# Werkgroep Identificatie en Authenticatie 1: Elementen voor een visie

Deze versie bevat alle aanpassingen zoals voorgesteld als ACTIES in het review verwerkingsdocument.

*"On the Internet, nobody knows you're a dog."*

## Inhoud

## 1. Inleiding

De digitale transformatie van onze samenleving vraagt om vertrouwen in de digitale wereld. Dit vertrouwen is geen gegeven en het blijkt een domein waar de overheid een bepaalde rol heeft in te vullen. Het opbouwen van vertrouwen in de digitale wereld is essentieel voor economische en sociale ontwikkeling. Een gebrek aan vertrouwen leidt ertoe dat burgers, bedrijven en overheden aarzelen om transacties digitaal uit te voeren, van nieuwe (overheids-)diensten gebruik te maken of een toevlucht zoeken in suboptimale of onveilige oplossingen (denk aan een kopie van een paspoort).

De vraag is echter hoe de rol van de overheid in dit domein er uit gaat zien en hoe de overheid bepaalde functies generiek (overheidsbreed) gaat organiseren? De uitdaging die de overheid in dit domein heeft, is om de voorwaarden te scheppen om het voor burgers en ondernemers mogelijk te maken om op een veilige, persoonlijke en gebruiksvriendelijke wijze digitale diensten af te nemen.[1] Een onderdeel van dit vertrouwen is een duidelijk verhaal vanuit de overheid over functies binnen het domein van identificatie en authenticatie. De komende vijf jaar zal de behoefte aan andere vormen van identificatie en authenticatie in het digitale domein zich blijven ontwikkelen.

Dit document is een aanzet tot een visie op identificatie en authenticatie als onderdeel van de Generieke Digitale Infrastructuur.

## 2. Aanleiding

De belangrijkste maatschappelijke aanleiding voor “herijking” van het huidige beleid is, dat een goed ingerichte identificatie- en authenticatiefunctie randvoorwaardelijk is voor zeer veel andere functies waar burgers en bedrijven behoefte aan hebben. Een van de belangrijke randvoorwaarden voor het afnemen van digitale diensten als burger of onderneming is een goed stelsel voor (digitale) identificatie en authenticatiemiddelen. Wanneer we als overheid natuurlijke personen, rechtspersonen en ondernemingen werkelijk centraal willen stellen, moeten zij gebruik kunnen maken van mogelijkheden en beschikbaarheid van (digitale) identificatiemiddelen om, vanuit al hun contexten en via alle mogelijke kanalen, met de benodigde betrouwbaarheid te bewijzen dat je “bent wie je zegt te zijn”.

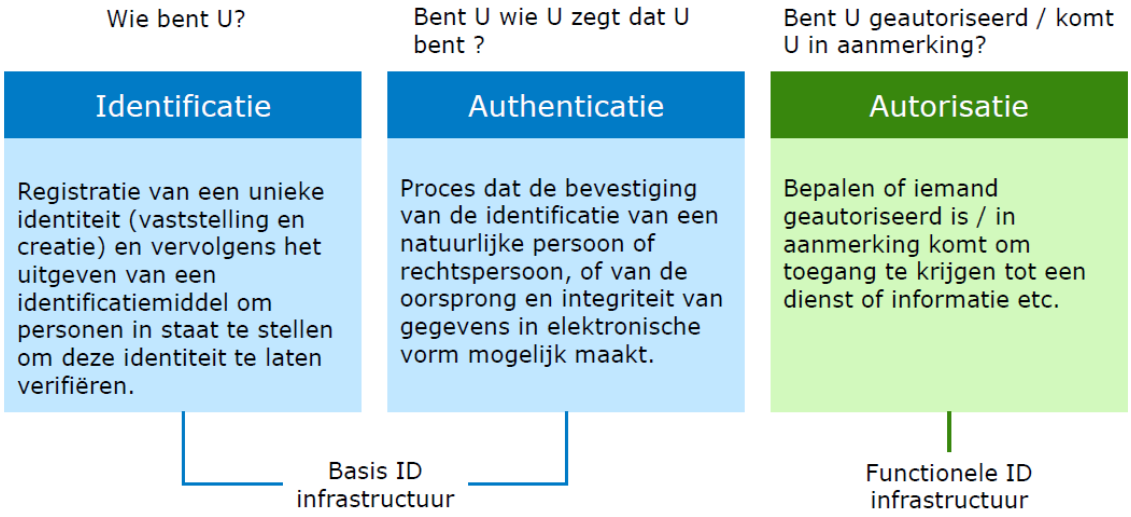
Het hebben van een unieke en betrouwbare, in een administratie vastgelegde identiteit is een voorwaarde voor het zowel online als offline kunnen vaststellen van iemands identiteit. Op basis van deze administratieve identiteit[2] en de gegevens die geregistreerd staan, kunnen bepaalde (digitale) identificatiemiddelen worden uitgegeven. Hiermee kunnen natuurlijke personen zich vervolgens digitaal identificeren en laten authentiseren om digitaal zaken te doen. De identificatie van een rechtspersoon en onderneming maakt (in de praktijk van digitale diensten in een portaal) altijd onderdeel uit van een proces waarbij een machtiging is afgegeven voor een natuurlijk persoon om die rechtspersoon of onderneming te vertegenwoordigen. Daarnaast onderscheiden we nog technische koppelingen van systeem naar systeem, waar op basis van technische sleutels het identificatiemiddel wordt gecontroleerd.

**Disclaimer:**
Deze visie gaat uit van een gewenste situatie over een periode van vijf jaar. Daarbij is als uitgangspunt genomen dat, in principe, huidige oplossingen, afspraken, standaarden en

[1] In deze visie beperken we ons tot de digitale identiteit van natuurlijke personen en rechtspersonen. De identiteit van objecten en apparaten zal buiten beschouwing gelaten worden, hoewel in een later stadium zeker de vraag zal opkomen naar generiek overheidsbeleid in deze domeinen.
[2] We gaan in deze visie uit van een identiteit die is afgebakend tot een administratieve entiteit en identiteit, die gekoppeld is aan een natuurlijk persoon of rechtspersoon.

mogelijkheden ter discussie gesteld worden. Vijf jaar is echter, niet zo ver in de toekomst, dat van een geheel nieuwe situatie uitgegaan mag worden. Voor bijvoorbeeld de huidige fysieke dragers van de door de overheid uitgegeven identiteit (de WID's) is binnen een periode van vijf jaar niet zomaar een nieuwe situatie te creëren (denk aan uitlezen van chips), die representatief kan zijn voor de gehele populatie. Met dit gegeven, is een goede migratiestrategie wenselijk.

## 3. Basisfuncties van een identiteitinfrastructuur[3]




De basisfuncties van een identiteitinfrastructuur bestaan uit de functies identificatie, authenticatie en autorisatie[4].
Op hoog functioneel niveau wordt onderscheid gemaakt tussen:

- Toekennen van digitale identiteit (ik besta + registratie daarvan)
- Identificeren (digitaal bewijs dat ik besta) (linker blok)
- Authentiseren (verifiëren/controleren van bewijs dat ik het ben) (middelste blok)
- Autoriseren (mag ik wat ik zeg dat ik mag) (rechter blok)

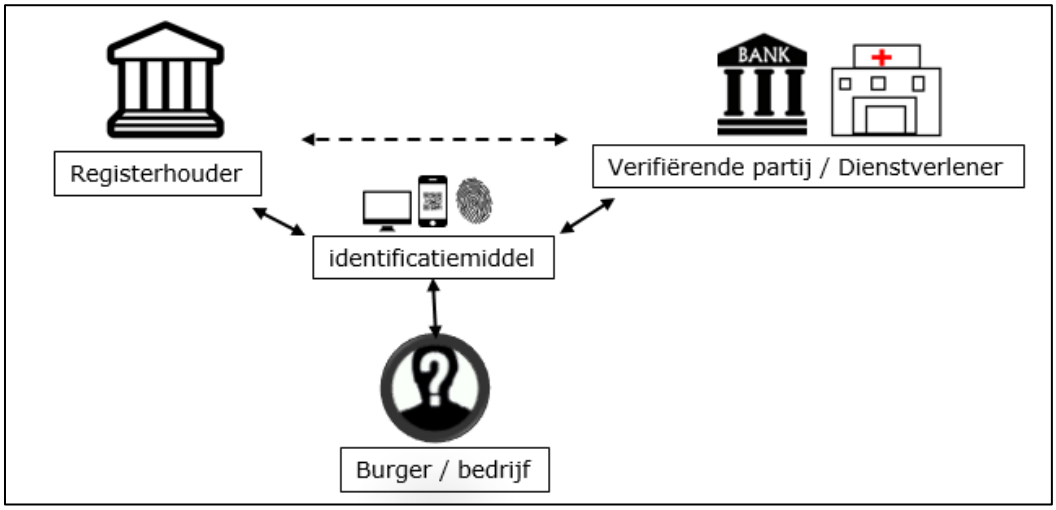
Dit document focust vooral op de functies identificatie en authenticatie voor burgers en ondernemers in het contact met de overheid, maar raakt deels ook identificatie- en authenticatie functies binnen overheidsorganisaties voor overheidsmedewerkers[5].

