Tweede Kamer
DER STATEN-GENERAAL

Rapportage

Digitale Identiteit

Verslag van rapporteur

datum 12 mei 2022

Vaste commissie voor Digitale Zaken

Inhoudsopgave

1 Inleiding 3
2 Digitale identiteit 4
2.1 Toegang tot het publieke domein 4
2.2 Doorontwikkeling toegang tot het publieke en private domein 5
3 Europese portemonnee voor digitale identiteit 8
3.1 Herziening eIDAS: raamwerk voor een Europese Digitale Identiteit 8
3.2 Stand van zaken onderhandelingen 10
3.3 Controle door de Tweede Kamer 11
4 Aandachtspunten digitale identiteit en portemonnee 13
4.1 Bescherming van persoonsgegevens 13
4.2 Inclusie 15
4.3 Ter beschikking stellen van attributen 15
4.4 Implementatie 16
4.5 Mobiele app (stores) 18
4.6 Browserstandaarden 18
5 Dossier digitale identiteit in twee commissies 20
5.1 Commissie Digitale Zaken 20
5.2 Commissie Binnenlandse Zaken 20
5.3 Advies 21
Bijlage 1 Wat is een digitale identiteit? 22
Bijlage 2 Wat is Self Sovereign Identity? 25
Bijlage 3 Self Sovereign Identity speelveld 27

1 Inleiding

Tijdens de procedurevergadering van de vaste commissie voor Digitale Zaken (DiZa) van 9 maart 2022 is besloten mij, Renske Leijten (SP), aan te stellen als rapporteur voor het EU-voorstel voor een *Verordening voor een raamwerk voor een Europese digitale identiteit* (COM(2021) 281) en hoe het Nederlandse beleid daarop aansluit. In de procedurevergadering van 23 maart 2022 is mijn voorstel voor de invulling van het rapporteurschap door de commissie akkoord bevonden en heeft de commissie mij als rapporteur mandaat verleend voor de voorgestelde activiteiten.

Op 3 juni wordt naar verwachting een raadsakkoord in de Telecomraad bereikt over het EU-voorstel. De Tweede Kamer voert voorafgaand aan de Telecomraad op 31 mei een commissiedebat over de positie en inbreng van het kabinet. In dit verslag heb ik aandachtspunten en vraagsuggesties opgenomen die u kunt betrekken bij dit debat.

In het verslag ga ik ook in op hoe het Nederlandse beleid voor een digitale identiteit aansluit op de nieuwe Verordening. Hiervoor heb ik verschillende kabinetsbrieven geraadpleegd die bij de commissie Digitale Zaken en de commissie Binnenlandse Zaken zijn geagendeerd. De commissie Binnenlandse Zaken heeft op 28 september 2022 een commissiedebat gepland staan over de Basisregistratie Personen en e-ID. Dit verslag kan daarom ook bij dat debat betrokken worden.

De uitwerking van de digitale identiteit is uiteindelijk vooral een nationale aangelegenheid op basis van de met lidstaten afgesproken Europese standaarden. Ik ga tenslotte kort in op de constatering dat de Kamer het onderwerp Digitale Identiteit in verschillende commissies behandelt en adviseer de Kamer om de nationale uitwerking van de digitale identiteit nauwgezet te (laten) volgen in het kader van de Kennisagenda (bijvoorbeeld in de vorm van een vervolg op dit rapporteurschap).

2 Digitale identiteit

Het Nederlandse beleid heeft tot doel dat alle burgers en bedrijven in Nederland en in andere Europese landen op een veilige, betrouwbare, toegankelijke en gebruiksvriendelijke manier zoveel mogelijk digitaal transacties kunnen verrichten in het *publieke* en in het *private* domein.

2.1 Toegang tot het publieke domein

Inlogmiddelen
Met DigiD (een publiek inlogmiddel voor burgers) en eHerkenning (een privaat inlogmiddel voor bedrijven) wordt toegang verleend tot de digitale dienstverlening van de overheid. Een van de doelstellingen van het wetsvoorstel Digitale Overheid (Wdo) is om burgers naast DigiD ook *private* inlogmiddelen te kunnen laten gebruiken waar hoge betrouwbaarheid van het inlogmiddel vereist is. Hiervoor moet een stelsel ingericht worden, waarin gezorgd wordt dat het publieke inlogmiddel voor burgers beschikbaar is, dat een systeem voor open toelating van private inlogmiddelen bevat en dat er voorzieningen zijn om deze inlogmiddelen te laten samenwerken. In voorbereiding op de inwerkingtreding van de Wdo is de staatssecretaris van BZK alvast gestart met de inrichting van dit stelsel.

Toezicht op veiligheid en betrouwbaarheid
Het wetsvoorstel Wdo voorziet in toezicht op de inlogmiddelen en op overheden om te zorgen dat inlogmiddelen veilig en betrouwbaar zijn en dat overheidsdienstverleners het juiste betrouwbaarheidsniveau inzetten. De staatssecretaris richt daarom toezicht en handhaving op het stelsel in. Het Agentschap Telecom zal toezicht houden op de aanbieders van inlogmiddelen. Voor toezicht op verplichtingen uit de Wdo die zich richten tot overheden wordt aangehaakt bij bestaand interbestuurlijk toezicht.

Stand van zaken Wet Digitale overheid
Het wetsvoorstel voor de Wdo ligt ter behandeling in de Eerste Kamer. In de schriftelijke behandeling zijn vragen gesteld en zorgen geuit over onder meer de borging van privacybescherming bij de inzet van (private) inlogmiddelen. Om tegemoet te komen aan die zorgen heeft de staatssecretaris van BZK een novelle ingediend bij de Tweede Kamer waarin eisen met betrekking tot privacy-by-design, een verhandelverbod van gegevens en open source op wetsniveau worden verankerd. De novelle is door de commissie DiZa aangemeld voor plenaire behandeling.

Analoge dienstverlening
Niet iedereen is even digitaal vaardig en een grote groep burgers heeft behoefte aan ondersteuning. Voor burgers die niet digitaal met de overheid zaken kunnen of willen doen, blijft een analoge dienstverlening openstaan (via een balie of per telefoon).

Wederzijdse acceptatie inlogmiddelen in Europa
Het Europese initiatief voor elektronische identificatie en vertrouwensdiensten (eIDAS-verordening) vormt de basis voor grensoverschrijdende elektronische identificatie, authenticatie en websitecertificering in de EU. Deze verordening verplicht lidstaten onder meer om elkaars inlogmiddelen kosteloos te accepteren in de grensoverschrijdende digitale dienstverlening tussen overheden en burgers en bedrijven. DigiD en eHerkenning zijn erkend voor gebruik over de grens.

2.2 Doorontwikkeling toegang tot het publieke en private domein

Kabinetsvisie op digitale identiteit
Voor veel maatschappelijke processen is het vertrouwen dat je zaken doet met de juiste organisatie of persoon cruciaal. Door de toenemende digitalisering van deze publieke en private processen 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. Het kabinet deelde daarom in haar brief van 11 februari 2021 haar visie op de 'digitale identiteit' en de taken en verantwoordelijkheden van de overheid (zie bijlage 1 voor meer informatie). Met die digitale identiteit kunnen burgers zich online identificeren voor het doen van transacties.

Het kabinet introduceert in haar visie het concept van de 'digitale bronidentiteit'. De digitale bronidentiteit moet een gezaghebbende bron van identiteitsgegevens zijn waar de burger zelf de regie over kan voeren en die de burger kan gebruiken in de *publieke* en de *private* sector. Dit moet een belangrijk bouwblok worden voor vertrouwen in de digitale wereld. Op dit moment wordt het concept van de digitale bronidentiteit uitgewerkt. Ook wordt een prototype ontwikkeld van hoe dit maatschappelijk goed zou kunnen functioneren. Doorontwikkeling van huidige Europees erkende inlogmiddelen (eID's, zoals DigiD) is hierbij een van de opties. De staatssecretaris heeft een onderzoek uitgezet om vanuit het gebruikersperspectief te onderzoeken hoe dit concept het beste ontworpen kan worden.

