INNOPAY
A business of Oliver Wyman

Ministerie van Economische Zaken
en Klimaat

De marktimpact van de eIDAS revisie op vertrouwens-diensten

Maart 2024

innopay.com

Inhoudsopgave

1. Managementsamenvatting

Dit rapport beschrijft de verwachte verandering in het gebruik van vertrouwensdiensten als gevolg van de eIDAS revisie, het effect van een veranderende vraag op de digitale economie en de investerings- en regeldrukkosten die ermee gemoeid zijn. De hoofdvraag luidt: Wat is de economische impact binnen Nederland, zowel op korte als lange termijn, van de voorgenomen aanpassingen in de eIDAS verordening op de verschillende vertrouwensdiensten? Dit rapport is opgesteld door INNOPAY in opdracht van het Ministerie van Economische Zaken en Klimaat op basis van deskresearch & interviews.

eIDAS definieert vertrouwensdiensten als elektronische diensten die bijdragen aan vertrouwen in een digitale omgeving. eIDAS1 bevat vijf vertrouwensdiensten: 1) elektronische handtekeningen; 2) elektronische zegels; 3) elektronische tijdstempels; 4) diensten voor elektronische aangetekende bezorging & 5) authenticatie van websites. De eIDAS revisie introduceert drie nieuwe vertrouwensdiensten: 1) elektronische attesteringen van attributen; 2) elektronische grootboekdiensten & 3) Elektronische archiefdiensten. Hiernaast is ook het beheer van middelen voor het zetten van elektronische handtekeningen en elektronische zegels op afstand een nieuwe dienst.

Gebruik van vertrouwensdiensten

Op basis van de gesprekken met verleners van vertrouwensdiensten is de veronderstelling dat het gebruik van gekwalificeerde elektronische handtekeningen en elektronische attesteringen van attributen toenemen in Nederland door de introductie van de European Digital Identity Wallet (EDIW). Het gebruik van de EDIW in Nederland is een belangrijke voorwaarde voor het volledig benutten van het marktpotentieel van elektronische handtekeningen en elektronische attesteringen van attributen. Voor het gebruik van (gekwalificeerde) attesteringen van attributen zijn duidelijkheid over de rol en verwachting van authentieke bronnen, gezamenlijke standaarden en (semantische) interoperabiliteit cruciaal.

Het gebruik voor gekwalificeerde elektronische zegels en gekwalificeerde authenticatie van websites zal naar verwachting toenemen. Het gebruik van deze diensten hangt deels af van de mogelijkheid om deze in combinatie met de EDIW in te zetten. De toename is onderdeel van een grotere trend, waarin diverse Europese wetgevingen het gebruik van deze diensten verplicht (zullen) stellen voor gegevensuitwisseling en door de toename van schaalbare data-uitwisseling in bepaalde sectoren.

Voor diensten voor gekwalificeerde elektronische archiefdiensten en gekwalificeerde elektronische grootboeken is de toename van het gebruik nog onzeker. Het gebruik van gekwalificeerde elektronische tijdstempels zal naar alle waarschijnlijk niet toenemen in Nederland door de eIDAS revisie.

Regeldruk & investeringskosten

De eIDAS revisie stelt verschillende extra eisen aan vertrouwensdienstverleners waardoor de regeldruk en als gevolg hiervan de met regeldruk samenhangende kosten stijgen. Deze toegenomen druk en kosten hebben meer invloed op kleinere partijen en nieuwkomers op de Nederlandse markt. De verwachting is dat, in de huidige situatie, een toename van de vraag niet direct zal leiden tot extra disproportionele kosten of grote noodzakelijke investeringen bij vertrouwensdienstverleners. Daarnaast is de stijging van kosten in de meeste gevallen gerelateerd aan de toegenomen omzet, waardoor de impact vanzelfsprekend kleiner is.

Concurrentie & verdienmodellen

De verwachting is dat de eIDAS revisie een extra bijdrage levert aan het ontstaan van een open Europese markt voor vertrouwensdiensten, maar deze kan ook leiden tot markconcentratie van een aantal grotere dienstverleners door schaalvoordelen. Voor een gelijk speelveld is geharmoniseerd toezicht van belang. Voor elektronische handtekeningen ontstaan nieuwe verdienmodellen door de eIDAS revisie, namelijk de uitgifte van handtekeningcertificaten, gratis voor burgers, via de EDIW.

Aanbevelingen

Het Ministerie van Economische Zaken en Klimaat speelt een belangrijke rol voor de interne markt van vertrouwensdiensten en bij het volledig benutten van de kansen die de eIDAS revisie biedt voor Nederland en haar digitale economie. Vertrouwensdiensten leveren een belangrijke bijdrage, maar voor

het succes is actief beleid en een actieve rol van het Ministerie van Economische Zaken en Klimaat gewenst. De volgende aanbevelingen zijn voorgelegd:

1. Formuleer meer beleid over vertrouwensdiensten en biedt de markt meer richting en visie
2. Draag actief bij aan het invullen van randvoorwaarden voor succes EDIW
3. Investeer in betere communicatie over vertrouwensdiensten

2. Inleiding

2.1. Introductie

Dit rapport beschrijft de resultaten van het onderzoek in opdracht van het Ministerie van Economische Zaken en Klimaat naar de markimpact van de eIDAS revisie op vertrouwensdiensten, uitgevoerd door INNOPAY. Het onderzoek gaat in op de gevolgen voor de markt (en het gebruik) van de verschillende vertrouwensdiensten, het effect op de digitale economie, de impact van de wetgeving op de kosten voor vertrouwensdienstverleners en de ontwikkelingen rondom verdienmodellen en concurrentie binnen deze markt.

2.2. Aanleiding

De huidige eIDAS verordening (EU 910/240), is vastgesteld op 23 juli 2014. Een gereviseerde tekst van die verordening, in combinatie met een impactanalyse, is door de Europese Commissie gepubliceerd op 3 juni 2021[1]. De ministeries van *Binnenlandse Zaken en Koninkrijksrelaties* (BZK) en *Economische Zaken en Klimaat* (EZK) zijn binnen Nederland beleidsverantwoordelijk voor eIDAS. De ministeriële verantwoordelijkheid voor vertrouwensdiensten wordt voorbereid door de Directie Digitale Economie (onderdeel van het ministerie van EZK). De directie werkt vanuit de Strategie Digitale Economie. Deze strategie is aangeboden door de Minister van Economische Zaken en Klimaat aan de tweede kamer op 18 november 2022[2].

Deze strategie heeft als doel een weerbare, ondernemende, vernieuwende en duurzame digitale economie, die toegankelijk is voor iedereen in Nederland. De eIDAS verordening is hierbij opgenomen als element voor het “creëren van de juiste randvoorwaarden voor goedwerkende digitale markten en diensten”.

Na de publicatie van de nieuwe revisietekst van de eIDAS verordening is het traject van de onderhandelingen tussen de lidstaten gestart. Het Nederlandse kabinet Rutte III heeft als onderdeel daarvan op 9 juli 2021 een fiche gepubliceerd met daarin de appreciatie en standpunten ten aanzien van de verordening[3]. Het kabinet heeft zich positief uitgesproken over het initiatief van de Europese Commissie en steunt de ambitie om de digitale interne markt te versterken met dit voorstel voor elektronische identiteiten en elektronische vertrouwensdiensten. Op 29 februari nam het Europees parlement het voorlopig akkoord van de eIDAS verordening aan[4][5].

De revisie van de verordening introduceert drie nieuwe vertrouwensdiensten: de uitgifte van elektronische attesteringen van attributen aan de *European Digital Identity Wallet* (EDIW), het aanbieden van elektronische grootboekdiensten en het aanbieden van elektronische archiefdiensten. Daarnaast zijn er kleine wijzigingen ten aanzien van de huidige vertrouwensdiensten of het toezicht daarop. De verwachting is dat met name de introductie van de nieuwe vertrouwensdiensten grote veranderingen zullen geven in het ecosysteem rond vertrouwensdiensten, vanwege het verband met de Europese Digitale Identiteit Wallet.

2.3. Doelstelling

Het overkoepelende doel van dit onderzoek is het leveren van een analyse ten aanzien van de veranderingen als gevolg van de eIDAS revisie op de markt van vertrouwensdiensten. Het Ministerie van EZK heeft behoefte aan die analyse, zodat het met de opgedane inzichten rekening kan houden bij nationale wetgeving, het opstellen van beleid en de communicatie naar stakeholders. Als onderdeel van het overkoepelende doel, tracht dit onderzoek kennis te vergaren over de economische impact, zowel op korte als op de lange termijn, voor de vertrouwensdiensten door de revisie van eIDAS. De economische impact wordt beschouwd door de kosten van extra regeldruk, de investeringskosten, de gevolgen van concurrentie en mogelijke businessmodellen in kaart te brengen voor de markt van vertrouwensdiensten. Tot slot, heeft dit onderzoek tot doel een kwalitatieve beschrijving te leveren ten

[1] EUR-Lex
[2] Rijksoverheid
[3] De gepubliceerde fiche
[4] Europees Parlement
[5] eIDAS revisie februari 2024

aanzien van het belang van vertrouwensdiensten in de (digitale) economie. De hoofdvraag van dit onderzoek is geformuleerd als:

> Wat is de economische impact binnen de EU, zowel op korte als lange termijn, van de voorgenomen aanpassingen in de eIDAS verordening op de verschillende vertrouwensdiensten?

Het onderzoek richt zich naast de hoofdvraag op zeven deelvragen:

1	Hoe ziet het verwachte gebruik van vertrouwensdiensten er uit zowel voor burgers als bedrijven?
2	Wat is het effect van een veranderende vraag naar vertrouwensdiensten op de digitale economie?
3	Wat is de invloed op de markt voor vertrouwensdiensten? Wakkert de eIDAS revisie de vraag naar vertrouwensdiensten aan? Welke interesse in de nieuwe vertrouwensdiensten is er te verwachten bij marktpartijen?
4	Welke investeringskosten moeten gemaakt worden door vertrouwensdienstverleners om potentie van (mogelijk) toegenomen vraag te realiseren?
5	Wat zijn de regeldrukkosten (volgens de methode die het Rijk gebruikt) voor de vertrouwensdienstverleners om compliant te zijn?
6	Welke gevolgen voor concurrentie op de markt voor vertrouwensdiensten kan worden verwacht?
7	Welke businessmodellen zijn voor de nieuwe vertrouwensdiensten op basis van de gereviseerde tekst van de verordening toegestaan en bieden een duurzaam toekomstperspectief?

2.4. Aanpak

Het onderzoek bestaat uit vier iteraties. De eerste iteratie richtte zich hoofdzakelijk op deskresearch en het opstellen van hypotheses per deelvraag. In de tweede iteratie zijn de hypotheses en opgestelde analyse getoetst. Daarnaast zijn in deze iteratie de eerste inhoudelijke resultaten uitgewerkt. De derde iteratie betrof een gedetailleerde uitwerking van de resultaten en verduidelijking van de resultaten op basis van validatie uit de laatste interviews. De laatste iteratie betrof het opleveren van het conceptrapport aan de begeleidingscommissie op 20 februari 2024 en na de laatste terugkoppeling is het eindrapport 19 maart 2024 opgeleverd aan de opdrachtgever.

De analyse bestaat uit drie onderdelen: effectenanalyse (deelvraag 1-3), kostenanalyse (deelvraag 4 en 5) en een concurrentie- en businessanalyse (deelvraag 6 en 7). Informatie is vergaard op basis van deskresearch en 19 interviews met verschillende vertrouwensdienstverleners & andere relevante marktpartijen.

De voortgang en resultaten van dit onderzoek zijn door een begeleidingscommissie bestaande uit vertegenwoordigers van het Ministerie van EZK, het Ministerie van BZK en de Rijksinspectie Digitale Infrastructuur gevalideerd.

2.5. Leeswijzer

Hieronder volgt per hoofdstuk een korte uitleg:

Hoofdstuk 3 Conclusies & aanbevelingen
Hoofdstuk 3 bevat de conclusies en aanbevelingen van dit onderzoek.

Hoofdstuk 4 Context
Hoofdstuk 4 schets de context van dit onderzoek door toelichting te geven over de eIDAS wetgeving. Daarnaast biedt dit hoofdstuk een omschrijving van de verschillende vertrouwensdiensten en relevante use cases.

Hoofdstuk 5 Effectenanalyse

Hoofdstuk 5 zet de effecten van de eIDAS revisie op de vertrouwensdiensten uiteen. Hierin wordt per dienst de impact van de nieuwe wetgeving in kaart gebracht en iedere dienst voorzien van een prognose over de marktontwikkeling.

Hoofdstuk 6 Kostenanalyse
Hoofdstuk 6 bevat de impact van de eIDAS revisie op kosten voor verleners van vertrouwensdiensten. Hierbij is onderscheid gemaakt tussen regeldrukkosten en marktadaptatiekosten.

Hoofdstuk 7 Verdienmodellen & Concurrentieanalyse
Het zevende hoofdstuk richt zich op de gevolgen van de eIDAS revisie op de verdienmodellen voor de verschillende vertrouwensdiensten en de concurrentie ontwikkelingen binnen de verschillende vertrouwensdienstmarkten.

2.6. Dankwoord

Dit rapport is mede tot stand gekomen door de expertise en hulp van vertrouwensdienstleverleners en de begeleidingscommissie. Wij willen onze dankbaarheid uiten aan alle betrokkenen voor hun waardevolle inzichten en ondersteuning.

Opdrachtgever & begeleidingscommissie

Ministerie van Economische Zaken en Klimaat

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Rijksinspectie Digitale Infrastructuur

Deelnemers aan het onderzoek

Aangetekend B.V.
BSI Group
Cleverbase ID B.V./Vidua
Dienst Uitvoering Onderwijs
Digidentity B.V.
Entrust EU SL
European Blockchain Services Infrastructure
Intesi Group S.p.A.
Kamer van Koophandel
KPN B.V.
Namirial S.p.A.
NotarisID
Open Preservation Foundation / Nationaal Archief
QuoVadis Trustlink BV (DigiCert+QuoVadis)
Signicat AS
SURF
The Bundesdruckerei Group
The Sovrin Foundation
Zivver

3. Conclusies & aanbevelingen

De revisie van eIDAS heeft impact op de markt voor vertrouwensdiensten. Uit ons onderzoek blijken de volgende vier kernconclusies:

Gebruik van (gekwalificeerde) vertrouwensdiensten neemt toe: Het gebruik van de meeste vertrouwensdiensten in Nederland zal naar verwachting stijgen. De trend is dat de Nederlandse markt beweegt van niet-gekwalificeerde naar gekwalificeerde diensten.

De eIDAS revisie leidt waarschijnlijk tot hogere kosten als gevolg van toenemende regeldruk: De eIDAS revisie stelt extra eisen aan QTSP's waardoor de regeldruk en als gevolg hiervan de met regeldruk samenhangende kosten stijgen.

Concurrentie in Europa neemt toe: Er ontstaat steeds meer concurrentie in Europa, mede doordat dienstverleners uit andere lidstaten zich steeds meer zullen mengen op de Nederlandse markt. Nederlandse partijen hebben hierdoor ook meer kans op buitenlandse markten.

Er ontstaan voldoende duurzame verdienmodellen: Naast verdienmodellen voor nieuwe vertrouwensdiensten ontstaat een nieuw verdienmodel voor gekwalificeerde handtekeningen. De nieuwe en bestaande verdienmodellen komen mogelijk wel onder druk te staan door hogere regeldrukkosten.

3.1. Gebruik van (gekwalificeerde) vertrouwensdiensten neemt toe

Het gebruik van de meeste vertrouwensdiensten in Nederland zal naar verwachting stijgen. De trend is dat de Nederlandse markt beweegt van niet-gekwalificeerde diensten naar gekwalificeerde diensten. Dit wordt gedreven door striktere wet- en regelgeving of eisen van betrokken partijen. Hiernaast moet benoemd worden dat de uitvoeringshandelingen nog niet gepubliceerd zijn. Omdat de uitvoeringshandelingen invloed hebben op de vertrouwensdiensten is de impact op alle vertrouwensdiensten op dit moment nog niet exact te bepalen.

3.1.1. Elektronische handtekeningen

De markt voor Qualified Electronic Signatures (QES) in Nederland is op dit moment klein. Met de eIDAS revisie kan iedere burger over een gratis certificaat voor gekwalificeerde handtekeningen in de wallet (EDIW) beschikken. Hierdoor is er een enorme potentiële groei van gekwalificeerde elektronische handtekeningen (op afstand) en wordt het gebruik hiervan waarschijnlijk de norm. In de toekomst zullen veel geavanceerde elektronische handtekeningen op afstand overgaan naar QES op afstand door de introductie van de EDIW. Het gebruik van de EDIW in Nederland is een belangrijke voorwaarde voor het volledig benutten van het marktpotentieel van gekwalificeerde elektronische handtekeningen (op afstand).

3.1.2. Elektronische zegels en authenticatie voor websites

Voor QESeal's en QWAC's is de prognose dat het gebruik in Nederland ook toeneemt. Het gebruik van deze diensten hangt deels af van de mogelijkheid dat ze in combinatie met de EDIW worden ingezet, namelijk via EDIW-bevragingen en in de verzegeling van (Q)EAA's. Dit is onderdeel van een grotere trend, waarin diverse Europese wetgevingen het gebruik van deze diensten verplicht (zullen) stellen voor gegevensuitwisseling, zoals de Payment Services Directive 2/3 (PSD2/PSD3), de Payment Services Regulation (PSR) en het framework for financial data access (FIDA)[6], en door de groei van schaalbare data-uitwisseling in bepaalde sectoren.
Daarbij wordt verwacht dat de toepassing van WAC's verder zal toenemen. Deze trend staat los van de revisie van eIDAS en heeft vooral te maken met de uitbreidende bruikbaarheid van deze certificaten. Ze worden niet langer alleen voor websites gebruikt, maar vinden ook hun weg naar andere toepassingen, zoals IoT-apparaten en e-mails.

3.1.3. Elektronische tijdstempels

Het huidige gebruik in Nederland voor QTimestamps als separate dienst is beperkt en de verwachting is dat deze dienst niet veel zal toenemen. De eIDAS revisie geeft weinig aanleiding voor een toename in het gebruik – de eisen zijn nagenoeg identiek aan de eisen voor deze dienst uit eIDAS1. Pas wanneer in nationale wetgeving QTimestamps worden verplicht voor bepaalde use cases, zal het gebruik stijgen.

[6] European Commission

3.1.4. Diensten voor elektronische aangetekende bezorging

Er is naar verwachting geen direct effect op het gebruik van QERDS in Nederland door de eIDAS revisie. Een belangrijke aanjager voor QERDS is verplichtstelling in lokale wetgeving of het opnemen van de dienst op de lokale 'Pas toe of leg uit-lijst'. Op dit moment gebeurt dit in Nederland niet/nauwelijks. Het gebruik van ERDS zal waarschijnlijk toenemen. Deze trend staat los van de revisie van eIDAS en wordt voornamelijk gedreven door het toenemende besef in diverse industrieën van het belang en de noodzaak van veilige bedrijfscommunicatie.

