Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Onderzoeksrapport Digitale bronidentiteit

Versie 1.0
7 oktober 2022

Inhoud

1 Samenvatting 4
1.1 Onderzoeksvraag 1: definiëren van de digitale bronidentiteit 5
1.2 Onderzoeksvraag 2: beschrijving van het identiteitsecosysteem 5
1.3 Onderzoeksvraag 3: juridische en ethische analyse 5
1.4 Onderzoeksvraag 4: analyse in verhouding tot bestaande voorzieningen 6
1.5 Onderzoeksvraag 5: prototype 6

2 Inleiding 7
2.1 Aanleiding en doelstelling 7
2.2 Aanpak 7
2.3 Scope 8
2.4 Kaders 8
2.5 Leeswijzer 8

3 De digitale bronidentiteit 10
3.1 Waarom een digitale (bron)identiteit 10
3.1.1 Visie op digitale identiteit 11
3.1.2 *Conceptverordening eIDAS* 12
3.2 Definitie digitale bronidentiteit 13
3.3 Wat kun je met de digitale bronidentiteit 13

4 Hoofdstuk 4 Ontwikkeling van de DBI 15
4.1 Inleiding 15
4.2 Welk proces wordt ondersteund door de DBI en het gebruiksdoel? 15
4.3 De specifieke opbouw van de DBI 16
4.4 Verbinding met bestaande administratieve systemen. 18
4.5 Minimale gegevensset 19
4.6 Biometrische gegevens 19
4.7 De rol van de basisregistratie en de noodzaak van de verwijzing. 20
4.8 De DBI duurzaam aanwijsbaar maken en waarom? 21
4.9 De combinatie van de DBI en de Wallet 22
4.10 Attesten en hun toegevoegde waarde 22
4.11 Ontstaan van de DBI 23
4.12 DBI ten opzichte van andere authenticatiemechanismen 23
4.13 Uitgangspunten 23
4.14 Verstrekking aan de burger 24

5 Het identiteitsecosysteem 26
5.1 De noodzaak van een identiteitsecosysteem 26
5.2 Processen 27
5.2.1 *Aanvraag en uitgifte* 27
5.2.2 *Beheer* 27
5.2.3 *Gebruik* 27
5.3 Actoren 30
5.3.1 *Samenvatting van eisen uit de conceptverordening* 31
5.4 ICT-middelen 32

6 Juridische en ethische analyse van de bronidentiteit 33
6.1 De juridische analyse van de bronidentiteit 33
6.2 Juridisch kader rondom identiteit 33
6.2.1 *ICAO* 33
6.2.2 *Algemene Verordening Gegevensbescherming (AVG)* 33
6.2.3 *eIDAS-verordening* 35

6.2.4 *Wet basisregistratie personen* 36
6.2.5 *Wet Digitale Overheid* 37
6.2.6 *Wet op de Identificatieplicht* 38
6.2.7 *Paspoortwet* 38
6.2.8 *Wetboek van Strafrecht* 39
6.3 Tussenconclusie 39
6.4 Juridische basis voor een DBI 40
6.5 Ethische analyse van de digitale bronidentiteit 41
6.5.1 *Privacy* 41
6.5.2 *Veiligheid* 41
6.5.3 *Autonomie* 42
6.5.4 *Controle over technologie* 42
6.5.5 *Inclusie* 42
6.5.6 *Menselijke waardigheid* 42
6.5.7 *Vertrouwen* 43
6.5.8 *Economie* 43
6.5.9 *Gemak* 43
6.5.10 *Transparantie* 43

7 Hoe verhoudt de digitale bronidentiteit zich tot bestaande voorzieningen? 44

7.1 NIK 44
7.2 Paspoort 45
7.3 Rijbewijs 46
7.4 DigiD 46
7.5 DigiD machtigen 47
7.6 Stelsel van Basisregistraties 47
7.7 Mijn Overheid 49
7.8 Wallet 49
7.9 Self Sovereign Identity (SSI) 50

8 Prototype DBI 52
8.1 Introductie 52
8.2 Houding naar en gebruik van een DBI 52
8.2.1 *Concept digitaal identificeren* 52
8.2.2 *Redenen om een digitale bronidentiteit te willen gebruiken* 53
8.2.3 *Redenen om een digitale bronidentiteit niet te gebruiken* 54
8.2.4 *Toegevoegde waarde, gevoel van veiligheid en gevoel van controle* 55
8.3 Ontwerp van een digitale bronidentiteit en (NL) wallet 57
8.4 Visualisaties 61
8.4.1 *Klantreizen (Samen met dit rapport gepubliceerd)* 61
8.4.2 Klikbaar model 61

9 Bijlage: maatschappelijke kansen en uitdagingen 62

10 Bijlage: diensten in het identiteitsecosysteem 63

11 Bijlage: de NL Wallet 65

12 Bijlage: de onderzoeksvragen 66

13 Bijlage: definitielijst 68

14 Bijlage: literatuurlijst 70

1 Samenvatting

De digitale transitie vindt razendsnel plaats. Steeds meer processen zijn deels of volledig digitaal en vertrouwen in de digitale wereld is essentieel. Zonder dit vertrouwen zullen burgers, ondernemers en overheden twijfelen om digitaal zaken te doen. Een betrouwbare digitale identiteit en identiteits-ecosysteem is hiervoor noodzakelijk. De Visiebrief digitale identiteit[1] (verder: Visiebrief) introduceert de digitale bronidentiteit (DBI): een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector.

Ook op Europees niveau onderkent men het belang van vertrouwen in de digitale wereld ten bate van economische en sociale ontwikkeling. In 2018 is dan ook de eIDAS-verordening[2] in werking getreden. In eIDAS (*Electronic Identities And Trust Services*) spraken de Europese lidstaten af om dezelfde begrippen, betrouwbaarheidsniveaus en digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Dit kan alleen met een betrouwbare online identiteitscheck.[3] De eIDAS-verordening bleek na evaluatie echter niet geheel te voldoen. De Europese Commissie diende daarom op 3 juni 2021 een voorstel in tot wijziging van de eIDAS-verordening (verder: concept-verordening).[4]

De Europese Commissie verplicht in dit voorstel de lidstaten onder meer tot de uitgifte van een Europese portemonnee voor digitale identiteit (*European Digital Identity Wallet*). Deze wallet stelt een gebruiker in staat om attributen met betrekking tot zijn/haar identiteit op te slaan en op verzoek aan vertrouwende partijen te verstrekken. Het voorstel van de Commissie moet tegen 2030 leiden tot een brede uitrol van een in Europa bruikbare digitale identiteit.[5] Het voorstel is dan ook in aanvulling op de Visiebrief als kader meegenomen in de uitwerking van de DBI.

Dit rapport schetst een conceptueel beeld van hoe de DBI eruit zou kunnen zien. Daarbij zijn vijf onderzoeksvragen[6] als leidraad genomen:
1. Definiëren van de digitale bronidentiteit;
2. Beschrijving van het identiteitsecosysteem;
3. Juridische en ethische analyse van de bronidentiteit;
4. Analyse bronidentiteit in verhouding tot bestaande voorzieningen;
5. Ontwerpen prototype: klantreis digitale bronidentiteit.

Dit conceptuele beeld van de DBI geeft inzicht in nog te beantwoorden beleidsvragen voordat een volgende stap gezet kan worden in de ontwikkeling van een DBI.

[1] Visiebrief digitale identiteit, Tweede Kamer, vergaderjaar 2020–2021, 26 643, nr. 743.
[2] Verordening (EU) 2014/910 van het Europese Parlement en de Raad 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L257).
[3] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/eidas/
[4] Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, com (2021) 281.
[5] Ibidem.
[6] Deze onderzoeksvragen komen uit de opdracht aan het project, zie de paragrafen 2.2 en 13.2.

1.1 Onderzoeksvraag 1: definiëren van de digitale bronidentiteit

Bij het definiëren van de digitale bronidentiteit is gekeken naar de verzameling gegevens die een persoon in het digitale domein representeert. Op basis van de DBI kunnen personen deze identiteit laten authentiseren. De DBI moet voldoende gegevens bevatten voor het beoogde gebruik:

1. Minimale gegevensset, zoals ook opgenomen in de Visiebrief. Een uitbreiding van deze set lijkt niet nodig; de minimale gegevens (familienaam, voornamen, geboortedatum, unieke identificatiecode) lijken voldoende. DBI kan gebruik maken van het BSN als unieke identificatiecode; maar DBI kan ook aanleiding zijn om een nieuwe code te introduceren.
2. Biometrische gegevens: welke kunnen worden gebruikt voor identificatie en/of authenticatie. Voor identificatie is centrale gegevensopslag nodig, dit is mogelijk niet gewenst. Voor authenticatie kan men ook decentrale opslag gebruiken. Dit rapport werkt uit welke biometrische kenmerken in aanmerking komen (vingerafdruk, gezicht, iris).
3. Verbinding met bestaande administratieve systemen, waarmee de betrouwbaarheid vergroot kan worden. Ook geeft dit voordelen indien bepaalde gegevens in de tijd veranderen. Het BSN kan als verbinding gebruikt worden.

Een unieke identifier is noodzakelijk om de DBI te gebruiken. Hiermee kan de DBI aangeroepen worden en gebruikt worden voor dienstverlening. Door van alle gegevens, inclusief de unieke identifier, bepaalde metagegevens vast te leggen, is de DBI persistent te gebruiken (dat wil zeggen: ook als een gegeven verandert, blijft de DBI goed toepasbaar). De unieke identifier kan vervolgens gekoppeld worden aan een digitale omgeving die het gebruik van de DBI voor dienstverlening mogelijk maakt: de wallet. Zodoende krijgt een persoon de beschikking over een wallet die verbonden is aan zijn/haar DBI.

1.2 Onderzoeksvraag 2: beschrijving van het identiteitsecosysteem

Het identiteitsecosysteem is het geheel aan (onder andere) wetten/afspraken, diensten/ producten, processen, applicaties en gegevensverzamelingen die nodig zijn om ervoor te zorgen dat een burger zich op een betrouwbare en veilige wijze digitaal kan identificeren en authentiseren bij publieke en private dienstaanbieders. Hierbij is een uitwerking gegeven van:

1. Processen. Dit zijn enerzijds de processen die nodig zijn voor de aanvraag en uitgifte van een DBI en voor het beheer ervan. Anderzijds betreft dit de processen die nodig zijn voor het gebruik van een DBI in het maatschappelijk verkeer. Bij de gebruiksprocessen is aangesloten bij de interactiepatronen van Regie op Gegevens.
2. Actoren. Dit zijn de actoren die (delen van) de processen uitvoeren om zo diensten te kunnen aanbieden, afnemen en onderling te kunnen afstemmen. Hierbij is aangegeven welke partijen aangewezen lijken voor bepaalde taken. Ook zijn enkele eisen aan specifieke actoren uitgewerkt, welke aansluiten op de Conceptverordening eIDAS.
3. ICT-middelen. Dit zijn de ICT-middelen die de uitvoering van de processen ondersteunen/mogelijk maken, zoals de DBI- beheervoorziening. Dit is vooralsnog een algemene aanduiding voor de voorzieningen die nodig zijn om een DBI te kunnen aanvragen, uitgeven en beheren. Ook gebruikers-ondersteuning is een functionaliteit van de DBI-beheervoorziening. Op een later moment wordt de DBI-beheervoorziening verder uitgewerkt in één of meerdere voorzieningen.

1.3 Onderzoeksvraag 3: juridische en ethische analyse

Vanuit juridische optiek is gekeken naar de vigerende wetgeving en de gevolgen van een DBI op bestaande en toekomstige wetgeving. Concluderend is de logische plek voor een wettelijke basis voor de DBI de (tweede tranche van de) Wet digitale overheid (Wdo). Op beleidsniveau zijn daarbij de volgende afwegingen te maken:

- Hoe privaat gebruik te bewerkstelligen, aangezien de Wdo nadrukkelijk is bedoeld voor het publieke domein;
- Hoe fysiek gebruik te blijven ondersteunen, aangezien de Wdo nadrukkelijk is bedoeld voor de digitale weg. Mogelijk dient de wallet (die gebruik maakt van de DBI) te worden aangewezen als identiteits-

middel in de Wet op de Identificatieplicht (Wid);
- Hoe de ontwikkelingen verlopen met betrekking tot de wijzigingen in de eIDAS-verordening en welke invloed deze hebben op de DBI en op nationale wet- en regelgeving;
- Hoe de verschillende verwerking(en) van persoonsgegevens voldoen aan de vereisten uit de Algemene Verordening Gegevensbescherming (AVG). Bijzondere aandacht is vereist voor verwerking van biometrische gegevens en het BSN;
- Hoe de verstrekking van gegevens uit de BRP juridisch kan worden ingericht volgens de Wet Brp.

Vanuit ethische optiek is gekeken naar de elementen die ten aanzien van de DBI aandacht behoeven. Wat technisch en juridisch mogelijk is, is namelijk niet altijd wenselijk in het licht van publieke waarden. Een eerste verkenning is gericht op privacy, veiligheid, autonomie, controle over technologie, inclusie, menselijke waardigheid, vertrouwen, economie, gemak en transparantie.

1.4 Onderzoeksvraag 4: analyse in verhouding tot bestaande voorzieningen

Beschreven zijn de voorzieningen die de grootste raakvlakken hebben met de DBI voor zover nu kan worden ingeschat. Per voorziening is stil gestaan bij de functie(s) en gebruiker(s). Ook is gekeken naar de bestaande functionaliteiten waar de DBI mogelijk gebruik van kan maken en wat voor eventuele gevolgen realisatie van de DBI op de voorziening heeft.

Hergebruik van DigiD (voor bijvoorbeeld het aanvraagproces) en van (onderdelen van) MijnOverheid is mogelijk. DigiD en MijnOverheid zijn ook te gebruiken om aan de hand van een DBI aanvullende gegevens van een persoon te ontsluiten in een wallet. De levering van die gegevens kan vanuit de basisregistraties. Hierbij is het mogelijk dat voor bepaalde diensten niet een bepaald gegeven vanuit een basisregistratie nodig is (bijvoorbeeld de geboortedatum), maar een attest (bewijs) dat de betreffende persoon 18 jaar of ouder is. Hiermee ontstaat een nieuwe manier van het ontsluiten van data.

1.5 Onderzoeksvraag 5: prototype

Centraal bij deze onderzoeksvraag staat het perspectief van de burger. De belangrijkste inrichtingskeuzen zijn in beeld gebracht. Daarnaast is visueel aangegeven hoe het ontwerp van een DBI en van een wallet er in de toekomst uit zouden kunnen zien en hoe een klantreis zou kunnen verlopen. Ook is een klikbaar prototype ontwikkeld.

Tot slot is onderzocht hoe burgers, met inbegrip van inclusie doelgroepen, tegen een digitale bron-identiteit aankijken. Dit onderzoek toont aan dat ruim vier op de tien burgers een digitale identiteit wel wil gebruiken. Onder inclusie doelgroepen blijkt zelfs meer dan de helft een digitale identiteit te willen gebruiken. Door het vergroten van toegevoegde waarde, gevoel van veiligheid en gevoel van controle neemt de gebruikersintentie van een digitale identiteit toe. Met deze drie aspecten moet dan ook rekening worden gehouden tijdens de ontwikkeling van een digitale identiteit.

2 Inleiding

2.1 Aanleiding en doelstelling

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft een visie op digitale identiteit[7] opgesteld met als thema: *Bouwen aan vertrouwen in de digitale wereld*. De digitale transitie gaat razendsnel en maatschappelijk vertrouwen in de digitale wereld is essentieel voor economische en sociale ontwikkelingen. In de visiebrief wordt het concept 'digitale bronidentiteit' geïntroduceerd, als een belangrijke bouwsteen voor een betrouwbaar digitaal identiteitsecosysteem. Dit onderzoeksrapport geeft invulling aan het concept 'digitale bronidentiteit'.

> ***Concept 'digitale bronidentiteit'***
> *'Wat willen we kunnen met een digitale bronidentiteit en hoe kan zo'n digitale bronidentiteit er dan uitzien?*
> *Hoe ziet het identiteitsecosysteem eruit en hoe verhoudt de digitale bronidentiteit zich tot bestaande voorzieningen?*
> *En wat is de juridische context van een bronidentiteit en de ethische wenselijkheid van een dergelijke voorziening?'*

Dit conceptueel beeld biedt de basis voor de volgende stappen in de verdere ontwikkeling van een digitale bronidentiteit.

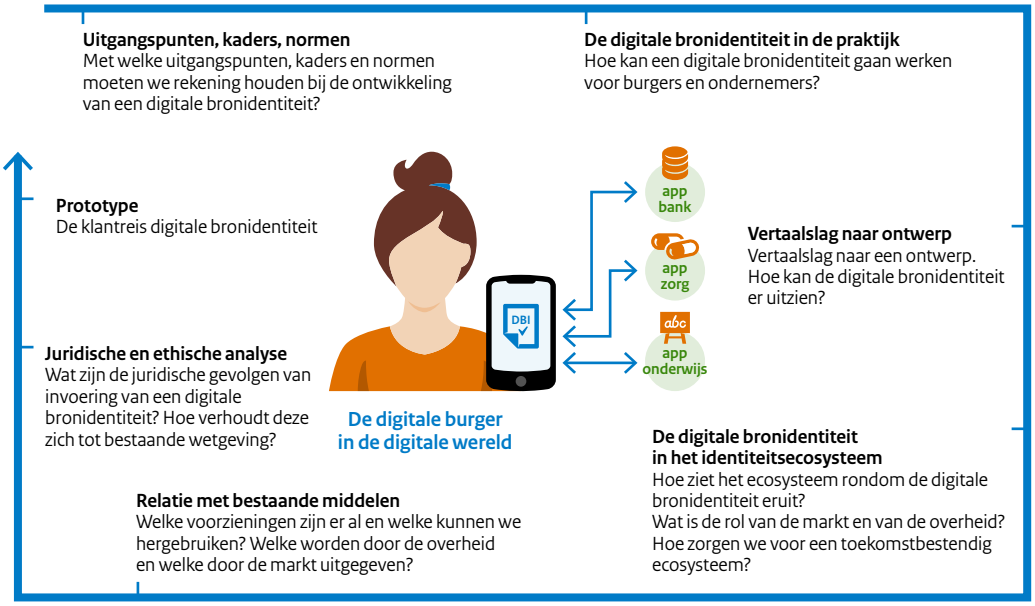
2.2 Aanpak

Het concept 'digitale bronidentiteit' wordt aan de hand van een vijftal onderzoeksvragen verdiept:
1. Definiëren van de digitale bronidentiteit;
2. Beschrijving van het identiteitsecosysteem;
3. Juridische en ethische analyse van de digitale bronidentiteit;
4. Analyse van de digitale bronidentiteit in verhouding tot bestaande voorzieningen;
5. Ontwerpen prototype: klantreis digitale bronidentiteit.

De belangrijkste uitgangspunten bij de uitwerking van deze onderzoeksvragen zijn:
- Relevante uitgangspunten, kaders en normen;
- De digitale bronidentiteit in de praktijk: welke functionaliteiten zijn noodzakelijk;
- Het centraal stellen van de burger.

[7] Visiebrief.

Figuur 1 *Aanpak*



2.3 Scope

- De scope omvat de beantwoording van de vijf onderzoeksvragen (zie de Bijlage: Onderzoeksvragen).
- Het rapport beperkt zich tot de digitale bronidentiteit van natuurlijke personen.
- De identiteit van rechtspersonen, objecten en apparaten wordt buiten beschouwing gelaten.

2.4 Kaders

Aan de uitwerking van de digitale bronidentiteit liggen de onderstaande kaders ten grondslag:
- Visiebrief Digitale Identiteit BZK;
- eIDAS Conceptverordening; en
- Relevante Wetgeving (zie ook hoofdstuk 6, Juridische en ethische analyse van de bronidentiteit).

2.5 Leeswijzer

Dit onderzoeksrapport schetst een conceptueel beeld van de digitale bronidentiteit en is als volgt opgebouwd: hoofdstuk 3 start met de aanleiding voor en de doelstelling van het rapport. Hier komen ook de aanpak, de scope en de kaders aan de orde.

Hoofdstuk 4 licht daarna toe waarom een digitale bronidentiteit (DBI) nodig is en wat de gewenste toepassingsmogelijkheden zijn. Vervolgens beschrijft hoofdstuk 4 hoe een DBI eruit zou kunnen zien en werken.

Hoofdstuk 4 bevat ook een uiteenzetting van de onderdelen, het uitgifteproces en het ontstaan van de DBI.

Hoofdstuk 5 beschrijft de DBI in het identiteitsecosysteem. Hier is het belang beschreven van een dergelijk ecosysteem en welke diensten, processen, actoren en middelen een rol spelen.

In hoofdstuk 6 volgt een juridische en ethische analyse van de DBI. Wat is de juridische basis en status van de DBI in wet- en regelgeving? In hoeverre moet wet- en regelgeving worden gemaakt of aangepast bij ontwikkeling van een DBI?

Hoofdstuk 7 beschrijft de voorzieningen die raakvlakken hebben met de DBI. Ook wordt onderzocht van welke voorzieningen de DBI mogelijk gebruik kan maken en wat de mogelijke gevolgen zijn van realisatie van de DBI voor de bestaande voorzieningen.

Per onderwerp zijn de te beantwoorden beleidsvragen genoemd alvorens de ontwikkeling van een DBI kan worden uitgewerkt. Een aantal onderwerpen worden verder toegelicht in de bijlagen waarnaar in het document verwezen wordt.

3 De digitale bronidentiteit

3.1 Waarom een digitale (bron)identiteit

Zowel binnen Nederland (*Visie op digitale identiteit*) als op Europees niveau (*eIDAS*) staat het onderwerp 'digitale identiteit' hoog op de agenda. De digitale transformatie gaat razendsnel, steeds meer processen en transacties vinden digitaal plaats. Denk aan online winkelen, een belastingaangifte indienen of bankzaken regelen. Andere voorbeelden zijn digitaal onderwijs volgen, examen doen en een diploma ontvangen.

In al deze transacties is een vorm van digitale identiteit nodig. Een burger moet zich in de digitale wereld kenbaar kunnen maken en kunnen authentiseren. *Ben jij wie jij zegt dat jij bent? Horen de attributen die jij met mij deelt bij jou? Zijn de attributen die jij met mij deelt betrouwbaar?* Daarbij is een hoge mate van betrouwbaarheid wenselijk of zelfs vereist.

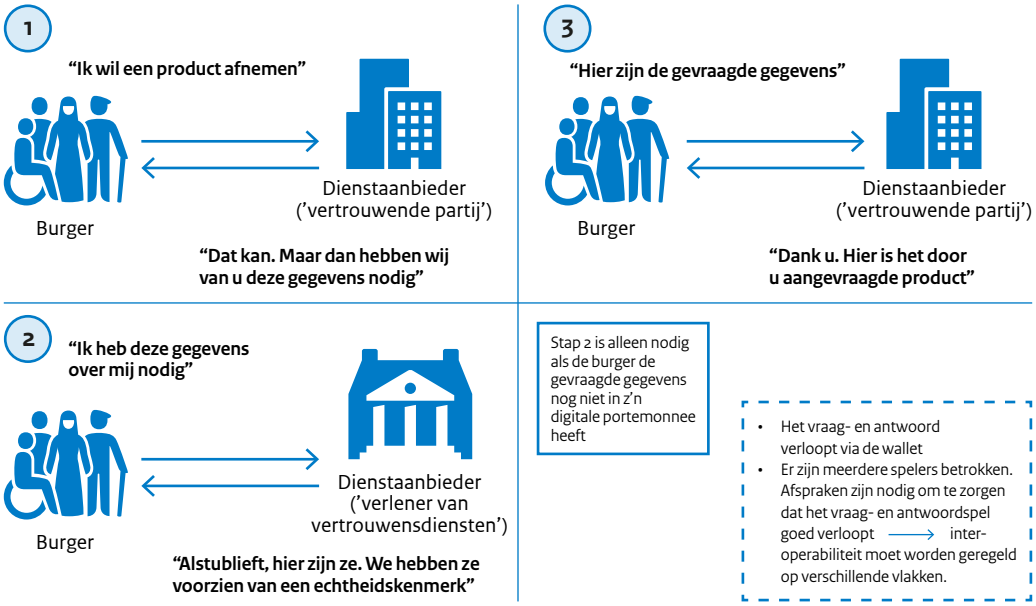
Onderstaande figuur geeft in het kort en op een vereenvoudigde wijze het nut aan van een betrouwbare digitale (bron-)identiteit. Uitgangspunten zijn:

- De burger gebruikt een digitale wallet om diensten/producten af te nemen en persoonsgegevens te delen met een dienstaanbieder.
- De burger vraagt (eenmalig) zijn persoonsgegevens op bij de overheid. Deze gegevens bewaart hij in de digitale wallet die hij op zijn smartphone heeft geïnstalleerd.
- Met persoonsgegevens wordt hier de digitale bronidentiteit bedoeld.

Stappen:

1. Een burger wil een digitaal product afnemen. Op de website van een dienstaanbieder vindt hij het gewenste product. Alvorens de dienstaanbieder de dienst kan leveren, heeft hij persoonsgegevens van de burger nodig.
2. De burger vraagt zijn persoonsgegevens op bij de overheid. Nadat de overheid enkele controles heeft uitgevoerd, ontvangt de burger zijn persoonsgegevens in zijn wallet.
3. Nu kan de burger de door de dienstaanbieder benodigde persoonsgegevens opsturen. Nadat de dienstaanbieder de authenticiteit van de gegevens heeft gecontroleerd bij de overheid (niet weergegeven in figuur 2), verstuurt de dienstaanbieder het product naar de wallet van de burger.

Figuur 2 *Toegevoegde waarde van een digitale (bron-)identiteit*



Doordat de burger over zijn persoonsgegevens beschikt in een wallet op zijn smartphone, kan hij op elk moment en op elke plek een dienst of product aanvragen en/of afnemen.

De volgende paragrafen lichten de noodzaak van een betrouwbare digitale (bron)identiteit verder toe. Daarbij zijn de Visiebrief en de conceptverordening eIDAS als uitgangspunt gebruikt.

3.1.1 Visie op digitale identiteit

De Visiebrief heeft als titel '*Bouwen aan vertrouwen in de digitale wereld*'. De brief benadrukt het belang van een hoge mate van vertrouwen in de digitale wereld. Een gebrek aan vertrouwen kan ertoe leiden dat burgers, bedrijven en overheden aarzelen om transacties digitaal uit te voeren en van nieuwe diensten gebruik te maken. De Visiebrief benoemt onder meer de volgende kansen rondom het digitale identiteitsecosysteem:

- Digitale veiligheid en betrouwbaarheid/maatschappelijk vertrouwen in het digitaal verkeer vergroten.
- Een betrouwbaar en efficiënt digitaal identiteitsecosysteem (zie hoofdstuk 5) helpt burgers en bedrijven digitaal zaken te doen en vermindert administratieve lasten en onnodige maatschappelijke kosten.
- De zelfstandigheid en autonomie van burgers bevorderen (regie op gegevens).

Zie ook de Bijlage: Maatschappelijke kansen en uitdagingen.

Vervolgens introduceert de Visiebrief het concept 'digitale bronidentiteit' (DBI). De DBI is één van de pijlers van de visie op digitale identiteit:

- Delen van betrouwbare gegevens: de visie is gebaseerd op een overheid als 'gezaghebbende bron'. Door ook in de digitale dienstverlening door de overheid geverifieerde gegevens te delen, wordt vertrouwen gecreëerd in het publieke en private domein. Dit sluit aan bij de beleidsdoelstellingen op het gebied van regie op gegevens en de Europese ambities van de Single Digital Gateway.
- Toegang: het organiseren van toegang tot cruciale dienstverlening in de Nederlandse maatschappij voor alle burgers en bedrijven op een passend (eIDAS) betrouwbaarheidsniveau, zowel in het publieke als private domein.
- Digitale bronidentiteit: een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector.
- Afsprakenset digitaal vertrouwen: De uitgangspunten en afspraken rond het delen van gegevens, toegang en het leveren van vertrouwen in de digitale wereld, inclusief de digitale bron identiteit (DBI), worden vastgelegd in een afsprakenset.

