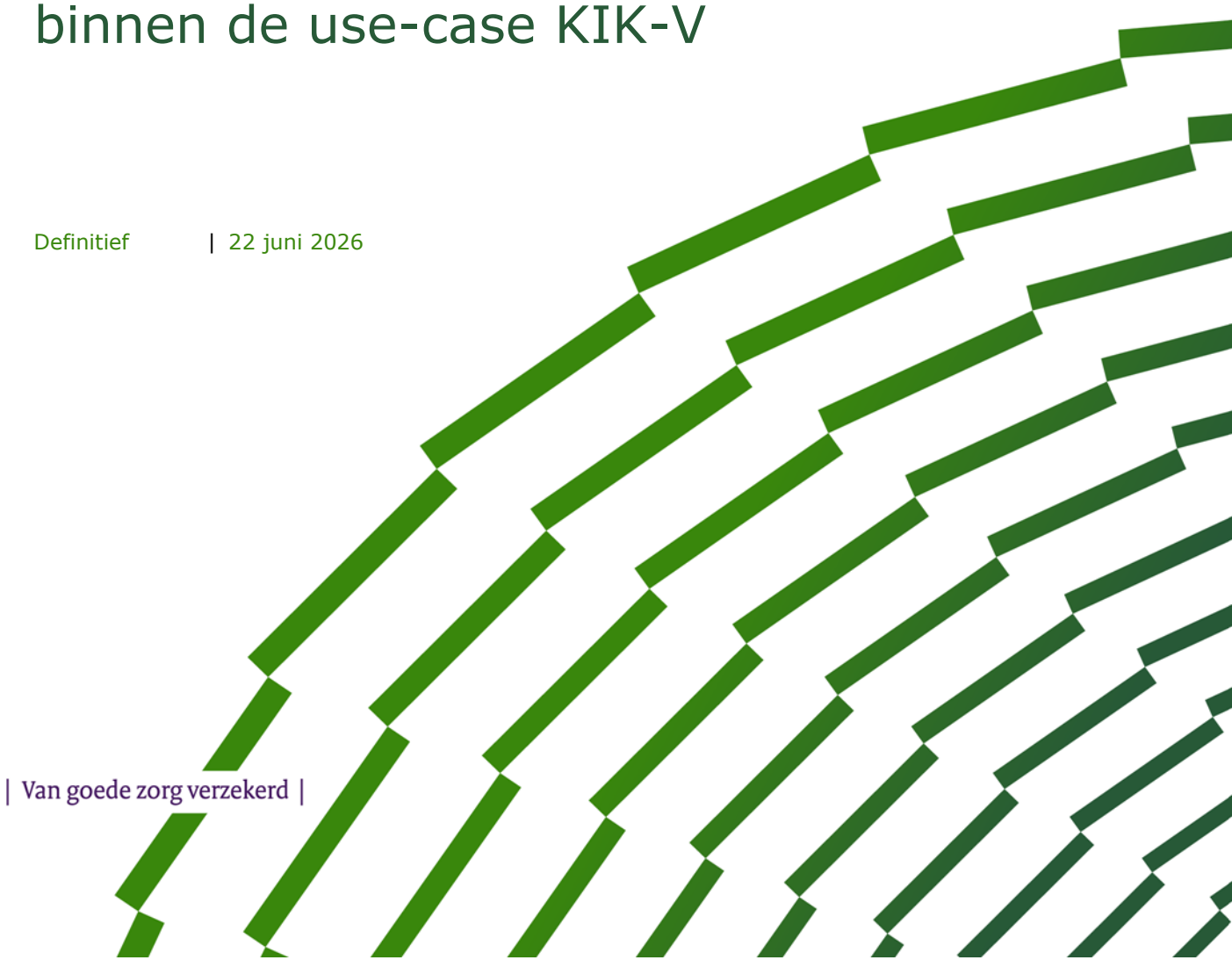
Zorginstituut Nederland

Europese digitale identiteit voor gegevensuitwisseling tussen organisaties

Verkennend onderzoek naar de impact van de eIDAS 2.0 en EBW binnen de use-case KIK-V

Definitief | 22 juni 2026



| Van goede zorg verzekerd |

Inhoudsopgave

	Samenvatting	**3**
	Inleiding	**5**
1	**eIDAS 2.0**	**6**
1.1	Europese identiteit voor personen én organisaties (PID)	6
1.2	Digitaal aantoonbare eigenschappen en kenmerken	6
1.3	Uitbreiding vertrouwensdiensten	6
1.4	EDI-wallet	6
2	**EBW-verordening**	**8**
2.1	Europese identiteit van organisaties (LPID/ EBWOID)	8
2.2	Verifieerbare organisatiegegevens	8
2.3	Digitale mandatering	8
2.4	Communicatiekanaal op basis van QERDS	9
2.5	European Business Wallet (EBW)	9
3	**Impact op gegevensuitwisseling zorgsector**	**10**
4	**KIK-V als praktijkvoorbeeld**	**11**
4.1	Programma KIK-V	11
4.1.1	KIK-V werkwijze	11
4.1.2	Nuts als vertrouwensstelsel	12
4.2	Impact eIDAS 2.0 en EBW-verordening op KIK-V	13
4.3	Voorbeeldbeproeving	15
4.3.1	Lessons learned uit beproeving	16
5	**Conclusies en aanbevelingen**	**17**
	Colofon	**18**

Samenvatting

De Europese Unie (EU) werkt aan regelgeving op het gebied van digitalisering en gegevensuitwisseling zodat burgers, bedrijven en overheden binnen de EU eenvoudig en betrouwbaar digitale diensten kunnen gebruiken om gegevens uit te wisselen over landsgrenzen heen. Onderdeel hiervan is de herziening van de eIDAS-verordening (eIDAS 2.0) en de ontwikkeling van de Verordening Europese Business Wallet (EBW).

Deze ontwikkelingen leggen de basis voor digitale identiteit en betrouwbare gegevensuitwisseling. eIDAS 2.0 richt zich hierbij op de basiselementen; een digitale identiteit voor burgers en organisaties én vertrouwensdiensten om veilige en betrouwbare gegevensuitwisseling binnen de EU te faciliteren. De EBW-verordening past deze basis toe en breidt deze uit voor de specifieke gegevensuitwisseling en interacties tussen overheden en organisaties.

Voor de zorgsector sluiten deze ontwikkelingen aan op de European Health Data Space (EHDS). Waar de EHDS bepaalt welke gezondheidsgegevens onder welke voorwaarden mogen worden gedeeld, voorzien eIDAS 2.0 en de EBW-verordening in de mechanismen om identiteiten vast te stellen, bevoegdheden aantoonbaar te maken en gegevensuitwisseling veilig en betrouwbaar te laten verlopen. Kort samengevat bepaalt de EHDS *wat* wordt gedeeld, terwijl eIDAS 2.0 en de EBW-verordening bepalen *hoe* en door wie dit gebeurt.

