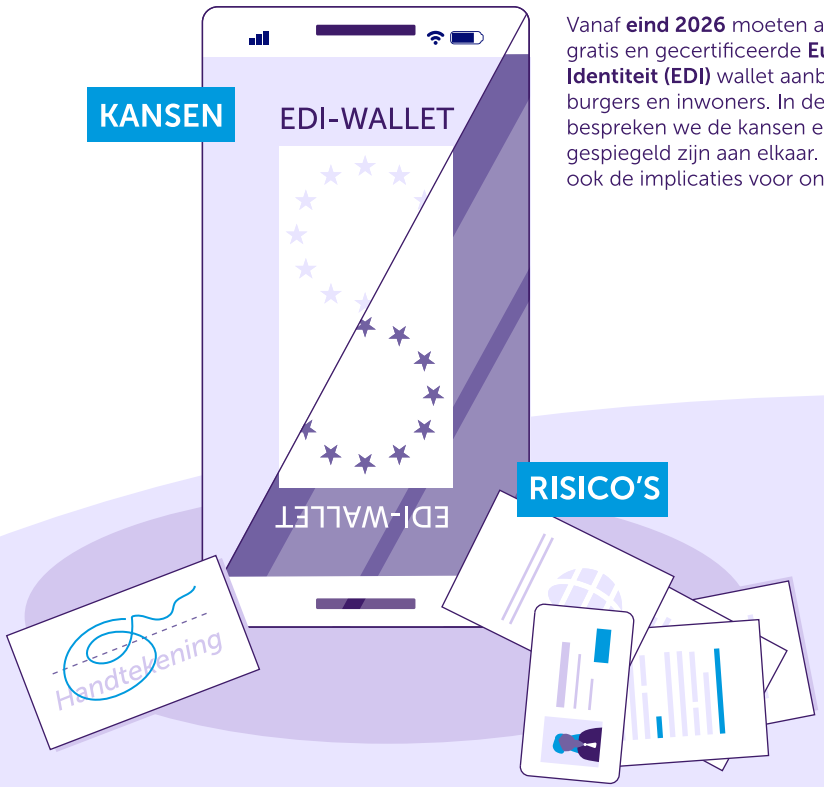
TOEZICHT RAPPORT

Europese Digitale Identiteit: de komst van de EDI-wallet

In het kort Financiële dienstverlening digitaliseert op een hoog tempo. Eind 2026 dienen alle EU-lidstaten haar burgers te voorzien van een digitale identiteit en bijbehorende wallet volgens de eIDAS2.0 regelgeving. Deze Europese digitale Identiteitswallet kan gebruikt worden als online identificatiemiddel, voor informatie-uitwisseling en het digitaal ondertekenen van documenten. Vanzelfsprekend biedt een digitale identiteit kansen en risico's voor burgers en bedrijven. In de voorbereiding op de komst van de identiteitswallet en bijbehorende vertrouwensdiensten (eIDAS2.0) geeft dit rapport inzicht in deze ontwikkeling en mogelijke impact op de financiële sector.



Vanaf **eind 2026** moeten alle EU-lidstaten een gratis en gecertificeerde **Europese Digitale Identiteit (EDI)** wallet aanbieden aan hun burgers en inwoners. In deze verkenning bespreken we de kansen en risico's, die veelal gespiegeld zijn aan elkaar. We onderzoeken ook de implicaties voor ons toezicht.

MAART 2025

AFM

TOEZICHT RAPPORT

Inhoudsopgave

1. Europese digitale identiteit vanaf 2026 – samenvatting 3

2. Inleiding en leeswijzer 5

3. Het regelgevend kader eIDAS 2.0 en de komst van de EDI-wallet 7

3.1 Europese verordening voor een Digitale Identiteit (eIDAS) 7

3.2 eIDAS 2.0 7

3.3 EDI referentie architectuur 8

4. De EDI-wallet en haar functies 9

5. Ontwikkeling use-cases – large scale pilots 11

6. Impact van EDI-Wallet 12

6.1 Impact op (financiële) dienstverlening 12

6.2 Impact op toezicht 13

7. Annex I - Het EDI-wallet eco-systeem 15

7.1 Wallet-provider 16

7.2 User - PID (Personal Identification Data) 17

7.3 Attribute-provider 17

7.4 Relying party 18

7.5 Validity information 19

7.6 De betrouwbaarheid van een wallet 19

AFM

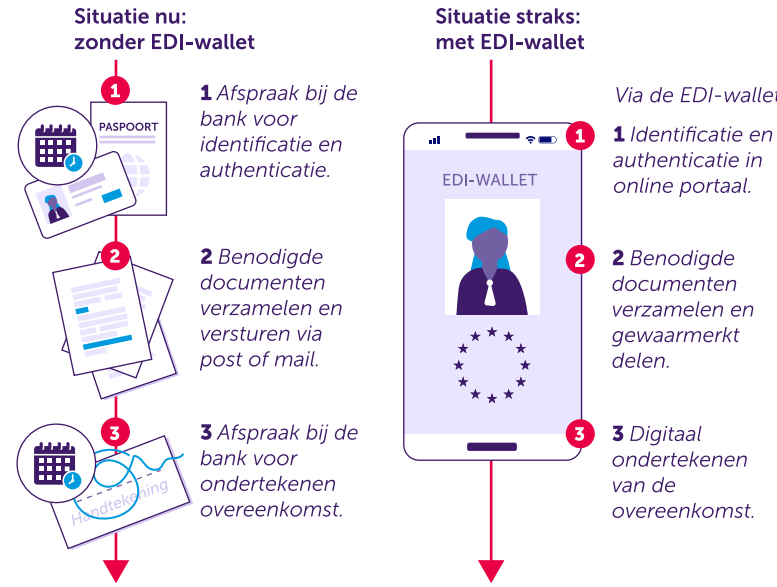
1. Europese digitale identiteit vanaf 2026 – samenvatting

Vanaf eind 2026 moeten alle EU-lidstaten een gratis en gecertificeerde Europese Digitale Identiteit (EDI) wallet aanbieden aan hun burgers en inwoners. Deze wallet bevat de digitale identiteit die nodig is om je online te identificeren voor zowel publieke als private diensten binnen de EU. Deze digitale identiteit is beschikbaar via een wallet-app op je mobiele telefoon en is ook in de fysieke wereld gelijkwaardig aan een identiteitsbewijs. Bovendien moet de gebruiker via de wallet (persoons) gegevens kunnen opvragen en delen met verschillende partijen. Tot slot zal de wallet de mogelijkheid bieden om documenten te voorzien van een elektronische handtekening.

We verwachten dat de EDI-wallet een grote impact kan hebben op het afnemen van financiële diensten en producten. We laten dit zien aan de hand van een illustratie van het klantproces voor het aanvragen van een lening bij een bank.

Figuur 1 bevat een weergave van een traditioneel klantproces, dus zonder EDI-wallet, waarbij de consument een fysieke afspraak maakt op een bankkantoor voor de identificatie en authenticatie met een geldig identiteitsbewijs (stap 1). Na onboarding dient de klant zelf de benodigde documenten te verzamelen en te versturen via post of e-mail (stap 2). Tot slot maakt de consument nogmaals een fysieke afspraak om de overeenkomst te ondertekenen (stap 3).

Figuur 1 laat ook zien dat het gebruik van de EDI-wallet het mogelijk maakt om identificatie en authenticatie als klant via een online portaal uit te voeren. Vervolgens biedt de wallet ook de mogelijkheid om bij publieke of private diensten (bv. mijnoverheid.nl) de benodigde (persoons)gegevens te verzamelen (stap 1). Daarnaast kunnen gebruikers de opgevraagde gegevens volledig digitaal selecteren en delen via de wallet. De EDI-wallet maakt het zo mogelijk om gewaarmerkte brongegevens te delen met dienstverleners (stap 2). Uiteindelijk kan de gebruiker met de EDI-wallet ook de resulterende overeenkomst digitaal ondertekenen met een elektronische handtekening (stap 3).