3.1.5. Elektronische attesteringen van attributen

Deelnemers aan dit onderzoek voorspellen een omvangrijke Europese markt voor (gekwalificeerde) elektronische attesteringen van attributen of (Q)EAA's als gevolg van de introductie van de EDIW. Het verwachte gebruik is gebaseerd op de vele online en offline use cases die mogelijk worden met behulp van (Q)EAA's en de EDIW. Het gebruik van de EDIW in Nederland is een belangrijke voorwaarde voor het volledig benutten van het marktpotentieel van elektronische attesteringen van attributen. Voor het gebruik van (Q)EAA's zijn duidelijkheid over de rol en verwachting van authentieke bronnen, gezamenlijke standaarden en (semantische) interoperabiliteit cruciaal.

3.1.6. Elektronische archiefdiensten

Er is een kleine kans dat (Q)E-Archiving als enkele dienst veel gebruikt gaat worden. Een deel van de geïnterviewden acht het waarschijnlijker dat (Q)E-Archiving vooral in combinatie met andere vertrouwensdiensten ingezet zal worden (bijv. samen met QES diensten). Doordat de toegevoegde waarde voor organisaties beperkt blijft, leeft het idee dat deze gekwalificeerde dienst een beperkte ontwikkeling zal doormaken.

3.1.7. Elektronische grootboeken

De verwachting is dat, op de korte termijn, het gebruik van QELedger in Nederland laag is en dat er een zeer gering aantal aanbieders zal zijn. De onduidelijkheid voor mogelijke aanbieders, zowel qua technische invulling als juridische kaders, van deze dienst remt de opkomst van een nieuwe markt voor deze vertrouwensdienst. Voor aanbieders van QELedgers kan het verkrijgen van de gekwalificeerde status vertrouwen verhogen in de markt, wat in deze sector wenselijk kan zijn.

3.2. De eIDAS revisie leidt waarschijnlijk tot hogere kosten als gevolg van toenemende regeldruk

De eIDAS revisie stelt verschillende extra eisen aan QTSP's waardoor de regeldruk en als gevolg hiervan de met regeldruk samenhangende kosten stijgen. Voor kleine partijen heeft dit waarschijnlijk meer impact dan voor grote partijen. Hiernaast kunnen bestaande QTSP's makkelijker de nieuwe diensten gaan aanbieden dan nieuwe toetreders. De regeldruk stijgt verder door de verplichting om dienstverlening beschikbaar en toegankelijk te maken voor mensen met beperkingen. Echter geven QTSP's zelf aan dat zij hier geen hoge extra kosten van verwachten. Ook moeten QTSP's voldoen aan additionele eisen van andere normen en standaarden (bijv. NIS2, CA/Browser Forum) voor specifieke vertrouwensdiensten. Specifiek voor elektronische handtekeningen op afstand leidt de verplichte SAM-certificering tot extra kosten voor dienstverleners.

Er is een risico op vertragingen in de kwalificatieprocedure waardoor dienstverleners niet op tijd gecertificeerd kunnen worden. Dit komt onder andere door het beperkte aantal auditors en krapte op de arbeidsmarkt, in combinatie met de gelijktijdigheid van het inwerking treden van de eIDAS revisie, de uitvoeringshandelingen en de accreditatie van auditors. De vertragingen kunnen leiden tot hogere kosten omdat ze de implementatie en operationele processen verlengen.

De eIDAS revisie schrijft voor dat de identiteit van degene aan wie de gekwalificeerde vertrouwensdienst (voor QEAA's, QWAC's, QES, en QESeals) geleverd wordt en hun attributen moeten geverifieerd worden met LoA hoog. QTSP's die momenteel niet aan deze eis voldoen, zullen inspanningen en kosten moeten maken om hieraan te voldoen. Op termijn (als er voldoende gebruikers zijn) biedt de EDIW de mogelijkheid om de identificatie op afstand te ondersteunen, wat kan leiden tot een verlaging van de met identificatie kosten van QTSP's.

De verwachting is dat marktadaptatiekosten weinig invloed hebben op marktpartijen. Onder de huidige situatie zal een toename van de vraag niet direct leiden tot extra disproportionele kosten of grote noodzakelijke investeringen. Het merendeel van de diensten is schaalbaar ingericht en zal een normale vraagstijging goed aankunnen. Daarnaast is de stijging van kosten gerelateerd aan een stijging in omzet.

3.3. Concurrentie in Europa neemt toe

De eIDAS revisie geeft verdere erkenning van een sterker juridisch kader aan de markt voor vertrouwensdiensten. De verwachting is dat de eIDAS revisie zorgt voor een meer open Europese markt voor vertrouwensdiensten. Er ontstaat steeds meer concurrentie op de markt, mede doordat dienstverleners uit Europa zich steeds meer zullen mengen op de Nederlandse markt. Nederlandse partijen krijgen hierdoor ook meer kans op buitenlandse markten.

De markt voor vertrouwensdiensten is een (sterk) compliance- en kosten gedreven markt waarbij diversificatie in product en dus onderscheidend vermogen beperkt is. Daarbij beperkt de EDIW een deel van het onderscheidend vermogen voor bijvoorbeeld elektronische handtekeningen. Beide werken concentratie van de markt in de hand. Grotere dienstverleners zijn in het voordeel, omdat zij eenvoudiger de (hoge) compliance kosten kunnen dragen en daarnaast door schaalvoordelen een meer competitieve prijs kunnen aanbieden. Ook verschillen de arbeidskosten per land. Deze factoren hebben het huidige Europese speelveld al vormgegeven en geresulteerd in een concurrentievoordeel voor een aantal grotere vertrouwensdienstverleners.

Specifiek voor gekwalificeerde elektronische handtekeningen ontstaat een andere marktdynamiek doordat het voor de hand ligt dat de overheid een aanbestedingsprocedure uitvoert en één of meerdere dienstverleners selecteert die gekwalificeerde elektronische handtekeningen leveren in de EDIW.

Voor een gelijk speelveld is het wel van belang dat toezicht is geharmoniseerd tussen verschillende nationale toezichthouders. De geïnterviewde partijen uitten een sterke behoefte aan zo min mogelijk ambiguïteit of interpretatieverschillen. Hiernaast geven geïnterviewde partijen aan dat de harmonisatie ook belangrijk is binnen een lidstaat. Als eIDAS toezicht en NIS2 toezicht bij verschillende toezichthouders ligt dan stijgen de kosten voor QTSP's. In Nederland is het daarom wenselijk dat de RDI ook de rol van toezichthouder op zich neemt voor NIS2 toezicht.

3.4. Er ontstaan voldoende duurzame verdienmodellen

Voor (Q)Timestamps en (Q)ERDS zijn er geen noemenswaardige specifieke gevolgen voor de verdienmodellen door de eIDAS revisie. Voor (Q)ESeals en (Q)WAC's kunnen er nieuwe omzetstromen ontstaan rondom de EDIW, waardoor bestaande verdienmodellen meer duurzaam worden. De verdienmodellen komen mogelijk wel onder druk te staan door hogere regeldrukkosten.

Voor elektronische handtekeningen ontstaan nieuwe verdienmodellen door de eIDAS revisie. Het huidige verdienmodel voor het proces van het zetten van geavanceerde handtekening (voor burgers) zal grotendeels vervallen. Daarvoor ontstaat het nieuwe verdienmodel voor de uitgifte van certificaten voor elektronische handtekeningen aan de EDIW voor burgers. Waarschijnlijk is een aanbesteding voor deze certificaten voor niet-professioneel gebruik vanuit de overheid nodig. Een neveneffect is dat burgers vertrouwder raken met het zetten van elektronische handtekeningen wat naar verwachting ook het gebruik van elektronische handtekeningen voor professioneel gebruik zal stimuleren waarvoor andere verdienmodellen bestaan, bijvoorbeeld een betaling per transactie, een eenmalige gekwalificeerde handtekening of een abonnementsvorm.

Voor elektronische attesteringen van attributen zijn er twee typen verdienmodellen: 1) verdienmodellen voor vertrouwensdienstverleners en 2) kosten/verdienmodellen voor authentieke bronnen. Voor vertrouwensdienstverleners ligt een maandelijkse/jaarlijkse prijs die authentieke bronnen betalen voor het gebruik van de vertrouwensdienst het meest voor de hand. Een alternatief verdienmodel is een gedeelde inkomstenstructuur voor de vertrouwensdienstverlener en de authentieke bron. Een derde alternatief is een afspraak tussen een vertrouwensdienstverlener en authentieke bron over het recht van het ontsluiten van de data van de authentieke bron. Voor authentieke bronnen zijn er drie kosten-/verdienmodellen: 1) De holder/burger betaalt; 2) De relying party betaalt en 3) De authentieke bron betaalt. Het meest voor de hand liggende model verschilt per attestering en/of use case daarvan.

3.5. Aanbevelingen

Het Ministerie van Economische Zaken en Klimaat speelt een belangrijke rol bij het volledig benutten van de kansen die de eIDAS revisie biedt voor Nederland en haar digitale economie. Vertrouwensdiensten leveren een belangrijke bijdrage, maar voor het succes is actief beleid en een actieve rol van het Ministerie van Economische Zaken en Klimaat gewenst. Dit wordt door Nederlandse vertrouwensdienstverleners ondersteund.

Formuleer meer beleid over vertrouwensdiensten en biedt de markt meer richting en visie

Voor optimaal gebruik van vertrouwensdiensten voor de digitale economie is meer beleid, richting en visie vanuit de rijksoverheid gewenst. In dit beleid zouden oplossingsrichtingen voor een deel van de huidige onduidelijkheden over de eIDAS revisie kunnen worden verkend. Denk hierbij aan onder andere:

- Wijze van uitgifte van certificaten voor gekwalificeerde handtekeningen voor burgers, inclusief afweging van voor- & nadelen
- Hoe er wordt omgegaan met ‘professioneel gebruik’ voor gekwalificeerde elektronische handtekeningen
- Kaders voor uitgifte en (semantische) interoperabiliteit van publieke en private (Q)EAA’s

Hiernaast is de markt op zoek naar verheldering over de uitvoeringshandelingen, informatie over de aansluiting van toezichthouders in Europa om het risico op verschillende lokale interpretaties te verkleinen en tot slot duidelijkheid over de samenhang tussen verschillende wetgeving, standaarden, normen en kaders (b.v. NIS2, eIDAS, Wdo, Wet Diaz, ETSI, ISO, Nen).

Beleid, richting en visie kan vertrouwensdienstverleners en andere stakeholders helpen bij het bepalen van hun strategie voor het aanbieden van vertrouwensdiensten. Daarnaast hebben zij behoefte aan duidelijkheid over de spelregels zodat zij kunnen acteren. Dit geldt ook voor mogelijke authentieke bronnen voor (Q)EAA’s en schema providers. Onzekerheid kan een vertragende werking hebben of zelfs het gebruik belemmeren. Een actieve rol en bijdrage van het Ministerie van EZK aan de invulling van de uitvoeringshandelingen en communicatie hierover kan bijdragen aan de duidelijkheid voor de Nederlandse markt.

Draag actief bij aan het invullen van randvoorwaarden voor succes EDIW

De onderlinge relatie van de EDIW met elektronische handtekeningen, zegels en elektronische attesteringen van attributen is groot. Daarnaast zijn mogelijk QESeals en QWAC’s noodzakelijk voor een goede werking van c.q. de interactie met de EDIW. Dit betekent dat de rol die de overheid heeft richting de EDIW, niet los gezien kan worden van de rol die de overheid heeft voor het goed functioneren van de markt van vertrouwensdiensten. Meer duidelijkheid over de werking van de EDIW zowel voor natuurlijke personen en ODIW voor rechtspersonen, het kosten-/verdienmodel van de EDIW, juridische aansprakelijkheid, normen en standaarden en interoperabiliteit van (Q)EAA’s zijn daarmee voorbeelden van belangrijke randvoorwaarden voor het succes van de EDIW. Een overlegstructuur waarin alle relevante partijen betrokken zijn en gezamenlijk bijdragen aan het invullen van de randvoorwaarden voor het succes van de EDIW helpt de tweezijdigheid van deze markt. Het Ministerie van EZK kan faciliteren bij het bij elkaar brengen van de verschillende relevante stakeholders en om centrale regie te organiseren. Daarnaast is verdere strategische afstemming binnen de overheid, bijvoorbeeld tussen de betrokken ministeries, cruciaal.

Investeer in betere communicatie over vertrouwensdiensten

Op korte termijn draagt de verbetering van communicatie over het nut, de noodzaak en de mogelijke toepassingen van vertrouwensdiensten bij aan het optimaliseren van het gebruik ervan. In Nederland wordt in zowel de publieke als de private sector het belang en de noodzaak van vertrouwensdiensten nog onvoldoende erkend en begrepen. Bij veel stakeholders ontbreekt het aan kennis over het bestaan van deze vertrouwensdiensten. Communicatie over het bestaan en de voordelen van vertrouwensdiensten is om die reden gewenst. Hiervoor kan de overheid bijvoorbeeld het initiatief *Trusted Information Partners* (TIP) benutten.

4. Context

4.1. eIDAS

De *electronic IDentification, Authentication and trust Services* (eIDAS) verordening is de Europese wettelijke verordening over elektronische identificatie en vertrouwensdiensten ten aanzien van elektronische transacties. Het doel van deze verordening is om het digitaal vertrouwen in de interne mark te vergroten en te voorzien van een gemeenschappelijk regelgevingskader. De eIDAS verordening is op 1 juli 2016 onder de officiële naam Regulation (EU) No 910/2014[7] in werking getreden. Nu streeft de Europese Commissie naar revisie van deze verordening via het Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) no910/2014 as regards establishing a framework for a European Digital Identity[8]. Dit onderzoek is gebaseerd op de versie van dat document van 10 november 2023 die gebaseerd is op de uitkomst van de trilogen inzake het voorstel voor de herziening van de eIDAS verordening.

4.1.1. eIDAS

De oorspronkelijke eIDAS verordening bestaat uit twee onderdelen: *elektronische identificatie* (eID) en de *vertrouwensdiensten*, ofwel *Trust Services* (TS).

De eID heeft betrekking op het online identificeren en authentiseren van natuurlijke personen en rechtspersonen. Vóór eIDAS1 kon elke lidstaat al één of meerdere eID's voor haar burgers en bedrijven aanbieden, maar sinds deze verordening is er de mogelijkheid om dergelijke eID's aan te melden voor wederzijdse grensoverstijgende erkenning van inlogmiddelen. Dit betekent dat eID's uit een bepaalde lidstaat, ook (gedeeltelijk) bruikbaar zijn in andere lidstaten. Kortom, eIDAS is een aanzet tot grensoverschrijdend gebruik van eID's.

De Nederlandse eID valt onder de beleidsverantwoordelijkheid van het *Ministerie van Binnenlandse Zaken en Koninkrijksrelaties* (BZK). In Nederland is gekozen voor een[9] publiek inlogmiddel voor burgers (DigiD), en de in publiek-private samenwerking geleverde inlogmiddelen voor ondernemingen en rechtspersonen: eHerkenning-stelsel.

eIDAS bevat vijf vertrouwensdiensten. De eIDAS wettekst definieert vertrouwensdiensten als elektronische diensten die bijdragen aan vertrouwen in een digitale omgeving. In sectie 4 t/m 8 van eIDAS worden de vijf vertrouwensdiensten toegelicht (zie **Figuur 1**). De vertrouwensdiensten behoren tot de beleidsverantwoordelijkheid van *Ministerie van Economische Zaken en Klimaat* (EZK). Het ministerie heeft de *Rijksinspectie Digitale Infrastructuur* (RDI) aangewezen als toezichthouder op de vertrouwensdiensten. Vertrouwensdiensten zijn in Nederland ondergebracht in de telcommunicatiewet[10].

Figuur 1: eIDAS kent vijf vertrouwensdiensten.

[7] eIDAS1
[8] De eIDAS revisie
[9] Na de invoering van het Stelsel Toegang kan een burger of bedrijf, naast DigiD of eHerkenning, gebruik maken van andere erkende inlogmiddelen, indien getoetst aan *Wet digitale overheid* (Wdo) eisen om bij verschillende overheidsdienstverleners in te loggen.
[10] Overheid.nl

4.1.2. De eIDAS revisie

De revisie van eIDAS introduceert drie nieuwe vertrouwensdiensten (zie **Figuur 2**). In secties (afdeling) 9 t/m 11 van de eIDAS revisie worden de nieuwe vertrouwensdiensten toegelicht.

Figuur 2: de eIDAS revisie introduceert drie nieuwe vertrouwensdiensten.

Elektronische attesteringen van attributen

Elektronische archiefdiensten

Elektronische grootboeken

Hiernaast introduceert de eIDAS revisie het concept van de *European Digital Identity Wallet* (EDIW). Een EDIW[11] helpt EU burgers en bedrijven om zichzelf te identificeren of authentiseren, bepaalde informatie te delen en om digitaal te kunnen tekenen. De EDIW valt onder de beleidsverantwoordelijkheid van BZK. De harde scheidslijn tussen beide Nederlandse ministeries wordt minder expliciet omdat bepaalde vertrouwensdiensten (bijv. elektronische handtekeningen en elektronische attesteringen van attributen) ook gebruikt worden in relatie tot EDIW's. In dit rapport is de keuze gemaakt om de in de revisie als nieuwe geïntroduceerde diensten rondom het zetten van handtekeningen en zegels op afstand onder te onder te brengen bij respectievelijk de vertrouwensdiensten 'Elektronische handtekeningen' en 'Elektronische zegels'.

4.2. Type vertrouwensdiensten

De in eIDAS beschreven vertrouwensdiensten zijn te verdelen over acht categorieën die elk weer een aantal (deel)diensten bevatten (zie **Figuur 3**)[12].

Figuur 3: de eIDAS revisie kent 8 vertrouwensdiensten met meerdere deeldiensten.

