Verkenning eWallets

Speelveldanalyse

Colofon

DATUM	11 januari 2022
VERSIE	1.0
VERTROUWELIJKHEID	Publiek
STATUS	Definitief
BEDRIJF	Innovalor Advies
AUTEUR(S)	Bob Hulsebosch, Jurjen Braakhekke

Inhoudsopgave

Managementsamenvatting

De in 2014 aangenomen eIDAS verordening (EU) nr. 910/2014 voor een Europees kader voor grensoverschrijdend gebruik van elektronische identiteiten (eIDs) en vertrouwensdiensten heeft niet tot het gewenste succes geleid. Vooral op het vlak van eIDs schiet de implementatie van de verordening tekort: te weinig lidstaten hebben een elektronisch identificatiemiddel Europees laten erkennen voor grensoverschrijdend gebruik (genotificeerd) en te weinig dienstverleners zijn aangesloten op de Europese eIDAS infrastructuur, waardoor de wel erkende eIDs bij onvoldoende diensten in de Europese Unie gebruikt kunnen worden.

De Europese Commissie heeft daarom een wetsvoorstel ingediend tot revisie van de eIDAS verordening om de werking ervan te versterken[1]. Deze verordening heeft onder meer tot doel om te komen tot een raamwerk voor een Europese Digitale Identiteit in de vorm van eWallets. Daarin worden digitale identiteiten opgenomen en gekoppeld met andere digitale gegevens en digitale bewijzen (documenten) die ontsloten kunnen worden via voornamelijk mobiele applicaties. Deze eWallets dienen toegelaten te worden door publieke dienstverleners en door bepaalde private partijen zoals grote platforms en bedrijven die voor hun diensten een hoge mate van identiteitszekerheid eisen.

Een kernfunctionaliteit van eWallets is dat ze de gebruiker op het hoogste betrouwbaarheidsniveau elektronische kunnen identificeren, ofwel authentiseren, op basis van een unieke set van attributen. Daarnaast bieden eWallets de gebruiker de mogelijkheid om extra attributen, attesteringen en credentials[2] bij authentieke bronnen op te halen en deze gecontroleerd te delen met vertrouwende partijen in Europa. Met de komst van de gereviseerde eIDAS verordening worden de technologische en functionele eisen aan eWallets nader gespecificeerd en geharmoniseerd. Daarnaast wordt er een Europees ecosysteem tot stand gebracht van toezicht op eWallets en veilige gegevensuitwisseling.

Hoewel eIDAS niets zegt over de vorm van de eWallets, zal dit in de praktijk vaak neerkomen op een mobiele applicatie die kan worden gebruikt als nationale eID, zowel online als offline, voor zowel publiek als particuliere diensten. eWallets ontvangen hun inhoud van gecertificeerde authentieke bronnen en attribuutproviders. Vertrouwende partijen moeten geregistreerd zijn, zodat eWallets hun authenticiteit kunnen verifiëren. Alle actoren in het eWallet-ecosysteem moeten voldoen aan de technische architectuur, standaarden, referenties en richtlijnen voor het implementeren van eWallets. Deze worden gedefinieerd in de zogenaamde Toolbox, die naar verwachting eind oktober 2022 wordt gepubliceerd. Tegen 30 juni 2024 moet in elk van de lidstaten minimaal één eWallet beschikbaar zijn.

De impact van eWallets op het Nederlandse ecosysteem van digitale identiteiten is nog onduidelijk. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft InnoValor gevraagd een speelveldanalyse op te stellen van ontwikkelingen rondom eWallets in Nederland en Europa, die het mogelijk maakt voor het ministerie om samen met andere departementen, uitvoerders en andere partijen verder beleid te ontwikkelen en verdiepend onderzoek uit te zetten.

Om dit doel te bereiken zijn de volgende analyses uitgevoerd:

1. Definiëring eWallet: Wat is een eWallet en welke eisen stelt de gereviseerde eIDAS verordening er aan?
2. Verschillen eID en eWallets: Hoe verschillen de huidige nationale elektronische identificatie oplossingen (eIDs) en eWallets van elkaar?
3. Huidig speelveld: Hoe ziet het huidige eWallet speelveld eruit in Nederland en Europa?
4. Bredere context: Wat is er al geregeld en onderzocht in voorschriften en standaarden op het terrein van eWallets en wat moet verder worden onderzocht?

Aan de hand van de analyses zijn conclusies getrokken en worden aanbevelingen gedaan. Deze staan hieronder beschreven.

[1] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&from=EN.
[2] Zie Bijlage 3 – Begrippenlijst.

Uitdagingen

Europa heeft grote ambities met het verplicht stellen van eWallets in de herziene eIDAS verordening. De eisen die aan eWallets worden gesteld zijn hoog. Een eWallet moet niet alleen gebruikers elektronisch kunnen identificeren op het hoogste betrouwbaarheidsniveau (authenticatie), maar daarnaast ook nog een veel rijkere set van gegevens (attributen, attesteringen, credentials) over die gebruiker en onder diens regie kunnen uitwisselen met geregistreerde vertrouwende partijen, ofwel dienstverleners. Aangewezen authentieke bronnen dienen voor de aanlevering van de gegevens te zorgen. Het geheel is complex en veelomvattend – zowel technisch, organisatorisch als juridisch – en de voorgestelde tijdspanne voor realisatie is kort. Het is dus zaak voor de Nederlandse overheid en de betrokken stakeholders om doortastend en pragmatisch aan de slag te gaan met de realisatie van een nationaal elektronisch identiteiten ecosysteem waarin eWallets naast andere eID-oplossingen zoals DigiD en eHerkenning opereren.

Het huidige landschap van eWallets is echter nog onvoldoende volwassen om direct een plaatsje in het beoogde ecosysteem voor identiteiten te veroveren. Bestaande eWallets voldoen nog niet aan alle eIDAS eisen voor niveau Hoog en ontberen vertrouwen bij de gebruiker en vertrouwende partijen. Hier zullen nog stappen moeten worden gezet en de voorgestelde eIDAS verordening helpt daarbij significant.

Een andere uitdaging is dat het gebruik van eWallets voor de gebruiker gratis moet zijn. Deze eis zet het verdienmodel voor aanbieders van eWallets onder druk.

Succesfactoren

Het hele speelveld overziend, zijn er drie factoren die essentieel zijn voor het succes van eWallets:

1. De aanwezigheid van authentieke bronnen die (EU-)gestandaardiseerde gegevens (attributen, attesteringen, credentials) over de gebruiker kunnen delen met een eWallet en geverifieerd kunnen worden door vertrouwende partijen. Immers, zonder betrouwbare en gestandaardiseerde gegevens kunnen vertrouwende partijen geen waarde creëren en verliezen eWallets hun meerwaarde. Hoe meer authentieke bronnen beschikbaar komen, des te groter is het aantal use cases dat vertrouwende partijen voor eWallets kunnen ontwikkelen.

2. De aanwezigheid van voldoende publieke en private vertrouwende partijen die gegevens van eWallets willen afnemen om hiermee de gebruiker toegang te geven tot diensten en om persoonlijke dienstverlening op maat aan te bieden. Zonder voldoende afnemende vertrouwende partijen heeft een eWallet voor een gebruiker geen meerwaarde.

3. De aanwezigheid van eWallets die het vertrouwen genieten van gebruikers voor het verwerken van hun gegevens. Immers, als er geen vertrouwen is, zal de gebruiker er niet mee aan de slag gaan en zijn alle investeringen aan de kant van de authentieke bronnen en vertrouwende partijen nutteloos geweest.

Gegeven de complexiteit van de realisatie van deze succesfactoren is een pragmatische en gebalanceerde beleidsmatige aanpak wenselijk. Hierbij dient de overheid een actieve rol te spelen door een gezonde voedingsbodem voor Nederlandse eWallets te realiseren en bovenal de betrokken publieke en private partijen daarbij actief te betrekken. De basisfunctionaliteit van eWallets betreft in ieder geval eID functionaliteit en de attestering van een set verplichte attributen. Door te focussen op ontwikkeling van use cases die voor Nederland relevant zijn kunnen eWallets succesvol worden. Deze use cases bepalen welke authentieke bronnen en vertrouwende partijen moeten worden opgelijnd en waardoor eWallets de mogelijkheid krijgen om te floreren door van meerwaarde te zijn voor eindgebruikers.

Conclusies en aanbevelingen

Voor **authentieke bronnen** doen wij hiervoor de volgende aanbevelingen:

1. Werk uit hoe de minimale set van attributen ten behoeve van eID functionaliteit op eWallets te krijgen. Kan dit middels afgeleide authenticatie met een al genotificeerd middel op eIDAS niveau Hoog (bijvoorbeeld DigiD) of zijn hiervoor andere registratie- en activatieprocessen door de aanbieder van een

eWallet zelf nodig of wenselijk? Is het mogelijk en nodig om BSN op een eWallet te hebben staan? Welke authentieke bronnen zijn hiervoor nodig? Kunnen deze bronnen ook geïnterpreteerde attributen vrijgeven, zoals 16+, 18+ en 65+ in plaats van geboortedatum?
2. Adresseer in de eIDAS Expert Group de wenselijkheid en haalbaarheid van standaardisatie van interfaces in het eWallet ecosysteem, met name ten aanzien van de interactie tussen eWallets en authentieke bronnen.
3. Bepaal welke eWallet use case de meest veelbelovende is voor de Nederlandse markt en welke authentieke bronnen hiervoor nodig zijn. Organiseer dat deze bronnen op tijd klaar zijn met het ontsluiten van de gewenste gegevens richting eWallets en zodanig dat de dienstverleners deze bij ontvangst kunnen verifiëren als authentiek.
4. Beleg de inrichting en het beheer van een register voor authentieke bronnen.

De eisen die worden gesteld aan **eWallets** zijn hoog en complex. Deze eisen komen voort uit de verordening en de uitwerking zal krachtens de verordening plaatsvinden in uitvoeringshandelingen of de Toolbox. De Nederlandse overheid zal deze eisen vervolgens moeten vertalen naar passende eisen voor ons nationale ecosysteem voor digitale identiteiten:

5. Definieer een raamwerk van eisen waaraan Nederlandse eWallets moeten voldoen op basis van de eIDAS Toolbox of uitvoeringshandelingen en op basis waarvan toezicht kan worden uitgevoerd. De kaders hiervoor zijn de eIDAS uitvoeringsverordening 2015/1502 over betrouwbaarheidsniveaus, de cybersecurity verordening en de nog te ontwikkelen Toolbox. Ook dient rekening te worden gehouden met aanpalende kaders zoals de Algemene Verordening Gegevensbescherming (AVG).

Andere eWallet gerelateerde activiteiten die volgen uit de gereviseerde eIDAS verordening zijn:

6. Organiseer een consultatieronde om interesse te peilen bij potentiële eWallet aanbieders. Doe dit tijdig om eWallet aanbieders de mogelijkheid te geven een eWallet te ontwikkelen die aan alle eIDAS eisen voldoet, dan wel om zelf de ontwikkeling van een eWallet te initiëren bij gebruik aan interesse vanuit de markt.
7. Verken de mogelijkheden voor het creëren van vertrouwen in eWallets bij gebruikers.
8. Voer een business case analyse uit op eWallets met eID-Hoog en gekwalificeerde onderteken functionaliteit om de kosten/baten transparant te maken. Probeer eventuele belemmeringen daarbij weg te nemen om zodoende de adoptie van eWallets te bespoedigen.
9. Onderzoek op welke manier identifiers en pseudoniemen en eventuele voorzieningen hiervoor in het Nederlandse ecosysteem voor het linken van digitale identiteiten en eWallets effectief en privacy-vriendelijk kunnen worden ingezet.
10. Onderzoek de voor- en nadelen van het laten doorontwikkelen van de huidige DigiD eID oplossing naar een DigiD eWallet.
11. Onderzoek oplossingen en implicaties voor het digitaal rechtsgeldig ondertekenen van verklaringen door de gebruiker middels een eWallet. Doe dit ook in de context van juridische personen (bedrijven) voor digitale verzegeling.

Betreffende **vertrouwende partijen** ofwel dienstverleners zijn de volgende activiteiten noodzakelijk:

12. Definieer de criteria op basis waarvan Nederlandse vertrouwende partijen gebruik mogen maken van eWallets. Dienen deze partijen, in analogie met bijvoorbeeld DigiD, periodiek een beveiligingsassessment te laten uitvoeren of zijn andere oplossingen mogelijk?
13. Informeer publieke en private vertrouwende partijen die met gegevens uit eWallets aan de slag (willen) gaan. Organiseer hiervoor bijvoorbeeld een overleg met dienstverleners in de publieke en private sector. Deze partijen kunnen zich dan tijdig voorbereiden op pilots met eWallets.
14. Beleg het inrichten en het beheer van een register van vertrouwende partijen en door hen aangeboden diensten.
15. Stem met Nederlandse vertegenwoordigers van de EU Single Digital Gateway (SDG) af waar eIDAS ophoudt en waar SDG begint, zodat vertrouwende partijen weten welke infrastructuur ze moeten gebruiken.

Generieke meer **ecosysteem**-gerelateerde aanbevelingen zijn:

16. Ontwerp de algehele architectuur van het Nederlandse ecosysteem voor digitale identiteiten inclusief eWallets en bijbehorende rollen. Houd rekening met bestaande voorzieningen als DigiD, eHerkenning,

BSNk en BRP-koppelpunt en nieuwe voorzieningen als de diverse registers en eventuele proxies. Doorloop de architectuur aan de hand van een aantal use cases voor eIDAS inkomend en uitgaand verkeer. Maak gebruik van bestaande architecturen zoals ontworpen voor de huidige eIDAS inrichting in Nederland. Breng eventuele risico's in kaart die volgen uit de architectuur, zoals een single-point-of-failure.

17. Verken en borg oplossingen voor het harmoniseren en effectief voeren van toezicht op het Nederlandse digitale identiteiten ecosysteem inclusief eWallets en het gebruik ervan door vertrouwende partijen. Ga daar bij na of en waar het huidige toezicht moet worden aangepast op de wijzigingen die het gevolg zijn van het eIDAS amendement of de uitwerking daarvan in de Toolbox.
18. Breng de gevolgen van eWallets op de bestaande identiteit-gerelateerde gegevensuitwisselingen door overheidsdienstverleners (uitvoeringsorganisaties, de gemeenten en andere medeoverheden) in kaart. Bijvoorbeeld: voorziet de eWallet de overheidsdienstverlener van alle gevraagde attributen, of volstaat de aanlevering van slechts het BSN op basis waarvan de overheidsdienstverlener via de BRP de overige benodigde attributen kan ophalen? De gekozen architectuur voor het ecosysteem is hierop van invloed.
19. Zoek naar oplossingen om alle nieuwe en bestaande stakeholders zoveel mogelijk te betrekken bij de nieuwe inrichting van het Nederlandse ecosysteem voor digitale identiteiten naar aanleiding van de gereviseerde eIDAS verordening om zodoende gezamenlijk daadkrachtig van start te kunnen gaan met pilots en versnippering te voorkomen.
20. Onderzoek de impact van eWallets op het eHerkenning afsprakenstelsel. Is het bijvoorbeeld wenselijk en mogelijk om de huidige machtigingenregisters van eHerkenning te gebruiken als authentieke bronnen voor eWallets?

Voor bijna alle aanbevelingen is het verstandig om te bepalen of de uitkomsten van eventuele vervolgactiviteiten hun beslag moeten krijgen in volgende tranches van de Wet digitale overheid (Wdo).

1 Aanleiding en onderzoeksopzet

1.1 Aanleiding

De huidige eIDAS verordening beoogt een goede werking van de digitale interne markt door met wederzijdse erkenning van elektronische identificatiemiddelen (eID's) en met harmonisatie van vertrouwensdiensten veilige en betrouwbare elektronische transacties tussen burgers, bedrijven en overheden te bevorderen.

Op 3 juni 2021 heeft de Europese Commissie een wetsvoorstel ingediend voor een 'raamwerk voor een Europese Digitale Identiteit', dat de huidige eIDAS-verordening herziet. Voor eID's amendeert het voorstel de huidige eIDAS-verordening in de eerste plaats met de verplichting in plaats van de mogelijkheid van lidstaten om een eID voor burgers en bedrijven te hebben en Europees te laten erkennen. Het huidige proces van wederzijdse erkenning door lidstaten op basis van 'peer review' (notificatie) wordt aangevuld met de mogelijkheid tot nationale certificering, waarbij wordt aangesloten bij de vereisten van de cyberbeveiligingsverordening. Daarnaast wordt verplicht om erkende eID-middelen toe te laten voor offline naast online authenticatie, zowel voor transacties in het publieke domein als in het private domein. Erkenning in het private domein geldt voor de sectoren transport, energie, finance, sociale zekerheid, zorg, drinkwatervoorziening, post, digitale infrastructuur, onderwijs en telecom.

Aanvullend heeft de Commissie een Aanbeveling opgesteld om met de lidstaten een 'Toolbox' te ontwikkelen om de implementatie van het raamwerk voor een Europese Digitale Identiteit, in het bijzonder van zogenaamde European Digital Identity Wallets (hierna eWallets) en gekwalificeerde vertrouwensdiensten, te ondersteunen. In de Toolbox worden de technische architectuur, het referentieraamwerk, gemeenschappelijke standaarden, technische specificaties, gemeenschappelijke richtlijnen en 'best practices' opgenomen.

1.2 Doel en aanpak van het onderzoek

Het doel van het onderzoek betreft het opstellen van een speelveldanalyse van ontwikkelingen rondom eWallets in Nederland en Europa, die het mogelijk maakt voor het Ministerie van BZK om verder beleid te ontwikkelen en verdiepend onderzoek uit te zetten. Om dit doel te bereiken zijn de volgende activiteiten uitgevoerd:

Definiëring eWallet

Door middel van desk research en interviews met stakeholders binnen en buiten de Europese Commissie is vastgesteld hoe het concept van een eWallet eruit ziet en welke eisen door de gereviseerde eIDAS verordening aan eWallets worden gesteld. Hierbij wordt kort ingegaan op beleid en visie van de Nederlandse overheid ten aanzien van eWallets.

Verschil eID en eWallet

In kaart is gebracht op welke punten de huidige nationale elektronische identificatie oplossingen (eID's) en eWallets van elkaar verschillen.

Huidig speelveld

Aan de hand van enkele voorbeelden van eWallets in de Nederlandse en Europese markt en een overzicht van de belangrijkste ontwikkelingen gerelateerd aan het eWallet concept is het huidige speelveld voor eWallets beschreven.

Bredere context

Wat is er al geregeld (en onderzocht) in voorschriften en standaarden op het terrein van eWallets en wat moet verder onderzocht worden? Specifiek om BZK te informeren op welke terreinen onderzoek, beleidsontwikkeling en regelgeving zou moeten plaatsen en in te kaart brengen welke onderdelen nader uitgewerkt en/of besloten moeten worden door lidstaten in samenwerking met de Europese Commissie.

Conclusies en aanbevelingen

Op grond van de analyse van de onderzochte onderwerpen zijn conclusies en aanbevelingen opgesteld ten aanzien van vervolgactiviteiten die BZK kan opnemen.

1.3 Leeswijzer

De hierboven genoemde activiteiten worden per hoofdstuk verder uitgewerkt. Het laatste hoofdstuk trekt conclusies en doet aanbevelingen voor beleidsmatige en inhoudelijke vervolgactiviteiten.

2 Definiëring eWallet

Dit hoofdstuk tracht het concept van eWallets nader te duiden en beschrijft de eisen die in de gereviseerde eIDAS verordening aan eWallets worden gesteld. Op moment van schrijven werkt de eIDAS Expert Group van de Commissie aan het nader definiëren van en het maken van keuzes ten aanzien van diverse aspecten van de eWallet. In het eIDAS amendement wordt gebruik gemaakt van diverse termen die nog niet duidelijk zijn gedefinieerd, zoals 'credentials', 'attributen' en 'persoonsidentificatiegegevens'. Daarnaast is er, afhankelijk van of men kijkt naar de eIDAS definitie van eWallets[3] of de eisen eraan[4] op diverse punten nog onduidelijkheid over wat er daadwerkelijk in een eWallet mag worden opgeslagen en beheerd (zoals attributen, inloggegevens, persoons identificatiegegevens, pseudoniemen en elektronische attesteringen van attributen).

2.1 Europese eWallet

2.1.1 Doelstelling

In de markt zien we een verschuiving van het verstrekken en gebruiken van rigide digitale identiteiten naar het verstrekken van en vertrouwen op specifieke attributen met betrekking tot die identiteiten. Daardoor ontstaat er een toenemende vraag naar digitale identiteitsoplossingen die deze 'personal data management' functionaliteiten kunnen leveren. Dergelijke oplossingen zijn bekend onder diverse noemers, waaronder 'identiteitsportemonnee' of 'wallet'.

Uit de evaluatie van de eIDAS-verordening bleek dat de huidige verordening onvoldoende kan inspelen op deze ontwikkeling, vooral vanwege de beperking tot gebruik in de publieke sector, de complexe mogelijkheden voor private dienstverleners om verbinding te maken met het systeem, de beperkte beschikbaarheid van genotificeerde eID-oplossingen in de lidstaten en het gemis aan flexibiliteit om verschillende gebruiksscenario's te ondersteunen. Bovendien vallen steeds populairder wordende identiteitsoplossingen zoals aangeboden door social media providers van buiten Europa en financiële instellingen buiten de scope van eIDAS, wat leidt tot toenemende zorgen over privacy en gegevensbescherming.

De gereviseerde eIDAS wetgeving heeft onder meer tot doel te voorzien in een European Digital Identity oplossing in de vorm van een eWallet die erkend dient te worden door publieke en private dienstverleners die voor hun diensten een bepaalde mate van identiteitszekerheid nodig hebben. Hoewel eIDAS niets zegt over de vorm van de eWallet zal dit in praktijk veelal neerkomen op een mobiele applicatie, uitgegeven door publieke of private partijen, die kan worden gebruikt als nationale eID, zowel online als offline, voor zowel openbare als particuliere diensten. Met deze Europese eWallet kan de gebruiker:

- Identificatiegegevens en de elektronische attesteringen van attributen veilig opvragen en verkrijgen, opslaan, selecteren, combineren en delen, om online en offline te authentiseren, op een voor hem transparante en herleidbare manier;
- Ondertekenen door middel van gekwalificeerde elektronische handtekeningen en zegels.

De gebruiker in deze kan een natuurlijk persoon, een rechtspersoon of een natuurlijk persoon die een rechtspersoon vertegenwoordigd zijn.

2.1.2 Definitie van eWallet in eIDAS amendement

In het eIDAS amendement wordt een 'European Digital Identity Wallet' gedefinieerd als:

'*een product en dienst dat de gebruiker in staat stelt om identiteitsgegevens, inloggegevens en attributen op te slaan die zijn gekoppeld aan haar/zijn identiteit, deze op verzoek aan vertrouwende partijen te verstrekken en te gebruiken voor authenticatie, online en offline, voor een dienst in overeenstemming met Artikel 6a; en om gekwalificeerde elektronische handtekeningen en zegels te creëren*' [5]

[3] eIDAS ontwerpverordening Art. 3
[4] eIDAS ontwerpverordening Art. 6a
[5] eIDAS ontwerpverordening Art. 3a(42)

Een eWallet is dus een elektronisch identificatiemiddel dat persoonsidentificatiegegevens bevat en dat wordt gebruikt voor authenticatie voor een online of offline dienst. Artikel 6a van het amendement spreekt met betrekking tot de diensten waarvoor een eWallet gebruikt kan worden over:

- het door gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten afgeven van gekwalificeerde en niet-gekwalificeerde elektronische attesteringen van attributen of andere gekwalificeerde en niet-gekwalificeerde certificaten aan de European Digital Identity Wallet;
- het door vertrouwende partijen opvragen en valideren van persoonsidentificatiegegevens en elektronische attesteringen van attributen;
- de presentatie aan vertrouwende partijen van persoonsidentificatiegegevens, elektronische attesteringen van attributen of andere gegevens zoals inloggegevens, in lokale modus waarvoor geen internettoegang voor de portemonnee nodig is.

2.1.3 Basis functionaliteit eWallet[6]

De basis functionaliteit van eWallets betreft de identificatie en authenticatie van gebruikers, het uitwisselen van attributen en credentials, en het voorzien in digitale handtekeningen.

Identificatie en authenticatie

Veilige en vertrouwde toegang tot online diensten door veilige elektronische identificatie en authenticatie vormt de basisfunctionaliteit van eWallets. Deze functionaliteit is relevant voor een groot aantal diensten en entiteiten in verschillende sectoren. Hierbij is een hoge mate van zekerheid voor elektronische identificatie vereist, bijvoorbeeld in de context van onlinediensten met aanzienlijke juridische of financiële risico's, zoals overheidsdiensten, financiën, vervoer en gezondheid. Een eWallet moet elektronische identificatie mogelijk maken wanneer een serviceprovider een sterke gebruikersidentificatie vereist.

Uitwisselen van attributen en credentials

Naast identificatie en authenticatie kan de gebruiker via een eWallet nog extra gegevens (attributen, attesteringen, credentials) uitwisselen met de dienstverlener. Bijvoorbeeld om een rijkere meer op maat gesneden dienst te ontvangen of om toegang te krijgen tot diensten. Voorbeelden hiervan zijn een leeftijdsverklaring (18+), een machtiging, een diploma of een registratie in een beroepsregister. Attributen en credentials zijn te verifiëren door de ontvangende partij.

Digitale handtekening

Het gemakkelijk en naadloos grensoverschrijdend gebruiken van elektronische handtekeningen is een belangrijke facilitator voor de Europese interne markt. De mogelijkheid om op afstand te ondertekenen bespaart tijd en kosten en maakt geavanceerdere online diensten mogelijk. Elektronische handtekeningen zijn relevant voor een groot aantal vertrouwende partijen in verschillende sectoren. eWallets bieden een gebruikersvriendelijke interface/integratie van ondertekeningsoplossingen die door onafhankelijke vertrouwensdiensten kunnen worden aangeboden.

2.1.4 Overige voorgestelde use cases eWallet[7]

Naast de basisfunctionaliteit worden diverse andere use cases voorzien waarvoor eWallets kunnen worden gebruikt. Een aantal van deze use cases zijn aangewezen als prioriteit bij de verdere uitwerking van het eWallet concept tot de zogenaamde Toolbox (zie ook paragraaf 2.4).