Het was onbekend welke impact deze nieuwe regelgeving heeft op bestaande vormen van gegevensuitwisseling. In het bijzonder wanneer het gaat om identificatie van organisaties bij digitale gegevensuitwisseling tussen organisaties en overheden (system-to-system gegevensuitwisseling). Een praktijkvoorbeeld is Programma KIK-V.

Binnen Programma KIK-V (Keteninformatie Kerngegevens Verbeteren) werken verschillende organisaties in de verpleegzorg samen aan het verbeteren van de informatievoorziening binnen de keten. Het doel is om het delen van verantwoordingsgegevens over kwaliteit en bedrijfsvoering tussen zorgaanbieders en informatievragende partijen eenduidig en eenvoudig te maken.

Dit wordt gerealiseerd door heldere afspraken te maken over welke gegevens, waarom uitgewisseld worden en het ontwikkelen van technologie die de uitwisseling mogelijk maakt. Centraal binnen de werkwijze staan het hergebruiken van gegevens uit het operationele proces, verlaging van administratieve lasten en het realiseren van meervoudig gebruik van eenmalig vastgelegd data. Binnen de KIK-V werkwijze worden zorgorganisaties én informatievragende partijen geïdentificeerd via een uitgegeven digitaal bewijs (verifiable credential).

Om meer inzicht te krijgen in de impact van de eIDAS 2.0 en EBW op de identificatie van organisaties in system-to-system gegevensuitwisseling heeft Zorginstituut Nederland van december 2025 tot en met mei 2026 een onderzoek uitgevoerd, met de KIK-V werkwijze als use-case.

De onderzoeksvraag luidde als volgt:
In hoeverre zijn de eIDAS 2.0 en de EBW van toepassing voor de identificatie van organisaties in een system-to-system gegevensuitwisseling, en welke aandachtspunten volgen hieruit voor de KIK-V werkwijze?

Uit het onderzoek blijkt dat de eIDAS 2.0 en EBW samen een Europees raamwerk vormen voor betrouwbare digitale interacties. Dit raamwerk introduceert een aantal fundamentele veranderingen in de manier waarop organisaties zich identificeren en gegevens uitwisselen.

Deze veranderingen zijn generiek van aard en gelden sectoroverstijgend. KIK-V fungeert in dit onderzoek als concreet voorbeeld om deze impact te duiden, maar de bevindingen zijn breder toepasbaar op andere vormen van gegevensuitwisseling tussen organisaties.

Het onderzoek bevestigt dat de EBW-verordening richtinggevend wordt voor de inrichting van gegevensuitwisseling tussen overheden en organisaties binnen Europa. eIDAS 2.0 introduceert de basiselementen voor een Europese digitale identiteit en vertrouwensdiensten voor gegevensuitwisseling binnen de EU. De EBW-verordening specificeert en breidt deze elementen uit voor de gegevensuitwisseling en interacties tussen overheden en organisaties.

Zodra de EBW-verordening in de EU wordt vastgesteld betekent dit voor KIK-V dat:
1. Diverse informatievragende partijen (die als publieke instantie worden aangemerkt) **verplicht** worden om de aanlevering van gegevens via een EBW te accepteren wanneer deze aanlevering behoort tot een administratief proces en/of rapportageverplichting.
2. Zorgaanbieders hiermee het **recht** hebben om een EBW te gebruiken voor de aanlevering van gegevens aan vorengenoemde informatievragende partijen.

De huidige KIK-V werkwijze sluit in de kern goed aan op de uitgangspunten van de Europese ontwikkelingen. De technische impact op de architectuur kan relatief beperkt blijven, als gekozen wordt voor een modulaire uitbreiding van de bestaande infrastructuur met een aanvullende vertrouwenslaag. Deze uitbreiding omvat:
- De acceptatie van een EBW bij de gegevensaanlevering;
- De aansluiting op Europese identificatie- en adresseringsmechanismen;
- De ondersteuning van mandatering en vertegenwoordiging;
- De toepassing van gekwalificeerde vertrouwensdiensten, zoals digitale zegels en QERDS.

De grootste impact ligt niet primair op techniek, maar op governance, afsprakenstelsels, toezicht, rollen en verantwoordelijkheden binnen de keten. Deze impact is alleen nog sterk afhankelijk van eventuele wijzigingen in de EBW-verordening, verdere uitwerking van de uitvoeringshandelingen en invulling vanuit de markt.

Daarnaast bevestigt het onderzoek dat de Europese ontwikkelingen niet alleen verplichtingen met zich meebrengen, maar ook kansen bieden. Door aan te sluiten op Europese standaarden kan KIK-V profiteren van bestaande Europese vertrouwensdiensten en infrastructuren, waardoor minder sectorspecifieke voorzieningen nodig zijn. Ook ontstaat meer uniformiteit, interoperabiliteit en herbruikbaarheid van oplossingen, zowel binnen als buiten de zorgsector.

Op basis van het onderzoek wordt Programma KIK-V aanbevolen om de ontwikkelingen rondom de eIDAS 2.0 en EBW-verordening actief te volgen, gerichte beproevingen uit te voeren en de architectuur én governance voor te bereiden op wallet-implementatie.

Inleiding

De Europese Unie (EU) heeft met de herziene Electronic Identification and Trust Services-verordening (eIDAS 2.0) een belangrijke stap gezet richting een Europese digitale identiteit. Een verordening van de EU is rechtstreeks van toepassing in alle EU-lidstaten. Dit betekent dat alle rechten en plichten uit de verordening direct gelden voor Nederlandse overheden, organisaties en burgers. Met de eIDAS 2.0 wordt een wettelijk kader gecreëerd voor de introductie van de European Digital Identity (EDI-)wallets: digitale voorzieningen waarmee burgers en organisaties hun identiteit en andere geverifieerde gegevens veilig kunnen beheren, delen en gebruiken binnen de EU.

Binnen deze ontwikkeling worden hoge eisen gesteld aan veiligheid, betrouwbaarheid, interoperabiliteit en transparantie. EDI-wallets moeten voldoen aan gezamenlijke technische standaarden, waaronder het Architecture and Reference Framework (ARF), en moeten uitwisseling en verificatie van gegevens binnen de gehele EU mogelijk maken.

De introductie van EDI-wallets wordt binnen de Nederlandse zorgsector niet alleen gezien als een technische of juridische ontwikkeling, maar ook als een belangrijke aanjager van digitale gegevensuitwisseling. Ook sluit deze ontwikkeling aan bij bredere nationale en Europese ambities rondom databeschikbaarheid en gestandaardiseerde gegevensuitwisseling, zoals de Nationale Visie en Strategie Gezondheidsinformatiestelsel (NVS) en de European Health Data Space (EHDS).