Vertrouwensdiensten	Deeldiensten
Elektronische handtekeningen	1. Aanmaken van elektronische handtekeningen en/of certificaten 2. Validatie van elektronische handtekeningen en/of certificaten 3. Preserveren van elektronische handtekeningen en/of certificaten 4. Beheer van middelen voor het zetten van elektronische handtekeningen op afstand[13]
Elektronische zegels	1. Aanmaken van elektronische zegels en/of certificaten 2. Validatie van elektronische zegels en/of certificaten 3. Preserveren van elektronische zegels en/of certificaten 4. Beheer van middelen voor het zetten van elektronische zegels op afstand.
Elektronische tijdstempels	1. Aanmaken van tijdstempels 2. Validatie van tijdstempels
Diensten voor elektronische aangetekende bezorging	1. Leveren van elektronische diensten voor aangetekende bezorging 2. Validatie van data verstuurd via elektronische aangetekende bezorging

[11] Elk land kan één of meerdere EDIW's voor burgers en één of meerdere EDIW's voor bedrijven hebben
[12] De 8 vertrouwensdiensten zijn gebaseerd op de acht secties (afdelingen) in de eIDAS wettekst
[13] Het beheer van middelen voor het zetten van elektronische handtekeningen op afstand is een nieuwe dienst onder eIDAS

Authenticatie van websites	1. Aanmaken van certificaten voor websiteauthenticatie 2. Validatie van certificaten voor websiteauthenticatie
Elektronische attesteringen van attributen	1. Uitgeven van elektronische attesteringen van attributen 2. Validatie van elektronische attesteringen van attributen
Elektronische archiefdiensten	1. Elektronische archiveren van data
Elektronische grootboeken	1. Opslaan van data in een elektronisch grootboeken

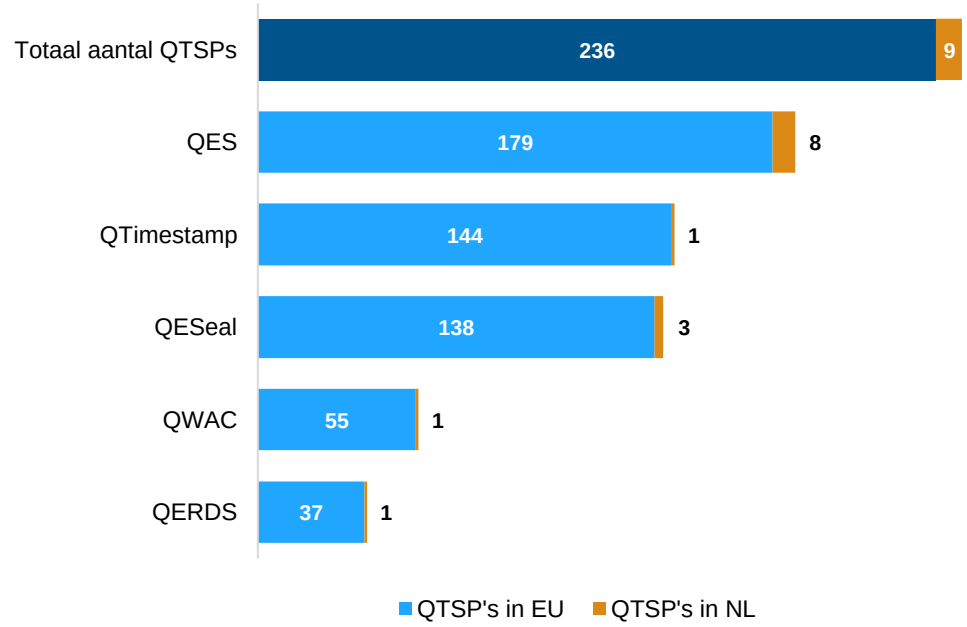
Bestaande eIDAS diensten
Nieuwe eIDAS diensten

Elke dienst kent een gekwalificeerde- en een niet-gekwalificeerde variant. Gekwalificeerde diensten voldoen aan aanvullende eisen die leiden tot een hoger niveau van betrouwbaarheid en rechtsvermoeden. Dit resulteert in een verschuiving van de bewijslast: bij een gekwalificeerde dienst keert de bewijslast om. In het voorbeeld van een gekwalificeerde handtekening dient de ondertekenaar aan te tonen dat hij of zij de handtekening niet heeft gezet. Dit in tegenstelling tot niet-gekwalificeerde handtekeningen, waarbij het de verantwoordelijkheid van de eisende partij is om te bewijzen dat de handtekening daadwerkelijk door de ondertekenaar is gezet.

Vertrouwensdiensten worden aangeboden door partijen die bekend staan als verleners van vertrouwensdiensten, ofwel *Trust Service Providers* (TSP). Wanneer deze partijen succesvol aantonen dat zij voldoen aan de eisen van eIDAS door middel van een evaluatie door een onafhankelijke auditor, kunnen TSP's bij de toezichthouder de status van gekwalificeerde verlener van vertrouwensdiensten aanvragen, oftewel *Qualified Trust Service Provider* (QTSP).

De Europese Commissie publiceert een actuele lijst met de *geregistreerde* QTSP's binnen de Europese Unie voor alle onder eIDAS1 gecategoriseerde vertrouwensdiensten[14]. In Europa zijn er meer dan 230 verleners van vertrouwensdiensten (zie **Figuur 4)**[15]. Deze partijen bieden samen ruim 700 vertrouwensdiensten aan. De meeste verleners bieden dus verschillende vertrouwensdiensten aan.

Figuur 4: Europa kent meer dan 230 verleners van de eIDAS1 vertrouwensdiensten.



Het is belangrijk om te vermelden dat niet-gekwalificeerde TSP's geen registratieplicht hebben. In verschillende landen, zoals Nederland, is er ook geen mogelijkheid voor registratie. Daarnaast is de

[14] Dashboard Europese Commissie
[15] eIDAS Dashboard op 01/11/2023

toegevoegde waarde voor registratie beperkt. Enkele voorbeelden van niet-geregistreerde TSP's zijn partijen zoals Zivver, Rpost, Bitdefender, Cloudflare en Google. In Nederland zijn er op dit moment negen QTSP's actief die veertien gekwalificeerde diensten leveren (zie **Figuur 5**).

Figuur 5: In Nederland is er ten minste 1 QTSP voor elke eIDAS1 vertrouwensdienst.

	QES	QESeals	QTimestamps	QERDS	QWAC's
Aangetekend B.V.				✓	
CIBG	✓				
Vidua / Cleverbase ID B.V.	✓				
Digidentity B.V.	✓	✓			
KPN B.V.	✓	✓			
Ministerie van Defensie	✓				
Ministerie van I&W	✓				
NotarisID B.V.	✓				
QuaVadis Trustlink B.V.	✓	✓	✓		✓

✓ = biedt de gekwalificeerde dienst aan

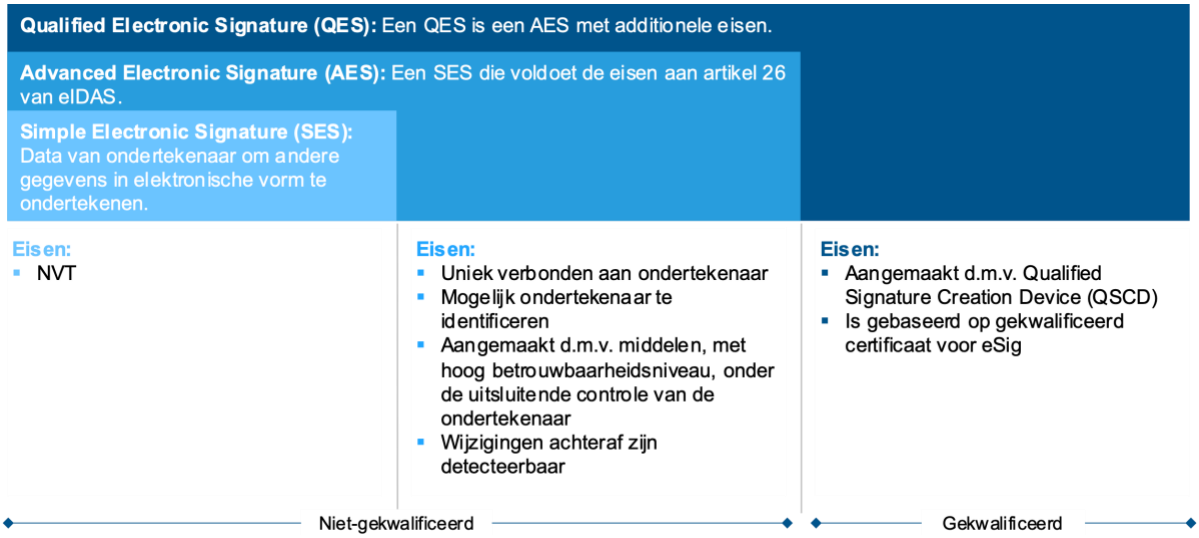
In de volgende paragrafen worden de vijf bestaande en drie nieuwe vertrouwensdiensten nader toegelicht en worden de belangrijkste use cases per dienst weergegeven.

4.2.1. Elektronische handtekeningen

Een *elektronische handtekening* (e-handtekening*)* of *electronic signature (*eSig*),* is een digitale wilsuiting van een persoon die instemt met de inhoud van een document of dataset waaraan de handtekening is gerelateerd[16]. Het is enerzijds de elektronische tegenhanger van de gelegaliseerde handtekening en zodoende een juridische binding die de ondertekenaar verplicht een vastgelegde overeenkomst van het ondertekende document na te komen[17]. Daarnaast kan de eSig gebruikt worden als middel om de authenticiteit en integriteit van een document te onderschrijven. Er zijn drie vormen van de elektronische handtekeningen met een oplopend betrouwbaarheidsniveau, namelijk de *simpel electronic signature* (SES), *advanced electronic signature* (AES) en de *qualified electronic signature* (QES). Dit oplopende betrouwbaarheidsniveau wordt verkregen door steeds additionele eisen aan de handtekening te stellen (zie **Figuur 6**).

[16]Zie Electronic signatures 1-pager
[17] European Commission

Figuur 6: Een QES is een AES met additionele eisen waar de bewijslast bij de ondertekenaar ligt.



Bij QES zijn drie individuele deeldiensten betrokken, namelijk het aanmaken, valideren en preserveren van QES. Hiernaast moet een *Qualified Signature Creation Device* (QSCD) beheerd worden die nodig is voor het aanmaken van QES. Ook bij het aanmaken van QES op afstand moet een QSCD beheerd worden. De QES verwijst naar de digitale ondertekening en het gekwalificeerde certificaat voor de QES is het bindmiddel tussen deze digitale ondertekendata en de identiteit van de ondertekenaar. Het certificaat is zodoende een elektronische attestering die valideringsgegevens voor een elektronische handtekening aan een natuurlijk persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt. Dit certificaat krijgt het label gekwalificeerd wanneer het is afgegeven door een QTSP en voldoet aan de eIDAS eisen uit ANNEX I[18]. **Figuur 7** bevat een overzicht van de belangrijkste use cases voor (Q)ES.

Figuur 7: Twee use cases zijn veel voorkomend bij (Q)ES.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Waarborgen integriteit en oorspronkelijkheid	Het eenzijdig ondertekenen van bestanden door één partij/persoon met als doel de integriteit en oorspronkelijkheid te garanderen.	Ik wil gevoelige digitale informatie voorzien een integriteits- en oorspronkelijkheidgarantie zodat de entiteiten waarmee ik die informatie deel daarop kunnen acteren.	▪ Ondertekenen medische documenten zoals een recept, verwijzing of medische verklaring. ▪ Ondertekenen van (jaar)verslagen of rapporten.
(juridische bindende) overeenkomst sluiten	Het tweezijdig ondertekenen van bestanden door twee partijen.	Ik en een andere partij willen een digitaal contract ondertekenen om onze overeenkomst vast te leggen en deze juridisch af te kaderen.	▪ Ondertekenen notariële akten en volmachten. ▪ Ondertekenen van hypotheken of verzekeringen. ▪ Ondertekenen van een leveringscontract, geheimhoudingsverklaring of arbeidsovereenkomst.

4.2.2. Elektronische zegels

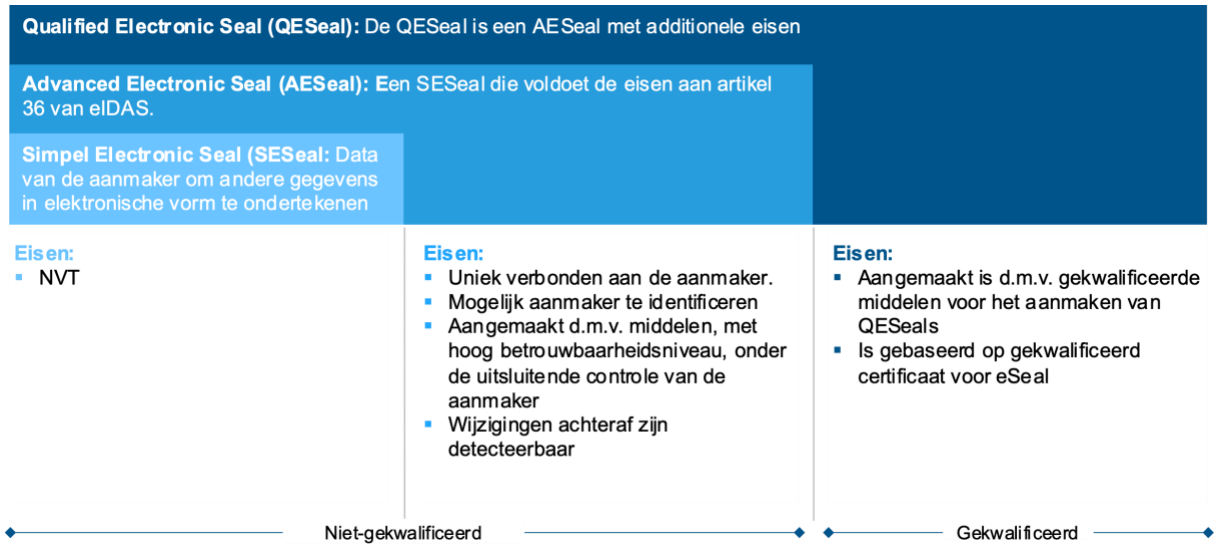
Het *elektronische zegel* (e-zegel) of *electronic seal* (eSeal) is het digitale equivalent van een fysieke bedrijfsstempel en wordt gezet door een rechtspersoon. Dit digitale bewijs hecht zich aan andere digitale data, bijvoorbeeld bedrijfscontracten of -documenten, om de oorspronkelijkheid en integriteit

[18] eIDAS ANNEX1

ervan te garanderen[19]. Op die manier dient de eSeal als bewijs dat dergelijke bestanden zijn uitgegeven door de desbetreffende rechtspersoon.

Net als bij de eSig heeft de eSeal drie vormen met een oplopend vertrouwensniveau: *de simple electronic seal* (SESeal), *advanced electronic seal* (AESeal) en *qualified electronic Seal* (QESeal) (zie **Figuur 8**). Bij het genereren van een QESeal zijn 4 deeldiensten betrokken. Dit zijn de diensten van het aanmaken, de validatie en het preserveren van zowel de QESeal als het certificaat voor de QESeal en hiernaast moet een *Qualified Seal Creation Device* (QsealCD) beheerd worden die nodig is voor het zetten van QESeals op afstand.

Figuur 8: Een eSeal kent drie verschillende oplopende vertrouwensniveaus.



Voor de QESeal is er eveneens sprake van een gekwalificeerd certificaat voor QESeals die, in dit geval, een elektronische attestering is die valideringsgegevens van de QESeal aan een rechtspersoon verbindt en de naam van die rechtspersoon bevestigd. Dit certificaat is *gekwalificeerd* wanneer deze is afgegeven door een QTSP en voldoet aan de eIDAS voorschriften in ANNEX III[20].

(Q)Eseals worden veelal gebruikt bij documenten, gegevens of transacties met grote rechtsgevolgen of risico's. **Figuur 9** bevat een overzicht van de belangrijkste use cases voor (Q)Eseals.

Figuur 9: (Q)Eseals worden voornamelijk gebruikt voor het garanderen van de integriteit van documenten.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Waarmerken	Het waarmerken van bestanden door juridische entiteiten d.m.v. (Q)Eseal met als doel haar integriteit en oorspronkelijkheid te garanderen.	Ik wil contracten digitaal waarmerken, zodat ik geen 'natte' zegel of handtekening meer nodig heb en processen efficiënter kan maken.	▪ Verzegelen van financiële, medische of strafrechtelijke gegevens. ▪ Verzegelen van facturen. ▪ Bedrijfscontracten verzegelen.
Attesteringen opvragen/ aanleveren	Een relying party gebruikt een QESeal bij een EDIW om te bewijzen dat het verzoek gedaan is door de specifieke relying Party.	Ik wil dat later bewijsbaar is dat een relying party mijn data heeft opgevraagd.	▪ Raadplegen van de wallet door een relying party.

[19] Zie (Q)ESeal 1-pager
[20] eIDAS ANNEX III

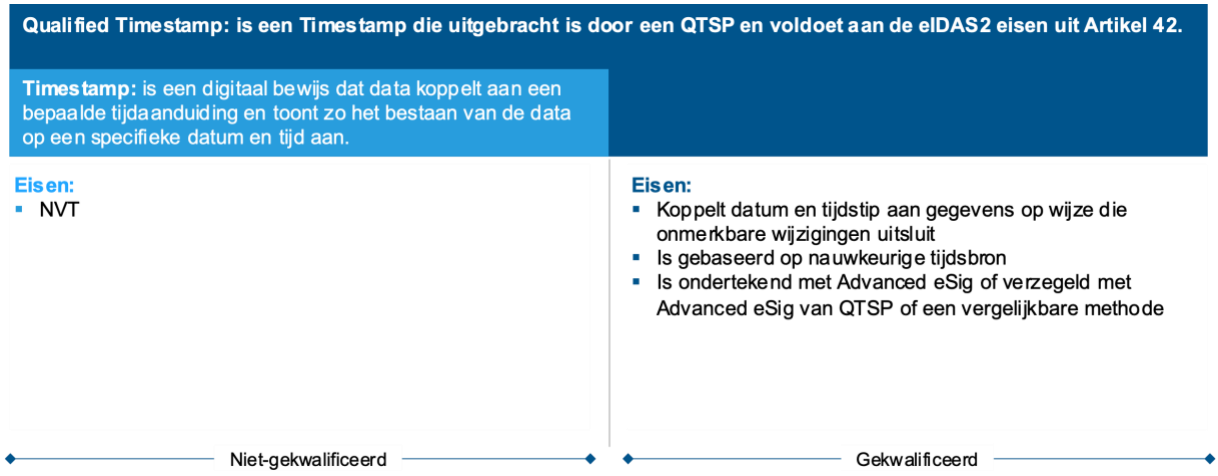
Verzegelen van Machine-2-Machine interactie	Het verzegelen van bestanden door twee partijen.	Ik wil veilig confidentiële informatie kunnen delen.	▪ Geautomatiseerde (machine-to-machine) processen, zoals het aanleveren van data uit bedrijfsprocessen of sensoren. ▪ Wederzijdse authenticatie tussen serviceproviders. ▪ Authenticatie van serviceproviders met specifieke rollen in niet-gereguleerde afsprakenstelsel.

4.2.3. Elektronische tijdstempel

Een *elektronische tijdstempel* (e-tijdstempel) of *electronic Timestamp* (Timestamp) is een digitaal bewijs dat data koppelt aan een tijdsaanduiding. Het toont zo het bestaan van de gegevens op een specifieke datum en tijd aan[21]. Hierdoor is het vast te stellen wanneer de inhoud is aangepast of ingezien.

Het fysieke equivalent van de Timestamp is een datumstempel die informatie bevat over de tijd en datum wanneer het document is gegenereerd. Bij de Timestamp zijn drie deeldiensten betrokken: het aanmaken, valideren en preserveren van de Timestamp. Hierbij krijgen dergelijke diensten het label *gekwalificeerde Timestamp* (QTimestamp) wanneer de Timestamp voldoet aan Artikel 42 van de eIDAS revisie[22] (zie **Figuur 10**).

Figuur 10: Een QTimestamp is een Timestamp met additionele eisen.