3.1.2 *Conceptverordening eIDAS*

In 2018 is de eIDAS-verordening in werking getreden. Deze verordening verplicht lidstaten onder meer dat de nationale elektronische identificatiemiddelen (eID) wederzijds worden erkend en geaccepteerd nadat zij zijn aangemeld en getoetst. Hierdoor kunnen burgers en bedrijven inloggen bij publieke en private organisaties in alle lidstaten om diensten af te nemen of zaken te regelen. In Nederland zijn DigiD (burgers) en eHerkenning (ondernemers) aangemeld.

Daarnaast stelt de eIDAS-verordening minimumeisen en criteria vast waaraan de eID's moeten voldoen om een bepaald betrouwbaarheidsniveau te bereiken: laag, substantieel of hoog.

Op 3 juni 2021 heeft de Europese Commissie een conceptwijziging van de eIDAS-verordening ingediend. De huidige eIDAS-verordening bleek volgens de Commissie niet te kunnen voldoen aan een nieuwe marktbehoefte: vertrouwen op basis van attributen die zijn verbonden aan een digitale identiteit.

Bovendien zijn de huidige eID's beperkt tot de overheidssector en kan met de huidige eIDAS-verordening het delen van identiteitsgegevens niet worden beperkt tot wat strikt noodzakelijk is voor een dienst.

De Europese Commissie stelt daarom met de conceptwijziging de verplichte uitgifte voor van een Europese portemonnee voor digitale identiteit (*European Digital Identity Wallet*). Met deze wallet kan de gebruiker bijvoorbeeld:
- Identiteitsgegevens, inloggegevens én attributen over zijn/haar identiteit opslaan;
- Dit op verzoek aan vertrouwende partijen verstrekken; en
- Zich online en offline authentiseren.

De Commissie stelt het gebruik van de Europese portemonnee voor digitale identiteit overigens niet verplicht. Het is aan een burger om te bepalen hoe hij een dienst of product wil afnemen.

Het voorstel van de Commissie wordt momenteel nog verder uitgewerkt. Daarna moet het voorstel nog worden aangenomen door het Europees Parlement en de Raad. Desondanks is bij de hierop volgende uitwerking van de DBI rekening gehouden met de doelstellingen en principes van het huidige voorstel tot aanpassing van de eIDAS-verordening.

3.2 Definitie digitale bronidentiteit

De Visiebrief hanteert de volgende definities van de digitale (bron)identiteit:

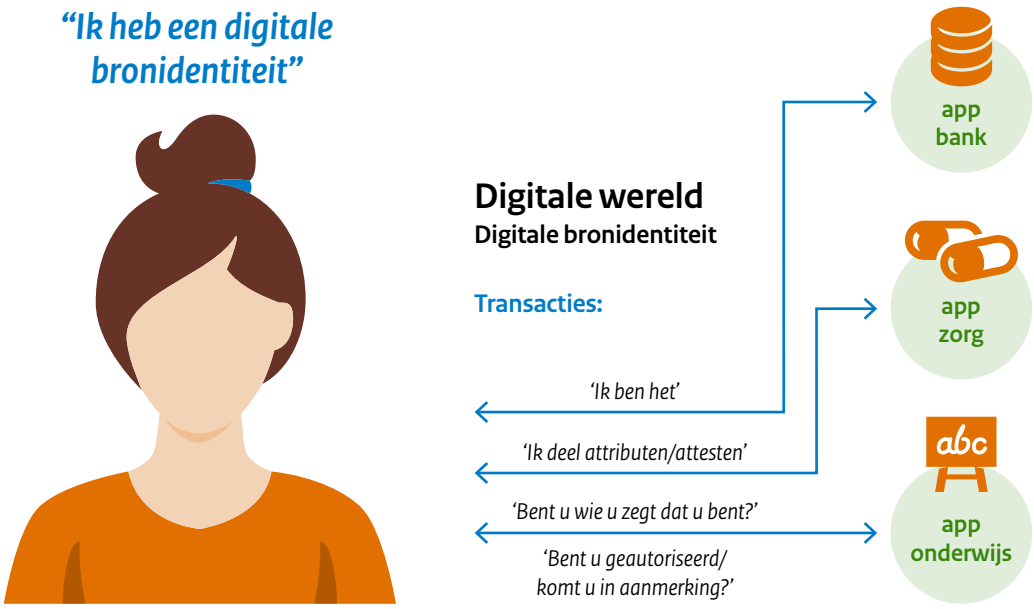
- Digitale identiteit: een verzameling gegevens die een entiteit (persoon of organisatie) in het digitale domein representeren.
- Digitale bronidentiteit: een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector.
  - De digitale bronidentiteit bevat een minimale set van identiteitsgegevens die nodig zijn in het maatschappelijk verkeer.
  - De overheid creëert met de digitale bronidentiteit een 'gezaghebbende bron' van betrouwbare persoonsidentificerende gegevens.
  - De DBI als 'gezaghebbende bron' maakt afgeleide digitale identiteitsmiddelen mogelijk.
  - De overheid biedt met de DBI een basisblok waarmee, binnen de kaders van het digitaal identiteitsecosysteem, publieke en private partijen betrouwbare diensten kunnen aanbieden.

Bij de beantwoording van de onderzoeksvragen is bovenstaande definitie als uitgangspunt genomen.

3.3 Wat kun je met de digitale bronidentiteit

Uitgaande van de doelstellingen van de DBI zoals beschreven in paragraaf 3.1, is de DBI in combinatie met het bijbehorende identiteitsecosysteem een middel waarmee gebruikers zich bij digitale transacties betrouwbaar kunnen identificeren, attributen kunnen delen, zich kunnen authentiseren en laten autoriseren.

Figuur 3 *Basisfuncties digitale identiteit in transacties*



Een voorbeeld van gebruik is om aan te geven dat je 18 jaar of ouder bent. Hiervoor is het niet nodig om andere identiteitsgegevens te delen. Op basis van de DBI kan een 18+-attest worden gegenereerd.[8] Dit attest kan bijvoorbeeld in de vorm van een QR-code met foto via de telefoon van de burger aan de verifiërende partij visueel aangeboden worden.

[8] In een 18+-attest staat alleen dat de betreffende gebruiker 18 jaar of ouder is. De daadwerkelijke leeftijd staat niet in het attest.

Met deze QR-code en foto is het mogelijk dat de verifiërende partij de persoon authentiseert door een visuele vergelijking van de foto boven de QR-code met de persoon voor hem. Daarnaast kan hij na het scannen van de QR-code ook zien dat de persoon ouder is dan 18 jaar. Met het scannen van de QR-code wordt alleen het 18+ attest gedeeld en geen andere identiteitsgegevens.

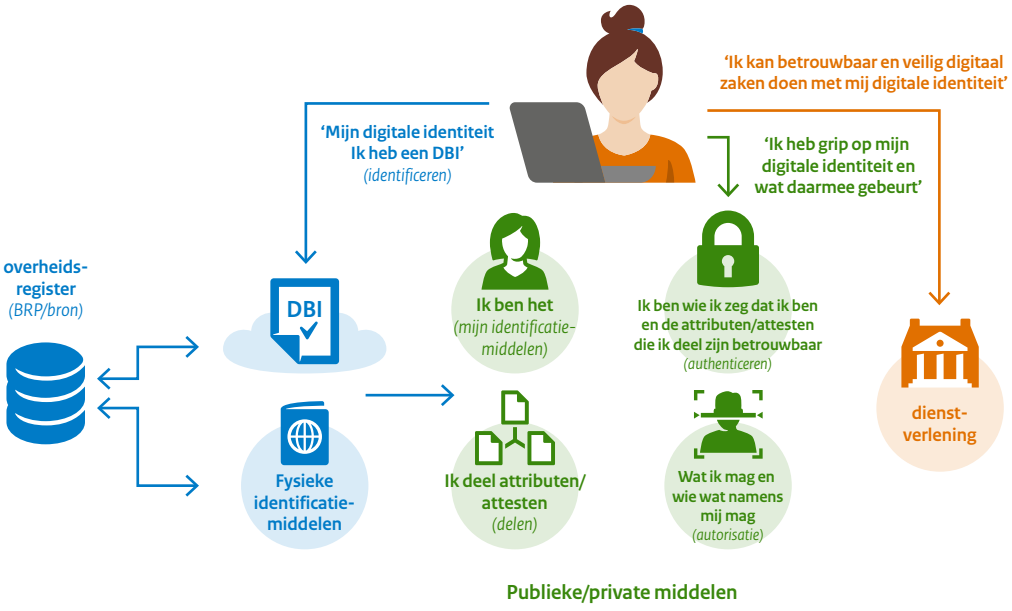
Bovenstaande uitwerking is slechts een voorbeeld., In plaats van een QR-code zou ook een andere manier gekozen kunnen worden. Kern is dat met gebruik van een DBI identiteitsgegevens kunnen worden gebruikt voor een bepaalde dienst. Onderstaand is het voorbeeld visueel weergegeven.

Figuur 4 *Delen van (persoons-)gegevens met een DBI*

Zoals het voorbeeld laat zien, maakt de DBI functies rondom transacties mogelijk en kunnen daardoor diensten afgenomen worden. Het geheel om dit te laten werken wordt het identiteitsecosysteem genoemd. Hoofdstuk 5 gaat verder op dit ecosysteem in.

Onderstaande figuur geeft een samenvatting van de DBI weer.

Figuur 5 *Basisfuncties DBI en het identiteitsecosysteem*



4 Hoofdstuk 4 Ontwikkeling van de DBI

4.1 Inleiding

In dit hoofdstuk wordt beschreven hoe de DBI kan worden gezien en hoe bepaalde inzichten leiden tot de opbouw van de DBI als een bouwblok in het ecosysteem.

Een belangrijk vraagstuk daarin is hoe naar de DBI kan of moet worden gekeken, als authenticatie-mechanisme of als mechanisme voor de verstrekking van gegevens. Daarin is de DBI niet opzichzelfstaand maar werkt in combinatie met een wallet, als middel tot het verkrijgen en vasthouden van attesten. De attesten kunnen dienen als middel voor het faciliteren van verstrekkingen.

Vanuit de visiebrief gelden de onderstaande items

Identificatie – hoog betrouwbaarheidsniveau
Daarnaast is het van belang om rekening te houden met het betrouwbaar kunnen vaststellen (identificatie) en authentiseren van de identiteit van een persoon. Een hoge mate van betrouwbaarheid van de digitale bronidentiteit moet onderdeel zijn van het ontwerp van een DBI. De identiteit van een persoon wordt bepaald door diens gecombineerde biometrische en biografische kenmerken, die uniek van toepassing zijn op die persoon. Identificatie en authenticatie zijn ingewikkelde processen, omdat 'identiteit' complex is en verandert in de tijd. Om een digitale identiteit betrouwbaar vast te kunnen stellen (uitgeven van een DBI) en in het vervolgproces te authentiseren (gebruik maken van een DBI) zijn drie onderstaande principes/uitgangspunten van toepassing: De beweerde identiteit is echt. Er is vertrouwen dat de persoon echt bestaat en nog steeds leeft, en niet ten onrechte gecreëerd is om iets te verkrijgen waar men geen recht op heeft; De persoon is met een hoge mate van betrouwbaarheid gekoppeld aan de identiteit. Het proces van aanvraag wordt zodanig ingericht dat is gewaarborgd dat de persoon die de aanvraag indient en de claim legt op de identiteit het recht heeft om de identiteit op te eisen, de persoon is geen bedreiger en is uniek binnen de context van de autoriteiten. Uniek binnen de context van de autoriteiten betekent hier dat de opgegeven identiteit precies één keer voorkomt. Er is vertrouwen dat de persoon die de geclaimde identiteit gebruikt, opereert onder deze identiteit binnen de gemeenschap, én dit consequent doet.
Het is belangrijk om een hoog betrouwbaarheidsniveau bij het eerste contactmoment met een individu te realiseren, d.w.z. bij de identificatie/registratie van diens digitale identiteit. Als de eerste identiteitsvaststelling 'sterk' is (uitgeven van een DBI), kan de kracht van deze eerste processtap goed gebruikt/ingezet worden bij daaropvolgende interacties. Hierbij is uitgegaan van een hoog betrouwbaarheidsniveau voor de DBI. Daarbij is niet gekeken naar specifieke gebruikstoepassingen waarvoor mogelijk een lager betrouwbaarheidsniveau volstaat.

4.2 Welk proces wordt ondersteund door de DBI en het gebruiksdoel?

Zoals in hoofdstuk 3 is aangegeven, is de digitale bronidentiteit een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector. Onder een digitale identiteit wordt een verzameling gegevens verstaan, die een entiteit (persoon of organisatie) in het digitale domein representeert. Met de DBI wordt een unieke identiteitsregistratie gecreëerd. Op basis van de DBI en afgeleide identificatiemiddelen kan van personen authenticatie van de identiteit plaatsvinden. Essentieel is dat de DBI voldoende gegevens bevat voor het beoogde gebruik, zowel in online als in offline situaties.

Belangrijk is dat de DBI in het licht wordt gezet van het gebruiksdoel. Deze gebruiksdoelen kunnen zijn:
- Verstrekking; of
- Authenticatie.

Vertrekkend vanuit het inhoudelijke betekent het dat de elementen en de gegevens die in de DBI worden opgenomen een betekenis krijgen in de vorm van inhoudelijke gegevens. Vanuit dat oogpunt kan men ervoor kiezen dat de DBI gezien wordt als een gegevensdrager van waaruit verstrekking plaatsvindt. Bij het kiezen van gebruiksdoel kiest men ook voor een uitgebreide inhoudelijke gegevensset die ook op de lange termijn bruikbaar moet blijven en synchroon met de basisregistratie.

Wordt gekeken vanuit het gebruiksdoel van authenticatie dan krijgen de elementen in de DBI een volledig andere betekenis. Bij authenticatie vindt toetsing plaats en wordt een validatie uitgevoerd. Zijn de gegevens die worden aangeboden gelijk aan de gegevens die zijn opgenomen in de DBI, is een biometrie die wordt aangeboden onderdeel van de DBI.

De bovenstaande zaken ten aanzien van het gebruiksdoel bepalen in de hoge mate de “plaatsing” van de DBI in het ecosysteem/ maatschappelijk verkeer en hoe deze in het proces zijn toepassing krijgt.

Kijken we naar de voorgaande hoofdstukken en de hierin genoemde de aspecten dan zien we vrij vertaald een 3-tal onderdelen terugkomen een verwijzing naar de basisregistratie. Het lijkt onvermijdelijk om net zoals bij het paspoort een verwijzing op te nemen naar de persoonsregistratie. Een reden hiervoor kan zijn het zekerstellen dat het een door de overheid uitgegeven item is. Zonder referentie in de basisregistratie wellicht geen DBI

De authenticatie wordt fysiek uitgevoerd door de persoon aan wie de DBI is uitgereikt.

Meervoudig vaststellen van de authenticatie indien nodig, Multi-factor. Het Multi-factor kan in deze een gelaagde opbouw zijn van inhoudelijke gegevens, biometrie als apparaten in de realisatie.

4.3 De specifieke opbouw van de DBI

Op basis van het bovenstaande en als we de DBI zien als bouwblok in het authenticatiemechanisme dan zou de DBI uit de onderstaande componenten kunnen bestaan:

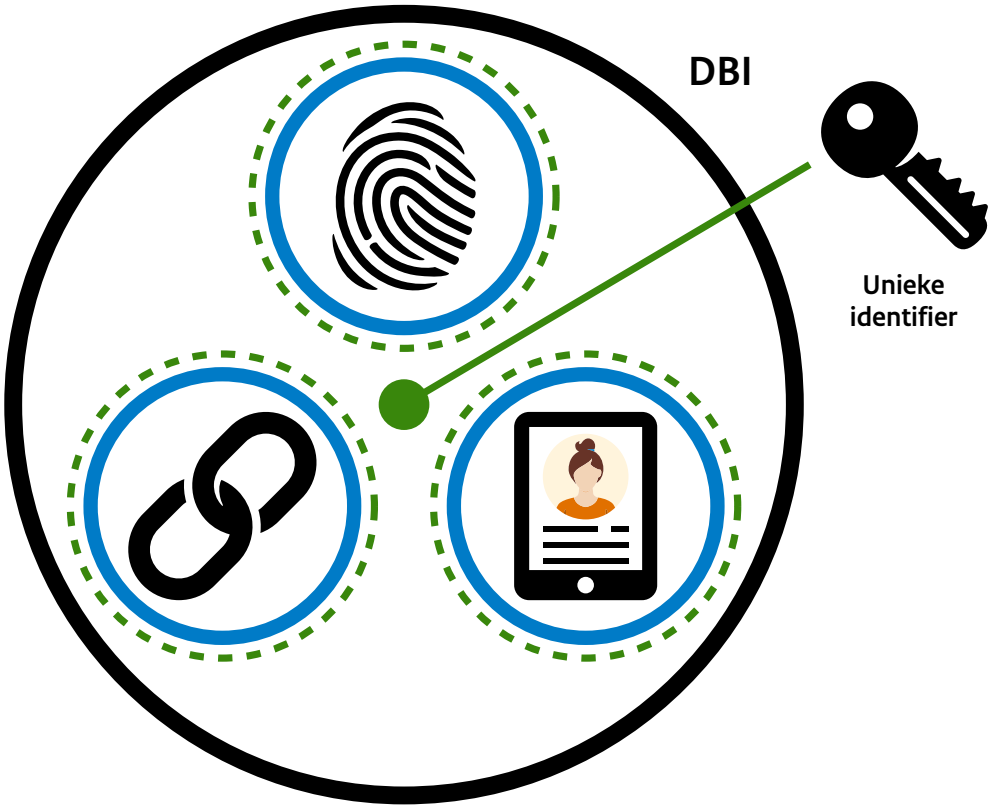
- Het opnemen van de referentie uit de basisregistratie, b.v. BSN;
- Het opnemen van fysieke kenmerken, biometrie; en
- Het opnemen van de inhoudelijke gegevens, conform eIDAS.

Figuur 6 *De DBI: combinatie van meerdere factoren*

We zien dat de DBI hier een drieluik vormt van de genoemde elementen. Het bijzondere daarbij is dat de elementen alle drie opzichzelfstaand zijn en kunnen bestaan. Zo hebben ze alle drie hun individuele waarde. De kracht zit in het samenstel van de drie componenten. In alle gevallen zullen ze als één DBI kunnen fungeren op het moment dat alle drie aanwezig zijn inclusief de onderlinge relatie tot elkaar. Anders gezegd, drie specifieke instanties van de componenten en met elkaar verbonden vormen één DBI:

- Een specifieke referentie naar de basisregistratie in combinatie met specifieke biometrie vormt geen DBI.
- Een specifieke gegevensset in combinatie met biometrie vormt geen DBI.
- Een specifieke referentie naar de basisregistratie in combinatie met een specifieke gegevensset vormt geen DBI.
- Een specifieke referentie naar de basisregistratie in combinatie met specifieke biometrie en in combinatie met een specifieke gegevensset vormt een geldige DBI.

Figuur 7 *De unieke identifier van een DBI*



Dat is wat de DBI bijzonder maakt qua opbouw, de combinatie van de drie factoren in relatie tot elkaar. Mist één van de drie factoren dan verliest de DBI ook zijn geldigheid. Hoe dit zich uiteindelijk vertaalt naar de praktijk met effectief en eenvoudig gebruik, inclusie, is een punt voor onderzoek en sterk afhankelijk van het gebruiksdoel dat vanuit beleid wordt gegeven aan de DBI en de "plaats" in het ecosysteem.

4.4 Verbinding met bestaande administratieve systemen.

Het toevoegen van een verbinding met bestaande administratieve systemen heeft als voordeel dat vanuit een digitale bronidentiteit de link met reeds bestaande administratieve gegevens van een persoon gemaakt kan worden. Tevens biedt het mogelijkheden om wijzigingen die in die administraties plaatsvinden, mogelijk ook door te laten werken in de DBI. In het gebruik van de DBI kan deze verbinding mogelijk gebruikt worden om gegevens uit de basisregistraties te ontsluiten richting de houder van een DBI. Dit zorgt tevens voor minder noodzaak de minimale gegevensset van de DBI (zie paragraaf 4.5) te verruimen.

Door de overheid uitgegeven middelen hebben het kenmerk 'veilig' en 'betrouwbaar' te zijn, waarbij deze kenmerken nogal wat betekenen. Het houdt voornamelijk in dat iedereen een door de Nederlandse overheid uitgegeven middel zoals de DBI vertrouwt en op basis van dit vertrouwen transacties aangaat. Bij bestaande identificatiemiddelen, zoals het paspoort, is ook een link met bestaande administratieve systemen opgenomen: het BSN. En evenzo is het documentnummer opgenomen in de basisregistratie. Een vergelijkbare systematiek wordt voorgesteld voor de DBI: gebruik van het BSN als verbinding met bestaande administratieve systemen en opname van de uitgegeven DBI's in een centrale registratie.

Nemen we het gebruiksdoel in ogenschouw en zetten we dat neer als het authenticatiemechanisme dan kan bij het gebruik van de DBI middels de component "referentie naar de basisregistratie" worden getoetst of de referentie een geldige is, is het een door de Nederlands overheid uitgegeven DBI.

4.5 Minimale gegevensset

Dit is de minimale set aan persoonsgegevens die nodig is om tot betrouwbare identificatie en authenticatie van de natuurlijke persoon te komen. Uitgaande van de Visiebrief bestaat deze set uit[9]:

- Familienaam;
- Voornamen;
- Geboortedatum; en
- Unieke Identificatiecode.

Deze gegevensset is een extractie uit de persoonsgegevens die bekend zijn bij de overheid. Denk hierbij bijvoorbeeld aan het paspoort en de Nederlandse Identiteitskaart dan wel de basisregistratie personen. Deze registratie /middelen bevatten ieder meer gegevens dan de genoemde minimale set[10].
De genoemde minimale gegevensset sluit overigens aan bij de Conceptverordening van eIDAS.

Een afweging kan gemaakt worden welke (extra) gegevens benodigd zouden zijn om tot het doel (identificatie van de natuurlijke persoon) te komen. Bij de afweging dient rekening gehouden te worden met principes als dataminimalisatie en beperking van duplicatie van data. Strikt genomen lijken extra gegevens niet noodzakelijk. Het derde element als unieke code, de verbinding met administratieve systemen (BRP), wordt opgenomen als onderdeel van de digitale bronidentiteit. Deze biedt de mogelijkheid tot het verifiëren of de DBI behoort bij een in de basisregistratie opgenomen persoon. Hierbij resteert de vraag of aanvullende gegevens onderdeel behoren te zijn van de DBI of dat het mogelijk is deze aanvullende gegevens op een andere wijze worden ontsloten, bijvoorbeeld via een uitbreiding in de wallet.

Ten aanzien van de unieke identificatiecode kan een nieuw uniek nummer geïntroduceerd worden, of er kan gebruik worden gemaakt van het BSN. Hergebruik heeft als voordeel dat er al een bestaande infrastructuur is. Wel dient ervoor gezorgd te worden dat het BSN niet ontsloten wordt als dat niet strikt noodzakelijk is. Denk aan het paspoort, daar staat het BSN op de achterkant zodat het bij kopieën niet zichtbaar is.

4.6 Biometrische gegevens

Het creëren van een register van unieke, geverifieerde identiteiten vormt de basis voor een betrouwbare identiteitsketen voor overheids- en particuliere gebruikers. Biometrie kan een belangrijk onderdeel zijn om de betrouwbaarheid te garanderen.

Voor een hoge betrouwbaarheid van de DBI, kunnen biometrische gegevens toegevoegd worden.

Biometrische gegevens kunnen ingezet worden bij zowel identificatie als authenticatie en het toewijzen van de DBI aan precies één fysiek persoon:

- **Identificatie:** het vaststellen van de identiteit van een persoon door het verzamelen en valideren van relevante identiteitsinformatie. Het creëren van een (unieke) identiteitsregistratie en vervolgens afgeven van referentie- en authenticatiefactoren om mensen in staat te stellen deze identiteiten te ‘doen gelden’;
- **Authentiseren van een identiteit:** controleren of een persoon die een identiteit beweert te hebben (claimt), de ware eigenaar van die identiteit is op basis van één of meer factoren die hij of zij heeft of is. Het gaat om een bevestiging of afwijzing dat een persoon dezelfde persoon is aan wie oorspronkelijk een identiteitsmiddel is verstrekt.[11]

[9] Voor Europese interoperabiliteit, dient de set eventueel uitgebreid te worden, zie https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eidas_saml_attribute_profile_v1.0_2.pdf?version=1&modificationDate=1497252920317&api=v2.
[10] Artikel 3 Paspoortwet
[11] ID4D Practitioner’s Guide: Version 1.0 (October 2019). Washington, DC: World Bank Group. World Bank Document, p.11.

Voor identificatie is een centrale database nodig. De betrouwbaarheid van een robuust en unieke DBI en het vermogen om een hoog niveau van zekerheid te bieden, wordt bereikt met name door biometrisch ontdubbelen en ervoor te zorgen dat elke persoon zich maar één keer kan registreren/ een DBI kan verkrijgen. Dus, zelfs als ze een valse naam hebben gegeven, kan men zich maar één keer registreren en na verloop van tijd worden geverifieerd als dezelfde persoon. Biometrie is momenteel de meest nauwkeurige en efficiënte technologie die beschikbaar is om grote populaties te ontdubbelen om statistische uniciteit te garanderen. Voor ontdubbelen is een gecentraliseerde opslag van biometrische gegevens nodig.

Zodra de personen zijn geregistreerd, kan biometrische herkenning in het vervolgproces worden gebruikt om een geclaimde identiteit te verifiëren. Biometrische verificatie wordt gewoonlijk geïntegreerd in een authenticatieproces en kan op gedecentraliseerde of gecentraliseerde wijze worden uitgevoerd. Het is een keuze of biometrie ingezet wordt voor dit ontdubbelen, of dat op andere manier de uniciteit geborgd wordt, zoals er ook al waarborgen zitten in het huidige systeem van uitgifte van paspoorten, ID-kaarten et cetera.

Voor authenticatie kan een keuze worden gemaakt tussen centrale en decentrale opslag. Denk voor decentrale opslag bijvoorbeeld aan de pasfoto op de eNIK. Bij gebruik van biometrie zou in een vervolgstap een verdieping op de te verkiezen wijze uitgevoerd moeten worden.

Er zijn verschillende modaliteiten van biometrie die gebruikt zouden kunnen worden. De meest kansrijke modaliteiten om toe te passen zijn de vingerafdruk, het gezicht en de iris. Die modaliteiten worden al toegepast in een aantal soorten civiele-, reis-, wetshandhavings- en beveiligingstoepassingen, juist vanwege hun eigenschappen. Denk aan het vastleggen van een pasfoto binnen de eNIK. Hierbij geldt dat het gebruiken van een combinatie van modaliteiten voordelen heeft (nog betrouwbaarder, beter toepasbaar in situaties en voor personen waar een specifiek modaliteit minder of niet werkt).

Tot slot kan hergebruik gemaakt worden van reeds vastgelegde biometrische gegevens, zoals in de eNIK. De betrouwbaarheid van dit hergebruik hangt samen met de betrouwbaarheid van het reeds uitgegeven middel en zal lager zijn dan de maximale betrouwbaarheid die te behalen is bij het nieuw vastleggen van de biometrie.