Het kabinet wil in de 2e tranche van de Wdo de grondslag verankeren voor het delen van gegevens in combinatie met de 'digitale bronidentiteit'. Die kan dan op termijn gebruikt worden in oplossingen zoals een 'e-wallet' (digitale portemonnee) waaraan allerlei attributen gekoppeld zouden kunnen worden. Het is de overheid die zulke oplossingen toelaat en er toezicht op houdt binnen het nationale eID-stelsel. Daarbinnen zullen burgers en bedrijven zoveel mogelijk zelf de regie moeten hebben over hun gegevens op hogere betrouwbaarheidsniveaus.

Regie op je digitale identiteit (Self Sovereign Identity)
Self Sovereign Identity (SSI) is een nieuwe manier van denken over digitale identiteit, gestoeld op het principe dat individuen controle zouden moeten hebben over hun digitale identiteit en de gerelateerde gegevens. De burger krijgt als het ware

zelfbeschikking over de gegevens (zie bijlage 2 voor meer informatie hierover). SSI is hierdoor bij de Nederlandse overheid, volgens de staatssecretaris, niet onopgemerkt gebleven. Inmiddels is SSI een onderwerp geworden bij diverse partijen, zoals overheden, bedrijven en kennisinstellingen, en vinden er veel projecten plaats. De staatssecretaris schrijft in de voortgangsbrief van 12 oktober 2021 deze ontwikkeling kritisch te onderzoeken en te blijven experimenteren. De staatssecretaris heeft ook een analyse laten uitvoeren van het SSI-ecosysteem (in bijlage 3 vindt u een korte samenvatting van dat onderzoek). Zij hoopt hiermee dat het kabinet een duidelijke positie kan innemen en richting kan geven aan toekomstige beleidskeuzes.

Samenwerken met lidstaten
Nederland wil graag met andere lidstaten samenwerken in de ontwikkeling van een digitale identiteit. Het kabinet ziet dat het concept van de digitale bronidentiteit in diverse landen ontwikkeld wordt. Het wordt ook wel 'foundational identity', 'source identity' of 'motherID' genoemd. Ook sluit dit concept aan bij de voorstellen van de Europese Commissie voor een Europees Raamwerk voor een Digitale Identiteit (zie hierna).

De staatssecretaris heeft in 2020 een zogenoemde Coalition of the Willing[1] opgericht. Dit is een samenwerkingsverband van acht Europese lidstaten[2] om de digitale transformatie van overheden te versnellen. De komende periode doet de staatssecretaris naar deze vraagstukken een voorbereidend onderzoek. In de volgende voortgangsrapportage die voor het zomerreces 2022 verwacht wordt zal de staatssecretaris de Kamer hierover informeren.

Daarnaast is Nederland een pilot gestart samen met Duitsland. Op 23 september 2021 tekenden de Duitse staatssecretaris en de Nederlandse staatssecretaris een verklaring om samen te werken op het gebied digitale identiteit. Met het ondertekenen van de verklaring zetten beide landen volgens het kabinet een stap richting een stelsel voor digitale identiteit waarin burgers meer controle hebben over hun gegevens die ze in Europa kunnen gebruiken. Deze samenwerking gebeurt in het verlengde van de Coalition Of The Willing. In antwoord op vragen van leden antwoordde de staatssecretaris in het commissiedebat Digitale overheid, datagebruik en algoritmen,

[1] Tijdens de behandeling van de begroting van Binnenlandse Zaken in 2020 is door de staatsecretaris aangegeven in 2021 te rapporteren over de resultaten en de voortgang van de samenwerking op de thema's binnen de Coalition of the Willing. Op 2 februari 2022 ontving uw commissie een brief van staatssecretaris van Huffelen waarin zij uitstel hiervan aankondigt. Uw commissie heeft deze brief voor kennisgeving aangenomen (d.d. 16 februari 2022). In mei 2022 worden de eindresultaten van de eerste agenda van de Coalition of the Willing gepresenteerd en zal de agenda voor 2022 en 2023 worden vastgesteld. Deze resultaten over de afgelopen periode en de plannen voor 2022/2023 wil zij graag laten meenemen in een brief aan de Tweede Kamer over de plannen van het nieuwe kabinet voor digitalisering op internationaal terrein, breder dan de Coalition of the Willing.

[2] Nederland, België, Duitsland, Denemarken, Estland, Finland, Frankrijk en Portugal.

digitale identiteit van 22 maart 2022 dat het gaat om een heel kleinschalige proef, waar ongeveer 100 mensen aan meedoen, om te kijken of de digitale identiteit ook grensoverschrijdend kan worden gebruikt. Het idee is, volgens de staatssecretaris, dat als je je in Duitsland kunt identificeren, of in Nederland bijvoorbeeld via DigiD, dit straks ook mogelijk is in het buitenland.

Verschillende landen zetten, volgens TNO en INNOPAY, de eerste stappen richting gebruik van een 'portemonnee'. Eind 2020 initieerde Duitsland de eerste use case voor gebruik van het European Digital Identity Initiative. Binnen deze use case kunnen zakenreizigers inchecken bij een hotel met gebruik van een credential gebaseerd op hun ID bewijs. Eind juli 2021 maakten Duitsland en Spanje bekend te gaan samenwerken rondom de SSI portemonnees. Hiertoe is een Memorandum of Understanding getekend, deze is open voor andere landen om bij aan te sluiten. Ook Nederland is sinds september aangesloten bij deze samenwerking. Binnen de samenwerking zullen best practices gedeeld worden, op technisch, operationeel en regelgevend niveau, en zal cross border interoperabiliteit worden geborgd.

3 Europese portemonnee voor digitale identiteit

3.1 Herziening eIDAS: raamwerk voor een Europese Digitale Identiteit

De Europese Commissie heeft op 3 juni 2021 een voorstel ingediend voor een 'raamwerk voor een Europese Digitale Identiteit', dat de huidige eIDAS-verordening herziet. Met het EU-voorstel voor een Verordening voor een raamwerk voor een Europese digitale identiteit (COM(2021) 281) stelt de Europese Commissie een Europese portemonnee voor digitale identiteit voor.

Online (social media) platformen bieden accounts aan waarmee ook op andere websites en online omgevingen kan worden ingelogd (bijvoorbeeld: bij Booking.com kun je onder meer inloggen met je Facebook-, Google- of Apple-account). Deze manier van inloggen wordt steeds dominanter in Europa, terwijl deze accounts, en de online transacties ermee, onvoldoende zekerheid bieden voor betrouwbaar en veilig gebruik en bescherming van gegevens van gebruikers. Het voorstel van de Commissie beoogt de werking van de eIDAS-verordening te bevorderen door lidstaten te verplichten eID's te erkennen voor Europees gebruik én de functionaliteiten van eID-middelen te vergroten in de vorm van een nationaal te introduceren digitale identiteit portemonnee. De portemonnee kunnen lidstaten in eigen beheer of onder mandaat uitgeven of ze kunnen een onafhankelijk uitgegeven wallet erkennen. Deze portemonnee dient burgers en bedrijven die dit willen, de mogelijkheid te bieden om onder een hoog beveiligingsniveau hun elektronische identiteit én daaraan gelinkte attributen, zoals kwalificaties, bevoegdheden en digitale documenten, zelf ter beschikking te stellen.

Met dit voorstel voor een digitale portemonnee bouwt de Europese Commissie voort op de eIDAS-verordening. Het nieuwe EU-voorstel (eIDAS2) bevat nu de *verplichting* voor lidstaten om burgers en bedrijven een systeem voor digitale identificatie te verschaffen dat een beveiligde toegang tot publieke diensten biedt en in de hele Europese Unie kan worden gebruikt. Daarnaast bevat het bepalingen over het gebruik van een dergelijke identificatie voor private diensten. Ook moet deze op de eigen smartphone of apparaat te downloaden, installeren en gebruiken zijn.