Naast eIDAS 2.0 is inmiddels ook de Europese verordening voor de European Business Wallet (EBW-verordening) in ontwikkeling. Waar eIDAS 2.0 zich primair richt op digitale identiteiten van natuurlijke personen en het gebruik van wallets in interactie tussen burgers en organisaties, richt de EBW-verordening zich nadrukkelijker op de digitale identificatie en gegevensuitwisseling tussen organisaties. Daarmee ontstaat een aanvullend Europees kader voor zakelijke identiteiten, bevoegdheden en machine-to-machine of system-to-system gegevensuitwisseling. De samenhang tussen eIDAS 2.0 en de EBW-verordening is daarmee relevant voor organisaties die werken aan betrouwbare digitale identificatie en uitwisseling van gegevens binnen ketens en netwerken.

Tegelijkertijd is de praktische uitwerking van deze Europese kaders voor organisatie-identificatie en system-to-system toepassingen nog volop in ontwikkeling. Hierdoor bestaat nog onzekerheid over de wijze waarop deze kaders toegepast moeten worden in concrete uitvoeringspraktijken binnen sectoren zoals de zorg.

Binnen de Nederlandse zorgsector bestaan al initiatieven waarin veilige en geverifieerde gegevensuitwisseling tussen organisaties wordt toegepast. Een voorbeeld hiervan is het Programma KIK-V (Keteninformatie Kerngegevens Verbeteren). Binnen KIK-V werken informatievragende partijen samen met zorgaanbieders aan het verbeteren van de informatie-voorziening in de verpleegzorg. Hierbij wordt onder andere gebruikgemaakt van verifiable credentials voor de identificatie van organisaties, ondersteund door Nuts-afspraken. Door organisaties vooraf te verifiëren en digitale handtekeningen toe te passen bij informatie-uitvragen, wordt geborgd dat gegevens uitsluitend worden uitgewisseld tussen betrouwbare en geautoriseerde partijen.

De ontwikkelingen rondom eIDAS 2.0 en de EBW-verordening roepen de vraag op in hoeverre bestaande werkwijzen, zoals die van KIK-V, aansluiten op de huidige en toekomstige Europese wet- en regelgeving. In opdracht van Zorginstituut Nederland is daarom een onderzoek uitgevoerd naar de toepassing van eIDAS 2.0 en de EBW-verordening bij organisatie-identificatie in system-to-system gegevensuitwisseling, met KIK-V als use-case. Dit rapport beschrijft welke aandachtspunten en kansen de Europese kaders bieden voor de huidige en toekomstige inrichting van de KIK-V werkwijze.

1 eIDAS 2.0

De eIDAS 2.0 is een verbreding en verdieping ten opzichte van de oorspronkelijke verordening uit 2014. De oorspronkelijke eIDAS richtte zich primair op wederzijdse erkenning van nationale elektronische identificatiemiddelen en vertrouwensdiensten. Het centrale doel van eIDAS 2.0 is dat 'burgers en organisaties binnen de EU digitaal zaken kunnen doen op een manier die juridisch betrouwbaar, technisch interoperabel en grensoverschrijdend bruikbaar is'. Daarbij verschuift de focus van enkel "inloggen" naar een breder **digitaal vertrouwensstelsel**, waarin vertrouwensdiensten in samenhang worden geregeld.

De eIDAS 2.0 ziet daarbij niet alleen toe op natuurlijke personen, maar expliciet ook op 'rechtspersonen en vertegenwoordiging': het gaat dus ook om het aantonen dat iemand namens een organisatie handelt en daartoe bevoegd is.

De volgende elementen worden daarom geïntroduceerd binnen de eIDAS 2.0:

1.1 Europese identiteit voor personen én organisaties (PID)

De eIDAS 2.0 introduceert het begrip 'Persoonsidentificatiegegevens (PID)', gedefinieerd als een set gegevens waarmee de identiteit van een natuurlijke persoon of rechtspersoon kan worden vastgesteld. Een PID kan dus zowel een persoon als een rechtspersoon identificeren. Voor de identificatie van een rechtspersoon wordt in dat geval gesproken over Legal Person Identification Data (LPID).

Aan deze PID kunnen digitale bewijzen en attributen (zie *1.2*) worden gekoppeld. Een PID vormt hiermee de basis voor verdere interacties, zoals gegevensuitwisseling, autorisatie en ondertekening.

1.2 Digitaal aantoonbare eigenschappen en kenmerken

Een tweede belangrijk nieuw element is de introductie van *'elektronische attestaties van attributen'*. Dit zijn digitale bewijzen van eigenschappen of kenmerken, afkomstig van een betrouwbare bron. Hiermee kan een persoon of organisatie bijvoorbeeld diens rol en bevoegdheid aantonen. Het doel hierbij is dat enkel de voor de uitwisseling relevante/noodzakelijke gegevens aangetoond hoeven te worden.

1.3 Uitbreiding vertrouwensdiensten

Daarnaast wordt het bestaande stelsel van elektronische vertrouwensdiensten uitgebreid met o.a. gekwalificeerde elektronische handtekeningen, tijdstempels en zegels. Dit versterkt de juridische waarde van digitale interacties en documenten.

1.4 EDI-wallet

Tot slot introduceert en verplicht de eIDAS 2.0 de European Digital Identity (EUDI) wallet, in Nederland vook aangeduid als Europese Digitale Identiteit (EDI-) Wallet. Deze EDI-wallet is gedefinieerd als een product en dienst (in de praktijk; app op telefoon) waarmee een *gebruiker – burger of organisatie* – digitale identiteitsgegevens, attestaties van attributen en andere gewaarmerkte gegevens kan opslaan en gecontroleerd kan delen met ***publieke instanties*** én andere ***vertrouwende partijen***.

- ***Publieke instanties*** die '*online diensten aanbieden*' waarbij identificatie of authenticatie nodig is, worden verplicht om EDI-wallets te accepteren als inlogmiddel en – afhankelijk van verdere uitwerking – ook om bepaalde attributen te accepteren. Denk hierbij bijvoorbeeld aan de belastingdienst voor de online aangifte van de inkomstenbelasting.

- ***Vertrouwende partijen*** zijn organisaties die op vrijwillige basis digitale diensten aanbieden en daarbij vertrouwen op elektronische identificatie, wallets of attestaties. Vertrouwende partijen die de wallet willen inzetten in hun dienstverlening moeten zich registreren in een openbaar register. Daarin geven zij aan voor welke diensten zij de wallet willen laten gebruiken en welke gegevens zij daarvoor van de gebruiker vragen. Alleen na registratie kan de wallet worden ingezet voor dat doeleinde door controle van een certificaat dat na registratie aan de vertrouwende partij wordt uitgegeven.

Lidstaten zijn verplicht om uiterlijk eind 2026 ten minste één kosteloze en gecertificeerde EDI-wallet beschikbaar te stellen die voldoet aan het Europese *'Architecture and Reference Framework (ARF)'*. Dit raamwerk bevat technische standaarden, protocollen en beveiligingseisen en wordt via uitvoeringshandelingen onderdeel van de verordening. De EDI-wallet fungeert daarmee als een uniform Europees instrument voor digitale identificatie, authenticatie en gegevensdeling.