Figuur 1: Voorbeeld aanvraag voor een banklening

De komst van de EDI-wallet heeft impact op belangrijke thema's voor het toezicht van de AFM. Daarom staan we in deze verkenning stil bij de kansen en risico's van de komst van de EDI-wallet:

- **Digitalisering:** de EDI-wallet maakt het mogelijk om financiële dienstverlening verder te digitaliseren met een hoog betrouwbaarheidsniveau. Voorbeelden hiervan zijn het onboarden van klanten en het aanleveren van de benodigde klantgegevens voor het afnemen van een dienst. Het delen van gewaarmerkte brongegevens kan bovendien leiden tot de verdere digitalisering van de dossiervorming voor het vervullen van de poortwachtersrol. De wallet biedt daarnaast gemak voor consumenten door financiële gegevens op één plek te verzamelen. Dit biedt consumenten meer inzicht in hun financiële situatie en verlaagt mogelijk de kans op overkreditering. Ondanks dat de wallet kan leiden tot efficiëntere digitale processen, kan dit ook leiden tot een vorm van gedwongen gebruik voor financiële diensten. Daarnaast kunnen consumenten het gebruik

van de wallet als complex ervaren. Bovendien maakt de wallet consumenten potentieel kwetsbaar voor nieuwe vormen van identiteitsfraude en misbruik.

- **Embedded finance:** de EDI-wallet maakt het makkelijker voor de houder om gegevens te delen met verschillende partijen. Ook stimuleert dit innovatie door de integratie van (financiële) diensten. Daarbij vermindert de EDI-wallet een aantal (fysieke) drempels om financiële producten af te nemen en maakt digitale dienstverlening daarmee zo veel mogelijk frictieloos. Dit verhoogt echter het risico op onveilig gedrag, indien gebruikers onvoldoende stilstaan bij de lange-termijn consequenties van het afsluiten van financiële diensten. Met de integratie van gegevens en diensten op de wallet neemt ook het risico toe dat dienstverleners mogelijk aanvullende persoonsgegevens opvragen om inzicht te krijgen in het (historische) gedrag van hun klanten.
- **Internationalisering:** de EDI-wallet is in principe binnen de gehele EU te gebruiken en beslecht daarmee barrières voor grensoverstijgende financiële dienstverlening. Door het gebruik van gewaarmerkte gegevens kan de EDI-wallet leiden tot betere klantbestanden voor fraudetoezicht of wwft-toezicht. De wallet kan daarnaast drempelverlagend werken voor het afnemen van buitenlandse financiële producten waar vanuit Nederland mogelijk minder goed toezicht op is.

2. Inleiding en leeswijzer

De digitalisering van de financiële sector en het aanbieden van producten en diensten via online platformen zetten in gestaag tempo door. Tot op heden is vaak het onboarding proces voor nieuwe klanten achtergebleven, namelijk het online identificeren en authentiseren van een potentiële klant. Deze stap wordt vaak nog uitgevoerd op basis van het delen van een (kopie) identiteitsbewijs of via een afgeleide identiteitsverificatie, zoals 1 cent overmaken op een bankrekening. Ook bestaan er online identificatieprocessen die gebruik maken van video-identificatie. Hiervoor dienen gebruikers een foto te maken van hun identiteitsbewijs en hun gezicht te scannen met een selfie-video. Vervolgens worden de gezichtskenmerken (geautomatiseerd) gecontroleerd met de kenmerken van de foto op het identiteitsbewijs.

Om deze digitale identificatieprocessen te verbeteren heeft de Europese Unie na een evaluatie van de huidige eIDAS verordening (Electronic Identities And Trust Services waar o.a. inlogmiddel DigiD uit voort is gekomen) deze regelgeving vernieuwd. Onderdeel hiervan is het initiatief voor het ontwikkelen van een 'European Digital Identity Wallet' (EDI-wallet).

De Europese Commissie definieert de 'European Digital Identity Wallet' als volgt in de verordening:
'een product en dienst dat de houder in staat stelt om identiteitsgegevens, inloggegevens en attributen op te slaan die zijn gekoppeld aan haar/zijn identiteit. Een houder kan deze op verzoek aan vertrouwende partijen verstrekken en gebruiken voor identificatie, authenticatie en autorisatie in online en offline situaties. Tevens is het mogelijk om gekwalificeerde elektronische handtekeningen te zetten'

Kort gezegd is de EDI-wallet dus een mobiele app waarin de gebruiker digitale persoonsgegevens en overige digitale bewijzen over zichzelf kan opslaan om op een later moment te gebruiken.

Het fenomeen van een digitale wallet is niet nieuw. We kennen dit fenomeen via crypto- of payment-wallets ,zoals Google Pay of Apple Pay. Ook zijn er al verschillende digitale ID-wallets op de markt om (persoons)gegevens te verzamelen en te delen, zoals o.a. Ockto, Datakeeper, Digidentity en Yivi. Deze ID-wallets van derde aanbieders, vaak ook datadeler-apps genoemd, worden steeds belangrijker voor het digitaal delen van gegevens met bijvoorbeeld een overheidsorganisatie of een hypotheekaanbieder. Deze wallets hebben niet de status van identiteitsbewijs en zijn vaak alleen "lokaal" bruikbaar, dus alleen in een specifiek land of bij een specifieke organisatie. Hierbij valt op te merken dat de Autoriteit Persoonsgegevens (AP) zich onlangs kritisch heeft uitgesproken over deze datadeler-apps van derde aanbieders. Ze uiten zorgen over de gevolgen van het gebruik van deze apps voor de bescherming van persoonsgegevens van de burgers die deze apps gebruiken. In dit rapport gaan we verder niet in op deze datadeler-apps.

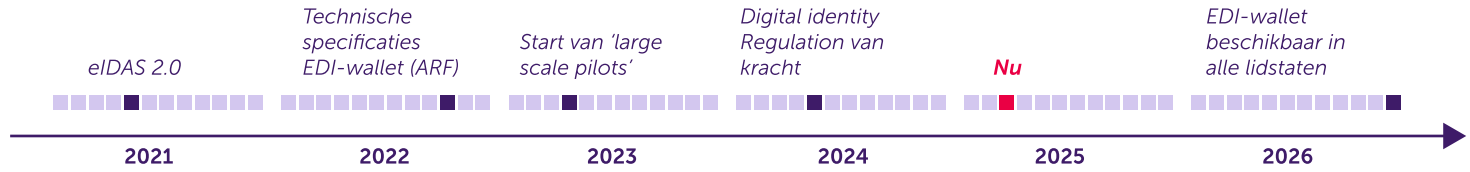
Vanaf eind 2026 moeten alle EU-lidstaten een kosteloos en gecertificeerde Europese Digitale Identiteit (EDI) wallet aanbieden aan hun burgers en inwoners. Deze wallet is meer dan enkel een identificatiemiddel en vormt de basis voor een elektronische wallet waarmee de gebruiker:

- Geverifieerde persoonsgegevens kan verzamelen en delen;
- Attestaties van persoonskenmerken kan afgeven zonder de achterliggende (persoons)gegevens te delen;
- Elektronische handtekeningen kan zetten, waarmee gebruikers in potentie ook transacties kunnen autoriseren.

Deze functionaliteiten worden op dit moment uitgewerkt en getest in reeds lopende 'Large Scale Pilots'.

Deze verkenning richt zich op de ontwikkelingen rondom de EDI-wallet en de impact op het toezicht op de financiële dienstverlening. De EDI-wallet staat namelijk hoog op de agenda van de Europese Commissie (EC) en de ontwikkeling is daarmee in een stroomversnelling gekomen. Recentelijk is er ook een uitgebreide website gelanceerd door de EC om de EDI-wallet verder te promoten.

Op 21 mei 2021 is de conceptversie van de Verordening Europese e-ID gepubliceerd als aanpassing van het bestaande eIDAS (Electronic Identities And Trust Services) regime. Hieronder is de huidige tijdslijn weergegeven voor de EDI-wallet met belangrijkste mijlpalen:



Figuur 2: Tijdslijn EDI-wallet

De Digital Identity regulation is een amendement op eIDAS en sinds 20 mei 2024 van kracht. Hierin staat dat EU-lidstaten minimaal één EDI-wallet moeten certificeren en kosteloos beschikbaar moeten stellen aan hun burgers vanaf eind 2026. De gebruiker kan dus mogelijk verschillende wallets kiezen mits deze voldoen aan het eIDAS architectuurvereisten en deze gecertificeerd zijn door de *national compentent authority*, zoals hoogstwaarschijnlijk de Rijksinspectie Digitale Infrastructuur (RDI) in Nederland.

De potentiële impact van de EDI-wallet op de financiële sector is groot en kan digitale dienstverlening een enorme impuls geven. De wallet beoogt namelijk een hoog betrouwbaarheidsniveau te bieden voor toegang tot hun digitale dienstverlening. Daarnaast biedt het de mogelijkheid voor datadeling tussen financieel dienstverleners door de gebruiker, zoals o.a. de Europese verordening FIDA voorschrijft. Deze digitaliseringsslag brengt ook risico's met zich mee en heeft daardoor tegelijkertijd invloed op het toezicht op financiële instellingen. Deze verkenning beoogt daarom om inzicht te bieden in de functionaliteiten van de EDI-wallet, de mogelijke impact op digitale dienstverlening en de raakvlakken met het gedragstoezicht op financiële instellingen.