4.7 De rol van de basisregistratie en de noodzaak van de verwijzing.

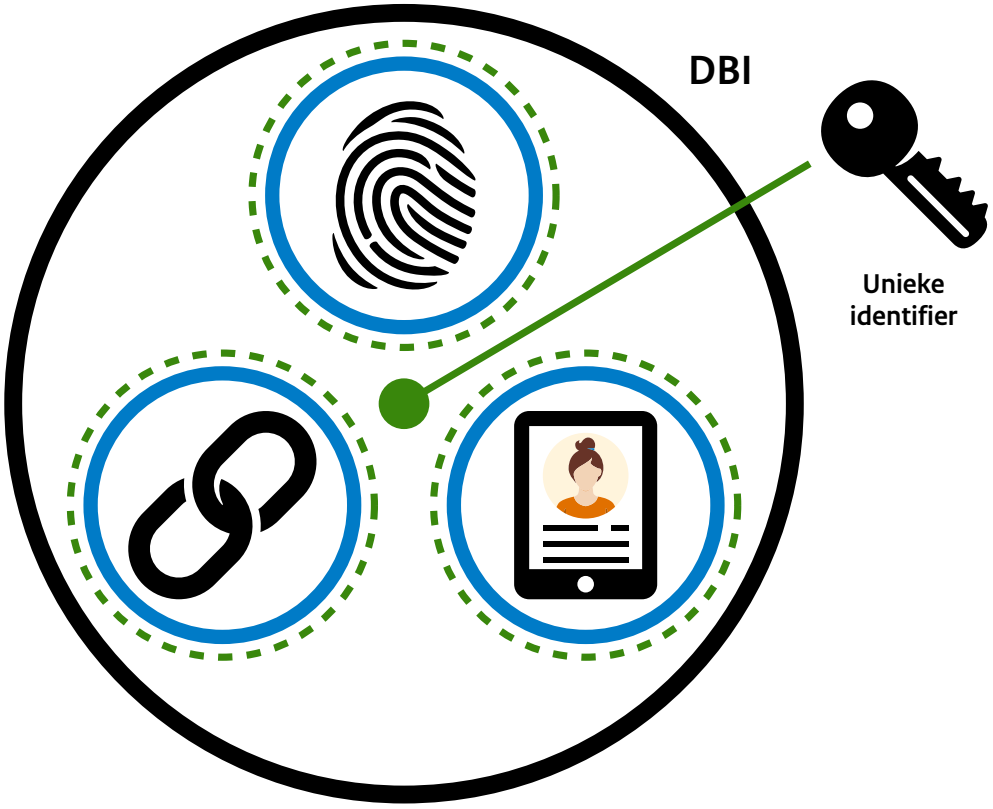
Voor deze verwijzing kan gebruik worden gemaakt van het BSN, het zij versleuteld of voorzien van een betekenis “token”. Zie ook paragraaf 4.2.3. Belangrijk hierbij is dat een DBI gekoppeld is aan precies één persoon in de basisregistratie. Bij het niet voorkomen van de referentie in de basisregistratie dan betreft het een ongeldige DBI, anders gezegd een niet door de Nederlandse overheid uitgegeven DBI.

- De rol van de koppeling naar fysiek.
  - Het koppelen van de DBI aan de fysieke persoon zorgt dat vastgesteld wordt dat de betreffende “credentials” niet alleen correct zijn maar dat het ook echt de fysieke persoon is die op dat moment de “credentials” ingeeft.
- De rol van de gegevensset.
  - De gegevenset wordt bij voorkeur gebruikt voor het toetsen van de inhoudelijke gegevens als authenticatiefactor. Dat betekent dat de DBI zelf een minimale gegevensset bevat en de houder van de DBI geen gegevens verstrekt uit zijn DBI. Wel kan de houder van de DBI een attest opvragen bij de basisregistratie wat gebruikt kan worden voor het verstrekken van gegevens. Het voordeel van die constructie is dat het attest is ondertekend en daarmee voldoet aan de eis dat het verifiable credentials betreft. Ook hiervoor geldt dat bepaald moet worden welke rol en gebruiksdoel de DBI krijgt in het maatschappelijk verkeer dan wel het ecosysteem.

4.8 De DBI duurzaam aanwijsbaar maken en waarom?

Om de DBI te kunnen gebruiken, dient de verzameling, het drieluik van de componenten, eenduidig aangeroepen kan worden. Dit kan door een duurzame unieke, willekeurige en betekenisloze identifier toe te voegen. Op basis van deze unieke identifier kan de DBI gekoppeld worden aan digitale toepassingen en gebruikt worden binnen een digitaal identiteitsecosysteem. Grafisch ziet dat er als volgt uit:

Figuur 8 *De DBI en de unieke identifier*



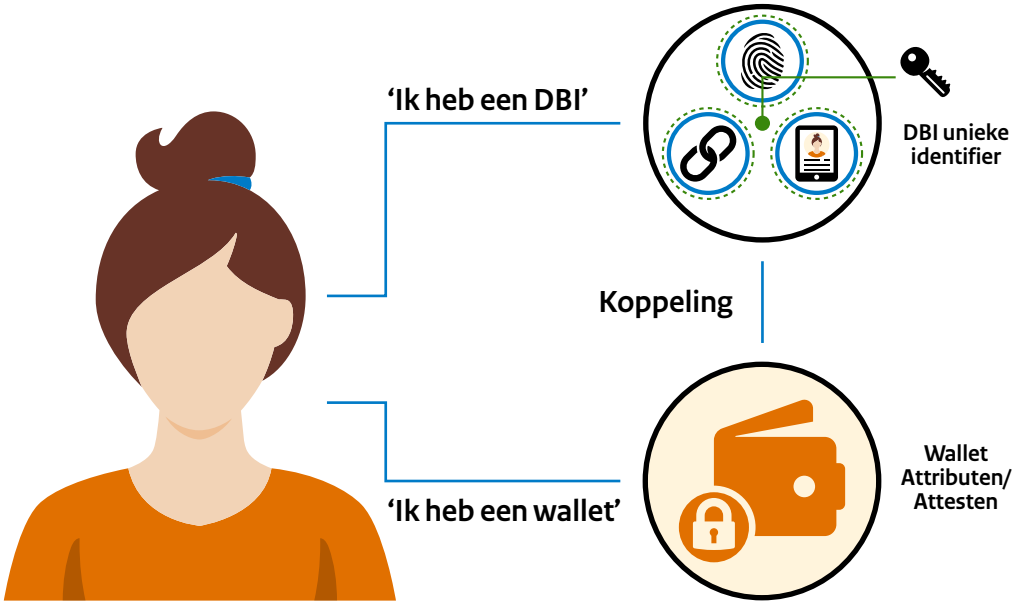
Voordeel van een unieke identifier is dat deze *persistent*[12] gemaakt kan worden, ook indien er bepaalde gegevens binnen een DBI veranderen. Denk bijvoorbeeld aan een persoon die een naams- of geslachtsverandering heeft ondergaan of waarbij nieuwe of andere biometrische gegevens gekoppeld zijn. Ook in die situaties dient de unieke referentie van de DBI nog onveranderd gebruikt te kunnen worden. De unieke en persistente identifier maakt dit mogelijk. De vorm van de unieke identifier kan een willekeurig gegenereerd token zijn. Gezien het feit dat bepaalde gegevens binnen een DBI kunnen veranderen, is het informatietechnisch vervolgens aanbevolen om van elk gegeven enkele metagegevens bij te houden en historie te ondersteunen. De belangrijkste hiervan zijn de datum vanaf welk moment een versie van het gegeven geldt en de datum tot wanneer die versie van het gegeven geldt. Zodoende kan historie in de DBI bijgehouden worden. De unieke identifier is daarmee losgemaakt van de inhoud van de DBI en ongevoeliger voor onregelmatigheden in gebruik.

[12] Persistent betekent letterlijk 'blijvend, volhardend': persistence refers to the characteristic of state of a system that outlives (persists more than) the process that created it. Met betrekking op digitale identiteit is het een unieke identifier die gegarandeerd blijft werken, ook al verandert iets in de gegevens die voor identificatie gebruikt zijn.

4.9 De combinatie van de DBI en de Wallet

De DBI betreft een digitale verzameling gegevens van een bepaald persoon. Die persoon kan pas iets met zijn/haar DBI als de DBI ontsloten wordt in een specifieke digitale omgeving. Die specifieke digitale omgeving wordt veelal de wallet genoemd (dat is ook de term die vanuit eIDAS wordt gebruikt). Dit kan een app zijn op een mobiele telefoon, maar bijvoorbeeld ook een cloud-omgeving die via een browser te benaderen is. Mogelijk zijn beide opties gewenst, bijvoorbeeld als back-up voorziening of voor het op afstand koppelen van een wallet op een telefoon. Voor gebruik dient de DBI van een persoon aan diens wallet te worden gekoppeld. De combinatie van de wallet en de DBI zou vanuit de huidige gedachtegang, in de realisatie, de basis vormen voor de identificatie en de authenticatie.

Figuur 9 *De DBI en de wallet*



Technisch gezien kan dit door de unieke identifier van de DBI te koppelen aan een identiteitskenmerk van de wallet (een 'wallet-ID'). Hiermee krijgt de betreffende persoon de beschikking over een wallet die verbonden is aan zijn/haar DBI. Daarnaast kan de gebruiker de mogelijkheid verkrijgen tot het gebruik van pseudoniemen voor omgevingen waar hij of zij liever niet de eigen identiteit gebruikt maar de zogenoemde verifiable credentials wel nodig zijn.

4.10 Attesten en hun toegevoegde waarde

Nadat de houder zijn of haar DBI heeft verkregen kan deze worden gebruikt. Eerder is duidelijk geworden dat de DBI een bouwblok in het ecosysteem is en de componenten is de DBI bepaald zijn en voor de gebruiker niet "onderhoudbaar". Om houder van de DBI in de gelegenheid te stellen op basis van de DBI betrouwbaar gegevens te delen dan wel te verstrekken wordt de DBI uitgebreid met een wallet.
Deze wallet is feitelijk de "container" waarin de aanvullende stukken, attesten, worden opgeslagen en vanuit worden gebruikt. Het gebruik van attesten geeft de houder van de DBI om heel selectief gegevens te delen met derden waarbij ook zekerheid kan worden gegeven over de herkomst van de zowel de persoon die verstrekt als de bron van de gegevens. Het betreft hier attesten die ondertekend, de verifiable credentials, zijn door de uitgevende instantie. De herkomst en de betrouwbaarheid van de gegevens in het ecosysteem neemt daarmee toe.

4.11 Ontstaan van de DBI

De DBI betreft gegevens die de overheid van een bepaalde persoon heeft en die gelinkt zijn aan die persoon. Randvoorwaardelijk voor het kunnen uitgeven van een DBI is dat de overheid de betreffende persoon kent: een inschrijving in de Basisregistratie Personen (hierna: BRP). Dat is de gezaghebbende bron in Nederland voor persoonsregistratie. Door de registratie in de BRP kan de beschikking verkregen worden over de gegevens voor de minimale dataset die onderdeel uitmaken van de DBI en kan de link naar gegevens van de basisregistraties gemaakt worden. Biometrische gegevens moeten of bij het ontstaan van de DBI afgenomen en toegevoegd worden, of hergebruikt worden vanuit al bestaande bronnen (zoals hergebruik van biometrische gegevens uit de chip op het paspoort of de eNIK).

Een mogelijkheid is om een DBI te laten ontstaan bij inschrijving in de BRP. In bepaalde gevallen kan dit lastig zijn, zoals bijvoorbeeld het vastleggen van biometrie bij pasgeborenen. Tevens, de DBI is pas waardevol voor een burger nadat de DBI aan een wallet is gekoppeld. De kans bestaat dat er vele DBI's gecreëerd worden, die daarna nooit gekoppeld worden.

Een andere mogelijkheid is om een DBI pas dan te creëren als een burger hierom verzoekt.

Een voordeel van het kiezen voor het creëren van de DBI bij aanvraag door een burger is dat de overheid dit dan doet op verzoek van die burger. Dit is vergelijkbaar met een paspoort of ID-kaart, die wordt ook pas gemaakt zodra een burger daarom verzoekt.

4.12 DBI ten opzichte van andere authenticatiemechanismen

Een bestaand authenticatiemechanisme is DigiD en dit kent verschillende niveaus. Waarin onderscheidt DBI zich van DigiD? Dat is een hele terechte vraag en we zien veel ontwikkelingen op de diverse gebieden. Deze vraag is pas goed te beantwoorden of te onderzoeken wanneer duidelijk is hoe een DBI zijn plaats, gebruiksdoel, krijgt in het maatschappelijk verkeer / ecosysteem. Wordt de DBI gezien als een authenticatie-mechanisme of als een inhoudelijk component van waaruit verstrekking van gegevens mogelijk is. Tevens is daarbij de vraag of DigiD zekerheid kan verschaffen over de fysieke persoon die de "credentials" ingeeft.

4.13 Uitgangspunten

Bij het ontwikkelen van de DBI is aangesloten bij enkele uitgangspunten uit de Visiebrief en de eIDAS-conceptverordening. Deze uitgangspunten zijn hieronder opgenomen.

Deze uitgangspunten zijn richtinggevend en bepalen vanuit het beleid welke grenzen gesteld kunnen worden aan de DBI dan wel de minimale eisen waar de DBI aan moet voldoen.

Visiebrief
Iedereen heeft recht op precies één digitale (bron)identiteit. Dit betreft personen die een relatie hebben met de Nederlandse overheid en beschikken over een BSN.
De digitale bronidentiteit bevat een minimale set van deelbare identiteitsgegevens.
De digitale identiteit is uniek. Dit wil zeggen dat een DBI met een specifieke referentie maximaal één keer voorkomt.
De overheid creëert met de digitale bronidentiteit een 'gezaghebbende bron' van betrouwbare persoonsidentificatiegegevens.
Burgers krijgen de mogelijkheid om zelf de regie te voeren over hun identiteitsgegevens.
De DBI als 'gezaghebbende bron' maakt afgeleide digitale identificatiemiddelen mogelijk.
De overheid geeft een erkende digitale bronidentiteit uit die toepasbaar is in zowel de publieke als private sector en toepasbaar is in zowel het burger- als het bedrijvendomein.
De digitale bronidentiteit zal een hoog betrouwbaarheidsniveau moeten hebben om bruikbaar te zijn in verschillende sectoren.

Visiebrief
De digitale identiteit infrastructuur en alle toegelaten identificatiemiddelen bieden waarborgen voor bescherming van de privacy van de burger (privacy-by-design).
Het verkrijgen en het gebruik van een digitale bronidentiteit is eenvoudig en intuïtief.
eIDAS Conceptverordening
De lidstaten moeten voor al hun onderdanen en ingezetenen gelijke toegang tot digitale identificatie waarborgen.
De lidstaten moeten krachtens de verordening specifieke maatregelen nemen om te waarborgen dat tijdens het elektronische identificatieproces de identiteit correct wordt gematcht. Voor datzelfde doel moet de verplichte minimale reeks gegevens uitgebreid worden en wordt het gebruik van een uniek en permanent elektronisch identificatiemiddel overeenkomstig het Unierecht vastgelegd voor die gevallen waarin het noodzakelijk is de gebruiker op eigen verzoek op unieke en permanente wijze wettelijk te identificeren.
Alle Unieburgers en andere ingezetenen moeten krachtens nationaal recht veilig, gebruiksvriendelijk en gemakkelijk gegevens over hun identiteit kunnen delen, waarbij de gebruiker volledige controle heeft. De op die doelstellingen (portemonnees) gerichte technologieën moeten worden ontwikkeld met het oog op: • het hoogste niveau van beveiliging; • het hoogste niveau van gebruiksgemak; brede inzetbaarheid. Alle Europese portemonnees voor digitale identiteit moeten gebruikers in staat stellen: • om zich grensoverschrijdend te identificeren en te authentiseren; • om zich online en offline te identificeren en te authentiseren; • om toegang tot een breed scala publieke en private diensten te krijgen.

4.14 Verstrekking aan de burger

De vorige paragraaf licht toe waarom een wallet nodig is om de DBI te kunnen gebruiken. De uitgifte van een DBI hangt dan ook samen met het koppelen van de DBI aan de wallet. De betrouwbaarheid van het gebruik van de DBI hangt af van de betrouwbaarheid van de wijze waarop de DBI wordt uitgegeven en wordt gekoppeld aan de wallet.

De hoogste mate van betrouwbaarheid wordt behaald met in-persoon identificatieverificatie. Dit kan door een fysieke afgifte van de DBI/koppeling aan de wallet bij een balie. Vergelijk dit ook met de uitgifte van een paspoort. Dit vereist capaciteit aan de balies, iets wat in de praktijk niet altijd voorhanden is. Zo heeft de gemeentebalie zeer beperkte extra ruimte voor extra taken. Indien daar een extra taak, zoals uitgifte van de DBI, wordt belegd, dan moet dit vooraf afgestemd worden met de gemeenten. Dit proces kan er op hoofdlijnen als volgt uitzien:

- Fysiek balieproces bij een gemeente in Nederland: dit proces is gebaseerd op het balieproces dat voor vID is uitgewerkt en in beperkte mate is beproefd.

Tijdens de uitvoering van dit proces wordt de RFID-chip van het (Nederlandse) identiteitsmiddel van de burger uitgelezen en een biometrische vergelijking uitgevoerd tussen de burger en de foto uit het identiteitsmiddel. Er wordt een beveiligde verbinding gemaakt tussen de DBI-kernvoorziening (zie paragraaf 5.4) en de telefoon van de burger waarop de NL Wallet is geïnstalleerd (en geconfigureerd). Nadat controles zijn uitgevoerd om onder andere de integriteit en authenticiteit van de NL Wallet vast te stellen, krijgt de NL Wallet de status ‘actief’ en kan de burger zijn DBI downloaden in de NL Wallet.

Een alternatief voor afgifte aan een balie betreft het plaats- en tijdonafhankelijk afgeven van de DBI en koppelen aan de wallet. Hierbij hoeft een persoon niet zelf fysiek aan een balie te verschijnen. Wel zijn waarborgen opgenomen voor de identiteitsverificatie. Dit proces kan er op hoofdlijnen als volgt uitzien:

- Virtueel balieproces met videogesprek[13]. Hiervoor dient de burger een afspraak te maken in het portaal van de uitgevende instantie. Hij kan dat doen met DigiD ‘laag’ of ‘substantieel’ of zonder enige vorm van authenticatie. Tijdens het videogesprek worden door de medewerker van de uitgevende instantie

[13] Bijvoorbeeld bij ‘Nederland Wereld’ van het ministerie van Buitenlandse Zaken.

controles uitgevoerd. Welke dat zijn, is mede afhankelijk van de authenticatiewijze bij het maken van de afspraak en bij het aanmelden bij het videogesprek. Als de medewerker van de uitgevende instantie geen redenen ziet om de uitgifte van een DBI te weigeren, stelt hij de DBI van de burger beschikbaar voor de burger.

- Of: Virtueel balieproces zonder videogesprek. Hiervoor moet de burger zich aanmelden met DigiD hoog (of een vergelijkbaar middel). Het uitgifteproces is grotendeels gelijk aan dat van het virtuele balieproces met videogesprek. Alleen worden de controles geautomatiseerd uitgevoerd door een of meerdere algoritmen. Als alle controles met positief resultaat zijn uitgevoerd, wordt de DBI beschikbaar gesteld voor download door de burger. Resulteren één of meerdere controles in een negatief resultaat dan wordt de burger geadviseerd een nieuwe afspraak te maken maar dan voor een fysiek balieproces of een virtueel balieproces met videogesprek. Technisch is dit alternatief mogelijk, waarbij biometrie vanuit bijvoorbeeld het paspoort en/of de eNIK hergebruikt kan worden. De vraag is of deze optie voldoende betrouwbaar wordt geacht om toe te passen.

Te maken beleidskeuzes

Keuzes
• Gebruik BSN (encryptie) als verbinding tussen DBI en administratieve systemen?
• Wordt de minimale set gegevens uitgebreid? In de wallet of in de DBI?
• Welke identificatiecode wordt gebruikt in de DBI?
• Welke alternatieven voor afgifte van de DBI worden betrouwbaar genoeg geacht en voor welke alternatieven wordt gekozen?

5 Het identiteitsecosysteem

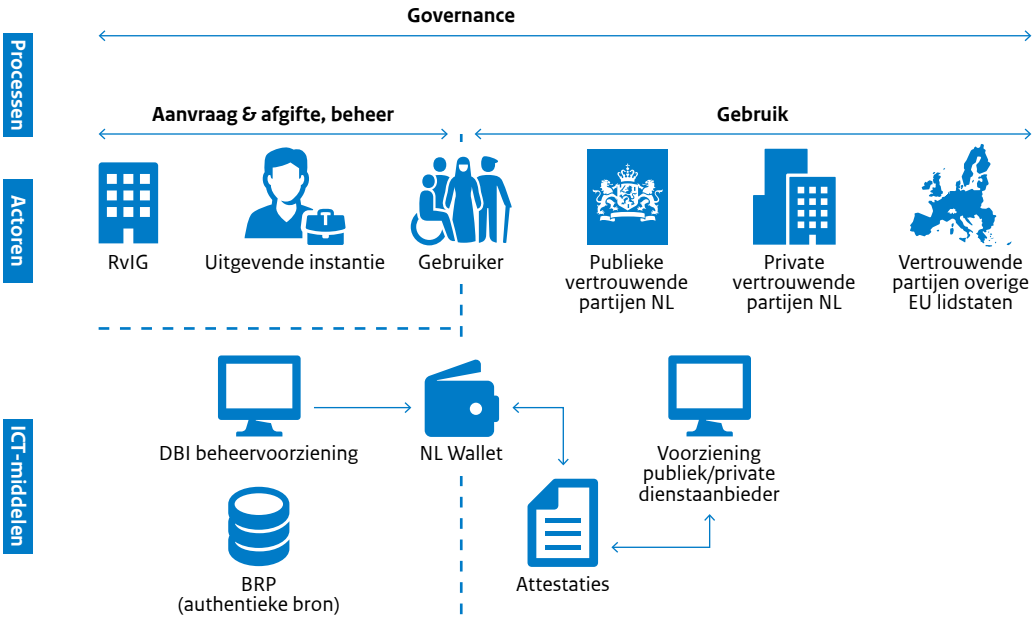
5.1 De noodzaak van een identiteitsecosysteem

Om ervoor te zorgen dat de DBI en de wallet op een betrouwbare, veilige, voorspelbare wijze kunnen worden gebruikt in het maatschappelijk verkeer, is een goed werkend identiteitsecosysteem nodig, waarin meerdere partijen een belangrijke rol spelen. Publieke én private dienstaanbieders bieden in het identiteitsecosysteem concrete diensten aan burgers aan. Ook ondersteunende diensten en een helder afsprakenstelsel maken deel uit van het ecosysteem.[14]

Met de term identiteitsecosysteem bedoelen wij het volgende: het geheel aan (o.a.) wetten/afspraken, diensten/producten, processen, applicaties, gegevensverzamelingen dat nodig is om ervoor te zorgen dat een burger zich op een betrouwbare en veilige wijze digitaal kan identificeren en authentiseren bij publieke en private dienstaanbieders.

Bovenstaande definitie is opgesteld vanuit gezichtspunt van de burger. Uiteraard hebben ook dienstaanbieders een groot belang bij een goed werkend ecosysteem (en dus onder andere bij een betrouwbare DBI en een betrouwbare wallet NL Wallet.) Figuur 10 geeft een vereenvoudigd beeld van het identiteitsecosysteem weer. Hierin is voor de wallet de naam 'NL Wallet' gebruikt, welke verwijst naar de wallet die onder beheer van de Nederlandse overheid wordt uitgegeven voor gebruik met de DBI, in lijn met de eIDAS Conceptverordening.

Figuur 10 *Vereenvoudigde weergave van het identiteitsecosysteem*



[14] In die zin kan een ecosysteem min of meer worden vergeleken met een ketenproces. In de 'visiebrief digitale identiteit' van de staatssecretaris van BZK d.d. 11-2-2021 wordt het identiteitsecosysteem 'digitale identiteit infrastructuur' genoemd.

In deze vereenvoudigde weergave bestaat het identiteitsecosysteem uit drie lagen:

1. Processen: dit zijn enerzijds de processen die nodig zijn voor de aanvraag en uitgifte van een DBI en voor het beheer ervan. Anderzijds betreft dit de processen die nodig zijn voor het gebruik van een DBI in het maatschappelijk verkeer.
2. Actoren: dit zijn de actoren die (delen van) de processen uitvoeren om zo diensten te kunnen aanbieden, afnemen en onderling te kunnen afstemmen.
3. ICT-middelen: dit zijn de ICT-middelen die de uitvoering van de processen ondersteunen/mogelijk maken, zoals de DBI- beheervoorziening. Dit is vooralsnog een algemene aanduiding voor de voorzieningen die nodig zijn om een DBI te kunnen aanvragen, uitgeven en beheren. Ook gebruikersondersteuning is een functionaliteit van de DBI- beheervoorziening. Op een later moment wordt de DBI-beheervoorziening verder uitgewerkt in één of meerdere voorzieningen.

Randvoorwaardelijk voor een goede werking van het identiteitsecosysteem is interoperabiliteit tussen de verschillende onderdelen van het ecosysteem. Interoperabiliteit staat voor het vermogen van organisaties (en hun processen en systemen) om effectief en efficiënt informatie te delen met hun omgeving.[15] De diensten en producten van dienstaanbieders in het identiteitsecosysteem moeten op elkaar aansluiten en 'dezelfde taal spreken'.

5.2 Processen

Zie de Bijlage: Diensten in het identiteitsecosysteem voor een beschrijving van de diensten die deel uitmaken van het identiteitssysteem.

5.2.1 *Aanvraag en uitgifte*

Iedereen kan de NL Wallet downloaden vanuit de Apple App Store of Google Play. Een specifieke DBI wordt echter uitgegeven aan een specifieke ingezetene van Nederland en op voorwaarde dat hij is ingeschreven in de BRP.

5.2.2 *Beheer*

Beheerprocessen voor de DBI betreffen onder meer de uitgifte van een DBI, het blokkeren of intrekken van een DBI, het leveren van ondersteuning aan dienstafnemers -en aanbieders en het bieden van een meldpunt voor het melden van verlies, fouten, fraude. Als daadwerkelijk een DBI aangeboden wordt aan burgers, dan dienen deze beheerprocessen ingericht en aangeboden te worden.

5.2.3 *Gebruik*

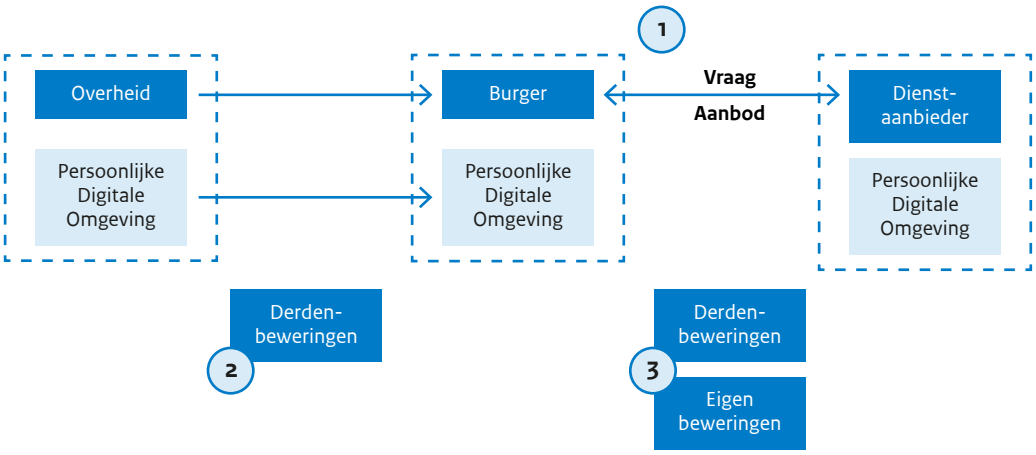
Burgers kunnen met een DBI op verschillende manieren gegevens delen. Dit kunnen gegevens zijn die (ook) opgenomen zijn in de DBI (bijvoorbeeld vanuit de minimale gegevensset), maar ook andere gegevens van de betreffende burger die met behulp van de DBI ontsloten kunnen worden.
Twee mogelijke interactiepatronen hiertoe zijn (gebaseerd op de interactiepatronen van het Programma Regie op Gegevens):[16]

1. De burger deelt zelf gegevens met een vertrouwende partij, of
2. De burger geeft (eenmalig) toestemming aan een vertrouwende partij om bepaalde gegevens op te vragen bij een (gekwalificeerde) verlener van vertrouwensdiensten.