Digitaal rijbewijs en mobiliteit (prioriteit)

eWallets maken een volledig digitaal Europees rijbewijs mogelijk, waarvoor op EU-niveau al een wetsvoorstel in voorbereiding is. Een digitaal rijbewijs draagt bij aan een meer efficiënte administratie en procesoptimalisaties door handhavingsinstanties en commerciële entiteiten. Een digitaal rijbewijs zou kunnen worden gekoppeld aan andere attesteringen die worden aangeboden door openbare of particuliere aanbieders, bijvoorbeeld met

[6] ARF nonpaper version 20210930, zie https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6689
[7] ARF nonpaper version 20210930, zie https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6689

betrekking tot wettelijke vereisten (bijv. bewijs van beroepsbekwaamheid) of zakelijke vereisten (bijv. voor tolheffing).

eHealth (prioriteit)

Eenvoudige toegang tot eHealth-gegevens is cruciaal in zowel nationale als grensoverschrijdende contexten. De ervaringen opgedaan in het EU Digital COVID-certificaat initiatief kunnen worden gebruikt voor use cases als het verstrekken van toegang tot digitale patiëntgegevens, vaccinatiekaarten, verzekeringscertificaten, voorschriften, en het mogelijk maken van de verificatie van gezondheidscertificaten. Ook kan een eWallet worden gebruikt om een zorgprofessional toegang te verlenen tot specifieke gezondheidsinformatie. De ePrescription / eDispensation-service van MyHealth@EU kan gebruik maken van een eWallet, waardoor de bruikbaarheid, veiligheid en privacy van deze service wordt verbeterd en de service naar andere landen kan worden uitgebreid. Gezondheidsgerelateerde use cases van een eWallet zouden de kwaliteit van de zorg verhogen en de patiëntveiligheid verbeteren, met name bij reizen naar het buitenland. Deze use cases kunnen worden ontwikkeld in nauwe samenwerking met het e-gezondheidsnetwerk, en meer specifiek de technische subgroep met betrekking tot het gebruik van het EU DCC.

Onderwijs/diploma's (prioriteit)

Het verstrekken van documenten voor kwalificatie-erkenningsprocedures kan kostbaar en tijdrovend zijn voor eindgebruikers, bedrijven en onderwijs- en academische instellingen. Door gebruik te maken van een eWallet kunnen authenticatie processen voor studenten en werknemers worden vergemakkelijkt. Digitale attesteringen waaruit een diploma blijkt kunnen bijvoorbeeld in een verifieerbaar, vertrouwd en consumeerbaar formaat worden gedeeld met een andere onderwijs- of opleidingsinstelling of een derde partij (bijv. een werkgever) in een andere lidstaat dan de lidstaat die het diploma heeft afgegeven. De use case maakt pan-Europese uitwisseling van onderwijsattesten (en mogelijk andere opleidings- en beroepscertificaten) met derden zoals universiteiten of bedrijven mogelijk, waardoor de verificatiekosten aanzienlijk worden verlaagd en het vertrouwen in de authenticiteit en integriteit van documenten wordt verbeterd. De use case kan profiteren van voorbereidend werk dat is uitgevoerd in het kader van het European Blockchain Partnership (EBP) en de European Blockchain Services Infrastructure (EBSI).

Betalingen

Deze use case betreft het hosten van betaalinstrumenten en vergemakkelijken van betalingen tussen portemonneehouders en retailers. eWallets kunnen betalingsauthenticatie met een hoge mate van beveiliging vergemakkelijken en een soepele ervaring bij betalingen mogelijk maken. Deze use case ondersteunt de strategie voor retailbetalingen van de Commissie waarin eIDAS een belangrijke rol speelt[8]. De use case kan worden ontwikkeld in nauwe coördinatie/overleg met de adviesgroepen van de Commissie over retailbetalingen en de retailsector.

Digitale reisdocumenten

Er kunnen digitale reisreferenties (Digital Travel Credentials, DTCs) worden ontwikkeld die op een eWallet worden geladen. DTCs maken naadloos reizen voor alle betrokken partijen mogelijk door identiteit-controlerende procedures in elke fase efficiënter maken. DTCs worden voornamelijk offline gebruikt, net zoals paspoorten, maar kunnen ook online use cases mogelijk maken, zoals vooraf inchecken of de uitgifte van nood-reisdocumenten op afstand.

Digitale machtigingen

Het gebrek aan uniforme grensoverschrijdende digitale presentaties van machtigingen vormt een belemmering voor het functioneren van de Europese interne markt voor met name gebruikers die handelen namens een rechtspersoon. Dit is in de eerste versie van de eIDAS verordening nauwelijks van de grond gekomen. Bedrijven kunnen machtigingen afgeven in de vorm van elektronische attesteringen, die kunnen worden opgeslagen in een eWallet van een vertegenwoordigingsbevoegde werknemer en door hem/haar kunnen worden gebruikt. Dit vereist een overeengekomen semantische weergave van deze machtigingen en vereist dat handelsregisters

[8] Digital finance strategy EU Commission, zie https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52020DC0591&from=EN.

of specifieke machtigingenregisters optreden als authentieke bron hiervoor. Deze use case zal ervoor zorgen dat eWallets geschikt zijn om medewerkers via machtigingen uit dergelijke bronnen namens hun bedrijf diensten te laten afnemen. Een eWallet kan daarnaast ook voorzien in een machtiging van een natuurlijk persoon door een ander natuurlijk persoon. Dit was onmogelijk in de eerste versie van eIDAS.

2.2 Eisen aan eWallets

In de navolgende paragrafen gaan we in op de hoofdlijnen van de eisen die de ontwerpverordening stelt aan eWallets, geordend naar de vier thema's die door de eIDAS Expert Group zijn benoemd voor de verdere uitwerking van het eWallet concept. Voor een gedetailleerd overzicht van eisen wordt verwezen naar Bijlage 1 waarin alle eisen aan eWallets zijn opgenomen, zoals gesteld in de eIDAS ontwerpverordening. In Bijlage 2 is een overzicht opgenomen van alle eisen gesteld aan de lidstaten met betrekking tot eWallets. Op het moment van schrijven worden deze eisen uitgewerkt en nader vastgesteld door de eIDAS Expert Group. Wij hebben onderstaande beschrijving mede gebaseerd op de eerste uitwerking zoals opgesteld in september 2021[9]. Voor de meest actuele beschrijving van de opzet en werking eWallets verwijzen we naar de meest recente publicaties van de eIDAS Expert Group[10].

2.2.1 Verstrekken en uitwisselen van gegevens

Dit betreft de eisen aan de gegevens die in een eWallet kunnen worden opgenomen. De eIDAS ontwerpverordening benoemt hier de volgende categorieën gegevens:

Persoonsidentificatiegegevens

Met persoonsidentificatiegegevens kan een gebruiker zichzelf identificeren (bijv. "Ik ben Leon Azdural, geboren xx/xx/xxxx in xxxx en ik ben Nederlands"). De verordening voorziet niet in elektronische attesteringen van persoonsidentificatiegegevens voor publieke diensten[11]. Echter, vertrouwende partijen en Qualifed Trusted Service Providers (QTSP's) moeten de authenticiteit en geldigheid van persoonsidentificatiegegevens wel kunnen verifiëren.

Persoonsidentificatiegegevens kunnen worden opgeslagen, geselecteerd, gecombineerd, gedeeld door eWallets en worden gepresenteerd/verstrekt aan vertrouwende partijen.

De huidige eIDAS verordening definieert de attributen van de natuurlijke en niet-natuurlijke persoon die uitgewisseld worden: de minimale dataset. De minimale dataset bestaat naast een unieke identificatiecode – de zogenaamde Uniqueness Identifier – uit een aantal verplichte en een aantal vrijwillige attributen. De verplichte set van attributen bestaat uit voornaam, achternaam en geboortedatum. De vrijwillige attributen zijn familienaam, geslacht, geboorteplaats en adres. Daarnaast mogen lidstaten ervoor kiezen om nog extra aanvullende attributen uit te wisselen. Deze zijn niet in de huidige verordening uitgewerkt, maar gaan bij eWallets een nadrukkelijkere rol spelen.

Attributen

Attributen geven kenmerken en kwaliteiten van de gebruiker weer, onafhankelijk van de context, en zijn onvoldoende specifiek om de gebruiker direct te identificeren. Bijvoorbeeld 'Ik ben ouder dan 18 jaar', 'Ik ben een man', 'Ik woon in Amsterdam', ' Ik heb een Nederlands rijbewijs'. Attributen en elektronische attesteringen van attributen kunnen worden opgeslagen, geselecteerd, gecombineerd en gedeeld door eWallets en kunnen worden gepresenteerd aan vertrouwende partijen.

Vertrouwende partijen moeten de authenticiteit van attributen kunnen valideren aan de hand van de authentieke bron, de verordening voorziet dan ook in elektronische attestatie van attributen. In de praktijk komt dit neer op het kunnen controleren van de digitale handtekening van de attestering van de bron door de vertrouwende partij. Indien attributen afkomstig zijn van authentieke bronnen binnen de publieke sector

[9] ARF nonpaper version 20210930, zie https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6689
[10] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3032&fromMeetings=true&meetingId=32634
[11] eIDAS ontwerpverordening Art. 45

moeten gekwalificeerde verleners van elektronische attesteringen van attributen de authenticiteit van de volgende attributen kunnen verifiëren:

- Adres
- Leeftijd
- Geslacht
- Burgerlijke staat
- Gezinssamenstelling
- Nationaliteit
- Onderwijskwalificaties, -titels en -diploma's
- Beroepskwalificaties, -titels en -diploma's
- Openbare vergunningen en licenties
- Financiële en bedrijfsgegevens

Deze attributen vormen de minimale lijst van attributen die eWallets moeten ondersteunen en komen uit Annex VI van de voorgestelde verordening.

Credentials

Credential is een juridische term voor een bewijs van bekwaamheid, ervaring, rechten of toestemming van een persoon. Credentials geven rechten/machtigingen aan die relevant zijn in een specifieke context. Bijvoorbeeld 'Ik mag personen medisch behandelen' of 'Ik ben 18 jaar of ouder (18+)'. Een credential kan worden gezien als een inlogggeven. Voor sommige diensten is het bijvoorbeeld alleen al voldoende om aan te tonen dat de gebruiker ouder dan 18 jaar is. In tegenstelling tot attributen voorziet de ontwerpverordening niet in elektronische attesteringen van credentials. Ook is er geen vereiste dat vertrouwende partijen of QTSPs de authenticiteit en geldigheid van credentials moeten kunnen valideren/verifiëren.

Credentials kunnen door eWallets worden opgeslagen en aan vertrouwende partijen worden gepresenteerd/verstrekt.

Overige gegevens

Naast voornoemde gegevens kunnen eWallets overige gegevens verwerken. Elektronische attesteringen van overige gegevens zijn niet vereist in de ontwerpverordening. Ook is er geen vereiste dat vertrouwende partijen of QTSPs de authenticiteit en geldigheid van overige gegevens moeten kunnen valideren/verifiëren.

Overige gegevens kunnen door eWallets worden opgeslagen en aan vertrouwende partijen worden gepresenteerd/verstrekt.

Interfaces

Het verstrekken en uitwisselen van gegevens door eWallets verloopt via interfaces. Op moment van schrijven zijn interfaces voorzien voor o.m:

- Het opvragen van persoonlijke identificatiegegevens van de gebruiker via een interface van de eWallet met officiële ID-documenten;
- Het vanuit eWallets delen van elektronische identificatie, gekwalificeerde elektronische handtekeningen en EAAs (gekwalificeerd en niet-gekwalificeerd) met vertrouwende partijen;
- Het door eWallets ophalen van gekwalificeerde en niet-gekwalificeerde elektronische attesteringen van attributen, via een interface met gekwalificeerde en niet-gekwalificeerde aanbieders van elektronische attesteringen van attributen, op een synchrone of asynchrone manier;
- Hergebruik van bestaande elektronische identiteiten van de gebruiker (bijvoorbeeld om een elektronische identiteit binnen een eWallet te genereren op basis van een eerder bestaand elektronisch identificatiemiddel, of om deze te gebruiken voor authenticatie/identificatie), via een interface met aangemelde eID-schema's;
- Het opslaan van gegevens in een gekwalificeerd grootboek, via een interface met een gekwalificeerde grootboek dienstverlener.

Het eIDAS amendement benoemt dat er 'gemeenschappelijke' (lees: standaard) interfaces[12] moeten zijn:

- tussen vertrouwensdiensten en eWallets;
- tussen vertrouwende partijen en eWallets;
- tussen vertrouwensdiensten en vertrouwende partijen.

Over standaardisatie van de overige interfaces doet het eIDAS amendement geen uitspraken. De standaardisatie van de in Art. 6b benoemde interfaces wordt op moment van schrijven door de eIDAS Expert Group uitgewerkt als onderdeel van de Toolbox ontwikkeling. Mogelijk worden in de Toolbox ook voor de overige interfaces standaarden vastgesteld.

eWallets stellen de gebruiker ook in staat om gekwalificeerde elektronische handtekeningen aan te maken:

- Ofwel door het gebruik van een lokaal token (smartcard, SIM, …);
- Of via een interface met een gekwalificeerde dienst voor het beheer van apparaten voor het maken van elektronische handtekeningen op afstand.

2.2.2 *Functionaliteit en beveiliging*

Functionaliteit van eWallets

Een eWallet kan worden gebruikt door zowel natuurlijke personen als rechtspersonen. De gebruiker kan diens eWallet online en offline gebruiken, voor publieke en private diensten. Hiertoe bieden eWallets de volgende functionaliteiten:

- Elektronische identificatie en authenticatie met een hoog betrouwbaarheidsniveau, inclusief het verstrekken van een unieke en persistente identifier;
- Elektronische authenticatie met betrouwbaarheidsniveau hoog, zonder de identiteit van de gebruiker bekend te maken (anonieme authenticatie of authenticatie onder een pseudoniem).
- Uitgifte van gekwalificeerde elektronische handtekeningen;
- Opvragen, opslaan en delen van niet-gekwalificeerde en gekwalificeerde elektronische attesteringen van attributen;
- Opslag van identiteitsgegevens, inloggegevens, attributen van de gebruiker;
- Toestemming krijgen van de gebruiker om handelingen uit te voeren (delen van attributen, elektronische identificatie & authenticatie);
- Authentiseren van andere partijen zoals vertrouwende partijen en vertrouwensdiensten;
- Opslag van bewijsmateriaal voor geschillenbeslechting;
- Mechanismen om de traceerbaarheid en koppelbaarheid van gebruik van eWallets zoveel mogelijk te reduceren;
- Overdraagbaarheid naar andere apparaten (inclusief back-up en herstel van eWallets functionaliteiten).

De nadere duiding van de functionaliteit en beveiliging van eWallets is op het moment van schrijven nog in volle ontwikkeling binnen de eIDAS Expert Group.

Niet-functionele aspecten van eWallets

eWallets zorgen voor volledige controle van de gebruiker over zijn gegevens en het gebruik van de wallet. Om de gebruiker in staat te stellen alleen die informatie te delen die hij wenst te delen maken eWallets gebruik van de modernste protocollen met betrekking tot privacy (bijvoorbeeld 'zero knowledge proof'). De gebruiker wordt geïnformeerd over alle handelingen die hij uitvoert met zijn eWallet.

eWallets dienen toegankelijk te zijn voor personen met een handicap, in overeenstemming met de toegankelijkheidseisen van Bijlage I bij Richtlijn 2019/882.

eIDAS vereist verder dat het gebruik van eWallets gratis is voor natuurlijke personen.

[12] eIDAS ontwerpverordening Art 6b

Beveiliging

Kritieke componenten die in eWallets zijn geïntegreerd of door eWallets worden gebruikt en die misbruik of wijziging van de identificatiegegevens, authenticatiemechanismen of toestemmingsmechanismen mogelijk zouden maken, moeten worden gecertificeerd door een overheidsinstantie volgens een relevante certificeringsregeling die is vastgelegd in de Cyberbeveiligingswet.

Indien reeds bestaande certificeringsschema's niet geschikt zijn voor eWallets, wordt een specifiek certificeringsschema voor de kritieke componenten van eWallets gespecificeerd, rekening houdend met de belangrijkste typen implementaties die in de lidstaten zijn voorzien, en waar nodig vertrouwend op bestaande certificeringsschema's.

De veiligheidscertificering moet er met name voor zorgen dat het authenticatiemechanisme voldoet aan de vereisten van betrouwbaarheidsniveau Hoog zoals gedefinieerd in CIR 2015/1502. Smartcards, tokens of ingebouwde beveiligde elementen moeten worden gecertificeerd volgens het EU CC-certificeringsschema.

Tenslotte wordt vereist dat persoonsgegevens met betrekking tot de levering van eWallets fysiek en logisch gescheiden van alle andere gegevens worden opgeslagen.

2.2.3 Betrouwbare identiteitsvaststelling

eWallets worden uitgegeven in het kader van genotificeerd elektronisch identificatiesysteem met een betrouwbaarheidsniveau Hoog. eWallets dienen te voldoen aan de ongewijzigde vereisten van eIDAS Artikel 8 met betrekking tot het betrouwbaarheidsniveau Hoog, met name zoals vereist voor identiteitsbewijs en -verificatie, en het beheer en de authenticatie van elektronische identificatiemiddelen.

eWallets dienen ervoor te zorgen dat de persoonsidentificatiegegevens op unieke en permanente wijze de natuurlijke of rechtspersoon vertegenwoordigen die ermee in verband wordt gebracht. De lidstaten dienen daartoe in de minimumreeks persoonsidentificatiegegevens die een natuurlijke of rechtspersoon op unieke wijze vertegenwoordigen een unieke en persistente identificatiecode op te nemen.

Er dient een mechanisme te bestaan om ervoor te zorgen dat de vertrouwende partij de gebruiker kan authentiseren en elektronische attesteringen van attributen kan ontvangen.

2.2.4 Governance

Om ervoor te zorgen dat alle natuurlijke en rechtspersonen in de Unie veilige, betrouwbare en naadloze toegang hebben tot grensoverschrijdende openbare en particuliere diensten, geeft elke lidstaat binnen twaalf maanden na de inwerkingtreding van de verordening een Europese digitale identiteitsportemonnee uit. De conformiteit van European Digital Identity Wallets met de vereisten zoals gesteld in eIDAS wordt gecertificeerd door geaccrediteerde, door de lidstaten aangewezen publieke of private instanties.

Lidstaten moeten voorzien in valideringsmechanismen voor eWallets zodat:

1. de authenticiteit en geldigheid van eWallets kan worden geverifieerd;
2. vertrouwende partijen kunnen verifiëren dat de attesteringen van attributen geldig zijn;
3. vertrouwende partijen en gekwalificeerde vertrouwensdienstverleners de authenticiteit en geldigheid van persoonsidentificatiegegevens kunnen verifiëren.

Net als bij de huidige eIDs, dienen lidstaten voorzieningen te treffen voor het opschorten of intrekken van eWallets in het geval van enige vorm van compromittering. Andere lidstaten dienen hiervan in kennis te worden gesteld.

Wanneer een vertrouwende partij wil gaan vertrouwen op eWallets moet hij dat mededelen aan de Lidstaat waar hij is gevestigd. Hierbij moet ook het beoogde gebruik van eWallets worden gemeld[13]. De lidstaten voeren een gemeenschappelijk mechanisme in voor de authenticatie van vertrouwende partijen.

[13] eIDAS ontwerpverordening Art. 6b

European Digital Identity Wallets die gecertificeerd zijn of waarvoor een conformiteitsverklaring is afgegeven in het kader van een cyberbeveiligingsregeling op grond van Verordening (EU) 2019/881 en waarvan de referenties zijn gepubliceerd in het Publicatieblad van de Europese Unie dienen te voldoen aan de cyberbeveiligingsrelevante vereisten van artikel 6 bis, leden 3, 4 en 5, voor zover het cyberbeveiligingscertificaat of de verklaring van conformiteit dit vereisen.

Vertrouwensdiensten van gekwalificeerde attesteringen van attributen mogen geen informatie kunnen ontvangen over het gebruik van deze attributen.

Uitgevers van eWallets mogen geen informatie vastleggen over het gebruik van de wallet die niet nodig is voor het verlenen van de walletdiensten. Ook mogen zij persoonsidentificatiegegevens en andere persoonlijke gegevens die verband houden met het gebruik van eWallets niet combineren met persoonsgegevens van andere diensten, tenzij de gebruiker hier uitdrukkelijk om heeft verzocht. Op basis van toestemming bestaat dus de mogelijkheid voor wallet uitgevers om eWallet-functionaliteit te combineren met of te integreren in andere (persoonlijke) toegevoegde waarde diensten.

2.3 Analyse

eWallet is een complex en functioneel rijk concept voor identificatie en authenticatie waarmee een breed scala aan use cases kan worden verbeterd of mogelijk worden gemaakt. De grootste verschillen met het huidige eIDAS identity framework zijn gelegen in het feit dat een eWallet veel meer functionaliteit biedt dan een eID, en het feit dat eWallets ook door de private sector mogen worden gebruikt. Hierdoor ontstaan tal van kansen voor de ontwikkeling van nieuwe innovatieve digitale diensten waarbij identificatie, authenticatie en attestatie van attributen van gebruikers een rol spelen. Dit vereist dat ook economische aspecten goed moeten worden meegenomen bij het ontwerp en de implementatie van eWallets in Nederland. Mede omdat het gebruik ervan bij grensoverschrijdende transacties gratis moet zijn.

Een belangrijke functionaliteit van eWallets is het kunnen authentiseren van gebruikers. Daardoor is een eWallet (ook) een eID-middel en komt het naast de huidige (genotificeerde) eID-middelen, zoals DigiD en eHerkenning, te staan. Dit betekent ook dat eWallets een minimale reeks van identificerende attributen moeten bevatten om een natuurlijk persoon of rechtspersoon op unieke en permanente wijze te identificeren. Uitgangspunt is betrouwbaarheidsniveau Hoog; een niveau dat binnen DigiD en eHerkenning wel mogelijk is, maar nog geen grote mate van adoptie kent. De eerste Nederlandse identiteitskaarten (eNIK) waarmee inloggen met DigiD Hoog mogelijk is, zijn pas in 2021 uitgeven en kennen nog een lage dekkingsgraad[14]. Ook eHerkenning kent middelen op betrouwbaarheidsniveau Hoog (eH4); het gebruik ervan is echter minimaal. Een belangrijke reden voor het beperkte gebruik zijn met name de hoge kosten van het middel door de hoge mate van beveiliging en de identiteitszekerheid die nodig zijn. Gewaakt dient te worden dat de ontwikkeling van eWallets niet eenzelfde lot ondergaat.

Complexiteit

Het gebruik van unieke identifiers en pseudoniemen is een belangrijke randvoorwaarde voor het betrouwbaar borgen van de privacy van gebruikers. Immers, hiermee wordt het linken van presentaties van identiteiten en attributen uit eWallets door verschillende vertrouwende partijen waar wenselijk onmogelijk gemaakt. Het aanmaken, beheren en uitgeven van identifiers en pseudoniemen voor eWallets kent de nodige uitdagingen en de architectuur hiervoor is nog niet vastgesteld. Mogelijk komt er een unieke Europese persistente identifier. Hoe verhoud deze identifier zich bijvoorbeeld tot het BSN en waarvan het gebruik is gebonden aan strikte wettelijke kaders. Bijkomende complexiteit is ook dat eHerkenning en DigiD gebruik maken van zogenaamde polymorfe pseudoniemen. Dergelijke pseudoniemen maken het mogelijk voor ontvangende partijen om de gebruiker uniek te kunnen identificeren en zodanig dat de privacy van de gebruiker maximaal is geborgd. Een nadeel van polymorfe pseudonimisering is dat de ontvangende partij hiermee cryptografisch overweg moet kunnen gaan. In Nederland is dit te regelen, op Europese schaal zal dat lastig zijn. Of en hoe polymorfe pseudoniemen van nut kunnen zijn bij eWallets is nog onduidelijk.

Europese gebruikers kunnen met hun eWallets gebruik maken van Nederlandse publieke diensten. Met name overheidsdiensten zijn ingericht op het ontvangen van een BSN hiervoor. Bij de huidige genotificeerde eIDAS

[14] Veilig inloggen met DigiD op eNIK, zie https://www.digitaleoverheid.nl/nieuws/veilig-inloggen-op-digi-d-met-enik/.

eID-middelen voorziet het BRP-koppelpunt in het koppelen van een BSN aan het buitenlandse eID[15]. Met eWallets zal dit minder eenvoudig te realiseren zijn omdat deze de authenticatie- en overige gegevens direct delen met de dienstverlener, zonder tussenkomst van een eIDAS-node of BRP-koppelpunt.

Standaardisatie

Zoals beschreven is standaardisatie van interfaces in het eWallet ecosysteem alleen wettelijk vereist voor de interactie tussen eWallets, vertrouwensdiensten en vertrouwende partijen[16]. Afhankelijk van de mate waarin de Toolbox ook voor andere interfaces standaarden vaststelt kan dit leiden tot nationale verschillen tussen eWallets. Bijvoorbeeld ten aanzien van de interactie tussen eWallets en de authentieke bronnen in de verschillende lidstaten.

Zo zou de situatie kunnen ontstaan dat een eWallet wel kan omgaan met bijvoorbeeld Duitse authentieke bronnen maar niet met Nederlandse authentieke bronnen, afhankelijk van de keuzes die een aanbieder maakt voor zijn eWallet. Illustratief voor de problemen die hierdoor kunnen ontstaan is de recente situatie rondom het halen van een Corona boosterprik door Nederlandse burgers in Duitsland en de registratie hiervan[17]. Dergelijke buitenlandse prikken verschijnen niet bij het vaccinatiebewijs in de CoronaCheck-app.

Bij het ontbreken van EU-brede standaards voor de interactie tussen eWallets en authentieke bronnen wordt de mate waarin een eWallet bruikbaar is in meerdere lidstaten en voor meerdere use cases bepaald door marktwerking; sterk internationaal georiënteerde aanbieders van eWallets zullen wellicht meerdere interface implementaties/standaarden willen ondersteunen, terwijl andere aanbieders zich zouden kunnen beperken tot implementatie van alleen die interfaces die worden gebruikt in specifieke lidstaten. In theorie kan de situatie ontstaan dat er alleen eWallets verschijnen die zich beperken tot ondersteuning van alleen de authentieke bronnen in de eigen lidstaat. Dit zou de doelstellingen van het EU Digital Identity Framework aanzienlijk schaden.