Lidstaten verstrekken nationale digitale identiteiten
Het voorstel betreft geen unieke Europese digitale identiteit die nationale digitale identiteiten vervangt, maar bouwt voort op nationale systemen en samenwerkingen die al bestaan in en tussen een aantal lidstaten, waaronder Nederland en Duitsland (zie paragraaf 2.2). Lidstaten blijven dus zelf digitale identiteiten verstrekken.

Het voorstel verplicht lidstaten nationale eID's en minstens één portemonnee te introduceren en deze nationaal te doen certificeren voor gebruik binnen de Europese Unie. De Europese Commissie beoogt het grensoverschrijdend gebruik te bevorderen door daarvoor een Europees raamwerk te bieden, dat verder technisch en

organisatorisch zal worden uitgewerkt door de lidstaten. De zeggenschap over en het toezicht op de nationale eID's en portemonnees zal, binnen het kader van de Europese verordening, blijven bij de lidstaten, die in de uitgifte en erkenning van hun nationale digitale middelen autonoom zijn. In die zin verandert het voorstel volgens het kabinet niets voor de huidige digitale inlogmiddelen DigiD en eHerkenning, die al zijn erkend voor grensoverschrijdend gebruik en waarvoor ook nu al de kaders van de eIDAS-verordening gelden. Deze middelen zullen, ook na herziening van deze verordening, gebruikt kunnen blijven worden.

Het belangrijkste verschil met bestaande regels is dat iedereen het *recht* zal hebben op een digitale portemonnee voor de digitale identiteit die in alle Europese lidstaten wordt aanvaard. De portemonnee wordt niet verplicht voor burgers. Publieke diensten en bepaalde private diensten worden daarentegen wel *verplicht* om digitale identiteiten te erkennen die aan de Europese eisen voldoen.

Om lidstaten te ondersteunen werkt de Europese Commissie samen met lidstaten aan een 'toolbox' die het uiterlijk september 2022 gereed wil hebben om te helpen om de nationale eID's doeltreffender maken, de voordelen ervan uit te breiden tot de private sector en persoonlijke digitale portemonnees te creëren. In deze toolbox zitten standaarden, technische specificaties en operationele aspecten. Zodra het technische kader is overeengekomen, kan dit in proefprojecten worden getest.

Verordening sluit aan op Nederlands beleid
Het Nederlandse kabinet (BNC-fiche) staat positief tegenover het Europese voorstel, want het Raamwerk sluit aan bij de wijze van denken van Nederland over de digitale identiteit, waaronder het principe van Self Sovereign Identity (SSI) en Nederland is betrokken bij de uitwerking. Een eerste prototype wordt momenteel in Nederland ontwikkeld en getest en wordt naar verwachting eind 2022 gepubliceerd. Nederland wil op dat punt dan, zoals ook in het Coalitieakkoord staat, het voortouw nemen.

Coalitieakkoord Kabinet Rutte IV
"*We nemen het voortouw en zetten in Europees verband in op versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op …, ontwikkeling van digitale identiteit en ….*"
…
"*We geven mensen een eigen 'online' identiteit en regie over hun eigen data.*" (p. 30)

Hoofdlijnenbrief Kabinet Rutte IV
"*Daarom krijgen burgers een breed bruikbare digitale identiteit, zodat zij zich in de digitale wereld op veilige wijze kunnen identificeren en meer regie over eigen gegevens hebben zonder dat iemand over de schouders meekijkt – vergelijkbaar met het gebruik van een paspoort in de fysieke wereld*."

…
"*Daarom stimuleren we het gebruik van privacy-by-design technologie, bijvoorbeeld bij een breed bruikbare digitale identiteit*…." (p. 8)

"*Daarbij onderstrepen we onze verantwoordelijkheid om analoge alternatieven aan te bieden voor onze digitale dienstverlening*." (p. 12)

Lidstaten moeten de nieuwe Europese portemonnees voor digitale identiteit één jaar na de inwerkingtreding van de verordening aanbieden. Lidstaten blijven zelf verantwoordelijk voor het uitgeven of certificeren van de eigen publieke en/of private portemonnees. In Nederland zullen de portemonnees door het Agentschap Telecom worden gecertificeerd. Als Nationaal Cybersecurity Certificeringsautoriteit (NCCA) houdt dit Agentschap toezicht op de certificering van IT-producten, diensten en processen.

3.2 Stand van zaken onderhandelingen

De onderhandelingen over dit EU-voorstel zijn in een vergevorderd stadium. Hieronder een overzicht, inclusief waar het voorstel is belegd:

Europese Commissie (DG CONNECT)

- 3 juni 2021: publicatie van het voorstel door de Europese Commissie (EC). Binnen de EC is dit dossier belegd bij DG CONNECT en meer in het bijzonder bij het departement Digitale Overheid en vertrouwen. DG CONNECT is verantwoordelijk voor EU-beleid op het gebied van de digitale eengemaakte markt, internetveiligheid en digitale wetenschap en innovatie. Verantwoordelijk Eurocommissaris is Thierry Breton.

Raad (Telecomraad)

- 3 juni 2022: Naar verwachting zal de volledige compromistekst worden goedgekeurd in de Telecomraad. Het (vanaf juli: Tsjechische) voorzitterschap van de Raad heeft dan mandaat om in het najaar te onderhandelen met de EC en het Europees Parlement, dat naar verwachting november 2022 een positie inneemt. NB: Het commissiedebat in de Tweede Kamer over de Telecomraad van 3 juni 2022 vindt plaats op 31 mei 2022. Dit is de laatste formele mogelijkheid voor de Tweede Kamer om de kabinetspositie in de Telecomraad te controleren.

Europees Parlement (ITRE)

- november 2022: Naar verwachting neemt het Europees Parlement (EP) een positie in over het voorstel (plenaire stemming). Hierna heeft rapporteur Romana Jerković (S&D, Kroatië) namens het EP mandaat om te onderhandelen met de Raad en de EC. NB: juli 2022 is de stemming in de (lead-) industriecommissie (ITRE) over het verslag van rapporteur Romana Jerković en de ingediende amendementen.

3.3 Controle door de Tweede Kamer

Sinds de publicatie van het voorstel heeft de Tweede Kamer op diverse momenten controle uitgeoefend op het kabinetsstandpunt en de onderhandelingen van het kabinet over het EU-voorstel voor een verordening voor een Raamwerk voor een Europese Digitale Identiteit:

- Op 30 november 2021 is door de vaste commissie voor BZK een schriftelijk overleg gevoerd over het BNC-fiche (verslag). Er zijn vragen gesteld door de fractie van VVD, D66, PVV, CDA en SP. De antwoorden (verslag) zijn door de commissie Binnenlandse Zaken (BiZa) op 2 december 2021 overdragen aan de vaste commissie voor Digitale Zaken (DiZa). DiZa heeft de antwoorden betrokken bij het schriftelijk overleg van 24 februari 2022 over de informele Telecomraad 2022 en heeft ze ook geagendeerd voor het commissiedebat over o.a. digitale identiteit, van 22 maart 2022.
- Op 14 december 2021 zijn Kamervragen gesteld door het lid Leijten (SP) over de ontwikkeling van een Europese digitale identiteit en de Nederlandse inzet daaromtrent. Deze vragen zijn op 10 februari 2022 beantwoord door de staatssecretaris van BZK.
- Op 2 februari 2022 zijn Kamervragen gesteld door het lid Jansen (FvD) over de ontwikkeling van een digitale identiteit en de positie van het kabinet. Deze vragen zijn op 21 maart 2022 beantwoord door de staatssecretaris van BZK.
- Op 24 februari 2022 is door de vaste commissie voor Digitale Zaken een schriftelijk overleg gevoerd over de informele Telecomraad van 8 en 9 maart 2022 (verslag). En marge van dit overleg werden door de CDA-fractie ook enkele vragen gesteld over de ontwikkeling van digitale identiteiten.
- Op 14 maart 2022 zijn Kamervragen gesteld door het lid Van Haga (Groep Van Haga) over het ontwikkelen van een Europese digitale identiteit in het algemeen en in het bijzonder in relatie tot het coronatoegangsbewijs. Deze zijn op 7 april 2022 beantwoord door de staatssecretaris van BZK.
- Op 29 maart 2022 is tijdens het tweeminutendebat volgend op het commissiedebat van de vaste commissie voor Digitale Zaken over o.a. digitale identiteit een motie ingediend door het lid Leijten (SP) over altijd een gebruiksvriendelijk niet-digitaal alternatief bieden bij het ontwikkelen van nieuwe digitale middelen (constaterende dat de regering voornemens is de sms-notificatie bij DigiD uit te faseren en een digitale identiteit wil ontwikkelen). Deze is aangenomen.
- Op 29 maart 2022 is tijdens het tweeminutendebat volgend op het commissiedebat van de vaste commissie voor Digitale Zaken over o.a. digitale identiteit een motie ingediend door de leden Van Haga (Groep Haga) en Leijten (SP) over het niet indirect verplichten van het gebruik van de eID door te waarborgen dat onlinetoegang tot overheidsdiensten mogelijk blijft met de nationale DigiD (o verwegende dat het nu mogelijk is om bij het inloggen op digitale overheidsdiensten te kiezen tussen de nationale DigiD en de Europese eID). Deze is aangenomen.