[15] https://www.noraonline.nl/wiki/Interoperabiliteit (24-11-2021).
[16] Deze interactiepatronen zijn overgenomen uit de Referentiearchitectuur Regie op Gegevens. Daar worden zij 'Burger wint in' resp. 'Dienstaanbieder wint in' genoemd.

Onderstaande figuur geeft het eerste interactiepatroon weer.

Figuur 11 *Interactiepatroon 'Burger wint in'*



De onderstaande beschrijving van het interactiepatroon is gebaseerd op de referentiearchitectuur van Regie op Gegevens:

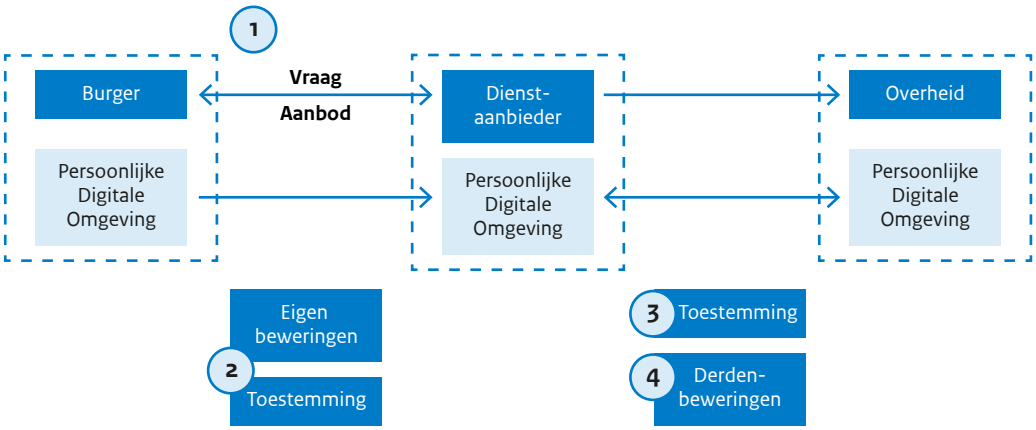
1. De burger wil een product of dienst afnemen van de dienstaanbieder. Om een aanbod te kunnen doen, heeft de dienstaanbieder (persoons)gegevens van/over de burger nodig. Een deel van die informatiepositie zal bestaan uit gegevens die de burger zelf kan/moet invullen (eigen beweringen). Een ander deel kan bestaan uit gegevens die (op verzoek van de dienstaanbieder) uit een andere bron afkomstig zijn. Die gegevens noemen we derdenbeweringen; zij zijn afkomstig van de overheid. Het deel van de informatiepositie dat de burger met eigen beweringen kan invullen, kan de burger direct aan de dienstaanbieder leveren.
2. Voor derdenbeweringen moet de burger dit gegeven eerst uit de bron van de overheid ophalen en in zijn eigen Persoonlijke Digitale Omgeving moeten brengen. Als hij nog over een geldig gegeven uit de overheidsbron in zijn eigen Persoonlijke Digitale Omgeving beschikt, dan kan hij deze natuurlijk direct gebruiken en is ophalen bij de overheid niet nodig.
3. Als de burger de gevraagde gegevens (dus derdenbeweringen en eigen beweringen) compleet heeft, kan hij deze aan de dienstaanbieder leveren. Vervolgens kan de dienstaanbieder het aanbod doen.

Kenmerken van dit interactiepatroon zijn:

- De positie van de burger. Deze staat letterlijk tussen dienstaanbieder en de bron in. Hij heeft by design volledig zicht op en controle over de gegevens die vanuit de overheidsbron met de dienstaanbieder gedeeld worden. De burger heeft dus zelf zicht op welke gegevens gedeeld worden. Hij kan zorgen dat er zo min mogelijk gedeeld wordt: alleen die gegevens die strikt noodzakelijk zijn.
- Geen koppeling tussen uitvraag bij de bron en doel waarvoor het gebruikt wordt: de burger hoeft niet aan de bronhouder te verantwoorden waarom/waarvoor het persoonsgegeven ingewonnen wordt.
- De wens van het waarmerk: de dienstaanbieder wil de garantie dat het gegeven uit de bron (de derden bewering) ook daadwerkelijk van die bron afkomstig is en overeenkomt met die bron.

Onderstaande figuur geeft het tweede interactiepatroon weer.

Figuur 12 *Interactiepatroon 'Dienstaanbieder wint in'*



De onderstaande twee opsommingen zijn gebaseerd op de referentiearchitectuur van Regie op Gegevens en beschrijven het interactiepatroon:

1. Ook dit interactiepatroon start met de relatie tussen dienstaanbieder en de burger. Om een aanbod te kunnen doen, heeft de dienstaanbieder (persoons)gegevens van/over de burger nodig. Een deel van die informatiepositie kan bestaan uit eigen beweringen en (mogelijk) een deel uit derdenbeweringen.
2. Het verschil met het vorige interactiepatroon is dat de burger de derden bewering niet inwint. De dienstaanbieder biedt aan om dat namens deze burger te doen. Het is dus de dienstaanbieder die zich bij de overheid digitaal meldt met het verzoek om een persoonsgegeven. De bronhouder zal vanwege zijn geheimhoudingsplicht deze gegevens alleen ter beschikking stellen als de dienstaanbieder toestemming heeft van de burger om namens hem de persoonsgegevens bij de overheid in te winnen.
3. De dienstaanbieder wint met toestemming van de burger zijn persoonsgegevens (derdenbeweringen) in bij de overheid.
4. De overheid deelt - na validatie van het verzoek – de derdenbeweringen met de dienstaanbieder.

Kenmerken van dit interactiepatroon zijn:

- De positie van de burger: in dit interactiepatroon staat de dienstaanbieder tussen de burger en de bron in. Vanuit deze positie heeft de burger by design veel minder zicht en controle op de gegevens die vanuit de overheidsbron met de dienstaanbieder gedeeld worden. Om de burger toch vertrouwen te geven in zowel dienstaanbieder als overheid, zijn aanvullende maatregelen gericht op dit vertrouwen noodzakelijk.
- Het onderwerp toestemming maakt altijd onderdeel uit van dit interactiepatroon.
- Koppeling tussen uitvraag bij de bron en doel waarvoor het gebruikt wordt: de burger geeft toestemming aan de dienstaanbieder om gegevens namens hem in te winnen. De eis aan de toestemming is dat deze voldoende specifiek en afgebakend is (dus geen toestemming zoals dat nu bij bijvoorbeeld cookies het geval is). Hierdoor kan de overheid mogelijk afleiden welke gegevens, waarvoor en aan wie geleverd worden.
- De wens van het waarmerk is in dit interactiepatroon minder relevant. De dienstaanbieder haalt namelijk zelf de gegevens rechtstreeks bij de vertrouwde bron. Daarmee heeft hij al de nodige garanties op afzender en integriteit van het gegeven. Natuurlijk staat het de dienstaanbieder vrij om tegen vergoeding extra vertrouwensservices zoals digitale handtekening en/of digitale seal te gebruiken.
- Het moment waarop de burger een toestemming verleent en aan wie kan verschillen en leiden tot een variant op bovenstaand interactiepatroon. Het is immers mogelijk dat de burger zijn toestemming aan de overheid kenbaar maakt voordat de dienstaanbieder een verzoek doet bij de overheid tot het leveren van de benodigde specifieke persoonsgegevens.[17] De overheid moet dan in haar eigen administratie nagaan of de specifieke toestemming van die burger bestaat om vervolgens dit gegeven met toestemming van die burger aan de dienstaanbieder te leveren.

[17] Toestemming tot het leveren van vooraf gedefinieerde persoonsgegevens aan vooraf gedefinieerde dienstaanbieders in vooraf gedefinieerde gevallen.

Beide interactiepatronen geven uiteindelijk hetzelfde resultaat. De vereisten die voortkomen uit de interactiepatronen (bijvoorbeeld waarmerken en toestemming) verschillen echter.

Een belangrijk uitgangspunt van Regie op Gegevens is dat de burger vrij is in zijn keuze voor een interactiepatroon. Welk interactiepatroon gevolgd wordt, kan dus per dienstafname verschillen.

5.3 Actoren

Natuurlijke - en rechtspersonen nemen diensten en/of producten af, of leveren deze. Ook voeren zij (delen van) processen uit. Dat doen zij vanuit een specifieke rol. Binnen het identiteitsecosysteem onderscheiden we onder andere de volgende actoren en rollen:

Actor	Rol	Opmerking
Burger	Dienstafnemer: • Gebruiker. Dienstaanbieder: • Vertrouwende partij in geval van een burger→burger transactie.	Denk bijvoorbeeld aan webwinkels.
Gemeente	Dienstaanbieder (uitgeven DBI).	
Ministerie van Buitenlandse Zaken ('Nederland Wereldwijd')	Dienstaanbieder (uitgeven DBI).	
RvIG	Beheerder kern-voorzieningen (zie volgende paragraaf).	
Publieke en private organisaties	Eigenaar/beheer van andere relevante apps.	Denk bijvoorbeeld aan banken, luchtvaart-maatschappijen. Kunnen ook onder de rol dienst-aanbieder vallen.
Publieke organisatie	Dienstaanbieder: • Gekwalificeerde verlener van vertrouwens-diensten. • Vertrouwende partij.	Dit betreft overheids-organisaties; zowel Neder-landse als die van andere lidstaten.
Private organisatie	Dienstaanbieder: • Gekwalificeerde verlener van vertrouwensdiensten. • Vertrouwende partij.	Dit betreft het bedrijfsleven; zowel Neder-landse als uit andere lidstaten. Ook 'zeer grote online plat-formen' vallen hieronder.
Bibliotheek/informatiepunt digitale overheid	In-persoon helpdesk voor burgers.	

Bovenstaand overzicht is nog niet compleet. Voor het ecosysteem voorzien we ook rollen als 'Toezichthouder', 'Helpdesk', 'Leverancier NL Wallet' en 'Beheerder kernvoorzieningen'. Aan die rollen kan op dit moment nog geen actor worden gerelateerd.

5.3.1 *Samenvatting van eisen uit de conceptverordening*

Eisen aan gekwalificeerde verleners van vertrouwensdiensten conform conceptverordening eIDAS (artikelen 24 lid 1 en 45 decies lid 1)

- Een gekwalificeerde verlener van vertrouwensdiensten moet de identiteit van een gebruiker (of diens specifieke attributen) verifiëren alvorens hij gekwalificeerde elektronische attesteringen van attributen afgeeft aan de betreffende gebruiker.
- Verleners van gekwalificeerde attesteringen van attributen mogen:
  - Geen informatie ontvangen over het gebruik van de door hen verstrekte attributen.
  - De via de NL Wallet ontvangen identiteitsgegevens niet combineren met identiteitsgegevens die zij hebben ontvangen t.b.v. andere vormen van dienstverlening.[18]
- Een gekwalificeerde verlener van vertrouwensdiensten kan een gekwalificeerd elektronisch register aanmaken.

Eisen aan vertrouwende partijen conform conceptverordening eIDAS (6 bis 4 (a)(2), 4 (b), 6 ter 1, 6 ter 2, 12 quater 1

Vertrouwende partijen moeten:

- Het voorgenomen gebruik van de NL Wallet bij een overheidsloket melden.
- Identiteitsgegevens en elektronische attesteringen van attributen, die zij ontvangen via een wallet, authentiseren.
- Identiteitsgegevens en elektronische attesteringen van attributen valideren.
- Gebruikers authentiseren.
- Aanvragen voor diensten, gedaan met gecertificeerde wallets uit andere lidstaten, in behandeling nemen.

Eisen aan de overheid conform conceptverordening eIDAS (6 bis 5, 6 ter 2, 20 lid 1, 45 quinquies lid 1)

De overheid dient te voorzien in verschillende valideringmechanismen om:

- De authenticiteit en geldigheid van de NL Wallet te kunnen verifiëren.
- Dat impliceert dat aan elke individuele uitgegeven NL Wallet een status moet kunnen worden toegekend.
- Vertrouwende partijen de mogelijkheid te geven te controleren of door hen ontvangen elektronische attesteringen van attributen geldig zijn.
- Gekwalificeerde verleners van vertrouwensdiensten en vertrouwende partijen de gelegenheid geven te controleren of de door hen ontvangen identiteitsgegevens (die zijn opgenomen in de bovengenoemde attesteringen) authentiek en geldig zijn.
- Gekwalificeerde verleners van elektronische attesteringen van attributen de mogelijkheid te geven de authenticiteit van attributen te kunnen verifiëren in een relevante authentieke bron.

Ook dient de overheid:

- Vertrouwenslijsten op te stellen met gekwalificeerde verleners van vertrouwensdiensten en de diensten die elke verlener aanbiedt.
- Een conformiteitsbeoordelingsorgaan in te richten. Dat orgaan voert minimaal eenmaal per 24 maanden een audit uit op de gekwalificeerde verleners van vertrouwensdiensten uit.
- Het conformiteitsbeoordelingsorgaan kan de status van een verlener of van (een of meerdere van) zijn diensten intrekken.

Daarnaast dienen de lidstaten te zorgen voor een gemeenschappelijk mechanisme om de authenticiteit van vertrouwende partijen te kunnen vaststellen.

[18] Ook al staat hier expliciet de NL Wallet genoemd, dit geldt ook voor gegevens die zijn ontvangen via andere verschijningsvormen van de Europese portemonnee voor digitale identiteit. Dus bijv. een in België uitgegeven wallet.

5.4 ICT-middelen

In het identiteitsecosysteem kunnen verschillende soorten voorzieningen worden onderscheiden:

- NL Wallet. Deze wordt door de gebruiker gebruikt om een DBI te activeren/beheren en om diensten/producten af te nemen. Van de 'NL Wallet' zijn twee verschijningsvormen mogelijk:
  - Eén die kan worden geïnstalleerd op een mobiele telefoon; en
  - Eén die in een cloud-oplossing is opgenomen. Denk bijvoorbeeld aan MijnOverheid.nl.
  - Een variant hierop is een datakluis. Deze heeft geen wallet-functionaliteit en kan alleen worden gebruikt om gegevens op te slaan en beschikbaar te stellen aan de NL Wallet.
- Kernvoorzieningen. Dit betreft de overheidsvoorzieningen die nodig zijn om onder andere:
  - DBI's te kunnen uitgeven en beheren.
  - Attesteringen die zijn gebaseerd op een DBI uit te geven, beheren en valideren.
  - Het overzicht van geautoriseerde dienstaanbieders te beheren en validatieverzoeken uit te voeren.
- Aanvullende voorzieningen. Dit zijn (bestaande) overheidsvoorzieningen die ondersteunende functionaliteit bieden.
- Voorzieningen van dienstaanbieders. Dit zijn voorzieningen die de Nederlandse publieke en private (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen nodig hebben om diensten te kunnen leveren.

6 Juridische en ethische analyse van de bronidentiteit

6.1 De juridische analyse van de bronidentiteit

De DBI behoeft een juridische basis in wet- en regelgeving. Om te bepalen hoe en waar deze juridische basis zou moeten worden vormgegeven, wordt eerst een overzicht van de bestaande wet- een regelgeving rondom identiteit uiteengezet. Dit in volgorde van internationaal naar nationaal. Ten tweede volgt een uiteenzetting van de juridische status van een DBI, waarbij wordt bezien in hoeverre wet- en regelgeving moet worden gemaakt dan wel aangepast met de daarbij behorende tijdslijnen.

6.2 Juridisch kader rondom identiteit

6.2.1 *ICAO*

De Internationale Burgerluchtvaartorganisatie (ICAO) stelt internationale standaarden en richtlijnen op voor de burgerluchtvaart. Zo heeft de ICAO standaarden ontwikkeld voor paspoorten en andere reisdocumenten (ICAO 9303)[19] en recent ook voor de uitgifte van een digitaal reisdocument: Digital Travel Credentials (DTC).[20]

Bij de ontwikkeling van de DBI zal rekening gehouden moeten worden met deze twee standaarden. Daarmee wordt aangesloten bij internationale ontwikkelingen op het gebied van contactloos reizen.

De nieuwe DTC-standaard moet echter nog wel in (Europese) wet- en regelgeving worden opgenomen. Dat betekent dat de nieuwe DTC (nog) geen geldig reisdocument is.

6.2.2 *Algemene Verordening Gegevensbescherming (AVG)*

De AVG reguleert de verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijk persoon.[21] De DBI bevat ten minste een minimale set van identiteitsgegevens die nodig is in het maatschappelijk verkeer,[22] waardoor de AVG van toepassing is. Het valt buiten de reikwijdte van dit onderzoeksrapport om elke verwerking die hiermee plaatsvindt aan alle vereisten van de AVG te toetsen. Wel worden hier de belangrijkste beginselen waar elke verwerking aan moet voldoen summier besproken.

Ten eerste moeten persoonsgegevens worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is.[23] Concreet betekent dit dat elke verwerking een grondslag nodig heeft. De DBI wordt door de overheid uitgegeven, erkend en verankerd in wet- en regelgeving.[24] Deze wet- en regelgeving zou dan dienen als verwerkingsgrondslag voor de overheid als verwerkingsverantwoordelijke.[25] Het doel is uiteindelijk dat met een DBI de burger meer regie, zelfbeschikking of controle krijgt over diens eigen persoonsgegevens.[26] Op basis van welke grondslag dit geëffectueerd zou kunnen worden, behoeft nader

[19] ICAO Doc 9303 Machine Readable Travel Documents.
[20] ICAO-TR Digital Travel Credentials.
[21] Artikel 4 onderdeel 1 AVG.
[22] *Kamerstukken II* 2020/21, 26643, nr. 743, p. 4.
[23] Artikel 1 lid 1 sub a AVG.
[24] *Kamerstukken II* 2020/21, 26643, nr. 743, p. 4-5.
[25] In samenhang met artikel 6 lid 1 sub e AVG.
[26] Zie ook overweging 7 AVG.

juridisch onderzoek; er zijn meerdere oplossingsrichtingen mogelijk.[27] Dit geldt ook voor de rol die de verschillende dienstverleners hebben in de persoonsgegevensstromen.

In de wettelijke grondslag moet ook het doel van de verwerking(en) komen te staan. Het tweede beginsel van de AVG luidt immers dat persoonsgegevens alleen mogen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (doelbinding).[28] Voor een deel is de doelbinding bijvoorbeeld al specifiek in de conceptverordening eIDAS geregeld (artikel 6bis, lid 4, onder b en lid 7). Zo mogen vertrouwensdiensten geen informatie ontvangen over het gebruik van attributen en mogen uitgevers van wallets geen informatie verzamelen over het gebruik van de wallet of deze combineren als dit niet noodzakelijk is.

Het derde beginsel uit de AVG is dataminimalisatie.[29] Aan dit beginsel wordt voldaan doordat de minimale gegevensset niet meer behelst dan wat noodzakelijk is voor gebruik in de publieke en private sector en dienstverleners alleen de gegevens verwerken die nodig zijn voor de te leveren dienst.[30] Daarnaast moeten de persoonsgegevens juist zijn en zo nodig worden geactualiseerd (beginsel van juistheid), niet langer worden bewaard dan noodzakelijk (beginsel van opslagbeperking) en goed worden beveiligd (beginsel van integriteit en vertrouwelijkheid).[31]

Het voorschrift van privacy by design schrijft voor dat reeds bij het ontwerp rekening wordt gehouden met privacy- en gegevensbescherming door passende technische en organisatorische maatregelen te treffen.[32] Een voorbeeld van zo'n technische maatregel is het gebruik van pseudonimisering. Ook moet een privacyvriendelijke verwerking van persoonsgegevens worden afgedwongen, gebruikers moeten zoveel mogelijk controle hebben en zij moeten worden geïnformeerd over de verwerking van hun persoonsgegevens.

Ook is een gegevensbeschermingseffectbeoordeling noodzakelijk (ook wel een Data Protection Impact Assessment (DPIA) genoemd).[33]

In de AVG is een onderscheid gemaakt tussen 'gewone' persoonsgegevens en 'bijzondere' persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die gezien hun aard extra gevoelig zijn. In beginsel geldt daarom een verbod om bijzondere persoonsgegevens te verwerken, tenzij de verwerking kan worden gebaseerd op toegestane uitzonderingen.[34] Een voorbeeld van bijzondere persoonsgegevens zijn biometrische gegevens. In paragraaf 4.2.2 is besproken op welke wijze biometrie een rol kan spelen bij de DBI. Er is sprake van een verwerkingsverbod wanneer deze biometrische gegevens worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijk persoon mogelijk maken.[35] De manier waarop de verwerking van biometrie in dit onderzoeksrapport is gepresenteerd, voldoet aan deze definitie. Meer concreet wordt ook de centrale opslag van biometrie noodzakelijk geacht om een hoog betrouwbaarheidsniveau te kunnen garanderen en identiteitsfraude te

[27] Zo wordt een grondslag geopperd op basis van de rechten van de betrokkenen in Regie op gegevens en de AVG (notitie door Pels Rijcken in opdracht van het programma Regie op Gegevens), Den Haag: Programma Regie op Gegevens 2018. Een andere mogelijkheid is de uitzondering van het huishoudelijk gebruik (artikel 2 lid 2 sub c AVG). Zie bijvoorbeeld ook P.J.C. Olsthoorn, Baas over eigen data. Zelfbeschikking in bescherming van persoonsgegevens, Den Haag: Boom Juridisch 2021 & M. Hildebrandt, De soeverein is niet thuis, Ars Aequi 20190546.

[28] Artikel 5 lid 1 sub b AVG.

[29] Artikel 5 lid 1 sub c AVG.

[30] Ibidem.

[31] Artikel 5 lid 1 sub d-f AVG.

[32] Artikel 25 AVG.

[33] Artikel 35 AVG.

[34] Artikel 9 AVG.

[35] Overweging 51 AVG.

voorkomen. Een dergelijk centraal register hebben wij niet in Nederland.[36] Een uitzondering voor het verwerkingsverbod kan worden gecreëerd middels nationale wetgeving om redenen van zwaarwegend algemeen belang.[37] Onder andere de noodzaak, proportionaliteit en subsidiariteit van de verwerkingen van biometrische gegevens bij de DBI zou dan grondig moeten worden afgewogen aan de privacyrisico's voor de burgers die deze verwerkingen met zich meebrengen. Dit vereist een brede maatschappelijke discussie over de wenselijkheid hiervan.

Het burgerservicenummer (BSN) verdient in het kader van de AVG nog bijzondere aandacht. Het BSN is een uniek, nationaal identificatienummer en de verwerking daarvan moet in Nederland bij wet zijn voorgeschreven.[38] De Wet algemene bepalingen burgerservicenummer (Wabb) bepaalt dat overheidsorganen gebruik kunnen maken van het BSN bij de uitvoering van hun taken.[39] Organisaties buiten de overheid mogen het BSN alleen gebruiken als dat wettelijk is bepaald, zoals in de Zorgverzekeringswet en de Pensioenwet. Hoewel de Autoriteit Persoonsgegevens het belang van gebruik van het BSN buiten de overheid onderkent, geeft ze nog geen toestemming voor een breder gebruik.[40] Dit maakt het breed inzetten van het BSN vooralsnog onmogelijk, tenzij de Wabb wordt herzien of andere technieken voorhanden zijn die het BSN onherleidbaar tot een individu maken [zie ook het document Bijlage: Koppeling met de Basisregistratie].

6.2.3 eIDAS-verordening

In paragraaf 3.1.2 is de eIDAS-verordening en het wijzigingsvoorstel van de Europese Commissie kort besproken. In deze paragraaf zullen we nader ingaan op een specifiek onderdeel van het wijzigingsvoorstel, namelijk de "European Digital Identity Wallet''.

Elke lidstaat is verplicht om tenminste één 'European Digital Identity Wallet' (EDIW) te introduceren. De lidstaten kunnen de EDIW in eigen beheer uitgeven, onder mandaat uitgeven of een onafhankelijk uitgegeven wallet erkennen. Met een EDIW kunnen burgers én bedrijven onder een hoog beveiligingsniveau hun digitale identiteit én daaraan gelinkte attributen zelf ter beschikking te stellen in online én offline transacties, in het publieke én het private domein. De EDIW staat onder volledige controle van de gebruiker. Dit uitgangspunt komt ook terug in programma Regie op Gegevens.

Aanvullend wil de Commissie samen met de lidstaten een 'Toolbox' ontwikkelen om de implementatie te ondersteunen van onder meer de wallet en gekwalificeerde vertrouwensdiensten. Daarin worden de technische architectuur, het referentieraamwerk, gemeenschappelijke standaarden, technische specificaties, gemeenschappelijke richtlijnen en 'best practices' opgenomen.

Het voorstel heeft ook gevolgen voor elektronische vertrouwensdiensten die tevens in de eIDAS-verordening worden gereguleerd. Een belangrijke wijziging is de toevoeging van vijf nieuwe soorten vertrouwensdiensten:

- Het op afstand beheren van middelen (hardware en software) voor Het aanmaken van elektronische handtekeningen;
- Het op afstand beheren van middelen (hardware en software) voor het aanmaken van elektronische zegels;
- Elektronische attestatie van attributen;
- Gekwalificeerde elektronische archiveringsdiensten en elektronische grootboeken (ledgers).

---

[36] Momenteel is een wijziging van de Paspoortwet in consultatie in verband met de invoering van een centrale voorziening voor biometrische gegevens. Deze biometrische gegevens worden echter slechts opgeslagen in een centrale voorziening ten behoeve van het aanvraag- en uitgifteproces van reisdocumenten, waarbij (nog) geen sprake is van bepaalde technische middelen die eenduidige identificatie mogelijk maken of bevestigen.

[37] Artikel 9 lid 2 sub g AVG.

[38] Artikel 87 AVG in samenhang met artikel 46 UAVG.

[39] Artikel 10 Wabb.

[40] *Onderzoeksrapport Onderzoek naar het Burgerservicenummer*, Auditdienst Rijk 2020, p. 7.

De verordening verplicht de lidstaten dat een aantal attributen geverifieerd kunnen worden aan de hand van authentieke bronnen binnen de publieke sector. Daarnaast moeten deze attestaties ook via de wallet beschikbaar kunnen worden gemaakt. Gekwalificeerde elektronische archiveringsdiensten verwerken data en documenten op een wijze dat de integriteit en nauwkeurigheid van de oorsprong, alsook juridische eigenschappen, bewaard blijven voor de bewaarperiode. Een elektronisch grootboek is een fraudebestendige elektronische documentatie van data waarbij de authenticiteit, integriteit van de data, datum, tijd en de chronologische ordening worden vastgelegd. Bij al deze vertrouwensdiensten geldt dat de elektronische en niet-elektronische variant hetzelfde rechtsgevolg zullen hebben. De Commissie is verplicht om binnen twaalf maanden na inwerkingtreding van het wijzigingsvoorstel uitvoeringsbesluiten te nemen ten aanzien van de relevante standaarden voor gekwalificeerde vertrouwensdiensten.
Ten aanzien van de attestatie van attributen geldt een termijn van zes maanden.