Toezicht

Tot slot benoemen we nog het toezichthoudende regime over eWallets. Naast het huidige proces van peer reviews voor erkenning van eID-middelen is er nu ook een mogelijkheid voor nationale certificering. Het proces van nationale certificering lijkt op het huidige proces voor eIDAS QTSPs, waarbij een zogenaamde conformiteitsbeoordelaar de QTSP beoordeel*t* op de eIDAS en onderliggende ETSI eisen en de nationale toezichthouder uiteindelijk besluit of de QTSP op de vertrouwenslijst komt te staan en erkend dient te worden door alle partijen in Europa. Een soortgelijk proces is ook denkbaar voor een eWallet. Voor het beoordelen van de eID-functionaliteit kan de conformiteitsbeoordelaar putten uit de eisen in eIDAS 2015/1502; voor de andere meer generieke eWallet functionaliteiten ontbreken de kader*s* nog. Het is de verwachting dat deze binnen de Toolbox worden ontwikkeld door de EU Expert Group (zie sectie 3.2). Een bijkomende complexiteit is de eis dat aangesloten dient te worden bij de vereisten van de cyberbeveiligingsverordening. De vraag is of een conformiteitsbeoordelaar in staat is en geaccrediteerd is om op een dergelijk breed kader een uitspraak te doen over de betrouwbaarheid van een eWallet. Daarbij rijst ook de vraag of een eWallet aanbieder bereid is de significante kosten hiervoor te betalen.

Daarnaast ontstaat de onwenselijke situatie van een dubbel toezichthoudend regime op eID-middelen: voor DigiD en eHerkenning eenmalig via een peer review en notificatieproces, en voor de eID-functionaliteit van eWallets periodiek via nationale certificering.

Ten aanzien van het toezicht op het gebruik van eWallets stelt eIDAS dat vertrouwende partijen zich als zodanig moeten laten registreren zodat eWallets kunnen controleren of een partij wel gemachtigd is om gegevens uit een eWallet op te vragen. De vraag is of en hoe vertrouwende partijen (periodiek) moeten worden gecontroleerd op het voldoen aan eisen gesteld aan het gebruik van eWallets, bijvoorbeeld ten aanzien van de authenticatie van persoonsidentiteitsgegevens en de bescherming tegen fraude en onrechtmatig

[15] BRP-koppelpunt (BRPk), zie https://www.rvig.nl/digitale-identiteit/brpk.
[16] eIDAS ontwerpverordening Art. 6a
[17] "GGD adviseert: haal geen boosterprik in het buitenland", RTL nieuws, 26 december 2021, zie https://www.rtlnieuws.nl/nieuws/nederland/artikel/5277020/ggd-advies-haal-geen-boosterprik-buitenland-duitsland-grens.

gebruik van identiteitsgegevens. DigiD doet dit middels de jaarlijkse DigiD ICT-beveiligingsassessments op basis waarvan Logius toezicht houdt op de DigiD-aansluitingen met vertrouwende partijen[18]. eHerkenning kent een lichte toets door de makelaar voor opname van de vertrouwende dienst in de dienstencatalogus[19]. Een dergelijk intake-proces is ook denkbaar voor vertrouwende partijen en hun diensten die gebruik maken van eWallets. Daar komt bij dat eWallets het voor gebruikers heel inzichtelijk moeten maken welke gegevens in welke context door wie worden opgevraagd; hierdoor zullen kritische gebruikers de facto een deel van de controle op het gebruik van eWallets door vertrouwende partijen voor hun rekening nemen. Het inrichten en communiceren van een 'meldpunt eWallets' kan dit proces in belangrijke mate faciliteren. Op basis hiervan en vergelijkbaar met GDPR kunnen nationale autoriteiten misstanden rond het gebruik van eWallets aankaarten bij vertrouwende partijen.

Vervolgactiviteiten

Concreet leidt deze bovenstaande analyse tot de volgende verdiepende vervolgactiviteiten:

1. Voer een business case analyse uit op eWallets met eID-Hoog en gekwalificeerde onderteken functionaliteit om de kosten/baten transparant te maken. Probeer eventuele belemmeringen daarbij weg te nemen om zodoende de adoptie van eWallets te bespoedigen.
2. Onderzoek op welke manier identifiers en pseudoniemen en eventuele voorzieningen hiervoor in het Nederlandse ecosysteem voor het linken van digitale identiteiten en eWallets effectief en privacy-vriendelijk kunnen worden ingezet.
3. Adresseer in de Expert Group de wenselijkheid en haalbaarheid van standaardisatie van interfaces in het eWallet ecosysteem, met name ten aanzien van de interactie tussen eWallets en authentieke bronnen.
4. Verken en borg oplossingen voor het harmoniseren en effectief voeren van toezicht op het Nederlandse digitale identiteiten ecosysteem inclusief eWallets en het gebruik ervan door vertrouwende partijen.

[18] DigiD ICT-beveiligingsassessments, zie https://logius.nl/diensten/digid/ict-beveiligingsassessments-digid.
[19] eHerkenning dienstencatalogus, zie https://eherkenning.nl/nl/voor-dienstverleners/aansluiten/handleidingen-en-ondersteuning en https://afsprakenstelsel.etoegang.nl/display/as/Proces+doorvoeren+nieuwe+dienstencatalogus.

3 eWallet ecosysteem

Wij beschrijven hier een eerste beeld van de rollen en processen rond eWallets. Deze rollen en processen worden de komende maanden door de eIDAS Expert Group verder uitgewerkt en vastgesteld. Op het moment van schrijven zijn verschillende onduidelijkheden en tegenstrijdigheden nog onderwerp van afstemming in de Expert Group. Voor de meest actuele beschrijving van de opzet en werking van het eWallet ecosysteem verwijzen wij naar de meest recente publicaties van de Expert Group.

Ook gaan wij in op de planning en aanpak van de implementatie van eWallets en het ecosysteem in de lidstaten, in het bijzonder in Nederland.

3.1 eWallet ecosysteem

Het concept eWallet ecosysteem door de EU Commissie beschreven in het non-paper "European Digital Identity Architecture and Reference Framework" (versie 20210930)[20]. Dit non-paper is gebruikt voor de onderstaande beschrijving van het ecosysteem.

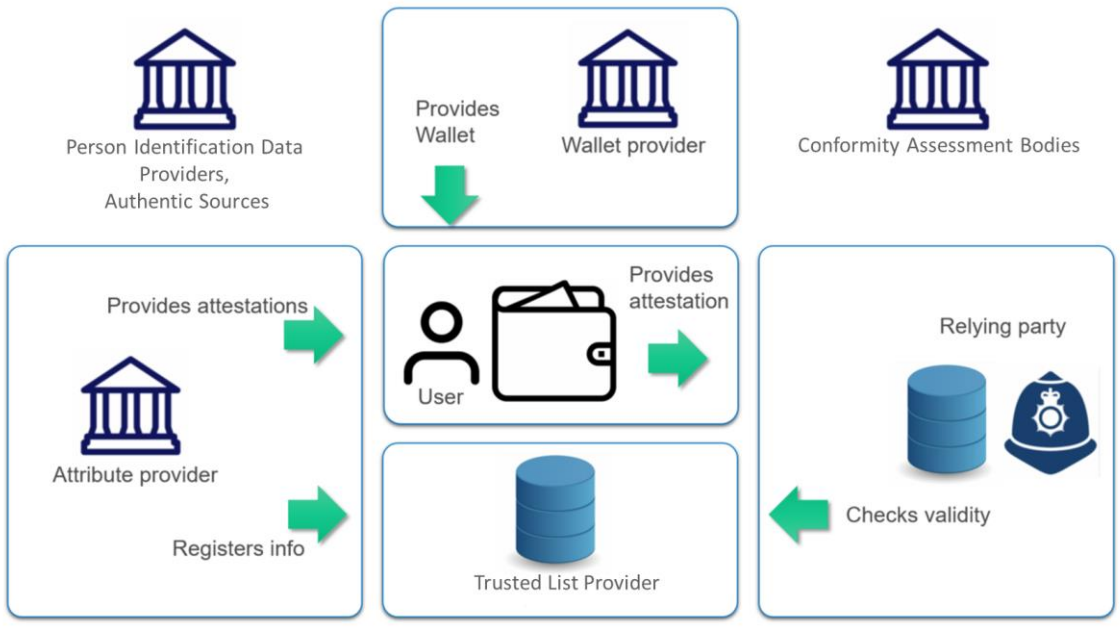
Voor de werking van eWallets zijn een groot aantal actoren vereist die in samenwerking en onderlinge afhankelijkheid de processen uitvoeren die nodig zijn voor:

- De uitgifte van eWallets;
- Het verstrekken van gegevens aan eWallets;
- Het uitwisselen van gegevens tussen eWallets en vertrouwende partijen;
- De verificatie van de ontvangen gegevens door vertrouwende partijen.

We beschrijven eerst de belangrijkste rollen en gaan daarna in op deze processen.

3.1.1 Rollen in het eWallet ecosysteem

Onderstaand diagram geeft een vereenvoudigd overzicht van het eWallet ecosysteem.



Figuur 1: Vereenvoudigde weergave European Digital Identity Wallet ecosyteem.

[20] ARF nonpaper version 20210930, zie https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6689

In dit ecosysteem zijn de volgende rollen te onderscheiden:

Eindgebruikers van Wallets ('User')

Eindgebruikers van eWallets zijn natuurlijke personen of rechtspersonen die eWallets gebruiken om attesteringen inclusief attributen te ontvangen, op te slaan en te presenteren aan vertrouwende partijen ('relying parties'), waarmee zij hun identiteit of een bepaald attribuut kunnen bewijzen.

Wallet Providers

eWallet aanbieders zijn lidstaten, of andere organisaties die gemachtigd of erkend zijn door de lidstaten, die eWallets beschikbaar maken voor gebruikers.

Person Identification Data Providers

Uitgevers van persoonsidentificatiegegevens (PID) verstrekken persoonsidentificatiegegevens veilig aan eWallets (in een geharmoniseerd gemeenschappelijk formaat) en bieden een voorziening om de geldigheid van deze gegevens te verifiëren. Het zullen doorgaans dezelfde organisaties zijn die vandaag de dag de officiële identiteitsdocumenten afgeven. Interessant om te melden is dat deze rol niet expliciet in de verordening wordt vermeld.

Authentieke Bronnen (Authentic Sources)

Authentieke Bronnen zijn die bronnen die wettelijk zijn aangewezen om gegevens te bewaren over een gedefinieerde reeks attributen, waaronder bijvoorbeeld adres, leeftijd, geslacht, burgerlijke staat, gezinssamenstelling, nationaliteit, titels en licenties voor onderwijskwalificaties, titels en licenties voor beroepskwalificaties, openbare vergunningen en licenties, en financiële en bedrijfsgegevens.

Elektronische Attestering van Attributen (EAA) Providers

Deze dienstverleners geven elektronische attesteringen van attributen (EAAs) af. Net als bij andere vertrouwensdiensten kunnen EAAs gekwalificeerd zijn (QEAA) zijn en worden uitgegeven door gekwalificeerde EAA-providers (QEAAPs), of niet-gekwalificeerd zijn en worden uitgegeven door gekwalificeerde of niet-gekwalificeerde providers. De vereisten die van toepassing zijn op alle huidige eIDAS (gekwalificeerde) vertrouwensdiensten zijn ook van toepassing op (Q)EAAPs en de (Q)EAAs die ze bieden.

Vertrouwende Partijen (Relying Parties, RPs)

Vertrouwende partijen vragen identiteitsgegevens, inloggegevens en attributen aan eWallets. Enkele belangrijke eisen waaraan zij moeten voldoen zijn de volgende. RPs zijn verantwoordelijk voor het verifiëren van deze gegevens. Om op eWallets te kunnen vertrouwen moeten RPs de lidstaat waar ze zijn gevestigd informeren over het beoogd gebruik van eWallets. RPs kunnen nodig zijn om de identiteit van eWallet-gebruikers te matchen met bestaande Conformiteitsbeoordelingsinstanties (CBI). De lidstaten implementeren een gemeenschappelijk mechanisme voor de authenticatie van RPs.

Trusted Lists Providers (TLPs)

De status van een gekwalificeerde vertrouwensdienst in het ecosysteem moet op een betrouwbare manier kunnen worden geverifieerd. Hiertoe moet de gekwalificeerde status van de dienstverlener door de lidstaten worden vastgelegd in vertrouwenslijsten.

Conformiteitsbeoordelingsinstanties

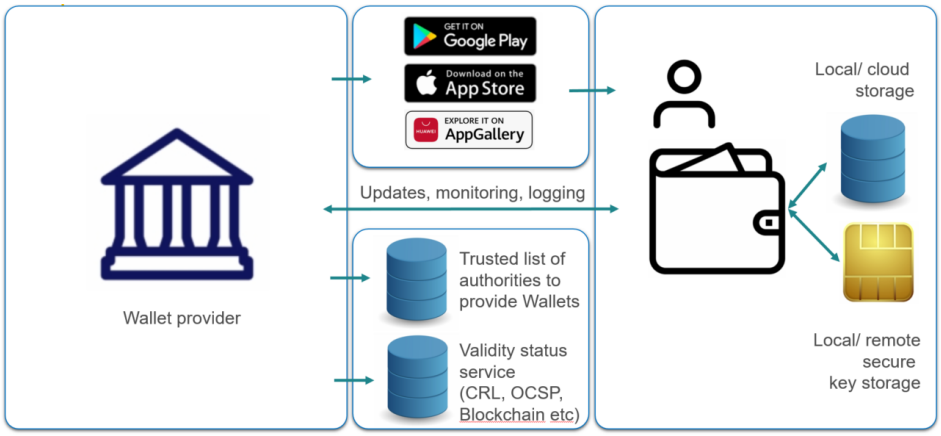
De eWallets en de QEAAP's moeten gecertificeerd zijn. Conformiteitsbeoordelingsinstanties (CBI's) worden door de lidstaten geaccrediteerd als verantwoordelijke voor het uitvoeren van beoordelingen waarop de lidstaten vertrouwen voordat ze een Europese eWallet uitgeven of de gekwalificeerde status aan een aanbieder van vertrouwensdiensten verstrekken.

Naast de beschreven rollen zijn ook andere actoren actief in het ecosysteem, ondersteunend aan de beschreven rollen. Bijvoorbeeld cloud serviceproviders, eiDAS nodes, ledger services en andere spelers die functionaliteiten van eWallets verzorgen. In de Toolbox moeten de rollen van en eisen aan dergelijke actoren nog worden vastgesteld. Op dit moment laten wij hen daarom buiten beschouwing.

3.1.2 Processen in het eWallet ecosysteem

Bij het gebruik van eWallets worden de volgende processen onderscheiden:

Uitgifte van eWallets

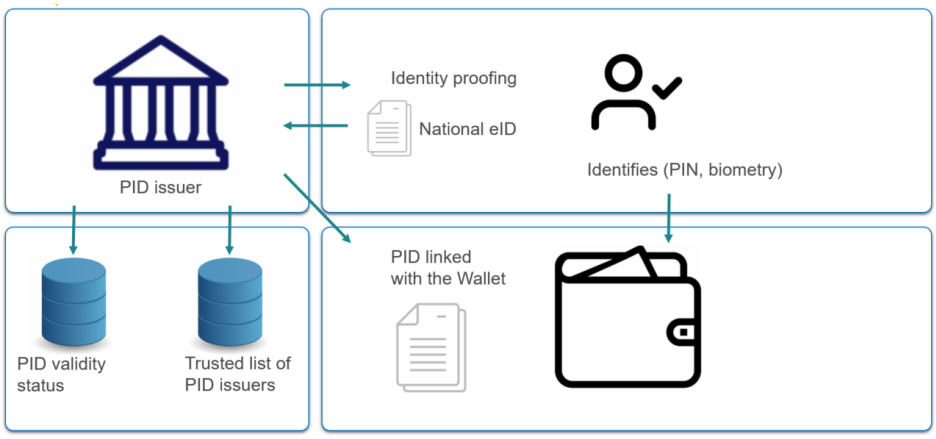


Figuur 2: Proces Uitgifte van eWallets.

eWallets worden typisch geleverd als mobiele applicaties die veilig kunnen communiceren met de relevante partijen en entiteiten in het ecosysteem. Dergelijke eWallet apps worden geleverd voor de belangrijkste mobiele platforms (bijv. iOS, Android). Om te worden gedistribueerd via de relevante App Stores moeten eWallets worden ontwikkeld in overeenstemming met de regels van deze platforms.

Alle aanbieders van eWallets moeten worden geregistreerd en kunnen worden geauthenticeerd, zodat kan worden geverifieerd dat het een erkende eWallet betreft. Dit is bijvoorbeeld ook het geval voor DigiD en eHerkenning.

On-boarding bij eWallets



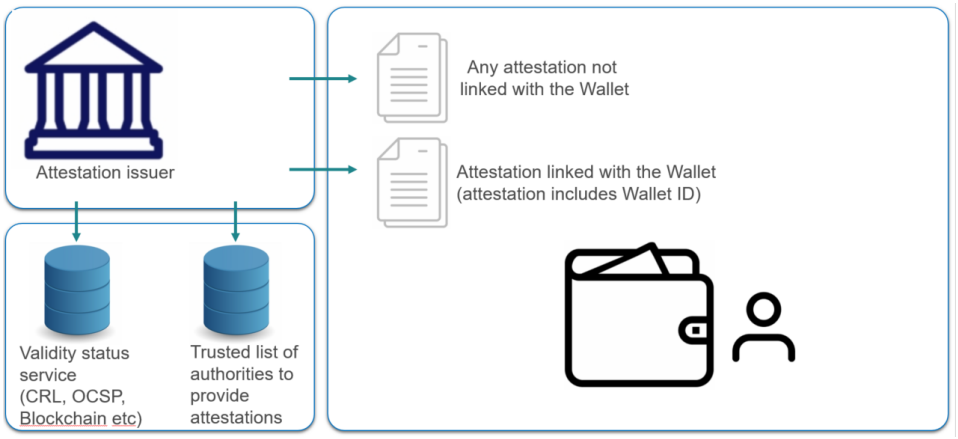
Figuur 3: Proces On-boarding bij eWallets.

Middels een on-boardingproces worden eWallets gepersonaliseerd en gekoppeld aan de gebruiker. In eerste instantie betreft dit de elektronische identificatie functionaliteit. Naar verwachting worden hiervoor de bestaande genotificeerde nationale elektronische identiteitsmiddelen met betrouwbaarheidsniveau Hoog gebruikt, zoals DigiD Hoog.

Maar ook andere methoden zijn denkbaar, zoals personalisering aan een fysieke balie, of het gebruik van een verificatiemethode op afstand die deel uitmaakt van een gecertificeerd nationaal eID-schema (zoals het afsprakenstelsel voor elektronische toegangsdiensten (ETD) dat voor eHerkenning geldt).

Als resultaat van het on-boardingsproces worden persoonsidentificatiegegevens (PID) gekoppeld aan en uitgegeven aan de eWallet. De eWallet is nu klaar voor authenticatiedoeleinden.

Uitgifte van attesteringen

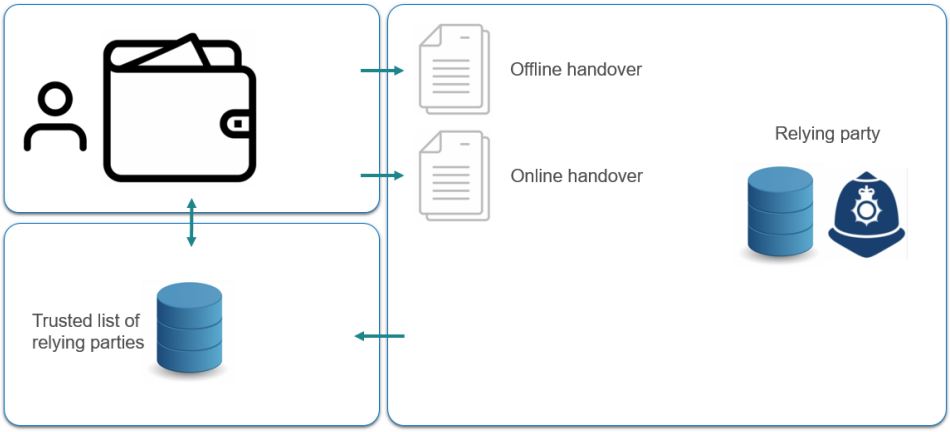


Figuur 4: Proces Uitgifte van attesteringen.

eWallets moeten op basis van de keuze en toestemming van de gebruiker de uitgevers van de gevraagde (set van) attesteringen van attributen kunnen ontdekken en selecteren.

De gebruiker vraagt een attestering (EAA) aan bij een authentieke bron. Typisch zal dit gebeuren door met een eWallet of een ander erkend authenticatiemiddel in te loggen bij de bron. EAAs worden uitgegeven met een unieke verwijzing (bijvoorbeeld een openbare sleutel of een verwijzing ernaar) naar de aanvragende eWallet (d.w.z. de gebruiker en diens PID). Hiermee wordt de eWallet, en daarmee de houder en de andere attesteringen, gekoppeld aan de opgevraagde EAA.

Verstrekken / presenteren van attesteringen



Figuur 5: Proces Verstrekken / presenteren van attesteringen.

Vaak maken dienstverleners de levering van een dienst of product afhankelijk van een gebruikersaccount of van het bestaan van bepaalde attributen. In veel gevallen zijn ze daartoe wettelijk verplicht. Gebruikers kunnen de relevante bewijzen overleggen door middel van PID/EAA's die op hun eWallet zijn opgeslagen.

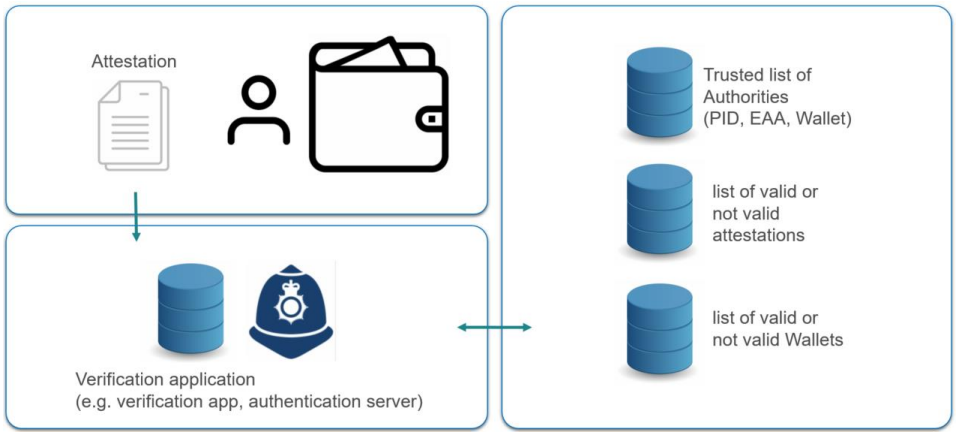
De vertrouwende partij initieert de overdracht van de PID/EAA via een eWallet, bijvoorbeeld door een QR-code te presenteren, of een deep-link of andere methoden aan te bieden. Vervolgens vraagt de eWallet bevestiging aan de eindgebruiker om de attributen te delen.

Als de gevraagde attributen niet in de eWallet aanwezig zullen deze moeten worden opgehaald bij een authentieke bron. Het zelfde geldt voor verlopen attesteringen.

Om gebruikers online te beschermen worden door een eWallet alleen opvragingen van vertrouwende partijen verwerkt die zijn geregistreerd in een trusted list (en mogelijk als rechthebbende staan vermeld).

In een offline scenario wordt de gebruiker gevraagd met zijn eWallet een attestering te presenteren in een leesbare vorm, gecombineerd met een machineleesbare weergave. De machineleesbare weergave wordt door een eWallet bijvoorbeeld middels een QR-code, Near Field Communication (NFC) of Bluetooth aan de vertrouwende partij verstrekt waarna deze de echtheid en geldigheid van het attestering kan controleren en een dienst kan aanbieden.

Authentiseren van attesteringen



Figuur 6: Proces Authentiseren van attesteringen.

Het vertrouwen in de wallet wordt gewaarborgd door de lidstaat die ofwel de persoonlijke identificatiegegevens en de portemonnee verstrekt, ofwel de uitgifte ervan garandeert als trust anchor voor de vertrouwende partij. Deze vertrouwensankers kunnen worden vastgelegd in vertrouwde lijsten (trusted lists). Het vertrouwen in (Q)EAAs wordt verzekerd doordat het vertrouwen in de (Q)EAA-aanbieder kan worden geverifieerd door middel van vertrouwenslijsten van de lidstaten (overeenkomstig art. 22 van de bestaande eIDAS-verordening).

QEAAs bevatten cryptografische elementen en informatie waarmee de vertrouwende partij de authenticiteit van attesteringen op verschillende manieren kan verifiëren:

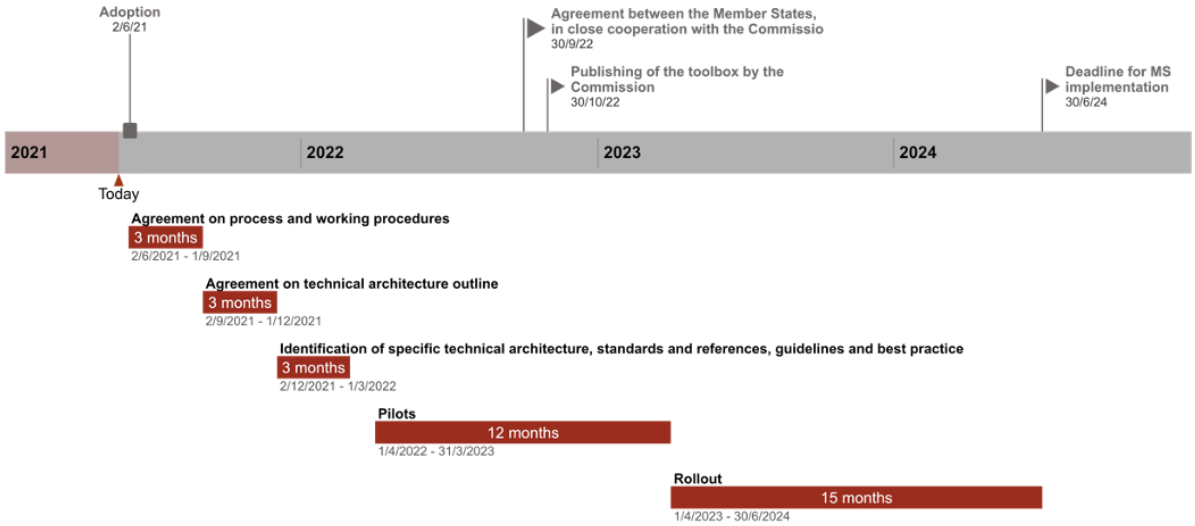
- De elektronische handtekening of zegel van de uitgever van de QEAAs kan worden geverifieerd aan de hand van de overeenkomstige vertrouwenslijst;
- Informatie over de geldigheid of de locatie van de geldigheidsstatus service die vragen over geldigheid afhandelt;
- Door het verstrekken van de public key van de eWallet waarmee presentaties van geattesteerde attributen van QEAAs zijn ondertekend kan de vertrouwende partij het bewijs van bezit van de bijbehorende private key verifiëren. Zo kan de vertrouwende partij de presentatie verifiëren als afkomstig van de eWallet van de gebruiker.