- Op 29 maart 2022 is tijdens het tweeminutendebat volgend op het commissiedebat van de vaste commissie voor Digitale Zaken over o.a. digitale identiteit een motie ingediend door de leden Van Baarle (DENK), Kathmann (PvdA) en Leijten (SP) over het wettelijk borgen dat gebruik van de digitale portemonnee te allen tijde vrijwillig is en niemand zonder portemonnee in publieke ruimten mag worden geweigerd (constaterende dat in Europees verband wordt gewerkt aan een digitale portemonnee waarmee mensen zich digitaal kunnen identificeren). Deze is aangenomen.
- Op 31 mei 2022 staat in de Tweede Kamer het commissiedebat gepland over de Telecomraad van 3 juni 2022.

4 Aandachtspunten digitale identiteit en portemonnee

De aandachtspunten van stakeholders voor het (EU-voorstel voor een) raamwerk voor een Europese digitale identiteit zijn dezelfde als die voor de nationale digitale identiteit. In dit hoofdstuk ga ik daar op in. Hiervoor put ik onder meer uit het schriftelijk overleg over het BNC-fiche en de beantwoording van Kamervragen door het kabinet. Ik heb ook vraagsuggesties opgenomen die desgewenst betrokken kunnen worden bij het commissiedebat over de Telecomraad op 31 mei 2022.

4.1 Bescherming van persoonsgegevens

AVG
In de compromistekst van de Raad, die in de Telecomraad van 3 juni a.s. wordt behandeld, staat vooralsnog dat aanbieders van vertrouwensdiensten voor digitale registers, waar gegevens worden opgeslagen, moeten voldoen aan het voorstel én aan andere geldende regels, afhankelijk van de betrokken sector. Zo moeten use cases waarbij sprake is van de verwerking van persoonsgegevens onder meer in overeenstemming zijn met de Algemene Verordening Gegevensbescherming (AVG).

Zowel in het EU-voorstel, als in de voorstellen voor de Wdo, is volgens het kabinet opgenomen dat gebruiks- en gebruikersgegevens en eventuele andere categorieën persoonsgegevens niet gebruikt mogen worden voor andere doeleinden dan de veilige uitgifte van inlogmiddelen en het inloggen met deze middelen. De data van mensen dienen dus niet het verdienmodel van een aanbieder van een digitaal identiteitsmiddel, omdat dit onder de voorgestelde wetgeving niet wordt toegestaan.

Verhandelverbod
In de compromistekst is tevens overeind gebleven dat de leverancier van een digitale portemonnee gebruiksgegevens *niet* voor commerciële doelen mag gebruiken. Ook de staatssecretaris van BZK heeft toegezegd dat er een verhandelverbod komt. De Kamer heeft verder benadrukt met een aangenomen motie dat het kabinet moet waarborgen dat er een publiek alternatief blijft voor een private digitale portemonnee.

Verantwoordelijkheid burger
In een rapport van Deloitte en Grabowsky (2021) wordt de zorg geuit dat de decentrale inrichting van digitale identiteit, waarbij de burger zelf regie kan en mag voeren over zijn persoonsgegevens, veel verantwoordelijkheid bij de burger legt. Hierdoor zouden organisaties buitenproportioneel gegevens kunnen opvragen als voorwaarde om gebruik te maken van hun dienstverlening. Dit brengt risico's met zich mee, zoals het misbruik van deze gegevens of een verhoogde kans op datalekken.

Blockchain
Het kabinet onderzoekt diverse mogelijkheden om blockchaintechnologie te gebruiken zonder daarop persoonsgegevens op te slaan. Dit heeft de voorkeur van het kabinet.

De mate waarin distributed ledger technologie (blockchain) in de Europese en Nederlandse digitale identiteit infrastructuur gebruikt gaat worden staat nog niet vast. Het kabinet kijkt hier naar eigen zeggen kritisch naar, niet alleen vanuit het oogpunt van privacy, maar ook vanuit duurzaamheid.

Marktwerking

Lidstaten kunnen meer dan één portemonnee introduceren en portemonnees kunnen zowel door overheden, door bedrijven als in publiek-private samenwerking uitgegeven worden. De staatssecretaris verkent de mogelijkheden en heeft hierin nog geen keuze gemaakt. De staatssecretaris beoogt met het voorstel voor de Wdo een regime van 'open toelating' te introduceren, waarbij marktwerking wordt ingezet binnen het digitale domein. De staatssecretaris is ervan overtuigd dat veilige en betrouwbare digitale interactie met inachtneming van de privacy gewaarborgd kan worden, ook bij door de markt uitgegeven digitale middelen die erkend en gecertificeerd zijn door de overheid, die bovendien toeziet op werking en gebruik.

Vraagsuggesties

- Hoe wordt voorkomen dat burgers toch in de verleiding worden gebracht om meer informatie te delen met grote bedrijven, bijvoorbeeld in ruil voor korting of een tegoedbon?
- Hoe gaat het kabinet waarborgen dat de leverancier van een digitale portemonnee gebruiksgegevens niet voor commerciële doelen zal gebruiken?
- Heeft het kabinet al voorkeuren ontwikkeld als het gaat om het gebruik van distributed ledger technologie (blockchain) in de infrastructuur van de digitale identiteit?
- In hoeverre kunnen persoonsgegevens van burgers verwijderd of aangepast worden als toch wordt gekozen voor het gebruik van blockchaintechnologie in de infrastructuur van de digitale identiteit?
- Kan een inperking van de burgerrechten ontstaan als bepaalde data in een systeem komt die niet meer kan worden verwijderd, bijvoorbeeld als je een extra paspoort hebt of vanwege je werk door een bepaald land hebt gereisd? Met andere woorden hoe voorkomen we dat mogelijke systeemfouten leiden tot onomkeerbare gevolgen voor personen, zoals in de toeslagenaffaire?
- In hoeverre worden door de overheid persoonsgegevens centraal opgeslagen ten behoeve van de digitale identiteit? Hoe worden deze gegevens beschermd om diefstal en misbruik, in de vorm van bijvoorbeeld identiteitsfraude, te voorkomen?
- Komt er een verplichting voor lidstaten om een unieke en consistente identificatiecode in te voeren om gebruikers te identificeren in gevallen waarin identificatie vereist is? In hoeverre maakt dit de profilering en tracking van burgers in de digitale wereld makkelijker en vormt dit dus een risico voor burgers?
- Welke concrete mogelijkheden ziet het kabinet voor het uitgeven van de digitale portemonnee door de overheid, door bedrijven of in publiek-private samenwerking?

Wat zijn de uitkomsten van de verkenning hiernaar? Wordt de Kamer geïnformeerd over de uitkomsten van deze verkenning en zo ja, wanneer?