Een Timestamp heeft verschillende toepassingsgebieden[23]. **Figuur 11** bevat een overzicht van de belangrijkste use cases voor (Q)Timestamps.

[21] Zie (Q)Timestamp 1-pager
[22] Artikel 42
[23] Datasure over toepassingen e-tijdstempel

Figuur 11: (Q)Timestamps worden gebruikt voor het onomstotelijk vastleggen van de juiste datum en tijd.

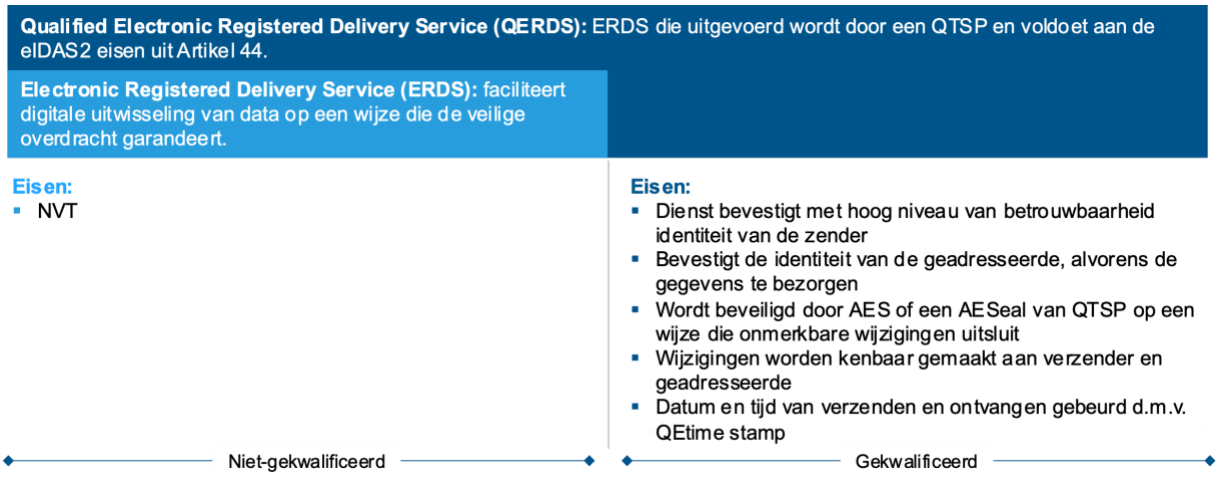
Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Tijd van een gebeurtenis vastleggen	Het registreren van de juiste tijd en datum waarop een gebeurtenis heeft plaatsgevonden.	Ik wil zeker weten dat een bestand verstuurd is op een bepaald tijdstip, zodat ik kan controleren of de voorwaarden nageleefd worden.	▪ Loggen van transacties in de financiële sector. ▪ Vastleggen van een octrooiaanvraag, de versie van een document, database of softwarecode etc. ▪ Garanderen tijdstip wanneer een (Q)ESig gezet is.

4.2.4. Diensten voor elektronische aangetekende bezorging

Een dienst voor elektronisch aangetekende bezorging of *Electronic Registered Delivery Service* (ERDS)[24] faciliteert het digitaal uitwisselen van data. ERDS garandeert een veilige overdracht van data door die te beschermen tegen bijvoorbeeld diefstal, ongeautoriseerde aanpassingen of vernietiging[25]. Een (Q)ERDS is vergelijkbaar met aangetekende post met de garantie van een postbedrijf om post veilig te bezorgen en dat onbevoegden *niet* op de hoogte zijn van de inhoud.

Er zijn twee deeldiensten binnen deze categorie, namelijk het leveren van de ERDS als end-to-end dienst en de validatie van de data verstuurd via ERDS. de eIDAS revisie beschrijft standaarden en kenmerken voor deze dienst. *Gekwalificeerde ERDS* (QERDS) krijgt dit label wanneer zij voldoen aan de eisen uit Artikel 44[26] (zie **Figuur 12**).

Figuur 12: QERDS is ERDS met additionele eisen om veilige digitale overdracht te verzekeren.



Figuur 13 bevat een overzicht van de belangrijkste use cases voor (Q)ERDS.

Figuur 13: (Q)ERDS zijn diensten die documenten bezorgen via push of pull.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Documenten of data bezorgen (push)	Het veilig en aantoonbaar elektronisch afleveren	Ik wil vertrouwen hebben dat mijn juridische documenten	▪ Versturen, gericht op een menselijke ontvanger, van

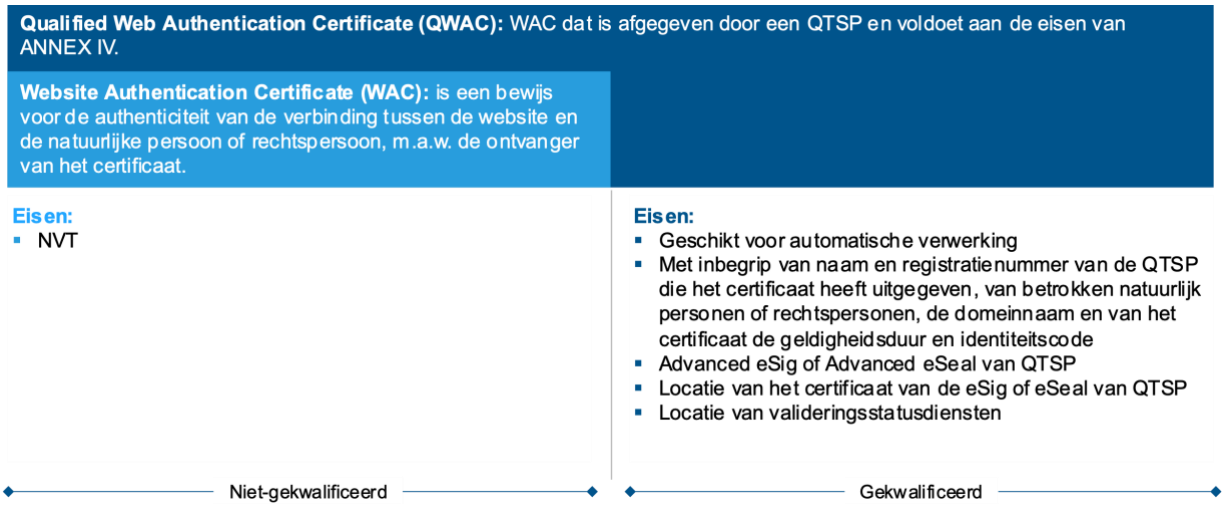
[24] Zie (Q)ERDS 1-pager
[25] Doxee over eIDAS
[26] eIDAS revisie Artikel 44

	van documenten of data bij de juiste persoon via e-mail.	veilig en correct verstuurd kunnen worden en bij de juiste persoon belanden.	contractstukken, facturen, diagnoses, intellectueel eigendom etc. ▪ Data versturen, gericht op automatische verwerking tussen machines, zoals vrachtbrieven, productiedata, energieverbruik, onderhoudsgegevens etc.
Documenten of data bezorgen (pull)	Het veilig en aantoonbaar elektronisch afleveren van documenten of data bij de juiste persoon in een portal.	Ik wil vertrouwen hebben dat mijn juridische documenten veilig en correct bezorgd worden bij een persoon, dus ik zet ze in een portaal en stuur de ontvanger een notificatie waar deze de documenten kan ophalen.	▪ De overheid stuurt een burger een notificatie dat er een bericht klaarstaat in zijn of haar persoonlijke inbox.

4.2.5. Authenticatie van websites

Authenticatie van websites of *Website Authentication Certificate* (WAC) verwijst naar het elektronische bewijs (certificaat) voor de authenticatie van websites. Dergelijke certificaten verzekeren de verbinding tussen een natuurlijk persoon of rechtspersoon en een website[27]. Er zijn twee type deeldiensten betrokken bij een WAC, namelijk het aanmaken en de validatie van het certificaat. Wanneer een WAC wordt afgegeven door een QTSP en voldoet aan de eisen van ANNEX IV[28] dan is het een *gekwalificeerd certificaat voor websiteauthenticatie*, oftewel een QWAC (zie **Figuur 14**).

Figuur 14: Een QWAC is een WAC met additionele authenticatie eisen.



Een QWAC is vergelijkbaar met een keurmerklogo bij een groenteboer, omdat consumenten weten dat het keurmerk enkel uitgegeven wordt door bevoegde instanties die nauwgezette procedures volgen om

[27] European Parliament
[28] eIDAS ANNEX IV

de groenteboer te keuren. Hierdoor kunnen klanten ervan uitgaan dat de groenteboer authentiek is en dus vertrouwd kan worden om bijvoorbeeld enkel biologische of lokale producten te leveren. Door de aanwezigheid van een QWAC op een website kunnen gebruikers vertrouwen wat de identiteit van de entiteit achter de website is en dat de communicatie met deze website (de dienst/verbinding zelf) veilig is. Een (Q)WAC tracht op die wijze vertrouwen in digitale context te realiseren. Een QWAC is technisch equivalent aan andere websitecertificaten, zoals een *Domain Validation* (DV) certificaat, *Organisation Validation* (OV) certificaat of een *Extended Validation* (EV) certificaat. De certificaten verschillen echter in hun uitgifteproces. Ieder certificaat heeft zijn eigen niveau van authenticatie, waarbij een DV-certificaat het laagste niveau is en een EV-certificaat of QWAC het hoogste niveau. **Figuur 15** voorziet in een overzicht van de belangrijkste use cases voor (Q)WAC's.

Figuur 15: Een (Q)WAC wordt gebruikt voor website authenticatie en M2M authenticatie.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Website authenticatie	Door certificaten voor website authenticatie kunnen EU-burgers erop vertrouwen dat de website die ze bezoeken legitiem is.	Ik wil zeker weten dat ik op de echte website van mijn bank zit, zodat ik veilig geld kan overmaken.	▪ Internetbankieren. ▪ Online winkelen. ▪ Belastingaangifte doen. ▪ Persoonlijke documenten bekijken.
Wederzijdse Machine-2-Machine authenticatie	Wederzijdse authenticatie tussen dienstverleners om een veilige verbinding op te zetten.	Ik wil zeker weten dat ik de juiste data ontvang zodat ik de juiste beslissingen maak op basis van correcte data.	▪ Geautomatiseerde (machine-to-machine) processen, zoals het aanleveren van data uit bedrijfsprocessen of sensoren. ▪ Wederzijdse authenticatie tussen serviceproviders (zoals gebruikelijk is bij PSD2 tussen banken en service providers). ▪ Authenticatie van serviceproviders met specifieke rollen in niet-gereguleerde afsprakenstelsels.

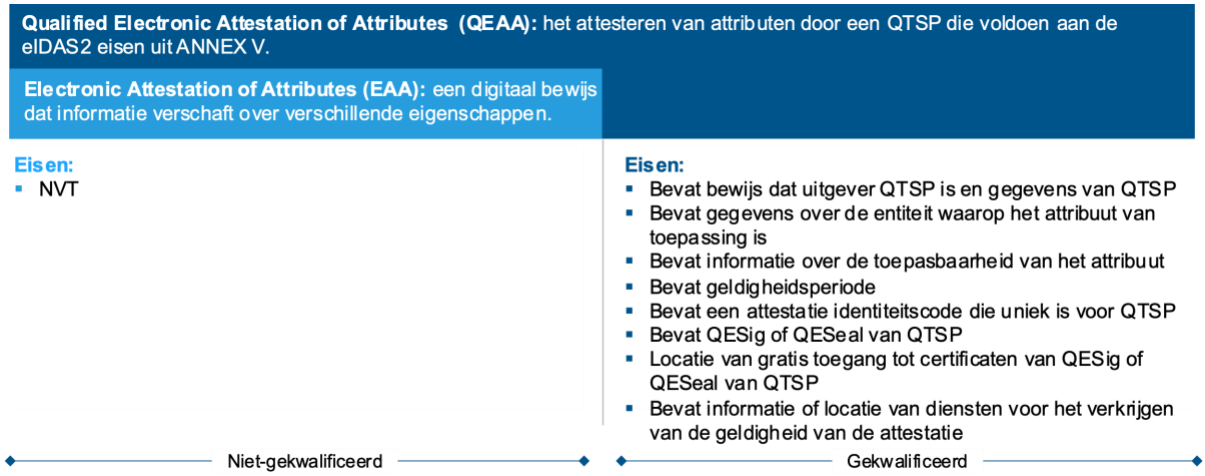
4.2.6. Elektronische attesteringen van attributen

Een *elektronische attestering van attributen* of *electronic attestation of attributes* (EAA) verwijst naar een digitaal bewijs dat informatie verschaft over verschillende eigenschappen, zoals leeftijd, geslacht of persoonlijke kwalificaties als lidmaatschappen, verzekeringsgegevens, een diploma of rijbevoegdheid[29]. EAA's zijn op te delen in twee verschillende deeldiensten: het uitgeven en het valideren van EAA's. Een digitale attestering is vergelijkbaar met een fysieke attesteringen zoals een diploma of rijbewijs. De uitgevende instantie schrijft een kwalificatie toe aan de entiteit waarop het document van toepassing is, en onderschrijft dit met een fysieke handtekening of bedrijfszegel. Hiernaast kan een zowel een natuurlijk persoon als een rechtspersoon ook zelfverklaarde attesteringen, als EAA aan zichzelf toeschrijven, bijvoorbeeld de eigen schoenmaat of het aantal medewerkers van je bedrijf.

De EAA bestaat uit twee vormen met een oplopend vertrouwensniveau: *electronic attestation of attributes* (EAA) en de *qualified electronic attestion of attributes* (QEAA). De gekwalificeerde dienst wordt geleverd door een QTSP met inachtneming van de vereisten opgesteld in ANNEX V van de eIDAS revisie[30] (zie **Figuur 16**). Hiernaast kan het voorkomen dat publieke entiteiten zelf EAA's uitgeven aan de EDIW (zogenoemde Public EAA's). deze publieke entiteiten moeten aan dezelfde eisen voldoen als QTSP's voor QEAA's.

[29] Zie (Q)EAA 1-pager
[30] eIDAS ANNEX V

Figuur 16: Een QEAA is een EAA met additionele eisen op basis van een authentieke bron.



Figuur 17 geeft een overzicht van de belangrijkste use cases voor (Q)EAA:

Figuur 17: Een (Q)EAA kent een uiteenlopend aantal verschillende gebruiken.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Online: Digitaal aanmelden	Het digitaal aanmelden op basis van geverifieerde attributen.	Ik wil mij snel en eenvoudig aanmelden bij een overheidsinstantie of bij een commerciële dienstverlener.	▪ Inschrijven in een gemeente. ▪ Aanvragen van een bankrekening. ▪ Aanmelden als klant bij een retailer.
Online: Digitaal data delen	Het digitaal delen van gevalideerde attributen met externe partijen.	Ik wil de benodigde informatie aanleveren voor de afhandeling van een dienst of product.	▪ Aanleveren van rijbewijsgegevens voor een huurauto. ▪ Aanleveren van een diploma voor een baan. ▪ Delen van paspoortgegevens voor vliegtickets. ▪ Lidmaatschap aantonen voor korting bij horeca/winkels/websites. ▪ Verzekeringsgegevens delen voor het boeken van een reis.
Offline: fysiek toegang tot een locatie	Het verlenen van toegang op basis van geverifieerde attributen.	Ik wil toegang tot bepaalde locaties en bewijs dit met (Q)EAA's.	▪ Toegang tot hotelkamers ▪ Toegang tot concert- of theatervoorstelling. ▪ Toegang krijgen tot kantoorruimtes.
Hybride: Verkoop-toestemming	Het legitimeren van het afnemen van producten of diensten met behulp van geverifieerde attributen.	Ik wil iets kopen waarvoor ik aan bepaalde voorwaarde moet voldoen en dat	▪ Kopen van alcohol (online of in een winkel). ▪ Het recht op persoonlijke aanbiedingen.

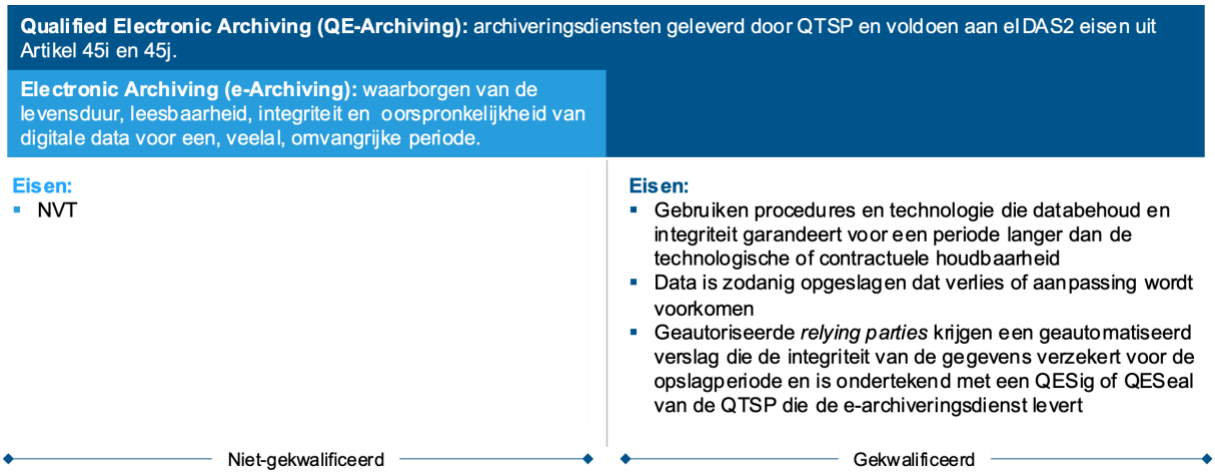
	bewijs ik met (Q)EAA's.	▪ 65+ korting in openbaar vervoer, musea of andere attracties.

4.2.7. Elektronische archiefdiensten

De digitale tegenhanger van het fysieke archief zijn de *elektronische archiefdiensten* (e-archivering) of *electronic archiving* (e-Archiving). Deze dienst legt zich toe op het waarborgen van de levensduur, leesbaarheid, integriteit en oorspronkelijkheid van digitale data voor een, veelal, omvangrijke periode[31]. E-Archiving kent één dienst: het archiveren van elektronische gegevens. De eIDAS regulering betreft de archivering van elektronische documenten en gegevens, maar spreekt zich niet uit over het proces van het omzetten van fysieke documenten naar waarheidsgetrouwe digitale kopieën.

Gekwalificeerde e-Archiving (QE-Archiving) voldoet aan Artikel 45i en Artikel 45j van de eIDAS revisie[32] (zie **Figuur 18**).

Figuur 18:QE-Archiving is e-Archiving met additionele eisen om preservering over lange periode te garanderen.



Figuur 19 presenteert een overzicht van de belangrijkste use cases voor (Q)E-Archiving.

