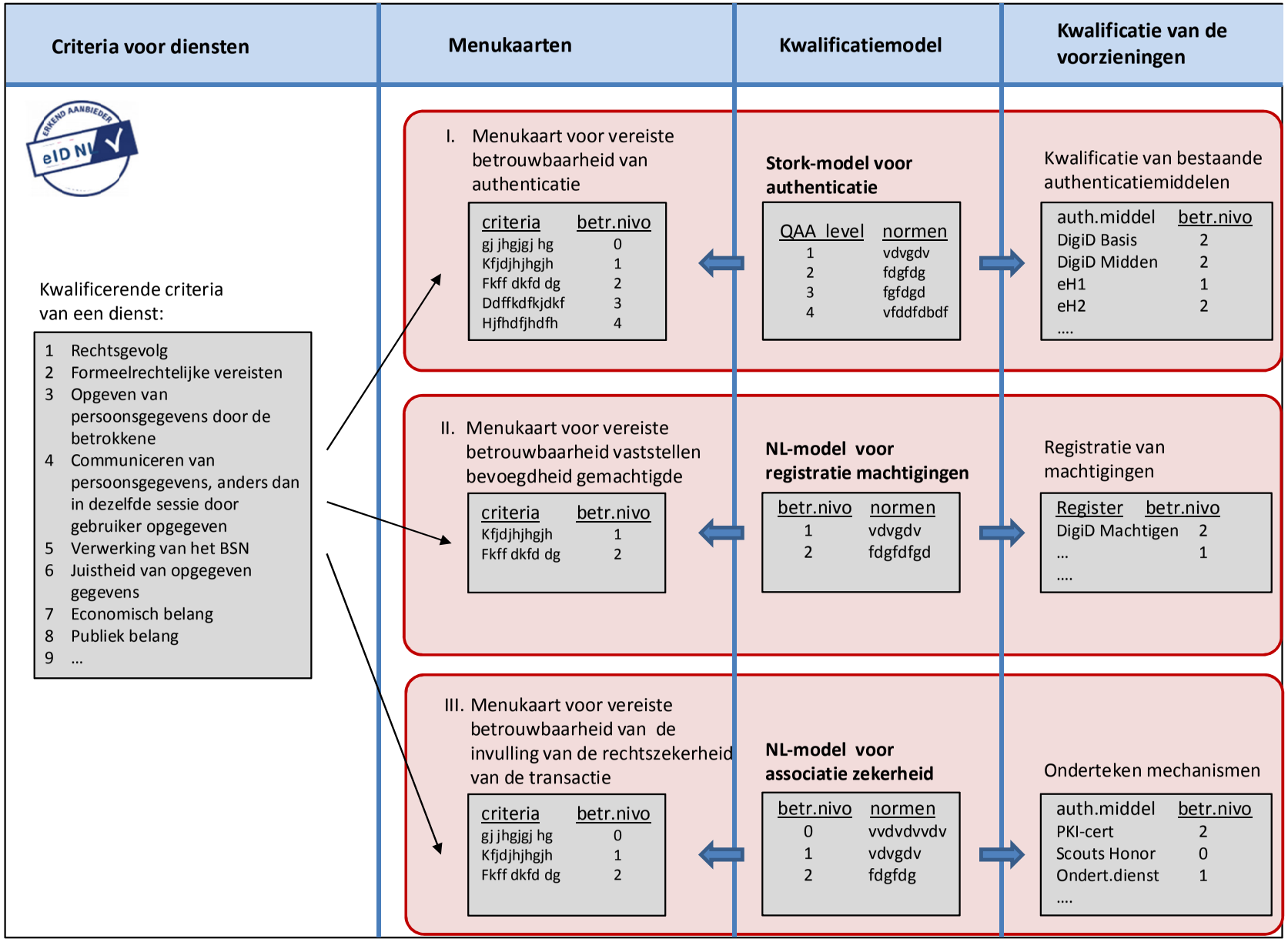
Bovenstaande modelmatige werkwijze maakt het mogelijk om voor eID deelnemers eenduidige criteria en normen voor te schrijven. Het in te richten toezicht vanuit het eID stelsel zal mede gebaseerd worden op deze modellen.

Voor het onderwerp authenticatie is dus het STORK-model als kwalificatiemodel beschikbaar en bruikbaar. Voor de twee overige onderwerpen:
A. de mate van betrouwbaarheid van een geregistreerde machtiging,
B. de mate van betrouwbaarheid van de associatie zekerheid van een transactie,
zijn nog geen kwalificatiemodellen beschikbaar. In de ontwikkeling van het eID stelsel worden deze ontwikkeld, waarbij uiteraard EU-ontwikkelingen worden betrokken.