Binnen de functie identificatie vallen in een infrastructuur grofweg vier rollen te spreken:

1. Burger: De entiteit van wie gegevens ergens geregistreerd staan
2. Registerhouder: De partij die gegevens registreert en daarmee een gezaghebbende bron kan vormen
3. Verifiërende partij (vertrouwende partij): de partij die om een interactie of transactie (dienstverlening) aan te gaan een identiteit geverifieerd wil hebben vanuit een gezaghebbende bron
4. Elektronisch identificatiemiddel uitgevende partij (middelenuitgever): de partij die het identificatiemiddel levert waarmee een gebruiker zich digitaal kenbaar maakt en met een bepaalde mate van betrouwbaarheid bewijst dat hij is wie hij stelt dat hij is.

[3] Model afkomstig uit: 'Worldbank practitioner guide' (2019). Definities zijn gebaseerd op: eIDAS regulering, 'Definities', artikel 3.
[4] De definities staan in de bijlage bij dit document.
[5] Deze visie beperkt zich tot de onderdelen Identificeren en Authentiseren voor burgers en bedrijven in contact met de overheid. Toekennen en Autoriseren is voor deze visie buiten scope, evenals aanvullende activiteiten als ondertekenen, wilsuiting en leveren van andere gegevens dan die nodig zijn voor vaststellen van identiteit en authenticatie

**De onderstaande weergave illustreert de weergave van rollen. De indeling is gemaakt vanuit het perspectief van de gebruiker en geeft niet direct de architectuur weer. Aanvullende functies als middelenuitgever en broker zijn niet opgenomen. Dit zal in een nadere uitwerking plaatsvinden.*




## 4. Huidige situatie (ist)

In Nederland bestaat er een uitgangssituatie waarin een 'gezaghebbende bron' voorhanden is. We hebben een gecentraliseerd identiteitenstelsel dat als gezaghebbende bron de Basisregistratie Personen (BRP) voor natuurlijke personen en het Handelsregister (HR) voor rechtspersonen kent. Dat is anders in vergelijking met het Angelsaksische model, waarbij overheden bijvoorbeeld geen registratie van ingezetenen hebben. Voor Nederland is een dergelijke bron in de vorm van diverse basisregistraties echter wel beschikbaar. Deze situatie rechtvaardigt, samen met het grote maatschappelijke belang, een actieve rol van de overheid in het identiteitsdomein vergelijkbaar met de analoge situatie (uitgifte van WID's). In dit stelsel zijn, voor zowel natuurlijke personen als voor rechtspersonen unieke identificerende nummers vastgelegd. Voor burgers is dat doorgaans het BSN en voor bedrijven is dit het KvK nummer[6]. Deze nummers worden tevens gebruikt in de digitale identificatie en authenticatie middelen in het publieke domein.
In het huidige publieke domein in Nederland wordt in 2020, DigiD en eHerkenning gebruikt voor de digitale identificatie en authenticatie.[7] DigiD als authenticatiemiddel en eHerkenning als afsprakenstelsel voor private identificatiemiddelen. Voor private dienstverlening worden verschillende inlogvormen gebruikt (vaak gebruikersnaam/wachtwoord) en zijn er in verschillende sectoren bewegingen richting stelsels voor een bepaalde sector, zoals bijvoorbeeld IDIN in de bancaire sector. Tenslotte is sprake van veel social logins, zoals Facebook, Google etc.

Als we het alleen over inloggen op portalen hebben, zouden we het alleen over personen moeten hebben. Als je dan bent ingelogd bij een dienstverlener, dan zou deze de vraag moeten stellen of je dat doet voor 1. jezelf, 2. voor een ander (en wie dat is), of 3. namens een bedrijf (voor welk bedrijf). Bij antwoord in de situatie 2 en 3, zou de dienstverlener dan bij resp. een machtigingsregister voor personen en een machtigingsregister voor bedrijven moeten navragen of die machtiging bestaat.

[6] Voor de verwezenlijking van deze visie is het randvoorwaardelijk te kijken naar die groepen die nu buiten het BSN- of KVK-domein vallen. Tevens zal er ook naar het internationale component via de eIDAS knooppunten gekeken moeten worden om buitenlandse entiteiten te kunnen (blijven) laten aansluiten.
[7] https://www.digid.nl/ en https://www.eherkenning.nl/ . Zowel DigiD als eHerkenning zijn beschikbaar op verschillende betrouwbaarheidsniveaus.

De werkgroep I&A1 gaat over de eerste stap. Werkgroep I&A2 (Machtigen) over de tweede stap.

**Verordening eIDAS**
De EU-Verordening eIDAS is een belangrijk wettelijk kader en zorgt voor regels en eisen waaraan identificatie- en authenticatiemiddelen moeten voldoen om een bepaald betrouwbaarheidsniveau te bereiken.[8] Ook omvat dit een stelsel van afspraken over de erkenning van internationale identificatie- en authenticatiemiddelen. Alleen middelen, die via de procedure eIDAS worden goedgekeurd mogen als substantieel of hoog betrouwbaarheidsniveau worden aangemerkt.

**Huidige wettelijke ontwikkelingen in het publieke domein**
Vanuit privacybescherming en het voorkomen van misbruik van beschikbare digitale persoonsgegevens worden (inter)nationaal en vanuit de EU steeds hogere eisen gesteld aan de betrouwbaarheid en informatieveiligheid van de huidige digitale identificatie- en authenticatiemiddelen. Naar verwachting zal op 1 januari 2021 de Wet Digitale Overheid van kracht worden.[9] De Wet Digitale Overheid schrijft voor dat publieke dienstverleners de digitale diensten die zij leveren moeten classificeren op het juiste betrouwbaarheidsniveau (laag, substantieel of hoog) en toegang tot die diensten alleen mogelijk is met het juiste (digitale) identificatie- en authenticatiemiddel op datzelfde niveau. Hiervoor schept de Wet Digitale Overheid de benodigde kaders en spelregels vanuit de overkoepelende verantwoordelijkheid van de Minister van BZK voor het stelsel van toegang tot digitale dienstverlening binnen de overheid. De wet Digitale Overheid schept ook erkenning van en toelating van private middelen voor burgers.

## 5. Ontwikkelingen

**Ontwikkeling van identiteiten vanuit de overheid**
De afgelopen jaren heeft de ontwikkeling en het gebruik van DigiD een vlucht genomen. Steeds meer gebruikers stappen over van het initiële gebruikersnaam+wachtwoord-construct naar een 2-factorauthenticatie (koppelen aan een telefoonnummer (sms) of via een app op een smartphone). De DigiD-app kent inmiddels 8 miljoen gebruikers, waarvan 1,6 miljoen accounts op substantieel niveau. In de periode januari tot mei 2020 is er 175 miljoen keer ingelogd bij een dienstverlener met behulp van DigiD. Vanaf 2021 wordt het mogelijk om in combinatie met de eNIK (de identiteitskaart met een chip en applet) en het eRijbewijs (met chip en applet) via een smartphone op eIDAS hoog in te loggen. Voor niet-natuurlijke personen is er reeds geruime tijd de mogelijkheid om op alle eIDAS-betrouwbaarheidsniveaus in te loggen met behulp van eHerkenning.
Met de eIDAS verordening is naast de eisen voor betrouwbaarheidsniveaus voor middelen, vastgelegd op welke manier erkende inlogmiddelen uit andere lidstaten toegang kunnen krijgen tot Nederlandse overheidsdienstverlening. Tevens zijn de middelen van eHerkenning en DigiD ge(pre-)notificeerd binnen Europa en als zodanig bruikbaar in andere lidstaten.