Ten slotte zal de Commissie de bevoegdheid krijgen om wetgeving van derde (niet-EU) landen te beoordelen als gelijkwaardig aan de eIDAS-verordening.

Het is van belang om bewust ervan te zijn dat het gaat om een conceptvoorstel dat aan wijzigingen onderhevig is voordat een definitieve versie in werking treedt. Inmiddels is dan ook op 10 maart 2022 onder Franse voorzitterschap een compromisvoorstel gepubliceerd als reactie op bovengenoemd voorstel van de Europese Commissie. Naast kleine aanpassingen en verduidelijkingen, zijn sommige onderdelen van het voorstel van de Commissie compleet herschreven of zijn bepaalde keuzes geïntroduceerd. Zo is naast het betrouwbaarheidsniveau hoog (was de enige optie in het voorstel van de Commissie), nu ook het betrouwbaarheidsniveau substantieel opgenomen in de bepaling over de wallet.

6.2.4 Wet basisregistratie personen

Binnen drie dagen na de bevalling moet aangifte zijn gedaan van de geboorte van een kind bij de burgerlijke stand. De ambtenaar van de burgerlijk stand maakt vervolgens een akte op van de geboorte. Voor velen is de geboorteakte het startpunt waarmee zij worden ingeschreven in de Basisregistratie Personen (hierna: BRP).[41] Inschrijving houdt in dat de persoonslijst, het geheel van gegevens over één persoon, wordt opgenomen in de BRP.[42] In zekere zin is deze registratie het administratieve beeld van de overheid over de burger: 'Ik sta geregistreerd, dus ik ben'.[43]

De BRP bevat de persoonsgegevens van alle ingezetenen en van niet-ingezetenen van Nederland.[44] Gemeenten zijn verantwoordelijk voor het bijhouden daarvan ten aanzien van ingezetenen en de Minister als het gaat om niet-ingezetenen.[45] Het primaire doel van de BRP is om overheidsorganen (of aangewezen derden) te kunnen voorzien van betrouwbare, juiste en authentieke gegevens over burgers bij de vervulling van hun taken.[46] Bij de inschrijving in de BRP wordt ook het BSN toegekend en opgenomen in de persoonslijst.[47]

De Wet BRP regelt naast bovenstaande ook het verstrekken van de gegevens uit de BRP. Net zoals gegevens uit de BRP worden gebruikt om een paspoort of identiteitskaart te voorzien van de juiste gegevens, zal de BRP ook gebruikt worden voor de minimale set aan gegevens voor een DBI.[48]
Om mede te kunnen voldoen aan de AVG, is het van belang dat deze gegevens juist en actueel zijn.

---

41 Artikel 2.2 WetBRP.
42 Artikel 1.1 Wet BRP.
43 T. Speelman, Visiedocument Dutch Self-Sovereign Identity Framework *(DSSIF)*, Dutch Blockchain Coalition 2021, p. 7.
44 Artikel 1.2 Wet BRP.
45 Artikel 1.4 Wet BRP.
46 Artikel 1.3 Wet BRP.
47 Artikel 8 Wet algemene bepalingen burgerservicenummer en artikel 2.24 Wet BRP.
48 Zo vervalt de geldigheid van een reisdocument wanneer de geslachtsnaam, de voornamen, de geboortedatum, het geslacht of het BSN van de houder zijn gewijzigd (artikel 47 Paspoortwet). Een Nederlandse Identiteitskaart kan niet vervallen worden verklaard (artikel 46a Paspoortwet).

De juridische wijze van het verstrekken van gegevens uit de BRP en van attestaties is echter afhankelijk van hoe, waar en bij welke overheidspartij (het beheer van) de DBI zal worden ingericht. Noemenswaardig is daarbij dat de Wet BRP sinds 2022 de mogelijk biedt om hiermee onder voorwaarden te experimenteren voor een beperkte duur.[49]

6.2.5 *Wet Digitale Overheid*

In het regeerakkoord Vertrouwen in de toekomst (2017-2021) is de noodzaak aangegeven voor de verdere digitalisering van het openbaar bestuur op verschillende niveaus.[50] De Wet Digitale Overheid (hierna: WDO) legt hiervoor de basis. Het betreft een zogenaamde kaderwet: de wet regelt algemene principes, verantwoordelijkheden en procedures maar bevat geen gedetailleerde regels. Deze regels komen in lagere regelgeving.

In 2018 is de eerste tranche ingediend van de WDO bij de Tweede Kamer.[51] Dit wetsvoorstel bevat de meest urgente onderwerpen van regelgeving, waaronder de codificatie van de huidige taken en verantwoordelijkheden van de Minister BZK om de infrastructuur voor identificatie en authenticatie in het publieke domein te doen functioneren.[52] Zo is de Minister verantwoordelijk voor de beschikbaarheid van publieke identificatiemiddelen voor burgers op een voldoende hoog betrouwbaarheidsniveau (substantieel en hoog).[53] Deze wijst de Minister aan als toegelaten identificatiemiddelen.[54] Hierbij wordt de classificatie van de betrouwbaarheidsniveaus en de regels waaraan deze middelen moeten voldoen gevolgd uit de eIDAS-verordening. Dienstverleners (bestuursorganen en aangewezen organisaties) zijn dan ook verplicht om bij hun digitale dienstverlening uitsluitend de toegelaten identificatiemiddelen te gebruiken. Afhankelijk van de dienstverlening geldt een verplichting om daarbij het betrouwbaarheids-niveau 'substantieel' dan wel 'hoog' te hanteren.[55] Deze verplichting borgt dat de wijze van inloggen is toegesneden op de vertrouwelijkheid van de gegevens die worden uitgewisseld met de overheid.[56]

Tot slot is expliciet bepaald dat de WDO is bedoeld voor het gebruik van publieke identificatiemiddelen in het publieke domein.[57] Uitgangspunt is dat publieke identificatiemiddelen niet buiten het (semi)publieke domein worden gebruikt.[58]

De invoering van de WDO is vertraagd. Na vragen van de Eerste Kamer is een verbetering van het wetsvoorstel ingediend (novelle). Behandeling van de novelle door de Tweede Kamer is vooralsnog begin april 2022 gepland. De door de Europese Commissie voorgestelde herziening van de eIDAS-verordening zal ook gevolgen hebben voor (de tweede tranche van) de WDO.

---

[49] Artikel 4.16a Wet BRP. Een voorbeeld is het kunnen verstrekken van informatie in plaats van BRP-gegevens, zoals leeftijd in plaats van geboortedatum.

[50] Bijlage bij *Kamerstukken II* 2017/18, 34700, nr. 34, p. 7.

[51] Kamerstukken II 2017/18, 34972, nr. 2.

[52] De overige onderwerpen uit het wetsvoorstel worden in dit onderzoeksrapport buiten beschouwing gelaten. Noemenswaardig in deze is dat het Besluit verwerking persoonsgegevens GDI en het Besluit digitale toegankelijkheid overheid een grondslag krijgen in de WDO (artikel 28).

[53] Artikel 5 lid 1 sub a WDO.

[54] Artikel 9 WDO. In dit artikel wordt tevens de mogelijkheid geboden om één of meerdere door private partijen uitgegeven identificatiemiddelen naast de toegelaten middelen te laten fungeren als gelijkwaardige elektronische toegangsvoorziening bij dienstverlening van de overheid (lid 2).

[55] Artikel 6 & 7 WDO.

[56] Kamerstukken II 2017/18, 34972, nr. 3, p. 13.

[57] Artikel 8 WDO.

[58] Kamerstukken II 2017/18, 34972, nr. 3, p. 20.

6.2.6 *Wet op de Identificatieplicht*

In de Wet op de Identificatieplicht (hierna: WID) zijn de documenten aangewezen waarmee de identiteit van personen kan worden vastgesteld. Aangewezen zijn onder meer de documenten uit de Paspoortwet[59], maar ook het rijbewijs.[60] In de WID is ook de algemene identificatieplicht geregeld: eenieder die de leeftijd van veertien jaar heeft bereikt is verplicht om op de eerste vordering een geldig identiteitsbewijs te tonen aan bepaalde ambtenaren, militairen of toezichthouders.[61] Een identiteitsbewijs als genoemd in de WID bevat in elk geval de achternaam, voornamen, geboortedatum en geslacht, een foto, het BSN (indien dat is toegekend) en verder de gegevens die nodig zijn voor het doel waarvoor het bewijs is uitgegeven.

Naast de algemene identificatieplicht zijn in een groot aantal specifieke wetten identificatie- en controleplichten opgenomen waarin – voor het voldoen aan die verplichting - wordt verwezen naar een of meer documenten aangewezen in de WID.[62] Zo staat in de Alcoholwet dat het verboden is om alcoholhoudende drank te verstrekken aan een persoon van wie niet is vastgesteld dat deze de leeftijd van 18 jaar heeft bereikt en dat de vaststelling van de leeftijd geschiedt aan de hand van een document uit de WID.[63] De WID en de verschillende wetten waarin identificatieplichten zijn opgenomen gaan uit van identiteitsbewijzen ten behoeve van de fysieke controle van de identiteit.[64]

Het is goed om te benadrukken dat iemand niet verplicht is om buiten de bij wet geregelde gevallen een identiteitsbewijs te tonen. Laat staan dat hiervan een kopie mag worden gemaakt. De Autoriteit Persoonsgegevens staat dan ook op het standpunt dat wanneer het tonen van een identiteitsdocument volstaat, zoals bij een leeftijdscontrole, het overnemen van gegevens van het identiteitsdocument of het kopiëren, scannen of uitlezen ervan niet is toegestaan.[65]

Zo kan bijvoorbeeld ook niet als voorwaarde gelden voor een lidmaatschap van een krant of het bestellen van een pakket bij bol.com dat hiervoor een geldig (digitaal) identiteitsdocument noodzakelijk is. Die noodzaak ontbreekt.[66]

Naast de specifieke wetten waarin specifiek wordt verwezen naar de documenten aangewezen in de WID, zijn er overigens nog andere wetten die verplichten tot identificatie. Op grond van de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft) hebben banken bijvoorbeeld bijzondere verplichtingen om de identiteit van hun klanten vast te stellen. Tegenwoordig doen sommige banken dit ook online via een app.

6.2.7 *Paspoortwet*

De Paspoortwet is een rijkswet en regelt welke documenten kwalificeren als reisdocument of identiteitskaart en hoe deze als zodanig kunnen worden aangevraagd en uitgegeven. Daarbij beschrijft de Paspoortwet telkens welke (persoons)gegevens de documenten vermelden en bevatten.

---

[59] Artikel 1 lid 1 sub 1 WID: geldige reisdocumenten behalve een nooddocument en de Nederlandse Identiteitskaart. Zie hierna paragraaf 7.1.1.4.

[60] Artikel 1 lid 1 sub 4 WID.

[61] Artikel 2 WID.

[62] Zie voor een opsomming van die wetten: wetten.nl - Informatie - Wet op de identificatieplicht - BWBR0006297 (overheid.nl).

[63] Artikel 20 Alcoholwet.

[64] Weliswaar bevat de Alcoholwet ook een bepaling voor verkoop op afstand met behulp van een leeftijdsverificatiesysteem (artikel 20a), dan nog moet bij aflevering van de alcohol aan het adres nog een keer een leeftijdsverificatie geschieden aan de hand van een geldig identificatiebewijs.

[65] Richtsnoeren identificatie en verificatie persoonsgegevens, CBP, 2012: rs_kopie-identiteitsbewijs.pdf (autoriteitpersoonsgegevens.nl).

[66] Onlangs heeft de AP nog een boete opgelegd van 525.000 euro door onnodig een kopie van het identiteitsbewijs te eisen: AP: Boete DPG Media voor onnodig opvragen identiteitsbewijs | Autoriteit Persoonsgegevens.

Reisdocumenten zijn onder andere het nationaal paspoort, het diplomatiek paspoort en andere reisdocumenten voor niet-Nederlanders.[67] Hoewel de Nederlandse Identiteitskaart (hierna: NIK) niet (meer) de formele status heeft van een reisdocument[68], zijn de meeste bepalingen uit de Paspoortwet wel van overeenkomstige toepassing verklaard.[69]

Sinds 1 januari 2021 is in de Paspoortwet ook de mogelijkheid opgenomen om documenten aan te wijzen waarop een publiek identificatiemiddel wordt geplaatst.[70] Dit betreft een doorwerking van de WDO. Momenteel is alleen de NIK aangewezen als drager van het publiek identificatiemiddel[71], oftewel de e-NIK. Het geplaatste publiek identificatiemiddel (een applet op de daarop gebrachte chip) maakt het mogelijk om met de e-NIK in te loggen via DigiD op betrouwbaarheidsniveau Hoog. Hiermee vindt dus authenticatie van de identiteit van de houder van een fysiek document plaats in het elektronisch verkeer. De e-NIK is ook een document waarmee de identiteit fysiek kan worden vastgesteld conform de WID.

Op dit moment worden voorbereidingen getroffen om in de toekomst de identiteitskaart uit de Paspoortwet te halen en in een aparte wet op te nemen. De Paspoortwet is namelijk een Rijkswet waardoor wijzigingen die alleen Nederland aangaan tijdrovend zijn.

6.2.8 Wetboek van Strafrecht

Burgers moeten in het maatschappelijk verkeer erop kunnen vertrouwen dat bepaalde documenten juist zijn. De wetgever heeft misbruik daarom strafbaar gesteld. Naast een algemeen fraude-artikel (valsheid in geschrifte) zijn in het Wetboek van Strafrecht een aantal specifieke vormen van fraude met documenten strafbaar gesteld. De artikelen over valse reisdocumenten of identiteitskaarten (artikel 231), valse biometrische kenmerken (artikel 231a) en identiteitsfraude (artikel 231b) kunnen gebruikt worden voor fraude met identiteitsdocumenten, biometrie en identiteitsgegevens. Deze artikelen kunnen ook worden ingezet als het gaat om identiteitsfraude in een digitale omgeving.

6.3 Tussenconclusie

In het juridisch kader rondom identiteit kan steeds een onderscheid worden gemaakt tussen de fysieke en de digitale wereld. De WID gaat uit van de fysieke identiteitsvaststelling, terwijl de WDO is bedoeld voor de gevallen waarin de identiteit langs de elektronische weg wordt vastgesteld.

De regering heeft bij het opstellen van de WDO de keuze gemaakt om voor die gevallen geen elektronische identificatiemiddelen aan te wijzen in de WID, maar te zijner tijd de verschillende wetten waarin identificatieplichten zijn opgenomen te wijzigen. Deze systematiek biedt de mogelijkheid om per dienst te bepalen welk betrouwbaarheidsniveau voor de dienst is vereist en of voor authenticatie bepaalde attributen, zoals leeftijd, verstrekt moeten worden.[72]

De Paspoortwet fungeert vooralsnog als basis voor de documenten die zowel bij de fysieke (het paspoort en de e-NIK) als de digitale identiteitsvaststelling (de e-NIK) worden gebruikt.

[67] Artikel 2 lid 1 Paspoortwet.
[68] *Stb.* 2014, 10. De NIK is wel een document voor grensoverschrijding gebleven voor landen die behoren tot de Europese Unie, alsmede voor Andorra, Liechtenstein, Monaco, Noorwegen, San Marino, Turkije, IJsland en Zwitserland.
[69] Artikel 2 lid 2 Paspoortwet.
[70] Artikel 3a Paspoortwet.
[71] Artikel 1.6 Paspoortbesluit. Met inwerkingtreding van de WDO wordt ook het rijbewijs aangewezen.
[72] Kamerstukken II 2017/18, 34972, nr. 3, p. 43. Zie ook Kamerstukken II 2018-19, 34972, nr. 6, p. 28.

6.4 Juridische basis voor een DBI

Ingevolge de definitie van een DBI, zoals uiteengezet in de Visiebrief digitale identiteit en hoofdstuk 3, bevat de DBI een minimale set van identiteitsgegevens die een persoon nodig heeft om zichzelf in het digitale maatschappelijke verkeer te kunnen identificeren. Doordat deze set van gegevens, al dan niet in combinatie met biometrie en een link naar de basisregistratie, moet worden vastgesteld met een hoog betrouwbaarheidsniveau, vormt de DBI een gezaghebbende bron van persoonsidentificatiegegevens (unieke identiteitsregistratie) als onderdeel van de basis identiteit infrastructuur. Hierdoor kunnen toegelaten elektronische identificatiemiddelen (zoals de wallet) aansluiten op en gebruikmaken van de DBI.

Het zou voor de hand liggen om de DBI, gezien de hiervoor beschreven status, te verankeren in de (tweede tranche van de)[73] WDO. De WDO beperkt zich vooralsnog tot het publieke domein. De regering stond destijds op het standpunt dat het niet tot de taak van de rijksoverheid behoort om publieke middelen te ontwikkelen en uit te geven die ook voor strikt commerciële transacties als het online kopen van kleding gebruikt kunnen worden.[74] De visiebrief voor digitale identiteit, de (concept) wijzigingen van de eIDAS-verordening, maar bijvoorbeeld ook Regie op Gegevens leggen daarentegen ook nadruk op het gebruik in de private sector. Op beleidsniveau moet worden bezien hoe het gebruik van de DBI in de private sector kan worden bewerkstelligd. Dit geldt ook voor het uitgangspunt dat personen die een relatie hebben met de Nederlands overheid recht hebben op één digitale (bron)identiteit.[75]

Op dit moment is het onduidelijk hoe de gewijzigde eIDAS-verordening er precies uit gaat zien. Hoe de WDO gewijzigd en aangevuld zou moeten worden is dan ook op dit moment niet aan te geven. Als er een wens is om de DBI ook in de fysieke wereld te kunnen gebruiken, zou de wallet (die gebruikt maakt van de DBI) moeten worden aangewezen in de WID als document waarmee de identiteit van personen kan worden vastgesteld bij een fysieke controle.

Gezien het feit dat het veld nog zeer in beweging is, is het lastig om een tijdslijn te schetsen voor de benodigde wetswijzigingen. Een deel zou meegenomen kunnen worden in de tweede tranche WDO, maar een en ander is mede afhankelijk van het tijdspad van de Conceptverordening eIDAS.

Het is moeilijk te voorspellen hoelang het Europese wetgevingsproces zal duren. Wanneer we ervan uitgaan dat de Verordening medio 2023 van kracht wordt, zou dit betekenen dat iedere Lidstaat medio 2024 in ieder geval één Europese Identity Wallet heeft aangewezen.

Een Verordening hoeft doorgaans niet naar nationaal recht omgezet te worden en heeft rechtstreekse werking. Het voorstel tot wijziging van de eIDAS verordening heeft mogelijk wel gevolgen voor het huidige wetsvoorstel WDO (de eerste tranche WDO). Aanvulling van de WDO met een tweede tranche en de Wet Nederlandse ID-kaart/Wet ontvlechting Paspoortwet zijn wenselijk in verband met het faciliteren van de Europese digitale wallet. Het wetgevingsproces wordt idealiter afgestemd op het verwachte Europese tempo.

[73] Vooruitblik op tweede tranche Wet digitale overheid Wet digitale overheid - Digitale Overheid.

[74] Kamerstukken II 2017/18, 34972, nr. 3, p. 20.

[75] Overigens krijgen burgers met de inwerkingtreding van de Wet modernisering elektronisch bestuurlijk verkeer het recht op elektronisch zakendoen met de overheid. Het recht op een digitale identiteit is een uitwerking van het amendement Middendorp/Verhoeven op de WDO (Kamerstukken II 2019/20, 34972, nr. 20.

6.5 Ethische analyse van de digitale bronidentiteit

Een onderdeel bij het beantwoorden van onderzoeksvraag drie is het verkrijgen van inzicht in de ethische effecten van de DBI. Dit onderdeel is van belang omdat dat wat technisch en wettelijk mogelijk is, niet altijd wenselijk is in het licht van publieke waarden. Publieke waarden beschrijven wat wij als samenleving waardevol vinden.[76] Soms kunnen publieke waarden met elkaar botsen. Deze ethische analyse beperkt zich tot het in beeld brengen van de publieke waarden die bij een DBI zijn gemoeid. In een later stadium zal het principe van ethics by design moeten worden toegepast, waarbij de publieke waarden met elkaar worden afgewogen en concrete oplossingen worden aangedragen.

6.5.1 *Privacy*

Een DBI maakt het mogelijk dat een burger alleen de persoonsgegevens deelt die nodig zijn voor een bepaalde transactie of het afnemen van een dienst. Dit versterkt het recht op gegevensbescherming van de burger en vermindert het 'datagraaien' door organisaties.

De invoering van een DBI zorgt ook voor een exponentiele toename van de verwerking van persoonsgegevens door een verscheidenheid aan verwerkingsverantwoordelijken. Dit is een paradox: om als burger je gegevens beter te kunnen beschermen, worden er meer gegevens verwerkt. Al deze gegevensverwerkingen maken het mogelijk om de bewegingen van de burger in het dagelijks leven op grote schaal vast te leggen. Kortom, een digitale versie van de identiteit van de burger maakt surveillance beter mogelijk dan bij een fysieke versie.[77]

Tot slot bestaat er een zeker gevaar dat de DBI op een andere manier zal worden gebruikt dan oorspronkelijk bedoeld. Dit fenomeen heet function creep. Het is denkbaar dat bijvoorbeeld de politie de vastgelegde informatie later wil gebruiken voor opsporingsdoeleinden. Andere doeleinden waarvoor het gebruik van vastgelegde en verzamelde data later juridisch kan worden gerechtvaardigd zijn bijvoorbeeld de nationale of openbare veiligheid.

6.5.2 *Veiligheid*

De digitalisering van de samenleving heeft ertoe geleid dat criminaliteit steeds meer online plaatsvindt (cybercriminaliteit). Eén van die veel voorkomende delicten is identiteitsfraude. Het gebruik van een DBI kan identiteitsfraude voorkomen: doordat je met een DBI met een hogere mate van zekerheid weet dat diegene waarmee je online zakendoet ook echt diegene is die hij/zij zegt te zijn, wordt het lastiger om identiteitsfraude te plegen.

De invoering van een DBI brengt daarentegen weer nieuwe risico's op kwetsbaarheden en fraude met zich mee. De gegevensverwerkingen die met een DBI zijn gemoeid brengen zeer waardevolle informatie op, waardoor een DBI doelwit kan zijn van criminaliteit. Ook de informatieveiligheid is gezien het aantal datastromen zeer complex en een inbreuk daarop heeft niet alleen een grote impact op de individuele burgers, maar ook op de maatschappelijk in zijn geheel.

---

[76] Overlegorgaan Fysieke Leefomgeving, *Rapport ethiek en digitalisering. Bezint eer ge begint*, p. 9. Zie ook Ratheneu Instituut, *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*, 2014 & de Toolbox Ethisch Verantwoorde Innovatie. Voor een diepere analyse van het perspectief vanuit de burger, zie hoofdstuk 8.

[77] Pseudonomisering zou daar eventueel uitkomst voor kunnen bieden.

6.5.3 Autonomie

Met een DBI kunnen burgers zelf bepalen met wie en welke gegevens zij willen delen. De burger krijgt daarmee in zekere zin de regie ofwel controle over diens eigen persoonsgegevens.

Belangrijk is daarbij wel dat burgers de keuzevrijheid behouden om een transactie of dienst ook offline af te handelen en dat het gebruik van een DBI niet verplicht wordt. Hoewel een DBI burgers bewuster maakt van de gegevens die over hen worden verwerkt[78], zou een verplichting voor het gebruik daarvan alsnog de autonomie aantasten.

Ook introduceert de DBI een risico op 'overidentificatie': organisaties kunnen afdwingen dat je jezelf kenbaar maakt met je digitale identiteit. De mogelijkheid om in anonimiteit te kunnen 'internetten' (daar waar identificatie niet noodzakelijk of verplicht is) moet dus gewaarborgd blijven.

Een ander aspect is digitale autonomie. Nederland en Europa zijn in zekere zin op verschillende manieren afhankelijk van de commerciële en machtige techindustrie.

6.5.4 Controle over technologie

Autonomie gaat gepaard met verantwoordelijkheid. Vragen die hierbij spelen zijn:
- Welke verantwoordelijkheid de burger krijgt bij het gebruik van een DBI;
- In hoeverre de burger in staat is om zelf te bepalen welke gegevens nodig zijn voor een bepaald doel; en
- Wie verantwoordelijk is als er iets misgaat.

Daarbij is het noemenswaardig dat er verschillende toezichthouders (Agentschap Telecom, AP, ACM etc.) verantwoordelijk zijn. Dat heeft een versnipperd toezicht als gevolg.[79] Niet alle toezichthouders hebben voldoende budget en capaciteit.

6.5.5 Inclusie

Iedereen moet mee kunnen doen in de (digitale) samenleving en de overheid wil voorkomen dat mensen worden buitengesloten. Voor de DBI heeft niet iedereen de benodigde apparatuur of kennis. Mensen met een handicap hebben hulpmiddelen nodig om gelijkwaardigheid te bereiken. In hoofdstuk 8 is een verdieping ten aanzien van het gebruik van een DBI door inclusiedoelgroepen opgenomen.

6.5.6 Menselijke waardigheid

- Dehumanisatie: een digitale identiteit is een administratief/juridisch beeld en representeert niet de fysieke persoon. Het volledige en unieke zijn van de mens is niet in gegevens te vatten.
- De digitale werkelijkheid is vaak een versimpeling en daarmee niet altijd hetzelfde als de 'fysieke werkelijkheid'. Wat zijn de gevolgen als de inhoud van een DBI niet klopt? Hoe moeilijk is het om fouten recht te zetten in de dataketen?

[78] Door middel van adversarial design zou je de gebruiker kunnen dwingen kritischer na te denken over de gegevens die hij/zij deelt.

[79] Verschillende toezichthouders hebben wel reeds aangekondigd de samenwerking op te zoeken: Nederlandse toezichthouders versterken toezicht op digitale activiteiten door meer samenwerking | Autoriteit Persoonsgegevens.

6.5.7 *Vertrouwen*

- De burger wil het DBI-systeem kunnen vertrouwen. De inhoud moet correct, juist en veilig zijn.
- Vertrouwen werkt online anders dan offline.[80] Een DBI bouwt aan vertrouwen in de digitale wereld.

6.5.8 *Economie*

Vertrouwen in de digitale wereld en daarmee het vertrouwen om digitaal zaken te doen, bevordert economische ontwikkeling.

6.5.9 *Gemak*

DBI bevordert het gemak bij maatschappelijke processen.

6.5.10 *Transparantie*

Met een DBI wordt voor burgers duidelijker welke gegevens echt nodig zijn om te verwerken voor een bepaalde transactie en/of dienst en welke gegevens over hen worden verwerkt.

[80] J. Spierings & T. Demeyer, Digitale Identiteit: een nieuwe balans, Waag 2019, p. 17-18.

7 Hoe verhoudt de digitale bronidentiteit zich tot bestaande voorzieningen?

De digitale bronidentiteit is een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde digitale identiteit voor gebruik in de publieke en private sector. De DBI zal in het maatschappelijk digitaal verkeer samen met een wallet worden gebruikt.

De DBI en de wallet kunnen alleen betrouwbaar, veilig en efficiënt worden gebruikt wanneer een goed werkend identiteitsecosysteem ingericht is. In dit identiteitsecosysteem bestaan naast de DBI en de wallet ook andere (digitale) voorzieningen. Deze voorzieningen hebben in meer of mindere mate raakvlakken met de DBI en de wallet (zie hoofdstuk 5).