4.2 Inclusie

Het gebruik van een digitale portemonnee door burgers en bedrijven is niet verplicht volgens de compromistekst (Overweging 28 en 32, artikel 12b). Het blijft voor iedereen dus mogelijk, indien lidstaten dit goed regelen, om openbare diensten te gebruiken zonder een digitale portemonnee te hebben. Ook de staatssecretaris van BZK heeft aangegeven dat burgers en bedrijven niet verplicht zijn een eID of een digitale portemonnee aan te vragen en te gebruiken, noch onder het EU-voorstel, noch onder het voorstel voor de Wet digitale overheid (Wdo). Mensen die dit niet wensen, zullen op een goede, analoge wijze gebruik moeten kunnen maken van de dienstverlening in het publieke domein.

De staatssecretaris vindt het belangrijk dat altijd speciale aandacht is voor die groep mensen die niet over voldoende digitale vaardigheden of middelen beschikken. Daarom brengt de staatssecretaris in kaart wie er niet mee kunnen en mee willen doen en hoe hiervoor oplossingen geboden kunnen worden.

De uitgifte van de digitale portemonnee is gratis (artikel 6), maar werkt op een mobiel apparaat.

Vraagsuggesties
- Wat zijn de uitkomsten van het in kaart brengen van wie er niet mee kunnen en mee willen doen met de digitale identiteit en portemonnee? Welke concrete oplossingen kunnen hiervoor geboden worden?
- In hoeverre dreigt uitsluiting van niet-digivaardigen wanneer het gebruik van een digitale identiteit en portemonnee gemeengoed wordt?

4.3 Ter beschikking stellen van attributen

In het EU-voorstel heeft de Europese Commissie in Bijlage VI een minimale lijst van attributen opgenomen die lidstaten uit authentieke bronnen ter beschikking zouden moeten stellen voor gebruik in portemonnees. Dit betreffen adres, leeftijd, geslacht, burgerlijke staat, gezinssamenstelling, nationaliteit, onderwijskwalificaties, -titels en -diploma's, beroepskwalificaties, -titels en -licenties, openbare vergunningen en licenties en financiële en bedrijfsgegevens. Het kabinet beraadt zich welke van deze attributen in welke volgorde in de Nederlandse portemonnee(s) dienen te worden opgenomen en op welke wijze. Het zal volgens de staatssecretaris niet makkelijk zijn om snel de door de Europese Commissie voorgestelde hoeveelheid attributen uit authentieke bronnen betrouwbaar en veilig ter beschikking te stellen voor gebruik in één of meer portemonnees.

De staatssecretaris verwacht dat de lidstaten gezamenlijk kunnen besluiten en organiseren dat met bepaalde attributen uit bepaalde sectoren zal worden gestart en dat er onderling afspraken worden gemaakt over gefaseerde uitbreiding van de in portemonnees op te nemen attributen. Dit heeft de voorkeur van de staatssecretaris in tegenstelling tot het centraal organiseren en uitrollen van één Europese eID of portemonnee dan wel één Europees systeem waarop alle publieke en private dienstverleners en alle aanbieders van eID's, portemonnees en attributen uit alle lidstaten zouden moeten aansluiten.

Vraagsuggesties
- Welke van de minimale attributen die na inwerkingtreding van het EU-voorstel door lidstaten uit authentieke bronnen ter beschikking gesteld moeten worden voor gebruik in portemonnees worden in welke volgorde en op welke wijze beschikbaar gesteld? Welke attributen verwacht het kabinet als eerste beschikbaar te stellen en welke volgen later?
- Welke nationale wetgeving moet hiervoor worden aangepast?
- In hoeverre moeten de Nederlandse basisregistraties attributen beschikbaar stellen? In hoeverre is het stelsel van basisregistraties hierop voorbereid? Waar zitten nog de grootste zorgen?

4.4 Implementatie

Het kabinet acht het EU-voorstel volgens het BNC-fiche uitvoerbaar als het gefaseerd wordt ingevoerd. De implementatie zal in nauw overleg gaan met de uitvoering. De potentiële gevolgen worden volgens het kabinet in kaart gebracht en begroot zodra het voorstel in triloog is gebracht.

Niet makkelijk
Het zal volgens de staatssecretaris niet makkelijk zijn om snel de door de Europese Commissie voorgestelde hoeveelheid attributen uit authentieke bronnen betrouwbaar en veilig ter beschikking te stellen voor gebruik in één of meer portemonnees. Evenmin zal het makkelijk zijn om één of meer portemonnees betrouwbaar en veilig beschikbaar te stellen voor gebruik in zowel de publieke sector als het private domein. Daarnaast dient de certificering van en het toezicht op de portemonnees en de daarin opgenomen eID's en attributen georganiseerd en geregeld te worden. Digitale portemonnees dienen door een toezichthoudend orgaan, zoals het Agentschap Telecom, gecertificeerd te worden overeenkomstig de eisen van de cyberbeveiligingsverordening.

Planning en knelpunten
Een planning voor de implementatie van de herziene eIDAS-verordening en inzicht in mogelijke knelpunten daarin kan nog niet door de staatssecretaris gegeven worden. Dit hangt af van de uiteindelijke inhoud van de verordening, het moment van adoptie

daarvan en de in het voorstel opgenomen termijnen voor inwerkingtreding. Nederland loopt voorop, omdat Nederland al voldoet aan de in het voorstel opgenomen plicht voor elke lidstaat om een eID Europees te laten erkennen (DigiD) en omdat Nederland al aangesloten is op de Europese infrastructuur voor grensoverschrijdend gebruik van eID's.

Aanpassing nationale wet- en regelgeving

De staatssecretaris laat de Kamer weten dat voor veilige en betrouwbare opname en gebruik van attributen in één of meer portemonnees uitvoeringbeleid, regelgeving en voorzieningen moeten worden ontwikkeld en gerealiseerd. Het EU-voorstel regelt namelijk meer dan de voorgenomen 1e tranche van de Wdo. In hoofdlijnen ziet het EU-voorstel op meer functionaliteiten en heeft het een bredere reikwijdte. Daar waar de huidige eIDAS-verordening, en in lijn daarmee de 1e tranche van de Wdo, voorschriften bevat voor het veilig en betrouwbaar gebruik van eID's bij overheidsdiensten, regelt het EU-voorstel het gebruik van eID's en attributen met een verplicht te introduceren portemonnee bij overheden en in de private sector onder regie van burgers en bedrijven. De introductie van de portemonnee zal nieuwe functionaliteiten en daarbij horende gegevensverwerking met zich meebrengen. Hiervoor zal nationale regelgeving gewijzigd of opgesteld moeten worden.

Kosten

De kosten voor de invoering van een raamwerk voor een Europese Digitale Identiteit zullen worden opgenomen in de begrotingen, zodra deze geraamd kunnen worden op basis van een geadopteerd voorstel. De hoogte van de uiteindelijke kosten zijn volgens het kabinet nu niet in te schatten en zijn afhankelijk van de uiteindelijke inhoud van de verordening en het tijdpad van inwerkingtreding.

Vraagsuggesties

- Wanneer verwacht het kabinet de Kamer te kunnen informeren over de concrete gevolgen van de implementatie van het EU-voorstel voor Nederland als in november 2022 de triloog gestart wordt?
- Bent u voornemens de Kamer zo spoedig mogelijk te informeren over deze gevolgen, waarbij u onder meer ingaat op de planning, verwachte knelpunten en risico's, aan te passen nationale wet- en regelgeving en de verwachte incidentele en structurele uitgaven?
- In hoeverre is het kabinet al in overleg met uitvoeringsorganisaties hierover?
- In hoeverre zal het Agentschap Telecom gereed zijn voor de certificering van en het toezicht op de portemonnees en de daarin opgenomen eID's en attributen? Beschikt het Agentschap over voldoende gekwalificeerd personeel om deze taak uit te voeren?
- Wanneer verwacht het kabinet de eerste bevindingen en resultaten naar de Kamer te kunnen sturen van de uitwerking van het concept digitale bronidentiteit en de

ervaringen die het heeft opgedaan met andere lidstaten? Welke beleidskeuzes staan open en welke overweegt u te kiezen? Hoe bent u voornemens de Kamer hierbij te betrekken?