Als het gaat om de potentiële impact voor AFM-toezicht dan is deze verkenning bedoeld als een eerste aanzet. Bovendien beoogt eIDAS 2.0 de komst van een bedrijvenwallet en een aantal nieuwe vertrouwensdiensten. Ondanks dat deze ook impact kunnen hebben op de financiële sector, laten we deze in dit rapport buiten beschouwing.

Leeswijzer

Dit is een bondige verkenning door de AFM naar de veranderingen die een Europese ID-wallet teweeg kan brengen. Dit omvat een uiteenzetting van het regelgevend kader van de EDI-wallet (hoofdstuk 3), de functies van de wallet (hoofdstuk 4), de ontwikkeling van use-cases om functionaliteiten te testen (hoofdstuk 5) en de impact van de wallet op financiële dienstverlening en toezicht (hoofdstuk 6).

De AFM stelt digitalisering als een centraal thema in haar strategie. Vanuit dat perspectief doet de AFM regelmatig verkenningen naar de betekenis van digitalisering voor financiële instellingen en voor het AFM toezicht. Een recent voorbeeld hiervan is de verkenning naar *Kansen en risico's van digitalisering verzekeringsmarkt de komende 10 jaar*. In dat kader moet ook deze verkenning gezien worden als een eerste inventarisatie van een digitaliseringstrend die in potentie grote gevolgen heeft voor de dienstverlening van financiële instellingen en daarmee voor het toezicht van de AFM.

Deze verkenning is tot stand gekomen met behulp van gesprekken met collega-toezichthouders, overheidspartijen en commerciële organisaties.

3. Het regelgevend kader eIDAS 2.0 en de komst van de EDI-wallet

In dit hoofdstuk gaan we in op de Europese verordening die de basis legt voor de totstandkoming van de EDI-wallet. Vervolgens beschrijven we de rol van het architectuur- en referentieraamwerk van de EDI-wallet.

3.1 Europese verordening voor een Digitale Identiteit (eIDAS)

De eIDAS verordening trad in 2014 in werking en biedt een kader voor Europees gebruik van digitale identificatiemiddelen voor digitale diensten. Deze verordening biedt een basis voor betrouwbare dienstverlening door afspraken over begrippen, betrouwbaarheidsniveaus en het gebruik van onderlinge digitale infrastructuur. In Nederland zijn burgers hier vooral mee bekend via inlogmiddelen DigiD voor burgers en eHerkenning voor bedrijven.

De eIDAS 2014 verordening heeft niet gebracht wat ervan werd verwacht. De implementatie door lidstaten liet te wensen over en te weinig lidstaten lieten hun ontwikkelde elektronisch inlogmiddel aansluiten op de eIDAS-infrastructuur. Ook waren te weinig dienstverleners aangesloten op eIDAS-infrastructuur, waardoor onvoldoende private diensten aangesloten waren. Dit is geëvalueerd en in 2021 is een voorstel gedaan voor de herziening van eIDAS.

3.2 eIDAS 2.0

Na de evaluatie van eIDAS is een voorstel gedaan voor de verdere invulling van een raamwerk voor een Europese digitale identiteit. In deze eIDAS 2.0 verordening is ook de ambitie opgenomen voor het beschikbaar stellen van een bijbehorende identiteitswallet. De verordening geeft ook de mogelijkheid voor commerciële partijen om wallets te ontwikkelen op basis van de referentie architectuur.

Het doel van de Europese Commissie (EC) is dat elke lidstaat een gratis en gecertificeerde wallet beschikbaar stelt aan haar burgers en inwoners. Voorwaarde is dat deze gecertificeerde wallet voldoet aan het architectuur- en referentieraamwerk waarin technische en functionele specificaties zijn opgenomen. Daarnaast dient de wallet gecertificeerd te zijn door een nationale toezichthouder. In Nederland wordt deze certificering hoogstwaarschijnlijk door de Rijksinspectie Digitale Infrastructuur afgegeven, omdat zij reeds toezichthouder zijn op elektronische vertrouwensdiensten. Na certificering van een wallet door de toegewezen toezichthouder van een lidstaat, kunnen in de toekomst wallethouders uit andere lidstaten deze wallet ook gebruiken.

Het ministerie van Binnenlandse Zaken bouwt momenteel een referentiewallet die de NL-Wallet wordt genoemd. De broncode van de NL-Wallet is beschikbaar in hun GitHub-repository. De verwachting is dat NL-wallet de eerste gecertificeerde EDI-wallet wordt die Nederlandse burgers en inwoners kunnen gebruiken. Later komt er een stelsel van open toelating waarmee ook wallets van commerciële partijen op de markt kunnen komen indien ze gecertificeerd zijn. Uiteindelijk heeft de EC tot doelstelling dat in 2030 70% van de burgers de EDI-Wallet op dagelijkse basis gebruikt. Dit betekent dat de EDI-Wallet in de toekomst DigiD en eHerkenning overbodig kunnen maken als inlogmiddel voor publieke diensten. Dit wil niet zeggen dat DigiD en eHerkenning verdwijnen uit de markt, maar dat de rol als inlogmiddel door de EDI-wallet kan worden overgenomen.

3.3 EDI referentie architectuur

Op 3 juni 2021 heeft de Europese Commissie een aanbeveling aangenomen waarin ze de lidstaten oproept om samen een referentie architectuur te creëren voor de bouw van EDI-wallets. Het Architectuur en Referentie Framework (ARF) is een set (technische) standaarden, gemeenschappelijke richtlijnen en *best practices* voor de EDI-wallet. Het door de lidstaten ontwikkelde ARF is door de eIDAS expert group doorontwikkeld en gepresenteerd in januari 2023, de zogenaamde *European digital Identity wallet architecture and reference framework* (EU ARF). Met de acceptatie van eIDAS 2.0 is er de verplichting ontstaan voor Europese lidstaten om de ARF verder te ontwikkelen. Het ARF wordt via zogenaamde *implementing acts* opgenomen in de eIDAS verordening.

De huidige publicatie van het ARF voor de EDI-wallet is niet de uiteindelijke versie. Via een proces van Large Scale Pilots (LSPs) worden er vervolgens verbeteringen in het ARF doorgevoerd. De ervaringen met het gebruik van de EDI-wallet, die volgens het dan geldende ARF gebouwd, kunnen leiden tot verbeteringen en aanvullingen op dit ARF. Via dit proces van aanvullingen en verbeteringen komt de EU dan tot een finale versie van het ARF. Uiteindelijk dient elke lidstaat een gratis EDI-wallet ter beschikking stellen die voldoet aan dit ARF. In het proces daaropvolgend, nadat eIDAS 2.0 van kracht is, zullen er als nodig updates en nieuwe versies verschijnen. Met het opleveren van het ARF is dus er geen einde gekomen aan dit iteratieve proces.

In annex I hebben we een korte uiteenzetting toegevoegd van het beoogde ecosysteem van de EDI-wallet. Hierin besteden we meer aandacht aan de verschillende rollen en onderdelen van het EDI-stelsel. Ook geven we meer achtergrond bij de betrouwbaarheidsniveaus van een digitale identiteit. Digitale veiligheid is namelijk essentieel voor de consument en instelling om vertrouwen te krijgen en te houden in deze vorm van digitalisering. Kortom, naast de functionaliteiten van de wallet, is ook de vraag of we deze net zo goed of beter vertrouwen dan het gebruik van onze fysieke identiteitsbewijzen.

4. De EDI-wallet en haar functies

De EDI-wallet dient beschikbaar te zijn voor de burgers en inwoners in EU-lidstaten vanaf eind 2026. Hieronder onderscheiden we de verschillende functionaliteiten van de beoogde wallet:

De functies van de EDI-wallet:

Identificatie *is de identiteitsclaim van een persoon, zoals een naam.*

Authenticatie *is de verificatie van de identiteitsclaim: hoort de deze naam bij deze persoon?*

Autorisatie *wordt verleend op basis van identiteit en toegekend toegangsniveau: heeft deze persoon toegang?*

Een **digitale handtekening** *zet de gebruiker met behulp van crypto-grafische sleutels. Deze sleutels kunnen bijvoorbeeld lokaal (in de Wallet-app) worden opgeslagen.*

Attestatie *is de bevestiging van een persoonskenmerk, ook wel attribuut of credential genoemd. Voorbeeld: de bevestiging dat een diploma behaald is.*

Deze functies worden momenteel uitgewerkt en getest in de reeds lopende **'large scale pilots'**.