Dit hoofdstuk beschrijft de voorzieningen die, voor zover nu kan worden ingeschat, de grootste raakvlakken kunnen hebben met de DBI. Per voorziening zijn de functionaliteiten en de gebruikers beschreven. Ook is aandacht besteed aan welke functionaliteit(en) van de voorziening DBI zou kunnen (her-) gebruiken en vice versa.

Het programma Regie op Gegevens is ook relevant voor DBI. Burgers moeten data kunnen gebruiken om hun leven, werk of bedrijf te organiseren. Daar staat tegenover dat belangrijke waarden zoals veiligheid en privacy geborgd zijn. Regie op Gegevens is een programma dat uiteindelijk leidt tot een, sectoroverstijgend kader voor veilige, betrouwbare en gebruiksvriendelijke digitale uitwisseling van gegevens. De interactiepatronen van Regie op Gegevens zijn beschreven in hoofdstuk 5.

7.1 NIK

De functie

In Nederland is iedereen van 14 jaar en ouder op basis van de Wet op de Identificatieplicht verplicht zich te kunnen identificeren. De Nederlandse ID-kaart, de NIK, is een van de toegestane identificatiemiddelen.[81]

Ook kan de houder zijn NIK gebruiken om binnen de EER, Monaco, Montenegro, San Marino, Servië, Turkije en Zwitserland grenzen te passeren.

De NIK is voorzien van een chip waarop biometrische en biografische gegevens staan van de houder. Deze gegevens kunnen elektronisch worden uitgelezen.

Sinds 4 januari 2021 kan de NIK met inlogfunctie worden aangevraagd (de zogenaamde e-functionaliteit). Na inwerkingtreding van de Wet Digitale Overheid (WDO) tranche 1 kan een houder, met met deze identiteitskaart via de DigiD app op betrouwbaarheidssniveau 'Hoog' inloggen bij de Nederlandse overheid, het onderwijs, de zorg of pensioenfonds.

De gebruiker

Iedere Nederlandse burger kan een NIK met inlogfunctionaliteit aanvragen.

Mogelijk hergebruik

Van welke functionaliteiten kan de DBI mogelijk gebruik maken?

De functies van de NIK zijn identificeren en reizen binnen Europa. Deze functies kunnen in de toekomst mogelijk ook uitgevoerd worden op basis van een DBI en met aanvullende gegevens uit de bijbehorende wallet. Er zullen dan onder andere attesten en attributen in de wallet moeten komen. De NIK kan dan als een van de DBI afgeleid identiteitsmiddel worden beschouwd.

[81] https://www.rvig.nl/reisdocumenten/faq-wijzigingen-nederlandse-identiteitskaart/faq-nik-met-e-functionaliteit

Het fysieke document beschikt over een chip en een QR-code met persoonsgegevens. Die gegevens kunnen wellicht worden gebruikt ter beveiliging of autorisatie van het gebruik van de DBI. Ook wordt de NIK ingezet voor DigiD betrouwbaarheidsniveau substantieel en voor het verhogen van het betrouwbaarheidsniveau van de DigiD app naar hoog. Daarmee kan de NIK gebruikt worden om het plaats- en tijdsonafhankelijk aanvragen en activeren van een DBI te ondersteunen, zoals genoemd in hoofdstuk 5.

Wat is het effect van de realisatie van de DBI op de voorziening?

Als de DBI tot een digitale versie van de NIK leidt, zijn er mogelijk minder fysieke documenten nodig. De functie van de ID-middelen blijft onveranderd, alleen de verschijningsvorm is anders.

Daarnaast is er nog ruimte op de chips in de fysieke documenten over. Hier kunnen indien gewenst relevante gegevens over de DBI op worden geplaatst.

7.2 Paspoort

De functie

In Nederland is iedereen van 14 jaar en ouder op basis van de Wet op de Identificatieplicht verplicht zich te kunnen identificeren. Het paspoort is een van de toegestane identificatiemiddelen. Ook is het paspoort een reisdocument op grond van de Paspoortwet.

Het paspoort is voorzien van een chip. Op deze chip staan o.a. biometrische en biografische gegevens van de houder die elektronisch kunnen worden uitgelezen.

De gebruiker

Iedere Nederlandse burger kan een paspoort aanvragen.

Mogelijk hergebruik

Van welke functionaliteiten kan de DBI mogelijk gebruik maken?

Met het paspoort kan een houder zich identificeren en wereldwijd reizen. Deze functies kunnen in de toekomst mogelijk deels ook uitgevoerd worden op basis van een DBI en aanvullende gegevens in de bijbehorende wallet.

Het fysieke document beschikt over een chip en een QR-code met persoonsgegevens. Die gegevens kunnen worden gebruikt ter beveiliging of autorisatie van het gebruik van de DBI. Bijvoorbeeld in combinatie met DigiD, zoals benoemd bij het uitgifte proces. Het paspoort kan op dit moment worden ingezet om in te loggen in DigiD op betrouwbaarheidsniveau substantieel.

Voor aanvraag, uitgifte en gebruik van fysieke documenten is op dit moment geen rol voorzien voor DBI. Wel is het zo dat er nog ruimte is op de chip van de fysieke documenten. Hier kunnen eventueel gegevens over de DBI op worden geplaatst.

ICAO werkt momenteel specificaties van de Digital Travel Credentials (DTC) uit. Er zijn drie types onderscheiden[82]:

- DTC type 1: de houder van een fysiek paspoort leest de chip uit met een app op zijn mobiele telefoon. Vervolgens kan hij een DTC Virtual Component (DTC-VC) opsturen naar bijvoorbeeld grensautoriteiten. Een burger heeft naast de DTC-VC ook nog een fysiek paspoort nodig.
  - Deze variant is gebaseerd op een fysiek paspoort. DBI heeft dus geen impact hierop.
- DTC type 2: naast een DTC-VC is er nu ook een DTC Physical Component (DTC-PC). Die is cryptografisch gekoppeld aan de DTC-VC. Een burger heeft naast de DTC-VC en DTC-PC ook nog een fysiek paspoort nodig.
  - Deze variant is gebaseerd op een fysiek paspoort. DBI heeft dus geen impact hierop.

[82] Guiding Core Principes DTC - ICAO

- DTC type 3: deze variant bestaat alleen uit een DTC-VC en een DTC-PC. Er is gen fysiek paspoort meer.
  - Deze variant kan deels zijn gebaseerd op een DBI. Dit vraagt nog wel om nader onderzoek.

7.3 Rijbewijs

De functie

Met een geldig rijbewijs mag een houder een gemotoriseerd voertuig besturen. Binnen Nederland kan het rijbewijs vaak ook gebruikt worden als identificatiemiddel. Het rijbewijs is niet áltijd geschikt voor identificatie, omdat er geen gegevens over verblijfsstatus en nationaliteit op staan.[83] Daarnaast is het rijbewijs geschikt voor authenticatie.

Het rijbewijs is voorzien van een chip. Op deze chip staan o.a. biometrische en biografische gegevens die elektronisch kunnen worden uitgelezen. De chip in het rijbewijs heeft inlogfunctionaliteit voor DigID (de zogenaamde e-functionaliteit).

De inlogfunctionaliteit kan worden gebruikt zodra de Wet Digitale Overheid (WDO) tranche 1 in werking treedt.

De gebruiker

Burgers die in Nederland hun rijvaardigheid en -geschiktheid hebben aangetoond (tijdens het rij-examen) kunnen een rijbewijs aanvragen. Daarnaast kunnen Nederlandse burgers met een buitenlands rijbewijs dat omwisselen naar een Nederlands rijbewijs. Dit kan alleen als het buitenlands rijbewijs is afgegeven door een bevoegde buitenlandse instantie.[84]

Mogelijk hergebruik

Van welke functionaliteiten kan de DBI mogelijk gebruik maken?

Het fysieke document beschikt over een chip en een QR-code met persoonsgegevens. Deze gegevens kunnen worden gebruikt ter beveiliging of autorisatie voor gebruik van de DBI. Bijvoorbeeld in combinatie met DigiD, zoals benoemd bij het uitgifte proces. Het rijbewijs kan op dit moment worden ingezet om in te loggen in DigiD op betrouwbaarheidsniveau substantieel. Zodra de Wet Digitale Overheid in werking treedt, kan het rijbewijs ook worden gebruikt om in te loggen in DigiD op betrouwbaarheidsniveau hoog.

Met een rijbewijs kan iemand zijn rijbevoegdheid aantonen. In de toekomst kan een digita(a)l(e) (representatie van een) rijbewijs mogelijk deels worden gebaseerd op de DBI. En als de DBI tot een digitale versie van het rijbewijs leidt, worden mogelijk minder fysieke documenten uitgegeven.

7.4 DigiD

De functie

DigiD is een systeem waarmee een burger zich online kan authentiseren.[85] Dit kan bij dienstverleners die het Burgerservicenummer (BSN) mogen verwerken. Dit zijn bijvoorbeeld de overheid, het onderwijs en de zorg.

Na authenticatie levert DigiD het BSN aan de organisatie waarvoor de authenticatie is uitgevoerd. Met het BSN kunnen organisaties de juiste persoon identificeren binnen hun systemen.

[83] Met welke identiteitsbewijzen kan ik mij identificeren? | Rijksoverheid.nl
[84] https://www.rdw.nl/particulier/voertuigen/auto/het-rijbewijs/buitenlands-rijbewijs/buitenlands-rijbewijs-omwisselen
[85] DigiD | Wat is DigiD?

De gebruiker
Iedereen die is ingeschreven in het Basisregistratie Personen (BRP) kan een DigiD aanvragen.

Mogelijk hergebruik
DigiD kan mogelijk gebruikt worden voor het (plaats- en tijdonafhankelijk) aanvragen en uitgeven van een DBI of het koppelen van een DBI aan een wallet.

DigiD Hoog kan indien nodig ook worden gebruikt voor het openen van de wallet. Ook is het mogelijk dat een burger via een DigiD bepaalde gegevens in een wallet kan zetten. Een voorbeeld hiervan is het ophalen van test- en/of vaccinatiebewijzen uit de Coronacheck-app.

Hierboven is een aantal mogelijke scenario's beschreven waarbij DBI en DigID samen worden gebruikt. Als deze scenario's daadwerkelijk worden gerealiseerd, kan het gebruik van DigID toenemen.

7.5 DigiD machtigen

De functie
Met DigiD machtigen kan een burger zich laten vertegenwoordigen door iemand anders bij het regelen van zaken met de overheid.[86] Dit doet hij zonder zijn DigID af te geven. De burger die de machtiging afgeeft, bepaalt waarvoor en voor hoelang de machtiging geldig is.

De gebruiker
Er zijn twee soorten gebruikers:
- De burger die iemand anders machtigt namens hem zaken te regelen met de overheid; en
- De burger die namens een ander zaken regelt met de overheid (de gemachtigde).

Mogelijk hergebruik
Als een burger overheidsdiensten gaat afnemen via een wallet, bestaat nog steeds de behoefte om iemand anders te machtigen. Dat is niet anders dan in de huidige situatie zonder wallet.

Het is op dit moment lastig in te schatten wat het effect van DBI en een wallet is op de behoefte aan machtigingen.

7.6 Stelsel van Basisregistraties

De functie
Dit betreft het geheel van afspraken en voorzieningen voor het doelmatige en efficiënte beheer van een beperkt aantal gegevens, dat nodig is voor de uitvoering van overheidstaken. Die gegevens zijn vastgelegd in gegevensverzamelingen met een wettelijke basis: de basisregistraties.[87]

De voor DBI mogelijk relevante basisregistraties zijn[88]:
- De Basisregistratie Personen (BRP). Het bevat persoonsgegevens over alle ingezetenen van Nederland en over personen die niet in Nederland wonen – of hier slechts kort verblijven – maar die een relatie hebben met de Nederlandse overheid, de 'niet-ingezetenen'. De Basisregistratie Personen (BRP) is een samenvoeging van de Gemeentelijke Basisadministratie Personen (GBA) en de Registratie Niet-Ingezetenen (RNI).
- Het Handelsregister (HR). Dit is de basisregistratie van alle rechtspersonen en ondernemingen in Nederland.

[86] https://www.digid.nl/digid-aanvragen-activeren/machtigen/
[87] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/
[88] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/stelsel-van-basisregistraties/10-basisregistraties/

- De Basisregistratie Adressen en Gebouwen (BAG). Deze registratie bevat gegevens van alle adressen en gebouwen in Nederland, zoals bouwjaar, oppervlakte, gebruiksdoel en locatie op de kaart.
- De Basisregistratie Kadaster (BRK). De BRK bevat informatie over percelen, eigendom, hypotheken, beperkte rechten (zoals recht van erfpacht, opstal en vruchtgebruik) en leidingnetwerken. Daarnaast staan er kadastrale kaarten in met perceel, perceelnummer, oppervlakte, kadastrale grens en de grenzen van het rijk, de provincies en gemeenten.
- De Basisregistratie Voertuigen (BRV). Hierin staan gegevens van voertuigen, kentekenbewijzen en personen aan wie het kentekenbewijs is afgegeven.
- De Basisregistratie Inkomen (BRI). In deze registratie staat van ongeveer 13 miljoen burgers het verzamelinkomen of het belastbaar jaarloon. Overheidsorganisaties gebruiken de BRI om toeslagen, subsidies of uitkeringen te bepalen. Burgers kunnen hun geregistreerd inkomen raadplegen op MijnOverheid.
- De Basisregistratie WOZ (WOZ). Deze registratie bestaat naast het authentieke gegeven “vastgestelde waarde” (WOZ-waarde) uit de gegevens die nodig zijn om deze waarde aan zowel een onroerende zaak te relateren als aan een belanghebbende. Voor het relateren van de WOZ-waarde aan een onroerende zaak is er aan de ene kant de (van een BAG-adres afgeleide) aanduiding van een onroerende zaak en aan de andere kant de koppeling aan kadastrale percelen en/of adressen en aan BAG verblijfsobjecten, standplaatsen, ligplaatsen en/of panden. Verder wordt vastgelegd voor welke belanghebbende de WOZ-waarde van betekenis is. De NAW-gegevens van deze belanghebbende zijn vastgelegd mede door een relatie naar de BRP of het Handelsregister. Er zijn ook belanghebbenden die niet in één van deze registraties zijn vastgelegd.

Vanuit deze basisregistraties kunnen aanvullende gegevens en attestaties geleverd worden op basis van en in combinatie met (onderdelen van) een DBI.

De Basisregistraties Topografie, Grootschalige Topografie en Ondergrond hebben betrekking op de fysieke leefomgeving en hebben hoogst-waarschijnlijk geen relatie met DBI.

De gebruiker

Alle gemeenten, provincies, waterschappen, zelfstandige bestuursorganen en overige organisaties met een publieke taak zijn verplicht gebruik te maken van de gegevens uit de basisregistraties.

Mogelijk hergebruik

De BRP is de authentieke bron voor gegevens uit de DBI. Deze gegevensset kan worden aangevuld met de gegevens uit de basisregistraties. Welke gegevens uit welke basisregistratie nodig zijn, is volledig afhankelijk van de digitale diensten die de burger kan afnemen via de wallet. Dat dient nader te worden onderzocht en uitgewerkt.

De DBI op zich heeft geen groot effect. Het gebruik van een DBI in combinatie met een wallet kan leiden tot meer bevragingen van basisregistraties. Dat is echter afhankelijk van de diensten die via de wallet worden aangeboden.

Er is al veel ervaring met het kunnen verstrekken van gegevens vanuit basisregistraties. Nieuw is dat er een extra leveringsvorm bij komt: rechtstreeks aan een burger (i.t.t. aan medeoverheden zoals nu). Vanuit de basisregistraties kunnen ‘kale’ gegevens worden geleverd aan de burger maar ook attestaties.

7.7 Mijn Overheid

De functie
MijnOverheid is het persoonlijke burgerportaal van de overheid.[89] Op MijnOverheid krijgt de burger toegang tot zijn gegevens bij verschillende overheidsregisters, zoals de BRP, het Diploma-register en voertuiggegevens. Daarnaast hebben burgers via MijnOverheid toegang tot de Berichtenbox.

Ter aanvulling op MijnOverheid, is de MijnGegevens-app ontwikkeld waarin alle gegevens van MijnOverheid kunnen worden geraadpleegd.

De gebruiker
Iedereen van 14 jaar en ouder die over een BSN beschikt en een DigID-account heeft, kan gebruikmaken van MijnOverheid.

Mogelijk hergebruik
De gegevens die in MijnOverheid staan zouden ook in de wallet van de DBI kunnen worden opgeslagen. Mogelijk kan hergebruik worden gemaakt van de voorzieningen die MijnOverheid gebruikt voor het beschikbaar stellen van gegevens die vanuit het BSN gekoppeld zijn/worden.

Realisatie van de DBI heeft geen direct effect op MijnOverheid. Het is denkbaar dat MijnOverheid in de toekomst attesten kan uitgeven, maar dat is nu niet het geval.

De volgende paragrafen geven een schets van (mogelijke) toekomstige voorzieningen.

7.8 Wallet

De functie
Zie hoofdstuk 4 voor een toelichting bij de wallet.

De gebruiker
Burgers met een EU-nationaliteit of EU-ingezetenen met een niet EU-nationaliteit. Natuurlijke personen kunnen daarbij handelen namens een organisatie.

Mogelijk hergebruik
Het is randvoorwaardelijk om een wallet te hebben om gebruik te kunnen maken van de DBI. Immers, zonder een wallet kan een burger wellicht wel een DBI hebben, maar kan hij die niet gebruiken. De wallet is namelijk het middel dat de burger gebruikt om zich te kunnen identificeren, authentiseren en om attributen en attestaties te delen.

In de conceptverordening eIDAS is het concept van de ‘Europese portemonnee voor digitale identiteit’ geïntroduceerd.

Deze wallet kan worden gevuld met identiteitsgegevens. De DBI kan daarvan (deels) de invulling zijn.

Een aantal mogelijke wallets wordt hieronder toegelicht. Het overzicht is niet uitputtend
- Europese referentie-wallet. De Europese Commissie laat een referentie-wallet ontwikkelen. Deze zal logischerwijs voldoen aan de vereisten uit de Conceptverordening. Een ander voordeel is dat als de EU deze laat maken, de Nederlandse overheid dat dus niet per se hoeft te doen. Verder is het lastig om hierover iets te zeggen zonder meer informatie over de referentie-wallet.

[89] Wat is MijnOverheid - ik ben nieuw | MijnOverheid

- Datakeeper.[90] Deze wallet is een initiatief van de Rabobank. Het is een wallet die op een mobiele telefoon of op een tablet kan worden geïnstalleerd. Het doel van Datakeeper is de gebruiker de regie op zijn gegevens (terug) te geven. Alleen de gebruiker van de Datakeeper wallet bepaalt welke gegevens hij deelt met derden. Eerst dient de gebruiker een identiteitsbewijs te scannen waarna de persoons- en documentgegevens worden opgeslagen in de wallet. Vervolgens scant de gebruiker een QR-code op bijvoorbeeld de website van een vertrouwende partij. Daarna ziet de gebruiker in de wallet welke gegevens de vertrouwende partij nodig heeft om een dienst te kunnen leveren. Op basis daarvan bepaalt de gebruiker of hij de gevraagde gegevens wil delen of niet. Datakeeper geeft aan te voldoen aan de vereisten uit de conceptverordening, maar geeft geen onderbouwing. Zie de website van Datakeeper voor een overzicht van vertrouwende partijen die gebruikmaken van Datakeeper.
- IRMA.[91] IRMA staat voor I Reveal My Attributes. Deze app is beschikbaar voor mobiele telefoon en tablet. Attributen kunnen - in de vorm van credentials - op verschillende manieren worden toegevoegd. Zo kunnen bepaalde persoonsgegevens rechtstreeks uit de BRP worden gehaald (na inloggen met DigiD). Het IBAN-bankrekeningnummer kan via iDEAL worden opgehaald. Andere gegevens kunnen worden ingeladen door een QR-code te scannen. Credentials zijn cryptografisch gekoppeld aan het apparaat van de gebruiker. Met deze app kan de gebruiker selectief persoonsgegevens delen met vertrouwende partijen. Sommige persoonsgegevens kunnen worden geanonimiseerd. IRMA-attributen zijn voorzien van een digitale handtekening van de (gekwalificeerde) verlener van vertrouwensdiensten. De vertrouwende partij kan via cryptografische berekeningen controleren of een attribuut echt is, niet verlopen, niet gemanipuleerd, uitgegeven is door een specifieke uitgever, en ook of het echt bij de gebruiker hoort (of eigenlijk: bij de telefoon van de gebruiker). Binnen de IRMA-methodiek wordt een betrouwbaarheidsniveau toegekend aan credentials en niet aan de app zelf. De IRMA app is open source. Zie de website van IRMA voor een overzicht van vertrouwende partijen die gebruik maken van IRMA.
- Itsme.[92] Dit is een Belgische identiteitsapp. Met de itsme app kan een gebruiker veilig inloggen op uiteenlopende websites. Ook kan een gebruiker met itsme selectief gegevens delen, transacties bevestigen en documenten ondertekenen. Voor dat mogelijk is, dient de gebruiker een account aan te maken op de website van itsme. Daartoe dient ook een plug-in te worden geïnstalleerd. Ook moet de gebruiker een kaartlezer aansluiten op zijn PC/laptop. Die is nodig om de ID-kaart te kunnen lezen tijdens het registratieproces. Daarna dient de gebruiker de itmse app te activeren. Itsme is geregistreerd op eIDAS betrouwbaarheids-niveau 'Hoog' en gaat door de gemeente Rotterdam worden gebruikt.

7.9 Self Sovereign Identity (SSI)

De functie

SSI staat voor Self Sovereign Identity. De essentie van SSI is dat een burger zelf de regie heeft op het delen van gegevens van zichzelf. Er hoeft immers niet meer informatie te worden gedeeld dan strikt noodzakelijk.

Voor een dienstverlener de gegevens ontvangt, dient er een hoge mate van betrouwbaarheid te zijn dat het inderdaad gegevens betreft van die specifieke burger.

In Europees verband wordt gewerkt aan een methode, inclusief onderliggende infrastructuur, die SSI mogelijk maakt.

Om SSI mogelijk te maken worden de volgende onderdelen uitgewerkt:
- Een wallet die met een hoge mate van betrouwbaarheid aan de burger gekoppeld is;
- Verifieerbare attesten die bijvoorbeeld identiteitsgegevens kunnen bevatten;
- Ondersteunende systemen voor het aantonen van de geldigheid van gegevens.

[90] https://datakeeper.nl/
[91] https://irma.app/
[92] https://www.itsme-id.com/nl-BE

De gebruiker

SSI kent een meerdere soorten gebruikers:

- De 'issuer' die een attestatie uitgeeft (de uitgever);
- De 'verifier' de een attestatie ontvangt controleert (de afnemer);
- Het'subject' waarop een attestatie betrekking heeft (de gebruiker).
  - Veelal valt deze rol samen met die van de 'holder' (de houder). Deze vraagt een attestatie aan bij de uitgever en verstuurt de attestatie naar de afnemer. De houder kan echter ook een gemachtigde zijn die namens de gebruiker handelt.

Mogelijk hergebruik

De kern van SSI is dat er een hoge mate van vertrouwen is dat een bepaald attest ook echt klopt en dat het ook echt hoort bij de persoon die het attest deelt. Hiertoe is het nodig dat de wallet die een burger gebruikt, met een hoge betrouwbaarheid wordt gekoppeld aan een persoon. De DBI kan het middel zijn om dit te doen. Daarnaast kan de DBI mogelijk gebruikt worden om betrouwbare persoonsgegevens in de wallet te ontsluiten, welke mogelijk als attest gebruikt kunnen worden.

Andersom kan de DBI gebruikmaken van de Europese SSI-ontwikkelingen. Immers, daar wordt nu gewerkt om een infrastructuur mogelijk te maken om het werken volgens de SSI-gedachte mogelijk te maken. Dit is in grote mate vergelijkbaar met het identiteitsecosysteem zoals in hoofdstuk 5 is beschreven. Bijkomend voordeel van het Europese SSI-traject is dat aangesloten wordt bij bepaalde standaarden opdat ook binnen Europa grensoverschrijdende diensten mogelijk worden.

De DBI maakt het mogelijk om een wallet op een hoog betrouwbaarheidsniveau te koppelen aan een persoon. Daarnaast kan de DBI mogelijk een basis zijn voor de identiteitsgegevens.

8 Prototype DBI

8.1 Introductie

Dit hoofdstuk beschrijft het ontwerp van de digitale bronidentiteit (DBI) en de (NL) wallet en de bijbehorende toegankelijke en gebruiksvriendelijke processen vanuit het perspectief van de gebruiker: de burger.

Het is nadrukkelijk niet de bedoeling om een volledige beschrijving te geven, maar om een overzicht te creëren waarin de belangrijkste *inrichtingskeuzen* in beeld zijn gebracht en een schets en visualisatie te geven over hoe het ontwerp er in de toekomst zou kunnen uitzien. Deze visualisaties betreffen de klantreizen welke afzonderlijk zijn gepubliceerd en het klikbaar prototype.[93] Belangrijk is om te realiseren dat het ontwerp 'werk in uitvoering' is.

Daarnaast is beschreven hoe de burger tegen een digitale bronidentiteit aankijkt. Daarbij is het perspectief van de inclusie doelgroepen meegenomen. Het ethisch perspectief op een aantal aspecten is in hoofdstuk 6 opgenomen.

8.2 Houding naar en gebruik van een DBI

Voordat ingegaan wordt op het ontwerp, zijn de belangrijkste bevindingen beschreven over hoe de burger tegen een digitale bronidentiteit aankijkt.

In dit onderzoekstraject naar een digitale bronidentiteit zijn twee kwalitatieve onderzoeken uitgevoerd:
- Gebruikersonderzoek digitale bronidentiteit vanuit burgerperspectief (2) (Jungleminds, 2021).[94]
- De attitude naar en het gebruik van een digitale bronidentiteit onder inclusie doelgroepen (Ruigrok Netpanel, 2022).[95]

In deze analyse wordt gesproken over "Nederlandse burger" wanneer de bevindingen in de onderzoeken met als doelgroep "gemiddelde" Nederlander[96] zijn benoemd en over "inclusie doelgroepen" wanneer de bevindingen in onderzoeken die zich richten op inclusie doelgroepen[97] zijn benoemd.

8.2.1 Concept digitaal identificeren

De houding van de Nederlandse burger ten aanzien van een digitale bronidentiteit is verdeeld. Een deel van de Nederlandse burgers is vooral nieuwsgierig en ervaart het als vernieuwend, handig en efficiënt. Zij zien ook wel in dat de overheid met de tijd mee moet gaan en zien een digitale bronidentiteit als laagdrempelig digitaal alternatief voor al bekende functies. Een ander deel uit vooral wantrouwen en ongerustheid. Het gevoel van veiligheid rondom een digitale bronidentiteit speelt hierbij een belangrijke rol. Het verschil in houding wordt ook teruggezien in de gebruiksintentie. Nederlandse burgers die positief reageren zijn meer bereid om een digitale bronidentiteit te gebruiken dan Nederlandse burgers die negatief reageren.

---

[93] Model met enkele QR-code, Model met multiple QR-code

[94] Gebruikersonderzoek digitale bronidentiteit vanuit burgerperspectief | Rapport | Rijksoverheid.nl

[95] Samen met dit rapport gepubliceerd.

[96] Personen die in Nederland woonachtig zijn.

[97] Inclusie doelgroepen: visueel beperkten, motorisch beperkten, auditief beperkten, licht verstandelijk beperkten, laaggeletterden, ouderen (vanaf 65 jaar), migratieachtergrond, minder digitaal vaardig. In de selectie is rekening gehouden met een spreiding in leeftijd en geslacht en sommige groepen opleidingsniveau.