2 EBW-verordening

Op 19 november 2025 heeft de Europese Commissie een voorstel gepubliceerd ter introductie van Europese Business Wallets (EBW). Het hoofddoel van de EBW-verordening is structurele lastenverlichting door interne-marktbelemmeringen weg te nemen en het realiseren van snellere administratieve processen in zowel B2B (business-to-business) als B2G (business-to-government) relaties.

Een EBW is daarmee een digitale oplossing waarmee *economische entiteiten – bedrijven, organisaties of publieke instanties –* veilig bedrijfsgegevens en andere informatie kunnen opslaan, beheren en **onderling** delen. Deze digitale oplossing is geen app op een telefoon zoals bij de EDI-wallet, maar draait in de bestaande ICT-infrastructuur van een entiteit.

De EBW-verordening bouwt voort op de technische en juridische infrastructuur van de eIDAS 2.0, maar richt zich op zakelijk gebruik en gegevensuitwisseling tussen economische entiteiten (hierna: organisaties). Een aantal elementen worden hierbij geïntroduceerd en geconcretiseerd:

2.1 Europese identiteit van organisaties (LPID/ EBWOID)

Organisaties krijgen een unieke digitale identiteit, gebaseerd op bestaande registraties, zoals in Nederland het Handelsregister van de Kamer van Koophandel.

Daarnaast wordt gewerkt aan een Europese adressengids, waarmee organisaties elkaar digitaal kunnen vinden voor gegevensuitwisseling. Hiermee ontstaat een Europees interoperabel stelsel voor identificatie, routering en authenticatie van organisaties.

2.2 Verifieerbare organisatiegegevens

De eIDAS 2.0 introduceert *elektronische attestaties van attributen* als juridisch en technisch mechanisme om eigenschappen, rollen en bevoegdheden digitaal aantoonbaar te maken.
De EBW-verordening past dit principe concreet toe op zakelijke gegevensuitwisseling. Hierdoor verschuift gegevensuitwisseling van traditionele documenten, zoals pdf-bestanden of scans, naar digitaal beveiligde (*cryptografische*) gegevens die aantoonbaar afkomstig zijn van betrouwbare bronnen.

Organisatiegegevens, registraties, certificeringen en bevoegdheden kunnen daarmee automatisch en machineleesbaar worden geverifieerd, zonder handmatige documentcontrole. Dit vermindert administratieve lasten en vergroot de betrouwbaarheid van gegevensuitwisseling.

2.3 Digitale mandatering

De eIDAS 2.0 introduceert het uitgangspunt dat vertegenwoordiging en bevoegdheden digitaal aantoonbaar moeten kunnen worden gemaakt.

De EBW-verordening werkt dit verder uit voor zakelijke processen en system-to-system interacties. Binnen de verordening wordt expliciet ondersteund dat organisaties:

- mandaten en volmachten digitaal kunnen beheren;
- bevoegdheden machineleesbaar kunnen uitwisselen;
- en vertegenwoordiging *cryptografisch* kunnen aantonen.

Hierdoor kan bijvoorbeeld digitaal worden vastgesteld dat een bestuurder bevoegd is om gegevens namens een organisatie aan te leveren of dat een medewerker gemachtigd is om namens een organisatie te handelen.

2.4 Communicatiekanaal op basis van QERDS

De EBW-verordening introduceert een beveiligd communicatiekanaal op basis van de in de eIDAS 2.0 geintroduceerde vertrouwensdiensten, de Qualified Electronic Registered Delivery Services (QERDS).

De *5 kernaspecten van QERDS* zijn als volgt:
1. Identiteitsverificatie
2. Beveiligde verzending
3. Tijdstempels
4. Bewijs van ontvangst en levering
5. Interoperabiliteit binnen EU

Zodoende kan met QERDS worden vastgesteld:
- wie gegevens heeft verzonden;
- wie gegevens heeft ontvangen;
- wanneer gegevens zijn verzonden en ontvangen;
- en dat de inhoud onderweg niet is gewijzigd.

Hiermee ontstaat een Europees gestandaardiseerd communicatiekanaal voor betrouwbare gegevensuitwisseling tussen organisaties en overheden. De toepassing van QERDS vervangt daarmee deels bestaande, versnipperde en vaak nationaal georganiseerde oplossingen voor veilige gegevensuitwisseling.

2.5 European Business Wallet (EBW)

Een EBW maakt het hiermee voor organisaties mogelijk om:
- zich digitaal te identificeren en authenticeren;
- bedrijfsgegevens en registraties gecontroleerd te kunnen delen;
- officiële documenten te kunnen indienen en ontvangen;
- documenten veilig te kunnen ondertekenen of verzegelen;
- mandaten/volmachten te kunnen beheren;
- en bevoegdheden en mandaten te kunnen aantonen (machineleesbaar).

De EBW-verordening stelt geen verplichting aan entiteiten om de EBW te gebruiken voor de aanlevering van gegevens. *Publieke instanties* worden wél verplicht om de aanlevering van gegevens via een EBW te accepteren wanneer deze gegevens aangeleverd worden om aan een **rapportageverplichting** te voldoen of onderdeel zijn van **administratieve procedure**. Hiervoor geldt een invoeringstermijn voor 24 maanden na het aannemen van de uitvoeringshandelingen die vallen onder de EBW-verordening.

Een EBW kan worden aangeboden door:
- In de EU gevestigde private bedrijven die voldoen aan strenge eisen op het gebied van beveiliging en governance
- EU-instellingen, -organen en -agentschappen

Aanbieders moeten voldoen aan de eIDAS-vereisten voor vertrouwensdiensten, de cyberbeveiligingswet (NIS2) en het toezicht. Een openbare EU-lijst met erkende aanbieders zal duidelijk maken welke aanbieders officieel erkend zijn.

Tussen EBW's en EDI-wallets moet bovendien volledige interoperabiliteit bestaan, onder meer voor het toegangsbeheer voor gebruikers van een EBW door het aantonen van de juiste machtigingen.

3 Impact op gegevensuitwisseling zorgsector

De eIDAS 2.0 en EBW-verordening vormen samen de basis voor een nieuw stelsel van digitale identiteit en vertrouwen voor gegevensuitwisseling binnen de EU. Waar eIDAS 2.0 zich richt op digitale identiteit en vertrouwensdiensten voor burgers, professionals en organisaties, werkt de EBW-verordening deze uitgangspunten verder uit voor gegevensuitwisseling tussen organisaties onderling. Hierdoor ontstaat een samenhangend stelsel waarin identiteit, bevoegdheden en gegevens op een gestandaardiseerde manier kunnen worden uitgewisseld binnen de EU.