Figuur 3: De functie van de EDI-wallet

Digitale identificatie & authenticatie

Nadat een EDI-wallet is gekoppeld aan een geverifieerde houder, dient de wallet zonder aanvullende middelen bruikbaar te zijn ter identificatie van deze houder in de online en fysieke wereld. Hiervoor is van belang dat de identificerende partij de identificatiegegevens van de wallethouder kan authentiseren.

De identificatie van de houder en het authentiseren van deze (persoons) gegevens zullen voor veel technische uitdagingen zorgen. De betrouw-bare opslag van persoonsgegevens is er één van. Op dit moment is de identificatie en authenticatie (verificatie van identiteitsclaim) van een persoon vaak enkel mogelijk met behulp van fysieke documenten als paspoort, ID-kaart of rijbewijs. Ook met het huidige inlogmiddel DigiD is identificatie met het hoogste betrouwbaarheidsniveau alleen mogelijk met een extra middel, bijvoorbeeld door het inlezen van de RFID chip in een paspoort (eNIK) via NFC.

De mogelijkheid tot digitale identificatie/authenticatie via de EDI-wallet is in het belang van de financiële sector, zoals bij het onboarden van nieuwe klanten of medewerkers. In de financiële sector is identificatie en authenticatie van personen van belang bij het verstrekken van een bankrekening, afsluiten van een verzekeringspolis of het openen van een beleggingsrekening om bijv. witwassen, fraude of terrorismefinanciering tegen te gaan. Daarnaast is identificatie/authenticatie relevant voor de interne bedrijfsvoering bij het aannemen van nieuwe medewerkers.

Ook in de fysieke wereld kan de EDI-wallet nuttig zijn voor het digi-taal opslaan van een rijbewijs of identiteitsbewijs in de wallet, zodat de houders hun fysieke documenten niet meer hoeven te dragen ter identificatie.

Digitale autorisatie

Nadat een digitale identiteit is gekoppeld aan een wallet, kunnen wallethouders vervolgens aanvullende persoonsgegevens of attributen opslaan in de EDI-wallet. Deze geverifieerde kwalificaties kunnen de houder toegang geven (autoriseren) tot bepaalde diensten.

Autoriseren betekent toegang verlenen aan een specifiek persoon, zoals toegang tot een beleggingsrekening of het doen van investeringen. Dit kan bijvoorbeeld ook fysieke toegang tot een bedrijfspand zijn. Een ander voorbeeld is het controleren van de identiteit voor het openen van een bankrekening en waar vervolgens toegang tot de bankrekening wordt afgegeven via een bankpas of een app op een mobiele telefoon.

De functie autoriseren kan de EDI-wallet ook geschikt maken voor het ontvangen en versturen van digitaal geld. De verwachtingen zijn dat in het aankomende voorstel van de Europese Commissie rondom de digitale euro, ook de EDI-wallet genoemd kan worden als mogelijk middel voor het autoriseren van betalingen.

Elektronische handtekeningen

Het zetten van een elektronische handtekening is ook een beoogde functionaliteit van de EDI-wallet. Dit kan de wallethouder gebruiken om een rechtsgeldige handtekening toe te voegen aan een digitaal document. Ook kan een wallethouder via het zetten van een elektronische handtekening bevestigen dat hij of zij degene is die bepaalde gegevens heeft gedeeld. Ook maakt deze functionaliteit het mogelijk voor een gegevensverstrekker om documenten te voorzien van een handtekening om de authenticiteit hiervan te garanderen, zoals we in de volgende paragraaf toelichten.

Delen van (persoons)gegevens

Een andere toepassing van de EDI-wallet is het selecteren en delen van geverifieerde (persoons)gegevens of attributen door de houder. Wanneer deze gegevens gewaarmerkt worden d.m.v. een elektronische handtekening, dan heet dit waarmerk de attestatie van het attribuut, ook wel 'verifiable credential' genoemd. De bijgeleverde elektronische handtekening maakt het namelijk verifieerbaar wie de gegevens heeft gedeeld. Maar ook de verstrekker van de brongegevens (bijvoorbeeld arbeidsverleden en loongegevens door UWW) kan als organisatie via een elektronische handtekening bevestigen dat ze deze de gegevens heeft verstrekt en dat deze gegevens dus authentiek zijn.

Via de wallet kan de houder kiezen welke aanvullende gegevens deze deelt met een publieke of private organisatie. De EDI-wallet maakt het dus mogelijk om bijvoorbeeld in plaats van de salarisstrook enkel te delen dat de houder meer dan het benodigde bedrag verdient voor bijvoorbeeld een hypotheek (ook bekend als *zero-knowledge proofs*). Dit gegeven zou een werkgever of UWV kunnen bevestigen en ondertekenen. Dit leidt tot een ander soort van dossiervorming van klanten met meer privacy voor de gebruiker.

De bovengenoemde functies en gebruikscenario's worden verder uitgewerkt en getest door middel van grootschalige pilots, die we verder bespreken in het volgende hoofdstuk.

5. Ontwikkeling use-cases – large scale pilots

In opdracht van de Europese Commissie worden op dit moment grootschalige pilots ('large scale pilots') uitgevoerd op basis van de initiële versie van het ARF van de EDI-wallet. Daarnaast wordt er een (Europese) open-source referentiewallet ontwikkeld die gebruikt kan worden tijdens deze pilots. Hiermee kunnen verschillende *use-cases* worden getest op functionaliteit van de EDI-wallet en daarmee iteratief worden verbeterd. Private en publieke partijen uit alle lidstaten kunnen hieraan meewerken. Zij zijn verenigd in vier consortia die zijn geselecteerd en gefinancierd door de Europese Commissie, zoals hieronder weergegeven. In mei 2024 is een tweede financieringsronde gestart.

- **Potential:** dit consortium (met coördinerende lidstaten Frankrijk en Duitsland) richt zich op use-cases rondom:
  - Toegang tot overheidsdiensten
  - Openen van bankrekening
  - Registratie van een simkaart
  - Mobiel rijbewijs
  - Elektronische handtekeningen
  - Elektronisch doktersrecept
- **EWC - EU Digital Wallet:** dit consortium (met coördinerend lidstaat Zweden) richt zich op use-cases in de context van reizen en betalingen, onder andere voor:
  - Veilig uitwisselen van passagiersgegevens
  - Online betalingen voor aanschaf van goederen en diensten in de context van het reizen
  - Digitale identiteit voor organisaties betrokken bij de customer journey.
- **NOBID:** dit consortium (met coördinerend lidstaat Noorwegen) werkt aan een use-case voor grensoverstijgende betalingen met de wallet.
- **DC4EU:** dit consortium (met coördinerend lidstaat Spanje) werkt aan het uitrollen van pilots voor diploma's, beroepskwalificaties en sociale zekerheid. Het doel hiervan is om deze attributen op de wallet te kunnen laden, dit kan in verschillende domeinen vallen:
  - Onderwijs domein: Doel is het ontwikkelen van use-cases voor het standaardiseren van onderwijs- en studiegegevens in de vorm van attributen (diploma's en deelresultaten van studies). Dit stimuleert de internationale beweging van studenten en vrije studiekeuze door Europa heen zo naadloos mogelijk te maken.
  - Sociale zekerheid domein: Doel is het mogelijk maken van de Europese data-uitwisseling m.b.t. sociale zekerheid via de EDI-wallet.

Een belangrijke eerste stap voor deze use-cases is om de juiste PID (*Personal Identification Data*, in Nederland is een subset van de BRP-gegevens) te kunnen koppelen aan de juiste wallet (apparaat) en gebruiker (houder). De PID is een set gegevens waarmee de identiteit van een natuurlijke of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld. Vervolgens zal de aanbieder van de PID (PID-provider) ook moeten kijken hoe deze PID later ingetrokken kan worden indien nodig. Het verstrekken en mogelijk intrekken van de PID is een rol van de lidstaten, net zoals dat geldt voor een identiteitsbewijs. In Nederland zal de RvIG (Rijksdienst voor Identiteitsgegevens) fungeren als PID-provider. De EDI-wallet dient dus eerst onlosmakelijk gekoppeld te zijn aan de identiteit van de houder. Een identificatienummer, zoals het burgerservicenummer (BSN) in Nederland, maakt geen deel uit van de PID. Nederland kan wel besluiten om het BSN separaat op te nemen als attribuut in aanvulling op de PID.