De eerste indruk van een digitale bronidentiteit is bij de inclusie doelgroepen overwegend positief. Ook hier is een deel nieuwsgierig en voelt het andere deel ongerustheid. De digitale bronidentiteit wordt ook gezien als vernieuwend en handig. Evenals bij de Nederlandse burger speelt het gevoel van veiligheid rondom de digitale bronidentiteit een grote rol. Deze houding is ook terug te zien bij de gebruiksintentie: meer dan de helft van de totale inclusie doelgroepen die deelnamen aan het onderzoek heeft de intentie de digitale bronidentiteit te gebruiken. Hierbij heeft vanzelfsprekend het bezit van een mobiele telefoon ook veel effect.

Daarnaast zijn inclusie doelgroepen niet verrast als zij over het concept van digitaal identificeren horen. Zij vinden dat het concept meegaat met de tijd en past bij de digitalisering van dagelijkse zaken zoals hun overheids- of bankzaken:

- *Digitale omgevingen zoals 'Mijn Overheid' en online bankieren worden al veelvuldig gebruikt.*
- *In een omgeving zoals 'Mijn Overheid' wordt al een zekere mate van veiligheid ervaren. Dit gevoel komt onder andere doordat men erop vertrouwt dat de overheid zorgvuldig met hun gegevens omgaat.*
- *In omgevingen zoals het online bankieren heeft het gebruikersgemak de overhand genomen, waardoor de zorgen rondom veiligheid naar de achtergrond verdwijnen.*

8.2.2 Redenen om een digitale bronidentiteit te willen gebruiken

Belangrijke redenen om een digitale bronidentiteit en (NL) wallet te gebruiken zijn:

1. **Gemak, altijd bij je**: het niet mee hoeven nemen van het fysieke paspoort wordt als groot voordeel gezien. Met een digitale bronidentiteit heeft de gebruiker altijd een digitaal identiteitsbewijs bij de hand, omdat de meeste burgers altijd een mobiele telefoon bij zich hebben. Dit geldt zowel voor de Nederlandse burger als de inclusie doelgroepen.
2. **Gemak, opslag van andere documenten**: sommige burgers geven aan dat ze het handig vinden om naast het identificeren ook de (NL) wallet te gebruiken om al hun documenten en gegevens bij elkaar te houden. Voor hen brengt het een meerwaarde om naast identificeren ook een (NL) wallet te kunnen gebruiken voor andere functies. Zij zien de (NL) wallet meer als een soort stocard waar verschillende documenten in toegevoegd kunnen worden.
3. **Selectief vrijgeven van persoonsgegevens**: dit voordeel is niet gelijk duidelijk, maar wanneer deze begrepen wordt dan ziet zowel de Nederlandse burger als de inclusie doelgroep dit als voordeel t.o.v. het reguliere paspoort.
4. **Veiligheid**: over de visie op veiligheid zijn de meningen verdeeld. Een deel vermoedt dat een digitale bronidentiteit minder fraudegevoelig is dan het huidige paspoort.

Een deel van de Nederlandse burgers vermoedt namelijk dat een digitale bronidentiteit minder makkelijk te vervalsen is dan een fysiek paspoort. Het feit dat de overheid betrokken is bij de ontwikkeling van een digitale bronidentiteit verhoogt het vertrouwen op een correcte omgang met de persoonsgegevens. Daarnaast is veiligheid rondom dataopslag en uitwisseling relevant in de perceptie van veiligheid.

Zowel de Nederlandse burgers als inclusie doelgroepen geven aan dat een mobiele telefoon juist een veiliger gevoel geeft, aangezien niemand de gegevens kan zien zonder een verificatie. Een nadrukkelijke eigen regie bij de beveiliging van een digitale bronidentiteit en (NL) wallet is relevant in de perceptie van veiligheid: bijvoorbeeld met DigiD, een vingerafdruk, een persoonlijke code en/of twee-stapsverificatie.

Zo geven Nederlandse burgers aan dat wanneer de mobiele telefoon met daarop een digitale bron-identiteit en (NL) wallet wordt gestolen of kwijtraakt, de kans kleiner is dat hier misbruik van gemaakt wordt. De achterliggende gedachten hierbij zijn:

- De verificatie stap (vingerafdruk, gezichtsherkenning of pincode) die benodigd is om de (NL) wallet te openen zorgt ervoor dat er geen fraude mee gepleegd kan worden. Wanneer dit gebeurt met het reguliere paspoort kan dat wel.
- Bij verlies kan de (NL) wallet op afstand "uitgeschakeld" worden. Hiermee kan er gegarandeerd geen gebruik meer van gemaakt worden.

Dit wordt ondersteund door het onderzoek onder inclusie doelgroepen: twee-stapverificatie, pincode en/of gezichtsherkenning kunnen helpen om het veiligheidsgevoel te versterken.

8.2.3 Redenen om een digitale bronidentiteit niet te gebruiken

Belangrijke belemmeringen om een digitale bronidentiteit en (NL) wallet te gebruiken zijn:

1. **Veiligheid:** anderen zijn juist huiverig om persoonsgegevens te digitaliseren. Er is zorg dat de gedigitaliseerde persoonsgegevens die opgeslagen zijn in een database aantrekkelijk zijn voor cybercriminelen waardoor de angst heerst dat alle gegevens op straat komen te liggen.

   Nederlandse burgers zijn ook bang voor mogelijke hacks en identiteitsfraude bij het verlies van de mobiele telefoon. In tegenstelling tot een fysiek bewijs, dat veilig opgeborgen zit in de portemonnee of tas.

   Daarnaast is een digitale bronidentiteit en (NL) wallet voor sommigen juist wel fraudegevoeliger dan het fysieke paspoort. De digitale bronidentiteit is in hun ogen gemakkelijker te falsificeren ('Je hoeft alleen de juiste QR-code aan te maken en dan heb je iemands identiteit!').

   Bovengenoemde geldt voor de Nederlandse burger en de inclusie doelgroepen. De inclusie doelgroepen hebben als voornaamste redenen genoemd voor het nog niet of nog niet weten te gebruiken van een digitale bronidentiteit en (NL) wallet: de bezorgdheid rondom privacy en veiligheid.

   Er is wel opgemerkt dat het (succesvol) gebruik van een digitale bronidentiteit en (NI) wallet door mensen in hun directe omgeving de zorgen mogelijk verkleinen of wegnemen.
2. **Incomplete informatievoorziening:** er leven nog veel vragen over een digitale bronidentiteit en (NL) wallet bij Nederlandse burgers en inclusie doelgroepen waarop zij eerst antwoord willen voordat er tot aanvraag over gegaan wordt.
3. **Kosten:** indien een digitale bronidentiteit of (NL) wallet dezelfde kosten met zich meebrengt als het fysieke paspoort, geeft een deel van de Nederlandse burgers aan dat de meerwaarde van een digitale bronidentiteit niet opweegt tegen de prijs. De Nederlandse burger is ook gewend dat een app of wallet gratis gebruikt kan worden.
4. **Bezit (juiste) mobiele telefoon:** niet in het bezit zijn van een mobiele telefoon of het niet mogen/kunnen gebruiken van een telefoon is met name specifiek benoemd door de inclusie doelgroepen.

   Daarnaast kunnen ook strenge voorwaarden m.b.t. veiligheid waaraan een mobiele telefoon moet voldoen ervoor zorgen dat bepaalde "verouderde" mobiele telefoons niet kunnen en mogen "deelnemen" in het ecosysteem. Een digitale bronidentiteit mag niet aan deze telefoons gekoppeld worden.
5. **Onvoldoende toegevoegde waarde:** ondanks de positieve houding is de verwachting dat een digitale bronidentiteit en (NL) wallet in het dagelijks leven weinig verschil gaat maken.
   - Er is namelijk **niet** het gevoel dat de digitale identificatie **sneller en/of gemakkelijker** gaat dan het identificeren met een fysiek identiteitsdocument.

     De vergelijking met het pakken van een rijbewijs of identiteitskaart is vaak gemaakt. Daarbij is het contactloos betalen met Apple Pay vaak het referentiekader. Alles wat moeilijker is en meer handelingen vergt wordt daardoor ervaren als niet gebruiksvriendelijk, stressvol en verlaagt de intentie voor gebruik. Dit geldt met name voor de inclusie doelgroepen en Nederlandse burgers die middelmatig tot geen ervaring hebben met het gebruik van apps. Voor digivaardige Nederlanders geldt dit veelal niet. Zij ervaren de digitale bronidentiteit en (NL) wallet als erg handig en een makkelijke manier om zich te identificeren.

- Ook is er over het algemeen geen moeite met de huidige middelen die gebruikt worden, zoals het paspoort, ID-kaart of rijbewijs. Nederlandse burgers en inclusie doelgroepen zien ondanks een positieve houding voor een digitale bronidentiteit en (NL) wallet graag dat het huidige fysieke identiteitsdocument blijft.
- Een ander argument waarom verwacht wordt dat een digitale bronidentiteit en (NL) wallet in het dagelijks leven weinig verschil gaat maken is: het sowieso **weinig** hoeven **identificeren**, op de controle van de

CoronaCheck app na en het ophalen van pakketjes, kopen van drank, huren van een auto en reizen.
- Verder blijkt dat niet alle door de concept eIDAS-verordening mogelijk verplichte attesten een toegevoegde waarde te hebben.

  In het toevoegen van een diploma wordt niet veel meerwaarde gezien, aangezien het hoeven tonen van een diploma vrijwel nooit plaatsvindt.

  Documenten die volgens inclusie doelgroepen interessant kunnen zijn om toe te voegen aan een digitale bronidentiteit zijn een rijbewijs, Verklaring Omtrent het Gedrag, zorgpas, visum of medicijnenpaspoort, maar ook buitenlandse documenten voor Nederlandse burgers met een migratie-achtergrond. Het is op deze wijze mogelijk om alle persoonlijke documenten op één plek te vinden.

8.2.4 Toegevoegde waarde, gevoel van veiligheid en gevoel van controle

Door het vergroten van toegevoegde waarde, gevoel van veiligheid en gevoel van controle neemt de gebruikersintentie van een digitale bronidentiteit en (NL) wallet toe. Met deze drie aspecten moet dan ook rekening worden gehouden tijdens de ontwikkeling van een digitale bronidentiteit en (NL) wallet.

Gevoel van veiligheid en de toegevoegde waarde

Onderzoek geeft aan dat bij het concept van digitaal identificeren er een afweging wordt gemaakt tussen het gevoel van veiligheid en de toegevoegde waarde van het concept.

Uit het onderzoek komt naar voren dat voor meerdere inclusie doelgroepen de digitale bronidentiteit en (NL) wallet (of in ieder geval het concept dat nu is voorgelegd) op dit moment niet een nadrukkelijke behoefte vervult. Juist omdat deze groepen geen duidelijke meerwaarde voelen boven de manieren die zij nu gebruiken voor identificatie, neemt het onzekere gevoel rondom veiligheid de overhand.

Echter bij visueel en motorisch beperkten is de nadrukkelijke behoefte voor digitaal identificeren wel aanwezig. Voor hen heeft een digitale bronidentiteit en (NL) wallet zoveel toegevoegde waarde, zoals meer regie en controle hebben over het delen van de gegevens, dat de zorgen rondom veiligheid minder aan bod komen. Hoewel deze groepen ook aangeven dat veiligheid belangrijk is, geeft de extra controle die de digitale identificatie hen biedt (tegenover de fysieke identificatie die zij nu gebruiken) de doorslag.

Overheid en gevoel van veiligheid

Meer dan de helft van de Nederlandse burgers vindt het aanbieden van een digitale bronidentiteit en (NL) wallet passen bij de Overheid:
- Nederlandse burgers die het aanbieden van een digitale bronidentiteit en (NL) wallet passend vinden bij de overheid lichten toe dat ze het goed vinden dat de overheid met de tijd meegaat.
- Nederlandse burgers die het minder of niet passend vinden geven als voorbeelden dat het niet werkbaar is voor ouderen en dat het gevoelig is voor fraude.

Verder is er meer vertrouwen in de overheid. Dit vertrouwen is er niet als de digitale bronidentiteit en (NL) wallet door een andere partij wordt aangeboden. Zij verwachten dat andere partijen misbruik maken van de data uit de digitale bronidentiteit. Daarnaast is er ook meer vertrouwen in de digitale bron-identiteit doordat deze door een uitgevende instantie van de overheid uitgegeven en gekoppeld wordt.

Dat het concept vanuit de overheid komt, schept ook vertrouwen bij de inclusie doelgroepen, omdat zij er ook vertrouwen in hebben dat de overheid op de juiste manier met hun gegevens omgaat. Desondanks zetten zij nog wel vraagtekens bij de veiligheid. Ook schept het een verwachting dat er een externe toezichthouder is die toeziet hoe er om wordt gegaan met gegevens en hoe er samengewerkt wordt met derde partijen.

Daarbij is de wens dat de controle gebeurt door een externe toezichthouder. Hoewel het niet duidelijk en concreet is wie de externe toezichthouder zou moeten zijn, is het wel van belang dat dit niet gebeurt door de overheidsinstantie die de digitale bronidentiteit ontwikkelt of door de commerciële partij met wie er wordt samengewerkt.

Als een digitale bronidentiteit en (NL) wallet door de overheid wordt uitgebracht, is wel de verwachting dat de overheid ook de mogelijkheid biedt voor ondersteuning. Het moet duidelijk zijn waar vragen over het gebruik van de digitale bronidentiteit, (NL) wallet en gegevens gesteld kunnen worden.

Private partij

Over de mogelijkheid dat een digitale bronidentiteit en (NL) wallet door een private partij uitgebracht zou worden, reageren Nederlandse burgers en inclusie doelgroepen huiverig. Aangezien een private partij ergens geld mee wil verdienen, verwachten zij dat dit misschien gebeurt door het (door)verkopen van gegevens, of in ieder geval de data, die in digitale bronidentiteit staan.

Het advies is dan ook om voor initiële acceptatie in te zetten op de zichtbaarheid van de overheid als afzender: in het design en de schrijfstijl van de oplossing.

Controle

Het gevoel van controle te hebben over wat er gedeeld wordt, is belangrijk.

Daarbij ervaart de ene inclusie doelgroep meer controle bij het hebben van een fysiek pasje in de portemonnee, terwijl de andere inclusie doelgroep meer controle voelt bij een digitale bronidentiteit en (NL) wallet.

Specifiek voor visueel beperkten en motorisch beperkten geldt dat digitaal identificeren een gevoel van controle geeft:

- Visueel beperkten voelen een grote meerwaarde in een digitale bronidentiteit en (NL) wallet.
  Zij kunnen bij het pakken van een fysiek document niet zien of voelen welk pasje de identiteitskaart is. Zij weten niet of ze het fysieke document goed tonen, maar zien ook niet wat de ontvangende partij met de fysieke identiteitskaart doet als deze afgegeven moet worden. En kunnen zij niet controleren of ze de juiste pas terugkrijgen. Bij het digitaal identificeren ervaren en hebben de visueel beperkten ook meer controle over de gegevens die zij delen. Zij kunnen immers goed gebruik maken van de hulpmiddelen op de mobiele telefoon waardoor zij waarnemen welke gegevens gevraagd en gedeeld worden.
- Het digitaal identificeren kan in een online omgeving hulp bieden bij het automatisch invullen van de persoonsgegevens i.p.v. het zelf invoeren. Dit verkleint de mogelijkheid tot het maken van spelfouten voor de Nederlandse burger en met name visueel-, en motorisch beperkten.
- Voor personen die problemen hebben met de fijne motoriek is het lastig om een fysiek identiteitsbewijs uit de tas of portemonnee te pakken. Een mobiele telefoon is voor hen prettiger en bruikbaarder.

Verder is opgevallen dat hoe betrouwbaarder de ontvangende partij ervaren wordt, hoe sneller de bereidheid er is om gegevens te delen en hoe minder er gedacht wordt aan de reden waarom gegevens gevraagd worden om te delen. Hoe minder vertrouwen, hoe lager de kans op delen van gegevens.

Dit vertrouwen lijkt gebaseerd te zijn op hoeveel de gebruiker in aanraking is geweest met de ontvangende partij, de algemene reputatie van de ontvangende partij en de persoonlijke ervaringen met de ontvangende partij.

Belangrijk is dat er duidelijkheid is en aangegeven wordt welke gegevens gedeeld worden en dat het delen pas plaatsvindt na het geven van toestemming. Dit zorgt er ook voor dat een dienstverlener niet zomaar allerlei gegevens van iemand kan ontvangen. Het ontvangen van een bericht in een (NL) wallet over welke gegevens uiteindelijk gedeeld zijn vergroot daarnaast ook het gevoel van controle te hebben.
Daarnaast zijn er wel vragen over welke gegevens worden opgeslagen bij een andere partij, waarom, voor hoelang en wie erbij kunnen.

Kortom, er zijn zorgen over veiligheid in het gebruik van digitale middelen in combinatie met persoonsgegevens en het hebben van controle over gegevens kan leiden tot een veilig gevoel bij digitale identificatie.

8.3 Ontwerp van een digitale bronidentiteit en (NL) wallet

Belangrijk bij het ontwerpen van een digitale bronidentiteit en (NL) wallet is dat iedereen deze zelfstandig kan aanvragen en gebruiken, zodat inclusieve en toegankelijke producten en processen ontwikkeld worden. De gebruiker hoort hierbij centraal te staan.[98]

Bij inclusie gaat het erom dat alle mensen kunnen meedoen in de samenleving, ongeacht hun diversiteit in fysieke, cognitieve (waaronder taal) en psychosociale vaardigheden, en de omstandigheden waarin zij leven. Ook de beschikbaarheid van benodigde middelen valt hieronder. In het tijdelijk besluit digitale toegankelijkheid overheid is bepaald dat websites en mobiele apps van Nederlandse overheidsinstanties moeten voldoen aan de toegankelijkheidseisen die zijn geformuleerd op Europees niveau[99].
Met de inwerkingtreding van de Wet Digitale Overheid krijgt het tijdelijke besluit een formeel wettelijke basis en wordt het een verplicht toe te passen standaard.

Ontwerpen voor inclusie, *inclusion by design*, betekent dat de volledige diversiteit van mensen optimaal gebruik kan maken van de producten. Het is een ontwerpaanpak waarin ontwerpers en andere betrokkenen bij het ontwerpen van hun producten, diensten of omgevingen:
- Rekening houden met diverse mogelijke langdurige, tijdelijke, situationele of veranderende beperkingen van gebruikers, in vaardigheden.
- De gebruiker centraal zetten in het gehele ontwerpproces en niet de techniek.
- Waarbij het uitgangspunt is dat het ontwerp niet specifiek is aangepast voor bepaalde groepen, maar toegankelijk is voor iedereen.

> ***"The key to inclusive design isn't to target specific groups, it's to not exclude groups"***

Dit betekent niet dat verschillende groepen worden benoemd waarvoor verschillende oplossingen voor één product worden bedacht. Het is de uitdaging om één product en proces voor alle gebruikers te ontwerpen. Echter, het product moet wel zo worden ingericht dat de gebruiker zijn manier van omgang met een mobiele telefoon (met name inzet van hulpmiddelen), bijvoorbeeld door gebruik van een voice over, gebruik van kleuren, vergroten en verkleinen van beeld niet in de weg staan.

Daarbij is de ervaring en de taak die uitgevoerd moet worden hetzelfde. Alleen de manier waarop dit kan, door inzet van hulpmiddelen, kan daarbij anders zijn. In het ontwerp komt dit o.a. tot uiting door:

Aanvraag-en uitgifte van een digitale bronidentiteit

Fysiek aanvraag en uitgifteproces:
- Aanvraag en uitgifte van een digitale bronidentiteit: een deel van het aanvraagproces vindt op eigen plek en in eigen tijd plaats: installatie en gereed maken van de (NL) wallet.

[98] Home - Gebruiker Centraal
[99] Wat is verplicht? | Digitoegankelijk

Uit onderzoek blijkt dat de gebruiker zoveel mogelijk stappen in de eigen tijd en eigen omgeving wil doen. Zodat de druk van een balie en rij niet ervaren wordt en de gebruiker rustig de (NL) wallet kan instellen. Voorwaarde is wel dat goede voorlichting zowel in de (NL) wallet als buiten de (NL) wallet nodig is en er een punt moet zijn waar mensen naartoe kunnen gaan als ze vragen hebben.

Het koppelen van de digitale bronidentiteit aan de (NL) wallet vindt plaats aan de balie van een uitgevende instantie.

- Secure channel tussen mobiele telefoon en backend DBI-voorziening opzetten voor het koppelen van de digitale bronidentiteit aan de (NL) wallet: uitdaging is om een oplossing te vinden die ook door visueel beperkten uitgevoerd kan worden en waarbij geen extra hardware op de balie nodig is. Een oplossing hiervoor is bijvoorbeeld dat de (NL) wallet een code genereert die na tonen door de baliemedewerker kan worden ingevoerd in de DBI-voorziening. Voordeel is dat de handeling door de baliemedewerker wordt uitgevoerd en hierdoor geen extra handeling van de gebruiker nodig is.

Remote aanvraag en uitgifte:

- Nederlanders woonachtig in het buitenland (niet ingezetenen) kunnen vanuit het buitenland via een proces waarbij ingelogd wordt met de DigiD op afstand een digitale bronidentiteit aanvragen en koppelen aan de (NL) wallet. Voorwaarde hierbij is dat de Nederlander ingeschreven is in de RNI.
- Europeanen die zaken willen doen met Nederland kunnen op afstand met hun Europese digitale bronidentiteit en (EU) wallet inloggen om een Nederlandse digitale bronidentiteit aan te vragen en te koppelen aan hun (EU) wallet. Voorwaarden is wel dat de Europeanen zich hebben ingeschreven in de RNI en in het bezit zijn van een BSN.

Cloud-based oplossing

Om de gebruiker een keuze te geven de digitale bronidentiteit via een mobiele telefoon, tablet of desktop te gebruiken is een oplossing bedacht waarmee de digitale bronidentiteit door de overheid in een cloud-based wallet opgeslagen kan worden. Deze cloud-based wallet heeft dezelfde functionaliteiten als de wallet op de mobiele telefoon.

De gebruiker kan de digitale bronidentiteit dan in eigen tijd op zijn apparaat naar keuze downloaden. Maar de gebruiker kan ook besluiten alleen de cloud-based wallet te gebruiken. Hiermee is het mogelijk de digitale bronidentiteit ook te gebruiken op andere apparaten dan een mobiele telefoon of een tablet.

Daarnaast hoeft de gebruiker bij een nieuwe telefoon niet meer naar een uitgevende instantie en is het mogelijk om de digitale bronidentiteit uit de cloud-based wallet te downloaden.

Er is nog niet besloten of een digitale bronidentiteit op meerdere apparaten geplaatst mag worden.

Gebruik van de digitale bronidentiteit en (NL) wallet

Inloggen:

- De gebruiker heeft een voorkeur voor een tweetraps verificatie om te voorkomen dat anderen bij de persoonsgegevens kunnen. Maar ook het idee dat een (NL) wallet automatisch opent als de mobiele telefoon tegen een scanapparaat aangehouden wordt is niet prettig, omdat gebruikers niet per ongeluk hun (NL) wallet willen openen. Inzet van tweetraps verificatie geeft daarom een veilig gevoel. Dit is mogelijk door naast een pincode biometrie in te zetten. De wijze waarop deze tweestapverificatie het meest gewenst is (door een code, vingerafdrukscan of gezichtsscan) verschilt echter per gebruiker:
  - De meeste gebruikers zijn bekend met de gezichtsherkenning en vingerafdruk. Zij ervaren dit als gebruiksvriendelijk en een snelle methode om in te loggen. Een pincode heeft als nadeel dat deze onthouden moet worden. Met name ouderen hebben hier moeite mee en vinden het vervelend om er weer een pincode bij te hebben.
  - Er zijn gebruikers die het gevoel hebben dat biometrische inlogmethoden niet altijd effectief zijn, bijvoorbeeld als er wijzigingen in het uiterlijk zijn, zoals een ooglidcorrectie of een baard, maar ook het hebben van vochtige vingers of door handwerk het verlies van de vingerafdruk.

- Er zijn ook gebruikers die het gevoel hebben dat biometrische inlogmethoden veiliger zijn aangezien die uniek zijn voor hen als persoon en een code te raden is.
- Voor motorisch beperkten met een fijne motoriek en visueel beperkten kan het gebruik van een gezichtsscan lastig zijn, omdat het recht voor de camera houden van het gezicht niet zichtbaar of mogelijk is.
- Voor visueel beperkten is er ook verschil in gemak tussen manieren van inloggen. Zo is een wachtwoord en naam moeilijker in te vullen dan een code.
- Verder beschikt niet iedereen over een mobiele telefoon waarbij manieren als inloggen met gezichts-herkenning of vingerafdruk werkt.

Delen gegevens:

- De voorkeur bij het delen van gegevens is een pull principe waar de dienstverlener bepaalt welke gegevens er nodig zijn voor de dienstverlening.

Redenen:

- Het aantal handelingen dat de gebruiker moet uitvoeren, is bij een pull concept minder dan bij het zelf moeten samenstellen van een set aan gegevens.
- Delen is minder complex voor de gebruiker.
- Het is voor de gebruiker soms moeilijk in te schatten welke gegevens de dienstverleners nodig hebben. Het is voor de gebruiker daarom veel eenvoudiger om slechts een verzoek tot delen van een set gegevens te accepteren of te weigeren.

Voorwaarden hierbij zijn:

- Het is belangrijk dat de gebruiker voor het delen van de gegevens:
  - Bekend is met wie de gegevens gedeeld worden.
  - Aangegeven wordt welke gegevens gevraagd worden.
  - Er een mogelijkheid is om aan te geven de gevraagde gegevens niet te willen delen.
  - De vormgeving zorgt dat het duidelijk is welke gegevens er gedeeld worden. Vormgeving kan helpen bij het vertrouwen dat de gebruiker heeft bij het delen van de gegevens, verduidelijken welke gegevens er door de dienstverlener gevraagd worden en de handelingen die er verricht moeten worden. Een idee kan zijn om een waarschuwing in te bouwen wanneer bijvoorbeeld het BSN in combinatie met andere persoonsgegevens gevraagd wordt.

    Daarnaast verwachten veel gebruikers dat de vormgeving een digitale versie is van hun fysieke document.
- Er goed toezicht is op wie het ecosysteem betreedt en wat een dienstverlener aan gegevens mag opvragen. De gebruiker moet ervan uit kunnen gaan dat de dienstverlener geen gegevens kan vragen die hij vanuit zijn uitvoerende taak niet nodig heeft.
- Verifiërend middel: integriteit en veiligheid van het middel dat de dienstverlener voor het verifiëren inzet is belangrijk. De gebruiker moet ervan uit kunnen gaan dat dit middel integer en veilig is.
  Dit wil bijvoorbeeld zeggen dat persoonsgegevens niet gelekt kunnen worden en dat de dienstverlener niet meer gegevens kan opvragen dan zij voor het uitvoeren van de taak nodig heeft.
- Om de gegevens te delen met een partij moet de gebruiker altijd toestemming geven. Dit is mogelijk door inzet van een pincode of biometrie. Nader onderzoek hiernaar is nodig.
- Over het opslaan van een “transactie” na het delen van gegevens wordt verschillend gedacht:
  - Sommige gebruikers zien er meerwaarde in om in hun (NL) wallet te zien wanneer en waar hun gegevens zijn gedeeld. Hiermee kunnen ze controleren of de transactie juist is gegaan, maar het kan ook dienen als “geschiedenis/naslagwerk”. Dit draagt bij aan een gevoel van controle.
  - Andere gebruikers hebben hier geen behoefte aan en geven aan dat zij dit nu ook niet weten met het laten zien van een fysiek bewijs. Of vinden het een vervelend idee dat hun activiteiten voor henzelf zichtbaar zijn, denk aan het kopen van drank.
  - Er zijn ook gebruikers die willen kunnen instellen wat er opgeslagen wordt aan de hand van bijvoorbeeld: type gegevens, welke partij en voor welke periode.
- Het is mogelijk om selectief attributen te kunnen delen. Hiermee wordt voorkomen dat persoonsgegevens worden gedeeld die de ontvangende partij niet nodig heeft.