**Toenemende focus op digitale dienstverlening en sterkere positie van de burger**
De digitale (overheids-) dienstverlening neemt de komende jaren toe[10],zowel in het reeds bestaand aanbod als in nieuwe vormen. Om de positie van de gebruiker (burger/bedrijf) te versterken en te beschermen, is op dit domein veel aandacht nodig voor inclusie, privacy en het voorkomen en aanpakken van meerdere vormen en soorten van ID-fraude.

**Verschuiving van gegevensuitwisseling naar verifieerbare beweringen (claim-gebaseerde architectuur)**

[8] eIDAS: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&from=EN Zie artikel 8 voor betrouwbaarheidsniveaus Laag, Substantieel en Hoog beschrijving.
[9] https://www.eerstekamer.nl/wetsvoorstel/34972_wet_digitale_overheid
[10] Zie bijvoorbeeld de Monitor Digitale Overheid, waar jaarlijks het aantal authenticaties met substantiële percentages toeneemt

Een belangrijke ontwikkeling in het internetdomein is dat, ook voor de identiteitvaststelling, langzaam een beweging ontstaat van gegevensuitwisseling naar het uitgeven van verifieerbare beweringen (claims zoals: ik ben ouder dan 18 etc.) over een (gecombineerde) identiteit. Ook bestaat de wens, in het kader van privacy en dataminimalisatie, om een minimale set van rechtsgeldige, tot de bron herleidbare attributen uit te wisselen (op basis van API's) die bijdragen aan vaststelling van identiteit en de bevoegdheid van de drager van het middel. In plaats van de hele doopceel levert de gebruiker alleen die (gewaarmerkte) attributen die nodig zijn voor de gewenste dienstverlening. De gebruiker krijgt meer regie over zijn/haar gegevens en gebruikt in verschillende elementen van dienstverlening telkens alleen de gegevens die in dat proces nodig zijn. Voor het domein van identificatie en authenticatie betekent dit, dat ook daar minder gegevens uitgewisseld zullen worden en er meer bewijsbare claims over gegevens uitgewisseld zullen worden via vertrouwensdiensten die een identificatie- en authenticatiefunctie aanbieden.

**Invloed van de markt**
De invloed van de markt is in het domein van identificatie en authenticatie middelen niet uit te vlakken. Wel is deze deels afhankelijk van de mogelijkheden en ondersteuning die de overheid nu en in de nabije toekomst kan bieden. In de Wet Digitale Overheid wordt hier een voorschot op genomen, waarbij de overheid nadrukkelijk de intentie heeft om privaat geleverde identificatie- en authenticatiemiddelen toe te laten tot het publieke domein. Eveneens bestaat er binnen de Wet Digitale Overheid de mogelijkheid om het publiek geleverde identificatie- en authenticatiemiddel op termijn in te zetten in het private domein.

**Innovatie en samenwerking: de behoefte aan flexibiliteit neemt toe**
Het domein van digitale vertrouwensdiensten, identificatiemiddelen, authenticatiemiddelen en attributendiensten ontwikkelt razendsnel. De toegevoegde waarde van innovaties is zichtbaar te maken door deze, naast de bestaande inrichting een plek te geven in de vorm van een 'sandbox' omgeving waarin research en development ruimte krijgen. Op die wijze kunnen we ontdekken hoe nieuwe inzichten, technologie en werkwijzen een toegevoegde waarde hebben bij de inrichting van capabilities. Opschalen van nieuwe technologie en transitie naar nieuwe functionaliteit zijn op die wijze stapsgewijs vorm te geven. Deze snelle ontwikkeling vraagt vanuit de overheid vooral de inrichting van een zo flexibel mogelijke infrastructuur met zo min mogelijk afhankelijkheid van specifieke middelen die een bepaalde functie inrichten.

**Fraude neemt toe**
Data en persoonsgegevens zijn steeds gevoeliger in het maatschappelijk verkeer en de eisen ten aanzien van privacy en security vragen en krijgen veel meer aandacht bij vernieuwingen van stelsels. Bij (grootschalige) digitale uitwisseling van persoonsgegevens kan snel sprake van zijn van misbruik, bijvoorbeeld door identiteitsfraude of schijnwerkelijkheid.[11]

**Toegenomen wensen vanuit de gebruiker**
Het bewustzijn rond het gebruik van identificatie- en authenticatiemiddelen neemt toe. De gebruiker (burger/bedrijf) heeft steeds meer wensen voor transparantie, privacy en de beveiliging van zijn gegevens door de overheid. Niet alleen is er wettelijk door de AVG een grotere druk op de verwerking van persoonsgegevens.[12] Er is ook een grotere maatschappelijke discussie over gegevensverwerking. Daarbij groeit de roep om meer regie op eigen gegevens (in de zin van transparantie en hergebruik binnen zowel het publieke als private domein) en de eis om niet onnodig gegevens meerdere keren uit te wisselen. Voor wat betreft Identificatie en Authenticatie is het verstrekken van

[11] Uit de *Monitor Identiteit 2019* (uitgevoerd in opdracht van Ministerie BZK) blijkt dat 4,1% van de onderzochte populatie dat jaar te maken heeft gehad met een vorm van identiteitsfraude waarbij een ander persoon zich ongewenst als hen had voorgedaan. Dat is bijna een verdubbeling t.o.v. 2014 (2,1%)
[12] Uitvoeringswet Algemene verordening gegevensbescherming https://wetten.overheid.nl/BWBR0040940/2020-01-01

authentieke gegevens, benodigd voor het vaststellen van identiteit en authenticatie, binnen scope. Het verstrekken van overige attributen (zowel uit basisregistraties als andere bronnen), is buiten scope.

**Meer kanalen dan website of mijn-omgeving**
De aandacht op de ontwikkeling van online mogelijkheden ligt nu vooral bij het toegankelijk krijgen van elektronische dienstverlening zoals deze via websites of gepersonaliseerde domeinen (mijn-omgeving) worden aangeboden. In de nabije toekomst zal er meer behoefte komen aan identificatie- en authenticatiemiddelen waarbij je in verschillende contexten en langs alle kanalen (apps, telefonisch, virtueel, videocalls) diensten kan afnemen en aanleveren.

## 6. Toekomstbeeld: visie (soll)

Het fundament van deze visie is gebaseerd op een overheid als “gezaghebbende bron” voor de digitale identiteit van natuurlijke personen en rechtspersonen. Hiervoor introduceren wij het concept van de digitale bronidentiteit. Een concept dat (zeker) nadere uitwerking vraagt (over de exact benodigde gegevens voor identiteitsvaststelling) en waarin deze visie een functionele aanzet geeft.
In de digitale dienstverlening worden geverifieerde identificatiegegevens vanuit de overheid beschikbaar gesteld aan natuurlijke of (niet natuurlijke) personen. Deze persoon kan ervoor kiezen, deze brongegevens voor identiteit in te zetten voor (het activeren van) afgeleide identificatiemiddelen.
En daarnaast zijn deze gegevens via nog te maken afspraken (zie hieronder bij ‘afsprakenkader’) te ontsluiten naar dienstverleners (in de vorm van *verifieerbare claims*, zie onder hoofdstuk 5, ontwikkelingen).
Zo kunnen burgers en bedrijven gemakkelijker zakendoen in het publieke en private domein.

**Doel Toegang**
Het doel van de identiteitinfrastructuur van de toekomst, is het betrouwbaar faciliteren van toegang door de overheid door:

- Het organiseren van toegang tot cruciale dienstverlening in de Nederlandse maatschappij voor alle natuurlijke en rechtspersonen op een passend (eIDAS) betrouwbaarheidsniveau, zowel in het publieke als private domein.
- Gemakkelijk, veilig en met voldoende privacy-borging, om op digitale wijze diensten af te kunnen nemen in NL en eventueel ook wereldwijd.

Voor deze zaken wordt gezorgd in de Wet Digitale Overheid. Hierin wordt de basis gelegd op de inzet van de DBI en bijbehorende publieke en/of private authenticatiemiddelen voor het faciliteren van toegang tot diensten in het publieke en private domein. De toegang zelf wordt geregeld door de betreffende dienstaanbieders.

**Concept Digitale Bron Identiteit (DBI)**
Om betrouwbare toegang te kunnen faciliteren, ontwikkelt de overheid een digitale bronidentiteit (DBI).

> “Een door de overheid uitgegeven, erkende en in wet en regelgeving verankerde, verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale domein voor gebruik in de publieke en de private sector”.