4.5 Mobiele app (stores)

De in lidstaten te introduceren portemonnee dient te werken op mobiele apparaten. Het voorstel van de Europese Commissie lijkt daarbij uit te gaan van het gebruik van de App Store van Apple en de Play Store van Google om applicaties te kunnen installeren. Hoewel zulke oplossingen voor adoptie en gebruiksgemak belangrijk zijn, zet het kabinet ook in op technologie- en leveranciersonafhankelijke oplossingen en het bevorderen van open standaarden en open software. De staatssecretaris verkent meer opties dan alleen digitale marktplaatsen van grote bedrijven en meer dan alleen mobiele applicaties, bijvoorbeeld door desktopoplossingen zoals voor DigiD.

Vraagsuggesties
- In hoeverre zullen burgers en bedrijven afhankelijk zijn van Apple en Google bij het gebruik van de digitale portemonnee?
- Beschikken burgers en bedrijven over reële alternatieven wanneer zich onverhoopt storingen voordoen bij Apple en Google die doorwerken op hun stores en verbonden apps en apparaten met de digitale portemonnee?
- In hoeverre zijn Apple en Google aansprakelijk wanneer door een storing in hun systeem burgers en bedrijven geen gebruik kunnen maken van de digitale portemonnee op hun apparaten?

4.6 Browserstandaarden

Met de wijziging van de eIDAS worden browserleveranciers verplicht om Europese standaarden voor betrouwbaarheid te accepteren. De standaarden waaraan gekwalificeerde certificaten voor websiteauthenticatie nu moeten voldoen, garanderen volgens de staatssecretaris van BZK en minister van EZK een hoog beveiligingsniveau. Juist door verplichte acceptatie van deze certificaten zal de veiligheid van websites volgens de staatssecretaris groter worden. In elk geval verhindert het verplicht accepteren van deze certificaten browserleveranciers niet om in geval van een opdoemend veiligheidsrisico snel gepaste maatregelen te nemen, zoals het intrekken van het certificaat. Verschillende cybersecurityexperts waarschuwen echter voor de risico's om browsers te verplichten bepaalde certificaten te accepteren. De meeste browsers hanteren strenge voorwaarden waar certificaatautoriteiten, die certificaten uitgeven gebruikt voor beveiligde verbindingen, aan moeten voldoen. De experts vrezen dat, door sommige websitecertificaten bestaande beveiligingseisen te laten omzeilen, het risico toeneemt dat er onveilige of kwaadaardige certificaten worden uitgegeven waarmee het internetverkeer van gebruikers is te onderscheppen of die

naar malafide websites zijn te leiden. Daarnaast zou het onmogelijk voor de cybersecuritygemeenschap zijn om snel op dergelijke certificaten te reageren.

Het EU-voorstel regelt de verplichte acceptatie van gekwalificeerde certificaten van websiteauthenticatie, maar geeft geen effectieve sanctie in het geval browserleveranciers hieraan niet voldoen. Hier vraagt de staatssecretaris aandacht voor in de onderhandelingen.

Vraagsuggestie

- Hoe weegt het kabinet de risico's die cybersecurityexperts zien om browsers te verplichten bepaalde certificaten te accepteren?

5 Dossier digitale identiteit in twee commissies

Het onderwerp Digitale Identiteit komt momenteel in twee Kamercommissies aan de orde, te weten bij de commissies Digitale Zaken en Binnenlandse Zaken. Beide commissies voeren het voortouw op relevante brieven van het kabinet.

5.1 Commissie Digitale Zaken

De commissie Digitale Zaken voerde op 22 maart 2022 het commissiedebat Digitale overheid, datagebruik en algoritmen, digitale identiteit. Op de agenda stonden de volgende brieven over het thema digitale identiteit en toegang:

- TK 26643-743 Visiebrief digitale identiteit (11 februari 2021)
- TK 26643-750 Voortgangsrapportage digitale toegang (13 maart 2021)
- TK 22112-3241 Antwoorden op vragen commissie over het fiche: Verordening Raamwerk Europese Digitale Identiteit (29 november 2021)

De commissie Digitale Zaken heeft op 31 mei het commissiedebat Telecomraad gepland staan. Op de agenda van dit debat staat onder meer de Verordening Raamwerk Europese Digitale Identiteit. De commissie Binnenlandse Zaken heeft een schriftelijk overleg gevoerd over het fiche van 22 september 2021. In haar procedurevergadering van 2 december 2021 heeft zij besloten de antwoorden van het schriftelijk overleg over te dragen aan de commissie Digitale Zaken. DiZa heeft de antwoorden betrokken bij het schriftelijk overleg van 24 februari 2022 over de informele Telecomraad 2022 en heeft ze ook geagendeerd voor het commissiedebat over o.a. digitale identiteit, van 22 maart 2022.

De Kamer voert naar verwachting in de week van 16 mei een plenair debat over de novelle Wet Digitale Overheid (Wdo; TK35868). De woordvoerders van de commissie Digitale Zaken zullen waarschijnlijk namens hun fracties de inbreng doen tijdens het plenaire debat.

5.2 Commissie Binnenlandse Zaken

De commissie Binnenlandse Zaken heeft op 28 september 2022 het commissiedebat Basisregistratie Personen en E-id gepland staan. Op de agenda staan de volgende brieven over het thema digitale identiteit en toegang:

- TK 34972-37 Invoering eHerkenning (29 januari 2020)
- 26643-788 Voortgangsrapportage domein Toegang (12 oktober 2021)
- 26643-791 Eindrapport Nederlandse Self Sovereign Identity ecosysteem: Een verkenning van het Nederlandse SSI speelveld, toekomstige ontwikkelrichtingen, impact op publieke waarden en de rol van de Nederlandse overheid (29 oktober 2021)

5.3 Advies

Het onderwerp Digitale Identiteit is een belangrijk maatschappelijk onderwerp. De Tweede Kamer heeft dan ook hiervoor al lange tijd aandacht. Met de komst van de commissie Digitale Zaken constateer ik dat dit onderwerp niet langer alleen bij de commissie Binnenlandse Zaken aan de orde komt. De commissie Digitale Zaken heeft op verschillende relevante kabinetsbrieven en het EU-voorstel over dit onderwerp het voortouw gekregen.

Aangezien het onderwerp Digitale Identiteit de komende jaren in mijn ogen een heel belangrijk en soms ingewikkeld onderwerp blijft, adviseer ik beide commissies om bij relevante brieven over dit onderwerp te blijven afwegen welke commissie een brief als voortouwcommissie zal behandelen. In ieder geval hoop ik dat mijn verslag behulpzaam is in de voorbereiding van commissiedebatten over dit onderwerp bij beide commissies.

Ik adviseer de commissies om de nationale uitwerking van de digitale identiteit nauwgezet te (laten) volgen in het kader van de Kennisagenda (bijvoorbeeld in de vorm van een vervolg op dit rapporteurschap).

Bijlage 1 Wat is een digitale identiteit?

Een digitale identiteit is volgens de staatsecretaris van BZK cruciaal voor de manier waarop wij het vertrouwen borgen dat zo belangrijk is in alle zaken die we zonder persoonlijk contact online met elkaar doen.

Het concept **digitale identiteit** wordt op veel manieren gebruikt. De staatsecretaris verstaat onder digitale identiteit een "verzameling van gegevens die een entiteit (persoon of organisatie) in het digitale domein representeren". Het gaat dus om online identificeren. Voorbeelden van dit type gegevens zijn 1) naam, geboortedatum, adres, 2) statische identificerende gegevens, identifiers (bijvoorbeeld BSN, rekeningnummer, KVK-nummer of telefoonnummer), 3) biometrie (bijv. gezicht of vingerafdruk), 4) certificaten (bijv. diploma's of rijvaardigheid) en 5) dynamische attributen zoals digitale transacties (bijv. bankafschrift). Zonder een betrouwbaar stelsel rond digitale identiteit is het volgens de staatssecretaris moeilijk om de persoon of organisatie met wie we digitaal zaken doen te vertrouwen.

Een ander kernbegrip is **digitale identiteit infrastructuur**. In de Visiebrief definieert de staatsecretaris dit begrip als het geheel van stelsels, afspraken, (beveiligings-) standaarden en voorzieningen, rond de digitale identiteit van personen[3]. Hierin worden drie *functies* onderscheiden, 1) identificatie (wie bent u?), 2) authenticatie (bent u wie u zegt dat u bent?) en 3) autorisatie (bent u geautoriseerd/komt u in aanmerking?). De staatsecretaris onderscheidt vier *rollen* in de digitale identiteit infrastructuur, en benoemt daarbij verschillende *taken en verantwoordelijkheden* die de overheid zal hebben.

Kernpunten uit visiebrief digitale identiteit
De visie van de staatsecretaris op digitale identiteit en de bijbehorende infrastructuur is gebaseerd op vier pijlers. Op de eerste twee pijlers heeft het kabinet reeds activiteiten lopen. De staatsecretaris zegt dat de overheid op de derde en vierde pijler haar activiteiten gaat versterken.

I. **Delen van betrouwbare gegevens** Het fundament van de visie is gebaseerd op een overheid als 'gezaghebbende bron'.[4] Door ook in de digitale

[3] De staatsecretaris laat de identiteit van rechtspersonen buiten beschouwing, hoewel deze visie daar volgens hem wel aan raakt. De redenering hierachter is dat een rechtspersoon of organisatie bij haar handelen altijd wordt 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.

[4] Hierbij zegt de staatssecretaris aan te sluiten 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". De staatsecretaris stelt met deze bronidentiteit een "behapbaardere vorm" voor dan de "online identiteit" als door het betreffende amendement

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[5] en de Europese ambities van de Single Digital Gateway.[6] Deze pijler volgt de activiteiten in het programma Regie op Gegevens en het voorstel van de EU Data Governance Act.

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).[7]
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. (NB dit punt wordt niet verder toegelicht in de visiebrief)

Ontwerpprincipes bij beoogde digitale identiteit infrastructuur
De staatssecretaris benoemt bij de beoogde digitale identiteit infrastructuur ook ontwerpprincipes die gehanteerd worden. Deze zijn hieronder integraal opgenomen.

---

beschreven. De doelen van zelfbeschikking, gegevens kunnen inzien, corrigeren en delen, zegt hij wel te onderschrijven. Zie: Kamerstuk 34972, nr. 20.

[5] Het programma Regie op gegevens heeft als uitgangspunt het vrije verkeer van persoonlijke gegevens goed te regelen op een manier die het vertrouwen van mensen in de samenleving (en de overheid) vergroot en beschermt. Uiteindelijk moet dit resulteren in een generiek sector-overstijgend kader dat veilige, betrouwbare en gebruiksvriendelijke digitale uitwisseling van gegevens tussen overheden, private en maatschappelijke organisaties mogelijk maakt.

[6] De Single Digital Gateway (SDG) geeft burgers en bedrijven makkelijk toegang tot digitale overheidsdienstverlening in de Europese Unie. Dat gebeurt met het portaal (gateway) Your Europe. Deze centrale toegangspoort verwijst gebruikers door naar de juiste websites in de verschillende lidstaten. Dit is bepaald via de Single Digital Gateway-verordening (in oktober 2018 aangenomen door het Europees Parlement). Daarmee heeft Nederland de wettelijke verplichting gekregen de verordening uit te voeren.

[7] eIDAS staat voor 'Electronic Identities And Trust Services'. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen.

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.

Vervolg

De visiebrief van de staatsecretaris bouwt voort op de lijn die is ingezet met de Wdo. De staatssecretaris concludeert: "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."

Bijlage 2 Wat is Self Sovereign Identity?

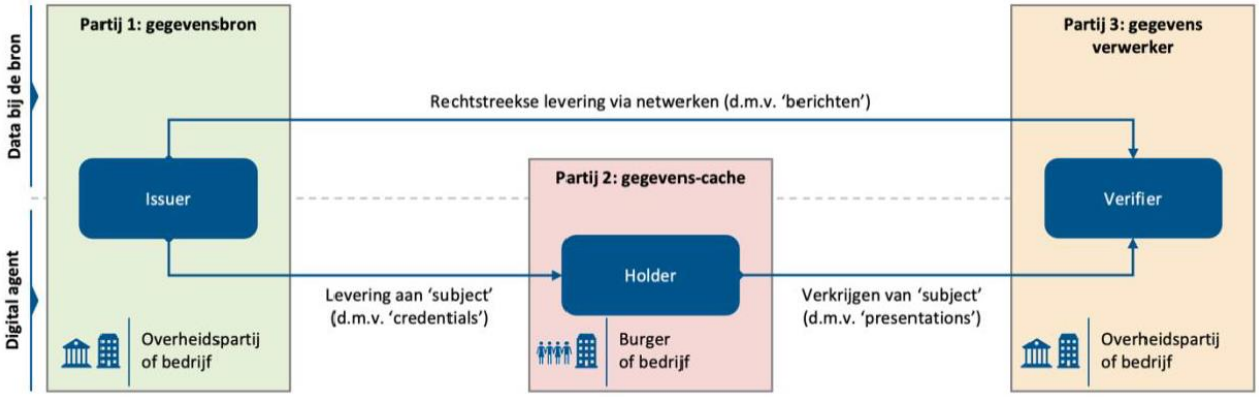
Sinds enkele jaren is een nieuwe manier van denken over digitale identiteit sterk in opkomst. Self Sovereign Identity (SSI) is gebaseerd op het principe dat individuen (en organisaties) controle zouden moeten hebben over hun digitale identiteit en daaraan gerelateerde gegevens, mits zij daartoe gerechtigd zijn. Deze controle en de mogelijkheid om gegevens ter beschikking te kunnen stellen, biedt potentieel verschillende voordelen: optimalisatie van (administratieve) processen waarbij burgers niet langer 'ingewikkelde' elektronische formulieren hoeven in te vullen, het verlagen van validatiekosten, het verhogen van data-kwaliteit, dataminimalisatie en controle over privacy, vergroten van autonomie en transparantie in het digitale domein en het stroomlijnen van dienstverlening.

Hoewel de genoemde potentiële voordelen van SSI niet uitsluitend door middel van SSI te realiseren zijn, kan SSI wel een belangrijke katalysator zijn om deze voordelen te realiseren. Deze aantrekkelijke beloftes rondom SSI zorgen de afgelopen jaren voor veel aandacht en activiteit rondom het onderwerp SSI en digitale gegevensuitwisseling. Er bestaat nog geen eenduidige definitie van Self Sovereign Identity (SSI). TNO INNOPAY noemen in hun rapport over de speelveld van SSI de volgende kenmerken van SSI:

- SSI te maken heeft met een digitale uitwisseling van gegevens over individuen, organisaties, 'things', enzovoorts, waarbij deze gegevens voorzien zijn van bewijzen over zaken als: herkomst, integriteit en dergelijke.
- De uitwisseling van deze gegevens loopt van partijen die ze in de vorm van credentials uitgeven (*Issuers*), via een digital agent (bijvoorbeeld een portemonnee) van betrokkenen (*Holders*) (individuen, maar ook wel organisaties) en onder hun expliciete controle terecht komen bij partijen die deze gegevens nodig hebben (*Verifiers*).
- Dit alles gebeurt zonder dat een Issuer weet heeft van waar (aan welke Verifier) de Holder zijn credentials toont.

Zoals uit onderstaand figuur blijkt kan zo'n digitale gegevensuitwisseling via het voor SSI kenmerkende 'digital agent' interactiemodel plaatsvinden. Binnen de SSI community is een portemonnee een veel voorkomende digital agent, maar ook digitale kluizen of andere personal data management oplossingen kunnen gebruikt worden. Zeker voor (cloud) agents die niet direct op bijvoorbeeld de smartphone of een ander lokaal device opereren, is het wel van belang dat er voldoende waarborgen zijn voor hoe met transacties, kennis of metadata over deze transacties en gegevensuitwisseling omgegaan wordt (bijvoorbeeld welke informatie, attributen of keys worden er in de cloud opgeslagen). Deze waarborgen, die wellicht niet allemaal technisch afgedwongen kunnen worden, kunnen bijvoorbeeld door certificering hard gemaakt worden.
Naast data ophalen via een digital agent kan een *Verifier* gegevens ook rechtstreeks bij de bron ophalen, waarbij afhankelijk van de gevoeligheid van de data mogelijk wel

consent van het individu nodig is (en dus: een voldoende betrouwbare digitale identiteit van de gebruiker). Deze twee methoden zijn niet de enige manier van gegevensuitwisseling (denk aan het posten van een brief), maar wel de twee meest relevante methoden om digitaal gegevens uit te wisselen samen met hun 'kwalificaties'. Deze kwalificaties, zoals 'assurances' en 'proofs', worden altijd meegestuurd.



Bijlage 3 Self Sovereign Identity speelveld

In 2021 heeft de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (BZK), als beleidsverantwoordelijke voor de Nederlandse (digitale) identiteitsinfrastructuur, een visie gepubliceerd over de rol van en houding met betrekking tot digitale identiteit in Nederland. Hierin schetst staatssecretaris dat de overheid een actieve rol voor zichzelf ziet in het creëren van vertrouwen in de digitale wereld voor burgers en bedrijven en het beschikken over een betrouwbare (bron-)identiteit is hierbij cruciaal.

In de visiebrief Digitale Identiteit staat niet omschreven hoe de overheid aankijkt tegen de ontwikkelingen op het gebied van Self Sovereign Identity en hoe zich dat verhoudt tot de visiebrief op Digitale Identiteit. Wel merkt de overheid dat hier vanuit de markt steeds meer behoefte aan is.

BZK heeft INNOPAY en TNO daarom gevraagd inzicht te bieden in de huidige staat van het Nederlandse SSI speelveld, wat de relatie is met digitale identiteit, en hoe dit speelveld zich lijkt te gaan doorontwikkelen. Op basis van deze inzichten doen INNOPAY en TNO aanbevelingen waarmee BZK haar eigen standpunt en beleid rondom SSI kan bepalen en verder concretiseren. INNOPAY en TNO komen tot de volgende conclusies over het SSI speelveld.

Veel SSI experimenten in Nederland, maar landschap is gefragmenteerd
Er is opvallend veel activiteit op het Nederlandse SSI speelveld. Veel verschillende partijen (soms in een cluster met andere partijen) experimenteren binnen hun use cases met het gebruik van verschillende SSI principes, architecturen, infrastructuren, technologieën en diensten. Dit levert een gefragmenteerd landschap op, vooral op de volgende thema's:

- De opvattingen over wat SSI wel/ niet is of zou moeten zijn: Er is veel discussie over de beste of meest zuivere SSI inrichting. Spelers in het speelveld vinden van zichzelf allemaal dat ze "SSI zijn" en soms ook dat andere partijen "geen SSI zijn".
- Opvattingen over wat de nut en noodzaak van SSI is: Voor sommigen is de nut en noodzaak van SSI een principekwestie waarbij traditionele invulling van digitale identiteit volledig zou moeten verdwijnen. Anderen richten zich vooral op het realiseren van waarde voor de burger en de Nederlandse economie waarbij de precieze gekozen inrichting (SSI of niet) van ondergeschikt belang is.
- Diversiteit aan technische inrichting zonder interoperabiliteit: Rondom verschillende oplossingen wordt vooral gekeken naar de technische werking binnen de eigen use case, hierbij is nog weinig oog voor interoperabiliteit met andere oplossingen in andere domeinen.

Sommige partijen binnen het SSI speelveld werken aan een generieke functioneel bouwblok voor SSI, met relatief weinig concrete use cases en betrokken partijen. Daar tegenover staan partijen die een single use case uitwerken en proberen om vanuit daar een springplank te zijn naar opschaling in gebruikers en toepassingen. Daarbij is het logisch dat nu nog verschillende technische inrichtingen bekeken worden. Dat er nu een zekere mate van fragmentatie is op met name technisch vlak, is dan ook niet heel verwonderlijk.

Ook de Nederlandse overheid draagt bij aan de fragmentatie in het speelveld doordat verschillende overheidsorganisaties zonder onderlinge coördinatie experimenteren met SSI-achtige producten. Dit maakt het voor andere spelers in het SSI speelveld alleen maar extra onduidelijk wat de positie en de rol van de overheid is en wat toekomstbestendige inrichtingskeuzes zijn.

In het gefragmenteerde Nederlandse SSI speelveld ontbreekt het nu aan samenhang. Er kan niet gesproken worden van één ecosysteem, partijen concentreren zich rondom verschillende eigen use cases en vormen daarmee verschillende ecosystemen naast elkaar, die vaak ook verschillende, onderling niet-interoperabele technologie gebruiken. SSI Speelveldanalyse (2021)

(Nog) geen kritieke massa individuele leveranciers SSI oplossingen
Het resultaat van het gefragmenteerde landschap is een hoeveelheid aan eilandjes die voor hun specifieke digitale gegevensuitwisselings-use case voor dezelfde uitdaging staan om kritieke massa te organiseren in het samenspel tussen Issuers, Holders en Verifiers. Zolang deze fragmentatie in de SSI markt blijft, zal het voor partijen een uitdaging blijven om netwerkeffecten en groei van hun SSI initiatief rondom de rollen (Issuer, Holder, Verifier) te realiseren, waardoor de maatschappelijke waarde van digitale gegevensuitwisseling niet ten volle gerealiseerd wordt. Dit vergt samenwerking en coördinatie, tussen zowel publieke en private partijen.

SSI gedachtegoed (nog) niet volwassen voor grootschalig gebruik
De fragmentatie komt voort uit de verschillende ideeën over de beste invulling van SSI Leveranciers, bijvoorbeeld op het gebied van technische inrichting en semantiek. Uit de verschillende experimenten is nog geen technische inrichting gekomen waaraan de initiatieven zich in de nabije toekomst zullen conformeren. Bovendien zijn nog niet alle functionele componenten voldoende uitgewerkt. Er is consensus in de markt dat voor een goed functionerend SSI ecosysteem in de Nederlandse maatschappij enkele concepten nog verder onderzocht, ingevuld en geïmplementeerd moeten worden (denk bijvoorbeeld aan zaken als onder curatele of bewind staan, of beperkte handelingsbekwaamheid waardoor mensen een vertegenwoordiger nodig hebben). Dit zijn typisch concepten die niet puur technisch van aard zijn, maar waar juist governance een groot vraagstuk is. Dit maakt dat de initiatieven momenteel nog ongeschikt zijn voor grootschalig gebruik in de maatschappij.

Beschikbaarheid brondata en herbruikbaarheid vormt barrière
Zowel overheid als private partijen bezitten (registers met) brondata die, wanneer een gebruiker hier bijvoorbeeld over zou kunnen beschikken via een digital agent waardevol is voor de optimalisering van bedrijfsprocessen in het private en publieke domein. Digitale gegevensuitwisseling is sterk afhankelijk van de beschikbaarheid van geverifieerde data. Diverse partijen onderzoeken zelfstandig of in samenwerkingsverbanden hoe digitale gegevensuitwisseling al dan niet via SSI op een verantwoorde manier kan gebeuren.

Echter, zolang de daadwerkelijke brondata die via deze systemen ter beschikking moet worden gesteld niet wordt aangeboden, kan er geen waarde uitwisseling plaatsvinden. De overheid heeft de beschikking over zeer diverse datasets over burgers en bedrijven en wordt door spelers in het SSI Speelveld gezien als belangrijke potentiële Issuer voor digitale gegevensuitwisseling.