Ad A.
Er is voor het machtigingen op dit moment nog geen kwalificatiemodel vergelijkbaar met het Stork-model voor authenticatie. Er loopt wel een initiatief in EU-verband, echter er moet in ieder geval een NL-invulling komen voor het kunnen kwalificeren van een verklaarde bevoegdheid (en de onderliggende geregistreerde machtigingen), het kwalificatiemodel. Beoordeeld moet worden of de huidige set van criteria voor diensten voldoende is. Vervolgens dient de menukaart voor dit onderwerp ingevuld te worden. Bovendien is een kwalitatieve beoordeling nodigvan mogelijke invullingen van het registeren van machtigingen.

Ad B.
Vergelijkbaar met ad A, dienen dezelfde onderdelen van het raamwerk ingevuld te worden voor het onderwerp authentieke wilsuiting en associatie zekerheid van de transactie. De vraag daarbij is welke betrouwbaarheidsniveaus in het kwalificatiemodel zinvol te onderscheiden zijn. Op basis van dat kwalificatiemodel is een beoordeling nodig welke verschillende onderteken mechanismen (bijvoorbeeld gekwalificeerd certificaat, ondertekendienst, vinkje zetten) mogelijk zijn en welke kwalificatie deze krijgen.

Op de volgende pagina is in schemavorm een totaalbeeld geschetst.


Criteria voor diensten
Menukaarten
Kwalificatiemodel
Kwalificatie van de voorzieningen
Kwalificerende criteria van een dienst:
1 Rechtsgevolg
2 Formeelrechtelijke vereisten
3 Opgeven van persoonsgegevens door de betrokkene
4 Communiceren van persoonsgegevens, anders dan in dezelfde sessie door gebruiker opgegeven
5 Verwerking van het BSN
6 Juistheid van opgegeven gegevens
7 Economisch belang
8 Publiek belang
9 ...
I. Menukaart voor vereiste betrouwbaarheid van authenticatie
criteria betr.nivo
gj jhgjgj hg 0
Kfjdjhjhgjh 1
Fkff dkfd dg 2
Ddffkdfkjdkf 3
Hjfhdfjhdfh 4
Stork-model voor authenticatie
QAA level normen
1 vdvgdv
2 fdgfdg
3 fgfdgd
4 vfddfdbdf
Kwalificatie van bestaande authenticatiemiddelen
auth.middel betr.nivo
DigiD Basis 2
DigiD Midden 2
eH1 1
eH2 2
....
II. Menukaart voor vereiste betrouwbaarheid vaststellen bevoegdheid gemachtigde
criteria betr.nivo
Kfjdjhjhgjh 1
Fkff dkfd dg 2
NL-model voor registratie machtigingen
betr.nivo normen
1 vdvgdv
2 fdgfdfgd
Registratie van machtigingen
Register betr.nivo
DigiD Machtigen 2
... 1
....
III. Menukaart voor vereiste betrouwbaarheid van de invulling van de rechtszekerheid van de transactie
criteria betr.nivo
gj jhgjgj hg 0
Kfjdjhjhgjh 1
Fkff dkfd dg 2
NL-model voor associatie zekerheid
betr.nivo normen
0 vvdvdvvdv
1 vdvgdv
2 fdgfdg
Onderteken mechanismen
auth.middel betr.nivo
PKI-cert 2
Scouts Honor 0
Ondert.dienst 1
....

6.2 Dienstencatalogus

Voor een goede werking van Authenticatie- en Machtigingsdiensten is een gestandaardiseerde Dienstencatalogus noodzakelijk. Het eID Stelsel definieert een minimale invulling van een dienstencatalogus die de voor de overheidsdienstaanbieders de bestaande catalogi van DigiD machtigen, eHerkenning SBR en Digipoort kan vervangen. Zo wordt een gedeelde set van benodigde gegevens over dienstaanbieders en diensten gevormd.

Een dienstencatalogus heeft twee belangrijke doelen:
1. Een beschrijving geven van de dienst en het gewenste betrouwbaarheidsniveau zodat dienstverlening van middelenuitgevers en machtigingregisters daarmee kan worden afgestemd.
2. Een taal definiëren waarmee de partijen in het stelsel kunnen communiceren over bevoegdheden. Deze taal stelt machtigingenregisters ook in staat om vormvrije machtigingen te vertalen naar een eenduidige registratie.

Een dienstencatalogus bevat minimaal de volgende gegevens:
- Gegevens van de dienstaanbieder
- Gegevens van diensten of delen daarvan
- Benoemen van dienstaanbieder overstijgende diensten
- Betrouwbaarheidsniveau per dienst of deel daarvan
- Attributen waar een dienstaanbieder recht op heeft
- Informatie over de sector of sectoren waarin de dienst wordt aangeboden en het benodigde sectorale nummer

6.3 Functionele invulling van de berichten

In dit hoofdstuk is de functionele inhoud van de verschillende eID-berichten toegelicht.