Dit concept biedt digitaal een belangrijk generiek bouwblok voor vertrouwen in de digitale wereld. De huidige visie van DBI is om naar een situatie te groeien waarin geen gegevensopslag en uitwisseling van identiteitsgegevens meer nodig is. Voor een eerste stap in die richting zou de DBI een minimale set van gezaghebbende, gewaarmerkte identiteitsgegevens bevatten die nodig zijn in het maatschappelijk verkeer. Deze identiteitsgegevens komen voort uit, ten minste twee basisregisters, het Handelsregister

en de BRP[13]. De DBI heeft als uitgangspunt vanuit een gezaghebbende bron, het hoogste betrouwbaarheidsniveau te bieden.
De DBI als 'gezaghebbende bron' maakt afgeleide identificatie- mogelijk. Deze afgeleide identificatiemiddelen zullen zowel publiek als privaat gebruikt kunnen worden. De keuzevrijheid van de gebruiker (burger/bedrijf) en de flexibiliteit van de infrastructuur moet centraal staan. De basis zal zijn dat er eenduidige eisen aan de toegelaten en geaccepteerde afgeleide identificatie- en authenticatiemiddelen worden gesteld. Het uitgangspunt is dat de DBI zelf zo min mogelijk als functioneel identificatiemiddel wordt ingezet.
Dit concept van een digitale bron identiteit kan als basis dienen voor vertrouwen vanuit de Nederlandse maatschappij. De overheid biedt hiermee, zoals dat in Nederland ook in het fysieke domein gebeurt, een vertrouwensbasis van betrouwbare gegevens die in identificatie- en authenticatieprocessen via vertrouwde (middelen-)leveranciers hergebruikt kunnen worden. Ook kan onder goed ingericht toezicht van de overheid dit concept, bijdragen aan online vertrouwen bij verschillende processen van dienstverlening, zowel in de publieke als private sector.

**Proactieve overheid in verschillende rollen**
Bovenstaande ontwikkelingen vragen om een meer proactieve overheid die haar maatschappelijke rol wil vervullen en vooral burgers en ondernemers wil ontzorgen bij het digitaal zaken doen. Als overheid is er daarnaast een belangrijke rol voor een 'veilige' samenleving. Dat vereist een proactieve overheid, die veiligheid niet alleen op straat waarborgt, maar ook op internet én:

- de belangrijke randvoorwaarden voor veilige en betrouwbare toegang tot dienstverlening organiseert en regelt vanuit de overheidsverantwoordelijkheid;
- innovaties stimuleert, omdat de digitale transformatie zich zodanig snel ontwikkelt dat de overheid het zich niet kan permitteren achter te blijven;
- een belangrijke schakel vormt richting een werkende identiteitinfrastructuur.

De overheid vervult dan, de rol van wetgever, kadersteller, handhaver, registerhouder, dienstverlener, leverancier van identificatiemiddelen en financier van stelsels.

**Afsprakenkader en Stelsel digitaal vertrouwen (Trust Framework)**
Om het concept van de DBI mogelijk te kunnen maken, is het voorstel een te ontwikkelen afsprakenkader digitaal vertrouwen op te stellen en een stelsel in te richten. Dit stelsel en afsprakenkader bevat:

- De uitgangspunten en afspraken rond het doorgeven van verifieerbare claims ten aanzien van identificatiegegevens, de toegang tot digitale dienstverlening en het leveren van vertrouwen in de digitale wereld, inclusief de digitale bron identiteit (DBI).
- Een dergelijk afsprakenkader is breder toepasbaar dan alleen de publieke dienstverlening en vraagt dat private partijen zich kunnen confirmeren.
- Dit stelsel moet qua afspraken, standaarden en koppelvlakken generiek en sectoronafhankelijk zijn.

Het is aan te bevelen dat er voortgebouwd wordt op de bestaande stelsels voor elektronische toegangsdiensten (ETD) en het eID stelsel. Er bestaat echter breed een behoefte aan een overkoepelend (publiek/privaat) stelsel voor digitale vertrouwensdiensten (Trust Services, eIDAS).

** Noot werkgroep I&A 1:de hierboven beschreven ontwikkeling van een DBI, met een proactieve overheid en de suggestie van een afsprakenkader moet nader uitgewerkt worden. In de beperkte tijd van de pressure cooker was er onvoldoende tijd om de genoemde concepten tot een verder detailleringsniveau uit te werken. Tevens geven deze concepten waarschijnlijk genoeg aanleiding tot discussie over interpretatie. Dit zal in een vervolgtraject nader moeten worden uitgewerkt.*

[13] Aanvullende voorwaarden voor de DBI moeten worden verder uitgewerkt.

## 7. Capabilities (functies)

Deze capabilities (functies) voor het domein Identificatie en Authenticatie zijn opgesteld op basis van de bovenstaande richting/visie, die de werkgroep ondersteunt. Het betreft capabilities op de hoofdlijnen. Na besluitvorming op de hoofdlijnen kan detailuitwerking plaatsvinden in het vervolgproces.

Mapping op het NORA Vijflaagsmodel

Doordat nog geen nadere uitwerking is gemaakt van de capabilities, is het nog niet goed mogelijk een waardevolle mapping te maken op het NORA vijflaagsmodel.
In het algemeen kan je echter stellen dat door de indeling in Afspraken – Standaarden – Voorzieningen al een 1e mapping wordt ingezet:

1. Afspraken zijn doorgaans bekrachtigd in beleid of Wet- en Regelgeving en daardoor onderdeel van de Grondslagenlaag;

2. De uitvoering van afspraken door (overheids)organisaties leidt tot processen van samenwerking en zijn onderdeel van de Organisatorische laag;

3. Standaarden zijn doorgaans toegepast op de Informatielaag en de Applicatielaag;

4. Voorzieningen (technische services) zijn onderdeel van de Applicatielaag en/of Netwerklaag.

Aansluiting bij “WHY van de GDI”
De visie en onderstaande capabilities dragen met name bij aan de volgende punten uit de WHY:

- De dienstverlening van de overheid sluit niemand uit, is toegesneden op de context van burgers en bedrijven en is eenvoudig te gebruiken.
- Moderne dienstverlening is vooral digitaal (en dit is dan ook de focus geweest van de Werkgroep IenA1), maar de overheid houdt altijd rekening met wie geen gebruik kan maken van digitale diensten.
- De functies van de GDI worden bij voorkeur gerealiseerd via generieke afspraken en standaarden. Als de beoogde doelen hiermee niet worden bereikt, worden voorzieningen geïntroduceerd.
- Generieke voorzieningen moeten voor vrijwel alle GDI gebruikers relevant zijn en de mogelijkheid bieden dat individuele organisaties of groepen organisaties, aanvullende voorzieningen eraan kunnen koppelen. Die aanvullende voorzieningen vallen buiten de GDI.

| | |
|---|---|
| **ID** | 1 |
| **Omschrijving** | Duidelijk kaders stellen vanuit de overheid voor Identificatie en Authenticatie én vertrouwen geven aan burgers en ondernemers. |
| **Beschrijving** | De overheid zorgt voor kaders en maakt het voor burgers en bedrijven duidelijk hoe de overheid de identificatie en authenticatie voor natuurlijke personen en rechtspersonen in Nederland gaat regelen. De relatie met identificatie en authenticatie van natuurlijke personen en rechtspersonen buiten Nederland (wereldwijd) moet in dit kader ook geadresseerd.<br>De verandering die wordt ingezet, zorgt voor: een verschuiving van de aandacht van de overheid voor middelen naar aandacht voor kaders die het ontwikkelen van middelen faciliteren, meer keuze voor burgers en bedrijven voor de middelen die ze kunnen gebruiken en meer duidelijkheid voor private partijen (leveranciers) voor het aanbieden van middelen die passen binnen de gestelde kaders.<br>Het kader schept bij voorkeur ook duidelijkheid over het wel of niet gescheiden houden van het persoonsdomein en het bedrijvendomein (hetgeen nu een ongunstige invloed heeft op het inloggen van een persoon bij de huidige voorzieningen voor identificatie en authenticatie, zoals DigiD en eHerkenning). |
| **Rationale** | Identificatie en Authenticatie is een belangrijke voorwaarde voor betrouwbaar digitaal zakendoen |
| **Implicaties** | 1. Afspraak<br>De overheid stelt kaders voor het beschikbaar stellen van en gebruik van digitale identiteiten voor natuurlijke personen en voor rechtspersonen.<br>Als doelgroep gaat het niet alleen om personen met een Nederlandse Nationaliteit, maar ook om alle niet-Nederlanders die te maken hebben met de dienstverlening van de Nederlandse overheid[14].<br>2. Afspraak<br>De overheid stelt kaders voor het beschikbaar stellen van en gebruik van identificatiemiddelen voor natuurlijke personen en voor rechtspersonen.<br>Hierbij moet het mogelijk zijn dat, naast door de Nederlandse overheid uitgegeven identificatiemiddelen, ook identificatiemiddelen mogen worden gebruikt die door private partijen zijn uitgegeven: zolang al die identificatiemiddelen maar voldoen aan de gestelde kaders.<br>Daarnaast bestaat de wens om de authenticatie van een rechtspersoon altijd te laten verlopen via de authenticatie van een natuurlijk persoon die vanuit die rechtspersoon daartoe bevoegd is. Dit uitgangspunt is momenteel nog nergens expliciet vastgesteld. Het vereist wel een uitwerking vanuit de GF Bevoegdheden en/of GF Machtigen.<br>3. Standaarden<br>Onderdeel van deze kaders is, dat de privacy wordt geborgd bij het gebruik van identificatiemiddelen: derden mogen niet zonder toestemming van betrokkene kennisnemen voor welke diensten een authenticatie wordt uitgevoerd.<br>Een belangrijke implicatie daarbij is dataminimalisatie (ook vereist vanuit de AVG): zo min mogelijk (meta-)gegevens over de identiteiten registreren en bovendien met beperkte bewaartermijnen. Dat geldt dus voor de Basisregistraties, maar ook voor registraties waar gegevens in gekopieerd |