Figuur 19: De enige use case van (Q)E-Archiving is het waarborgen van de integriteit over langere tijd.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Integriteit van documenten bewaken	Zorgen voor de onveranderlijkheid van documenten en bijbehorende (Q)ESig's en (Q)ESeals in de loop van de tijd.	Ik wil de zekerheid hebben dat digitale bestanden en hun verzegeling gedurende lange tijd hun integriteit en wettelijk geldig behouden.	▪ Terugvinden van de juiste data in de gewenste staat, bijvoorbeeld in een bedrijfs- of overheidscontext. ▪ Registreren van omgevingsvergunning, bouwvergunning, parkeervergunning etc. ▪ Opslaan van data in overeenstemming met compliance.

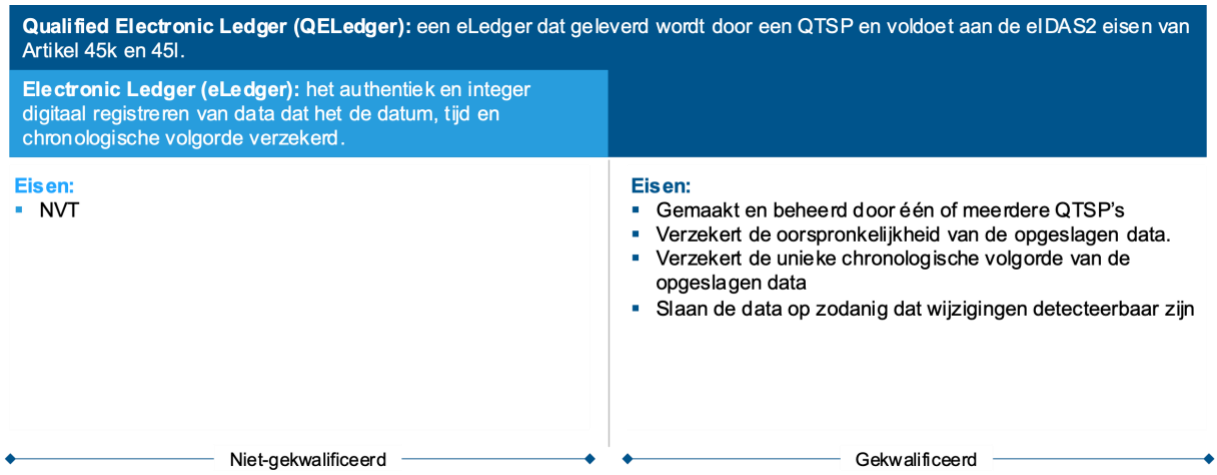
[31] Zie (Q)E-Archiving 1-pager
[32] eIDAS revisie Artikel 45i en 45j

4.2.8. Elektronische grootboeken

Elektronische grootboeken (in eIDAS ook bekend als elektronische registers) of *electronic ledgers* (eLedgers) zijn manipulatiebestendige digitale registraties van data op een wijze die haar authenticiteit en integriteit op het gebied van datum, tijd en chronologische volgorde verzekerd[33]. Deze categorie bevat geen andere diensten behalve het genoemde veilig opslaan van data. ELedgers zijn het digitale equivalent van fysieke registers, zoals handgeschreven financiële bedrijfsadministratie. De definitie van de eLedger is met opzet technologieneutraal verwoord, zodat het zowel *distributed ledger technology* (DLT), hoofdzakelijk blockchain, omvat als de non-distributed varianten zoals digitale dubbel boekhoudsystemen die gebruikt worden door banken.

Door de eisen van de eIDAS revisie te implementeren[34], verkrijgen eLedgers het stempel: gekwalificeerd of QELedger (zie **Figuur 20**).

Figuur 20: QELedger is een eLedger met additionele eisen die de controle over het netwerk vergroten.



Figuur 21 bevat een overzicht van de belangrijkste use cases voor (Q)ELedgers.

Figuur 21: De use case van (Q)ELedger betreft alleen het onomstotelijk chronologisch opslaan van gegevens.

Use case	Beschrijving	Voorbeeld user story	Voorbeelden toepassing
Onomstotelijk chronologisch opslaan van gegevens	Bijhouden van een database waarin transacties chronologisch vastgelegd en opgeslagen worden.	Ik wil transacties chronologisch opslaan, zodanig dat dit verifieerbaar is en opgeslagen op een (de)centrale wijze.	▪ Centraal vastleggen bestuurders KVK. ▪ Centraal opslaan eigendom onroerend goed Kadaster. ▪ Centraal bijhouden financiële transacties voor banken. ▪ Decentraal vastleggen van digitaal eigenaarschap, zoals NFT's. ▪ Decentrale opslag van lijsten met betrouwbare partijen voor digitale identiteit. ▪ Decentraal bijhouden en bewijzen van

[33] Zie (Q)ELedger 1-pager
[34] eIDAS Artikel 45k en 45l

herkomstinformatie van gebruikte grondstoffen.

5. Effectenanalyse

In de komende drie tot vijf jaar[35] zal de markt voor vertrouwensdiensten aanzienlijke veranderingen ondergaan. Deze veranderingen zijn grotendeels toe te schrijven aan de herziening van eIDAS, die leidt tot een herdefiniëring van de eisen en beschrijvingen van vertrouwensdiensten. Daarnaast draagt de ontwikkeling van de EDIW bij aan de opbouw van een nieuwe infrastructuur, wat de vraag naar vertrouwensdiensten kan stimuleren. Verder is er ook andere Europese wetgeving die een significante invloed heeft op de markt voor vertrouwensdiensten. **Figuur 22** biedt een overzicht van de ontwikkelingen in verwachte vraag naar (gekwalificeerde) vertrouwensdiensten.

Figuur 22: De verwachting is dat de vraag naar veel gekwalificeerde vertrouwensdiensten groeit (indicatief).

Vertrouwensdienst	Vraag naar de niet-gekwalificeerde vertrouwensdienst	Vraag naar de gekwalificeerde vertrouwensdienst
Elektronische handtekeningen	−	+ +
Elektronische zegels		+ +
Elektronische tijdstempels		− +
Diensten voor elektronische aangetekende bezorging	+	− +
Authenticatie van websites	+	+
Elektronische attesteringen van attributen	+	+ +
Elektronische archiefdiensten		+
Elektronische grootboeken		− +

− = Vraag naar dienst daalt
\+ = Vraag naar dienst stijgt
− + = Vraag naar dienst stijgt of daalt
\+ + = Vraag naar dienst stijgt veel

Naast de impact op afzonderlijke vertrouwensdiensten, ervaren we ook bredere effecten op de algehele markt van vertrouwensdiensten. Deze effecten zijn niet exclusief verbonden aan één specifieke dienst. In de volgende paragrafen zullen deze specifieke en bredere effecten gedetailleerd worden toegelicht.

5.1. Elektronische handtekeningen

De markt voor (Q)ES ondergaat aanzienlijke veranderingen. Momenteel wordt deze markt overheerst door organisaties die zich richten op het proces van het zetten van niet-gekwalificeerde handtekeningen. Daarentegen bestaat de markt voor gekwalificeerde elektronische handtekeningen voornamelijk uit beroepscertificaten en eenmalige certificaten in combinatie met processen voor onboarding. Er zijn twee belangrijke ontwikkelingen te verwachten die voortvloeien uit de introductie van de EDIW en de revisie van eIDAS:

[35] Onderhevig aan verandering in tijdslijnen van de eIDAS revisie en de oplevering van EDIW's.

- De markt voor QES groeit, omdat elke burger een certificaat voor gekwalificeerde handtekeningen kan krijgen[36].
- De EDIW zorgt voor een groei in de markt van QES van burgers waardoor QES de norm worden.

De ontwikkelingen volgen de aanname (zie kader) dat de adoptie van de EDIW hoog wordt.

Aanname 1: De adoptie van de EDIW onder burgers wordt hoog en vergelijkbaar met de adoptie DigiD
Met de introductie van de EDIW ontstaat een aantrekkelijke oplossing met een hoog betrouwbaarheidsniveau die zowel in publieke als private sector gebruikt kan worden. Elke lidstaat is verplicht om de wallet te introduceren. De acceptatie van de wallet is voor een deel van de marktpartijen verplicht. Voor burgers is gebruik van de EDIW niet verplicht. Hoewel de acceptatie van de EDIW ook voor veel marktpartijen niet verplicht wordt, verwachten we dat de EDIW daarnaast een aantrekkelijk middel is voor veel marktpartijen voor identificatie en authenticatie processen. De verwachting is namelijk dat de EDIW te integreren is in bestaande diensten en processen.

Het businessmodel van aanbieders van eenmalige (Q)ES komt onder druk te staan
Het huidige proces voor het creëren van QES is tijdrovend. QTSP's moeten voor elke eenmalige handtekening een identificatie proces doorlopen. Dit proces omvat veel stappen die vergelijkbaar zijn met 'Know Your Customer' (KYC) procedures. Dit proces kost geld voor de QTSP op uit te voeren. Met de introductie van de EDIW verschuift het identificatie proces naar de EDIW. Dit zet druk op het business model van eenmalige (Q)ES omdat het eenvoudiger wordt voor partijen om dit als dienst aan te bieden. Voor beroepscertificaten zal er waarschijnlijk niet veel veranderen omdat de EDIW in veel gevallen niet per se handiger is dan een fysieke pas.

De EDIW zorgt voor een groei in de markt van QES waardoor het de norm wordt
De eIDAS revisie beschrijft dat lidstaten verantwoordelijk zijn voor het gratis beschikbaar stellen van een QES-certificaat in de EDIW voor hun burgers voor niet professioneel gebruik. In het geval van hoge adoptie van de EDIW ontstaat er een nagenoeg compleet nieuwe markt. Aangezien QTSP's deze certificaten niet kosteloos aan burgers kunnen verstrekken, ontstaat de vraag wie de kosten voor uitgifte zal dragen. Omdat dit een bestaande markt is, is het moeilijk voor de overheid om te beargumenteren dat zij zelf QTSP moeten worden om deze certificaten uit te geven. De overheid zou dan optreden als marktpartij en om concurrentievervalsing te voorkomen, moet de overheid zich aan gedragsregels houden[37]. Het alternatief is het uitgifteproces uitbesteden aan één of meerdere QTSP's.

De introductie van de EDIW maakt elektronische handtekeningen toegankelijker en vergroot het bewustzijn en gebruik van elektronische handtekeningen onder burgers. Dit kan eveneens zorgen voor een hogere adoptie van elektronische handtekeningen in professionele contexten. Zo wordt de drempel voor 'relying parties' lager om een QES te vereisen in plaats van een niet-gekwalificeerde eSig, wat de markt voor AES doet verschuiven richting QES.

Niet al het gebruik van QES zal verschuiven naar QES op afstand met behulp van de EDIW. Bestaande fysieke QES, zoals de *Unieke Zorgverlener Identificatie* pas (UZI-pas), zullen blijven bestaan vanwege bijvoorbeeld praktische overwegingen of andere overstapbarrières. Een voorbeeld hiervan is een huisarts die het handiger vindt om recepten te blijven ondertekenen via de UZI-pas en een kaartlezer op zijn PC. Het gebruik van dezelfde UZI-pas in een operatiekamer is ook logischer omdat het gebruik van een telefoon niet praktisch of zelfs verboden is.

In de professionele context kan er wel een financiële vergoeding worden gerekend voor het gebruik van QES. Onduidelijk is hoe dit in de praktijk wordt gewaarborgd. Als bijvoorbeeld het aantal handtekeningen dat kan worden gezet met het QES certificaat uit de wallet gelimiteerd wordt, dan kan dit resulteren in lager gebruik, ook in niet-professionele context. Met andere woorden, wanneer er regelgeving en handhaving plaatsvindt op de scheiding tussen de kosteloze burgercertificaten en haar

[36] Tot het moment komt waarop EDIW's gecertificeerd kunnen worden als QSCD, zullen QES die via de EDIW gezet gaan worden de remote QES zijn (met behulp van remote QSCD).
[37] Rijksoverheid

betaalde tegenhanger, dan heeft de wijze waarop dit gebeurt impact op het gebruik van handtekeningen, zowel professioneel als niet-professioneel.

Voor het gebruik van QES via de EDIW is ook een vloeiende customer experience van belang. Dit betreft niet alleen een gebruiksvriendelijke interface, maar eveneens het integreren van het gebruik in bestaande digitale tekenomgevingen, zoals Docusign en Adobe sign. Wanneer die omgevingen documenten getekend met een QES vanuit de wallet niet of onduidelijk weergeven, en gebruikers dus niet in staat zijn de authenticiteit ervan te controleren, vermindert de toegevoegde waarde van deze technologie.

Wanneer QES de norm zijn, dan is een sterke groei van de markt voor het zetten van handtekeningen op afstand aannemelijk

Er is een grotere markt voor het beheren van QSCDs op afstand te verwachten. Een QSCD is nodig voor het uiteindelijke 'zetten' van de elektronische handtekening. De private keys van de certificaten moeten volgens specifieke en strenge eisen worden opgeslagen. Binnen de EU is er nog debat over de locatie van deze private sleutels, oftewel welk type QSCD in combinatie met de European Digital Identity Wallet (EDIW) gebruikt dient te worden. **Figuur 23** illustreert een aantal van deze varianten[38].

Figuur 23: De private keys die nodig zijn voor QES kunnen op verschillende plekken opgeslagen worden (niet uitputtend).

QSCD variant	Omschrijving
Smart cards	Private keys kunnen opgeslagen worden in de chip van smart cards. Dit kan bijvoorbeeld in de chip van een nationale ID kaart, of een defensiepas. De chip kan worden uitgegeven door een lidstaat zelf waardoor controle en veiligheid blijft liggen bij een lidstaat. De burger (de holder) heeft een telefoon, die *near field communication* (NFC) technologie kan benutten, nodig om de wallet te ontgrendelen met behulp van zijn smart card.
SIM/eSIM kaart in een telefoon	Private keys kunnen opgeslagen worden in een SIM of eSIM die in een telefoon zit. Dit kan een betere gebruikerservaring geven omdat burgers geen ID kaart moeten gebruiken om de wallet te ontgrendelen. Telecom aanbieders geven de SIM kaarten uit.
Secure element in een telefoon	Private keys kunnen opgeslagen worden in het secure element van een telefoon. Dit kan een betere gebruikerservaring geven omdat burgers geen ID kaart moeten gebruiken om de wallet te ontgrendelen. In dit geval moet het secure element wel gecertificeerd worden. Telefoon producenten ontwikkelen het secure element (bijv. Apple, Samsung, Google, Huawei).
USB token	Private keys kunnen opgeslagen worden in een USB token (een gecertificeerde USB stick). Hoewel het gebruik van een USB-token samen met een telefoon niet intuïtief lijkt, is het toch mogelijk wanneer de EDIW als een webbrowser plug-in functioneert.
HSM & SAM in verbinding met de EDIW	Private keys worden opgeslagen in een *Hardware Security Module* (HSM), die zich in de cloud bevindt en geen fysieke hardware op telefoons vereist. Het gebruik van een HSM & *Signature Activation Module* (SAM) vereist nog steeds een sterke authenticatie van de gebruikers van de EDIW.

Over de invulling van het opslaan van de private keys zullen de uitvoeringshandelingen meer duidelijkheid geven. De meerderheid van de huidige mobiele telefoons bezitten niet de juiste eigenschappen om de private keys lokaal op te slaan (bijv. in het secure element of op een eSIM). Daarbij zijn de huidige telefoon producenten niet gebaat bij het implementeren van een Secure Element, omdat dit de kostprijs van hun producten alleen doet toenemen zonder dat het een specifieke klantenbehoefte bevredigd. Dit betekent dat een aanzienlijk deel van de huidige en toekomstige mobiele telefoons niet in staat zal zijn om private keys lokaal op te slaan. Op de lange termijn, als

[38] Methics, IDEMIA

mobiele telefoons in staat zijn op private keys lokaal op te slaan, zullen de meeste private keys in secure elements in telefoons opgeslagen worden.

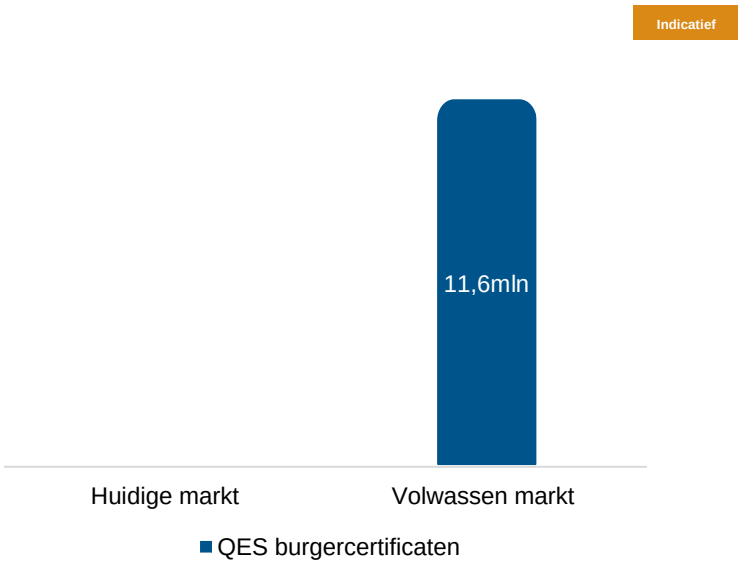
Het is waarschijnlijk dat de vraag naar het beheer van QSCDs op afstand (HSM & SAM), waarbij private keys (die niet lokaal opgeslagen kunnen worden) in de cloud worden opgeslagen, toeneemt op de korte termijn. De cloud variant biedt echter geen oplossing voor offline situaties. De eIDAS-wetgeving vereist dat de functies van de EDIW ook beschikbaar zijn voor offline gebruik. In de praktijk leidt dit er waarschijnlijk toe dat meerdere opties gebruikt gaan worden voor EDIW's, afhankelijk van de use case.

De markt voor QES zal groeien over de komende jaren

De markt voor QES kan opgesplitst worden op basis van twee gebruiksdomeinen, namelijk private certificaten en arbeidscertificaten. De eerste categorie betreft een QES die burgers gebruiken als privaat persoon, in tegenstelling tot arbeidscertificaten waarin het toepassingsgebied de werkomgeving betreft.

Met de introductie van de wallet is de verwachting dat de adoptie van de QES-burgercertificaten eenzelfde patroon zal volgen als de adoptie van DigiD over de jaren heen[39]. Dit betekent dat er een compleet nieuwe markt ontstaat, omdat de huidige QES-burgercertificatenmarkt nagenoeg nihil is. De verwachting is dat er ongeveer 11.6 miljoen QES burgercertificaten in omloop zijn bij een volwassen markt (zie **Figuur 24**).

Figuur 24: Er ontstaat een nieuwe omvangrijke markt voor QESig bij hoge EDIW adoptie[40].