Voor de zorgsector zijn deze ontwikkelingen relevant omdat zij aansluiten op de sectorspecifieke invulling van de Europese datastrategie voor de zorg, namelijk de European Health Data Space (EHDS). De EHDS bepaalt welke gezondheidsgegevens onder welke voorwaarden worden uitgewisseld, terwijl eIDAS 2.0 en de EBW-verordening voorzien in de mechanismen om identiteiten vast te stellen, bevoegdheden aantoonbaar te maken en gegevensuitwisseling betrouwbaar en juridisch houdbaar te laten plaatsvinden.

In die zin kunnen de drie ontwikkelingen als volgt worden gepositioneerd:

- eIDAS 2.0 (EDI-wallet): wie ben je? (identiteit van burgers en professionals)
- EBW: namens wie handel je? (identiteit en bevoegdheden van organisaties)
- EHDS: welke gezondheidsgegevens worden gedeeld en onder welke voorwaarden?

Kortom; de EHDS bepaalt wát er gedeeld wordt, de eIDAS 2.0/EBW bepaalt hóe en door wie dat veilig gebeurt.

Voor *private zorginstanties* zoals individuele zorgaanbieders en zorginstellingen volgt op dit moment geen directe verplichting om gebruik te maken van een EDI-wallet of EBW. Die verplichting rust wel op overheidsorganisaties. Het is alleen nog niet duidelijk in hoeverre het gebruik van QERDS, onderdeel van de eisen in de EBW-verordening, verplicht zal zijn voor specifieke typen interacties binnen de zorgsector. En in welke gevallen alternatieve vormen van gegevensuitwisseling volstaan. Met name de afbakening tussen zorginhoudelijke gegevensuitwisseling enerzijds en administratieve of juridische processen anderzijds vraagt om nadere duiding.

De geïntroduceerde elementen uit beide verordeningen, waaronder de QERDS, zijn echter wel breed toepasbaar en zouden daarmee een rol kunnen spelen om de inrichting van gegevensuitwisseling in de zorg verder te optimaliseren. De uitdaging hierbij ligt in het vinden van een balans tussen aansluiting op deze Europese ontwikkelingen en het beheersbaar houden van de complexiteit en impact op bestaande systemen en processen.

4 KIK-V als praktijkvoorbeeld

Om de impact van de eIDAS 2.0 en EBW-verordening op bestaande vormen van system-to-system gegevensuitwisseling concreter te kunnen duiden is KIK-V als use-case geselecteerd.

Programma KIK-V is een praktijkvoorbeeld van gestandaardiseerde, bron gebaseerde gegevensuitwisseling binnen een complexe keten. De eIDAS 2.0 en EBW-verordening stellen eisen aan betrouwbare, herbruikbare en gestandaardiseerde gegevensuitwisseling, waarbij het principe van gegevens bij de bron centraal staat. De KIK-V werkwijze kan gezien worden als bestaande implementatiepraktijk die aanknopingspunten biedt voor de toepassing van de Europese kaders binnen de zorgsector.

4.1 Programma KIK-V

Binnen Programma KIK-V werken verschillende organisaties[1] in de verpleegzorg samen aan het verbeteren van de informatievoorziening binnen de keten. Het doel is om het delen van verantwoordingsgegevens over kwaliteit en bedrijfsvoering tussen zorgaanbieders en informatievragende partijen eenduidig en eenvoudig te maken.

Dit wordt gerealiseerd door heldere afspraken te maken over welke gegevens, waarom uitgewisseld worden en het ontwikkelen van technologie die de uitwisseling mogelijk maakt. Centraal binnen de werkwijze staan het gebruik van gegevens uit het operationele proces, verlaging van administratieve lasten en het realiseren van meervoudig gebruik van eenmalig vastgelegde data. Hiermee sluit KIK-V aan bij bredere ontwikkelingen rondom databeschikbaarheid en digitalisering van de zorg.

4.1.1 KIK-V werkwijze

De KIK-V werkwijze bestaat in de basis uit de volgende onderdelen:

1. Afsprakenset
    - De afsprakenset bevat de *algemene afspraken* die onderling tussen ketenpartijen zijn vastgelegd over wie wat vraagt, waarom en wanneer. Uit te wisselen gegevens dienen hierbij uniforme definities en peildata te hanteren, zodat de informatie van goede kwaliteit en vergelijkbaar is.
2. Uitwisselprofielen
    - Een uitwisselprofiel bevat de *specifieke afspraken* tussen een informatievragende partij en zorgaanbieder. In een uitwisselprofiel staat welke grondslag een informatievragende partij heeft om antwoorden op uitvragen bij zorgaanbieders op te halen, welke gegevens daarbij gebruikt kunnen worden om tot de antwoorden te komen, op welke wijze de aanlevering van gegevens plaatsvindt én waarvoor die gegevens worden gebruikt. Elke informatievragende partij heeft een (of meerdere) uitwisselprofiel(en), waarin alle informatievragen zijn uitgewerkt. Gepubliceerde uitwisselprofielen zijn te vinden op het publicatieplatform van KIK-V.
3. Datastation
    - Een datastation biedt de *technische ondersteuning* voor de KIK-V werkwijze. Een KIK-V datastation is een voorziening in het IT-landschap van de zorgaanbieder en werkt als slimme rekenmachine. Een KIK-V datastation haalt ruwe gegevens op uit de gekoppelde bronsystemen. Op basis van de gestelde vragen berekent het datastation antwoorden, die veilig beschikbaar worden gesteld aan de informatievragende partij. Een zorgaanbieder geeft zelf akkoord op de data voordat deze verstuurd wordt.
4. KIK-starter
    - De KIK-starter biedt de technische ondersteuning voor informatievragende partijen. Met de KIK-starter is het mogelijk om gegevens tussen datastations en

[1] Zorgaanbieders, ActiZ, Zorgkantoren en Zorgverzekeraars Nederland (ZN), Inspectie Gezondheidszorg en Jeugd (IGJ), Nederlandse Zorgautoriteit (NZa), Ministerie van VWS, Zorginstituut Nederland en cliënten en/of hun naasten via Patiëntenfederatie Nederland.

informatievragende partij uit te wisselen. Gebruikt een aanbieder een datastation, dan bevraagt de KIK-starter dit datastation. De ketenpartij krijgt een melding als de aanbieder het antwoord retour heeft gestuurd. Deze partij kan zelf bepalen op welke manier en in welk format de gegevens uit de KIK-starter ontsloten worden.

In plaats van centrale opslag blijven gegevens zoveel mogelijk bij de bron, en worden alleen de benodigde antwoorden op specifieke vragen gedeeld. Door deze aanpak ontstaat een uniform en schaalbaar model voor gegevensuitwisseling dat niet alleen binnen de verpleegzorg wordt toegepast, maar ook potentieel breder inzetbaar is binnen andere zorgsectoren.

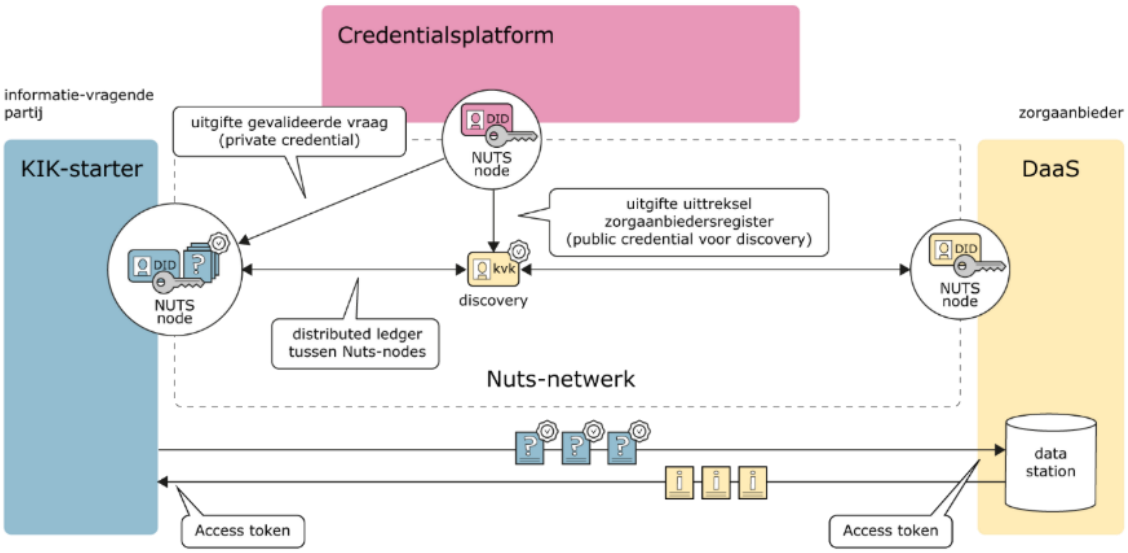
4.1.2 Nuts als vertrouwensstelsel

Binnen de KIK-V werkwijze wordt gebruikgemaakt van de Nuts-infrastructuur als vertrouwensstelsel voor veilige en betrouwbare gegevensuitwisseling tussen informatievragende partijen en zorgaanbieders. Hierbij worden *Verifiable Credentials* (VC's) toegepast: digitale bewijzen waarmee organisaties, bevoegdheden en rechten om gegevens uit te wisselen gecontroleerd kunnen worden.

Binnen KIK-V worden verschillende soorten credentials gebruikt. Zo beschikken informatievragende partijen én deelnemende zorgaanbieders over een credential waarmee zij zich namens hun organisatie kunnen identificeren bij het onderling uitwisselen van vraag en antwoord tussen de KIK-starter en het KIK-V datastation. Daarnaast verstrekt de KIK-V beheerorganisatie per informatievraag een gevalideerde vraag credential. Hiermee kan een zorgaanbieder controleren dat een partij gerechtigd is om een specifieke uitvraag te doen.

Het uitwisselproces, zoals in *Figuur 1* geïllustreerd, verloopt op hoofdlijnen als volgt:

1. Een informatievragende partij logt in op de KIK-starter.
2. De informatievragende partij selecteert in de KIK-starter de vragen (uit het voor deze partij betreffende uitwisselprofiel) én de zorgaanbieders aan wie deze vragen gesteld mogen worden.
3. Zorgaanbieder ontvangt melding dat er vragen zijn ontvangen en logt in op het KIK-V datastation.
4. Het datastation heeft op basis van de gekoppelde gegevens uit de bronsystemen van de zorgaanbieder antwoorden berekend op de vragen. Zorgaanbieder controleert deze antwoorden, past deze indien nodig handmatig aan, en verstuurt de antwoorden (en dus niet de onderliggende gegevens) terug naar de KIK-starter van de informatievragende partij.



Figuur 1: Toepassing Nuts binnen KIK-V gegevensuitwisseling

4.2 Impact eIDAS 2.0 en EBW-verordening op KIK-V

Zoals in hoofdstuk *1.4* vermeld worden publieke instanties die '*online diensten aanbieden*' waarbij identificatie of authenticatie nodig is, vanuit de eIDAS 2.0 verplicht om EDI-wallets te accepteren als inlogmiddel en – afhankelijk van verdere uitwerking – ook om bepaalde attributen te accepteren.

Binnen Programma KIK-V zijn de volgende ketenpartijen aan te merken als *publieke instantie* voor de eIDAS 2.0 en EBW-verordening:

- Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
- Inspectie Gezondheidzorg en Jeugd (IGJ)
- Nederlandse Zorgautoriteit (NZa)
- Zorginstituut Nederland
- Zorgkantoren

De gegevensuitwisseling tussen informatievragende partij (KIK-starter) en zorgaanbieder (KIK-V datastation) kwalificeert waarschijnlijk niet als *aangeboden online dienst*.
Het inloggen van een informatievragende partij op de KIK-starter valt mogelijk wel te kwalificeren als een door het Zorginstituut *aangeboden online dienst*. Dit past echter minder in de geest van de eIDAS 2.0 waarbij het vooral gaat om bredere online dienstverlening aan personen en rechtspersonen (dan de beperkte doelgroep binnen KIK-V). De **directe** impact van de eIDAS 2.0 op KIK-V is hiermee beperkt en vereist waarschijnlijk geen fundamentele architectuurwijzigingen.

Desondanks kan de toepassing van een EDI-wallet wel potentiële meerwaarde bieden in het uitwisselproces. Met een EDI wallet kan namelijk worden gecontroleerd of de persoon die inlogt op de KIK-starter ook daadwerkelijk namens die organisatie mag optreden.

Daarnaast vormen de geïntroduceerde vertrouwensdiensten de basis voor de EBW-verordening, waardoor de eIDAS 2.0 waarschijnlijk wel **indirecte** impact zal hebben. Na vaststelling van de EBW-verordening worden *publieke instanties* binnen KIK-V namelijk verplicht om de aanlevering van gegevens via een EBW te accepteren, voor zover het uitwisselprofiel een verplichte uitvraag betreft waarbij administratieve gegevens en/of rapportage-informatie opgevraagd worden.