[14] Het onderscheid Nederlanders en niet-Nederlanders is nodig om te komen tot een goed werkend stelsel van Federatief Identiteitenbeheer, waarbij elk land betrouwbare Digitale Bron Identiteiten (DBI) uitgeeft aan de eigen burgers en zo min mogelijk landen een DBI uitgeven aan eenzelfde natuurlijke persoon.

| | |
|---|---|
| | worden, audit- en loggingsregistraties, fraude-preventie-registraties e.d.<br>En vanuit de AVG is ook een inzage mogelijkheid van burgers vereist: hoe gemakkelijk kunnen burgers dan inzage krijgen in wie deze gegevens inziet? Een papieren aanvraag (conform afspraken met de AP) ligt niet voor de hand bij een digitale werkelijkheid.<br>4. Standaarden<br>De richtlijnen uit de AVG en BIO worden gevolgd bij het verzamelen van metadata (IP-adres, tijdstip authenticatie, afgenomen dienst) tijdens het gebruik van een identificatiemiddel.<br>5. Afspraak<br>Bij het stellen van een kader hoort ook Toezicht houden op de naleving van dat kader.<br>De overheid zorgt voor onafhankelijk toezicht op onder meer het afgesproken gebruik van de digitale bronidentiteit en het handelen van de betrokken partijen in de digitale identiteitinfrastructuur.<br>Standaarden<br>Reeds beschikbare algemene kaders zijn: WDO, AVG, BIO en de Wabb.<br>Aanvullend zijn de ISO norm 24760 en de W3C norm DID voor de inrichting van Identiteitenbeheer en de eIDAS voor (federatief) Identiteitenbeheer. |
| **Voorbeelden** | |

| | |
|---|---|
| **ID** | 2 |
| **Omschrijving** | Uitgeven en beheren van unieke en betrouwbare digitale bronidentiteiten. |
| **Beschrijving** | De overheid zorgt voor betrouwbare digitale identiteiten die we kunnen beschouwen als de digitale bronidentiteit (DBI)[15] voor de Nederlandse burgers en bedrijven.<br>En indien geen afdoende betrouwbaar alternatief bestaat, zorgt de Nederlandse overheid ook voor een DBI voor personen die géén Nederlandse Nationaliteit hebben, maar wel te maken hebben met de dienstverlening van de Nederlandse overheid.<br>Deze digitale bron-identiteiten kunnen burgers en bedrijven gebruiken in contact met de overheid. Van belang is dat de gegevens van zo'n DBI door alle overheidsorganisaties gebruikt kunnen worden voor de identificatie en authenticatie van burgers en andere natuurlijke personen waaraan diensten worden verleend.<br>En ook in contact met andere overheden die deze bron-identiteiten erkennen (zoals in de EU is geregeld conform de eIDAS Verordening).<br><br>Bedrijven (private partijen) kunnen ook diverse digitale identiteiten van personen en rechtspersonen uitgeven en beheren. Die beschouwen we niet als bron-identiteit, maar als afgeleide of andersoortige identiteiten, afhankelijk van het daarbij gehanteerde normenkader. |
| **Rationale** | Een betrouwbare digitale identiteit is een voorwaarde voor digitaal actief kunnen zijn. |

[15] Het kan alleen een bron-identiteit zijn als we het over Nederlandse burgers en bedrijven hebben. Immers, als we ook Buitenlandse burgers en bedrijven een "bron-identiteit" verstrekken, dan wordt dat verwarrend met de "bronidentiteit" die het land van hun Nationaliteit uitgeeft. De eIDAS verordening gaat ook uit van zo'n federatieve opzet van Identiteitenbeheer: je hebt het recht de aan jou verstrekte bron-identiteit van jouw land te hergebruiken in andere landen van de EU.

| | |
|---|---|
| **Implicaties** | 6. Afspraak<br>Er is geen algemeen erkende instantie die nu wereldwijd betrouwbare digitale bronidentiteiten uitgeeft voor alle mensen op aarde.<br>Als elk land daarom z'n eigen bronidentiteiten uitgeeft, dan is aanvullend nog een wereldwijd afsprakenstelsel nodig voor Federatief Identiteitenbeheer (te vergelijken met het wereldwijde afsprakenstelsel voor het erkennen van elkaars Nationaliteiten en paspoorten).<br>Nederland zal daartoe een DBI uitgeven aan alle personen die met de dienstverlening van de Nederlandse overheid te maken hebben.<br>7. Afspraak<br>Het uitgeven en beheren van een DBI door de overheid volgt een nauwgezet proces, dat eisen bevat voor onder meer de vaststelling van de fysieke gebruiker (burger/bedrijf), de juistheid en real-time actualiteit van de geregistreerde gegevens[16] (ook bij het optreden van diverse levensgebeurtenissen), tijdelijke blokkade bij verlies, revocatie bij diefstal of misbruik e.d., waarvoor de overheid zorgdraagt.<br>8. Afspraak<br>RvIG, in samenwerking met het huidige netwerk van gemeenten, is de verstrekker van digitale bronidentiteiten aan natuurlijke personen met de Nederlandse Nationaliteit.<br>Daarnaast kan RvIG ook digitale bronidentiteiten toekennen aan personen die geen Nederlandse Nationaliteit hebben, maar wel met de Nederlandse overheid te maken krijgen, zoals asielaanvragers, tijdelijke werkenden uit buitenland en tijdelijke studenten uit buitenland.<br>Als RvIG dat eenmalig doet voor niet-Nederlanders, dan hoeven grote uitvoeringsorganisaties als IND, DUO, Politie, Belastingdienst, SVB, UWV en Kadaster niet zelf meer digitale identiteiten aan die personen toe te kennen.<br>Voorziening<br>Het ligt voor de hand dat de BRP wordt (her)gebruikt als authentieke bron voor identiteiten van Nederlanders en niet-Nederlanders, aangezien het nu dé bron is voor het BSN en door de Nederlandse overheid gehanteerde digitale identiteiten en ook het life-cycle management daar goed kan worden beheerd. De DBI wordt echter niet gebaseerd op "ingezetene zijn" en behoeft vooral een "levenslange" unieke ID.<br>Het BSN kan mogelijk dienen als unieke identificerende gegeven van een DBI.<br>9. Afspraak<br>KvK is de verstrekker van digitale bronidentiteiten aan bedrijven (rechtspersonen).<br>Voorziening<br>Het HR kan mogelijk dienen als authentieke bron voor identiteiten van ondernemingen en stichtingen.<br>Het KVK-nummer kan mogelijk dienen als unieke identificerende gegeven van een bedrijf.<br>Het OIN-register kan mogelijk dienen als authentieke bron voor overige rechtspersonen met het OIN als uniek identificerend gegeven.<br><br>Standaarden<br>De huidige standaarden voor digitale identiteiten kunnen nog een grote uitdaging worden: de wereldwijde standaarden voor toegang tot digitale diensten verloopt op basis van ISO-normen, terwijl de wereldwijde standaarden voor reisdocument de ICAO-normen hanteren. Dit kan zorgen voor een belangenstrijd (wie moet aanpassen, betaalt hoge kosten e.d.).<br>10. |