Identiteitsverklaring

Element / Attribuut	Invulling
Verklaring ID	Verklaring ID, gegarandeerd uniek in eID-Stelsel
Uitgiftemoment	Datum Tijd waarop de Verklaarder deze Verklaring uitgeeft
Verklaarder (Issuer)	Unieke identificatie van de partij die deze verklaring heeft gecreëerd. Dit kan Belanghebbende, Gemachtigde of een Gecertificeerde Partij zijn, onderliggend is een PKI-certificaat.
Ondertekening	Technische ondertekening van deze verklaring met een PKI-Certificaat
HandelendePartij	Bevat de identificerende gegevens van de Handelende Partij (NHP of NNHP). En de IdentificatieSoort (verzameling waar de HP-ID uniek in te vinden is), bijv BSN of eID-Stelsel Pseudo-ID's
Betrouwbaarheid	Specificeert de Stork betrouwbaarheid van de Verklaring, afhankelijk van authenticatie middel en het registratieproces.
Condities	Specificeert bv. tijd, doel of doelgroep restricties waaronder de Verklaring gebruikt mag worden
Comfort Informatie tbv Belanghebbende	(verplicht igv Gemachtigde) samengestelde naam van de Handelende Partij in een toegankelijke duidelijke manier zoals bekend bij de 'machtigende' (meestal Belanghebbende). Verklaarder staat garant voor de correcte naam.
Herleidbaarheid	Optioneel igv afgeleide verklaring: identificatie van de Verklaring (en Verklaarder) waar deze verklaring van is afgeleid.

Bevoegdheidsverklaring

Element / Attribuut	Invulling
VerklaringID	Verklaring ID, gegarandeerd uniek in eID-Stelsel
Uitgiftemoment	Datum Tijd waarop de Verklaarder deze Verklaring uitgeeft
Verklaarder (Issuer)	Unieke identificatie van de partij die deze verklaring heeft gecreëerd. Dit kan Belanghebbende, Gemachtigde of een Gecertificeerde Partij zijn, onderliggend is een PKI-certificaat.
Ondertekening	Technische ondertekening van deze verklaring met een PKI-Certificaat
Bevoegde Partij	Bevat de identificerende gegevens van de GemachtigdePartij (NHP of NNHP). En de IdentificatieSoort (verzameling waar de HP-ID uniek in te vinden is), bijv BSN of eID-Stelsel Pseudo-ID's
Vertegenwoordigde	Bevat de identificerende gegevens van de Vertegenwoordigde Partij (NHP of NNHP). En de IdentificatieSoort (verzameling waar de persoon uniek in te vinden is), bijv BSN of eID-Stelsel Pseudo-ID's
Bevoegdheid	Formele beschrijving van de bevoegdheid.
Betrouwbaarheid	Specificeert de (soort van) Stork betrouwbaarheid van de Verklaring, voor namelijk afhankelijk van het registratieproces.
Condities	Specificeert bv. tijd, doel of doelgroep restricties waaronder de Verklaring gebruikt mag worden
Comfort Informatie tbv Belanghebbende	(igv Gemachtigde) samengestelde naam van de Handelende Partij in een toegankelijke duidelijke manier zoals bekend bij de 'machtigende' (meestal Belanghebbende). Verklaarder staat garant voor de correcte naam.
Herleidbaarheid	Identificatie van de brongegevens waar deze verklaring van is afgeleid.

Associatieverklaring

Element / Attribuut	Invulling
Verklaring ID	Verklaring ID, gegarandeerd uniek in eID-Stelsel
Uitgiftemoment	Datum Tijd waarop de Verklaarder deze Verklaring uitgeeft
Verklaarder (Issuer)	Unieke identificatie van de partij die deze verklaring heeft gecreëerd. Dit kan Belanghebbende, Gemachtigde of een gecertificeerde Partij zijn, onderliggend is een PKI-certificaat.
Ondertekening	Technische ondertekening van deze verklaring met een PKI-Certificaat
Belanghebbende	(ter ondersteuning van meervoudig ondertekenen) Bevat de identificerende gegevens van de Belanghebbende waarvoor ondertekend is.
Bevoegdheidsketen	Verwijst naar de Identiteits- en BevoegheidsVerklaringen die samen de Bevoegdheidsketen vormen waarmee Handelende Partij voor Belanghebbende heeft ondertekend.
Accoderings-moment	Datum Tijd, is gelijk aan het moment van accodering door de Handelende partij (mogelijk niet relevant als deze gegarandeerd het zelfde is als het uitgiftemoment)
Accoderings-Betrouwbaarheid	Specificeert de (soort van) Stork betrouwbaarheid van het accoderingsproces