Diverse informatievragende partijen voldoen aan deze criteria met de volgende uitvragen:

- Zorginstituut Nederland – Kwaliteitsbeeld

- VWS – Uitwisselprofiel Jaarverantwoording Zorg
- NZa – Basisinformatie kostenonderzoek
- Zorgkantoren - Inkoopondersteuning en beleidsontwikkeling
- IGJ – Contextinformatie t.b.v. aangekondigd inspectiebezoek

Deze verplichting heeft impact op meerdere elementen binnen de KIK-V architectuur:

- KIK-starter
  - Bovengenoemde informatievragende partijen zijn niet verplicht om een EBW te gebruiken bij het stellen van een vraag aan zorgaanbieders, maar moeten de aanlevering van gegevens via een EBW wel accepteren, inclusief bijbehorende standaarden voor gegevensuitwisseling.
  - Dit **vereist** binnen de KIK-starter minimaal de implementatie van:
    - Software om berichten die door een EBW van de zorgaanbieder zijn opgezet/ een claim uit de EBW te kunnen verifiëren, en
    - Software om beveiligde communicatie (QERDS uitwisseling) vanuit een EBW van de zorgaanbieder te ondersteunen. QERDS voegt aan de gegevensuitwisseling meer zekerheid van verzending en ontvangst van een bericht toe, evenals het feit dat het bericht onderweg niet aangepast is (door de zogenoemde verzegeling van het bericht).
  - De toepassing van de EBW en de onderliggende vertrouwensdiensten biedt **aanvullend** mogelijkheden om binnen KIK-V niet alleen organisaties, maar ook vertegenwoordiging en bevoegdheden beter digitaal aantoonbaar te maken. Daarmee kan bijvoorbeeld worden gecontroleerd dat een medewerker daadwerkelijk namens een organisatie handelt. Ook ontstaat de mogelijkheid om bestuurlijke akkoordverklaringen of andere formele bevestigingen digitaal en controleerbaar vast te leggen. Dit versterkt de bestaande vertrouwenslaag binnen de KIK-V gegevensuitwisseling.
  - De impact van de EBW-verordening op de KIK-starter ligt vooral in de ondersteuning van wallet-gebaseerde gegevensuitwisseling en het toepassen van de bijbehorende vertrouwensdiensten, zoals QERDS. De KIK-starter blijft daarbij de applicatie waarmee informatievragende partijen vragen stellen aan datastations van zorgaanbieders, credentials verwerken en antwoorden ontvangen. De EBW-elementen zijn dus geen vervanging van de functionaliteit van de KIK-starter, maar vormen vooral een aanvulling voor het nog veiliger en betrouwbaarder uitwisselen van gegevens tussen organisaties.
- KIK-V datastation
  - Leveranciers van een KIK-V datastation moeten bepalen of zij de dienstverlening aan zorgaanbieders zelf uitbreiden met een functionaliteit voor EBW (inclusief bijbehorende standaarden voor gegevensuitwisseling) of de inzet daarvoor door derde partijen laten ondersteunen.
  - Net als voor informatievragende partijen kan het ook voor zorgaanbieders van meerwaarde zijn om zowel een EBW als EDI wallets te implementeren. Voor een aantal uitwisselprofielen is het namelijk relevant om te weten of de antwoorden zijn verstuurd door een daartoe bevoegd persoon. Denk hierbij bijvoorbeeld aan een bestuurlijke bevestiging van de Jaarverantwoording Zorg. Momenteel wordt dit opgelost door een ‘zelfverklaring’ en is het dus niet controleerbaar.
- Nuts
  - De Nuts specificaties kunnen de toepassing van de EBW faciliteren als functionaliteit aanvullend op de bestaande Nuts nodes (zie *Figuur 1*), met name voor het opslaan van identificerende gegevens, vertegenwoordigingsrelaties en de gevalideerde vraag credential die de KIK-V beheerorganisatie verstrekt.
  - Voor het implementeren van beveiligde communicatie, een QERDS uitwisseling, moet een QERDS-laag bovenop NUTS-communicatie worden geïmplementeerd of gekoppeld worden aan een EU-gecertificeerde QERDS-provider.
- Afsprakenset
  - Benodigde wijzigingen van de KIK-V afsprakenset zijn afhankelijk van de architectuurkeuzes die gemaakt moeten worden om te voldoen aan de

verplichtingen uit de verordeningen en eventuele vrijwillige implementaties van de EBW en EDI wallets.

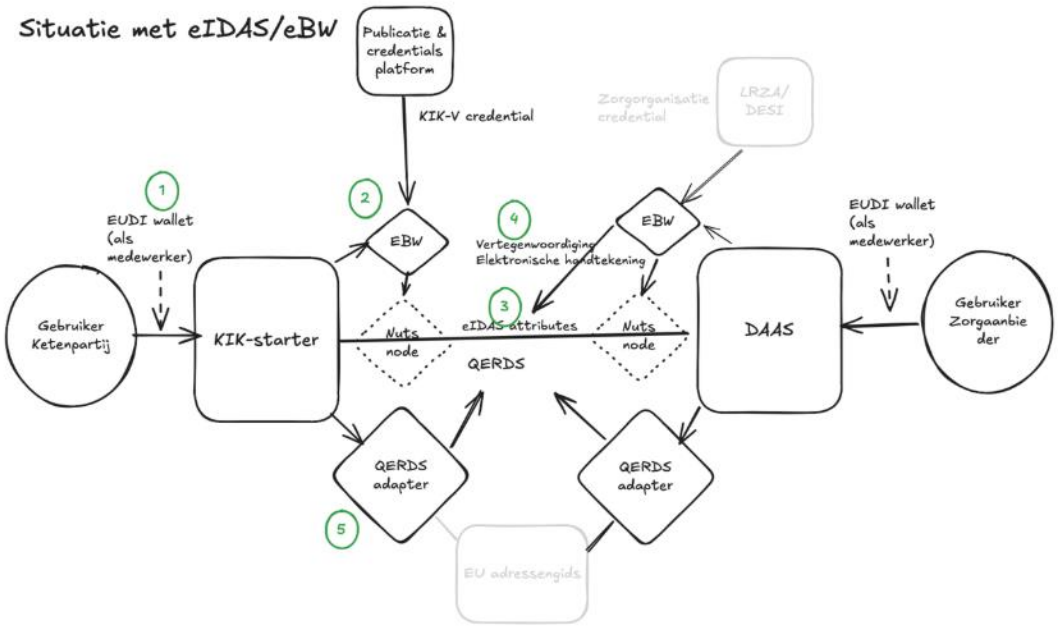
4.3 Voorbeeldbeproeving

Om de impact van de eIDAS 2.0 en EBW-verordening in de praktijk te concretiseren is een verkennende voorbeeldbeproeving uitgevoerd voor KIK-V. Dit heeft als doel om de inzichtelijk te maken hoe verschillende vertrouwensdiensten uit beide verordeningen een mogelijke plek kunnen krijgen binnen het proces van de KIK-V gegevensuitwisseling.

De eIDAS 2.0 en EBW-verordening vragen binnen KIK-V niet direct om een nieuwe architectuur/infrastructuur, maar om een **logische uitbreiding**. Het ontwerp van de voorbeeldbeproeving binnen KIK-V is dus geen vervanging van het huidige proces, maar voegt een extra vertrouwenslaag toe. Het huidige proces voor KIK-V gegevensuitwisseling, met toepassing van de Nuts-specificaties, blijft dus intact.