Ondertekenen van gegevens met gekwalificeerde elektronische handtekeningen en zegels

eWallets worden beoogd te voorzien in het ondertekenen van gegevens met een gekwalificeerde elektronische handtekening. Dit kan middels een privé-sleutel op de mobiele telefoon zelf of op een server ergens in het netwerk. Hierop van toepassing zijn de huidige eisen die gelden voor Qualified Signature and Seal Creation Devices (QSCDs), zowel voor de mobiele telefoon als de server op afstand.

3.2 Ontwikkeling Toolbox

De Toolbox beschrijft de technische architectuur, normen, referenties, richtlijnen en best practices voor het implementeren van eWallets. Deze worden vastgesteld in de periode tot april 2022 en vervolgens getoetst door het uitvoeren van pilots in de periode tot april 2023. De Toolbox wordt eind oktober 2022 gepubliceerd. Uiterlijk 30 juni 2024 dient in elk van de lidstaten minstens één eWallet beschikbaar te zijn.



Figuur 7: Planning ontwikkeling Toolbox en eWallet uitrol.

Inzet bij de invulling van de Toolbox is het benutten van zoveel mogelijk open standaarden op het gebied van uitgifte en levering van attributen, digitale documenten en op het gebied van verificatieprotocollen.

De ontwikkeling van de Toolbox is door de Commissie gepland zoals getoond in Figuur 7. Conform de planning zal vanaf april 2022 daadwerkelijk gestart moeten worden met het inrichten en uitvoeren van pilots. Wellicht dat deze planning niet wordt gehaald, maar de urgentie is hoog en Toolbox werkzaamheden worden met prioriteit uitgevoerd. Met betrekking tot deze pilots is nog niet duidelijk welke aspecten en use cases van eWallets getoetst gaan worden, en in welke mate lidstaten de pilots onderling gaan coördineren. Ook lijkt er nog geen zicht te bestaan op de betrokkenheid en rol(len) van de private sector bij deze pilots.

3.3 Nederlands beleid

Het voorstel van de Commissie sluit nauw aan op het Nederlandse beleid[21] voor elektronische identificatie en uitwisseling van gegevens. Evenals de Commissie, wil het kabinet dat alle ingezetenen 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, ook over de grens.

Daarom is Nederland nu al aangesloten op het Europese eIDAS-netwerk dat grensoverschrijdend gebruik van elektronische identificatie en authenticatie mogelijk maakt. Daarnaast heeft Nederland zowel het publieke

[21] Kamerstukken II, 2020-2021, 22 112, nr. 3161 (Fiche: Verordening raamwerk Europese Digitale Identiteit), Kamerstukken II, 2020-2021, 26 643, nr. 750 (Voortgangsrapportage Domein Toegang) en Kamerstukken II, 2020-2021, 26 643, nr. 743 (Visiebrief Digitale Identiteit).

middel DigiD voor burgers als het publiek-private stelsel eHerkenning voor bedrijven, doen erkennen voor gebruik over de grens.

Tevens bereidt het kabinet nieuw beleid en wetgeving voor. De Wet digitale overheid (Wdo), waarvan de eerste tranche momenteel aanhangig is in de Eerste Kamer der Staten-Generaal, is het beoogde fundament voor regulering en doorontwikkeling van het nationale eID-stelsel. Het kabinet is van plan om in de tweede tranche van de Wdo de grondslag te verankeren voor het delen van gegevens in combinatie met een digitale bronidentiteit. De digitale bronidentiteit zal op termijn gebruikt kunnen worden in oplossingen zoals een wallet, waaraan allerlei 'attributen', zoals kwalificaties en bevoegdheden, gekoppeld kunnen worden.

De overheid laat zulke oplossingen toe tot het nationale eID-stelsel en houdt daar toezicht op. Daarbinnen zullen burgers en bedrijven zoveel mogelijk zelf de regie hebben over hun gegevens op een hoog betrouwbaarheidsniveau.

Het kabinet streeft ernaar onder de Wdo een regime van open toelating te introduceren. Daarbij wordt marktwerking ingezet binnen de kaders voor veilige en betrouwbare digitale interactie. De keuze voor een stelsel van open toelating waarbinnen publiek en privaat uitgegeven middelen naast elkaar beschikbaar kunnen zijn, is ingegeven door de gedachte dat een stelsel van open toelating inherente voordelen heeft en zal leiden tot innovatie, kostenreductie, versterking van de marktpositie van Nederlandse bedrijven en vermindering van het risico van een 'single point of failure'.

Die nieuwe voorgestelde eIDAS verordening verplicht elke lidstaat tot introductie van ten minste één 'European Digital Identity Wallet'. Volgens het voorstel kunnen dergelijke eWallets op drie manieren worden uitgegeven: door de lidstaat, onder mandaat van de lidstaat en onafhankelijk, maar erkend door de lidstaat. Dit brengt mee dat eWallets altijd onder regie en beheer van overheden worden uitgegeven, die zorgdragen voor toetsing op het voldoen aan Europees en nationaal gestelde normen en eisen en die toezicht dienen te houden op werking en gebruik. Dit geldt zowel voor eIDs en eWallets die uitgegeven worden door overheden, in publiek-private samenwerking als door bedrijven. Daarnaast dienen eWallets door een toezichthoudend orgaan, zoals het Agentschap Telecom, gecertificeerd te worden overeenkomstig de eisen van de cyberbeveiligingsverordening.

Het kabinet zal zich verder dienen te beraden over welke van de in het voorstel genoemde attributen te ontsluiten via authentieke bronnen richting eWallets en op welke wijze.

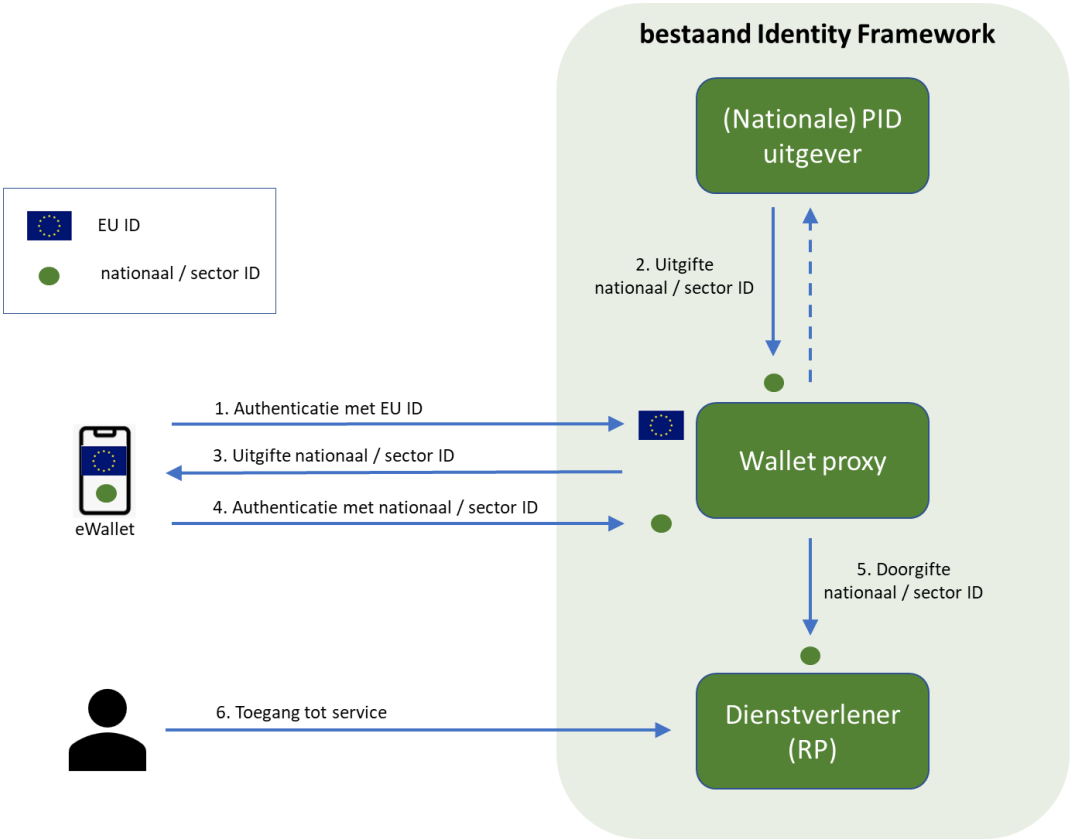
Het voorstel leunt daarnaast sterk op het gebruik van mobiele apparaten en biometrie voor authenticatie. Het voorstel van de Commissie lijkt daarbij uit te gaan van het gebruik van App Store van Apple en Play Store van Google om applicaties te kunnen installeren. Hoewel zulke oplossingen voor adoptie en gebruiksgemak belangrijk zijn, zet het kabinet in op technologie- en leveranciersonafhankelijke oplossingen en het bevorderen van open standaarden en open software, en tot oplossingen die ook voor mensen met minder digitale vaardigheden en/of mogelijkheden eenvoudig te gebruiken zijn.

De gevolgen voor uitvoeringsorganisaties, de gemeenten en andere medeoverheden en de door hen gebruikte ICT-systemen zal BZK nader in kaart brengen, in eerste instantie in een uitvoeringsanalyse. Deze organisaties zullen hierbij betrokken worden en, zoals nu ook het geval is bij de implementatie van de huidige eIDAS-verordening, in de implementatie worden ondersteund binnen de 'Generieke Digitale Infrastructuur' (GDI), onder meer in de aanpassing van hun systemen. Inzet is om de benodigde aanpassingen gefaseerd door te voeren, aansluitend op reguliere trajecten voor doorontwikkeling van digitalisering binnen deze organisaties. Daarbij zal in het bijzonder gelet worden op het gebruik van sectorale uitwisselingssystemen en de basisregistraties die al werken of in een vergevorderd stadium van ontwikkeling zijn. Onnodige investeringen en concurrentie tussen systemen zullen daarbij voorkomen moeten worden. Ook is uitgangspunt dat de huidige systematiek van gegevensuitwisseling binnen de overheid in stand blijft.

3.4 eWallet en bestaande Identity Frameworks

Het eIDAS amendement gaat niet of nauwelijks in op de rol van de bestaande nationale eIDAS infrastructuren in relatie tot eWallets. Hetzelfde geldt voor de rol van andere bestaande, sectorale Identity Frameworks in relatie tot eWallets, zoals eHerkenning voor bedrijven[22], SURFconext voor het hoger onderwijs en onderzoek[23], MedMij voor de zorg[24], en iDIN als herbruikbare bankauthenticatie-oplossing[25].

Door diverse partijen is een 'bootstrap' concept voorgesteld waarmee eWallets worden gekoppeld met bestaande nationale en sectorale identity infrastructuren. De werking van dit concept is weergegeven in onderstaand diagram.



Figuur 8: Gebruik eWallets voor bestaande identity frameworks.

Het diagram toont de stappen die worden doorlopen als een gebruiker met zijn eWallet toegang wenst tot een dienst in een Identity Framework dat eWallets nog niet ondersteunt.

De eerste keer dat de gebruiker aansluit identificeert hij zich met zijn EU ID bij de Wallet Proxy van het Identity Framework (1). De Wallet Proxy is opgenomen als RP (vertrouwende partij) in het eWallet ecosysteem en authenticeert de gebruiker middels het EU ID. Vervolgens geeft de Wallet Proxy een signaal aan de PID uitgever van het Identity Framework, hetgeen er toe leidt dat de PID uitgever een nationaal / sector ID aan de eWallet verstrekt (2, 3), waarna de eWallet dit ID aan de Wallet Proxy verstrekt (4). De Wallet Proxy geeft het ID door aan de dienstverlener (5) die aan de hand van het ID de gebruiker toegang verleent aan de gebruiker (6).

Elke volgende keer dat de gebruiker toegang vraagt worden zowel zijn EU ID als zijn nationaal / sector ID aan de Wallet Proxy verstrekt. Naarmate dienstverleners ook het EU ID en eWallets gaan ondersteunen zal de Wallet

[22] eHerkenning, zie https://www.eherkenning.nl.
[23] SURFconext, zie https://www.surf.nl/surfconext-overal-veilige-toegang-met-1-set-credentials.
[24] MedMij, zie https://www.medmij.nl.
[25] iDIN, zie https://www.idin.nl/.

Proxy alleen het EU ID doorgeven aan de ontvangende dienstverlener. Op termijn kan zo het nationaal / sector ID worden uitgefaseerd en worden vervangen door het gebruik van eWallets.

Dit 'bootstrap' concept is aan de eIDAS Expert Group voorgesteld om te worden opgenomen in de Toolbox[26]. Het is nog niet duidelijk of het eWallet-proxyconcept zal worden opgenomen in de Toolbox en of het concept zal worden toegestaan voor het bootstrappen van sectorale identiteitskaders naar de eWallet.

3.5 Analyse

De implementatie van eWallets vereist de totstandkoming van een complex ecosysteem waarin overheid, private sector en particuliere en zakelijke eindgebruikers met gestandaardiseerde en (waar vereist) gecertificeerde werkwijzen en middelen zullen interacteren. Voor de totstandkoming van een eerste invulling van dit ecosysteem is een termijn van ca. twee jaar voorzien, waarbinnen tal van nieuwe en gewijzigde componenten, entiteiten, diensten en processen moeten worden ontworpen, gebouwd, getoetst en gecertificeerd.

Nieuwe stakeholders waaronder authentieke bronnen, eWallet aanbieders en EAA-aanbieders moeten integreren in het huidige Nederlandse ecosysteem voor digitale identiteiten, bestaande uit infrastructuren voor DigiD en eHerkenning, het eIDAS knooppunt, en voorzieningen als het BSN-koppelregister (BSNk, voor polymorfe pseudoniemen) en het BPR-koppelpunt. Het zelfde geldt voor registers van erkende eWallets, authentieke bronnen, en vertrouwende partijen en hun diensten. Deze moeten raadpleegbaar zijn voor stakeholders. Ook nieuw zijn de infrastructuren voor het verifiëren van door eWallets verstrekte attributen en attesteringen. De nog te ontwikkelen Toolbox speelt bij deze integratie op technisch en organisatorisch vlak een belangrijke rol.

Hier beschouwen wij een aantal aandachtspunten voor de ontwikkeling van het eWallet ecosysteem in Nederland. In de volgende hoofdstukken gaan wij nader in op de introductie van eWallets in de markt, met name ten aanzien van het betrekken van stakeholders, het ontwikkelen van use cases, en de daarvoor relevante context.

Organisatorische en technische aandachtspunten

De processen voor het koppelen van een eWallet aan een gebruiker, het 'laden' ervan met identificerende persoonsgegevens en attributen, en het verifieerbaar delen met vertrouwende partijen zijn inmiddels op hoofdlijnen beschreven. Echter, de duivel zit vaak in de details. Aspecten waar mogelijk in de context van de Toolbox nog aandacht aan zal moeten worden besteed zijn:

- Het tijdig en betrouwbaar kunnen intrekken van een eWallet in het geval van verlies of diefstal van het apparaat waarop deze is geïnstalleerd. Vooral in de situatie dat een kwaadwillende gebruiker toegang heeft tot de eWallet.
- Het tijdig kunnen intrekken van een specifiek attestering over een bepaalde gebruiker. Kan een vertrouwende partij controleren of het vanuit een eWallet verkregen attestering ingetrokken is of niet? Moeten er afspraken worden gemaakt over de levensduur van bepaalde attesteringen?
- Op welke manieren wordt de beveiliging van het gegevenstransport geregeld tussen eWallets en de andere stakeholders? Is dit op basis van TLS-beveiliging? Dient de eWallet hiervoor zelf ook een TLS-certificaat te hebben? Hoe zit het dan met de periodieke vernieuwing van dergelijke certificaten?

Specifiek voor Nederland gelden de volgende aandachtspunten:
- Hoe om te gaan met het BSN tijdens het laden van een eWallet? Is dit één van de attributen die met eWallets worden gedeeld? Mag een private eWallet-aanbieder het BSN verwerken? Immers, het gebruik van BSN is gebonden aan wettelijke grondslagen.
- Uitgangspunt van het vigerende overheidsbeleid is dat de huidige systematiek van gegevensuitwisseling binnen de overheid in stand blijft. De vraag is of dit uitgangspunt met de komst van eWallets gehandhaafd kan blijven en of dit niet tegenstrijdig is met het eWallet principe van controle op gegevensuitwisselingen door de gebruiker. Bijvoorbeeld, gaat een overheidsdienstverlener, nadat een gebruiker met diens eWallet heeft ingelogd, nog steeds op basis van het verkregen BSN bij de BRP extra persoonsgegevens ophalen

[26] Bootstrapping identity wallet authentication with national eIDs, Agency for Digitisation, Denmark

(huidige situatie), of vraagt de overheidsdienstverlener de betreffende gegevens direct aan de eWallet (nieuwe situatie)? De tweede optie past beter in het gedachtengoed van eWallets, maar heeft een enorme impact op de gegevensuitwisseling binnen de overheid.

Ontwikkelen use cases

Naast deze meer technische aspecten wordt het succes en de acceptatie van eWallets in de markt vooral bepaald door de te realiseren economische baten. Baten van use cases rond identificatie en authenticatie op betrouwbaarheidsniveau Hoog zoals beschreven in hoofdstuk 2, maar die ook kunnen worden gevonden in andere use cases, met lagere betrouwbaarheidseisen. Denkbaar is dat juist in de private sector eWallets een rol gaan spelen in dergelijke use cases met lagere betrouwbaarheidseisen; immers, meer en meer ontwikkelen producten en diensten zich tot een persoonlijk en op maat gesneden aanbod. Het (her)kennen van de individuele gebruiker is daarbij steeds de basis. eWallets vormen daarvoor een veilig, betrouwbaar, gestandaardiseerd, internationaal en toekomstvast middel.

Een belangrijke fase in de ontwikkeling van eWallets is die van de pilots, waarbij praktijkproeven de werking en werkbaarheid van eWallets en de governance daarvan moeten aantonen. Deze pilots kunnen daarnaast een bron zijn om zakelijke partijen te inspireren tot tal van nieuwe vormen van processen en dienstverlening waarin eWallets een rol spelen. Het is daarom zaak de private sector tijdig te betrekken bij het benoemen en realiseren van pilots rond eWallets.

Een randvoorwaarde voor pilots is dat de benodigde authentieke bronnen tijdig beschikbaar zijn. Er moet worden bezien of en welke wettelijke beperkingen hier spelen. Zoals hierboven al is benoemd, vereist bijvoorbeeld de uitgifte van het BSN aan eWallets wellicht een nieuw construct om op landelijk niveau een authentieke bron dan wel een gekwalificeerde vertrouwensdienst in te richten.

Uit het betrekken van de private sector bij de pilots kan naar voren komen dat naast de door eIDAS vereiste bronnen ook andere bronnen en providers zouden voorzien in marktbehoeften. Als voorbeeld kan gedacht worden aan de machtigingenregisters voor eHerkenning, voor het uitgeven van machtigingen aan eWallets van gebruikers die aan meerdere bedrijven hun diensten aanbieden. Denk hierbij bijvoorbeeld aan accountants, die nu per bedrijf een apart eHerkenningsmiddel moeten aanschaffen.

Mogelijk kan een meer structurele pilot infrastructuur bijdragen aan het ontwikkelen van de beschreven (internationale) use cases en het faciliteren de private sector bij het toepassen van eWallets in eigen innovatieve dienstverlening. Zo kunnen eWallet Proxies het gebruik van eWallets stimuleren door een brug te vormen tussen eWallets en bestaande nationale of sectorale identity frameworks. Bijvoorbeeld, voor research en hoger onderwijs kan SURF als Wallet Proxy fungeren ten behoeve van de aangesloten instellingen die dan vooralsnog met hun eduID kunnen blijven werken.

Met betrekking tot de pilots is nog niet duidelijk welke aspecten en use cases van de eWallet getoetst gaan worden, en in welke mate lidstaten de pilots onderling gaan coördineren. Een aantal aspecten van de eWallet zijn generiek voor alle lidstaten. Denkbaar is dat lidstaten afstemmen elk een ander aspect in een pilot te beproeven en collectief de pilotresultaten te delen onder regie van de eIDAS Expert Group.

Het huidige beleid voor open toetreding van gecertificeerde eWallets tot het Nederlandse ecosysteem valt te appreciëren. Het kan ertoe leiden dat er een competitief speelveld ontstaat tussen aanbieders van eWallets, waar vooral de gebruikers van zullen profiteren.

Vervolgactiviteiten

Concreet leidt bovenstaande analyse tot de volgende aanbevolen vervolgactiviteiten:

1. Ontwerp de architectuur van het Nederlandse ecosysteem voor digitale identiteiten inclusief eWallets en bijbehorende rollen. Houd rekening met bestaande voorzieningen als DigiD, eHerkenning, BSNk en BRP-koppelpunt en nieuwe voorzieningen als de diverse registers en eventuele proxies. Doorloop de architectuur aan de hand van een aantal use cases voor eIDAS inkomend en uitgaand verkeer. Maak

gebruik van bestaande architecturen zoals ontworpen voor huidige eIDAS inrichting in Nederland[27]. Breng eventuele risico's in kaart die volgen uit de architectuur, zoals een single-point-failure.

2. Onderzoek de mogelijkheden voor het uitwisselen van het BSN via eWallets.

3. Breng de gevolgen van eWallets op de bestaande identiteit-gerelateerde gegevensuitwisselingen door overheidsdienstverleners (uitvoeringsorganisaties, de gemeenten en andere medeoverheden) in kaart. Bijvoorbeeld: voorziet de eWallet de overheidsdienstverlener van alle gevraagde attributen, of volstaat de aanlevering van slechts het BSN op basis waarvan de overheidsdienstverlener via de BRP de overige benodigde attributen kan ophalen? De gekozen architectuur voor het ecosysteem is hierop van invloed.

4. Zoek naar oplossingen om alle nieuwe en bestaande stakeholders zoveel mogelijk te betrekken bij de nieuwe inrichting van het Nederlandse ecosysteem voor digitale identiteiten naar aanleiding van de gereviseerde eIDAS verordening om zodoende gezamenlijk daadkrachtig van start te kunnen gaan met pilots en versnippering te voorkomen.

[27] Start architectuur Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten, april 2017, zie https://www.noraonline.nl/images/noraonline/b/b2/Startarchitectuur_NL_implementatie_eIDAS_met_eTD_1_2_%28002%29.pdf.

4 Verschil eID en eWallet

Wat zijn de verschillen tussen nationale elektronische identificatie oplossingen (eIDs) en eWallets? Deze sectie zet ze op een rijtje.

4.1 Vergelijking eID en eWallet

Een van de kernfunctionaliteiten van een eWallet is elektronische identificatie (eIDAS Art. 6). Daarmee schaart de eWallet zich in het rijtje van nationale elektronische identificatie (eID) oplossingen als DigiD en eHerkenning. Deze laatste oplossingen zijn inmiddels genotificeerd voor de betrouwbaarheidsniveaus Substantieel en Hoog. Mogelijk komen hier nog andere elektronische identificatie-oplossingen bij. Dit zal mede afhangen van de nog in ontwikkeling zijnde Wet digitale overheid (Wdo).

Net als DigiD en eHerkenning zal ook de eWallet moeten voldoen aan de betrouwbaarheidseisen die worden gesteld in eIDAS 2015/1502. Het betekent ook dat eWallets de verplichte minimale set van attributen moeten kunnen uitwisselen (art. 11): voornamen, achternaam en geboortedatum. Optioneel kunnen daarbij attributen als geslacht en adres nog bij komen. De uitwisseling van deze attributen gaat altijd gepaard met een persistente en unieke identifier. Idealiter is deze identifier het zelfde voor alle genotificeerde Nederlandse middelen. Dit voorkomt dat dienstverleners identiteiten moeten gaan linken/matchen als een gebruiker de ene keer met DigiD inlogt en de andere keer met zijn/haar eWallet. Een dergelijke unieke identifier voor alle middelen is echter niet verplicht vanuit eIDAS.

Voor het realiseren van een eWallet als elektronisch identificatiemiddel is eIDAS 2015/1502 leidend. Dit betekent dat er sprake moet zijn van een betrouwbaar identificatie- en activatieproces en dat het gebruik en beheer van een eWallet bepaalde veiligheidsgaranties biedt. Betrouwbaarheidsniveau Hoog is hiervoor vereist. De meest effectieve manier om dit te doen is gebruik te maken van zogenaamde afgeleide identificatie waarbij de gebruiker zichzelf eerst authentiseert met bestaande elektronische identificatiemiddelen op dit niveau. Voor de hand ligt om hiervoor DigiD Hoog te gebruiken. Voorwaarde hiervoor is wel dat eWallets gebruik mogen maken van DigiD als authenticatieoplossing. Voor een eWallet die wordt aangeboden door de overheid zal dit geen probleem zijn, voor een private eWallet-aanbieder ligt dit complexer gezien het vigerende wettelijke kader rondom het gebruik van DigiD. Authenticatie-oplossingen als het Belgische Itsme en het Nederlandse IRMA maken gebruik van afgeleide identificatie. Itsme lift mee op de authenticatie van de door de overheid uitgeven Belgische identiteit; IRMA doet dit via een DigiD authenticatie. De eWallet wordt tijdens een dergelijke authenticatiesessie gekoppeld aan de betreffende gebruiker en ‘geladen’ met de set van eIDAS attributen die deze gebruiker uniek identificeert. Deze set kan vervolgens weer gebruikt worden tijdens een authenticatiesessie met de eWallet zelf.