[16] De set gegevens die een DBI in ieder geval omvat, bestaat uit de identificerende attributen zoals nu ook voorkomen op de WID's: naam, adres, woonplaats en postadres, geboortedatum en geslacht voor personen en naam, adres, postadres, rechtsvorm en vestigingsplaats voor bedrijven (rechtspersonen).
Overige authentieke attributen uit deze en andere basisregistraties zijn buiten scope van de DBI en dienen op een andere wijze ontsloten te worden. Dit valt buiten de scope van het identificatie en authenticatie domein.

| | |
|---|---|
| | 11. Afspraak<br>De behoefte bestaat dat de digitale bronidentiteiten van burgers ook gebruikt mogen worden in contact met bedrijven.<br>Daartoe zou wellicht de Wabb[17] op onderdelen moeten worden aangepast.<br>Een alternatief is dat betrouwbare, van de bronidentiteit afgeleide (pseudonieme) identiteiten worden gebruikt.<br>12. Voorziening<br>Ook bestaat behoefte aan een Nationaal Entiteiten Register, waarin digitale identiteiten kunnen worden opgenomen van voorzieningen en computers (servers) e.d. Dit vereist nog nadere uitwerking, maar kan gezien worden als een soortgelijke registratie als de BRP voor persoonsgegevens. |
| **Voorbeelden** | |

| | |
|---|---|
| **ID** | 3 |
| **Omschrijving** | Afsprakenstelsel digitaal vertrouwen ten behoeve van uitgifte en beheer van betrouwbare identificatie- en authenticatiemiddelen. |
| **Beschrijving** | Als een gebruiker (burger/bedrijf) bij een publieke of private dienstverlener inlogt, dan wordt via het gebruikte identificatiemiddel nagegaan wie die gebruiker is. De inloggegevens worden daartoe geverifieerd en vergeleken met de gegevens die zijn geregistreerd over reeds bekende gebruikers. Als er een match is, dan is de gebruiker geïdentificeerd (dan is zijn digitale identiteit met een bepaalde zekerheid bekend) en kunnen de identiteitsgegevens mogelijk worden hergebruikt voor andere aan die digitale identiteit gerelateerde gegevens. Deze functie richt zich op betrouwbaarheid van identificatie- en authenticatiemiddelen, niet op het hergebruik van de identiteitsgegevens (dat regelt de generieke functie Regie op gegevens en is een breder domein)[18].<br><br>De rol van de overheid bij digitale identificatie- en authenticatiemiddelen is vooral kaderstellend, gericht op toezicht en de werking en de betrouwbaarheid van de middelen en het stelsel als geheel.<br><br>De overheid biedt via private en publieke partijen de mogelijkheid om door de overheid uitgegeven administratieve identiteiten (de digitale bron-identiteiten) van burgers en bedrijven te verifiëren.<br>Voor dat verifiëren zijn betrouwbare authenticatiemiddelen nodig (ook wel inlogmiddelen genoemd). De overheid zal die authenticatiemiddelen zelf aanbieden als daarmee de werking, betrouwbaarheid en veiligheid van het digitaal zaken doen wordt bevorderd, of wanneer dit gedreven wordt door relevante Europese en/of internationale ontwikkelingen en standaarden (zoals bijvoorbeeld de internationale luchtvaartstandaarden voor identificatie, ICAO/DTC).<br>De overheid wil echter ook private partijen de mogelijkheid geven om de markt |

[17] De Wabb bepaalt het gebruik van het BSN. Voor private partijen is het gebruik van het BSN momenteel niet toegestaan. Door pseudonimisering kan de overheid regelen dat een organisatie (privaat of publiek) na een authenticatie tegen de BRP niet een BSN ontvangt, maar een ander identificerend gegeven. Het BSN-koppelregister is daartoe opgezet.

[18] Identificatie en authenticatie liggen dicht tegen elkaar aan, maar is functioneel gezien verschillend en daarom als aparte generieke functie benoemd. Er is daarbij verschil tussen de fysieke wereld en de digitale wereld. Zo bevat een fysiek WID-document gegevens die de identiteit van een persoon weergeven. Aan de hand van de foto op het WID-document kan je verifiëren of het document behoort bij de persoon die voor je staat en dan kan je de identiteitsgegevens (her)gebruiken. In de digitale wereld is slechts het identificatiemiddel in handen van de persoon en zijn de identiteitsgegevens opgenomen in een registratie die zowel bij de dienstverlener zelf kan staan als bij een andere partij (ook wel een Identity Provider genoemd). Als de dienstverlener de identiteitsgegevens wil krijgen, zal de Identity Provider die op basis van een overeenkomst aan de dienstverlener kunnen verstrekken via een digitaal “Identificatiemiddel”.

| | |
|---|---|
| | voor authenticatiemiddelen te betreden, zodat ook private inlogmiddelen te gebruiken zijn in het contact tussen burgers en de overheid. Zoals dat reeds mogelijk is in het contact tussen bedrijven en de overheid via het Afsprakenstelsel eHerkenning. |
| **Rationale** | Zonder authenticatiemiddelen kunnen we niet vaststellen hoe betrouwbaar een gebruikte digitale identiteit is. |
| **Implicaties** | 13. Afspraak<br>De overheid organiseert een open samenwerkingsplatform voor het opstellen en beheren van een Afsprakenstelsel Digitaal Vertrouwen (Trust Framework), waarin alle leveranciers van authenticatiemiddelen kunnen meewerken en discussiëren over de te hanteren afspraken, standaarden en voorzieningene.<br>14. Afspraak<br>De overheid zal als dienstverlener alle publieke en private authenticatiemiddelen accepteren die voldoen aan dat Trust Framework.<br>15. Voorziening<br>De overheid biedt alle personen en rechtspersonen waaraan een DBI is toegekend, tenminste één authenticatiemiddel per betrouwbaarheidsniveau waarmee ze hun eigen identiteit kunnen bewijzen.<br>DigiD is zo'n authenticatiemiddel.<br>Dit impliceert dat verstrekking ook aan niet-Nederlanders zal geschieden. Voorheen is vernomen (onder meer door de SVB), dat BZK voornemens is om het authenticatiemiddel DigiD Substantieel alleen beschikbaar te stellen voor Nederlanders. Als dat komt omdat DigiD Substantieel nu alleen werkt met een Nederlands WID, dan zou een aanpassing van de regelgeving nodig zijn om ook niet-Nederlanders van DigiD substantieel te voorzien (als niet-Nederlander kan je er dus wel gebruik van maken als je een Nederlands rijbewijs hebt). Met het voorliggende voorstel wordt het wel mogelijk dat de SVB diensten aan niet-Nederlanders kan gaan leveren op basis van het authenticatiemiddel DigiD Substantieel of DigiD Hoog. Dat zou een goede vooruitgang zijn. Dan ligt nog wel de vraag voor wie dat gaat regelen en op welke termijn dat beschikbaar is.<br>16. Afspraak<br>Voor elk soort authenticatiemiddel wordt het betrouwbaarheidsniveau vastgesteld[19] en dat wordt publiekelijk gepubliceerd opdat alle betrokken partijen daar gebruik van kunnen maken.<br>17. Voorziening<br>Aanvullend daaraan zal er een mogelijkheid zijn om te controleren of een (specifiek) authenticatiemiddel wel of niet mag worden gebruikt (omdat het in onderzoek is, of ingetrokken oid.).<br>18. Voorziening<br>Om efficiënt om te gaan met al deze mogelijke authenticatiemiddelen, kunnen "routerings" voorzieningen worden ingezet die de verschillende authenticatiemiddelen van de gebruikers kunnen verwerken en meer standaardiserende en uniformerende aansluitingen verzorgen naar de dienstverleners (overheidsorganisaties en private partijen).<br>19. Standaarden<br>Alle inlogmiddelen van de overheid moeten gebruik maken van BSN-gebaseerde pseudoniemen.<br>Deze stelling zou je bijna kunnen afleiden uit de Wabb, waarin is bepaald dat een burger (en overigens zijn ambtenaren ook burgers, maar dan met een specifieke rol) het recht heeft om het BSN te gebruiken in contact met de overheid.<br>De Autoriteit Persoonsgegevens heeft voorheen (in 2011) geoordeeld dat |

[19] Deze betrouwbaarheidsniveau 's kunnen worden bepaald o.b.v. de AMvB van de WDO die recent door BZK is opgeleverd.