Aanname 2: De meeste burgers beschikken over één wallet voor privézaken en extra wallets voor werk gerelateerde zaken

In Nederland wordt onder regie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties gewerkt aan de NL voorbeeldwallet[41]. De eerste versie zal zich richten op online identificatie, het delen van gegevens en elektronisch ondertekenen bij publieke en private diensten[42].
Het is te verwachten dat, als een dergelijke wallet gratis ter beschikking wordt gesteld voor burgers door de overheid, de kans op het gebruik van meerdere wallets voor privézaken *zeer gering is.*

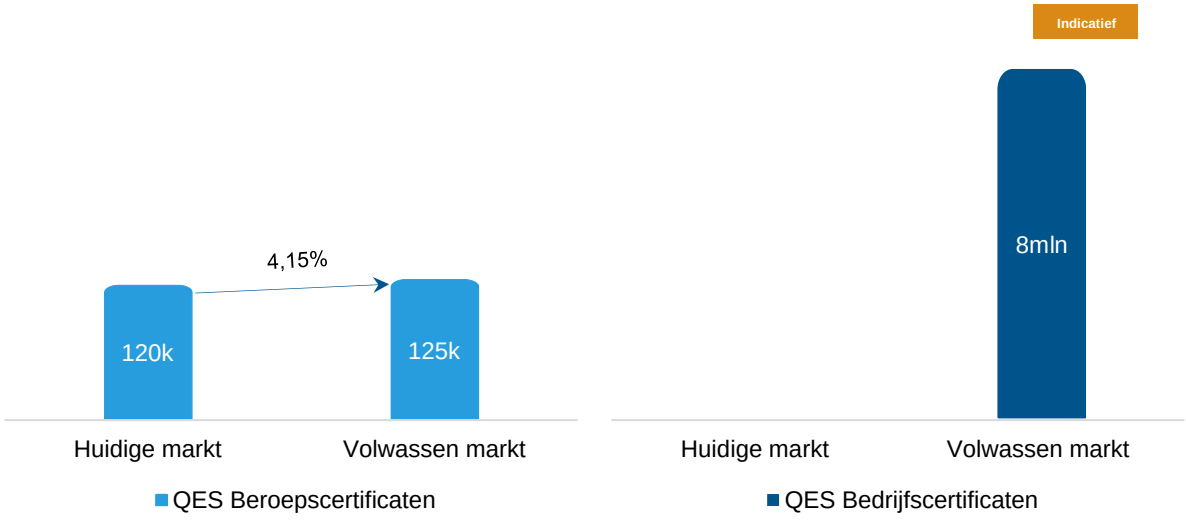
[39] In 2008, toen DigiD verplicht werd voor overheidsinstanties, was de adoptie ongeveer 40%. Dit is inmiddels uitgegroeid tot 95% van Nederlanders van 14 jaar en ouder.
[40] Defensiepassen zijn niet meegenomen in de markt voor beroepscertificaten
[41] EDI Pleio
[42] NL wallet op GitHub

Mogelijk zullen ook andere wallets gecertificeerd worden onder de eIDAS revisie. Met name voor het gebruik in de werk gerelateerde zaken is er een mogelijkheid dat burgers kiezen voor een extra wallet om privé en werk gescheiden te houden met daarin een QES-certificaat. Ook in de fysieke wereld is dit al de praktijk: burgers zijn vrij om verschillende geschreven handtekeningen te gebruiken. De verwachting is dat iedere werkende burger dan beschikt over een privé QES-certificaat en werk gerelateerd QES-certificaat. Als alternatief zouden burgers ook een privé wallet kunnen gebruiken die machtigingen bevat voor zakelijk gebruik.

Binnen de arbeidscertificaten zijn twee soorten te onderscheiden: beroepscertificaten en persoonsgebonden bedrijfscertificaten. Het beroepscertificaat wordt uitgegeven (of ingetrokken) door de beroepsorganisatie, zoals het geval bij advocaten, notarissen of artsen. Dit in tegenstelling tot persoonsgebonden bedrijfscertificaten waar de werkgever de certificaten beheert. Dergelijke certificaten geven werknemers specifieke bevoegdheden, bijvoorbeeld het tekenen namens een bedrijf, toestemming om te werken met apparatuur of toegang tot afgesloten ruimtes. Een bestaand voorbeeld van een persoonsgebonden bedrijfscertificaat betreft de uitgifte van certificaten aan automonteurs zodat zij toegang hebben tot data van de auto's waaraan ze werken of gemachtigd zijn om te werken met waterstof- of elektronische voertuigen.

Er is een markt voor QES wat betreft de beroepscertificaten (zie **Figuur 25**). De te bedienen markt is op dit moment ongeveer 120.000 (hierin zijn defensiepassen niet meegenomen). Hierbij verschilt het daadwerkelijke gebruik van de QESig certificaten per beroepsgroep. De verwachting is dat in een volwassen markt het aantal certificaten meestijgt met de groei van het aantal werknemers in de desbetreffende sectoren[43]. De markt voor QES persoonsgebonden bedrijfscertificaten is op dit moment zeer gering. In een volwassenmarkt is de verwachting dat een groot deel van de beroepsbevolking gebruik zal gaan maken van dergelijke certificaten.

Figuur 25: QES beroepscertificaten groeien en mogelijk ontstaat nieuwe markt voor QES Bedrijfscertificaten.



De groei in de markt van arbeidscertificaten is momenteel nog omringt met onzekerheid, omdat de functie die zij vervullen ook door (Q)EAA's ingevuld kan worden. Daarnaast is er voorlopig geen juridische duidelijkheid over de betekenis van een persoonlijke handtekening in de vorm van een persoonsgebonden bedrijfscertificaat in de context van een bedrijf.

[43] Deze groei hangt samen met de groei van de Nederlandse bevolking en de ontwikkelingen op de arbeidsmarkt.

5.2. Elektronische zegels

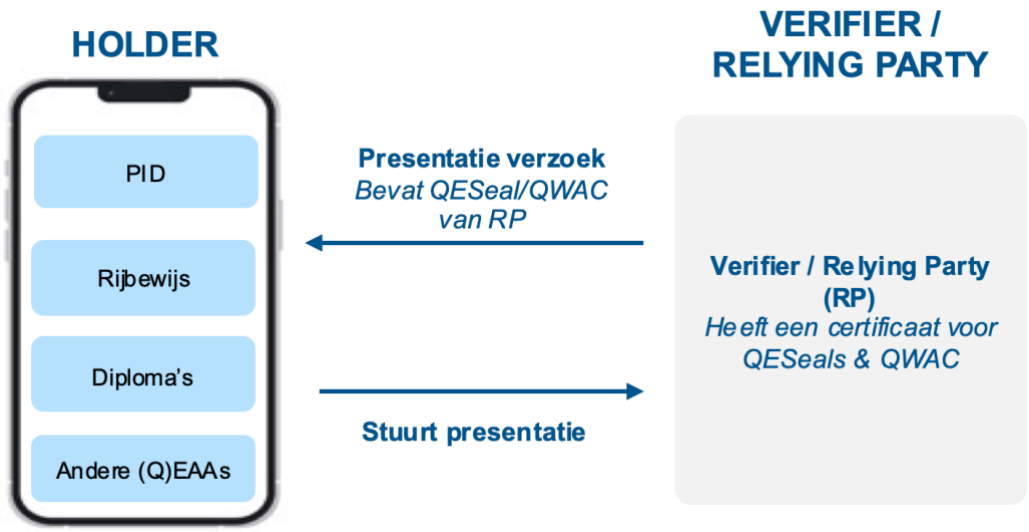
De markt voor eSeals verandert voor marktpartijen. De verwachting is dat er een hoge adoptie van de Organisational Digital Idenity wallet (ODIW) zal ontstaan. Echter, de snelheid van de adoptie zal trager verlopen dan bij de EDIW vanwege hogere complexiteit. Desondanks is de verwachting dat er een sterke groei gaat optreden in de Nederlandse markt voor QESeals.

Aanname 3: De adoptie van de Organisational Digital Identity Wallet (ODIW) wordt hoog, maar de ODIW heeft meer tijd nodig dan de EDIW om geadopteerd te worden.
De Organisational Digital Identity Wallet bevat attributen die verband houden met de (identificatie van) organisaties. Bijvoorbeeld (officiële) identifiers en eigenschappen op organisatieniveau. Typische kenmerken zijn het KVK-nummer of het bewijs dat een IBAN hoort bij een organisatie. Terwijl er voor burgers al diverse wallet-oplossingen in de markt beschikbaar zijn, zijn dergelijk wallets nog niet gangbaar voor organisaties. Daarnaast wordt in Nederland veelal eHerkenning gebruikt voor geautoriseerde toegang van bedrijven tot digitale (overheids)diensten.

QESeal gebruik neemt toe omdat relying parties zich moeten authentiseren met een QESeal bij wallet bevragingen

QESeals gaan naar verwachting een rol spelen tussen de EDIW en relying parties. De verwachting is dat data verzoeken richting EDI wallets alleen mogelijk zijn als ze verzegeld worden met een QESeal door de *relying party* (RP). **Figuur 26** bevat een visuele weergave van dit proces.

Figuur 26: Het is de verwachting dat relying parties berichten naar EDIW's verzegelen met QESeals en QWAC's.



De QESeal fungeert als een elektronische handtekening die de identiteit van de afzender waarborgt en ongeautoriseerde toegang tot wallets van mensen voorkomt. In Nederland dienen RP's zich voorafgaand aan de dienstverlening te registreren, zodat bekend is wanneer zij attesteringen verifiëren. De wallet kan zo zien of een RP wel bevoegd is. Doordat QESeals hiervoor gebruikt gaan worden, is de verwachting dat alle partijen die gebruik willen maken van de wallet, een certificaat voor QESeals nodig hebben.

Hoewel de authenticatie van RP's nog niet is vastgesteld is het heel onlogisch dat er een ander nieuw authenticatiemiddel bedacht wordt voor deze situatie. Zeker omdat vertrouwensdiensten en QESeals al bestaan. Deze hypothese wordt ook bevestigd door andere Europese wetgeving rondom datadelen waar QESeals ook verplicht gesteld worden (PSD2).

Andere relevante trends m.b.t. data uitwisseling en compliance druk wakkeren het gebruik van QESeals aan

Er is een zichtbare trend van toenemend gebruik van QESeals en de veronderstelling is dat deze zal toenemen, aangezien diverse Europese wetgevingen voor gegevensuitwisseling het gebruik verplicht

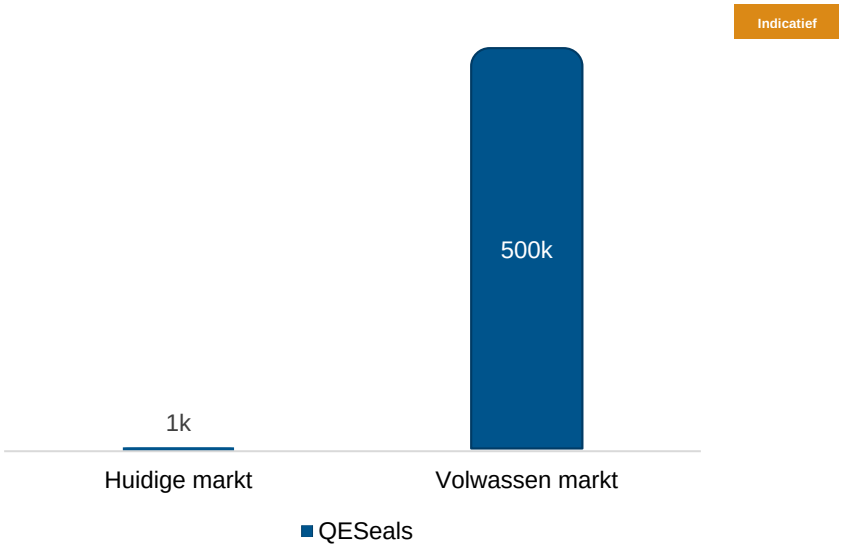
stellen. Dit fenomeen heeft zich voorgedaan bij de introductie van de *Payment Services Directive 2* (PSD2), waarbij het gebruik van QESeals en QWAC's verplicht wordt gesteld voor data-uitwisseling tussen banken en derde partijen. Ook zijn QESeals verplicht voor bedrijven die elektrische apparaten willen registreren in het *European Product Registry for Energy Labelling* (EPREL)[44].

De verwachting is dat een soortgelijke vereiste zal worden opgenomen in het *framework for Financial Data Access* (FIDA). Dit houdt in dat naast banken, ook andere financiële instellingen zoals pensioenfondsen en verzekeraars, verplicht gesteld worden om QESeals en QWAC's te gebruiken voor data-uitwisseling.

Ook voor schaalbare data-uitwisseling tussen partijen in specifieke sectoren, zoals de pensioensector, logistiek, zorg en gebouwde omgeving zijn QESeals gewenst. De verwachting is dat de noodzaak en vraag naar schaalbare data-uitwisseling tussen partijen toeneemt, denk bijvoorbeeld aan de ontwikkeling van data spaces in Europa. Hiermee zal ook het gebruik van QESeals voor deze partijen toenemen.

Een digitaal volwassen bedrijfsleven in Nederland betekent grootschalige integratie van de QESeal
Het geheel van deze trends betekent dat de markt voor QESeals sterk gaat veranderen. De huidige Nederlandse markt wordt geschat op ongeveer 1000 QESeals. De verwachting is dat in een digitaal volwassen economie nagenoeg het gehele MBK en grootbedrijven in de toekomst een QESeal moeten bemachtigen. De aanjager van deze ontwikkeling is dat op termijn de huidige PKI overheidscertificaten grotendeels vervangen gaan worden door de combinatie van QESigs, QWAC's en hoofdzakelijk QESeals. Wanneer het Nederlandse bedrijfsleven zich ontwikkeld tot het stadium van digitale volwassenheid waarin ieder jaarverslag, elk factuur en tal van andere bedrijfsdocumenten voorzien zijn van een QESeal, dan is de schatting dat er ongeveer 500.000 QESeal certificaten in omloop zijn (zie **Figuur 27**).

Figuur 27: In een digitaal volwassen Nederlands bedrijfsleven heeft nagenoeg ieder bedrijf een QESeal.



5.3. Elektronische tijdstempels

Naar verwachting zal er weinig tot geen verandering plaatsvinden in de Nederlandse markt van QTimestamps als gevolg van de eIDAS revisie. Dit volgt uit het huidige lage gebruik in de hedendaagse markt van QTimestamps in Nederland. De beperkte wijzigingen in de eIDAS revisie lijken daarin geen verandering te brengen.

De Nederlandse markt voor (Q)Timestamps is en blijft beperkt
De Nederlandse markt voor QTimestamps heeft op dit moment een gelimiteerde omvang. Timestamps maken een cruciaal onderdeel uit van de verschillende vertrouwensdiensten, omdat een tijdsaanduiding extra zekerheid biedt en dus vertrouwen schept. Zo is het bijvoorbeeld in het proces van een (Q)ESig

[44] Intensi Group

belangrijk om niet alleen kennis te hebben van wie er getekend heeft en dat de handtekening correspondeert met de juiste persoon, maar eveneens wanneer deze persoon getekend heeft. Daarom hebben (Q)ESigs veelal een Timestamp om de handtekening te verzegelen met het bewijs van een bepaalde tijd en datum.

De oorzaak dat er *geen* markt is, is dat er in de Nederlandse praktijk vaak geen onafhankelijke partij nodig is om een QTimestamp toe te voegen. Een Timestamp voldoet en wordt niet als onafhankelijk dienst aangeboden. De tijdsaanduiding wordt in die instanties gedaan door de betrokkenen zelf. De enige use cases voor een onafhankelijke tijdsaanduiding van de (Q)Timestamp zijn gevallen waar elke microseconde en de volgorde van transacties cruciaal zijn, bijvoorbeeld bij de handel in financiële producten.

Dit verandert wanneer een wetgever, vaak in een specifieke context, wel een onafhankelijke derde partij voor het uitvoeren van de tijdsaanduiding verplicht stelt. Zo eist de Italiaanse overheid dat bedrijven hun belastingaangifte voorzien van een (Q)Timestamp[45]. De Nederlandse markt kent op dit moment niet een dergelijke verplichting en er zijn geen aanwijzingen dat deze verplichting op korte termijn ontstaat.

De eIDAS revisie geeft weinig aanleiding toename gebruik QTimestamps

De vereisten voor (Q)Timestamps zijn in de eIDAS revisie nagenoeg identiek aan de eisen uit eIDAS1. Er is geen verplichting opgenomen voor het gebruik van QTimestamps in de nieuwe verordening.

In een toekomstige meer volwassen digitale markt waarin tal van diensten compleet gedigitaliseerd zijn, is het voor te stellen dat er *wel* een verplichting komt voor het gebruik van QTimestamps voor die diensten waarin de tijd onomstotelijk vastgesteld dient te worden. Een volledig digitale controle door een accountant of digitaal vastgelegde afspraken door notaris zijn voorbeelden waarin er een meerwaarde kan ontstaan van een onafhankelijke gekwalificeerde partij om de datum en tijd onomstotelijk voor een langere periode te garanderen.

5.4. Diensten voor elektronische aangetekende bezorging

Waarschijnlijk zal de markt voor (gekwalificeerde) elektronische aangetekende bezorging ((Q)ERDS) weinig als gevolg van de eIDAS revisie weinig veranderen. Het huidige gebruik van QERDS-gebruik is laag en de eIDAS revisie bevat beperkte prikkels om het gebruik te verhogen.

De Nederlandse markt voor QERDS is beperkt

De huidige markt voor QERDS is gering in omvang. Een belangrijke aanjager voor QERDS is verplichtstelling in sectorale wetgeving of het opnemen van de dienst op de landelijke ‘Pas toe of leg uit-lijst’. Op dit moment gebeurt dit in Nederland niet/nauwelijks. De gekwalificeerde dienst bevat additionele verificatieprocedures die de veiligheid vergroten. In de praktijk is dit voor de meeste toepassingen overbodig en wegen de additionele kosten niet op tegen de baten. Er zijn verschillende instanties, bijvoorbeeld binnen de rechtspraak, die QERDS mogelijk willen gaan gebruiken. Dit is echter momenteel nog niet grootschalig het geval.

In tegenstelling tot QERDS, is er een omvangrijke bestaande markt voor ERDS. ERDS-aanbieders zijn actief in verschillende sectoren, zoals de gezondheidszorg, juridische dienstverlening, financiële dienstverlening, de publieke sector, bouwsector en het onderwijs.

Gebruik neemt waarschijnlijk toe door bredere rechtsgeldigheid en interoperabiliteit

De eIDAS revisie bevat minimale aanpassingen m.b.t. (Q)ERDS. De toegevoegde verplichte Europa-brede erkenning van de verschillende vertrouwensdiensten is wel een mogelijke stimulans voor toename van de QERDS-markt.