6. Impact van EDI-Wallet

Ter afronding van deze verkenning bespreken we de mogelijke impact van de EDI-wallet op de financiële sector en het toezicht door de AFM.

6.1 Impact op (financiële) dienstverlening

De EDI-wallet kan zowel voor consumenten als financiële dienstverleners waarde creëren door snellere, eenduidige en veiligere klantprocessen. Ook kan de wallet de toegang tot financiële diensten vergroten door barrières uit klantprocessen weg te halen en grensoverstijgende diensten aan te bieden. Dit kan financiële diensten inclusiever maken en een verlaging van de kosten opleveren. Tot slot biedt het kansen voor innovatie door diensten te integreren in de EDI-wallet en financiële gegevens makkelijker te delen.

Daar tegenover staat dat de vergaande digitalisering van dienstverlening betekent dat consumenten die nu al moeite hebben met deze ontwikkeling hierdoor verder op achterstand raken. Daarbij speelt dat de EDI-wallet klantprocessen betrouwbaarder kan maken, maar consumenten ook kwetsbaarder kan maken voor nieuwe manieren van identiteitsfraude of misbruik via de wallet. Tot slot dreigt met de integratie van gegevens en diensten op de wallet ook het risico dat dienstverleners mogelijk steeds laagdrempeliger persoonsgegevens kunnen opvragen om inzicht te krijgen in het (historische) gedrag van hun klanten.

Kortom, het gebruik van de EDI-wallet kan op verschillende manieren impact hebben op financiële dienstverlening. De geïdentificeerde kansen en uitdagingen lijken vaak gespiegeld te zijn aan elkaar, zoals in het overzicht hieronder bondig weergegeven.

Kansen	Risico's
Gemak - één plek voor het bewaren en delen van (persoons) gegevens voor financiële diensten. Dit werkt drempelverlagend voor het afnemen van financiële diensten. Ook vergroot dit het financieel inzicht van consumenten om bijvoorbeeld overkreditering te voorkomen.	**Complexiteit** – toegang via één applicatie tot verschillende diensten en gegevens kan als complex ervaren worden. Door de verlaging van drempels kunnen ook sneller overeenkomsten afgesloten worden met mogelijk onvoorziene gevolgen op lange termijn. Dit maakt wallethouders potentieel kwetsbaar.
Betrouwbaarheid - wallethouders kunnen hun gegevens en documenten delen via gecertificeerde wallets met een hoog betrouwbaarheidsniveau. Ook kunnen (bron)gegevens worden voorzien van een elektronisch waarmerk.	**Misbruik** – nieuwe mogelijkheden voor identiteitsfraude door een kwaadwillende via de EDI-wallet, o.a. misbruik via technische kwetsbaarheden of kwetsbare consumenten. De impact van ongeautoriseerde toegang tot de wallet is hoog.
Dataminimalisatie - door het gebruik van attestaties is dataminimalisatie mogelijk, doordat houders alleen de gegevens of attestaties kunnen delen die daadwerkelijk nodig zijn voor een bepaalde dienst of een product (ook bekend als zero knowledge proofs). Dit verhoogt de privacy van de gebruiker.	**Datamaximalisatie** - door de effectiviteit van wallets wordt de drempel verlaagd voor het delen en opvragen van gegevens. Consumenten zullen niet altijd kunnen beoordelen of zo'n gegevensverzoek legitiem en wenselijk is. Daarbij kunnen ze over de streep getrokken worden door kortingen aan te bieden, zonder oog te hebben voor mogelijke consequenties van de datadeling.
Individuele controle – de wallet geeft houders de mogelijkheid om meer regie op eigen gegevens te voeren. Ook kan de Wallet consumenten helpen meer inzicht te krijgen in hun financiële situatie.	**Gedwongen gebruik** - hoe makkelijker het is om je online te identificeren, hoe vaker dit ook gevraagd zal worden. Het niet delen van gegevens (via de EDI-wallet) kan vervolgens leiden tot dreiging van uitsluiting van een dienst of product.
Inclusie – een digitale identiteit haalt barrières weg uit (digitale) klantprocessen en maakt grensoverstijgende diensten eenvoudiger beschikbaar voor consumenten.	**Exclusie** – niet-digitaalvaardige burgers komen steeds verder op afstand en kunnen deel van de markt niet bereiken. Ook zal de EDI-wallet eisen stellen aan de veiligheid van een apparaat en dit sluit mogelijk een deel van de consumenten uit.

6.2 Impact op toezicht

De adaptatie van de EDI-wallet binnen de financiële dienstverlening betekent ook een verandering van het toezicht van de AFM op de financiële sector. De komst van de EDI-wallet heeft impact op belangrijke thema's voor het gedragstoezicht door de AFM:

Digitalisering

- Digitale dienstverlening
  - Digitalisering klantcontact: de EDI-wallet kan een grote invloed hebben op de start van de procesketen voor financiële diensten, zoals het online onboarden van een klant. De wallet neemt hierdoor drempels weg en het mogelijk maken om het klantcontact volledig te digitaliseren. Hierdoor kan het aantal *all digital* ondernemingen groeien waarop AFM toezicht moet houden.
  - Attributen delen: de huidige beschikbare ID-wallets automatiseren de gegevensuitwisseling tussen klant en insteling. De EDI-wallet digitaliseert deze stap verder. Het maakt namelijk het delen van gewaarmerkte brongegevens mogelijk en realiseert hier de infrastructuur voor. Dit leidt tot een ander soort van dossiervorming, mogelijk met meer privacy voor de gebruiker. Een andere manier van dossiervorming heeft ook impact op het uitvoeren van de poortwachtersrol. Bijkomend zou het toezicht hierop ook verder gedigitaliseerd kunnen worden.
  - Betrouwbaarheid van wallet: Op dit moment zijn er allerlei ID-wallets of datadeler-apps van de derde partijen op de markt die dienstverleners al inzetten voor hun klantprocessen. Een gecertificeerde EDI-wallet die voldoet aan de gestelde eisen kan zorgen voor hogere betrouwbaarheidsniveaus voor digitale identificatie en autorisatie. De EC heeft de European Union Agency for Cybersecurity (ENISA) gevraagd om geharmoniseerd certificeringschema op te stellen waarin ook cybersecurity eisen worden opgenomen. We verwachten daarin aandacht voor oplossingen voor de veilige opslag en uitwisseling van gegevens. Daarnaast dient in het ontwerp van de wallet verder uitgewerkt te zijn hoe (doorlopend) controle plaatsvindt, zodat alleen de geautoriseerde persoon deze wallet gebruikt ter voorkoming van identiteitsfraude.
- Bescherming consument
  - Identiteitsfraude & -diefstal: Ondanks dat een gecertificeerde EDI-wallet een hoog betrouwbaarheidsniveau kan garanderen, dienen consumenten ook voorbereid te zijn op het juiste gebruik van de EDI-wallet om nieuwe vormen van identiteitsfraude of -diefstal te signaleren en te voorkomen.
  - Inzicht en inclusie: De wallet biedt gemak voor consumenten door financiële relevante gegevens op één locatie te verzamelen. Dit biedt consumenten meer inzicht in hun financiële situatie en verlaagt mogelijk de kans op overkreditering. Daarnaast verhoogt de wallet de regie op persoonsgegevens voor de houder en maakt dataminimalisatie mogelijk door het afgeven van attestaties. Bovendien kan de EDI-wallet een deel van de markt toegankelijker maken, maar er dient ook oog te zijn voor kwetsbare consumenten die niet digitaalvaardig zijn of geen toegang hebben tot een mobiele telefoon met de juiste vereisten. De wallet kan dus leiden tot een toename van complexiteit en zo ook ervaren worden door consumenten. Daarbij dient ook oog te zijn voor het voldoen aan de toegankelijkheidsrichtlijnen.
  - Wwft: Het digitaal delen van gewaarmerkte brongegevens kan ook leiden tot de verdere digitalisering van de dossiervorming voor het vervullen van de poortwachtersrol. Na toestemming van de wallethouder hebben financiële dienstverleners toegang tot (een subset van de) BRP-gegevens van klanten, waardoor klantbestanden opgeschoond kunnen worden. Daarnaast kunnen wallethouders via de EDI-wallet brongegevens opvragen die gewaarmerkt zijn door de organisatie die de gegevens heeft verleend. Dit maakt de mogelijkheden voor fraude lastiger en het voldoen aan de Wwft vereisten eenvoudiger voor financiële dienstverleners.

- Financiële keten
  - Wallet-providers: door de komst van de EDI-wallet krijgen wallet-providers een belangrijke positie in de keten van financiële dienstverlening. Dit zijn nieuwe partijen waarop verkend dient te worden of deze activiteiten verrichten die mogelijk vergunningplichtig zijn. Wallet-providers kunnen potentieel op langere termijn zelf ook (financiële) diensten gaan aanbieden via de wallet.
  - Attribute-providers: vooraf aan het afnemen van een financiële

dienst kunnen dienstverleners verschillende (bron)gegevens van de aanvrager opvragen. Om gebruik te maken van de mogelijkheid om gegevens in de EDI-wallet te verzamelen, dienen de attribute-providers deze brongegevens toegankelijk te maken via de EDI-wallet. Deze partijen krijgen daarmee dus een belangrijke rol in de financiële keten. Ook dienen dienstverleners bij het beschikbaar stellen van financiële klantgegevens rekening te houden met de aankomende Financial Data Access (FIDA) regelgeving.

Embedded finance

- Frictieloze dienstverlening
  - Drempelverlagend: doordat de online onboarding voor financiële diensten frictieloos wordt, kunnen consumenten mogelijk gedachteloos financiële overeenkomsten aangaan (polissen afsluiten, betalingen doen, etc) waarvan ze de consequenties wellicht niet kunnen overzien op de langere termijn. Dit verhoogt de kans op onveilig gedrag en schulden.
  - Integratie van diensten: door het hoge betrouwbaarheidsniveau van de EDI-wallet kan deze ook gebruikt worden voor de integratie van financiële diensten en producten. Hierdoor kan de waardeketen van financiële diensten innoveren en transformeren.
  - Impact klantrelatie: de klantrelatie kan in potentie vluchtiger worden door het gebruik van de EDI-wallet. Er zullen mogelijk minder en kortere contactmomenten zijn, omdat de EDI-wallet deze kan vervangen voor een digitale handeling via de wallet. Met de integratie van gegevens en diensten op de wallet neemt ook het risico toe dat dienstverleners mogelijk meer persoonsgegevens opvragen om inzicht te krijgen in het (historische) gedrag van hun klanten.

Internationalisering

- Grensoverstijgende dienstverlening
  - Grensoverstijgende dienstverlening kan toenemen, omdat de wallet drempelverlagend kan werken voor het afnemen van buitenlandse financiële producten waar vanuit Nederland mogelijk minder goed toezicht op is.
- Certificering van wallet in andere lidstaat
  - Certificering loopt in NL hoogstwaarschijnlijk via RDI. Het is de bedoeling dat ook derde aanbieders op termijn gecertificeerde EDI-wallets kunnen gaan aanbieden. Het staat de consument dan vrij om een in de EU gecertificeerde wallet te kiezen, een wallet gecertificeerd in een andere lidstaat die in principe aan de dezelfde (beveiligings)eisen moet voldoen anders ondermijnt dit het betrouwbaarheidsniveau van de digitale identiteit.

Mogelijke toepassingen van EDI-wallet voor AFM

De EDI-wallet kan toekomstig ook impact kan hebben op de bedrijfsvoering van de AFM.

- AFM als attribute-provider
  - Vergunningenregister: Een doelstelling is om de EDI-wallet ook geschikt te maken voor bedrijven als rechtspersoon. Dit biedt o.a. de mogelijkheid voor de AFM om het vergunningenregister te koppelen aan de EDI-wallet van de desbetreffende instelling. Recentelijk heeft de KvK bijvoorbeeld besloten hun handelsregistergegevens te ontsluiten via de IRMA-app, een initiële versie van een ID-wallet (nu Yivi genoemd).
  - Checkjeaanbieder.nl: AFM biedt een openbaar register dat een overzicht van malafide financiële dienstverleners bevat. Als een automatische controle van een financiële dienstverlener geïntegreerd kan worden in de EDI-wallet, dan kan dit een potentiële klant direct waarschuwen in de toekomst.

- Toetsing bestuurders
  - De EDI-wallet maakt het in potentie mogelijk om de toetsing van een bestuurder als attribuut te koppelen aan de persoonlijke EDI-wallet van deze bestuurder.
  - Daarnaast kunnen de documenten die worden opgevraagd voor het toetsen van bestuurders (certificaten, diploma's, etc.) toekomstig via de EDI-wallet aangeleverd worden. Dit is nu veelal een handmatig proces. Door het opvragen van (bron)gegevens via de EDI-wallet kan het proces van de AFM vereenvoudigen en verder digitaliseren.

7. Annex I - Het EDI-wallet eco-systeem

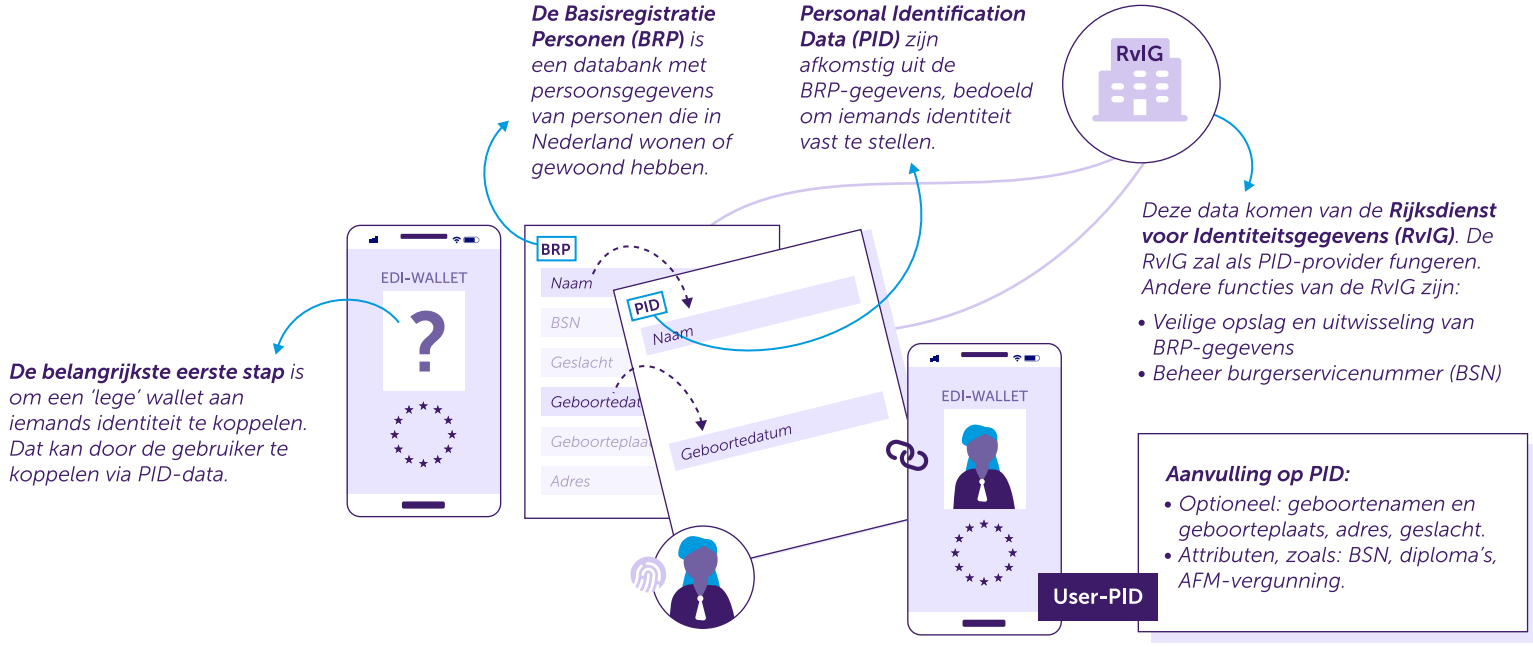
In 2021 heeft de eIDAS expert group een non-paper gepubliceerd over de *European Digital Identity Architecture and Reference Framework*. Hierin is schematisch aangegeven wat de belangrijkste rollen zijn binnen het wallet eco-systeem. Met de komst van de EDI-wallet komen er namelijk nieuwe rollen die digitale identificatie, authenticatie, autorisatie en het delen van gewaarmerkte gegevens mogelijk maken. In dit hoofdstuk gaan we in op deze rollen. Deze zijn te zien in het onderstaande figuur en vervolgens bespreken we deze relevante rollen:

Een schematische weergave van de belangrijkste rollen binnen het ecosysteem van de EDI-wallet.