| | |
|---|---|
| | het BSN niet voor en door ambtenaren gebruikt zou mogen worden. Met een pseudonimisering van het BSN kan het euvel dat daarmee de privacy van de persoon kan worden geschaad, worden verholpen.<br>20. Voorziening<br>Wat betreft de huidige voorziening BSNk zal aanpassing nodig zijn om die in lijn te brengen met Europese en Internationale standaarden en voorzieningen.<br>21. Afspraak<br>De overheid is nu erg gericht op het verwerken van digitale identiteiten via het BSN. Gezien de wereldwijde ontwikkelingen van Self Sovereign Identity (SSI) en Decentralized Identities (DID's), zou de overheid zich wellicht beter ook gaan voorbereiden op het kunnen omgaan met digitale identiteiten die niet zijn gebaseerd op het BSN. Daarbij is het nodig vooral te kijken naar mogelijkheden i.p.v. uitsluitingen. Dus niet iets met Wet- en regelgeving verbieden, maar aangeven wat geregeld wordt en open laten wat daarnaast allemaal mogelijk is. |
| **Voorbeelden** | |

| | |
|---|---|
| **ID** | 4 |
| **Omschrijving** | Single-Sign-On by default |
| **Beschrijving** | De overheid zorgt ervoor dat burgers en rechtspersonen in contact met de overheid zichzelf zo min mogelijk telkens opnieuw kenbaar hoeven te maken door extra in te loggen c.q. een authenticatie uit te laten voeren.<br>Dat extra inloggen is een grote ergernis bij gebruikers.<br>Single Sign On (SSO) zorgt er voor dat een persoon zich minder vaak hoeft te identificeren c.q. dat opnieuw hoeft te worden ingelogd e.d. Daarmee is SSO dus van invloed op de wijze waarop de authenticatie moet worden ingericht om het "gebruiker centraal" te maken (in plaats van te veel techniek gedreven).<br>Dat wringt soms met de noodzaak voor de overheid om zorg te dragen voor veiligheid en privacy. Hierom moet een balans worden gevonden. |
| **Rationale** | Het beperkt houden van het aantal digitale drempels om gemakkelijk zaken te kunnen doen met de overheid. |
| **Implicaties** | 22. Afspraak<br>Overheidsorganisaties moeten (toekomst WDO) burgers laten inloggen met een identificatiemiddel dat past bij het benodigde betrouwbaarheidsniveau van de betreffende dienst(en). In principe niet met een hoger betrouwbaarheidsniveau dan nodig.<br>NB. Door dit uitgangspunt zal in bepaalde gevallen geen sprake kunnen zijn van een volledige SSO. Het zorgt echter wel voor een redelijke balans tussen informatieveiligheid / privacy en gebruiksgemak.<br>23. Voorziening<br>Als een burger al is ingelogd met een identificatiemiddel, dan kan de burger zonder opnieuw in te hoeven loggen alle diensten afnemen met een gelijkwaardig of lager betrouwbaarheidsniveau dan het betrouwbaarheidsniveau van dat identificatiemiddel.<br>Bij een hoger benodigd betrouwbaarheidsniveau moet wel opnieuw worden ingelogd met een meer betrouwbaar identificatiemiddel.<br>24. Afspraak<br>Vanuit het oogpunt van informatieveiligheid kunnen termijnen worden |

| | |
|---|---|
| | gesteld aan de duur van een online sessie, waarna wederom een authenticatie mag plaatsvinden. |
| **Voorbeelden** | |

| | |
|---|---|
| **ID** | 5 |
| **Omschrijving** | Regie op de eigen identiteitsgegevens. |
| **Beschrijving** | De overheid biedt burgers en bedrijven de mogelijkheid om de gegevens uit de door de overheid aan hen uitgegeven administratieve identiteit (de digitale bronidentiteit) te hergebruiken.<br>Je kunt deze generieke functie zien als een digitale variant van het aflezen van de uitgegeven fysieke WID-documenten, zoals een paspoort of identiteitskaart. Daarmee is niet gezegd dat de overheid die gegevens aan derden ter beschikking moet stellen. Dat kan de burger c.q. het bedrijf in kwestie immers zelf verzorgen, indien hij zich volledig bewust is van de gevolgen van dit delen. Na toestemming van de persoon of het bedrijf, kan ook de overheid die gegevens binnen de overheid aan partijen buiten de overheid beschikbaar stellen.<br>Een belangrijk aandachtspunt is dan, de mate waarin gebruikers (burgers/bedrijven) in staat zijn om zelfstandig overzicht te houden over de consequenties voor identificeren en authentiseren en in welke mate de overheid bescherming zou moeten bieden vanuit een zorgplicht[20]. Dit vraagt nog veel aandacht vanuit ook het bepalen van behoefte burgers en bedrijven. |
| **Rationale** | Het beperkt houden van het aantal digitale drempels om gemakkelijk zaken te kunnen doen met de overheid en andere partijen. |
| **Implicaties** | 25. Voorziening<br>De overheid biedt burgers en rechtspersonen de mogelijkheid om hun identiteitsgegevens naar een informatiedrager te laten kopiëren.<br>Diverse oplossingen uit de markt sorteren hier reeds op voor (o.a. ItsMe, IRMA). Ook zijn er voorbeelden van het gebruik van identiteitsgegevens bij private partijen, zoals voor leeftijdscontroles in Horeca en slijterijen.<br>26. Afspraak<br>De overheid geeft aan welke zorgplicht bestaat bij het (door-)verstekken van de identiteitsgegevens. |
| **Voorbeelden** | |

| | |
|---|---|
| **ID** | 6 |
| **Omschrijving** | Toezicht en Handhaving bij ID-fraude. |
| **Beschrijving** | Identiteitsfraude treedt op wanneer illegaal gebruik wordt gemaakt van iemands persoonsgegevens (bijvoorbeeld voor een bestelling via internet).<br>Een gecompromitteerde digitale identiteit maakt dat je niet digitaal actief kunt zijn, sluit je uit van de maatschappij en heeft daardoor een enorme persoonlijke impact.<br>De overheid zal maatregelen nemen om dat zo veel mogelijk te voorkomen. |

[20] In dat kader ter suggestie een vervolgstap om een visie te formuleren rondom ethisch datagebruik

| | |
|---|---|
| | En tegelijkertijd, wetend dat het voorkomt, zal de overheid bij zo'n ID-fraude zo snel en goed mogelijk de gevolgen (laten) herstellen.<br><br>Vanuit het gezichtspunt van een natuurlijke persoon is herstel c.q. her-uitgifte van de DBI en gelieerde identificatie- en authenticatiemiddelen erg afhankelijk van de persoonlijke wensen en eisen die zijn gesteld aan de mate van privacy, veiligheid e.d.<br>En vanuit het gezichtspunt van de overheid als dienstverlener aan vele individuele personen, worden snel eisen en wensen gesteld aan de "beheersbaarheid" en het beheer-gemak van de voorzieningen, waardoor snel centrale registers e.d. in beeld komen.<br>En hoe verhoudt dit zich dan met (het herstel van) identificatie- en authenticatiemiddelen die vanuit private partijen aan wereldburgers beschikbaar is gesteld voor de (private) dienstverlening?<br><br>Er zijn natuurlijk nog veel meer vormen van fraude[21], maar deze generieke functie hebben we beperkt tot de ID-fraude. |
| **Rationale** | Borgen van de digitale inclusiviteit. |
| **Implicaties** | 27. Afspraak<br>De Overheid stelt eisen aan de beveiliging in het stelsel ter voorkoming van misbruik.<br>28. Afspraak<br>De overheid monitort het gebruik van identificatie- en authenticatiemiddelen en speurt actief naar misbruik daarvan.<br>Daar waar overheidsorganisaties het vermoeden hebben van fraude, bestaat reeds een signalerings- en meldingsplicht bij de door overheid aangestelde opsporingsinstanties.<br>29. Voorziening<br>De overheid realiseert een Nationale fraude-preventie-voorziening waarmee alle betrokken organisaties tot een meer gezamenlijke aanpak kunnen komen, onder meer door relevante informatie gezamenlijk te delen.<br>30. Voorziening<br>De overheid zorgt voor een landelijk Centraal Meldpunt Identiteitsfraude (CMI), dat samen met Slachtofferhulp binnen redelijke termijn zorgt voor het herstel van de gevolgen.<br>31. Afspraak<br>De overheid geeft binnen een zeer korte termijn[22] een nieuwe unieke en betrouwbare digitale identiteit uit aan burgers en rechtspersonen waarvan de digitale identiteit gecompromitteerd is. |
| **Voorbeelden** | |

[21] We kennen meer dan identiteitsfraude. De meest voorkomende zijn: Acquisitiefraude (versturen van spookfacturen, telefonisch misleiden of misleiden via een vertegenwoordiger), Slamming (ongewild overzetten van de ene telefonieaanbieder naar de ander, ook wel lijnkaping waar de Autoriteit Consument en Markt (ACM) voor waarschuwt), Voorschotfraude (tegen het geven van een voorschot wordt onterecht een hoge vergoeding beloofd), Afpersing (eisen van een geldbedrag, onder dreiging van bijvoorbeeld geweld of het openbaar maken van belastende informatie) en Schijnwerkelijkheid / Katvangers (stroman die, bij illegale of criminele activiteiten, in naam eigenaar of houder van een voertuig, bedrijf, bankrekening etc. is, met als doel om de werkelijke eigenaar of houder buiten bereik van de autoriteiten te houden).
Al deze vormen van fraude kunnen leiden tot een situatie waarin het goed zou zijn als een (her)nieuwe DBI wordt uitgegeven.