- Voor het maken van een verbinding tussen de digitale bronidentiteit en (NL) wallet van de gebruiker en het verificatiemiddel van de dienstverlener kan gebruik gemaakt worden van een QR-code.
  De voorkeur van de gebruiker ligt in dit geval bij het laten scannen van de QR-code bij de fysieke processen. Hierdoor ligt de actie bij de ontvangende partij, hetgeen minder stress oplevert en voor visueel, en motorisch beperkten een fijne methode is.

De reden hiervoor is dat bepaalde groepen zoals de ouderen, digitaal minder vaardigen en de visueel beperkten zich bij voorbaat onzeker voelen bij het gebruiken van een QR-code:

- Het richten van een mobiele telefoon kan moeilijk zijn voor visueel-, en motorisch beperkten, maar ook voor digitaal minder vaardigen met weinig tot geen ervaring in het gebruik van een QR-code.
  - Visueel beperkten zien niet waar de scanner zich bevindt en motorisch beperkten beschikken niet altijd over de juiste motoriek om de mobiele telefoon tegen de scanner te houden.
  - Visueel beperkten hebben ook problemen om de QR-code op andermans scherm te scannen, omdat onduidelijk is of de QR-code goed in beeld is. Voor motorisch beperkten kan het lastig zijn de mobiele telefoon stil te houden bij het scannen of de armen te bewegen.
  - Digitaal minder vaardigen zijn onzeker over de handelingen die verricht moeten worden en begrijpen ook niet wat de QR-code nu precies doet.
- Met name bij fysieke processen verwachten de inclusiedoelgroepen dat dit voor een onzeker gevoel en stressvolle situaties gaat zorgen (denk aan een rij bij de kassa). Zij willen niet dat anderen op hen moeten wachten en zien dat zij fouten maken. De verwachting bij hen is dat het digitaal identificeren meer tijd vergt dan het identificeren met een fysiek document die slechts gepakt en getoond hoeft te worden. Het aantal handelingen is daarbij minder en de handelingen zijn ook minder complex.
- In een online situatie is dit onzekere en stressvolle gevoel minder aanwezig, omdat ze de druk bekeken en beoordeeld te worden niet ervaren. Het is mogelijk om de tijd te nemen en zonder haast de stappen te doorlopen.
- Voor Nederlanders met een migratieachtergrond uit de EU zou het mogelijk moeten zijn om buitenlandse attesten aan de (NL) wallet te kunnen toevoegen.

Algemeen

- Het voldoen aan de WCAG 2.1 AA[100], denk aan:
  - Tijdslimieten kunnen door gebruiker worden verlengd of ingesteld;
  - Kleurcontrast is 4,5:1 en kleuren kunnen door gebruiker worden aangepast;
  - (NL) wallet is met standaard hulpmiddelen van de telefoon (voiceover, reader, inzoomen, spraakassistenten als siri) te gebruiken;
  - Maar ook: teksten zijn op 2F niveau geschreven en mogelijk ondersteund door visuele weergave.
- Wees taakgericht: kort en bondige omschrijvingen van functionaliteiten verrijken de gebruikerservaring:
  - Omschrijf wat gebruikers kunnen doen of inzien.
  - Omschrijf wat gebruikers aan het doen zijn of bekijken.
  - Omschrijf wat gebruikers hebben gedaan en hoe dat is gegaan.
- Zet herkenbare interactievormen in: gebruikers herkennen methodes uit eerdere ervaring en dit vergroot de ervaring van gebruiksgemak.

Met name inclusie doelgroepen geven aan een voorkeur te hebben voor “standaard” gebruik van overheidsapps. Zij hebben vaak moeite om het gebruik aan te leren en vinden het lastig om weer iets nieuws erbij te leren. Als voorbeeld wordt vaak de DigiD app gegeven.

- Afzender overheid: de gebruiker geeft aan dat ze verwachten dat de overheid een belangrijke rol heeft te vervullen om de privacy, betrouwbaarheid etc. te waarborgen en ook om de digitale bronidentiteit en (NL) wallet uit te geven. Commerciële partijen worden minder vertrouwd, omdat er een verwachting is dat er een verdienmodel achter zit. De overheid heeft geen winstoogpunt.
- De gebruiker heeft de voorkeur dat de (NL) wallet zo eenvoudig mogelijk is en dat attesten niet verplicht worden om in de wallet op te nemen.

[100] Wcag.nl en digitoegankelijk.nl

Met name digitaal minder vaardigen, laaggeletterden, visueel beperkten en ouderen geven aan dat zij behoeften hebben aan een simpele applicatie. Zij willen korte stappen, eenvoudige en bekende handelingen, alleen essentiële (en simpele, Nederlandse) teksten, de mogelijkheid tot voorlezen en weinig afleiding. Het hoeft voor deze groepen niet te uitgebreid en zij willen liever focus op de belangrijkste functie van de app: identificeren.

- Helpfunctie in de (NL) wallet en fysieke helpdesk waar hulp over gebruik en algemene vragen geboden wordt.
- Het moet voor de gebruiker mogelijk zijn om de digitale bronidentiteit op afstand te deactiveren, bijvoorbeeld als de telefoon gestolen is. Hiermee kan gedacht worden om deze functie aan de StopID-app/website toe te voegen.

8.4 Visualisaties

8.4.1 Klantreizen (Samen met dit rapport gepubliceerd)

Om een beeld te geven over hoe de digitale bronidentiteit en (NL) wallet in de praktijk gebruikt zouden kunnen worden zijn een aantal klantreizen uitgewerkt. Daarbij zijn de volgende use cases beschreven:

- Aanvraag en uitgifte digitale bronidentiteit: fysiek aan de balie.
- Aanvraag en uitgifte digitale bronidentiteit: remote in Australië.
- Gebruikerstoepassing fysieke leeftijdsverificatie 18+.
- Gebruikerstoepassing reizen.
- Gebruikerstoepassing overschrijven van een auto.
- Gebruikerstoepassing wallet van een EU lid (over de grens).

8.4.2 Klikbaar model

Bevindingen uit het onderzoek naar de houding en gebruik van een digitale bronidentiteit onder inclusie doelgroepen zijn door het bureau Koos Service Design vertaald naar 2 klikbare modellen die in Figma en met de onderstaande links te zien zijn[101]:

- Model met enkele QR-code
- Model met multiple QR-code

Deze modellen zijn ter inspiratie door gemaakt en kunnen gezien worden als een eerste uitgewerkte schets. De modellen zijn bijvoorbeeld niet aan respondenten voorgelegd.

[101] Enkele QR https://www.figma.com/proto/K9500UocEsouJeGdLbwDFi/Digitale-Bronidentiteit-Prototype?pageid=60%3A2812&node-id=198%3A17836&viewport=241%2C48%2Co.03&scaling=scale-down&starting-point-nodeid=198%3A17836&show-proto-sidebar=1
Multiple QR: https://www.figma.com/proto/K9500UocEsouJeGdLbwDFi/Digitale-Bronidentiteit-Prototype?pageid=213%3A21179&node-id=216%3A27077&viewport=241%2C48%2Co.03&scaling=sca le-down&starting-point-node-id=216%3A27077&show-proto-sidebar=1

9 Bijlage: maatschappelijke kansen en uitdagingen

Bron: Visiebrief digitale identiteit, Tweede Kamer, vergaderjaar 2020–2021, 26 643, nr. 743

Kansen

- De overheid kan door op te treden als gezaghebbende beheerder van de basisregistratie personen een betrouwbare digitale identiteit gaan leveren aan de burger, dit alles binnen Europese context
- Daardoor zal vertrouwen in de digitaal identiteit van de burger kunnen worden vergroot.
- Door de beschikbaarheid van deze digitale identiteit van de burger zal
  - De zelfstandigheid en autonomie van burgers worden bevorderd.
  - Het grondrecht op privacy (beter) kunnen worden waarborgen.
- Een veilige digitale identiteit van de burger, in combinatie met een betrouwbare wallet waarin publieke en private partijen betrouwbare gegevens van de burger kunnen plaatsen,
  - Helpt de burger en bedrijven om veilig digitaal zaken te doen en vermindert administratieve lasten en onnodige maatschappelijke kosten.
  - Bevordert de cyberveiligheid van burgers omdat het de kans ID-fraude verkleint.

Uitdagingen

- Digitale inclusie: de burger loopt het risico dat de herkenbaarheid, gebruiksvriendelijkheid en begrijpelijkheid van processen waarin hij een rol speelt afneemt. Dit draagt het risico in zich dat mensen die minder digitaal vaardig zijn niet meer volwaardig digitaal mee kunnen doen. Goede voorlichting zou hierbij kunnen helpen.
- Digitale veiligheid en betrouwbaarheid: burgers en bedrijven voeren digitale transacties uit met gebruik van een digitale authenticatie midden. Naar de toekomst zal het aantal veilige digitale transacties dat de burger wil realiseren nog veel sterk zal gaan toenemen. In essentie zullen die transacties allemaal in het teken staan om het uitwisselen van waarde tussen burgers en bedrijven mogelijk te maken. Omdat het maatschappelijk en economisch verkeer gebaat is bij vertrouwen zal de investering een betrouwbare digitale Identiteit gaan leiden tot een hogere betrouwbaarheid van digitaal verkeer. Het betrouwbaar leveren van de digitale identiteit gaat dus zorgen voor extra vertrouwen, omgekeerd als er geen vertrouwen is in de digitale identiteit zal dit de adoptie (het gebruik er van) in de weg gaan staan.
- Economische kansen: Nederland zal (binnen Europa) economische en maatschappelijke kansen missen als er geen goede veilige, betrouwbare en toekomstbestendige manier van digitaal zakendoen beschikbaar komt, waarbij een digitale identiteit infrastructuur (veilige digitale identiteit en wallet) cruciale bouwstenen zijn.

10 Bijlage: diensten in het identiteitsecosysteem

Primaire dienst	Bijbehorende product(en)	Opmerking
Leveren ondersteuning aan dienstafnemers en -aanbieders ('helpdesk').		
Melden verlies, fouten, vermoeden van fraude.	Digitale portemonnee (wallet), DBI, attesten.	Wellicht kan dit worden belegd bij het Meldpunt Fouten in Overheids-registraties resp. Centraal Meldpunt Identiteitsfraude.
Blokkeren DBI.		Wellicht hergebruik van StopID functionaliteit.
Uitgeven DBI.	DBI, transactie-geschiedenis.	
Uitgeven attest.	Attesteren, transactie-geschiedenis.	Voor nu is dit een verzamelbegrip. Op een later moment worden – i.s.m. de dienstaanbieders en op basis van de prioriteit van de use cases - de uiteenlopende attesten in detail uitgewerkt.
Intrekken attest.	Attest, transactiegeschiedenis (inden intrekking door burger zelf).	Zie conceptverordening artikel 45 quater lid 3 blz. 45.
Identificeren gebruiker – online.	Attest, transactiegeschiedenis.	Zie conceptverordening artikel 1lid 3(i) blz. 25.
Aanmaken elektronische handtekening op afstand	Elektronische handtekening, transactiegeschiedenis.	Zie verordening artikel 6 bis lid 4 (a)(3), artikel 12 ter lid 3 en artikel 12 quater lid 1.
Leveren bewaringsdienst voor gekwalificeerde elektronische handtekening.		Zie conceptverordening artikel 29 bis lid 1.
Aanmaken elektronische zegel op afstand.	Elektronische zegel, transactie-geschiedenis.	Zie conceptverordening artikel 34.
Verifiëren NL Wallet.	NL Wallet.	Zie conceptverordening artikel 39 bis.
Verifiëren identiteit.	Attestatie(s).	Zie conceptverordening blz. 28artikel 6 bis lid 5.
Verifiëren attribuut.	Attribuut.	Zie conceptverordening artikel xx
Toekennen machtiging/ vertegenwoordiging.	DBI.	Zie conceptverordening artikel 6 bis lid 4(a)(2) en lid 5(b), artikel 24 lid 1, artikel 45 quinquies lid 1.
Intrekken machtiging/ vertegenwoordiging.	DBI.	
Aantonen machtiging/ vertegenwoordiging.	DBI.	

Secundaire dienst	Bijbehorende product(en)	Opmerking
Houden van toezicht op het identiteitsecosysteem.	-	Dit is inclusief de tweejaarlijkse audit van 'gekwalificeerde verleners van vertrouwens-diensten'. Zie conceptverordening artikel 18.
Uitvoeren van governance van het identiteits-eco-systeem.		
Beheren DBI.	DBI.	
Ontwikkelen & beheren NL Wallet.	NL Wallet.	Dit is inclusief o.a. het opschorten van de afgifte c.q. intrekken van de geldigheid van de NL Wallet. Zie conceptverordening artikel 10 bis.
Authentiseren vertrou-wende partijen.	Register van vertrouwende partijen.	Zie conceptverordening artikel 6 ter lid 2. Dienstaanbieders (vertrouwende partijen) moeten hun voornemen om gebruik te maken van de NL Wallet, melden bij de Lidstaat waarin zij zijn gevestigd.
Verifiëren authenticatie dienstaanbieder.	Register van geautoriseerde dienstaanbieders.	
Beheren Register van geautoriseerde vertrou-wende partijen.	Register van geautoriseerde vertrouwende partijen.	
Certificeren (gekwalificeer-de) verlener van vertrou-wensdiensten.	Register van gekwalificeerde aanbieders van vertrouwens-diensten.	Zie conceptverordening, overweging 35.
Verifiëren certificaat gekwalificeerde verlener van vertrouwensdiensten.	Register van gekwalificeerde aanbieders van vertrouwens-diensten.	
Beheren Register van gekwalificeerde verleners van vertrouwensdiensten.	Register van gekwalificeerde aanbieders van vertrouwens-diensten.	
Beheren van middelen voor het aanmaken van elektronische zegels op afstand.		Zie conceptverordening artikel 39 bis.
Opstellen & beheren dienstencatalogus.	Dienstencatalogus.	Alle primaire en secondaire diensten (en hun eventuele voorwaarden) worden opgenomen in een openbaar dienstencatalogus. Zie conceptverordening artikel 6 ter lid 1 en 2.
Certificeren NL Wallets.	NL Wallet, Register van gecertificeerde NL Wallets.	Zie conceptverordening artikel 6 quater.
Verifiëren certificaat NL Wallet.	NL Wallet, Register van gecertificeerde NL Wallets.	
Beheren Register van gecertificeerde NL Wallets.	Register van gecertificeerde NL Wallets.	
Verzamelen statistieken over de werking van de NL Wallet.		Zie conceptverordening artikel 48 bis.
Verzamelen statistieken over de werking van gekwalificeerde vertrou-wensdiensten.		Zie conceptverordening artikel 48 bis.

Bij het prioriteren van diensten en producten mag het burgerperspectief niet ontbreken. Als de eerste diensten/producten die beschikbaar worden gesteld niet aansluiten bij de (dagelijkse) behoeften van burgers, kan dat ten koste gaan van de acceptatie van DBI en de NL Wallet.

11 Bijlage: de NL Wallet

Onderstaande beschrijving van de NL Wallet, een verschijningsvorm van de Europese portemonnee voor digitale identiteit, is ontleend aan de conceptverordening. Voor het gemak wordt in het vervolg op de volgende manier verwezen naar het relevante lid van het artikel: '(6 bis 4(a))'.

Enkele algemene kenmerken van de NL Wallet (6 bis 2, 6 bis 4(b), 6 bis 6, 6 bis7, 6 bis 10, 45 septies, 45 bis)

- De NL Wallet kan worden uitgegeven door de Nederlandse overheid of een door de overheid gemandateerde of erkende partij.[102] De laatste twee situaties geven de mogelijkheid om het uitgeven van de NL Wallet over te laten aan private organisaties. Wel is dan een certificerende overheidsorganisatie nodig om partijen te mandateren/erkennen.
- De NL Wallet dient in alle gevallen te voldoen aan eIDAS-betrouwbaarheidssniveau 'Hoog'. Dat heeft ook gevolgen voor de aanvraag-, uitgifte- en activatieprocessen.[103]
- De NL Wallet moet worden gecertificeerd. De certificering wordt uitgevoerd door een door de overheid aangewezen publieke of private organisatie.
- De Nederlandse overheid kan de uitgifte van de NL Wallet opschorten en de geldigheid van (een specifieke versie van) de NL Wallet intrekken. In dat geval informeert de overheid de Europese Commissie en de overige lidstaten hierover.
- De overheid kan een opschorting/intrekking herstellen. Ook hiervan worden de Europese Commissie en de overige lidstaten op de hoogte gesteld.
- De NL Wallet moet kosteloos te gebruiken zijn. Dat laat overigens onverlet dat voor de activatie van een DBI wel kosten in rekening zouden kunnen worden gebracht.
- De gebruiker heeft de volledige controle over de NL Wallet.
- De uitgever van de NL Wallet mag geen informatie verzamelen over het gebruik ervan. Uitzondering is informatie over portemonneediensten.
- De NL Wallet moet waarborgen bevatten zodat verleners van gekwalificeerde attesteringen van attributen geen informatie ontvangen over het gebruik van de attributen.
- Een gekwalificeerde elektronische attestering van attributen heeft dezelfde rechtsgevolgen als wettelijk uitgegeven attesteringen op papier.

Kernfunctionaliteit voor de gebruiker (6 bis 3, 6 bis 4 (a)(3), 6 bis 7, 11 bis 1)

Een gebruiker kan met de NL Wallet:

- Wettelijke identiteitsgegevens en elektronische attesteringen van attributen inwinnen, verstrekken en opslaan (zie ook paragraaf 5.4 over de verschillende verschijningsvormen van de NL Wallet en over de datakluis).
- Wettelijke identiteitsgegevens en elektronische attesteringen van attributen eerst selecteren, eventueel combineren en vervolgens presenteren.[104]
  - Van 'presenteren' onderscheiden wij twee verschijningsvormen:
    - Tonen. Hier laat de gebruiker de gegevens/attesteringen zien aan een vertegenwoordiger van een vertrouwende partij. Er vindt dus geen geautomatiseerde gegevensoverdracht plaats. De vertegenwoordiger leest de gegevens/attesteringen van het scherm van de mobiele telefoon van de gebruiker.
    - Delen. In deze situatie verstuurt de gebruiker de gegevens/ attesteringen op een geautomatiseerde manier vanuit zijn NL Wallet naar de vertrouwende partij.
- Zich, na positieve identificatie, on- en offline authentiseren om publieke en private diensten af te nemen.
- Ondertekenen met gekwalificeerde elektronische handtekeningen.

---

[102] De beschrijving van de NL Wallet in deze paragraaf is gebaseerd op de concept-verordening, artikel 6 bis.

[103] Deze processen dienen te worden ingericht conform UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

[104] De concept-verordening heeft het consequent over 'delen'. Wij zien echter een duidelijk onderscheid tussen tonen en delen vandaar dat hier het containerbegrip 'presenteren' wordt gebruikt. In de uitwerking over mobiele versus cloud-based NL Wallet (zie paragraaf 5.4) wordt op de toepasbaarheid van tonen en delen ingegaan.

12 Bijlage: de onderzoeksvragen

Onderzoeksvraag 1: definiëren van de bronidentiteit

Dit betreft een beschrijving van het doel, de functie, de technische ontwerpprincipes en inhoud van de bronidentiteit. Deze activiteit levert de verdere uitwerking van het concept van bronidentiteit.

In de uitwerking komen minimaal de volgende onderwerpen aan bod:
- Op welk moment ontstaat een bronidentiteit?
- Waar bestaat een bronidentiteit uit?
- Hoe wordt de bronidentiteit aan de bijhorende persoon verbonden?
- Hoe wordt de bronidentiteit uitgegeven?

Zie hoofdstuk 3 en 4.

Onderzoeksvraag 2: beschrijving identiteitsecosysteem

Beschreven wordt hoe het identiteitsecosysteem met bronidentiteit eruit kan zien, inclusief de rol van de verschillende belanghebbenden. Concrete voorzieningen en voorwaarden worden beschreven, op een detailniveau dat voldoende is om een duidelijke start te bieden voor het realiseren hiervan.

De volgende vragen komen in elk geval aan bod:
- Hoe ziet de ontwikkeling van een toekomstbestendig identiteitsecosysteem eruit?
- Hoe past de DBI in dit ecosysteem?
- Hoe ervaart een ondernemer of burger dit ecosysteem en hoe zorgen we dat dit toegankelijk en begrijpelijk is voor iedereen?
- Wat is de rol van de overheid in dit ecosysteem? Welke voorzieningen worden er publiek aangeboden? Welke voorzieningen warden er aan de markt overgelaten?
- Welke voorzieningen of (identiteits-)middelen vanuit de overheid zijn voorwaardelijk?

Zie hoofdstuk 5.

Onderzoeksvraag 3: juridische en ethische analyse van de bronidentiteit

In een samenwerking tussen DO, CZW en RvIG, en in afstemming met Logius wordt onderzocht wat de juridische en ethische gevolgen zijn van het invoeren van een digitale bronidentiteit. Ook wordt onderzocht hoe deze bronidentiteit zich verhoudt tot bestaande wetgeving rondom identiteit.

De uitwerking bevat minimaal:
- Inzicht in de maatschappelijke/ethische/economische effecten van de DBI.
- Analyse van de juridische basis voor een bronidentiteit.
- Tijdslijn en advies voor wijzigingen in wet- en regelgeving.

Zie hoofdstuk 6.

Onderzoeksvraag 4: analyse bronidentiteit in verhouding tot bestaande voorzieningen

Er bestaan al allerlei voorzieningen en middelen die te maken hebben met identiteit en identiteitsgegevens, zoals het paspoort, de eNIK, de Basisregistratie Personen, DigiD, etc. In deze lijn is onderzocht wat de verhoudingen zijn tussen de digitale bronidentiteit en de (doorontwikkeling van) bestaande voorzieningen.

Zie hoofdstuk 7.

Onderzoeksvraag 5: ontwerpen prototype

Zodra er iets meer duidelijkheid is over het concept bronidentiteit, kan een prototype worden beschreven waarmee we concreet maken hoe een bronidentiteit kan gaan werken voor burgers en dienstverleners. De klantreis staat hierin centraal. Dit prototype is niet per se een applicatie, het zal zeker in eerste instantie een papieren (conceptuele) uitwerking zijn.

Zie hoofdstuk 8.

13 Bijlage: definitielijst

Begrip	Definitie
Attest	Een attestering in elektronisch formaat aan de hand waarvan attributen kunnen worden geauthentiseerd.
Authenticatie	Een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt.
Authentieke bron	Een register of systeem, onder de verantwoordelijkheid van een publiek-rechtelijk orgaan of particuliere entiteit, dat attributen omtrent een natuurlijke of rechtspersoon bevat en als de primaire bron van die informatie wordt beschouwd of krachtens nationaal recht als authentiek wordt erkend.
Autoriseren	Bepalen of iemand in aanmerking komt om toegang te krijgen tot een dienst of informatie etc.
Autoriseren	Bepalen of iemand in aanmerking komt om toegang te krijgen tot een dienst of informatie etc.
Betrouwbaarheidsniveau	De mate waarin vertrouwen kan worden gesteld in een identificatiemiddel.
Digitale bronidentiteit	Een door de overheid uitgegeven, erkende en in de wet en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector.
Europese portemonnee voor digitale identiteit.	Een product en dienst die de gebruiker in staat stelt identiteitsgegevens, inloggegevens en attributen met betrekking tot zijn/haar identiteit op te slaan, op verzoek aan vertrouwende partijen te verstrekken, voor online en offline authenticatie voor een dienst overeenkomstig artikel 6 bis te gebruiken, en gekwalificeerde elektronische handtekeningen en zegels aan te maken.
(NL) Wallet	Registratie van een unieke identiteit (vaststelling en creatie) en vervolgens het uitgeven van een identificatiemiddel om personen in staat te stellen om deze identiteit te laten verifiëren.
Identificatie	Een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:
Vertrouwensdienst	a. het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging, elektronische attestering van attributen en certificaten die betrekking hebben op deze diensten; b. het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites; c. het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben; d. het elektronisch archiveren van elektronische documenten; e. het beheer van middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand; f. het opslaan van elektronische gegevens in elektronische registers.
Attribuut	Een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat.
Elektronische attestering van attributen	Een attestering in elektronisch formaat aan de hand waarvan attributen kunnen worden geauthentiseerd.
Gekwalificeerde elektronische attestering van attributen	Een elektronische attestering van attributen die is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage V [van de Conceptverordening].
Gekwalificeerde vertrouwensdienst	Een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in deze verordening.
Verlener van vertrouwensdiensten	Een natuurlijke persoon of rechtspersoon die een of meer vertrouwens-diensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten.

Begrip	Definitie
Gekwalificeerde verlener van vertrouwensdiensten	Een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen.
Vertrouwende partij	Een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst.
Gebruiker	Een natuurlijk of rechtspersoon die gebruik maakt van diensten van vertrouwende partijen en gekwalificeerde verleners van vertrouwensdiensten.
Elektronisch register	Middels elektronische registers beschikken gebruikers over bewijs en een vaststaand controlespoor voor de volgorde van transacties en gegevens-bestanden.
Gekwalificeerd elektronisch register	[Bewaart] gegevens op zodanige wijze dat het unieke karakter, de authenticiteit en de juiste volgorde van de ingevoerde gegevens onvervalsbaar worden verzekerd. Een elektronisch register combineert het effect van tijdstempels van gegevens met zekerheid over de gegevensbron, wat lijkt op een e-handtekening, met als bijkomend voordeel dat de governancemodellen meer kunnen worden gedecentraliseerd, wat voor samenwerking tussen meer partijen geschikt is.

14 Bijlage: literatuurlijst

- Visiebrief digitale identiteit, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2-2021)
- Conceptverordening eIDAS, Europese Commissie
- Visie op digitale identiteit, Bouwen aan vertrouwen in de digitale wereld, Directie Digitale Samenleving (11-2020)
- Digitale Bronidentiteit - Uitwerking concept, use cases en scenario's voor gebruik, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (1-2021)
- Anil K. Jain, Karthik Nandakumar, Arun Ross (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. DOI: 10.1016/j.patrec.2015.12.013
- Didier Meuwly, Nigel Baker (2020). Biometrics in the aliens' identity chain. A literature study. Universiteit Twente. Wetenschappelijk Onderzoek- en Documentatiecentrum. Project 2965.
- Digital Identity Guidelines: Enrollment and Identity Proofing (June 2017). NIST 800-63A:2017
- Esther Keymolen, Merel Noorman, Bart van der Sloot, Colette Cuijpers, Bert-Jaap Koops, Bo Zhao (2020).
- Op het eerste gezicht. Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties. Universiteit van Tilburg. Wetenschappelijk Onderzoek- en Documentatiecentrum.
- ID4D Practitioner's Guide: Version 1.0 (October 2019). Washington, DC: World Bank Group. World Bank Document
- Jungleminds (2021). Gebruikersonderzoek digitale bronidentiteit vanuit burgerperspectief, fase 2
- Ruigrok Netpanel (2022). De attitude naar & het gebruik van een digitale bronidentiteit onder inclusie doelgroepen

Dit is een uitgave van:

Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Postbus 10451 | 2501 HL Den Haag

December 2022