Als afgeleide identificatie niet mogelijk is zal een eWallet op een andere manier gekoppeld moeten worden aan de gebruiker en moeten worden geladen met attributen. Het proces met de ID-check zoals momenteel voor DigiD Substantieel gebruikt wordt kan hier als voorbeeld dienen. De gebruiker leest in dat geval de chip van diens identiteitsdocument met NFC-technologie.

Tot zover de overeenkomsten tussen een eID en een eWallet. Verschillen zijn er meer. Een belangrijk verschil tussen de bestaande authenticatiemiddelen en een eWallet als authenticatiemiddel is de aanlevering van de identiteitsverklaring. Bij authenticatiemiddelen als DigiD en eHerkenning komt deze verklaring bij de authenticatieserver vandaan. Dit kan bij de eWallet ook zo gebeuren, maar voor de hand liggender is dat de eWallet zelf de identiteitsverklaring verstrekt. In het al eerder genoemde voorbeeld van Itsme, levert de Belgische federale authenticatieserver de verklaring aan nadat Itsme de gebruiker heeft geauthentiseerd. In het geval van IRMA, levert de mobiele IRMA app zelf de verklaring aan tijdens de authenticatiesessie.

Een voordeel van identiteitsverstrekking door eWallets is dat er geen gebruik hoeft worden gemaakt van de eIDAS infrastructuur bestaande uit de nationale nodes waarop partijen moeten aansluiten. Voor een dienstverlener is het op deze manier veel eenvoudiger om de gebruiker te authentiseren en identiteitsgegevens te verkrijgen.

Een ander verschil is de rijkheid van attributen en persoonsgegevens die worden uitgewisseld. Deze is voor de beoogde eWallet veel rijker dan bij DigiD of eHerkenning het geval is. De laatste oplossingen focussen met name op unieke identificering van een natuurlijk of juridisch persoon, terwijl een eWallet bijvoorbeeld ook diploma, medische of financiële gegevens van verschillende bronnen kan uitwisselen. Daar waar DigiD en eHerkenning een enkele identiteitsverklaring afgeven, kan een eWallet veel meer verklaringen afgeven uit verschillende bronnen. Een eWallet zou ook machtigingen kunnen uitwisselen waardoor het een alternatieve oplossing voor de huidige eHerkenningsmiddelen wordt. Een oplossing die, in tegenstelling tot de huidige meer bedrijfscentrale middelen, veel meer persoonsgebonden is met machtigingen als extra attributen. Een accountant die namens diverse bedrijven belastingopgave doet, heeft op dit moment per bedrijf een eHerkenningsmiddel nodig. Met een persoonsgebonden eWallet en bijbehorende machtigingen per bedrijf is dit nog maar één middel.

De rijkere mogelijkheden van eWallets komen ook met uitdagingen rondom user experience en data en consent management waar traditionele elektronische identificatieoplossingen minder 'last' van hebben. Gezien de diversiteit aan eWallet toepassingen (use cases) valt ook nog maar te bezien of alles technisch met een beperkte set aan standaarden en koppelvlakken te realiseren is. Met andere woorden, de kans is groot dat een eWallet oplossing vele malen complexer is dan een elektronische identificatieoplossing.

De relatieve complexiteit van een eWallet en het achterliggende concept van regie op gegevens staan op gespannen voet met het vertrouwen dat nodig is voor de gebruiker om ermee aan de slag te gaan. eID oplossingen genieten dit vertrouwen al omdat redelijk duidelijk is wat ze doen, ze minder complex zijn en ze al enkele jaren in gebruik zijn. Daarnaast zijn er kaders opgebouwd waaraan ze moeten voldoen en is het toezicht hierop ingevuld. Dergelijke kaders voor het borgen van vertrouwen zijn er nog niet voor eWallet oplossingen.

Een eWallet moet gebruikt kunnen worden voor publieke en private dienstverlening. Voor eHerkenning is dit geen probleem, hoewel er in de praktijk nog maar weinig gebruik in de private sector te constateren is. Voor DigiD echter wel op dit moment. Het is wettelijk geregeld dat DigiD slechts gebruikt kan worden binnen de overheid, de zorg- en de pensioensector. Centraal daarbij staat het BSN dat in de DigiD verklaring zit en het bij wet geregelde gebruik ervan. Het inzetten van een oplossing als iDIN in het publieke domein (specifiek het BSN-domein) is niet mogelijk omdat iDIN het BSN niet mag verwerken. Enige jaren geleden is in de Idensys pilot geëxperimenteerd met het gebruik van iDIN en andere private middelen in het publieke domein[28]. De kennis die is opgedaan in de pilot zal zijn beslag vinden in de Wdo. Door van het BSN een polymorf pseudoniem te maken, zouden ook private partijen gebruik kunnen maken van DigiD[29]. Op dit moment is lastig in te schatten of en hoe polymorfe pseudoniemen ook in de context van Europese eWallets werkbaar zijn.

Veel overheidsdienstverleners zijn 'gewend' om via DigiD een BSN te ontvangen en om vervolgens de bijbehorende persoonsgegevens uit de BRP te halen. Ook de eWallet zal het BSN moeten kunnen verwerken en doorgeven aan deze overheidsdienstverleners. De vraag is of dit juridisch op dit moment kan bij een door een private partij aangeboden eWallet. De eWallet zou, naast BSN, ook andere persoonsgegevens met overheidsdiensten kunnen delen onder regie van de gebruiker. De uitstap naar de BRP is dan niet meer nodig.

Technisch gezien maken de huidige eID middelen allemaal gebruik van het SAML protocol voor het uitwisselen van identiteitsverklaringen[30]. Deze standaard staat ook op de "pas toe of leg uit" lijst van het Forum Standaardisatie[31]. In opkomst zijn de meer moderne protocollen OpenID Connect[32] en FIDO[33]. Dergelijke protocollen zal de eWallet voor elektronische identificatie ook moeten ondersteunen. Voor het uitwisselen van een rijkere en grotere set van gegevens of zelfs documenten zijn deze protocollen echter niet geschikt. De eWallet zal daarvoor andere protocollen moeten ondersteunen. Dit betekent dat dienstverleners dat ook zullen moeten doen. Naast de standaard SAML-gebaseerde interface, zullen zij andere interfaces moeten implementeren om gegevens via de eWallet te kunnen ontvangen.

[28] Idensys pilot, 2018, zie https://www.digitaleoverheid.nl/nieuws/pilot-met-idensys-stopt-per-31-december-2018/.
[29] Polymorfe pseudonimisering BSN, zie https://www.logius.nl/diensten/bsnk-pp/bsnk-pp-hoe-werkt-het.
[30] SAML, zie http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.
[31] Pas toe of leg uit lijst van het Forum Standaardisatie, zie https://www.forumstandaardisatie.nl/open-standaarden/verplicht.
[32] OpenID Connect, zie https://openid.net/connect/.
[33] FIDO, zie https://fidoalliance.org/fido2/.

Een ander verschil tussen een eWallet en een eID middel is het toezichthoudende regime. De erkenning van eID middelen verloopt middels een door de lidstaten zelf gecoördineerd notificatie- en peer-review proces. Een eWallet daarentegen komt op de lijst van erkende wallets na beoordeling door een onafhankelijke conformiteitsbeoordelaar (CAB) en goedkeuring door de nationale toezichthouder. Het toezicht op een eWallet is daarmee te vergelijken met de huidige toezichtsconstructie op eIDAS vertrouwensdiensten.

Tot slot kan een eWallet voorzien in het digitaal ondertekenen van documenten of verklaringen door de gebruiker zelf. Een dergelijke (gekwalificeerde) ondertekenfunctionaliteit ontbreekt op dit moment bij DigiD of eHerkenning. De bankauthenticatieoplossing iDIN daarentegen biedt deze functionaliteit wel[34]. Bij iDIN Ondertekenen wordt een te ondertekenen document gekoppeld aan de iDIN authenticatiesessie waarbij de gebruiker bevestigt dat hij/zij op die manier het document digitaal ondertekent met het inlogmiddel van zijn bank. Dit resulteert in een geavanceerde rechtsgeldige handtekening. Vanuit eIDAS wordt beoogd om ook gekwalificeerde rechtsgeldige handtekening te kunnen zetten. Ook met de applicaties van Itsme en IRMA kan digitaal worden ondertekend. Daarnaast zijn er natuurlijk ook nog partijen die ondertekenen met gekwalificeerde certificaten aanbieden. Denk daarbij aan Digidentity, Cleverbase en DigiCert+QuoVadis.

Hoewel eWallets ook het bedrijvendomein (rechtspersonen) beogen te bedienen, is het rechtsgeldig digitaal onderteken of zegelen namens een bedrijf een nog onderbelicht aspect. Hoe dit middels een eWallet vorm te geven is niet triviaal en onderwerp voor toekomstig onderzoek.

De tabel hieronder zet alle verschillen tussen eWallets en de huidige nationale elektronische identificatieoplossingen op een rijtje voor diverse aspecten.

Aspect	eWallet	DigiD (eID)	eHerkenning (eID)	iDIN (eID)
Authenticatie	Op Substantieel en Hoog	Op Substantieel en Hoog	Op Substantieel en Hoog	Op Substantieel
Locatie gegevens	Server en eWallet	Server	Server	Server
Rijkheid gegevens	Minimale set en extra gegevens uit diverse bronnen	Minimale set van attributen uit één bron	Minimale set van attributen uit één bron	Minimale set van attributen uit één bron (de bank)
Complexiteit	Complex	Eenvoudig	Redelijk eenvoudig	Eenvoudig
Vertrouwen	Nog op te bouwen	Aanwezig	Aanwezig	Aanwezig
Publieke en/of private domein	Beide domeinen	Alleen publiek (inclusief zorg- en pensioensector)	Beide domeinen	Alleen privaat
Technisch / standaarden	Meerdere protocollen	Eén protocol – SAML	Eén protocol – SAML	Eén protocol – SAML
Toezicht	Via CAB en nationale toezichthouder	Via peer review	Via peer review	Is nog niet genotificeerd. Toezicht nu via financiële toezichthouders
Ondertekenen	Mogelijk op gekwalificeerd niveau	Niet mogelijk	Niet mogelijk	Mogelijk op geavanceerd niveau

[34] iDIN Ondertekenen, zie https://www.idin.nl/bedrijven/idin-ondertekenen/.

4.2 Analyse

De verschillen tussen een eID en een eWallet zijn groot. De impact van de in eIDAS voorgestelde eWallet op de huidige nationale eID infrastructuur betreft dan ook vele aspecten, waaronder infrastructuur, standaarden, toezicht, juridische kaders, en rollen en verantwoordelijkheden van spelers. Mogelijk zijn eWallets zelfs ondermijnend voor bestaande constructies als eHerkenning en concurreren zij met andere bestaande eID oplossingen. Daar komt bij dat de complexiteit van eWallets voor een deel nog niet volledig inzichtelijk is, en dat de implementatie van eWallets een majeure veranderopgave lijkt voor overheid en marktpartijen.

Daar staat tegenover dat eWallets ten opzichte van eIDs een enorm potentieel bieden om (nieuwe) use cases te faciliteren en te versnellen. Ze kunnen daardoor een grote rol gaan spelen in de (digitalisering van de) Europese economie. Dit komt met name door twee factoren waarin de eWallet verschilt van eIDs:

1. Naast een identificatiemiddel is een eWallet ook een personal data management oplossing. Daardoor kunnen eWallets worden toegepast in tal van use cases waar persoonlijke gegevens een rol spelen.
2. De rijke functionele mogelijkheden van eWallets kunnen EU-breed voor zowel publieke als private toepassingen worden ingezet. Een eWallet aanbieder heeft daardoor toegang tot een enorme markt, niet alleen van eindgebruikers maar ook van mogelijke ketenpartners die eWallets integreren in de oplossingen en diensten waarmee de hiervoor genoemde use cases worden gefaciliteerd.

Het is voor de overheid dus zaak om de introductie van eWallets in de Nederlandse markt enerzijds beheersbaar en doelgericht te organiseren en faciliteren (in lijn met het Minimum Viable Product gedachtegoed) , en anderzijds om de markt van publieke en private partijen (vertrouwende partijen, authentieke bronnen, eWallet providers) goed te betrekken om (nieuwe) use cases rond eWallets van de grond te krijgen die daadwerkelijk bijdragen aan het succes ervan in Nederland.

Vervolgactiviteiten

Concreet leidt de bovenstaande verschilanalyse tot de volgende aanbevolen vervolgactiviteiten:

1. Onderzoek hoe middels een eWallet namens een bedrijf rechtsgeldig digitaal te onderteken of te zegelen.
2. Voer een impact assessment uit van eWallets op het stelsel voor eHerkenning. Worden de machtigingenregisters van eHerkenning straks authentieke bronnen? Is het wenselijk om eHerkenningsmiddelen meer persoonsgebonden te maken?
3. De introductie en het gebruik van eWallets is complex en gebaat bij een daadkrachtige en pragmatische aanpak waarbij de overheid een sturende rol moet spelen en zelf het goede voorbeeld moet geven door op te treden als vertrouwende partij en authentieke bron. Werk de invulling van beide rollen nader uit.

5 Huidig speelveld eWallets

In dit hoofdstuk gaan wij in op voorbeelden van wallet applicaties/oplossingen en ontwikkelingen die als eWallet gekwalificeerd kunnen worden in de Nederlandse en Europese markt.

5.1 Voorbeelden in Nederland

In Nederland zijn er tal van oplossingen beschikbaar voor het delen van persoonsgegevens middels een eWallet. Vaak worden deze oplossing ondergebracht onder termen als Personal Data Management (PDM) of Self-Sovereign Identity (SSI). In opdracht van de overheid zijn hier recent zeer volledige overzichten en analyses voor opgesteld[35].

De huidige oplossingen zijn niet volgens een bepaald architectuurmodel ingericht. Om een beeld te geven van de verscheidenheid in opzet en inrichting van oplossingen beschrijven wij hier een aantal kenmerken van vier Nederlandse initiatieven die elk model staan voor de verschillende manieren waarop eWallets kunnen worden vormgegeven. Voor een meer volledig overzicht van alle oplossingen in Nederland verwijzen wij naar de bovenstaande rapporten.

5.1.1 IRMA

IRMA is een steeds populairder wordende mobiele applicatie voor het uitwisselen van persoonsgegevens op een privacy- en gebruikersvriendelijke manier[36]. Een gebruiker van IRMA kan met de IRMA-app zijn of haar gegevens ophalen bij verschillende uitgevers, zoals bij banken via iDIN, of bij BRP via DigiD bij een aantal gemeentes onder leiding van Nijmegen[37]. Vervolgens kan de gebruiker deze gegevens (“attributen”) in IRMA aan andere (controlerende) partijen laten zien. Het betrouwbaarheidsniveau dat IRMA aan gegevens hangt, is afhankelijk van het betrouwbaarheidsniveau van het middel dat wordt gebruikt om de attributen te verkrijgen.

Bij BRP-gegevens is dat nu in de meeste gevallen DigiD Midden, wat in feite eIDAS betrouwbaarheidsniveau Laag is. Voor veel diensten in de sector is dit voldoende, maar voor diensten die Substantieel of Hoog behoeven is het wachten op een hogere dekkingsgraad van DigiD Substantieel en DigiD Hoog.

De onderliggende technologie van IRMA is gebaseerd op Idemix, een privacy enhancing technologie, die het mogelijk maakt om alleen de geselecteerde attributen te ontsluiten richting de dienstverlener. Gegevens worden vanuit de app in JSON-formaat gedeeld met de dienstverleners. Validatie van de gegevens vindt plaats op de IRMA server.

Naast gegevensuitwisseling biedt IRMA ook digitale ondertekenfunctionaliteit[38].

IRMA is eigendom van de stichting Privacy by Design en wordt beheerd door SIDN.

5.1.2 *Datakeeper*

De Datakeeper wallet app is nog volop in ontwikkeling[39]. Met kleine groepjes gebruikers worden er verschillende pilots gedaan. De ambitie van Datakeeper is dat uiteindelijk iedereen in Nederland van de app gebruik kan maken.

Datakeeper maakt onder andere gebruik van NFC-technologie om chips van identiteitsdocumenten uit te lezen. Deze data kan dan gecontroleerd worden gedeeld met derden.

---

[35] PDM Landschap 2020: Regie op gegevens in Nederland, zie https://www.rijksoverheid.nl/documenten/rapporten/2021/01/11/pdm-landschap-2020-regie-op-gegevens-in-nederland#:~:text=Onderzoek%20naar%20de%20mogelijkheden%20die,PDM%20staat%20voor%20persoonlijk%20datamanagement en Eindrapport Nederlandse Self-Sovereign Identity Ecosysteem (SSI), zie https://www.rijksoverheid.nl/documenten/rapporten/2021/10/01/eindrapport-nederlandse-self-sovereign-identity-ecosysteem-ssi.

[36] IRMA app, zie https://irma.app/.

[37] Zie https://privacybydesign.foundation/uitgifte-brp/.

[38] IRMA ondertekenen, zie https://privacybydesign.foundation/demo/ondertekenen/.

[39] Datakeeper wallet, zie https://datakeeper.nl.

Datakeeper maakt gebruik van blockchain technologie om de via de wallet aangeleverde (persoons)gegevens te verifiëren. In de blockchain wordt alleen het bewijs van uitgifte van deze gegevens opgeslagen, dus niet de (persoons)gegevens zelf.

De innovatie afdeling van de Rabobank heeft de Datakeeper app ontwikkeld.

5.1.3 Ockto

Ockto is een platform waarmee individuen data kunnen verzamelen vanuit verschillende databronnen en deze data kunnen doorgeven aan een aangesloten (financieel) dienstverlener[40]. De dienstverlener geeft hierbij aan welke gegevens uit welke bronnen nodig zijn voor de dienst. Ockto zorgt ervoor dat consumenten snel en simpel informatie kunnen verzamelen en deze met adviseurs, banken, hypotheekverstrekkers of andere dienstverleners kunnen delen.

De gebruiker en data aanbieder kunnen Ockto gratis gebruiken, data afnemers betalen een transactie vergoeding als zij data vanuit Ockto willen gebruiken. Ockto is een Nederlands initiatief en focust zich op de Nederlandse financiële markt. Ockto is operationeel: op dit moment kan een gebruiker met de Ockto app onder andere gegevens ophalen bij de Belastingdienst, UWV, Mijnpensioenoverzicht en MijnOverheid. Ook biedt Ockto de mogelijkheid DUO studieschuld-gegevens op te halen. De aankondiging van deze databron was daarin niet onomstreden: het voornemen om studieschuld toegankelijk te maken voor hypotheekverstekkers leidde tot Kamervragen, maar werd toegestaan op basis van de AVG (dus mits het gegeven met toestemming van de burger wordt opgevraagd).

Ockto beschikt ook over een PSD2-vergunning en werkt samen met Linx van Invers om gefilterde, gecategoriseerde transactiegegevens in combinatie met van de overheid afkomstige persoonlijke gegevens te ontsluiten.

Ockto is geïmplementeerd bij onder meer Rabobank, ABN AMRO, AEGON, Allianz en recentelijk ING. Daarnaast wordt Ockto ook toegepast in verschillende applicaties voor het bieden van financieel overzicht, zoals FinanceBook van Achmea en MyLife van Yellowtail. Specifiek voor de hypotheekketen heeft Ockto, samen met onder andere HDN, de Ockto Brondata Service ontwikkeld. Dit zorgt ervoor dat de consument minder documenten hoeft op te leveren bij de aanvraag van een hypotheek.

De gegevensuitwisseling tussen Ockto en data aanbieders en afnemers verloopt via API's, of via screen scraping indien er geen API beschikbaar is. Hierbij moet beseft worden dat er bij screen scraping geen waarmerking vanuit de data aanbieder is. De data wordt opgeslagen op het apparaat van de gebruiker en verwerkt op de server van Ockto. Een data-afnemer kan de gebruiker daarnaast vragen om de gegevens maximaal 90 dagen bij Ockto beschikbaar te houden. Zo kan een geldverstrekker de persoonsgegevens maximaal 90 dagen gebruiken voor het uitbrengen van een (hypotheek)aanbod.

5.1.4 Schluss

Schluss is een service voor opslag van, regie op en overzicht over persoonlijke gegevens[41]. Schluss levert een persoonlijke digitale kluis, waarin gegevens opgeslagen kunnen worden. Dit kan gaan om bijvoorbeeld adresgegevens, medische of financiële gegevens. Identificatie en autorisatie wordt gewaarborgd via derden. De gebruiker bepaald wie toegang krijgt, voor welk doel en voor welke periode. Er is een overzicht van welke inzagen verleend zijn, zodat deze ook weer ingetrokken kunnen worden (afhankelijk van de juridische kaders).

De toekomstvisie van Schluss richt zich op het opstellen als kluis voor alle digitale informatie, maar tevens als 'sluis' variant waarbij alleen consent gegeven wordt via Schluss en uitwisseling tussen data aanbieder en afnemer verloopt. Daarbij wordt ook gewerkt aan de mogelijkheid om een persoon te machtigen, die in geval van nood toegang krijgt tot de kluis.

[40] Ockto, zie https://www.ockto.nl.
[41] Schluss, zie https://www.schluss.org.

5.2 Voorbeelden in het buitenland

Ook in het buitenland worden eWallets ontwikkeld en gebruikt. Ook hier bestaan geen standaarden voor de architectuur of governance van eWallets. Ter illustratie beschrijven wij enkele buitenlandse ontwikkelingen rond eWallets, elk met een eigen invalshoek en invulling van het eWallet concept.

5.2.1 Itsme

Itsme is een Belgische variant van DigiD, die Belgische burgers een uniek digitale identiteit geeft. Er zijn echter drie essentiële verschillen. Allereerst wordt itsme niet door een overheidspartij beheerd, maar door een consortium van grootbanken en netwerkoperators: Belgian Mobile ID. Ten tweede zijn er, geen wettelijke inperkingen over waar Itsme gebruikt kan worden: de oplossing wordt zowel in de publieke sector gebruikt om alle overheidsapplicaties te ontsluiten, als in het private domein op moment van schrijven ruim 400 partijen in verschillende sectoren. Ten derde gaat ook het functionele toepassingsgebied verder: Itsme biedt naast identificatie en login ook consent-beheer en gekwalificeerde handtekeningen aan.

Itsme identificeert gebruikers door ze zich te laten identificeren met de Belgische identiteitskaart. Dit kan zowel direct met het eID als via een bank die de identiteit hier al mee heeft vastgesteld. Na registratie kunnen gebruikers de Itsme app gebruiken om op verschillende plekken desgevraagd hun digitale identiteit te laten zien. De belangrijkste gegevens om een identiteit te bewijzen staan centraal bij Itsme opgeslagen. Hiernaast maakt Itsme het ook mogelijk om gegevens tussen verschillende partijen uit te wisselen tussen de data aanbieder en data afnemer. In dit geval slaat Itsme de gegevens niet zelf op, maar fungeert het louter als sluis die de data-uitwisseling mogelijk maakt. Met deze functionaliteit kan Itsme, ondanks dat de focus nu voornamelijk op identificatie ligt, ook als eWallet gezien worden.

ING biedt haar klanten in België sinds kort de Helena app. Met deze app kunnen gezondheidsgegevens (met name rond COVID-19) worden opgeslagen en getoond. Helena is gekoppeld aan de Itsme identiteit van de gebruiker. Dit is een voorbeeld van integratie van een digitale identiteitsoplossing met andere apps om digitale services aan te bieden. Itsme koppelt al met een reeks bank- en niet-bancaire diensten rond ondermeer gezondheidsdiensten, belastingen en pensioenen.

Momenteel kunnen alleen mensen in het bezit van een Belgische eID-kaart of Belgische verblijfskaart zich registreren bij Itsme, maar binnenkort wordt het ook mogelijk een Itsme aan te maken met behulp van identiteitsbewijzen met NFC, zoals de Nederlandse identiteitskaart. Itsme is eIDAS genotificeerd op niveau Hoog, wat betekent dat het binnenkort door de Nederlandse overheid geaccepteerd zal moeten worden.

De komende periode staan er een aantal pilots met Itsme binnen het Nederlandse overheidsdomein gepland. Bij verschillende gemeentes, waaronder Helmond en Molenland, zal Itsme naast de bestaande inlogmiddelen aangeboden worden.

5.2.2 ID Oostenrijk

ID Oostenrijk is onlangs onder eIDAS voor-genotificeerd en wordt op dit moment beoordeeld door de andere lidstaten. Oostenrijk is daarmee een van de laatste lidstaten.

ID Oostenrijk is de nationale mobiele app oplossing voor elektronische identificatie. De oplossing heeft als uitgangspunt het ‘once only principle’, stelt de gebruiker centraal en moet business innovatie versnellen. Het once only principe gaat er van uit dat burgers, instellingen en bedrijven bepaalde standaardinformatie slechts één keer hoeven aan te leveren aan de overheden. Door het opnemen van gegevensbeschermingsregels en de uitdrukkelijke toestemming van de gebruikers, mag het openbaar bestuur de gegevens hergebruiken en met elkaar uitwisselen. Het principe maakt ook deel uit van de plannen van de Europese Unie (EU) om de digitale interne markt verder te ontwikkelen door de administratieve lasten voor burgers en bedrijven te verminderen.

ID Oostenrijk is te gebruiken door publieke en private dienstverleners, kosteloos voor gebruikers en dienstverleners, kan gekwalificeerde digitale handtekeningen plaatsen, maakt gebruik van vertegenwoordiging en machtigingen, en hanteert sectorspecifieke identifiers als privacymaatregel. De verstrekking ervan lift mee op het aanvraagproces van paspoorten of ID-kaarten. Gegevens worden uit diverse authentieke overheidsbronnen (basisregistraties) gehaald. Duidelijk is dat deze mobiele app oplossing, ten opzichte van alternatieve fysieke kaart-oplossingen in Oostenrijk, de voorkeur geniet bij de eindgebruiker.

Naast bovengenoemde landen, zijn er nog diverse andere landen zoals Polen, Spanje en Denemarken waar met name elektronische identificatie via eWallets plaats vindt. Dit zijn alle overheidsgedreven oplossingen.

5.2.3 Wallets van techgiganten

Belangrijke ontwikkelingen rond eWallets zijn te zien bij de grote Internet en IT spelers. Zo hebben eerder dit jaar in de VS acht staten met Apple een overeenkomst gesloten om ID's en digitale rijbewijzen in de Apple Wallet-app te laden en te presenteren. Deze functionaliteit wordt naar verwachting in 2022 operationeel. Gebruikers kunnen zich dan snel en betrouwbaar identificeren door hun iPhone kort tegen een reader aan te houden. Dit versnelt bijvoorbeeld beveiligingscontroles op luchthavens. Apple heeft eerder aangegeven dergelijke functionaliteit ook in Europa te willen aanbieden.

In maart van dit jaar lanceerde Google de Android Ready SE Alliance, een groep ontwikkelaars die bouwstenen maakt voor de in steeds meer Android devices ingebouwde beveiligde hardware ('Secure Elements'). Hiermee wil Google de ontwikkeling versnellen van veilige digitale sleutels (voor auto's en panden), rijbewijzen, nationale identiteitskaarten, ePassports en eMoney-oplossingen (waaronder Wallets).[42] Een van de partijen in de Alliance is het Franse technologieconcern Thales.

Een laatste voorbeeld is het dit jaar geïntroduceerde Azure AD Verifiable Credentials platform van Microsoft. Hiermee zijn op W3C standaarden gebaseerde eWallet oplossingen te maken. Het platform is nu als pilotomgeving beschikbaar en komt naar verwachting begin 2022 als supported service beschikbaar. De Vlaamse overheid maakt al gebruik van het platform, in combinatie met Solid PDM technologie, voor het met een app met hoge betrouwbaarheid uitgeven en verifieren van identiteits- en financiële gegevens bij het opstarten van een nieuw bedrijf, volledig onder regie van de aanvrager[43].

5.3 Analyse

Doorbreken van gefragmenteerd aanbod

Op nationaal niveau zijn er diverse vooral private initiatieven rondom eWallets. Ondanks dat het concept van een eWallet al enkele jaren bestaat, valt het huidige speelveld te karakteriseren als onvolwassen en gefragmenteerd. Dit komt door diverse factoren.

Een belangrijke factor is het ontbreken van een architectuurmodel en van standaarden voor gegevensuitwisseling en onderliggende technologieën, wat ten koste gaat van de interoperabiliteit en het hergebruik van gegevens. Standaarden zijn nodig voor de gegevens zelf (gegevensmodellen en semantiek) en voor de uitwisseling ervan tussen de stakeholders (bronnen, eWallets en dienstverleners).

Daarnaast ontbreken er goed gespecificeerde kaders waaraan eWallets qua functionaliteit en beveiliging minimaal aan moeten voldoen. Iedere eWallet ontwikkelaar heeft een eigen opvatting over de beste invulling van een eWallet en onderlinge samenwerking ontbreekt. Hierdoor is een heterogeen landschap van eWallets ontstaan. Het gevolg is dat bronnen en dienstverleners niet goed weten met welke eWallet ze zaken moeten gaan doen.

Een derde factor is het ontbreken van kaders op basis waarvan het onderling vertrouwen tussen betrokken stakeholders in een eWallet situatie voor het delen van (persoons)gegevens onder regie van de gebruiker te borgen is.

Tot slot vormt het ontbreken van een business case voor met name de (authentieke) bronnen een drempel om eWallets te faciliteren waardoor er een kip-ei-probleem ontstaat. Als er geen bruikbare bronnen kunnen worden ontsloten via eWallets is het voor dienstverleners minder aantrekkelijk om gebruik te maken van een eWallet. Zijn er minder dienstverleners die van eWallets gebruik maken, dan is het voor bronnen minder interessant om gegevens te ontsluiten. De business case voor een dienstverlener is evident: via de rijke set van gegevens uit de eWallet kunnen zij een betere dienstverlening aanbieden. Hier verdient de eWallet aanbieder op zijn beurt weer aan.

[42] https://security.googleblog.com/2021/03/announcing-android-ready-se-alliance.html
[43] https://customers.microsoft.com/en-us/story/1351115614634143059-flanders-government-of-belgium-government-azure-active-directory

De meeste van deze punten worden door de herziene eIDAS verordening geadresseerd, zoals in het vorige hoofdstuk is beschreven. Een architectuurmodel, standaarden voor gegevensuitwisseling en functionele en beveiligingseisen worden gespecificeerd in de Toolbox. Op dit moment wordt hier door de Commissie en in samenwerking met alle lidstaten hard aan gewerkt. Grote delen van de eisen waaraan eWallets moeten voldoen zijn al bekend: de eIDAS 2015/1502 uitvoeringsverordening rondom betrouwbaarheidsniveaus en de cybersecurity verordening. Vanuit de Toolbox zullen nog nieuwe eisen komen die specifiek voor eWallets gelden. Dit moet leiden tot gecertificeerde eWallets die op een interoperabele manier met bronnen en dienstverleners kunnen communiceren. Authentieke bronnen worden aangewezen die gegevens ontsluiten naar eWallets. Tot slot komt er een toezichthoudend regime op eWallets om het vertrouwen in eWallets te borgen.

Ontwikkeling eWallet ecosysteem

Kijkende naar de eisen die door eIDAS aan eWallets worden gesteld dan ligt de lat hoog. Ons beeld is dat geen van de huidige Nederlandse eWallets voldoet aan alle door eIDAS gestelde eisen om te kunnen opereren op betrouwbaarheidsniveau Hoog en met gekwalificeerde certificaten. Daarnaast verwachten wij dat veel, zo niet alle, eWallets (nog) niet kunnen voldoen aan een aantal generieke eisen gesteld door eIDAS, bijvoorbeeld ten aanzien van wettelijke aansprakelijkheid en cybersecurity. Dit is ook logisch omdat de kaders voor eWallets nu pas gedefinieerd worden.

Aanbieders zullen dus tijd nodig hebben om te voldoen aan de bestaande en nog te ontwikkelen eIDAS eisen. Om te kunnen certificeren dient de Nederlandse overheid het governance regime tijdig te organiseren. Ook het aantonen van compliance richting conformiteitsbeoordelaars en toezichthouders zal de nodige doorlooptijd vergen. Gezien de ambities van de EU Commissie en de tijdslijnen die ze hierbij voor ogen heeft, kan dit alles problemen opleveren om tijdig te voldoen aan de gewijzigde eIDAS wetgeving.

Business case

Qua business model is een uitdaging dat het gebruik van eWallets voor de gebruiker gratis moet zijn. Hier valt dus voor een aanbieder van een eWallet niets te halen. Een oplossing kan zijn dat er binnen Nederland een ecosysteem ontstaat waar er voor aanbieders van eWallets wél een business case is. Wij zien kansen in bestaande use cases waarbij dienstverleners hun klanten en business partners slimme services aanbieden waarbij een betrouwbare identiteit een rol speelt. Bijvoorbeeld voor het op afstand inchecken in een hotel of voor leeftijdsverificatie bij online alcoholverkoop en bezorging. Daarvoor zou de Nederlandse overheid met private stakeholders kunnen focussen op het faciliteren van private, nationale use cases; als deze een succes zijn kunnen eWallet aanbieders ook de kosten van (grensoverschrijdend) Wallet gebruik in door eIDAS verplichte gebruikscenario's als uitbreiding op hun business cases dragen.

Een alternatief scenario is dat de Nederlandse overheid vooraleerst een eWallet voor gebruikers als kosteloze nutsvoorziening beschikbaar stelt, in ieder geval zolang private partijen niet zelf met eWallets op de markt verschijnen die aan de eIDAS-eisen voldoen. Dit kan door bijvoorbeeld de huidige DigiD eID voorziening verder door te laten ontwikkelen tot een DigiD eWallet. Om vanuit dit scenario de hiervoor geschetste ontwikkeling van private use cases te versnellen moet deze nutsvoorziening voorzien in goede mogelijkheden voor naadloze integratie in digitale dienstverleningsconcepten van dienstverleners. Een dergelijk alternatief scenario past niet bij het huidige open beleid van de overheid.

Hiermee zijn we er nog niet. Illustratief hiervoor is IRMA. Deze oplossing is privacy-vriendelijk en ontsluit persoonsgegevens uit een betrouwbare authentieke overheidsbron. Ondanks deze belangrijke pluspunten neemt de oplossing nog geen grote vlucht. De reden hiervoor is dat naast de bovengenoemde factoren, er nog een factor een belangrijke rol speelt: de eindgebruiker. Vertrouwen van de eindgebruiker in eWallets is cruciaal. Dit vertrouwen van de eindgebruiker is niet zomaar opgebouwd. Dit kost tijd en verdwijnt weer snel als zaken niet goed gaan. eIDAS schept de kaders om dit vertrouwen te borgen, maar zorgt niet direct voor de opbouw ervan. Vooral voor private aanbieders van eWallets lijkt het moeilijk om dit vertrouwen op te bouwen. In een aantal gevallen probeert men mee te liften op het vertrouwen dat banken genieten (b.v. Ockto, Datakeeper). Door de overheid aanboden of gecertificeerde eWallets zouden sneller vertrouwd en dus geaccepteerd kunnen worden.

Met de wijziging van de eIDAS wetgeving ontstaat een uniforme Europese markt van zo'n 450 miljoen gebruikers voor eWallet aanbieders. Het is niet ondenkbaar dat techgiganten als Apple en Google deze markt met gecertificeerde eWallets zullen betreden. Ondanks het feit dat de eWallet gratis moet worden aangeboden is een verdienmodel te vinden in de integratie van eWallets met andere, betaalde toegevoegde waarde diensten. Deze diensten kunnen (met toestemming van de gebruiker) gegevens uit de eWallet en gegevens uit het gebruik van de eWallets verwerken voor tal van innovatieve toepassingen. De techgiganten hebben op dat vlak in veel opzichten een zeer sterke uitgangspositie. Het huidige beleid van de Nederlandse overheid staat toe dat eWallets van dergelijke techgiganten kunnen toetreden tot het Nederlandse ecosysteem voor digitale identiteiten en erkend moeten worden als zij voldoen aan de wettelijke kaders.

Vervolgactiviteiten

Concreet leidt de bovenstaande analyse tot de volgende aanbevolen vervolgactiviteiten:

1. Verken de mogelijkheden voor het creëren van vertrouwen in eWallets bij gebruikers.
2. Voer een business case analyse uit op eWallets met eID-Hoog en gekwalificeerde ondertekenfunctionaliteit om de kosten/baten transparant te maken. Probeer eventuele belemmeringen daarbij weg te nemen om zodoende de adoptie van eWallets te bespoedigen.
3. Verken de haalbaarheid en wenselijkheid van het laten doorontwikkelen van DigiD tot een eWallet oplossing.
4. Organiseer een consultatieronde om interesse te peilen bij potentiële eWallet aanbieders. Doe dit tijdig om aanbieders van eWallets de mogelijkheid te geven om een eWallet te ontwikkelen die aan alle eIDAS eisen voldoet, of, in het geval er geen interesse is vanuit de markt, om zelf de ontwikkeling van een eWallet te initiëren (zie het vorige punt).

6 Bredere context

Wat is er al geregeld en onderzocht in voorschriften en standaarden op het terrein van eWallets en wat moet verder onderzocht worden? Deze sectie gaat hier dieper op in. Aanbevelingen voor vervolgactiviteiten zijn cursief in de tekst opgenomen.

6.1 Huidige eIDAS infrastructuur

De huidige Nederlandse infrastructuur voorziet in elektronische identificatie van Europese gebruikers die willen inloggen bij aangesloten Nederlandse dienstverleners en van Nederlandse gebruikers die bij buitenlandse dienstverleners willen inloggen. De architectuur hiervoor is beschreven[27]. Centraal daarbij staat het Nederlandse eIDAS koppelpunt dat in verbinding staat met soortgelijke koppelpunten in de andere lidstaten, verbindingen heeft met de achterliggende stelsels als eHerkenning en DigiD, en koppelingen kent met de BRP- en BSN-koppelpunten. Over deze infrastructuur worden identiteitsgegevens ten behoeven van unieke identificatie van gebruikers uitgewisseld; de set van attributen zoals in de huidige versie van de eIDAS verordening is gedefinieerd.

Binnen de technische subgroep van eIDAS vindt de doorontwikkeling van de huidige infrastructuur plaats. Eén van die ontwikkelingen is het uitbreiden van de set van attributen met bijvoorbeeld sectorspecifieke attributen of met specifieke attributen op verzoek van een lidstaat voor een bepaalde dienst. Niet altijd zullen deze attributen door de huidige eIDAS eID-aanbieders zelf kunnen worden geleverd. Typisch zullen deze attributen uit authentieke bronnen komen. Dat zullen dezelfde bronnen zijn waar eWallets gebruik van maken. Zal het de moeite lonen om authentieke bronnen op de huidige eIDAS-infrastructuur aan te laten sluiten?

De interactie tussen een eWallet en een vertrouwende partij verschilt aanzienlijk ten opzicht van de huidige interactie tussen een eID-middel en een vertrouwende partij (zie hoofdstuk 4). Daar waar vooral publieke vertrouwende partijen zelf nog extra informatie over de gebruiker ophalen bij de basisregistraties, bieden eWallets de mogelijkheid om deze gegevens direct aan te leveren. Gegevensuitwisselingen in de Nederlandse infrastructuur voor identiteit kunnen dus anders gaan verlopen met de komst van succesvolle eWallets.

De Nederlandse eIDAS infrastructuur is ten opzichte van andere lidstaten relatief succesvol. In de maand november van dit jaar bedroeg het aantal authenticaties vanuit andere lidstaten bij Nederlandse dienstaanbieders meer dan 10.000[44]. Bijna 300 Nederlandse dienstverleners zijn aangesloten. Dit aantal is redelijk stabiel. Vanaf 1 september 2021 is het mogelijk geworden om met een Nederlands erkend inlogmiddel (eHerkenning) over de grens online zaken te regelen. In november waren dit er 114 ten opzichte van 82 in oktober.

De gereviseerde verordening geeft aan dat de huidige eIDAS infrastructuur en bijbehorende genotificeerde eID-middelen blijven bestaan.

Overweeg de inrichting van een Wallet Proxy in deze infrastructuur om de transitie naar eWallets te faciliteren en vertrouwende partijen te ontzorgen. Overweeg een herinrichting van de huidige eIDAS infrastructuur pas als eWallets zich daadwerkelijk hebben ontwikkeld tot primair eID in de markt.

6.2 Wet digitale overheid

De voorgestelde Wet digitale overheid (Wdo) betreft een infrastructuur voor het authentiseren van burgers; publieke dienstverleners zijn verplicht de authenticatiemiddelen die zijn toegelaten onder de Wdo te accepteren[45]. In ieder geval zullen dit DigiD en eHerkenning zijn. Tevens stelt het eisen aan het gebruik van authenticatiemiddelen met passend betrouwbaarheidsniveaus voor de dienst die er mee ontsloten wordt. De gegevens die onder Wdo kunnen worden uitgewisseld zijn ook de gegevens die de toegelaten authenticatiemiddelen kunnen verwerken. De wet regelt hiernaast dat standaarden overheidsbreed verplicht

[44] Dashboard eIDAS, Logius, editie december 2021.
[45] Wet digitale overheid, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/.

kunnen worden opgelegd bij Algemene Maatregelen van Bestuur. Standaarden die hier in vastgelegd zullen worden gaan onder meer over toegankelijkheid en veiligheid.

In februari 2020 hebben de heren Middendorp en Verhoeven nog een amendement voorgedragen op de Wdo waarin geregeld wordt dat iedere Nederlandse burger een unieke online identiteit krijgt, die het mogelijk maakt gegevens die de burger betreft digitaal in te zien, en waar mogelijk te corrigeren en uit te wisselen met derden[46]. Dit amendement is aangenomen en is dus onderdeel wat het wetsvoorstel zoals het momenteel bij de eerste kamer ligt. Het toont duidelijke gelijkenissen met wat eIDAS beoogt met de eWallet. Bovendien valt de eWallet in de functie van eID-middel al binnen de scope van de huidige voorgestelde Wdo.

Het is aan te bevelen om in de volgende tranche van de Wdo specifieke elementen uit de gereviseerde eIDAS verordening op te nemen rondom eWallets, en dan met name rondom de authentieke bronnen.

6.3 Onderzoeken regie op gegevens / Self Sovereign identity

De InnoValor studie “PDM landschap 2020 - Regie op gegevens in Nederland” geeft een overzicht van het nationale en internationale landschap van oplossingen voor personal data management[35]. Het beschrijft tal van oplossingen die een invulling proberen te geven aan het eWallet concept. De studie geeft aan dat om tot een daadwerkelijk volwassen en interoperabel personal data management landschap te komen, er nog stappen gezet moeten worden. De overheid kan hierin een stimulerende en kaderstellende rol spelen:

- Wetgeving kan legitimeren en stimuleren, zoals de Payment Services Directive (PSD2) dit doet in de financiële sector;
- Kaders stellen kan interoperabiliteit bevorderen. Dit is nodig om op termijn echt regie op gegevens te voeren. Tevens kunnen kaders het vertrouwen van de eindgebruiker in personal data management (PDM) vergroten;
- Eisen stellen aan verdienmodellen, zowel op business als maatschappelijk niveau;
- Door te subsidiëren kunnen ontwikkeling gestimuleerd worden, zoals VWS doet in de zorg.

Het uitwerken van dergelijke stappen tot een routekaart, waarin beslismomenten en scenario’s helder in kaart gebracht worden, kan hierbij helpen.

Het recente rapport “SSI speelveldanalyse” van Innopay en TNO doet de volgende aanbevelingen voor de Nederlandse overheid om de bijdragen van het digitaal kunnen uitwisselen van geverifieerde gegevens op verschillende publieke waarden te helpen realiseren[35]:

1. Stel geïntegreerde visie op voor het Nederlandse landschap van digitale identiteit en gegevensuitwisseling en koppel dat aan een ambitieuze uitvoeringsagenda
2. Stuur op consolidatie van het speelveld rond digitale gegevensuitwisseling via een Publiek Private Samenwerking.
3. Doorbreek als overheid het kip-ei probleem voor digitale gegevensuitwisseling door als ‘first mover’ zelf pro-actief brondata aan te bieden en te consumeren.

Het rapport “SSI speelveldanalyse” beschrijft ook een bredere context van initiatieven die van nut is voor dit onderzoek. Denk hierbij aan het programma Regie op Gegevens, de Revised Payment Services Directive (PSD2) en internationale initiatieven rondom SSI en blockchain. We verwijzen naar dit rapport voor inhoudelijke details. De uitkomsten zijn herkenbaar: er zijn veel nationale en internationale ontwikkelingen en initiatieven die van invloed zijn op de door eIDAS beoogde Europese eWallet. Het omgekeerde geldt echter ook: veel van de initiatieven krijgen met de kaders die eIDAS gaat stellen voor eWallets de mogelijkheid om zich te ontwikkelen tot volwassen oplossingen.

Ook het Europese agentschap voor netwerk- en informatiebeveiliging (ENISA) heeft een studie uitgevoerd naar de mogelijkheden van het SSI concept voor digitale identiteiten[47]. ENISA stelt dat SSI-technologie een solide basis vormt voor het realiseren van decentrale identiteiten middels eWallets. Het constateert dat vanuit

[46] Zie https://zoek.officielebekendmakingen.nl/kst-34972-20.html.
[47] ‘Digital identity – leveraging the SSI concept to build trust’, ENISA, November 2021, Final Draft.

bestuurlijk perspectief certificatie van eWallets en toezicht op authentieke bronnen en de gedistribueerde identifier infrastructuur wenselijk is.

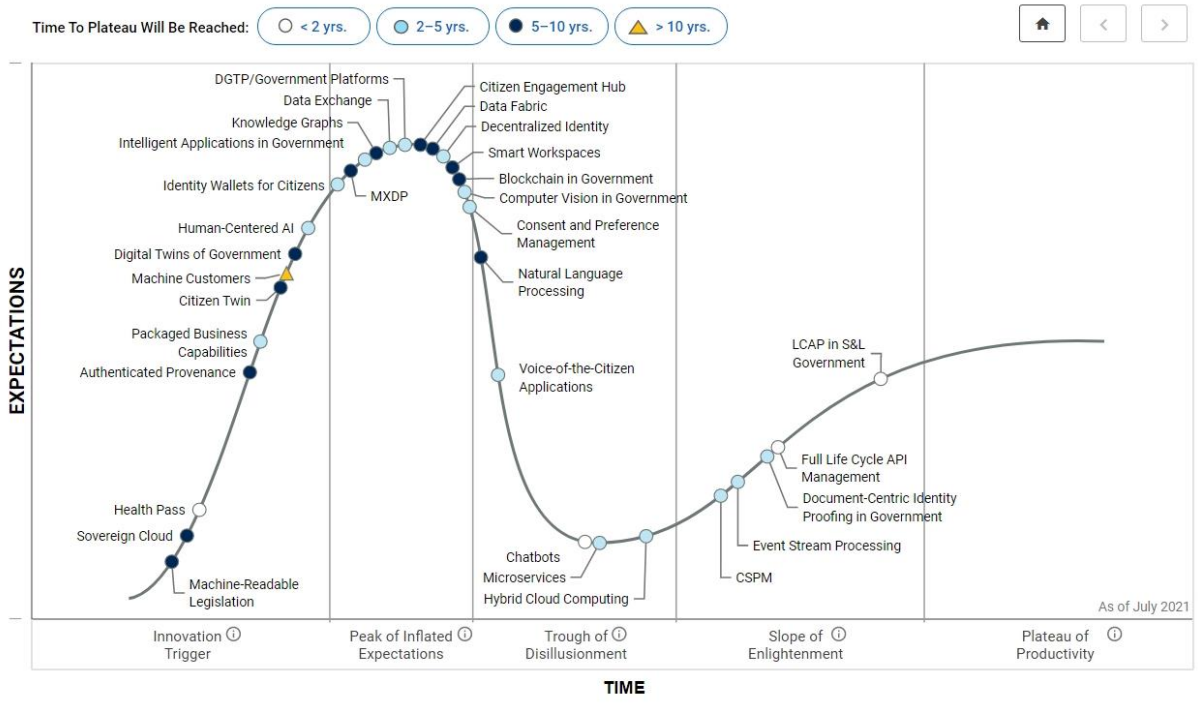
Het is aan te bevelen om na te gaan of het huidige toezicht op authentieke bronnen en de eID infrastructuur in Nederland moet worden aangepast op de wijzigingen die het gevolg zijn van het eIDAS amendement of de uitwerking daarvan in de Toolbox.

Met de gedistribueerde identifier infrastructuur doelt ENISA op de zogenaamde Decentralized Identifiers (DIDs). DIDs vormen een essentieel onderdeel van SSI (en dus eWallets) en maken het verifiëren van een decentrale digitale identiteit mogelijk. Vaak wordt er op de achtergrond gebruik gemaakt van blockchain en publieke sleutel cryptografie. De W3C heeft deze standaard ontwikkeld[48]. Mogelijk gaan DIDs onderdeel uitmaken van de Toolbox. Het is nog onduidelijk hoe deze DIDs zich verhouden tot de huidige identifier infrastructuur van eIDAS en de Nederlandse infrastructuur met BSN en polymorfe pseudoniemen.

Onderzoek hoe Decentralized Identifiers (DIDs) zich verhouden tot de huidige identifier infrastructuur van eIDAS en de Nederlandse infrastructuur met BSN en polymorfe pseudoniemen.

6.4 Overig marktonderzoek - Gartner

De 'hype cycle for digital government technology 2021' van Gartner positioneert eWallets en gedecentraliseerde identiteiten hoog in de hype cycle[49] (Figuur 9).



Figuur 9: eWallets in de Gartner 'hype cycle for digital government technology, 2021'.

Duidelijk uit de hype cycle is dat het nog wel enkele jaren zal duren voordat eWallets het zogenaamde 'Plateau of Productivity' bereikt hebben. Gartner identificeert daarbij de volgende obstakels:

- Het ontbreken van volwassen normen en definities voor eWallets. Leveranciers en overheden bestempelen propriëtaire mobiele apps die slechts beperkt gebruik en interoperabiliteit hebben als eWallets. Het is onwaarschijnlijk dat deze zullen worden opgeschaald voor nieuwe en onvoorziene use cases.

[48] 'Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations', W3C Proposed Recommendation, 3 August 2021, zie https://www.w3.org/TR/did-core/.
[49] Gartner, Hype Cycle for Digital Government Technology, 2021.

- Politieke onzekerheden. (Digitale) identiteit is een controversieel onderwerp met een grote variatie aan connotaties en gevoeligheden tussen geografische en maatschappelijke groepen. Nationale debatten over digitale soevereiniteit dragen bij aan de onzekerheid over waar regeringen de adoptie en regulering van met name digitale identiteit en eWallets zullen proberen te sturen.
- Adoptie door burgers. Burgers mogen geen eWallets accepteren zonder zekerheid over controle, privacy en veiligheid. Ze kunnen ook weinig interesse tonen, tenzij er use cases met toegevoegde waarde zijn en een gebruikerservaring met weinig wrijving.
- Smartphone penetratie. eWallets zijn afhankelijk van burgers die in het bezit zijn van een geschikte smartphone, waardoor de digitale kloof groter kan worden. Dit moet worden aangepakt om te voorkomen dat burgers hun rechten worden ontnomen.

Gartner doet de volgende aanbevelingen met betrekking tot eWallets:

- Identificeer kansen en implicaties van burgergerichte eWallets door use cases te identificeren, proof-of-concepts te ontwikkelen en pilots te doen waarbij belanghebbenden in verschillende sectoren betrokken zijn en die concrete voordelen nastreven voor houders, uitgevers en verificateurs van identiteitsgegevens.
- Realiseer de verschillende rollen die de overheid kan spelen, bijvoorbeeld als authentieke bron, vertrouwende partij, toezichthouder, aanbieder van een eWallet of bij de verificatie van attributen/attesteringen. Overheden kunnen onderzoeken hoe eWallets interageren met de evoluerende digitale identiteitsecosystemen, met name voor gedecentraliseerde en zelf-soevereine identiteiten. Overheden kunnen ook manieren identificeren waarop ze burgers kunnen ondersteunen bij het maken van weloverwogen keuzes over hun vertrouwen in en gebruik van identiteitsportefeuilles.
- Promoot open, transparante en schaalbare infrastructuren voor eWallets door compatibiliteit met opkomende standaarden en deelname aan consortia voor eWallets onderdeel te maken van de ontwikkeling van het nationale ecosysteem voor identiteiten en door voortijdige lock-ins van leveranciers of technologie te voorkomen.

Aangaande gedecentraliseerde identiteiten, ofwel SSI, ziet Gartner ook nog diverse obstakels:

- Ondanks veel belofte en hype, verloopt de acceptatie traag vanwege gebrek aan vooruitgang en inactiviteit door de meeste grote ecosysteemspelers, CIAM-leveranciers en verschillende identiteitsleveranciers (identity providers), waaronder overheden.
- Normen bevinden zich nog in de ontwikkelingsfase.
- Gebrek aan blockchain-prestaties, interoperabiliteit, schaalbaarheid en volwassenheid.
- Gebrek aan duidelijke beveiligingsstandaarden voor eWallets en eventuele onderliggende blockchain technologie.
- Gebrek aan oplossingen op productieniveau, waardoor sommige organisaties niet kunnen implementeren vanwege zorgen dat ze in de nabije toekomst moeten "rippen en vervangen" wanneer de oplossingen zich stabiliseren.

De aanbevelingen die Gartner dan ook doet voor gedecentraliseerde identiteiten zijn:

- Ga aan de slag met haalbare use cases die met beperkte implementatie-effort te realiseren zijn in de vorm van een pilot of proof-of-concept. Participeer in consortia voor een breder draagvlak.
- Wees voorzichtig met te optimistische claims van leveranciers. Evalueer de technische beveiligingsaspecten van blockchain-platforms die worden overwogen. Onderzoek in het bijzonder leveranciersplannen voor ondersteuning van standaarden, zoals World Wide Web Consortium (W3C)[50] en Decentralized Identity Foundation (DIF)[51].

De gesignaleerde obstakels en aanbevelingen komen op hoofdlijnen overeen met de uitkomsten van de eerder genoemde nationale onderzoeken over regie op gegevens en SSI. Duidelijk is ook dat de voorgestelde eIDAS verordening een aantal obstakels weg zal nemen en invulling geeft aan diverse aanbevelingen.

[50] World Wide Web Consortium, zie https://www.w3.org/.
[51] Decentralized Identity Foundation, zie https://identity.foundation/.

6.5 Afsprakenstelsels

Nederland kent diverse afsprakenstelsels voor gecontroleerd data delen: eHerkenning (bedrijvendomein), MedMij (zorgdomein), iShare (logistiek), SURFconext (onderwijs), etc. Zoals in hoofdstuk 3 benoemd, kan de eWallet van invloed zijn op hoe gegevens binnen dergelijke afsprakenstelsels uit te wisselen. Anderzijds kunnen dergelijke afsprakenstelsel ook als bron fungeren voor het laden van eWallets met machtigingen, zorgdata, logistieke data of onderwijsdata.

Hoe dit in de eWallet precies wordt ingevuld moet nog worden vastgesteld. Vertegenwoordigers van de diverse afsprakenstelsels lijken soms nog ver af te staan van de ontwikkeling van de Toolbox waarin dit soort ontwerpbeslissingen worden genomen. Een voorbeeld; uit een door Innovalor in opdracht van het Europese GÉANT uitgevoerd onderzoek naar de impact van eIDAS eWallets op de Europese trust & identity providers voor het hoger onderwijs en onderzoek kwam naar voren dat eWallets veel kansen bieden voor het verbeteren van student mobiliteit en het faciliteren van Lifelong Learning. Maar tegelijkertijd is het de sector nog niet duidelijk of eWallets hiervoor daadwerkelijk 'fit for use' zullen zijn. Koepels en vertegenwoordigers van sectorale identity frameworks kunnen hier een rol pakken, door inbreng in de Toolbox ontwikkeling en door standaards en afsprakenstelsels te ontwikkelen rond de voor hen relevante eWallet content.

6.6 Standaarden voor gegevensuitwisseling en -verificatie

De werking van eWallets is mede gebaseerd op het W3C Verifiable Credentials Data Model[52]. Voor elk van de processen in dit model zijn relevante standaarden beschikbaar. Deze sectie geeft een overzicht van de belangrijkste standaarden. Naar verwachting worden in de Toolbox een aantal standaarden voorgeschreven of geadviseerd.

6.6.1 SAML, OpenID Connect, FIDO2.0

SAML, OpenID Connect en FIDO2.0 zijn standaarden voor het uitwisselen van identiteitsverklaringen ten behoeve van het authentiseren van de gebruiker. Typisch bevatten de identiteitsverklaringen hiervoor een aantal attributen en/of identifiers. Oplossingen als DigiD, eHerkenning, SURFconext en iDIN zijn SAML-gebaseerd. Ook het huidige eIDAS is gebaseerd op SAML. OpenID Connect en FIDO2.0 kunnen worden gezien als meer moderne en eenvoudigere varianten van SAML.

Deze standaarden zijn niet geschikt om grotere hoeveelheden gegevens in een identiteitsverklaring te verwerken. Daarvoor zijn andere standaarden nodig. Kandidaten hiervoor zijn bijvoorbeeld JSON, XML of PDF. Deze standaarden zijn ook te vinden op de verplichte en aanbevolen lijsten van het Forum Standaardisatie[53]. In het geval nieuwe standaarden deel gaan uitmaken van de eWallet Toolbox is het verstandig het Bureau Forum Standaardisatie hiervan op de hoogte te stellen.

SAML, OpenID Connect en FIDO2.0 gebaseerde verklaringen zijn met een digitale handtekening beschermd. Typisch op basis van eIDAS gekwalificeerde certificaten. Deze handtekeningen zijn middels een Public Key Infrastructuur (PKI) eenvoudig te verifiëren. Hetzelfde geldt voor de JSON, XML en PDF standaarden.

6.6.2 Mobile driving license (mDL)

Onlangs is een nieuwe internationale norm gepubliceerd met technische eisen voor het opslaan van het rijbewijs op de mobiele telefoon: ISO/IEC 18013-5:2021 mobile driving license (mDL) application[54]. De norm stelt eisen aan de interface van het rijbewijs op een mobiele telefoon. Andere organisaties dan de uitgevende instantie, kunnen daardoor de gegevens van het mobiele rijbewijs verkrijgen, het mobiele rijbewijs aan de rijbewijshouder koppelen en de oorsprong en integriteit van het mobiele rijbewijs verifiëren. Ook maakt deze norm het mogelijk om de gebruiker de volledige controle te geven over welke data met wie wordt gedeeld. Naast de omschrijving van het datamodel voor het mobiele rijbewijs, bevat de norm ook algemene protocollen om de uitwisseling en controle van andere identiteitsdocumenten mogelijk te maken.

[52] W3C Verifiable Credentials, zie https://www.w3.org/TR/vc-data-model/.
[53] Forum Standaardisatie lijsten van standaarden, zie https://www.forumstandaardisatie.nl/open-standaarden
[54] Zie https://www.nen.nl/nen-iso-iec-18013-5-2021-en-288068.

6.6.3 Overige

Voor het plaatsen van een gekwalificeerde digitale handtekening met de eWallet dient gebruik gemaakt te worden van certificaten van eIDAS vertrouwensdiensten. Standaarden hiervoor hebben zich de afgelopen periode onder de huidige eIDAS verordening bewezen.

De voorgestelde eIDAS verordening benoemd geen standaarden voor gegevensuitwisselingen maar stelt wel dat de interfaces tussen eWallets, vertrouwensdiensten en vertrouwende partijen gestandaardiseerd moet zijn (zie paragraaf 2.2.1). Voor gegevensuitwisseling tussen eWallets en authentieke bronnen kan het ontbreken van standaarden mogelijk onwenselijke gevolgen hebben (zie paragraaf 2.3). Aan de andere kant is het van belang van eWallets dat ze gegevens uit zoveel mogelijk bronnen kunnen ontsluiten. eWallets zullen zich dan moeten aanpassen aan de standaarden die door de bronnen worden gehanteerd. Dit kan de ene keer SAML zijn via afgeleide authenticatie, de andere keer het middels NFC-uitlezen van de chip van een paspoort, of om via een applicatie interface van de bron zelf een PDF op te halen. Tot slot zullen ook de use cases van invloed zijn op de te gebruiken standaard. De verwachting is dat er use case specifieke (ofwel sector-specifieke) standaarden gebruikt zullen worden voor gegevensuitwisselingen met eWallets.

Adresseer in de eIDAS Expert Group de wenselijkheid en haalbaarheid van standaardisatie van interfaces in het eWallet ecosysteem, met name ten aanzien van de interactie tussen eWallets en authentieke bronnen.

6.7 EU Single Digital Gateway

De Single Digital Gateway (SDG) is een Europese verordening met als doel om burgers en bedrijven makkelijk toegang tot digitale overheidsdienstverlening in de Europese Unie te verlenen[55]. Dat gebeurt met het portaal Your Europe. Deze centrale toegangspoort verwijst gebruikers door naar de juiste websites in de verschillende lidstaten. Via Your Europe kunnen burgers en bedrijven op een eenvoudige manier betrouwbare informatie vinden over overheidsdiensten,-producten en -procedures in Europa. Sommige procedures kunnen ze bovendien online doorlopen. Daarbij kunnen burgers en bedrijven overheden toestemming geven om onderling digitaal relevante bewijsstukken uit te wisselen.

In de SDG verordening worden 21 procedures genoemd die online en grensoverschrijdend moeten worden aangeboden, waaronder:

- Geboorte: het aanvragen van een bewijs van registratie van een geboorte;
- Verblijf: aanvraag van bewijs van verblijf;
- Verhuizing: registratie van een adreswijziging en inschrijving van een motorvoertuig;
- Starten, exploiteren en sluiten van een bedrijf: kennisgeving van een bedrijfsactiviteit en vergunningen voor de uitoefening van een bedrijfsactiviteit.

Dergelijke procedures en de gegevensuitwisseling die daarvoor nodig is, zouden ook via een eWallet kunnen worden uitgevoerd. De eIDAS eWallet vertoont dus grote raakvlakken met de SDG.

Voorkomen dient te worden dat er twee onafhankelijke architecturen gaan ontstaan voor gegevensuitwisseling in Europa. Afstemming met de Nederlandse SDG vertegenwoordigers over wat waar te regelen is noodzakelijk.

6.8 Blockchain – ESSIF – EBSI - DBC

Blockchain wordt gezien als een mogelijke infrastructuur en bron voor eWallets. In Europa wordt er gebouwd aan een Europees Self-sovereign Identity Framework (ESSIF). Dit maakt deel uit van de Europese Blockchain Service Infrastructuur (EBSI). De Europese Commissie en het European Blockchain Partnership (EBP) willen met deze digitale infrastructuur een standaard realiseren waarbinnen EU-brede bouwstenen passen voor grensoverschrijdende openbare diensten, waaronder eWallets. Het ministerie van BZK en RvIG zijn vertegenwoordigd in deze initiatieven en denken na over beleid en toepassingsmogelijkheden. Ook wordt er in dit kader nauw samengewerkt met de Dutch Blockchain Coalition (DBC), een samenwerkingsverband tussen partners uit de overheid, kennisinstellingen en het bedrijfsleven. De missie van de DBC is om kennis over en het gebruik van blockchain te vergroten en daarmee de decentrale inrichting van de digitale infrastructuur in

[55] SDG, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/europa/single-digitale-gateway/#:~:text=De%20Single%20Digital%20Gateway%20(SDG,portaal%20(gateway)%20Your%20Europe%20.&text=Eind%202023%20is%20het%20voor,te%20regelen%20met%20Europese%20overheden.

Nederland te versnellen. De DBC is hierin vooral een katalysator en een facilitator, die een omvangrijk publiek-privaat netwerk activeert en verbindt. Al met al kan worden geconcludeerd dat Nederland goed is geïntegreerd in Europese blockchain initiatieven en er voldoende kennis op dit vlak aanwezig is.

7 Conclusies en aanbevelingen

Conclusies

Europa heeft grote ambities met het verplicht stellen van eWallets in de herziene eIDAS verordening. De eisen die aan eWallets worden gesteld zijn hoog. Een eWallet moet niet alleen gebruikers elektronisch kunnen identificeren op het hoogste betrouwbaarheidsniveau (authenticatie), maar daarnaast ook nog een veel rijkere set van gegevens (attributen, attesteringen, credentials) over die gebruiker en onder diens regie kunnen uitwisselen met geregistreerde vertrouwende partijen, ofwel dienstverleners. Aangewezen authentieke bronnen dienen voor de aanlevering van de gegevens te zorgen. Het geheel is complex en veelomvattend – zowel technisch, organisatorisch als juridisch – en de voorgestelde tijdspanne voor realisatie is kort. Het is dus zaak voor de Nederlandse overheid en de betrokken stakeholders om doortastend en pragmatisch aan de slag te gaan met de realisatie van een nationaal elektronisch identiteiten ecosysteem waarin eWallets naast andere eID-oplossingen zoals DigiD en eHerkenning opereren.

Het huidige landschap van eWallets is echter nog onvoldoende volwassen om direct een plaatsje in het beoogde ecosysteem voor identiteiten te veroveren. Bestaande eWallets voldoen nog niet aan alle eIDAS eisen voor niveau Hoog en ontberen vertrouwen bij de gebruiker en vertrouwende partijen. Hier zullen nog stappen moeten worden gezet en de voorgestelde eIDAS verordening helpt daarbij significant.

Een andere uitdaging is dat het gebruik van eWallets voor de gebruiker gratis moet zijn. Deze eis zet het verdienmodel voor aanbieders van eWallets onder druk.

Het hele speelveld overziend, zijn er drie factoren die essentieel zijn voor het succes van eWallets:

1. De aanwezigheid van authentieke bronnen die (EU-)gestandaardiseerde gegevens (attributen, attesteringen, credentials) over de gebruiker kunnen delen met een eWallet en geverifieerd kunnen worden door vertrouwende partijen. Immers, zonder betrouwbare en gestandaardiseerde gegevens kunnen vertrouwende partijen geen waarde creëren en verliezen eWallets hun meerwaarde. Hoe meer authentieke bronnen beschikbaar komen, des te groter is het aantal use cases dat vertrouwende partijen voor eWallets kunnen ontwikkelen.

2. De aanwezigheid van voldoende publieke en private vertrouwende partijen die gegevens van eWallets willen afnemen om hiermee de gebruiker toegang te geven tot diensten en om persoonlijke dienstverlening op maat aan te bieden. Zonder voldoende afnemende vertrouwende partijen heeft een eWallet voor een gebruiker geen meerwaarde.

3. De aanwezigheid van eWallets die het vertrouwen genieten van gebruikers voor het verwerken van hun gegevens. Immers, als er geen vertrouwen is, zal de gebruiker er niet mee aan de slag gaan en zijn alle investeringen aan de kant van de authentieke bronnen en vertrouwende partijen nutteloos geweest.

Gegeven de complexiteit van de realisatie van deze succesfactoren is een pragmatische en gebalanceerde beleidsmatige aanpak wenselijk. Hierbij dient de overheid een actieve rol te spelen door een gezonde voedingsbodem voor Nederlandse eWallets te realiseren en bovenal de betrokken publieke en private partijen daarbij actief te betrekken. De basisfunctionaliteit van eWallets betreft in ieder geval eID functionaliteit en de attestering van een set verplichte attributen. Door te focussen op ontwikkeling van use cases die voor Nederland relevant zijn kunnen eWallets succesvol worden. Deze use cases bepalen welke authentieke bronnen en vertrouwende partijen moeten worden opgelijnd en waardoor eWallets de mogelijkheid krijgen om te floreren door van meerwaarde te zijn voor eindgebruikers.

Aanbevelingen

Voor **authentieke bronnen** doen wij hiervoor de volgende aanbevelingen:

1. Werk uit hoe de minimale set van attributen ten behoeve van eID functionaliteit op eWallets te krijgen. Kan dit middels afgeleide authenticatie met een al genotificeerd middel op eIDAS niveau Hoog

(bijvoorbeeld DigiD) of zijn hiervoor andere registratie- en activatieprocessen door de aanbieder van een eWallet zelf nodig of wenselijk? Is het mogelijk en nodig om BSN op een eWallet te hebben staan? Welke authentieke bronnen zijn hiervoor nodig? Kunnen deze bronnen ook geïnterpreteerde attributen vrijgeven, zoals 16+, 18+ en 65+ in plaats van geboortedatum?
2. Adresseer in de eIDAS Expert Group de wenselijkheid en haalbaarheid van standaardisatie van interfaces in het eWallet ecosysteem, met name ten aanzien van de interactie tussen eWallets en authentieke bronnen.
3. Bepaal welke eWallet use case de meest veelbelovende is voor de Nederlandse markt en welke authentieke bronnen hiervoor nodig zijn. Organiseer dat deze bronnen op tijd klaar zijn met het ontsluiten van de gewenste gegevens richting eWallets en zodanig dat de dienstverleners deze bij ontvangst kunnen verifiëren als authentiek.
4. Beleg de inrichting en het beheer van een register voor authentieke bronnen.

De eisen die worden gesteld aan **eWallets** zijn hoog en complex. Deze eisen komen voort uit de verordening en de uitwerking zal krachtens de verordening plaatsvinden in uitvoeringshandelingen of de Toolbox. De Nederlandse overheid zal deze eisen vervolgens moeten vertalen naar passende eisen voor ons nationale ecosysteem voor digitale identiteiten:

1. Definieer een raamwerk van eisen waaraan Nederlandse eWallets moeten voldoen op basis van de eIDAS Toolbox of uitvoeringshandelingen en op basis waarvan toezicht kan worden uitgevoerd. De kaders hiervoor zijn de eIDAS uitvoeringsverordening 2015/1502 over betrouwbaarheidsniveaus, de cybersecurity verordening en de nog te ontwikkelen Toolbox. Ook dient rekening te worden gehouden met aanpalende kaders zoals de Algemene Verordening Gegevensbescherming (AVG).

Andere eWallet gerelateerde activiteiten die volgen uit de gereviseerde eIDAS verordening zijn:

2. Organiseer een consultatieronde om interesse te peilen bij potentiële eWallet aanbieders. Doe dit tijdig om eWallet aanbieders de mogelijkheid te geven een eWallet te ontwikkelen die aan alle eIDAS eisen voldoet, dan wel om zelf de ontwikkeling van een eWallet te initiëren bij gebruik aan interesse vanuit de markt.
3. Verken de mogelijkheden voor het creëren van vertrouwen in eWallets bij gebruikers.
4. Voer een business case analyse uit op eWallets met eID-Hoog en gekwalificeerde onderteken functionaliteit om de kosten/baten transparant te maken. Probeer eventuele belemmeringen daarbij weg te nemen om zodoende de adoptie van eWallets te bespoedigen.
5. Onderzoek op welke manier identifiers en pseudoniemen en eventuele voorzieningen hiervoor in het Nederlandse ecosysteem voor het linken van digitale identiteiten en eWallets effectief en privacy-vriendelijk kunnen worden ingezet.
6. Onderzoek de voor- en nadelen van het laten doorontwikkelen van de huidige DigiD eID oplossing naar een DigiD eWallet.
7. Onderzoek oplossingen en implicaties voor het digitaal rechtsgeldig ondertekenen van verklaringen door de gebruiker middels een eWallet. Doe dit ook in de context van juridische personen (bedrijven) voor digitale verzegeling.

Betreffende **vertrouwende partijen** ofwel dienstverleners zijn de volgende activiteiten noodzakelijk:

1. Definieer de criteria op basis waarvan Nederlandse vertrouwende partijen gebruik mogen maken van eWallets. Dienen deze partijen, in analogie met bijvoorbeeld DigiD, periodiek een beveiligingsassessment te laten uitvoeren of zijn andere oplossingen mogelijk?
2. Informeer publieke en private vertrouwende partijen die met gegevens uit eWallets aan de slag (willen) gaan. Organiseer hiervoor bijvoorbeeld een overleg met dienstverleners in de publieke en private sector. Deze partijen kunnen zich dan tijdig voorbereiden op pilots met eWallets.
3. Beleg het inrichten en het beheer van een register van vertrouwende partijen en door hen aangeboden diensten.
4. Stem met Nederlandse vertegenwoordigers van de EU Single Digital Gateway (SDG) af waar eIDAS ophoudt en waar SDG begint, zodat vertrouwende partijen weten welke infrastructuur ze moeten gebruiken.

Generieke meer **ecosysteem**-gerelateerde aanbevelingen zijn:

1. Ontwerp de algehele architectuur van het Nederlandse ecosysteem voor digitale identiteiten inclusief eWallets en bijbehorende rollen. Houd rekening met bestaande voorzieningen als DigiD, eHerkenning, BSNk en BRP-koppelpunt en nieuwe voorzieningen als de diverse registers en eventuele proxies. Doorloop de architectuur aan de hand van een aantal use cases voor eIDAS inkomend en uitgaand verkeer. Maak gebruik van bestaande architecturen zoals ontworpen voor de huidige eIDAS inrichting in Nederland. Breng eventuele risico's in kaart die volgen uit de architectuur, zoals een single-point-of-failure.
2. Verken en borg oplossingen voor het harmoniseren en effectief voeren van toezicht op het Nederlandse digitale identiteiten ecosysteem inclusief eWallets en het gebruik ervan door vertrouwende partijen. Ga daar bij na of en waar het huidige toezicht moet worden aangepast op de wijzigingen die het gevolg zijn van het eIDAS amendement of de uitwerking daarvan in de Toolbox.
3. Breng de gevolgen van eWallets op de bestaande identiteit-gerelateerde gegevensuitwisselingen door overheidsdienstverleners (uitvoeringsorganisaties, de gemeenten en andere medeoverheden) in kaart. Bijvoorbeeld: voorziet de eWallet de overheidsdienstverlener van alle gevraagde attributen, of volstaat de aanlevering van slechts het BSN op basis waarvan de overheidsdienstverlener via de BRP de overige benodigde attributen kan ophalen? De gekozen architectuur voor het ecosysteem is hierop van invloed.
4. Zoek naar oplossingen om alle nieuwe en bestaande stakeholders zoveel mogelijk te betrekken bij de nieuwe inrichting van het Nederlandse ecosysteem voor digitale identiteiten naar aanleiding van de gereviseerde eIDAS verordening om zodoende gezamenlijk daadkrachtig van start te kunnen gaan met pilots en versnippering te voorkomen.
5. Onderzoek de impact van eWallets op het eHerkenning afsprakenstelsel. Is het bijvoorbeeld wenselijk en mogelijk om de huidige machtigingenregisters van eHerkenning te gebruiken als authentieke bronnen voor eWallets?

Voor bijna alle aanbevelingen is het verstandig om te bepalen of de uitkomsten van eventuele vervolgactiviteiten hun beslag moeten krijgen in volgende tranches van de Wet digitale overheid (Wdo).

Bijlage 1 – Eisen aan eWallets

Deze bijlage bevat de specifiek eisen aan eWallets zoals gesteld in de eIDAS ontwerpverordening. De Engelstalige teksten zijn leidend.

Bron	Requirement	Eis
Art. 6a (3)	European Digital Identity Wallets shall enable the user to: (a) securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services; (b) sign by means of qualified electronic signatures.	Met Europese digitale identiteitsportemonnees kan de gebruiker: (a) veilig opvragen en verkrijgen, opslaan, selecteren, combineren en delen, op een manier die transparant is voor en herleidbaar is voor de gebruiker, van de noodzakelijke identificatiegegevens van rechtspersonen en elektronische attesteringen van attributen om online en offline te authentiseren om online te gebruiken openbare en particuliere diensten; (b) ondertekenen door middel van gekwalificeerde elektronische handtekeningen.
Art. 6a (4a)	Digital Identity Wallets shall provide a common interface: (1) to qualified and non-qualified trust service providers issuing qualified and non-qualified electronic attestations of attributes or other qualified and non-qualified certificates for the purpose of issuing such attestations and certificates to the European Digital Identity Wallet (2) for relying parties to request and validate person identification data and electronic attestations of attributes (3) for the presentation to relying parties of person identification data, electronic attestation of attributes or other data such as credentials, in local mode not requiring internet access for the wallet (4) for the user to allow interaction with the European Digital Identity Wallet and display an “EU Digital Identity Wallet Trust Mark”	Digitale identiteitsportemonnees bieden een generieke interface: (1) aan gekwalificeerde en niet-gekwalificeerde vertrouwens-diensten die gekwalificeerde en niet-gekwalificeerde elektronische attesteringen van attributen of andere gekwalificeerde en niet-gekwalificeerde certificaten afgeven met het oog op de afgifte van dergelijke attesteringen en certificaten aan de European Digital Identity Wallet (2) voor vertrouwende partijen om persoonsidentificatiegegevens en elektronische attesteringen van attributen op te vragen en te valideren (3) voor de presentatie aan vertrouwende partijen van persoonsidentificatiegegevens, elektronische attestering van attributen of andere gegevens zoals inloggegevens, in lokale modus zonder internettoegang voor de portemonnee (4) voor de gebruiker om interactie met de European Digital Identity Wallet mogelijk te maken en een "EU Digital Identity Wallet Trust Mark" te tonen
Art. 6a (4b)	Ensure that trust service providers of qualified attestations of attributes cannot receive any information about the use of these attributes.	Zekerstellen dat vertrouwensdiensten van gekwalificeerde attesteringen van attributen geen informatie kunnen ontvangen over het gebruik van deze attributen.

Art. 6a (4c)	Meet the requirements set out in Article 8 with regards to assurance level “high”, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication.	Voldoen aan de vereisten van Artikel8 met betrekking tot het betrouwbaarheidsniveau "hoog", met name zoals toegepast op de vereisten voor identiteitsbewijs en -verificatie, en beheer en authenticatie van elektronische identificatiemiddelen.
Art. 6a (4d)	Provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes.	Zorgen voor een mechanisme om ervoor te zorgen dat de vertrouwende partij de gebruiker kan authentiseren en elektronische attesteringen van attributen kan ontvangen.
Art. 6a (4e)	Ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural or legal person is associated with it.	Ervoor zorgen dat de in Artikel12, lid 4, punt (d), bedoelde persoonsidentificatiegegevens op unieke en duurzame wijze de natuurlijke of rechtspersoon vertegenwoordigen die ermee in verband wordt gebracht.
Art. 6a (6)	The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance ‘high’.	De Europese digitale identiteitsportemonnees worden uitgegeven in het kader van een ‘notified’ elektronisch identificatiesysteem met een betrouwbaarheidsniveau "hoog".
Art. 6a (6)	The use of the European Digital Identity Wallets shall be free of charge to natural persons.	Het gebruik van de European Digital Identity Wallets is gratis voor natuurlijke personen.
Art. 6a (7)	The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it	De gebruiker heeft de volledige controle over de European Digital Identity Wallet. De uitgever van de European Digital Identity Wallet verzamelt geen informatie over het gebruik van de wallet die niet nodig is voor het verlenen van de walletdiensten, noch combineert hij persoonsidentificatiegegevens en andere persoonlijke gegevens die zijn opgeslagen of verband houden met het gebruik van de European Digital Identity Wallet met persoonsgegevens van andere diensten die door deze uitgever worden aangeboden of van diensten van derden die niet nodig zijn voor het leveren van de walletdiensten, tenzij de gebruiker hier uitdrukkelijk om heeft verzocht.

Art. 6a (7)	Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held.	Persoonsgegevens met betrekking tot de levering van Europese digitale identiteitsportemonnees worden fysiek en logisch gescheiden van alle andere gegevens bewaard.
Art. 6a (7)	If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.	Als de Europese digitale identiteit Wallet wordt geleverd door private partijen in overeenstemming met lid 1 (b) en (c), is het bepaalde in Artikel 45f lid 4 van overeenkomstige toepassing.
Art. 6a (8)	Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet.	Artikel 11 is van overeenkomstige toepassing op de European Digital Identity Wallet.
Art. 6a (9)	Article 24(2), points (b), (e), (g), and (h) shall apply mutatis mutandis to Member States issuing the European Digital Identity Wallets.	Artikel 24, lid 2, punten b), e), g) en h) zijn van overeenkomstige toepassing op Lidstaten die de Europese digitale identiteitsportemonnees uitgeven.
Art. 6a (10)	The European Digital Identity Wallet shall be made accessible for persons with disabilities in accordance with the accessibility requirements of Annex I to Directive 2019/882.	De European Digital Identity Wallet wordt toegankelijk gemaakt voor personen met een handicap in overeenstemming met de toegankelijkheidseisen van Bijlage I bij Richtlijn 2019/882.
Art. 6a (11)	Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications and reference standards for the requirements referred to in paragraphs 3, 4 and 5 by means of an implementing act on the implementation of the European Digital Identity Wallet. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Binnen zes maanden na de inwerkingtreding van deze verordening heeft de Commissie technische en operationele specificaties en referentienormen vastgesteld voor de eisen bedoeld in de leden 3, 4 en 5 door middel van een uitvoeringswet betreffende de uitvoering van de Europese digitale identiteitsportemonnee. Deze uitvoeringswet wordt vastgesteld in overeenstemming met de onderzoeksprocedure bedoeld in Artikel 48, lid 2.
Art. 6c (1)	European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a paragraphs 3, 4 and 5 in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.	European Digital Identity Wallets die gecertificeerd zijn of waarvoor een conformiteitsverklaring is afgegeven in het kader van een cyberbeveiligingsregeling op grond van Verordening (EU) 2019/881 en waarvan de referenties zijn gepubliceerd in het Publicatieblad van de Europese Unie, wordt verondersteld te voldoen aan de cyberbeveiligingsrelevante vereisten van Artikel6 bis, leden 3, 4 en 5, voor zover het cyberbeveiligingscertificaat of de verklaring van conformiteit of delen daarvan dekken die eisen.
Art. 12b (6)	For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9.	Voor de toepassing van dit Artikelhoeven Europese digitale identiteitsportemonnees niet te voldoen aan de eisen genoemd in de artikelen 7 en 9.

Bijlage 2 – Eisen gesteld aan lidstaten

Deze bijlage geeft een overzicht van de eisen gesteld aan de lidstaten met betrekking tot de eWallet. De Engelstalige teksten zijn leidend.

Source/Bron	Requirements	Eisen
Art. 6a (1)	For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless access to cross-border public and private services, each Member State shall issue a European Digital Identity Wallet within 12 months after the entry into force of this Regulation.	Om ervoor te zorgen dat alle natuurlijke en rechtspersonen in de Unie veilige, betrouwbare en naadloze toegang hebben tot grensoverschrijdende openbare en particuliere diensten, geeft elke lidstaat binnen twaalf maanden na de inwerkingtreding van deze Regulatie een Europese digitale identiteitsportemonnee uit.
Art. 6a (2)	European Digital Identity Wallets shall be issued: (a) by a Member State; (b) under a mandate from a Member State; (c) independently but recognised by a Member State.	Europese digitale identiteitsportemonnees worden uitgegeven: (a) door een lidstaat; (b) op grond van een mandaat van een lidstaat; (c) onafhankelijk maar erkend door een lidstaat.
Art. 6a (5)	Member States shall provide validation mechanisms for the European Digital Identity Wallets: - to ensure that its authenticity and validity can be verified; - to allow relying parties to verify that the attestations of attributes are valid; - to allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data.	Lidstaten voorzien in valideringsmechanismen voor de Europese digitale identiteitsportemonnees: - om ervoor te zorgen dat de authenticiteit en geldigheid ervan kan worden geverifieerd; - om vertrouwende partijen te laten verifiëren dat de attesteringen van attributen geldig zijn; - om vertrouwende partijen en gekwalificeerde vertrouwensdienstverleners in staat te stellen de authenticiteit en geldigheid van toegekende persoonsidentificatiegegevens te verifiëren.

Art. 6b (1)	Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall communicate it to the Member State where the relying party is established to ensure compliance with requirements set out in Union law or national law for the provision of specific services. When communicating their intention to rely on European Digital Identity wallets, they shall also inform about the intended use of the European Digital Identity Wallet.	Waar vertrouwende partijen van plan zijn te vertrouwen op European Digital Identity Wallets overeenkomstig deze verordening zijn afgegeven, delen zij dit mee aan de Lidstaat waar de vertrouwende partij is gevestigd om te zorgen voor naleving van: vereisten die zijn vastgelegd in het Unierecht of het nationale recht voor het verstrekken van specifieke Diensten. Bij het communiceren van hun intentie om te vertrouwen op Europese Digitale Identiteitsportemonnees, zullen zij ook informeren over het beoogde gebruik van de Europese Digitale Identiteitsportemonnee.
Art. 6b (2)	Member States shall implement a common mechanism for the authentication of relying parties	De lidstaten voeren een gemeenschappelijk mechanisme in voor de authenticatie van vertrouwende partijen
Art. 6c (2)	Compliance with the requirements set out in paragraphs 3, 4 and 5 of Article 6a related to the personal data processing operations carried out by the issuer of the European Digital Identity Wallets shall be certified pursuant to Regulation (EU) 2016/679.	Naleving van de vereisten uiteengezet in de leden 3, 4 en 5 van Artikel6a met betrekking tot de verwerkingen van persoonsgegevens door de uitgevende instelling van de Europese digitale identiteitsportemonnees worden gecertificeerd volgens Verordening (EU) 2016/679.
Art. 6c (3)	The conformity of European Digital Identity Wallets with the requirements laid down in article 6a paragraphs 3, 4 and 5 shall be certified by accredited public or private bodies designated by Member States.	De conformiteit van European Digital Identity Wallets met de vereisten als bedoeld in Artikel6a lid 3, 4 en 5 wordt gecertificeerd door geaccrediteerde door de lidstaten aangewezen openbare of particuliere instanties.
Art. 6c (5)	Member States shall communicate to the Commission the names and addresses of the public or private bodies referred to in paragraph 3. The Commission shall make that information available to Member States	De lidstaten delen de Commissie de namen en adressen mee van de in lid 3 bedoelde openbare of particuliere instanties. De Commissie stelt die informatie ter beschikking van de lidstaten.
Art. 6d (1)	Member States shall inform the Commission without undue delay of the European Digital Identity Wallets that have been issued pursuant to Article 6a and certified by the bodies referred to in Article 6c paragraph 3. They shall also inform the Commission, without undue delay where the certification is cancelled.	De lidstaten informeren de Commissie onverwijld over European Digital Identity Wallets die zijn uitgegeven op grond van Artikel6a en die zijn gecertificeerd door de in Artikel6c lid 3 bedoelde instanties. Zij stellen de Commissie onverwijld op de hoogte wanneer de certificering is geannuleerd.
Art. 7	Pursuant to Article 9(1) Member States shall notify, within 12 months after the entry into force of this Regulation at least one electronic identification scheme including at least one identification means.	Overeenkomstig Artikel9, lid 1, notificeren Lidstaten binnen twaalf maanden na de inwerkingtreding van deze verordening ten minste één systeem voor elektronische identificatie, met inbegrip van ten minste één identificatiemiddel.

Art. 10a (1)	Where European Digital Wallets issued pursuant to Article 6a and the validation mechanisms referred to in Article 6a(5) points (a), (b) and (c) are breached or partly compromised in a manner that affects their reliability or the reliability of the other European Digital Identity Wallets, the issuing Member State shall, without delay, suspend the issuance and revoke the validity of the European Digital Identity Wallet and inform the other Member States and the Commission accordingly.	Wanneer overeenkomstig Artikel6 bis uitgegeven Europese digitale portefeuilles en de in Artikel6 bis, lid 5, punten a), b) en c), bedoelde valideringsmechanismen worden geschonden of gedeeltelijk worden gecompromitteerd op een manier die hun betrouwbaarheid of de betrouwbaarheid van de andere Europese digitale identiteitsportefeuilles, schort de uitgevende lidstaat de uitgifte onverwijld op en trekt hij de geldigheid van de Europese digitale identiteitsportefeuille in, en stelt hij de andere lidstaten en de Commissie daarvan in kennis.
Art. 10a (2)	Where the breach or compromise referred to in paragraph 1 is remedied, the issuing Member State shall re-establish the issuance and the use of the European Digital Identity Wallet and inform other Member States and the Commission without undue delay.	Wanneer de in lid 1 bedoelde inbreuk of inbreuk wordt verholpen, hervat de uitvaardigende lidstaat de uitgifte en het gebruik van de Europese digitale identiteitsportefeuille en stelt hij de andere lidstaten en de Commissie daarvan onverwijld in kennis.
Art. 10a (3)	If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the Member State concerned shall withdraw the European Digital Wallet concerned and inform the other Member States and the Commission on the withdrawal accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without delay.	Indien de in lid 1 bedoelde inbreuk of compromittering niet binnen drie maanden na de opschorting of intrekking wordt verholpen, trekt de betrokken lidstaat de betrokken Europese digitale portemonnee in en stelt hij de andere lidstaten en de Commissie op de hoogte van de intrekking. Indien de ernst van de inbreuk dit rechtvaardigt, wordt de betrokken Europese digitale identiteitsportefeuille onverwijld ingetrokken.
Art. 11a (1)	When notified electronic identification means and the European Digital Identity Wallets are used for authentication, Member States shall ensure unique identification.	Wanneer aangemelde elektronische identificatiemiddelen en de Europese digitale identiteitsportefeuilles worden gebruikt voor authenticatie, zorgen de lidstaten voor unieke identificatie.
Art. 11a (2)	Member States shall, for the purposes of this Regulation, include in the minimum set of person identification data referred to in Article 12.4.(d), a unique and persistent identifier in conformity with Union law, to identify the user upon their request in those cases where identification of the user is required by law.	Voor de toepassing van deze verordening nemen de lidstaten in de in Artikel12, lid 4, onder d), bedoelde minimumreeks persoonsidentificatiegegevens een unieke en permanente identificatiecode op in overeenstemming met het Unierecht, om de gebruiker op diens verzoek in die gevallen waarin identificatie van de gebruiker wettelijk verplicht is te identificeren.

Art. 12a (1)	Conformity of notified electronic identification schemes with the requirements laid down in Article 6a, Article 8 and Article 10 may be certified by public or private bodies designated by Member States.	De overeenstemming van aangemelde elektronische-identificatiestelsels met de vereisten van Artikel6 bis, Artikel8 en Artikel10 kan worden gecertificeerd door door de lidstaten aangewezen openbare of particuliere instanties.
Art. 12a (2)	The peer-review of electronic identification schemes referred to in Article 12(6), point (c) shall not apply to electronic identification schemes or part of such schemes certified in accordance with paragraph 1. Member States may use a certificate or a Union statement of conformity issued in accordance with a relevant European cybersecurity certification scheme established pursuant to Regulation (EU) 2019/881 to demonstrate compliance of such schemes with the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes.	De collegiale toetsing van elektronische-identificatieschema's als bedoeld in Artikel12, lid 6, onder c), is niet van toepassing op elektronische-identificatieschema's of delen van dergelijke schema's die zijn gecertificeerd overeenkomstig lid 1. De lidstaten mogen een certificaat of een verklaring van de Unie gebruiken conformiteitsverklaring afgegeven in overeenstemming met een relevante Europese cyberbeveiligings certificeringsregeling die is vastgesteld overeenkomstig Verordening (EU) 2019/881 om aan te tonen dat dergelijke regelingen voldoen aan de vereisten van Artikel8, lid 2, met betrekking tot de betrouwbaarheidsniveaus van regelingen voor elektronische identificatie.
Art. 12a (3)	Member States shall notify to the Commission with the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.	De lidstaten stellen de Commissie in kennis van de namen en adressen van de in lid 1 bedoelde openbare of particuliere instantie. De Commissie: die informatie beschikbaar stellen aan de lidstaten.
Art. 12b (1)	Where Member States require an electronic identification using an electronic identification means and authentication under national law or by administrative practice to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets issued in compliance with this Regulation.	Indien de lidstaten een elektronische identificatie met behulp van een elektronisch identificatiemiddel en authenticatie op grond van de nationale wetgeving of administratieve praktijk vereisen om toegang te krijgen tot een onlinedienst die wordt aangeboden door een overheidsinstantie, aanvaarden zij ook Europese digitale identiteitsportefeuilles die zijn uitgegeven in overeenstemming met deze verordening.

Art. 12c (1)	Where electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access an online service provided by a public sector body in a Member State, the electronic identification means, issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that online service […]	Wanneer elektronische identificatie met behulp van een elektronisch identificatiemiddel en authenticatie krachtens de nationale wetgeving of administratieve praktijk vereist is om toegang te krijgen tot een onlinedienst die wordt aangeboden door een overheidsinstantie in een lidstaat, wordt het elektronische identificatiemiddel dat in een andere lidstaat is uitgegeven, erkend in de eerste lidstaat met het oog op grensoverschrijdende authenticatie voor die onlinedienst […]
Art. 45a (3)	A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.	Een gekwalificeerd elektronisch attestering van attributen dat in een lidstaat is afgegeven, wordt erkend als een gekwalificeerd elektronisch attestering van attributen in een andere lidstaat.
Art. 45d (1)	Member States shall ensure that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the attribute directly against the relevant authentic source at national level or via designated intermediaries recognised at national level in accordance with national or Union law.	De lidstaten zorgen ervoor dat, ten minste voor de in bijlage VI vermelde attributen, overal waar deze attributen berusten op authentieke bronnen in de publieke sector, maatregelen worden genomen om gekwalificeerde aanbieders van elektronische attesteringen van attributen in staat te stellen om op verzoek van de gebruiker, de authenticiteit van het attribuut rechtstreeks tegen de relevante authentieke bron op nationaal niveau of via aangewezen tussenpersonen die op nationaal niveau worden erkend in overeenstemming met het nationale recht of het Unierecht.

Annex VI	Further to Article 45d, Member States shall ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with national or Union law and in cases where these attributes rely on authentic sources within the public sector: 1. Address; 2. Age; 3. Gender; 4. Civil status; 5. Family composition; 6. Nationality; 7. Educational qualifications, titles and licenses; 8. Professional qualifications, titles and licenses; 9. Public permits and licenses; 10. Financial and company data.	Aanvullend op Artikel45d zorgen lidstaten ervoor dat maatregelen worden genomen om gekwalificeerde aanbieders van elektronische attesteringen van attributen in staat te stellen op verzoek van de gebruiker langs elektronische weg de authenticiteit van de volgende attributen te verifiëren aan de hand van de relevante authentieke bron op nationaal niveau of via aangewezen tussenpersonen die op nationaal niveau worden erkend, in overeenstemming met het nationale of het Unierecht en in gevallen waarin deze attributen berusten op authentieke bronnen in de publieke sector: 1. Adres; 2. Leeftijd; 3. Geslacht; 4. Burgerlijke staat; 5. Gezinssamenstelling; 6. Nationaliteit; 7. Onderwijskwalificaties, titels en licenties; 8. Beroepskwalificaties, titels en licenties; 9. Openbare vergunningen en licenties; 10. Financiële en bedrijfsgegevens.
Art. 48a (1)	Member States shall ensure the collection of statistics in relation to the functioning of the European Digital Identity Wallets and the qualified trust services.	De lidstaten zorgen voor de verzameling van statistieken met betrekking tot de werking van de Europese digitale identiteitsportefeuilles en de gekwalificeerde vertrouwensdiensten.
Art. 48a (4)	By March each year, Member States shall submit to the Commission a report on the statistics collected […]	Elk jaar dienen de lidstaten uiterlijk in maart bij de Commissie een verslag in over de verzamelde statistieken […]

Bijlage 3 – Begrippenlijst

In onderstaande tabel worden de belangrijkste gehanteerde begrippen toegelicht.

Attestatie	Het verstrekken van een attestering.
Attestering	Een getuigschrift, een verklaring die dient om iets te bewijzen of te staven. Bijvoorbeeld een schriftelijke verklaring van een dokter dat iemand gezond is, of juist dat hij een aandoening of ziekte heeft, om bepaalde faciliteiten te verkrijgen.
Attribuut	Een kenmerk van de gebruiker dat in een eWallet kan zijn opgeslagen. Attributen geven kenmerken en kwaliteiten van de gebruiker weer, onafhankelijk van de context, en zijn onvoldoende specifiek om de gebruiker direct te identificeren. Bijvoorbeeld 'Ik ben ouder dan 18 jaar', 'Ik ben een man', 'Ik woon in Amsterdam', ' Ik heb een Nederlands rijbewijs'.
Blockchain	Een decentraal digitaal grootboek voor het vastleggen van transacties. Gebruikers kunnen vertrouwen op de gegevens die door anderen zijn vastgelegd. Blockchains gebruiken meestal gedistribueerde databases waarbij verschillende knooppunten een consensusprotocol gebruiken om de volgorde van cryptografisch ondertekende transacties te bevestigen. Het in volgorde koppelen van de digitaal ondertekende transacties maakt de vastlegging ervan in de blockchain onveranderlijk.
Certificaat	Een certificaat wordt uitgereikt voor het voltooien van een opleiding. Het toont aan dat een opleiding is gevolgd, het is geen diploma.
Credential	Een bewijs van bekwaamheid, ervaring, rechten of machtiging van een persoon. Bijvoorbeeld een diploma of een deelcertificaat, of een opname in een beroepsregister. Een credential wordt toegekend na een examen op gevorderd niveau dat is ontwikkeld en gevalideerd volgens strikte protocollen en dat wordt afgenomen door een geauthoriseerde partij.
Customer Identity and Access Management (CIAM)	Een verzameling tools, processen en beleidsregels om de authenticatie, authorisatie, rollen en privileges van klanten te beheren, binnen een organisatie of over organisatiegrenzen heen.
Decentralized Identifier (DID)	Een wereldwijd unieke persistente identifier waarvoor geen gecentraliseerde registratieautoriteit is vereist en die vaak cryptografisch wordt gegenereerd en/of geregistreerd.
Gekwalificeerde elektronische attestering van attributen	Een elektronisch getuigschrift van een kenmerk van iemand. Zie ook Gekwalificeerde vertrouwensdienst, Attestering en Attribuut.

Gekwalificeerde en niet-gekwalificeerde certificaten	Een (gekwalificeerd) elektronisch getuigschrift van een kenmerk van iemand. Zie ook Gekwalificeerde vertrouwensdienst en Certificaat.
Gekwalificeerde vertrouwensdienst	De EIDAS verordening maakt onderscheid tussen het verlenen van niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten. De functie van de dienst is steeds dezelfde. Het verschil is dat aan het verlenen van gekwalificeerde vertrouwensdiensten en de verleners daarvan specifieke eisen worden gesteld en het toezicht daarop specifieker en verdergaand is geregeld.
Identity and Access Management (IAM)	Een verzameling tools, processen en beleidsregels om de authenticatie, authorisatie, rollen en privileges van medewerkers te beheren, veelal binnen een organisatie.
Lifelong Learning	Het gedurende het hele leven blijven verwerven van kennis en vaardigheden, op vrijwillige basis en vanuit eigen motivatie. Een onderdeel kan zijn dat professionals tijdelijk terugkeren naar instituten waar zij eerder als student waren ingeschreven.
Personal Data Management (PDM)	Een concept om eigen (persoons)gegevens te beheren en gericht te delen, waarbij de gebruiker alle gegevens zelf beheert en gegevens alleen onder expliciete controle van de gebruiker worden gedeeld.
Privacy Enhancing Technology (PET)	Een verzameling informatie- en communicatietechnologieën die de bescherming van de persoonlijke levenssfeer van individuen binnen een informatiesysteem versterken door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens of door het bieden van middelen en maatregelen tot het vergroten van de controle van de betrokkene over zijn of haar persoonsgegevens. (Bron: TNO.)
Qualified Electronic Attestations of Attributes Provider (QEAAP)	Een gekwalificeerde verlener van elektronische attesteringen van attributen. Zie Gekwalificeerde vertrouwensdienst.
Qualified Trust Service Provider (QTSP)	Zie Gekwalificeerde vertrouwensdienst.
Self-Sovereign Identity (SSI)	Een concept voor de uitwisseling van gegevens over individuen, organisaties of objecten waarbij deze gegevens zijn voorzien van bewijzen van herkomst, integriteit en dergelijke. Kenmerkend is dat de uitwisseling van deze gegevens verloopt onder expliciete controle van de betrokkene en dat de partijen die de gegevens uitgeven niet kunnen weten welke gegevens aan welke ontvangers worden verstrekt. SSI is een vorm van Personal Data Management.
Trust Service Provider (TSP)	Zie Vertrouwensdienst.
Vertrouwensdienst	Een elektronische dienst voor het aanmaken, verifiëren en valideren van o.a. elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, en elektronische attestering van attributen en certificaten die betrekking hebben op deze diensten.

Bijlage 4 – Literatuurlijst

Deze bijlage geeft een overzicht van de geraadpleegde bronnen.

- eIDAS ontwerpverordening, zie https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&from=EN
- ARF nonpaper version 20210930
- Digital finance strategy EU Commission, zie https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52020DC0591&from=EN
- Veilig inloggen met DigiD op eNIK, zie https://www.digitaleoverheid.nl/nieuws/veilig-inloggen-op-digi-d-met-enik
- BRP-koppelpunt (BRPk), zie https://www.rvig.nl/digitale-identiteit/brpk
- Kamerstukken II, 2020-2021, 22 112, nr. 3161 (Fiche: Verordening raamwerk Europese Digitale Identiteit)
- Kamerstukken II, 2020-2021, 26 643, nr. 750 (Voortgangsrapportage Domein Toegang)
- Kamerstukken II, 2020-2021, 26 643, nr. 743 (Visiebrief Digitale Identiteit).
- Bootstrapping identity wallet authentication with national eIDs, Agency for Digitisation, Denmark
- Start architectuur Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten, april 2017, zie https://www.noraonline.nl/images/noraonline/b/b2/Startarchitectuur_NL_implementatie_eIDAS_met_eTD_1_2_%28002%29.pdf
- Idensys pilot, 2018, zie https://www.digitaleoverheid.nl/nieuws/pilot-met-idensys-stopt-per-31-december-2018
- Polymorfe pseudonimisering BSN, zie https://www.logius.nl/diensten/bsnk-pp/bsnk-pp-hoe-werkt-het
- SAML, zie http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
- Pas toe of leg uit lijst van het Forum Standaardisatie, zie https://www.forumstandaardisatie.nl/open-standaarden/verplicht
- OpenID Connect, zie https://openid.net/connect
- FIDO, zie https://fidoalliance.org/fido2
- iDIN Ondertekenen, zie https://www.idin.nl/bedrijven/idin-ondertekenen
- PDM Landschap 2020: Regie op gegevens in Nederland, zie https://www.rijksoverheid.nl/documenten/rapporten/2021/01/11/pdm-landschap-2020-regie-op-gegevens-in-nederland#:~:text=Onderzoek%20naar%20de%20mogelijkheden%20die,PDM%20staat%20voor%20persoonlijk%20datamanagement
- IRMA app, zie https://irma.app/ en https://privacybydesign.foundation/uitgifte-brp
- IRMA ondertekenen, zie https://privacybydesign.foundation/demo/ondertekenen
- Datakeeper wallet, zie https://datakeeper.nl
- Ockto, zie https://www.ockto.nl
- Schluss, zie https://www.schluss.org
- Announcing the Android Ready SE Alliance, March 25, 2021, zie https://security.googleblog.com/2021/03/announcing-android-ready-se-alliance.html
- Announcing Azure AD Verifiable Credentials, zie https://customers.microsoft.com/en-us/story/1351115614634143059-flanders-government-of-belgium-government-azure-active-directory
- Dashboard eIDAS, Logius, editie december 2021.
- Wet digitale overheid, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid
- Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), zie https://zoek.officielebekendmakingen.nl/kst-34972-20.html
- Digital identity – leveraging the SSI concept to build trust', ENISA, November 2021, Final Draft
- Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations', W3C Proposed Recommendation, 3 August 2021, zie https://www.w3.org/TR/did-core
- W3C Verifiable Credentials, zie https://www.w3.org/TR/vc-data-model
- Forum Standaardisatie lijsten van standaarden, zie https://www.forumstandaardisatie.nl/open-standaarden
- ISO/IEC 18013-5:2021 mobile driving license (mDL) application, zie https://www.nen.nl/nen-iso-iec-18013-5-2021-en-288068
- SDG, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/europa/single-digitale-gateway/#:~:text=De%20Single%20Digital%20Gateway%20(SDG,portaal%20(gateway)%20Your%20Europe%20.&text=Eind%202023%20is%20het%20voor,te%20regelen%20met%20Europese%20overheden
- Eindrapport Nederlandse Self-Sovereign Identity Ecosysteem (SSI), https://www.rijksoverheid.nl/documenten/rapporten/2021/10/01/eindrapport-nederlandse-self-sovereign-identity-ecosysteem-ssi
- Gartner, Hype Cycle for Digital Government Technology, 2021.
- Alcoholwet, zie https://www.rijksoverheid.nl/onderwerpen/alcohol/alcohol-wetgeving en https://wetten.overheid.nl/BWBR0002458/2021-07-01 voor de wet zelf.

- Onderzoek “Inventarisatie van leeftijdsverificatiesystemen voor het aankopen van alcohol”, 2021, zie https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2021/07/20/inventarisatie-van-leeftijdsverificatiesystemen/inventarisatie-van-leeftijdsverificatiesystemen.pdf
- Start architectuur Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten, april 2017, zie https://www.noraonline.nl/images/noraonline/b/b2/Startarchitectuur_NL_implementatie_eIDAS_met_eTD_1_2_%28002%29.pdf