Figuur 4: Schematisch overzicht van eco-systeem van EDI-wallet

7.1 Wallet-provider

Allereerst dient er een gecertificeerde wallet beschikbaar te zijn die de gebruiker op een mobiele telefoon kan installeren. Op dit moment laat de EU een referentiewallet ontwikkelen op basis van de voorgestelde ARF, zodat hiermee de verschillende pilots uitgevoerd kunnen worden. Deze referentiewallet is een Deens initiatief door Netcompany en Scytales.



Figuur 5: Benodigde data voor een EDI-wallet

De verordening geeft ook de mogelijkheid voor commerciële partijen om wallets te ontwikkelen op basis van de referentie architectuur. Na certificering van een wallet door de toegewezen toezichthouder van een lidstaat, kunnen houders uit andere lidstaten deze 'commerciële' wallet ook gebruiken in de toekomst. Er zijn op dit moment verschillende bedrijven die een wallet ontwikkelen. In opdracht van het ministerie van BZK heeft Innovalor de *Verkenning eWallets Speelveldanalyse* uitgewerkt. Uit deze speelveldanalyse blijkt dat er in Nederland al tal van oplossingen beschikbaar zijn voor het delen van persoonsgegevens middels een datadeel-app. In de Innovalor Verkenning worden er een aantal Nederlandse initiatieven besproken, namelijk IRMA (nu omgedoopt tot Yivi), Datakeeper, Ockto en Schluss. In de Innovalor verkenning wordt geconcludeerd dat het speelveld gefragmenteerd en onvolwassen is. Dit kan verklaard worden o.a. door het ontbreken van een architectuurmodel, standaarden van gegevensuitwisseling en gespecificeerde eisen qua functionaliteit en beveiliging. De nieuwe

eIDAS 2.0 verordening ondervangt deze punten. Wel blijft een duidelijk verdienmodel ontbreken voor de wallet-providers, omdat de EDI-wallet gratis moet worden aangeboden. Er zal mogelijk een verdienmodel te vinden zijn in de integratie van ID-wallets met andere betaalde diensten, de bedrijven-wallet en het aanbieden van gewaarmerkte gegevens (zie 'attribute-provider') of elektronische handtekeningen.

7.2 User - PID (Personal Identification Data)

Een bijzondere set van gewaarmerkte persoonsgegevens is de zogenaamde *Personal Identification Data* (PID). De PID is een bijzondere set van persoonsgegevens (ook wel 'attributen' genoemd), want dit is een set gegevens waarmee de identiteit van een natuurlijk persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld. De PID-gegevens zijn veelal afkomstig uit het BRP (Basis Registratie Persoonsgegevens) en de RvIG (Rijksdienst voor Identiteitsgegevens) fungeert daarmee als PID-provider in Nederland.

PID kan opgedeeld worden in verschillende categorieën:
- Verplicht: dit is de minimale set persoonsgegevens die zijn gespecificeerd in eIDAS CIR 2015/1501, namelijk huidige achternaam, voornamen, geboortedatum en unieke identificatie;
- Optioneel: achternaam bij geboorte, voornamen bij geboorte, geboorteplaats, huidige adres en geslacht;
- Mogelijke aanvullende optionele attributen: nationaliteit en nationale attributen, zoals BSN.

Van belang is dat deze persoonlijke attributen geattesteerd (digital ondertekend/bevestigd) worden door een daartoe bevoegde en bovenal vertrouwde partij. Bijvoorbeeld via het Ministerie van Binnenlandse Zaken die ook nu paspoorten verstrekt.

Een belangrijke stap bij het gebruik van de EDI-wallet is de stap waarmee de houder wordt gekoppeld aan de wallet. Deze stap gaat samen met het plaatsen van de PID-gegevens in de wallet van de houder en het koppelen of linken van deze aan de houder. Dit is complex, want het mag niet zo zijn dat iemand anders dan de gekoppelde houder deze PID kan gebruiken. Er zijn grofweg drie opties om de verplichte PID attributen uit te geven door de overheid en te koppelen aan de EDI-wallet:
- Online en ID-scan: zoals via DigiD i.c.m. eNIK (identiteitsbewijs scannen met telefoon via NFC, daarvan zijn slechts een miljoen geschikte ID's voor in omloop);
- Fysiek proces: afspraak aan een balie incl. paspoort om identiteit fysiek te verifiëren;
- Volledig online: bijvoorbeeld via een webportaal met digitale verificatie, bv. een video-verificatie als de wallet is gecompromitteerd zoals bij verlies of diefstal in het buitenland.

Nadat de verplichte PID-categorie is toegevoegd aan de EDI-wallet, kunnen gebruikers vervolgens de vrijwillige attributen toevoegen via gekwalificeerde derde partijen, namelijk de Quality Trusted Service Providers (QTSP). Ook is het mogelijk om de wallet te gebruiken voor het plaatsen van niet-gekwalificeerde attributen die geen persoonskenmerken bevatten, zoals een treinkaartje.

7.3 Attribute-provider

Naast de benodigde gegevens voor identificatie en authenticatie van de wallet (o.a. door de PID) en de mogelijkheid voor het zetten van digitale handtekeningen, kunnen gebruikers ook andere (persoons) gegevens aan de wallet toevoegen. Deze zogenaamde 'attribute' is een kenmerk, karakteristiek of kwaliteit van een natuurlijk persoon, rechtspersoon of van een entiteit. Via een attestatie in elektronische vorm door de 'attribute-provider' kan de authenticatie en toekenning van attributen mogelijk gemaakt worden via de EDI-wallet.

Iedereen kan gegevens in een wallet zetten, maar gegevens krijgen pas waarde als de partij die de gegevens verstrekt (via 'attribute-provider') deze waarmerkt en dit controleerbaar is. Bijvoorbeeld:
- Overheid kan persoonsgegevens waarmerken
- Verzekeraar kan bevestigen dat je verzekerd bent
- DUO uittreksel opleveren van diploma's of kwalificaties
- Ouders, school of overheid kan bevestigen dat je ouder bent dan 18 jaar
- De AFM kan bevestigen dat je een AFM-vergunning hebt of als bestuurder getoetst bent

Dit waarmerken van gegevens gaat door middel van een digitale handtekening door de uitgevende instantie of persoon. De nieuwe eIDAS verordening stelt de eis om met de EDI-wallet zelf gekwalificeerde elektronische handtekeningen te kunnen zetten.

Gegevens die in een wallet opgeslagen kunnen worden, worden vaak aangeduid als attributen of credentials. Wanneer de bronhouder deze gegevens waarmerkt d.m.v. een elektronische handtekening, dan heet dit waarmerk de attestatie van het attribuut, ook wel 'verifiable credential' genoemd. De bijgeleverde elektronische handtekening maakt het namelijk verifieerbaar wie de handtekening heeft gezet.

Als we het hebben over het delen van (persoons)gegevens via de EDI-wallet dan dienen we een kanttekening te plaatsen. Met digitalisering is de kans op datamaximalisatie toegenomen, doordat partijen de consument op een laagdrempelig manier kan vragen om persoonsgegevens te delen. De consument is zich hierbij niet altijd bewust welke data ze nu feitelijk delen en het is niet altijd zichtbaar omdat het digitaal plaatsvindt. Een doel van de EDI-wallet is dan ook om het mogelijk te maken enkel de benodigde gegevens te delen of enkel verklaringen van deze gegevens te delen (ook wel dataminimalisatie genoemd). Een voorbeeld hiervan is de mogelijkheid om geen geboortedatum te delen, maar alleen een gewaarmerkte verklaring dat je ouder bent dan 18 jaar, ook bekend als *zero-knowledge proofs*. Deze verklaring kan afgegeven worden door je ouders, gemeente of opleiding. Hier komt het zetten van een digitale handtekeningen van pas. De verklaring in dit voorbeeld ('ik ben ouder dan 18') wordt gewaarmerkt door ouders, gemeente of opleiding. Het is aan de ontvangende partij om te bepalen of de waarmerkende partij voldoende vertrouwen geeft. Hiervoor zullen ook gecertificeerde partij aangewezen worden, de eerdere genoemde attribute-provider, die dit kunnen uitvoeren namens de bronhouder van de gegevens. Vanzelfsprekend kan er een hogere betrouwbaarheid toegekend worden aan attributen die door een gecertificeerde attributed-provider (Qualified trusted service providers, QTSPs) zijn toegevoegd.

Voorbeeld van datamaximalisatie
Instellingen vragen bij kredietverstrekking naar ID-gegevens. De consument kan dit doen door via mijnoverheid.nl de Basis Registratie Persoonsgegevens (BRP) data te delen. De indruk bij de consument is dat het hier slechts om ID-gegevens gaat, terwijl de BRP veel meer persoonsgegevens omvat. Niet iedereen is zich bewust welke data BRP feitelijk bevat.

De overheid is een QTSP, deze kan namelijk de PID-gegevens waarmerken, want deze zijn afkomstig van de Basis Registratie Persoonsgegevens (BRP). De eigenaar van de wallet kan vervolgens deze geattesteerde gegevens vervolgens delen met een verzekeraar. De verzekeraar kan valideren in een daarvoor bestemd register ('trust list') of de attestatie/waarmerk en daarmee de gegevens kloppen. De verzekeraar wordt in dit voorbeeld de ontvangende rol ('relying party') genoemd.

7.4 Relying party

Zoals hierboven gezegd, de *relying party* vertrouwt op de gegevens in de wallet, maar kan deze ook controleren, bijvoorbeeld op de vraag of inderdaad een BRP de persoonsgegevens heeft uitgegeven (gewaarmerkt) door de digitale handtekening in dit geval van BZK, te controleren.

De relying parties zullen vertrouwen op de gewaarmerkte gegevens uit de wallet. Ieder land dient een register of trustlist met gegevens bij te houden, zodat de relying parties kunnen valideren of de afgegeven attestaties correct en authentiek zijn. Het is een taak van de overheid om een dergelijk register bij te houden, in Nederland onderhoudt het RDI deze lijst. Als een Nederlandse bank bijvoorbeeld wil controleren dat de gegevens van een nieuwe Belgische klant betrouwbaar zijn, dan zal de bank de Belgische trustlist hiervoor raadplegen. De Belgische trustlist zal informatie beschikbaar moeten stellen over wie in België de handtekening gezet heeft. Deze trustlists en het bijbehorende register vallen onder de rol van 'validity information' in figuur 5.

7.5 Validity information

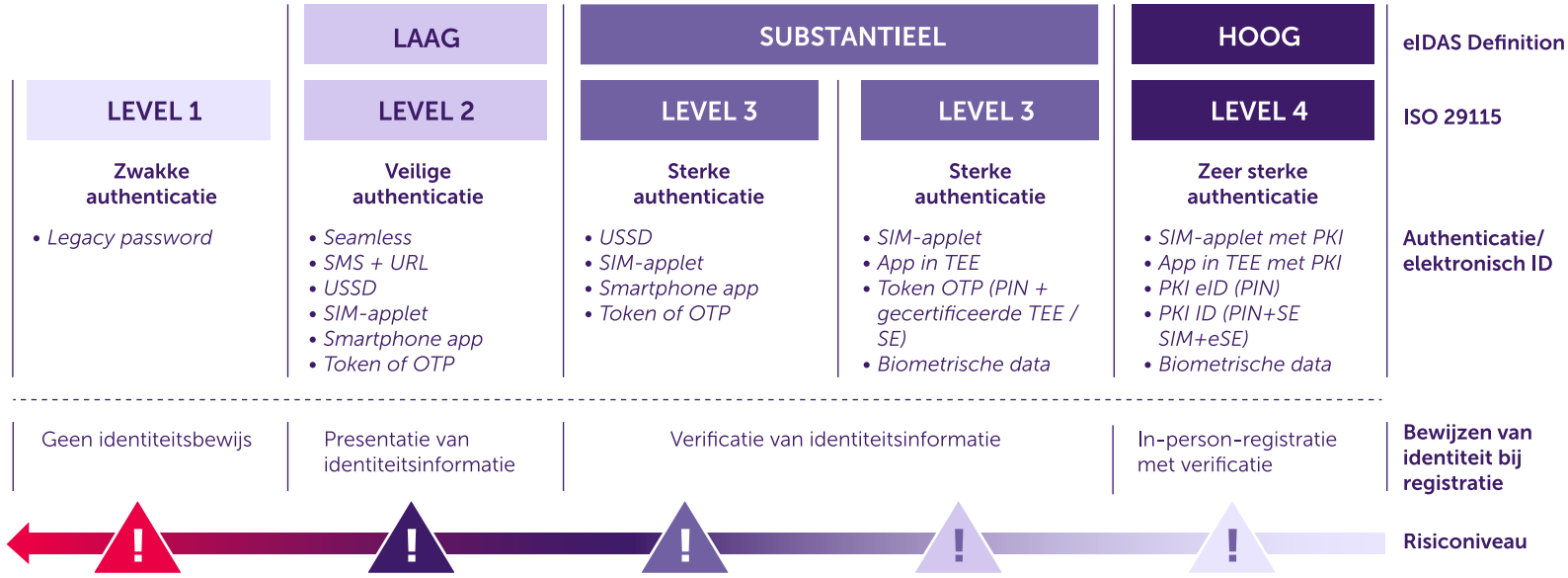
In ieder land zullen er openbare (online) registers beschikbaar worden gesteld via welke men de waarmerken van de gegevens uit de wallet kan verifiëren. Initieel gaat dit via het *European Blockchain Service Infrastructure* (EBSI). Het EBSI is een netwerk van gekoppelde registers in Europa. De beschikbare gegevens dienen wel door een *qualified trusted service provider* in de wallet geplaatst of gewaarmerkt te zijn.

Hoe deze trust lists in de toekomst gehost gaan worden, staat nog niet vast. Verschillende landen hebben voorgesteld de European Blockchain Services Infrastructure (EBSI) te gebruiken hiervoor.

7.6 De betrouwbaarheid van een wallet

De EDI-wallet gaat online identificatie en authenticatie van personen mogelijk maken. Tot op heden is identificatie van een persoon enkel mogelijk m.b.v. een paspoort, rijbewijs of ID kaart. Dit zijn fysieke (papier of plastic) documenten en in Nederland zijn deze sinds 2006 voorzien van een RFID chip die uitgelezen kan worden voor aanvullende toepassingen, zoals geautomatiseerde paspoortcontrole op Schiphol. Deze fysieke documenten zijn niet initieel ontworpen met online identificatie in gedachte. Daarnaast is er in Nederland ook de DigiD-app die in eerste instantie is ontworpen als identificatie/toegang middel voor overheidswebsites als onderdeel van het eIDAS1.0 regime.

Identificatie via de EDI-wallet verloopt geheel online en hierbij zouden geen extra middelen nodig zijn, enkel de EDI-wallet die is geïnstalleerd op een mobiele telefoon. Vanzelfsprekend wil de partij die de identificatie/authenticatie uitvoert er zeker van zijn dat een persoon die zich via de EDI-wallet identificeert ook daadwerkelijk die persoon is. Via betrouwbaarheidsniveaus wordt de mate van vertrouwen weergegeven die in een elektronisch identificatiemiddel, de wallet, gesteld kan worden. De betrouwbaarheidsniveaus zijn vastgelegd in de eIDAS2.0 verordening, de zogenaamde Levels of Assurance (LoA), zie figuur 6. eIDAS beschrijft drie eIDAS2.0 Levels of Assurance; Laag, Substantieel en Hoog. Als een wallet slechts voldoet aan het laagste niveau dan betekent dit niet dat er geen identificatie plaats kan vinden op basis van enkel de wallet. De wallet in combinatie met bijvoorbeeld het paspoort (Chip uitlezen via NFC) kan een oplossing zijn hier. De LoA 1 - 4 zijn vastgelegde normen. Het hoogste LoA dient zich op het niveau van paspoortidentificatie te bevinden en zou dus geschikt moeten zijn voor het digitaal openen van een bankrekening.



Figuur 6: De levels of assurance voor eID

De identificatie/authenticatie via de EDI-wallet lijkt eenvoudig, maar er dient wel een proces aan vooraf te gaan. De EDI-wallet dient namelijk eerst onlosmakelijk gekoppeld te worden aan de houder (via PID gegevens). Bij LoA Hoog vindt de uitrol veelal plaats bij een balie van bijvoorbeeld een gemeente, net als het huidige paspoortuitgifte proces werkt. Cruciaal is dat de persoonsgegevens en de sleutels waarmee digitale handtekeningen gezet worden veilig opgeslagen zijn. Dat kan op een simkaart of in een veilige enclave (bv. 'secure element') op een mobiele telefoon.