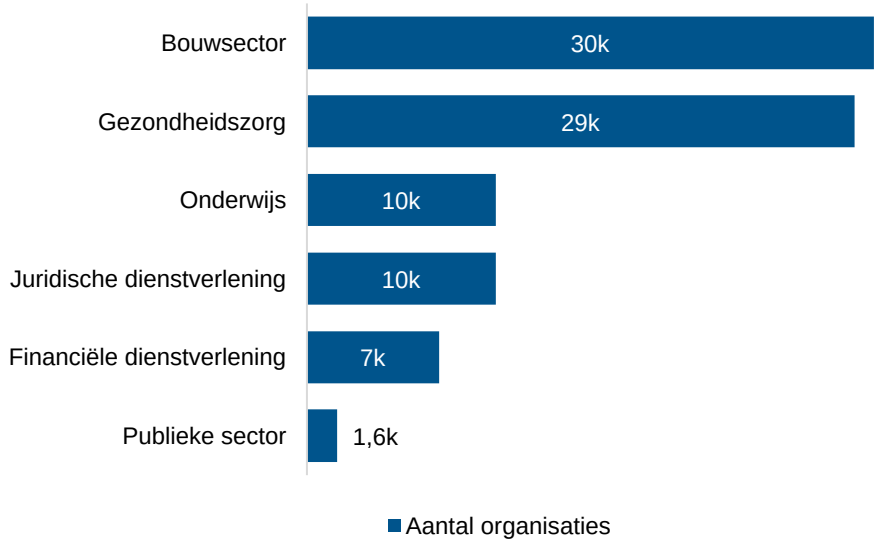
Artikel 24a (8)[46] van de eIDAS revisie beschrijft dat een QERDS erkend in één lidstaat dezelfde status heeft voor alle andere lidstaten. Onder eIDAS1 was het mogelijk voor lidstaten om QERDS-diensten van QTSP’s uit andere lidstaten *niet* te erkennen als gekwalificeerd. Dit resulteerde in een nationale beperking wat betreft de rechtsgeldigheid en acceptatie van de dienst. Nu is er vastgelegd in de eIDAS

[45] Ernst & Young
[46] eIDAS Artikel 24a

revisie dat andere lidstaten de dienst moeten erkennen, betekent dit dat er toegevoegde waarde zit in een QERDS ten opzichte van ERDS, omdat haar juridische status en acceptatie nu Europees breed onomstotelijk wordt vastgesteld. Het is mogelijk dat hierdoor de vraag naar QERDS toeneemt en dat aanbieders van deze dienst ook eenvoudiger diensten kunnen aanbieden in andere lidstaten. In de praktijk blijken er echter soms ook beperkende factoren voor deze interoperabiliteit te kunnen ontstaan, zoals specifieke eisen in implementatiewetgeving of andere bureaucratische factoren. Voor de toename van de vraag voor QERDS is het daarom belangrijk dat beperkende factoren actief worden voorkomen.

Deze ontwikkelingen gezamenlijk resulteren in een marginale huidige markt. De belangrijkste sectoren, de gezondheidszorg, financiële dienstverlening, publieke sector, bouwsector en het onderwijs, bevatten gezamenlijk een potentiële markt van ongeveer 95.000 organisaties (zie **Figuur 28**). De verwachting is dat alleen verplichtingen deze markt doen groeien en organisaties doet bewegen van ERDS naar QERDS. Daarnaast zou de overheid mogelijk groei kunnen aanwakkeren wanneer het voor correspondentie en haar interne processen QERDS gaat hanteren. Dit zijn echter geen directe gevolgen van de eIDAS revisie.

Figuur 28: De potentiële markt bij verplichting van QERDS betreft ongeveer 95.000 organisaties.



5.5. Authenticatie voor websites

Het gebruik van QWAC's verandert op een vergelijkbare manier als de markt voor QESeals. Meer organisaties hebben in de toekomst behoefte aan een QWAC. De toegenomen vraag naar QWAC ontstaat, net als bij QESeals, naar verwachting door compliance druk en de noodzaak voor hogere rechtszekerheid. De toename in vraag komt waarschijnlijk niet voort uit het gebruik van QWAC's voor website authenticatie. Hiernaast is er veel afhankelijk van de oplossingsrichting die uiteindelijk gekozen wordt over wat 'acceptatie van QWAC's' inhoudt[47].

QWAC's blijven vergelijkbaar concurreren voor website authenticatie

Met de eIDAS revisie moeten webbrowsers QWAC's accepteren waardoor QWAC's op een gelijkere voet concurreren met niet gekwalificeerde WAC's[48]. QWAC's hebben als voordeel dat ze een sterkere verificatie hebben tijdens het uitgifte proces waardoor er een hogere rechtszekerheid ontstaat. Dit heeft ook een keerzijde: een ingewikkelder en duurder uitgifte proces. Voor veel websites is dit overbodig waardoor de verwachting is dat de meeste websites WAC's blijven gebruiken.

[47] Security risk ahead
[48] Europese commissie

Andere relevante trends m.b.t. data uitwisseling en compliance druk wakkeren het gebruik van QWAC's aan

Net als voor QESeals, is de trend zichtbaar dat de vraag voor QWAC's toeneemt, omdat diverse Europese wetgevingen voor gegevensuitwisseling het gebruik verplicht stellen. In paragraaf 5.2 is de verplichting van het gebruik van QWAC's onder PSD2 en de verwachting van dezelfde eisen in het FIDA framework beschreven.

QWAC's zijn gewenst voor authenticatie voor schaalbare data-uitwisseling tussen partijen in specifieke sectoren, zoals de pensioensector, logistiek, zorg en gebouwde omgeving. De verwachting is dat de noodzaak en vraag naar schaalbare data-uitwisseling tussen partijen toeneemt, denk bijvoorbeeld aan de ontwikkeling van data spaces in Europa. Hiermee zal ook het gebruik van QWAC's voor deze partijen toenemen.

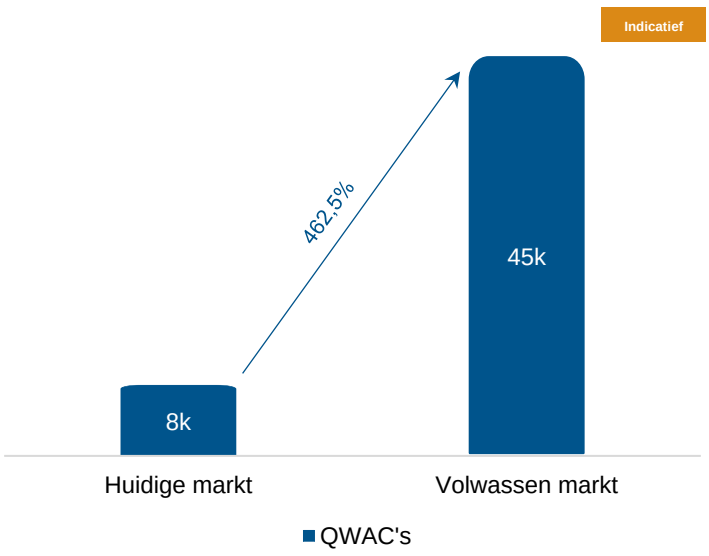
Gebruik QWAC's neemt toe doordat relying parties zich moeten authentiseren met een QWAC bij wallet bevragingen

Net als QESeals gaan ook QWAC's een belangrijke rol spelen tussen de EDIW en relying parties. De verwachting is dat data verzoeken richting EDI wallets alleen mogelijk zijn als ze een QWAC bevatten van de relying party (zie **Figuur 26**). De QWAC fungeert als veilige verbinding tussen de wallet en de relying party. De veilige verbinding zorgt ervoor dat data die verstuurd wordt (informatie uit (Q)EAA's) niet aangepast is tussen de wallet en de relying party. Hiernaast waarborgt de veilige verbinding dat niemand anders de data heeft kunnen lezen. Dit is relevant voor de integriteit en confidentialiteit van de data. De verwachting is dat alle partijen die gebruik willen maken van de wallet, een QWAC nodig hebben.

Hoewel dit proces nog niet is vastgesteld is het onlogisch dat er een ander nieuw authenticatiemiddel bedacht wordt voor deze situatie. Deze hypothese wordt ook bevestigd door andere Europese wetgeving rondom datadelen waar QWAC ook verplicht gesteld worden (bijv. PSD2)[49].

Dit alles leidt ertoe dat de markt voor QWAC's in 2030 in Nederland meer dan verdriedubbeld is ten opzichte van de huidige situatie. De schatting is dat er momenteel ongeveer 8000 QWAC's in omloop zijn. De geschatte voorspelling is dat dit in een volwassen markt mogelijk kan oplopen naar 45.000 gekwalificeerde certificaten (zie **Figuur 29**). Ondanks de forse groei blijft het aandeel van gekwalificeerde certificaten op de totale markt beperkt.

Figuur 29: Bij een digitaal volwassen bedrijfsleven neemt de groei van QWAC's sterk toe.



[49] Infocert

5.6. Elektronische attesteringen van attributen

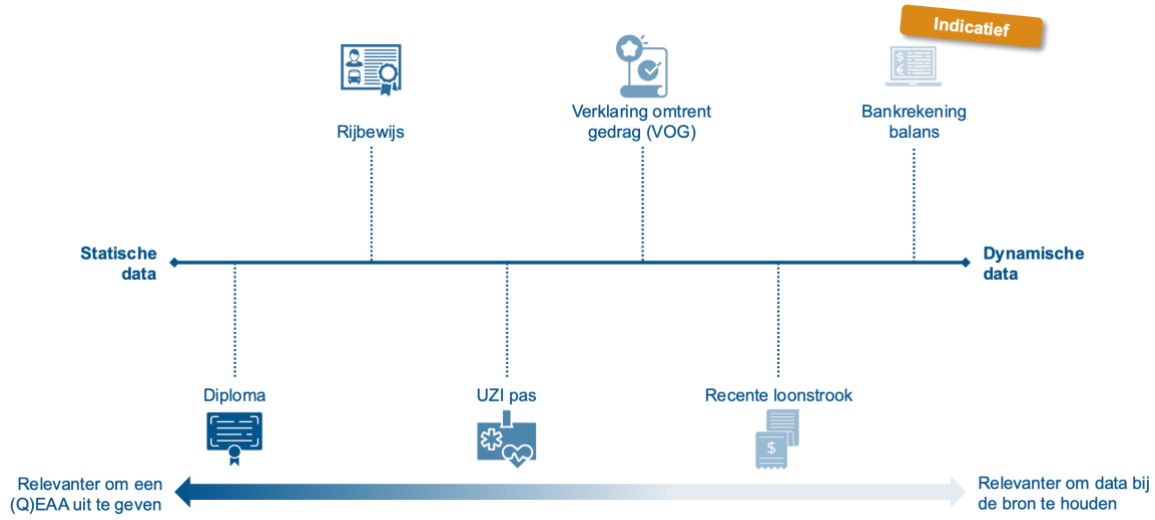
Naar verwachting ontstaat er op korte termijn een omvangrijke Europese markt voor (gekwalificeerde) elektronische attesteringen van attributen of (Q)EAA's als gevolg van de introductie van de EDIW.

Het verwachte gebruik is gebaseerd op de vervanging van huidige fysieke attesteringen, zoals diploma's en rijbewijzen. Daarnaast is de verwachting dat er in de toekomst ook nieuwe typen attesteringen zullen worden gebruikt. Een deel van deze attesteringen gaan wellicht uitgegeven worden door overheden/marktpartijen zelf, maar waarschijnlijk zullen QTSP's attesteringen uitgeven namens deze partijen.

(Q)EAA's worden vooral uitgegeven uit statische attributen

De bruikbaarheid van QEAA's kan inzichtelijk gemaakt worden door ze te bezien langs het spectrum dat loopt van statisch tot dynamisch attributen (zie **Figuur 30**).

Figuur 30: Statische data zijn relevanter om uit te geven als (Q)EAA.



De verwachting is dat (Q)EAA's bestaand gebruik van attributen die in meer of mindere mate statisch zijn, grotendeels overneemt. Statische attributen kenmerken zich door hun onveranderlijkheid en hebben een geldigheidsduur van grofweg enkele jaren tot levenslang. Daarnaast is er geringe kans op revocatie. Voorbeelden van meer statische attributen zijn universiteitsdiploma's, rijbewijzen of UZI-passen. Een diploma is voor het leven en wordt in praktijk zelden ingetrokken[50].

Er zijn attesteringen die zich ergens in het midden van het spectrum begeven en de hypothese is dat deze categorie zich gedeeltelijk verplaatst naar (Q)EAA's. Een VOG of een BRP-uittreksel heeft een geldigheid van enkele maanden en door die korte tijdsduur verkleint het de kans op foutieve beweringen. Voor dergelijke voorbeelden is te verwachten dat het gebruik zich verplaatst naar (Q)EAA's. Uitzondering zijn die situaties waarbij de directe koppeling al veel gebruikt worden, denk aan de bestaande koppelingen met het KVK-register of het Kadaster.

Aan de andere kant van het spectrum bevinden zich bijvoorbeeld dynamische financiële data, zoals een actueel banksaldo, of locatiegegevens. Voor deze gegevens is de actuele status erg belangrijk. Voor sterk dynamische attributen biedt een directe koppeling tussen issuer en relying party de meeste zekerheid. Voor sommige dynamische attributen geven (Q)EAA's wel voldoende zekerheid, maar hier zal per individueel geval en afhankelijk van de context een risicoafweging nodig zijn om dat te bepalen.

Gebruik van (Q)EAA's neemt een vlucht doordat het huidig gebruik vervangt

Er bestaat op dit moment, naast de hierboven al genoemde voorbeelden, een nog omvangrijker aantal digitale of fysieke documenten met beweringen over personen of organisaties. Dienstverleners vragen

[50] Observant online

deze documenten op om risico af te dekken of vanwege wettelijke verplichtingen. Deze documenten worden vaak op een eigen wijze uitgegeven en gecontroleerd op juistheid en geldigheid.

Door de EDIW ontstaat een generieke en schaalbare infrastructuur die partijen faciliteert in het op een gebruiksvriendelijke en kostenefficiënte wijze delen van deze documenten. Deze nieuwe infrastructuur is, in potentie, een goedkoper, veiliger en gebruiksvriendelijker alternatief in vergelijking met de huidige wijze van het delen van deze documenten. In sommige gevallen dienen overheidsbronnen hun gegevens open te stellen voor verificatie door QTSP's. De verwachting is dat het gebruik van (Q)EAA's een vlucht neemt, omdat het in veel gevallen de huidige werkwijze kan vervangen.

Een illustratief voorbeeld is de aanvraag van een uittreksel uit het Basisregistratie Personen (BRP) voor het verkrijgen van een huurwoning. Deze moeten burgers online aanvragen, waarna men 48 uur moet wachten tot ontvangst per post en vervolgens moet een fotokopie worden gestuurd naar de desbetreffende instantie. Een (Q)EAA faciliteert dit gehele proces binnen één minuut. De verhuurorganisatie kan direct tot het verhuurbesluit overgaan, omdat menselijke controle van de documenten niet meer nodig is.

Een ander mogelijk gevolg van de EDIW is dat het gebruik verandert van eenmalig naar periodiek.
Uit de interviews met de betrokken partijen kwam naar voren dat periodiek gebruik mogelijk kan zorgen voor een verrijking van huidige data. Dit zou dan gelden voor meer dynamische attributen, bijvoorbeeld in het bepalen van de kredietwaardigheid van een entiteit waarbij telkens nieuwe financiële gegevens worden meegewogen in plaats van te oordelen op basis van één tijdsmoment.

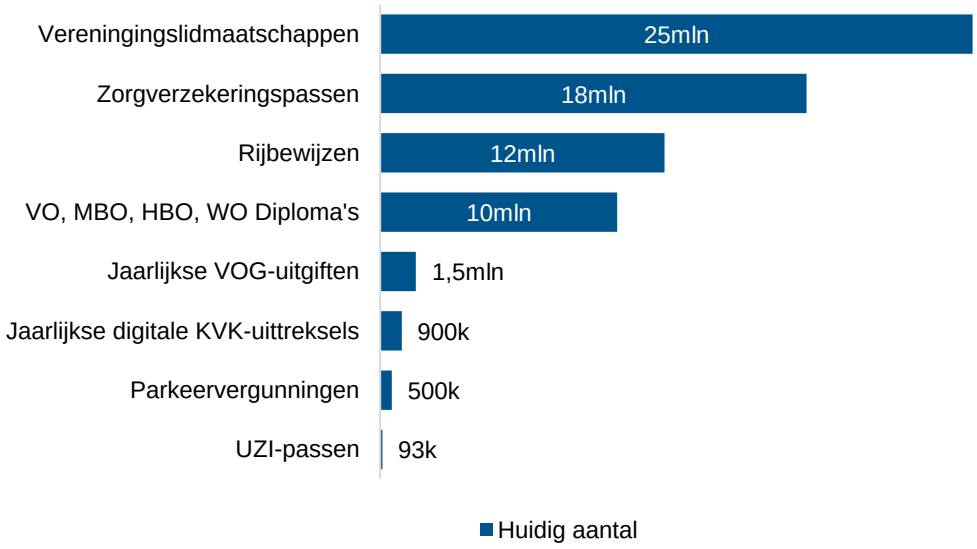
Duidelijkheid over authentieke bronnen en schema providers belangrijk voor gebruik
Voor het gebruik van een grootschalige (Q)EAA markt is duidelijkheid nodig over de betekenis van de term 'authentieke bron'. Welke partijen authentieke bronnen worden is nog onduidelijk. Het kan ook voorkomen dat meerdere partijen de authentieke bron zijn voor dezelfde datapunten. In Nederland zijn universiteiten een authentieke bron voor diploma's, maar ook DUO is een authentieke bron voor diploma's. Het is in het belang van overheden om een (Q)EAA ecosysteem te faciliteren.

Schema providers spelen een belangrijke rol bij de ontwikkeling van de (Q)EAA markt en per toepassingsgebied zal deze rol ingevuld moeten worden. Het is op dit moment nog onduidelijk wie deze rollen gaan vervullen. Schema providers voorzien in gezamenlijke standaarden, regels en taal voor specifieke attesteringen. Hierdoor ontstaat een uniform kader waarbinnen de attributen geverifieerd en uitgewisseld kunnen worden. Wanneer er een dergelijk gemeenschappelijk raamwerk ontbreekt dan zal dit het gebruik sterk limiteren. Een mogelijk probleem in de huidige opzet is dat de EDIW alleen technische interoperabiliteit vereist, maar er ook onduidelijkheid is over semantische interoperabiliteit.

De markt voor EAA's neemt toe vanwege nieuw gebruik
De EDIW opent ook een weg voor het delen van attesteringen die nu nog niet online worden gedeeld. Denk hierbij bijvoorbeeld aan het bewijzen van een lidmaatschap of loyaliteitscampagnes. Hier is het delen van attesteringen via de EDIW een toegevoegde waarde die partijen aan hun klanten/leden kunnen bieden. Het online delen van deze data gebeurt nu vaak nog niet door hoge kosten, beperkt bereik of een beperkte klantervaring. De EDIW is hiervoor een specifieke oplossing voor kleinere lokale ondernemingen. Daarnaast ontstaan er mogelijk nieuwe toepassingen door technologische innovatie die nog niet zijn voorzien.

Al deze ontwikkelingen gezamenlijk brengen de verwachting tot stand dat er een aanzienlijk nieuwe Europese voor (Q)EAA's gaat ontstaan. **Figuur 31** voorziet in kwantificering van slechts een beperkt aantal voorbeelden van huidige attesteringen bevat die direct de potentie van deze markt inzichtelijk maakt.

Figuur 31: De markt voor QEAA's en EAA's kan zich ontvouwen tot een zeer omvangrijke nieuwe markt.