[22] Het verkrijgen van een nieuwe digitale identiteit zal binnen een zeer korte tijd moeten gebeuren (denk aan dagen en niet weken), aangezien je in zo'n situatie in het geheel NIET meer digitaal zaken kunt doen met de overheid en derden.

| | |
|---|---|
| **ID** | 7 |
| **Omschrijving** | IAM-functies binnen de overheid |
| **Beschrijving** | IAM voor burgers en bedrijven zorgt voor adequate toegang tot de dienstverlening van de overheid.<br>Om die diensten te kunnen leveren, zal bijvoorbeeld de overheid ook IAM-functies moeten toepassen binnen de bedrijfsvoering van al haar organisaties. De medewerkers hebben immers eenvoudig en adequate toegang nodig tot alle relevante informatie en voorzieningen.<br>IAM-functies binnen de overheidsorganisaties zorgt er voor dat de medewerkers van de overheid (ambtenaren, ingehuurden, servicepersoneel e.d.) niet achtergesteld blijven bij de mogelijkheden die ze als burger of ondernemer e.d. kunnen ervaren op basis van de voorgestelde GF's . Waarom zouden burgers immers op 1 plek diverse diensten kunnen afnemen met een goede toeleiding met SSO e.d. en ambtenaren -die goed met elkaar moeten samenwerken om die diensten aan die burgers te leveren- niet gebruik mogen maken van de GF's die we daar juist voor hebben ontwikkeld?<br>De personen die daarbij worden betrokken hebben feitelijk al een bron-identiteit van de overheid verkregen: het zijn personen met een Nederlandse Nationaliteit, dan wel personen die in Nederland werken en daartoe in de RNI zijn geregistreerd en een BSN en een VOG e.d. hebben.<br>Desondanks worden personen in de rol van ambtenaar of ingehuurde medewerkers e.d. door de Autoriteit Persoonsgegevens (AP) als aparte groep beschouwd en mag het BSN niet worden gebruikt voor identificatie en authenticatie van deze personen in deze rol. Dit leidt ertoe dat afzonderlijke voorzieningen moeten worden gebruikt voor het identiteitenbeheer en toegangsbeheer van overheidsmedewerkers. |
| **Rationale** | Het beperkt houden van het aantal digitale drempels om gemakkelijk samen te kunnen werken binnen de overheid. |
| **Implicaties** | 32. Afspraak<br>De overheid maakt afspraken over de toepassing van IAM-functies bij de overheidsorganisaties.<br>Standaard<br>Denk hierbij aan wat de Rijksoverheid heeft opgesteld in het Normenkader IdM (pdf 361 kB), dat tevens de basis is geweest voor de uitrol van de Rijkspas.<br>33. Voorzieningen<br>De overheid stelt voorzieningen beschikbaar voor deze IAM-functies.<br>Denk aan de RidM en het RIN voor de identificatie van medewerkers van de Rijksoverheid, of de Rijkspas voor fysieke- en logische toegang bij de Rijksoverheid.<br>Deze voorzieningen zijn nog niet geheel dekkend voor de gehele overheid ! |
| **Voorbeelden** | |

## Bijlage: Definities:

Voor de leesbaarheid zijn onderstaande gehanteerde definities opgenomen. Een meer uitgebreid overzicht van de begrippen die overheidsorganisaties en programma's zoals eTD en eID hanteren voor Identiteitenbeheer en Toegangsbeheer, zijn opgenomen in de NORA: https://www.noraonline.nl/wiki/Begrippen_IAM.
Door de werkgroep is echter geconstateerd dat definities in verschillende wetten/verordeningen en documenten verschillen. Dat heeft de werkgroep niet opgelost.

**Afgeleid digitaal / elektronisch identificatiemiddel:** een middel om een (rechts)persoon aan een bepaalde geregistreerde identiteit te linken. Deze identiteit is afgeleid van een digitale bronidentiteit van een (rechts)persoon zoals door de overheid vastgelegd.
**Attribuut:** Een uniek kenmerk of gegeven van een entiteit
**Authenticatie:** een proces dat de bevestiging van de identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt.
Authenticatiemiddel: Een middel op grond waarvan authenticatie van een gebruiker kan plaatsvinden.
**Authenticatiefactor:** een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de drie volgende categorieën valt.

- Op bezit gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is.
- Op kennis gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt.
- Inherente authenticatiefactor: een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit.

**Autorisatie:** Autorisatie is het proces van vaststelling van het mandaat dat een geauthentiseerde identiteit heeft en de rechten die er bij dit mandaat horen.
**Betrouwbaarheidsniveau:** de mate waarin vertrouwen kan worden gesteld in een identificatiemiddel
**Bronidentiteit:** Een bronidentiteit (of basisidentiteit) is de identiteit van een (rechts)persoon zoals nu door de overheid vastgelegd en vormgegeven via identificatiemiddelen (identiteitsbewijzen) die in het maatschappelijk verkeer te gebruiken zijn (paspoort, identiteitskaart of rijbewijs of in de toekomst mogelijk meer).
**Digitale Bronidentiteit:** Een door de overheid uitgegeven, erkende en in de wet en regelgeving verankerde, verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale domein voor gebruik in de publieke en private sector. De DBI bevat een minimale set van identiteitsgegevens die nodig zijn in het maatschappelijk verkeer.
**Digitale / elektronische identiteit:** een identiteit in de onlinewereld voor entiteiten. Een digitale identiteit kan bestaan uit verschillende aspecten (attributen) die over een bepaalde entiteit geregistreerd staan. ISO/IEC stelt: een digitale identiteit is een set attributen die te relateren zijn aan een entiteit.
**Digitale / elektronische identiteitinfrastructuur:** het geheel van stelsels, afspraken, standaarden en voorzieningen, rond de digitale identiteit van (rechts)personen.
**eID:** eID staat voor Electronic Identification.
**eIDAS:** eIDAS staat voor Electronic Identification (eID) and Trust Services (AS). Het is een initiatief van de Europese Commissie met als doel om elektronische interacties tussen ondernemingen, burgers en organisaties veiliger en efficiënter te maken en alle EU-landen elkaars eID en AS erkennen.
**Digitale / elektronische identificatie:** het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.
**Digitaal / elektronische identificatiemiddel**: een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst;
**Gezaghebbende bron:** elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond.

**Identificatie:** het proces van het kenbaar maken van een identiteit.
Identificatiemiddel: (fysiek of digitaal) middel uitgegeven zodat degene voor wie het is uitgegeven zich kan identificeren.
**Identiteit:** Een identiteit bestaat uit de geregistreerde aspecten (attributen) die in voldoende mate bepalen wie iemand of iets is.
**Juridische identiteit:** een juridische identiteit (of publiekrechtelijke identiteit) is een identiteit die door de wet vastgelegd en gereguleerd is.
**Persoonsidentificatiegegevens**: een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld;
**Registerhouder:** De partij die gegevens registreert en daarmee een gezaghebbende bron kan vormen
**Self Sovereign Identity (SSI):** Het concept Self Sovereign Identity legt de controle en de macht over een digitale identiteit volledig bij de entiteit die deze digitale identiteit representeert. Dit vereist volledige onafhankelijkheid van een centraal register of centrale autoriteit.
**Vertrouwende partij:** een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst