Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 743

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 februari 2021

1. Inleiding

In deze brief informeer ik uw Kamer over mijn visie op het onderwerp digitale identiteit. Het doel hiervan is om een krachtige richting neer te zetten op dit voor onze maatschappij belangrijke onderwerp. De brief begint met de maatschappelijke uitdagingen op dit onderwerp, mijn visie op dit domein en tot slot de internationale context en het vervolg.

Duidelijk is dat de behoefte aan een strategisch verhaal op dit onderwerp breed leeft en van veel waarde kan zijn.[1] Ik heb in het werken aan deze visie vooropgesteld dat dit een gedragen visie moet zijn. Dat is het geworden. In samenwerking met meerdere departementen, medeoverheden, kennisinstellingen, dienstaanbieders en identiteitsmiddelen leveranciers ben ik tot deze visie op digitale identiteit gekomen. Ook is er input ontvangen van internationale experts op dit domein. We hebben in het werken aan deze visie een zo open mogelijke werkwijze gehanteerd, omdat dit vraagstuk de gehele maatschappij raakt.

Deze brief beschrijft de visie voor onze digitale identiteit en de taken en verantwoordelijkheden die de overheid invult in deze digitale identiteit infrastructuur. De brief sluit aan bij de recente brieven van het Kabinet over digitale inclusie, regie op gegevens, digitale toegang en de Agenda Digitale Overheid.[2]

---

[1] Zie onder andere: Brede Maatschappelijke Heroverwegingen, Thema 13 Een betere dienstverlening voor Burgers en Bedrijven: Kamerstuk 32 359, nr. 4.

[2] Kamerstuk 26 643, nr. 721.
Kamerstuk 32 761, nr. 147.
Kamerstuk 26 643, nr. 711.
Kamerstuk 26 643, nr. 700.

kst-26643-743
ISSN 0921 - 7371
's-Gravenhage 2021

In bijlage 1 vindt u een heldere beschrijving van de concepten digitale identiteit, de digitale identiteit infrastructuur en de verschillende functies en rollen die we hierin herkennen. Dit biedt een duidelijke afbakening en focus voor dit onderwerp.

2. Maatschappelijke uitdagingen en kansen

Onze wereld verandert momenteel razendsnel en veel veranderingen hebben een impact op de manier waarop wij met onze digitale identiteit omgaan. Een digitale identiteit die onderhand cruciaal is geworden voor de manier waarop wij het vertrouwen borgen dat zo belangrijk is in alle zaken die we zonder persoonlijk contact online met elkaar doen. Zonder een betrouwbaar stelsel rond onze digitale identiteit is het moeilijk om de persoon of organisatie met wie we digitaal zaken doen te vertrouwen.[3]

Voor veel maatschappelijke processen is het vertrouwen dat je zaken doet met de juiste organisatie of persoon cruciaal. Denk hierbij aan de toenemende digitalisering van vele cruciale maatschappelijke processen die door de Coronacrisis in een stroomversnelling is gekomen. Van eHealth tot digitale bankzaken, van digitaal shoppen tot digitaal onderwijs. Al deze processen maken gebruik van een bepaalde vorm van onze digitale identiteit.[4] Denk ook aan de internationalisering van transacties en de behoefte aan een betrouwbare manier om jezelf, tot in de mate dat het nodig is, kenbaar te maken in diverse grensoverschrijdende digitale processen. Telkens speelt de vraag hoe iemand zich kenbaar kan maken met behoud van zijn/haar privacy. Zonder een bepaalde mate van kenbaarheid is er geen vertrouwen om samen zaken te doen. We zullen moeten bouwen aan vertrouwen in de digitale wereld met een betrouwbare digitale identiteit infrastructuur.

De sterkere afhankelijkheid van onze digitale identiteit infrastructuur zorgt ervoor dat we met nieuwe uitdagingen op het gebied van cyberdreigingen en online identiteitsfraude worden geconfronteerd.[5] Op dit moment zorgt de snelheid van innovatie ervoor dat mensen veelal zonder alternatief afhankelijk zijn van grote niet-Nederlandse techbedrijven. Hierbij zien we te vaak dat de diensten zogenaamd «gratis» zijn, maar men eigenlijk «betaalt» met gegevens.

We zien dat er een grotere aandacht komt voor de transparantie en openheid van de technologie die we gebruiken. Zeker als het om technologie gaat waar burgers moeilijk zonder kunnen. Ook zorgt de snelheid van innovatie er soms voor dat voor groepen burgers het domein van digitale identiteitsmiddelen te complex is geworden.[6] De inclusie van deze groepen, ook op het domein van onze digitale identiteit, is een cruciaal aandachtspunt voor mij.

---

[3] Voor een toelichting op de «vertrouwen» op het internet als belangrijkste drijfveer voor een digitale identiteit infrastructuur zie: World Economic Forum Community Paper, «Reimagining Digital Identity: A Strategic Imperative»: https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative McKinsey, «Digital identification: A key to inclusive growth»: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

[4] Zie voor een overzicht van de maatschappelijke kansen: World Economic Forum Community Paper, «Reimagining Digital Identity: A Strategic Imperative»: https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative

[5] Zie bijvoorbeeld CBS bericht toename cybercrime en identiteitsfraude: https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

[6] Zie voor voorbeelden en de voortgang op het domein digitale inclusie: Kamerstuk 26 643, nr. 721.

Vraagstukken die vragen om een betrouwbare digitale identiteit infrastructuur:

- **Digitale inclusie:** De burger loopt het risico dat de herkenbaarheid, gebruiksvriendelijkheid en begrijpelijkheid van processen en identiteitsmiddelen afneemt. Dit draagt het risico in zich dat mensen die minder digitaal vaardig zijn niet meer volwaardig digitaal mee kunnen doen.
- **Digitale veiligheid en betrouwbaarheid:** Burgers en bedrijven voeren momenteel soms transacties uit met gebruik van een digitale identiteit op een onvoldoende betrouwbaarheidsniveau.[7] Ook lopen burgers en bedrijven veelvuldig het risico om hun gegevens onvoldoende beveiligd te hebben bij het aangaan van digitale (grensoverschrijdende) transacties.
- **Toekomstbestendige (overheids-)dienstverlening**: Overheden en bedrijven kunnen op termijn met de huidige infrastructuur van identificatiemiddelen niet op een veilige, betrouwbare en toekomstbestendige manier dienstverlening blijven bieden.
- **Economische kansen**: Nederland mist economische kansen door het niet goed beschikbaar hebben van een veilige, betrouwbare en toekomstbestendige manier van digitaal zaken doen, waarbij een digitale identiteit infrastructuur een cruciale bouwsteen is.[8]

Ik zie door deze vraagstukken kansen voor Nederland om te werken aan een betrouwbare digitale identiteit infrastructuur. Er liggen duidelijke kansen om vanuit de overheid enkele belangrijke publieke waarden beter te dienen. Enkele kansen:

- De overheid kan door op te treden als gezaghebbende bron van een betrouwbare digitale identiteit het **vertrouwen in het digitaal verkeer** vergroten.[9]
- **Zelfstandigheid en autonomie** van burgers bevorderen.
- Het grondrecht op **privacy** (beter) waarborgen.
- Een stevige digitale identiteit infrastructuur kan het **verdienvermogen** van Nederland versterken.
- Een duidelijke en herkenbare digitale identiteit infrastructuur helpt burgers en bedrijven digitaal zaken te doen en **vermindert administratieve lasten** en onnodige maatschappelijke kosten.
- Een duidelijke en herkenbare digitale identiteit infrastructuur bevordert de **cyberveiligheid** van burgers en bedrijven.
- Door de basis van de digitale identiteit infrastructuur duidelijk te leggen (zoals bij de fysieke identificatiemiddelen zoals paspoorten) kan **de overheid een betrouwbare partner** zijn voor andere partijen die innovaties willen toevoegen aan dit domein.
- **Veilige gegevensuitwisseling** in bijvoorbeeld de zorg met toestemming van de patiënt.
- Een veilige, betrouwbare en toekomstbestendige digitale identiteit infrastructuur kan helpen om **identiteitsfraude tegen te gaan**.

---

[7] Europese regelgeving (eIDAS) onderscheid verschillende betrouwbaarheidsniveaus van identificatie. Voor bepaalde diensten is een hoger betrouwbaarheidsniveau nodig. Zie: Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1612282424576

[8] McKinsey spreekt in het rapport «Digital identification: A key to inclusive growth» van een economisch groeipotentieel van 3%-13% BBP bij realisatie van een betrouwbare digitale identiteit infrastructuur: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

[9] Onder andere de Wereldbank adviseert een strategie waarbij de overheid de rol pakt van gezaghebbende bron in een digitale identiteit infrastructuur: World bank Identification for Development (ID4D) Programma, «ID4D Practitioner's Guide» (2019): https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide

Nederland hoort op dit domein momenteel bij de landen die voorop lopen, maar het kan en het moet beter.[10] Daarom wil ik bouwen aan vertrouwen in de digitale wereld door een betrouwbare digitale identiteit infrastructuur in te richten.

3. Visie: bouwen aan vertrouwen in de digitale wereld

Mijn visie op digitale identiteit is dat we in gezamenlijkheid gaan bouwen aan vertrouwen in de digitale wereld. Burgers en bedrijven willen digitaal zaken doen met elkaar en met de overheid. In de digitale wereld waarin Nederlandse burgers en bedrijven actief zijn heeft de overheid een actieve rol in het creëren van vertrouwen door een zorgvuldige identificatie, betrouwbare authenticatie en gecontroleerde autorisatie mogelijk te maken. Dit vertrouwen is essentieel voor economische en sociale ontwikkeling.

Een gebrek aan vertrouwen leidt ertoe dat burgers, bedrijven en overheden zullen aarzelen om transacties digitaal uit te voeren en van nieuwe diensten gebruik te maken. We moeten daarom werken aan een digitale identiteit infrastructuur die het mogelijk maakt om op een betrouwbare, veilige en erkende manier digitaal zaken te doen. Burgers krijgen de mogelijkheid om zelf de regie te voeren over een gezaghebbende bron van identiteitsgegevens.

Digitale bronidentiteit

Deze gezaghebbende bron bevat de digitale identiteit van burgers zoals door de overheid vastgesteld en geregistreerd. Ik hanteer voor deze gezaghebbende bron het concept van een «digitale bronidentiteit» (DBI).[11] Een door de overheid uitgegeven, erkende en in de wet en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector. Deze digitale bronidentiteit bevat een minimale set van identiteitsgegevens die nodig zijn in het maatschappelijk verkeer.[12] De overheid creëert met de digitale bronidentiteit een «gezaghebbende bron» van betrouwbare persoonsidentificerende gegevens. Dit biedt een belangrijk generiek bouwblok voor vertrouwen in de digitale wereld. De DBI als «gezaghebbende bron» maakt afgeleide digitale identiteitsmiddelen mogelijk, net zoals je met een fysiek paspoort andere afgeleide identiteiten mogelijk kunt maken. Bijvoorbeeld bij een bank, verzekeraar of energiebedrijf. Het doel is dus dat de overheid een basisblok biedt waarmee, binnen de kaders van de digitale identiteit infrastructuur, andere partijen betrouwbare diensten kunnen aanbieden. Allemaal onder regie en zelfbeschikking van de burger.

---

[10] EU eGovernment Benchmark 2020: https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-2020-egovernment-works-people

[11] Hierbij sluit deze visie aan bij de richting die het amendement van de leden Middendorp en Verhoeven op de Wet Digitale Overheid voorstellen met de introductie van een «online identiteit». Deze bronidentiteit stel ik voor een behapbaardere vorm te geven dan de «online identiteit» als door het betreffende amendement beschreven. De doelen van zelfbeschikking, gegevens kunnen inzien, corrigeren en delen, onderschrijf ik echter. Zie: Kamerstuk 34 972, nr. 20.

[12] Deze digitale bronidentiteit verschilt hiermee van het huidige DigiD. DigiD biedt burgers een authenticatiemiddel (inlogmiddel) op verschillende betrouwbaarheidsniveaus. Het biedt de burger momenteel niet de mogelijkheid om door de overheid geverifieerde identiteitsgegevens (bijvoorbeeld voornaam, achternaam of geboortedatum) zelfstandig en betrouwbaar te gebruiken in diverse maatschappelijke processen (publiek en privaat).

De principes die ik wil hanteren voor de beoogde digitale identiteit infrastructuur vindt u in bijlage 2. In bijlage 3 vindt u een nadere beschrijving van de digitale identiteit infrastructuur inclusief een weergave van deze beoogde infrastructuur.

4. Vier pijlers

Mijn visie op digitale identiteit en de bijbehorende infrastructuur is gebaseerd op vier pijlers. Op de eerste twee van deze pijlers hebben wij reeds de nodige activiteiten lopen. Op de derde en vierde pijler gaat de overheid haar activiteiten versterken.

I. **Delen van betrouwbare gegevens**
   Het fundament van de visie is gebaseerd op een overheid als «gezaghebbende bron». Door ook in de digitale dienstverlening geverifieerde gegevens vanuit de overheid 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. Deze pijler volgt de activiteiten in het programma Regie op Gegevens en het voorstel van de EU Data Governance Act.[13]
II. **Digitale Toegang**
   Het organiseren van toegang tot digitale dienstverlening in de Nederlandse maatschappij voor alle burgers en bedrijven op een passend (eIDAS) betrouwbaarheidsniveau, zowel in het publieke als private domein. Deze pijler volgt de activiteiten van het programma digitale toegang (eerder eID).[14]
III. **Digitale bron identiteit**
   Een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector.
IV. **Wet en regelgeving rond digitaal vertrouwen**
   Wet- en regelgeving die de uitgangspunten en afspraken rond het delen van gegevens, digitale toegang en het leveren van vertrouwen in de digitale wereld, inclusief de digitale bronidentiteit vastlegt. Deze wet- en regelgeving stellen we op in samenwerking met alle betrokken partijen en zal ook de kaders voor een duidelijke governance bevatten.

5. Internationale/EU context

Op Europees niveau raakt het onderwerp digitale identiteit aan het onderdeel elektronische identificatie (eID) in de eIDAS-verordening. Voor dit onderdeel ben ik eerstverantwoordelijk.

De eIDAS-verordening van 23 juli 2014 (EU No 910/2014) verplicht lidstaten onder meer om elkaars inlogmiddelen te accepteren in de grensoverschrijdende digitale dienstverlening tussen overheden en burgers en bedrijven binnen een jaar nadat deze middelen Europees zijn erkend, ofwel genotificeerd. Op basis van deze verordening zijn eHerkenning en DigiD genotificeerd voor grensoverschrijdende dienstverlening en heb ik de technische voorzieningen gerealiseerd die nodig zijn voor het gebruik van inlogmiddelen uit andere lidstaten in onze digitale dienstverlening van overheden en organisaties met een publiekrechtelijke taak.

---

[13] Kamerstuk 32 761, nr. 147.
Kamerstukken 22 112 en 26 643, nr. 2890.
Proposal for a Regulation on European data governance (Data Governance Act):
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[14] Kamerstuk 26 643, nr. 711.

De eIDAS-verordening is onderwerp van revisie door de Europese Commissie die momenteel wetsvoorstellen ambtelijk voorbereidt. Jongstleden juli heeft de Commissie haar «roadmap» gepubliceerd in de vorm van een «Inception Impact Assessment».[15] Daarin zet de Commissie in lijn met haar *«Strategy on Shaping Europe's Digital Future»*[16] haar doelstellingen uiteen om de effectiviteit van de eIDAS-Verordening te vergroten met onder meer verdere harmonisatie, standaardisatie en certificering, om het werkingsgebied van de verordening te verbreden naar digitale dienstverlening in de private sector en om betrouwbare digitale identiteiten en dienstverlening te realiseren voor álle EU-burgers. Hierin zitten ook globale plannen voor een European Digital Identity (euID). Zodra de Commissie haar wetsvoorstellen presenteert, zal Uw Kamer hierover worden geïnformeerd. «Digital Identity» is niet alleen een speerpunt in de «Digital Strategy» van de Commissie, maar ook één van de belangrijke aandachtspunten van de «Coalition of the Willing», waarbinnen Nederland samen met Finland trekker is van dit thema.[17]

6. Vervolg

Deze brief schetst mijn visie op de digitale identiteit van burgers die voortbouwt op de lijn die ik heb ingezet met het wetsvoorstel Wet Digitale Overheid (Kamerstuk 34 972). Ik heb in werking gezet dat ambtelijk de voorbereidingen getroffen worden om deze visie een solide wettelijke basis te bieden en om te zetten in concrete beleidsregels en uitvoering. Ook heb ik met betrekking tot de digitale bronidentiteit de uitwerking hiervan en enkele pilots in gang gezet gefinancierd door de investeringspost verbonden aan de Agenda Digitale Overheid.

Deze brief zou mogelijk als richtinggevend discussiestuk kunnen dienen voor de in te richten vaste commissie voor Digitale Zaken.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

---

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

[16] Zie: https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy

[17] Kamerstukken 29 362 en 26 643, nr. 288.

BIJLAGE 1: AFBAKENING EN FOCUS

Betreffende de digitale identiteit van Nederlandse burgers is het relevant te melden dat iedere burger meerdere digitale identiteiten heeft. Meerdere organisaties houden een registratie bij waarbij burgers door een set gegevens gerepresenteerd worden. De overheid en specifiek mijn departement heeft echter een unieke rol doordat zij maatschappelijk en juridisch gezien de meest betrouwbare vorm van identiteiten valideert, creëert, bijhoudt en maatschappelijk bruikbare identificatiemiddelen gelinkt aan deze identiteiten uitgeeft.[18] De overheid is hiermee de meest gezaghebbende bron waar het gaat om maatschappelijk bruikbare en betrouwbare identiteitsgegevens.[19]

Het concept digitale identiteit wordt op veel manieren gebruikt, dus start ik met een duidelijke uitleg van wat ik eronder versta. Onder digitale identiteit wordt een verzameling gegevens verstaan die een entiteit (persoon of organisatie) in het digitale domein representeren. Voorbeelden hiervan zijn:

– Naam, geboortedatum, adres;
– Statische identificerende gegevens, identifiers (bijvoorbeeld BSN, rekeningnummer, KvK nummer of telefoonnummer);
– Biometrie (bijv. gezicht of vingerafdruk);
– Certificaten (bijv. diploma's of rijvaardigheid);
– Dynamische attributen[20] zoals digitale transacties (bijv. bankafschrift).

In deze visie beperk ik mij tot de digitale identiteit van natuurlijke personen.[21] De identiteit van objecten en apparaten zal buiten beschouwing gelaten worden, hoewel in een later stadium zeker de vraag zal opkomen naar generiek overheidsbeleid in deze domeinen.

Bij de digitale identiteit die de overheid geregistreerd heeft in haar registers liggen veel vraagstukken rond onze «digitale identiteit infrastructuur». Hiermee bedoel ik het geheel van stelsels, afspraken, (beveiligings-)standaarden en voorzieningen, rond de digitale identiteit van personen.

In een digitale identiteit infrastructuur worden drie functies onderscheiden. Deze worden weergegeven in onderstaande figuur.[22]

---

[18] Het meest betrouwbare identificatiemiddel in Nederland is het paspoort. Hier worden veel andere geregistreerde identiteiten die een burger heeft van afgeleid. Identiteitsgegevens staan geregistreerd in de Basisregistratie Personen (BRP).

[19] Wanneer ik in deze brief spreek van maatschappelijk bruikbare identiteitsgegevens bedoel ik dat deze, net als fysieke identificatiemiddelen, zowel in de publieke als in de private sector gebruikt kunnen worden.

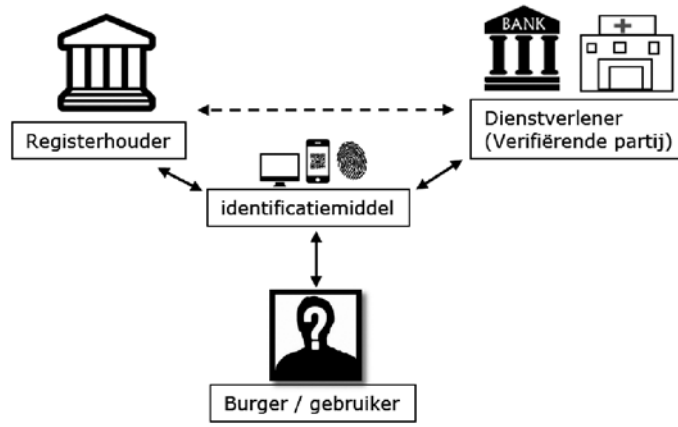
[20] Een attribuut is een gegeven dat hoort bij een bepaalde entiteit die ergens geregistreerd staat. «Jan» kan bijvoorbeeld een attribuut zijn die hoort bij een bepaalde entiteit (persoon). Het attribuuttype is dan «voornaam». Een attribuut is dynamisch wanneer de waarde veranderlijk is. Een «jaarlijks inkomen» is bijvoorbeeld een attribuut dat ieder jaar van waarde verandert.

[21] De identiteit van rechtspersonen laat ik buiten beschouwing, hoewel deze visie daar zeker aan raakt. Een rechtspersoon of organisatie wordt bij haar handelen immers altijd vertegenwoordigd door een natuurlijke persoon. Voor deze natuurlijke persoon zijn eveneens de functies van identificatie, authenticatie en autorisatie van belang in de context van zijn/haar rol bij een rechtspersoon.

[22] Model afkomstig uit: World bank Identification for Development (ID4D) Programma, «ID4D Practitioner's Guide» (2019): https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide
Definities gebaseerd op eIDAS verordening: Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1612282424576

Wie bent u?	*Bent u wie u zegt dat u bent?*	*Bent u geautoriseerd / komt u in aanmerking?*
Identificatie	Authenticatie	Autorisatie
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.	Proces dat de bevestiging van de identificatie van een, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt.	Bepalen of iemand geautoriseerd is / in aanmerking komt om toegang te krijgen tot een dienst of informatie etc.

Om deze functies op een gedegen manier in te vullen worden in een digitale identiteit infrastructuur vier rollen onderscheiden die door diverse partijen ingevuld kunnen worden. Onderstaande figuur geeft deze rollen weer.



Rollen in een digitale identiteit infrastructuur:

1. Burger/gebruiker: De persoon van wie gegevens ergens geregistreerd staan.
2. Registerhouder: De partij die na identificatie gegevens registreert en daarmee een gezaghebbende bron kan vormen (bijvoorbeeld de overheid).
3. Verifiërende (authentiserende) partij: De partij die om een interactie of transactie (dienstverlening) aan te gaan bepaalde claims geverifieerd wil hebben vanuit een gezaghebbende bron.
4. Identificatiemiddel (leverancier): De partij die het identificatiemiddel levert waarmee een persoon zich digitaal kenbaar maakt.

De overheid kan in een digitale identiteit infrastructuur verschillende taken en verantwoordelijkheden hebben. In dit verhaal zal expliciet aangegeven worden welke taken en verantwoordelijkheden de overheid in de toekomst zal hebben:[23]

– Wetgever (hoeder van grondrechten, deels ingevuld door Europese regelgeving en internationale afspraken en steller van rechten en plichten voor justitiabelen)
– Handhaver (op de naleving van wet- en regelgeving zal moeten worden toegezien en gehandhaafd)
– Registerhouder (vaststelling en opslag van elementen/aspecten van iemands identiteit, attributen)
– Dienstenleverancier (alle uitvoering van de overheid door middel van dienstverlening)

[23] Deze taken en verantwoordelijkheden zijn anders dan in de traditionele bestuurskundige context. Ze zijn zo geformuleerd omdat in de digitale identiteitsinfrastructuur de taken en verantwoordelijkheden van de overheid zeer verschillend worden ingevuld en gedeeltelijk los van elkaar staan.

– Leverancier van (digitale) identificatiemiddelen (plus beheer, aanvraag en uitgifteproces)
– (mede) Financier van identiteitsmiddelen of stelsels

BIJLAGE 2:

PRINCIPES DIGITALE IDENTITEIT INFRASTRUCTUUR

Bij deze beoogde digitale identiteit infrastructuur hanteer ik de volgende principes:

Inclusie

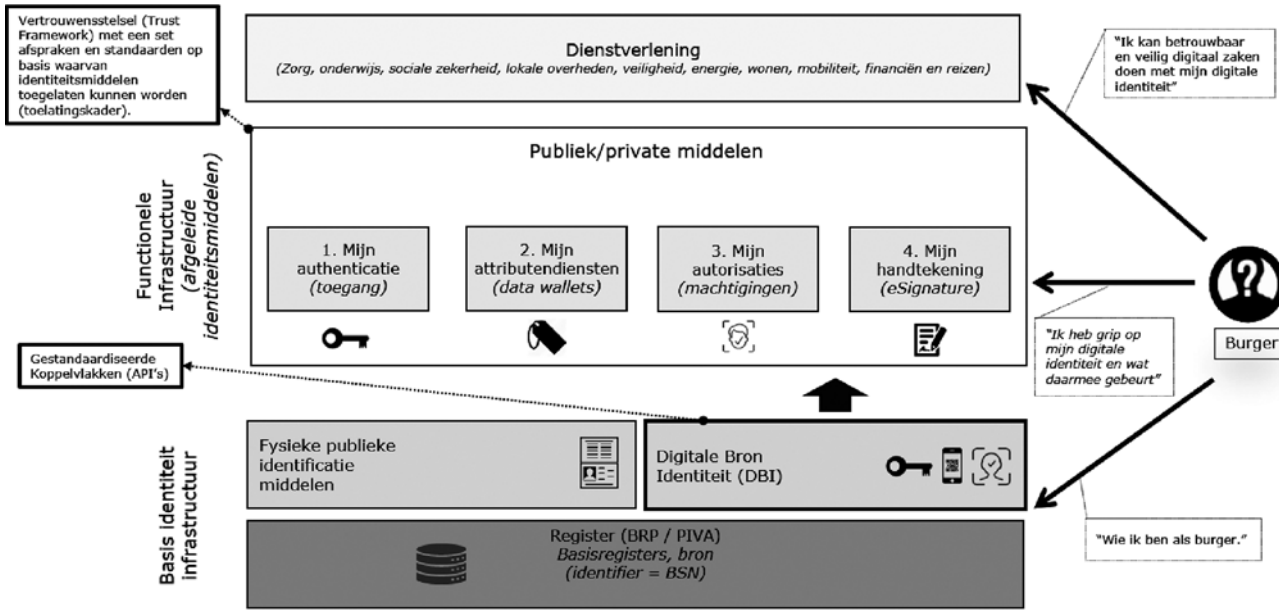
1. Iedereen heeft recht op één digitale (bron)identiteit. Dit betreft personen die een relatie hebben met de Nederlandse overheid.
2. Het verkrijgen en het gebruik van een digitale (bron)identiteit is eenvoudig en intuïtief.
3. Mensen die moeite hebben met het gebruik van een digitaal identificatiemiddel kunnen hulp krijgen of zich digitaal laten vertegenwoordigen door iemand te autoriseren.

Ontwerp

4. De digitale identiteit is voor personen voor gebruik in de publieke en private sector. De digitale identiteit is uniek.
5. De digitale identiteit infrastructuur is robuust, transparant, betrouwbaar, uniek en veilig.
6. De digitale identiteit infrastructuur sluit aan bij huidige en toekomstige (inter)nationale ontwikkelingen en standaarden.
7. De digitale identiteit infrastructuur en alle toegelaten identificatiemiddelen bieden waarborgen voor bescherming van de privacy van de burger (privacy-by-design).
8. Er zijn keuzemogelijkheden qua identiteitsmiddelen en er is ruimte voor innovatie voor het gebruik van de digitale (bron)identiteit (flexibele infrastructuur).

Governance

9. De overheid stelt de eisen en basisvoorwaarden voor een veilige en betrouwbare digitale identiteit infrastructuur op.
10. De uitgifte van een digitale bron identiteit is een overheidstaak.
11. De digitale identiteit infrastructuur wordt verankerd in wet- en regelgeving.
12. Er is onafhankelijk toezicht op het gebruik van de digitale bron identiteit en de toegelaten identiteitsmiddelen in de digitale identiteit infrastructuur.
13. In de digitale identiteit governance neemt een onafhankelijke organisatie zitting die de burger vertegenwoordigt.


Vertrouwensstelsel (Trust Framework) met een set afspraken en standaarden op basis waarvan identiteitsmiddelen toegelaten kunnen worden (toelatingskader).
Dienstverlening
(Zorg, onderwijs, sociale zekerheid, lokale overheden, veiligheid, energie, wonen, mobiliteit, financiën en reizen)
"Ik kan betrouwbaar en veilig digitaal zaken doen met mijn digitale identiteit"
Publiek/private middelen
Functionele Infrastructuur (afgeleide identiteitsmiddelen)
1. Mijn authenticatie (toegang)
2. Mijn attributendiensten (data wallets)
3. Mijn autorisaties (machtigingen)
4. Mijn handtekening (eSignature)
Burger
"Ik heb grip op mijn digitale identiteit en wat daarmee gebeurt"
Gestandaardiseerde Koppelvlakken (API's)
Basis Identiteit Infrastructuur
Fysieke publieke identificatie middelen
Digitale Bron Identiteit (DBI)
Register (BRP / PIVA)
Basisregisters, bron
(identifier = BSN)
"Wie ik ben als burger."

BIJLAGE 3: WEERGAVE BEOOGDE DIGITALE IDENTITEIT INFRASTRUCTUUR[24]

Drie aspecten die ik bij deze weergave zou willen benadrukken zijn de taken en verantwoordelijkheden van de overheid hierin, de digitale bronidentiteit en de uitgangspunten rond digitale identiteit infrastructuur.

Taken en verantwoordelijkheden van de overheid

- De basis identiteit infrastructuur is een verantwoordelijkheid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Deze moet qua standaarden en koppelvlakken generiek en sector onafhankelijk zijn.
- De burger maakt keuzes in de functionele infrastructuur voor bepaalde middelen. De overheid schept kaders en houdt toezicht.
- 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 bevat een minimale set van deelbare identiteitsgegevens.
- De overheid zal zo min mogelijk generieke identiteitsmiddelen leveren in het functionele domein. Dit vanwege verandersnelheid in dit domein die een generieke overheidsvoorziening niet kan leveren. Het streven is een flexibele infrastructuur.
- De overheid biedt gestandaardiseerde koppelvlakken (API's) waarmee burgers hun basisgegeven uit de digitale bronidentiteit kunnen toevoegen aan toegelaten digitale identificatiemiddelen (bijv. digitale data wallets). De burger krijgt dus keuzevrijheid in het functionele identificatiemiddel.
- De overheid ontwikkelt zo min mogelijk functionele digitale identificatiemiddelen. De overheid levert het basis authenticatiemiddel (DigiD) om diensten bij de overheid af te nemen op het benodigde betrouwbaarheidsniveau (conform wetsvoorstel Wet Digitale Overheid).
- De uitgangspunten en afspraken rond het delen van gegevens en het leveren van vertrouwen in de digitale wereld, inclusief de digitale identiteit, worden vastgelegd in wet- en regelgeving met betrokkenheid van private partijen en kennisinstellingen.

Digitale Bronidentiteit

- Elke burger krijgt een unieke DBI die toepasbaar is in zowel de publieke als private sector en toepasbaar is in zowel het burger- als het bedrijvendomein. De DBI is een unieke digitale representatie van de erkenning van de overheid dat jij bent. Net als in het fysieke domein het identiteitsdocument.
- De digitale bronidentiteit vormt een generiek element in de digitale identiteit infrastructuur. Het zal zo klein en zuiver mogelijk zijn qua opgenomen persoonsgegevens.
- Bij de digitale bronidentiteit worden koppelvlakken ter beschikking gesteld aan toegelaten partijen inclusief eenduidige taxonomie van gegevens. Hiermee kunnen burgers hun basisgegevens geverifieerd toevoegen aan toegelaten identificatiemiddelen.
- De digitale bronidentiteit zal een hoog betrouwbaarheidsniveau moeten hebben om bruikbaar te zijn in verschillende sectoren.

---

[24] API = Application Programming Interface. Een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma.
BRP = Basisregistratie Personen. De Basisregistratie Personen bevat persoonsgegevens van inwoners van Nederland (ingezetenen) en van personen die Nederland hebben verlaten (niet ingezetenen).
PIVA = Persoonsinformatievoorziening Nederlandse Antillen en Aruba. De bevolkingsadministratie van Caribisch Nederland (Bonaire, Sint-Eustatius en Saba) en de Caribische landen (Aruba, Sint Maarten en Curaçao).

– De digitale bronidentiteit zal aan eisen moeten voldoen die betrekking hebben op de check op de fysieke gebruiker en de (periodieke) check op de juistheid van de gegevens.
– De middelen in de functionele ID infrastructuur moeten kunnen aansluiten op de basis identiteit infrastructuur zoals nu ook verschillende functionele toepassingen bestaan voor de fysieke publieke identificatie middelen.[25]
– Burgers kunnen via de bronidentiteit inzien welke overheid gerechtigd is om deze gegevens te verwerken, checken of een gegeven mogelijk incorrect is en op termijn zelfs welke overheid deze gegevens heeft verwerkt (één bron, once-only principe).[26]

Uitgangspunten digitale identiteit infrastructuur

– De overheid laat toe dat publieke en private partijen persoonsidentificatiegegevens gebruiken in een identificatiemiddel. Deze worden afgeleid ofwel van de bronidentiteit en/of vanuit een sectoraal (basis)register. Deze partijen kunnen privaat, semi-privaat of overheid zijn. Het toelatingskader zal hiervoor leidend zijn. De burger kan zelf bepalen welke functionele identificatiemiddelen hij/zij wil gebruiken.
– De overheid biedt zo min mogelijk functionele identificatiemiddelen. Voorlopig in ieder geval het publieke authenticatiemiddel (DigiD) en identificatiemiddelen die gedreven worden door relevante Europese en/of internationale ontwikkelingen en standaarden.
– De overheid laat verschillende sectoren verschillende functionele identificatiemiddelen gebruiken. Er wordt wel naar gestreefd om een eenduidig toelatingsstelsel en toezichtstelsel vast te leggen. Centraal wordt gekeurd en toegelaten. Sectoraal wordt de keuze voor middelen gemaakt.
– De overheid organiseert een open samenwerkingsplatform rond de wet- en regelgeving rond digitaal vertrouwen (pijler 4) waar leveranciers van identificatiemiddelen (autorisatie, attributen, authenticatie en ondertekening) mee kunnen denken over de door de overheid voor te schrijven standaarden, eisen, toezicht en doorontwikkeling. Ook worden experts uit de publieke sector, private sector en wetenschap betrokken.
– Er zal een centrale toezichthouder aangewezen worden belast met toezicht op de naleving van de wet- en regelgeving rond digitaal vertrouwen en hergebruik van identiteitsgegevens die de overheid beheert via identificatiemiddelen.
– De overheid biedt via innovatiesubsidies mogelijkheden om binnen de kaders die gesteld worden identificatiemiddelen verder te ontwikkelen.[27]

[25] Rijksoverheid. Wettelijke identiteitsbewijzen: https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/met-welke-identiteitsbewijzen-kan-ik-mij-identificeren

[26] Het once-only principe is het idee dat een burger zijn/haar gegevens slechts eenmalig bij de overheid hoeft aan te leveren. Hiermee worden de administratieve lasten voor burgers en bedrijven verkleind. Zie: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle
Dit principe sluit aan bij de doelstellingen van het amendement van de leden Middendorp en Verhoeven op de Wet Digitale Overheid: Kamerstuk 34 972, nr. 20.

[27] Denk hierbij onder andere aan het door mij ingestelde Innovatiebudget Digitale Overheid. Zie: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/innovatie/innovatiebudget/