Figuur 2 toont een vereenvoudigde weergave van de beproeving. Hierin is af te lezen dat niet alle mogelijke functionaliteiten uit de eIDAS 2.0 en EBW-verordening worden meegenomen. Zo worden officiële identificatiegegevens van zorgorganisaties uit bestaande registers nog niet gebruikt, omdat hierover nog geen landelijke afspraken zijn. Ook de Europese adressengids voor business wallets wordt nog niet toegepast. De beproeving gaat wél uit van de volgende nieuwe functies:

1. EDI-wallet voor inloggen door medewerkers namens een organisatie
2. EBW voor organisaties
3. Erkende digitale bedrijfsidentiteit (LPID/EBWOID)
4. Aantoonbare vertegenwoordiging – mandatering vanuit EBW
5. Beveiligde communicatie – toepassing van de *5 kernaspecten van QERDS*



Figuur 2: Ontwerp voorbeeldbeproeving KIK-V

Het ontwerp van de beproeving is nadrukkelijk een voorbeeld. Concrete implementatievereisten zijn nog afhankelijk van de acceptatie van de EBW-verordening en nader te ontwikkelen uitvoeringshandelingen. Binnen het ontwerp van deze voorbeeldbeproeving zijn daarom verschillende aannames gedaan over implementatiemogelijkheden. Zo is er bijvoorbeeld de aanname gedaan dat een EBW digitale bewijzen kan vertrekken aan de EDI-wallet van een

medewerker. Een alternatieve optie is dat de verstrekking van deze digitale bewijzen door een organisatie of onafhankelijk register plaatsvindt.

4.3.1 Lessons learned uit beproeving

Uit de analyse blijkt dat KIK-V conceptueel goed aansluit op de uitgangspunten van de eIDAS 2.0 en EBW-verordening. De beproeving bevestigt dat KIK-V een goede basis biedt waarop kan worden uitgebreid om aan te sluiten op de Europese ontwikkelingen.

Binnen de huidige KIK-V werkwijze is vertrouwen vooral gebaseerd op technische koppelingen, accounts en afspraken met daarbij een belangrijke rol voor de KIK-V beheerorganisatie. Vertegenwoordiging van medewerkers is daarbij vaak impliciet geregeld.

In een situatie mét EDI-wallet en EBW wordt vertrouwen gebaseerd op digitaal verifieerbare bewijzen en elektronische handtekeningen van verantwoordelijke personen. Hierdoor zijn verantwoordelijkheden beter controleerbaar en herleidbaar, en ontstaat minder afhankelijkheid van de beheerorganisatie.

Hiermee laat de beproeving zien dat wallets een belangrijke rol kunnen spelen in system-to-system gegevensuitwisseling.

Hoewel de technische impact op de KIK-V architectuur beperkt lijkt, is er waarschijnlijk wél meer impact voor organisaties en de onderlinge afspraken. Deze impact is alleen nog sterk afhankelijk van eventuele wijzigingen in de EBW-verordening, verdere uitwerking van de uitvoeringshandelingen en invulling vanuit de markt.

5 Conclusies en aanbevelingen

Uit het onderzoek blijkt dat de eIDAS 2.0 en de EBW-verordening samen richtinggevend worden voor de inrichting van betrouwbare digitale gegevensuitwisseling tussen overheden en organisaties binnen Europa. De eIDAS 2.0 introduceert de basiselementen voor een Europese digitale identiteit en vertrouwensdiensten voor gegevensuitwisseling binnen de EU. De EBW-verordening specificeert en breidt deze elementen uit voor de gegevensuitwisseling en interacties tussen overheden en organisaties.

Voor de zorgsector betekent dit dat gegevensuitwisseling steeds meer plaatsvindt binnen een Europees digitaal vertrouwensraamwerk. Hierin worden identiteit, bevoegdheden, authenticatie en veilige communicatie op gestandaardiseerde wijze ingericht. De combinatie van de eIDAS 2.0, EBW-verordening en de EHDS versterkt deze beweging richting een geïntegreerd Europees datastelsel.

De belangrijkste conclusie uit dit onderzoek is dat de impact van eIDAS 2.0 op de huidige KIK-V werkwijze beperkt en vooral indirect is. De EBW-verordening heeft daarentegen potentieel grote impact. Een deel van de gegevensuitwisseling binnen KIK-V bestaat namelijk uit verplichte informatie-uitvragen vanuit publieke instanties waarbij administratieve en rapportage-informatie opgevraagd worden bij zorgaanbieders. Daarmee valt een substantieel deel van de KIK-V gegevensuitwisseling naar verwachting binnen de reikwijdte van de EBW-verordening.

Tegelijkertijd laat het onderzoek zien dat de huidige KIK-V werkwijze in de kern goed aansluit op de uitgangspunten van de Europese ontwikkelingen. Binnen KIK-V wordt al gewerkt met gestandaardiseerde gegevensuitwisseling, bronregistratie, verifiable credentials en een vertrouwensraamwerk via Nuts. De bestaande architectuur biedt daarmee een solide basis voor verdere aansluiting op Europese standaarden.

Wel zijn aanpassingen nodig om toekomstbestendig aan te sluiten op de Europese ontwikkelingen. Hierbij gaat het onder andere om:

- De acceptatie van een EBW bij de gegevensaanlevering;
- De aansluiting op Europese identificatie- en adresseringsmechanismen;
- De ondersteuning van mandatering en vertegenwoordiging;
- De toepassing van gekwalificeerde vertrouwensdiensten, zoals digitale zegels en QERDS, en
- Het explicieter organiseren van governance, toezicht en vertrouwen binnen de gegevensuitwisseling.

De beproeving bevestigt dat de technische impact op de bestaande KIK-V architectuur relatief beperkt kan blijven, mits gekozen wordt voor een modulaire uitbreiding van de bestaande infrastructuur met een aanvullende vertrouwenslaag. De grootste impact ligt niet primair op techniek, maar op governance, afsprakenstelsels, toezicht, rollen en verantwoordelijkheden binnen de keten. Deze impact is alleen nog sterk afhankelijk van eventuele wijzigingen in de EBW-verordening, verdere uitwerking van de uitvoeringshandelingen en invulling vanuit de markt.

Daarnaast bevestigt het onderzoek dat de Europese ontwikkelingen niet alleen verplichtingen met zich meebrengen, maar ook kansen bieden. Door aan te sluiten op Europese standaarden kan KIK-V profiteren van bestaande Europese vertrouwensdiensten en infrastructuren. Hierdoor zijn minder sectorspecifieke voorzieningen nodig. Ook ontstaat meer uniformiteit, interoperabiliteit en herbruikbaarheid van oplossingen, zowel binnen als buiten de zorgsector.

Op basis van het onderzoek wordt Programma KIK-V aanbevolen om de ontwikkelingen rondom de eIDAS 2.0 en EBW-verordening actief te volgen, gerichte beproevingen uit te voeren en de architectuur én governance voor te bereiden op wallet-implementatie.

Colofon

Volgnummer	2026012189
Contactpersoon	Auteur: Ilonka Tersteeg Verantwoordelijke manager: Suzan Orlebeke
E-mail	vragen@zinl.nl
Telefoonnummer	+31 (0)20 797 82 27
Afdeling	Fondsen & Informatiemanagement
Team	Programma KIK-V