5.7. Elektronische archiefdiensten

Het is niet de verwachting dat het gebruik van (gekwalificeerde) elektronische archiveringsdiensten of (Q)E-Archiving een vlucht gaat nemen. De verwachting is dat de huidige gebruikers van e-Archiving diensten niet significant over zullen stappen naar de QE-Archiving door gebrek aan toegevoegde waarde. Daarnaast is er geen verplichting voor het gebruik voorzien.

Gebruik QE-Archiving neemt geen vlucht, vanwege gebrek aan toegevoegde waarde

Door verdere digitalisering is een toename in het aantal e-Archiving diensten te verwachten. Meer en meer archieven zullen in de toekomst worden gedigitaliseerd. Met e-Archiving diensten ontstaat er een onafhankelijke partij die de geldigheid van het archief garandeert. Voor de publieke sector en waarschijnlijk een groot deel van de private sector is de verwachting dat zij dit in eerste instantie intern trachten te organiseren. Er bestaat echter een kans op groei van deze markt, specifiek voor private partijen, wanneer blijkt dat zij met hun interne systemen onvoldoende in staat zijn de integriteit van hun bestanden en de daaraan verbonden certificaten te waarborgen.

De toegevoegde waarde van QE-Archiving ten opzichte van e-Archiving is een hoger niveau van veiligheid en de rechtsgeldigheid[51]. Daarnaast moeten door één lidstaat erkende QE-Archiving dienst ook erkend worden door alle anderen lidstaten.

De verwachting is dat deze elementen op zichzelf onvoldoende zijn om de huidige markt van e-Archiving te bewegen naar QE-Archiving, omdat de toegevoegde waarde niet voldoende is voor de meeste toepassingen. De extra eisen zorgen daarmee in veel gevallen alleen voor een meer kostbare dienst. QTSP's verwachten dat de meeste klanten zullen kiezen voor de niet gekwalificeerde dienst.

De groei van de markt van QE-Archiving zal om bovenstaande reden waarschijnlijk afhangen van eventuele nationale of Europese verplichting tot het gebruik ervan. De revisie van eIDAS bevat *geen* verplichting van dien aard.

5.8. Elektronische grootboeken

De verwachting is dat, op de korte termijn, de markt voor QELedger een zeer gering aantal aanbieders heeft en dat het gebruik laag is. De redenen hiervoor zijn het gebrek aan helderheid van de technisch invulling en onduidelijke juridisch kaders.

[51] eIDAS Artikel 24 & 45l

Onduidelijkheid over de gestelde eisen voor aanbieders van QELedgers en de QELedger zelf remt de opkomst van een nieuwe markt

Op dit moment is er onduidelijkheid over welke concrete voorwaarden er aan een leverancier van een QELedger en aan het product zelf worden gesteld. De eisen voor certificering moeten nog beschreven worden. In de eIDAS revisie is aangegeven dat deze eisen binnen 12 maanden beschikbaar moeten zijn. Het is echter nog onduidelijk of het mogelijk is om binnen deze termijn te komen tot voorwaarden die helder genoeg zijn voor audits van een certificerende instantie. Hierdoor is er een risico op uitstel of ontstaan mogelijk eisen die niet goed aansluiten bij toekomstige technologische ontwikkeling en ontwikkelingen van de markt.

In de interviews uitten betrokken partijen dat nadere detaillering nodig is betreft de definitie van de QTSP als leverancier van een QELedger. Afhankelijk van de inrichting van de technologie, bijvoorbeeld het gebruikte consensus mechanisme, zijn er verschillende entiteiten of rollen aan te wijzen die gezamenlijk zorgen voor het functioneren van een (Q)ELedger.

De geïnterviewde partijen gaven aan hier zelf ook nog geen beeld van te hebben. De definitie van een QTSP kan enorm nauw, maar ook enorm breed worden geformuleerd. In het geval van de nauwe definitie is de QTSP slechts die entiteit of entiteiten die de (Q)ELedger hebben ontwikkeld en monitoren. Echter, in een decentrale wereld waarin met behulp van open source software de (Q)ELedger wordt ontwikkeld en er potentieel grote aantallen (validator) nodes zijn, wordt het aanwijzen van die entiteiten heel complex. Om die ambiguïteit te omzeilen, is er de mogelijkheid om het begrip QTSP ruimer te interpreteren, bijvoorbeeld in het uiterste geval iedere entiteit die een dienst levert en hiervoor gebruik maakt van een QELedger is een QTSP. Dit wordt eveneens heel complex, omdat dan alle deelnemers van het netwerk QTSP zijn.

Op basis van de interviews is de verwachting dat de nauwe definitie van QTSP het meest waarschijnlijk is. Een mogelijke reden is dat controle over de QELedger één van de eisen voor certificering wordt. Wanneer dit het geval gaat zijn, dan betekent dit dat de term QELedger alleen verwijst naar zogenaamde ‘permissioned’ blockchains of netwerken. Daarin hebben één of meerdere partijen de controle en bepalen wie mag deelnemen en wie niet. In dat geval beperkt de eIDAS revisie het mogelijke aantal aanbieders van QELedgers tot een klein aantal partijen, namelijk overheid gedreven initiatieven, bijvoorbeeld EBSI, en private partijen die in staat zijn een eigen blockchain infrastructuur op te tuigen en te monitoren, zoals Microsoft, Amazone of IBM. Decentrale ecosystemen, zoals cryptovaluta (b.v. Bitcoin, Ethereum of Solana) en digitaal bezit met behulp van *non-fungible tokens* (NFT’s), komen dan waarschijnlijk niet in aanmerking voor het stempel QELedger.

Juridische complexiteit belemmert ontstaan van een markt

Een andere belemmerende factor voor gebruik van de QELedger is de juridische complexiteit. Onduidelijkheid over de aansprakelijkheid binnen een QELedger ecosysteem levert de belangrijkste juridische complexiteit. Momenteel is het onbekend hoe dit eruit gaat zien. Er is helderheid nodig over de aansprakelijkheid van de QTSP voor bijvoorbeeld illegale activiteiten op de QELedger zelf, illegale activiteiten die gebruik maken van de QELedger of de aansprakelijkheid in het geval van geschillen tussen deelnemers van de QELedger. De complexiteit van dit vraagstuk neemt toe wanneer er sprake is van meerdere entiteiten die gezamenlijk de QTSP zijn die de QELedger dienst leveren, omdat de aansprakelijkheid in die gevallen mogelijk niet evenredig verdeeld is. Zonder heldere specificaties hierover zal de markt voor QELedgers waarschijnlijk niet van de grond komen.

EDIW is een eventuele use case voor de QELedger

Een mogelijke use case voor (Q)ELedgers is de EDIW. Dit betreft het opslaan van gegevens rondom de uitgifte en het terugtrekken van elektronische attesteringen van attributen. Daarbij zouden bijvoorbeeld DID’s, issuer credential definitions, schema’s en revocatie updates in een decentraal grootboek kunnen worden opgeslagen, zoals bijvoorbeeld bij Sovrin het geval is[52].

Er is echter nog geen consensus over de toegevoegde waarde van deze toepassing ten opzichte van gecentraliseerde methoden. De specificatie van de EDIW, (Q)EAA en (Q)ELedger is op dit moment technologieneutraal beschreven en laat beide vormen toe. Verschillende marktpartijen geven aan dat zij deze toepassing niet haalbaar achten, mede door de weerstand in sommige landen voor het gebruik van blockchain voor de EDIW. Daarnaast is voor deze use case ook nadere precisering van een

[52] https://sovrin.org/faqs/

QELedger ecosysteem nodig, bijvoorbeeld over wie gemachtigd is de informatie van DID's, issuer credential definitions, schema's en revocatie updates aan te leveren. Dit alles tezamen maakt dat deze mogelijkheid voorlopig niet waarschijnlijk is.

6. Kostenanalyse

De kostenanalyse bevat de relevante kosten voor vertrouwensdienstverleners die het gevolg zijn van de eIDAS revisie. Hierbij wordt gekeken naar het verschil tussen eIDAS en de eIDAS revisie. Veranderingen in gebruik die niet gedreven worden door de eIDAS revisie, zoals marktomstandigheden, andere wet- en regelgeving (bijv. GDPR, PSD2/PSR), worden buiten beschouwing gelaten. Er kan onderscheid worden gemaakt tussen twee typen kosten:

1	**Regeldrukkosten:** kosten die vertrouwensdienstverleners maken om compliant te zijn als gevolg van nieuwe of gewijzigde eisen die voortvloeien uit de eIDAS revisie.
2	**Boetes gerelateerd aan de eIDAS revisie:** Boetes voor het niet voldoen aan de wetgeving.
3	**Marktadaptatiekosten:** kosten die vertrouwensdienstverleners maken door een veranderende markt als gevolg van de eIDAS revisie, zoals een toegenomen vraag.

In de volgende paragrafen zullen deze kosten gedetailleerd worden toegelicht.

6.1. Regeldrukkosten

Volgens het Handboek Meting Regeldrukkosten zijn regeldrukkosten “die kosten die bedrijven (en burgers) maken om verplichtingen uit wet- en regelgeving correct na te leven en alle voorschriften op te volgen”[53]. De eIDAS revisie verhoogt de regeldruk voor QTSP’s. Er zijn in dit verband twee onderdelen aan te wijzen:

1. Regeldruk om QTSP te worden en te blijven
2. Regeldruk gerelateerd aan specifieke gekwalificeerde vertrouwensdiensten

6.1.1. Regeldruk om QTSP te worden en te blijven

De belangrijkste factoren die de regeldruk verhogen hebben niet alleen met kosten te maken, maar ook met een tijdselement. QTSP’s lopen het risico dat het langer duurt dan gewenst om compliant worden met de eIDAS revisie. In de paragrafen hieronder worden de belangrijkste factoren toegelicht.

Kosten stijgen voor organisaties om compliant te worden en te blijven

De eIDAS revisie stelt verschillende additionele eisen aan QTSP’s ten opzichte van eIDAS1. Hierdoor zijn bestaande en nieuwe (Q)TSP’s verplicht om nieuwe interne processen op te tuigen om compliant te blijven. Daarbij zijn de compliance kosten om QTSP te worden hoger dan de kosten voor bestaande QTSP’s om gekwalificeerd te worden voor een nieuwe dienst.

Marktpartijen gaven aan significante kosten te verwachten voor het aanpassen van interne processen om compliant te zijn/blijven. **Figuur *32*** bevat een aantal voorbeelden van wijzigingen met impact, in meer of mindere mate, op de regeldrukkosten. Regeldrukkosten die toenemen worden besproken in de tekst hieronder. De identiteitsvaststelling voor qualified certificates wordt besproken in paragraaf 6.1.2.

Figuur 32: Verschillende wijzigingen vergroten de compliance druk voor QTSP’s (niet uitputtend).

	Wijzigingen in eIDAS	Van toepassing op TSP’s	Van toepassing op QTSP’s	Regeldrukkosten
1	Bepaalde eID-services moeten waar toepasselijk ook offline toegankelijk zijn (art. 3)	✓	✓	➡
2	Verplichting om dienstverlening beschikbaar en toegankelijk te maken voor mensen met beperkingen (art. 15)	✓	✓	➡

[53] Handboek Meting Regeldrukkosten, 2023

3	Niet-gekwalificeerde TSP's moeten maatregelen nemen om risico's te mitigeren (art. 19a) t.a.v.: • Registratie en onboarding voor een dienst • Procedurele en administratieve controles om een TS aan te bieden • Beheer en implementatie van een TS	✓	✗	➡
4	Meldplicht aan toezichthouder bij incidenten binnen 24 uur (art. 19b, 24)	✓	✓	➡
5	Gekwalificeerde diensten en producten in één lidstaat moeten ook in andere lidstaten als zodanig worden erkend (art. 24a)	✗	✓	➡
6	Identiteitsvaststelling voor Qualified Certificates (QWAC, QESig, QESeal) en QEAA op niveau hoog (art. 24)	✗	✓	↗
	✓ = van toepassing = ✗ niet van toepassing			
	➡ = Geen aanzienelijke verandering in regeldrukkosten			
	↗ = Stijging in regeldrukkosten			

Een belangrijke eis, voortkomend uit artikel 15, is dat diensten verplicht moeten voldoen aan de 'Accessibility Act'. Dit houdt in dat QTSP's verplicht zijn hun diensten toegankelijk te maken voor mensen met een beperking. Een voorbeeld van zo'n aanpassing is de implementatie van voorleesfuncties. De Europese commissie schat in dat in 2020 Europese bedrijven voor €20 miljard aan kosten maakten gerelateerd aan het voldoen aan toegankelijkheidseisen[54].

Voor QTSP's zijn er initiële en terugkerende kosten gerelateerd aan de toegankelijkheidseis. Initiële kosten omvatten de extra investeringen die benodigd zijn om de producten en/of diensten zo te ontwerpen of in te richten dat deze voldoen aan de toegankelijkheidseis. Terugkerende kosten omvatten kosten die gemaakt worden bij het aanbieden/leveren van de dienst en daarbij het ondersteunen van mensen met een beperking. Voor beide gevallen worden hogere kosten verwacht maar er is nog een grote mate van onzekerheid.

Vertrouwensdienstverleners geven verder aan dat ze op dit moment voor een aantal van hun diensten al moeten voldoen aan toegankelijkheidseisen (zoals de Web Accessibility Directive[55] en ETSI EN 301 549). Ze hebben hierop hun diensten aangepast, of maken gebruik van 'third parties' om te voldoen aan de eisen (bijv. het mogelijk maken dat VoiceOver van Apple gebruikt kan worden voor hun diensten). Om deze redenen verwachten meerdere QTSP's niet dat deze eis grote problemen zal opleveren.

Echter gaat de European Accessibility Act nog wat verder dan de eerdergenoemde Directive en hiervoor wordt een vernieuwde ETSI-norm geschreven. Dit kan leiden tot extra implementatiekosten.

Naast de Accessibility Act kampen QTSP's met een hoge regeldruk, bijvoorbeeld de *Network and*

[54] EC, 2021
[55] EC, 2016

information security directive, oftewel de NIS2-richtlijn. Deze door de Europese Unie vastgestelde richtlijnen zijn bedoeld om verbetering aan te brengen in de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten. Ook moeten QTSP's momenteel voldoen aan *European Technical Standard Institute*, ook wel ETSI-normen, die ontwikkeld zijn voor het garanderen van interoperabiliteit. De verwachting is dat de trend van steeds verdergaande compliance doorzet. Dit is een generieke trend en QTSP's verwachten in de toekomst aan nog meer normen te moeten voldoen. Dit leidt tot een toename in de kosten gerelateerd aan regeldruk voor QTSP's. Dit maakt het voor (kleinere) QTSP's uitdagender om de kosten die gepaard gaan met de regeldruk te dragen. Daarnaast uitten een deel van de deelnemers aan dit onderzoek de wens voor harmonisatie van alle verschillende standaarden waar zij aan moeten voldoen en de centralisatie van het toezicht erop met als doel kosten te besparen door dubbele audits voor vergelijkbare eisen te voorkomen.

Regeldrukkosten nemen toe omdat QTSP's ook moeten voldoen aan eisen van andere normen en standaarden voor specifieke vertrouwensdiensten

QTSP's moeten zich houden aan veel eisen, niet alleen met betrekking tot eIDAS. Een voorbeeld hiervan is de normen en standaarden van QWAC's. Wanneer QTSP's QWAC's willen uitgeven, moeten zij niet alleen voldoen aan de normen van ETSI (ETSI EN 319 411), maar ook aan de vereisten opgelegd door webbrowsers. Dit betekent dat QTSP's niet uitsluitend door de RDI worden gecertificeerd, maar ook door andere instanties. Een voorbeeld hiervan zijn de WebTrust for Certification Authorities criteria, uitgegeven door de WebTrust for Certification Authorities Task Force. Hoewel deze twee certificeringen in theorie alternatieven voor elkaar zijn, blijkt uit de praktijk dat QTSP's vaak beide certificeringen behalen. Daarnaast wordt van een QTSP verwacht dat zij voortdurend updates volgen via blogs en de community in de gaten houden op bugs om verbeteracties uit te voeren. Dit vereist een constante inspanning op het gebied van compliance, geen eenmalige of jaarlijkse taak. Grote organisaties kunnen deze last dragen, maar kleinere organisaties kunnen moeite hebben om hun bedrijfsmodel rendabel te maken.

Overige kosten zijn geen showstoppers

Naast de kosten om compliant te zijn/blijven, vormen externe audits, die elke twee jaar plaatsvinden, een andere belangrijke kostenpost. Dit proces omvat een (her)certificeringsaudit in het ene jaar en een controleaudit in het volgende jaar. De (her)certificering omhelst een volledige audit, terwijl de controleaudit beperkter is. Een uitzondering hierop vormen de audits voor QWAC's, waarvoor webbrowsers jaarlijks een volledige audit vereisen. Hoewel externe audits kosten met zich meebrengen, worden ze niet gezien als de grootste financiële last voor QTSP's.

Een initiële audit voor het verkrijgen van de gekwalificeerde status kost aan interne kosten tussen de €12.000 en €25.000 (in het beste geval), afhankelijk van de grootte van het bedrijf, in welk land het bedrijf de audit uitvoert, en voor welke gekwalificeerde vertrouwensdienst de certificering aangevraagd wordt[56]. Dit bedraagt de kosten die vertrouwensdienstverleners intern maken voor het aanleveren van de gevraagde bewijslast (bijv. documentatie). Naast deze interne kosten moet ook de CAB betaald worden voor het uitvoeren van de certificering. Deze kosten worden geschat op € 12.000 tot € 25.000.

De geschatte initiële audit kosten voor het verkrijgen van gekwalificeerde status voor een vertrouwensdienst bedragen dus ongeveer €24.000 tot € 50.000 (zie **Figuur *33***).

Figuur 33: De initiële audit kosten voor QTSP's liggen tussen de €24.000 en €50.000 (illustratief).

Beschrijving	Aannames kosten	Totaal
Interne ondersteuning	20 – 40 persoonsdagen Gemiddeld uurtarief: €77[57]	€ 12.000 - € 25.000
Externe kosten audit CAB	10 – 20 persoonsdagen[58] Gemiddeld uurtarief: €150	€ 12.000 - € 25.000
Totaal kosten initiële audit		**€ 24.000 - € 50.000**

[56] EY, 2021
[57] Handboek Meting Regeldrukkosten, 2023
[58] EY, 2021

Voor grote ondernemingen zullen de kosten voor audits hoger liggen, doordat een uitgebreider deel van de organisatie en de processen geëvalueerd moet worden. Bovendien vereist elke afzonderlijke vertrouwensdienst zijn eigen certificering.

Naast de initiële kosten voor het verkrijgen van de gekwalificeerde status zijn er ook periodieke kosten voor het behouden van de gekwalificeerde status. eIDAS schrijft voor dat er minimaal één keer per twee jaar een audit gedaan wordt door de CAB om te evalueren of er nog voldaan wordt aan de vereisten. In de praktijk worden deze audits vaak één keer per jaar uitgevoerd. De kosten hiervoor zijn volledig voor rekening van de QTSP. Aan interne kosten moet men gemiddeld rekening houden met €20.000 tot €25.000 (0,2FTE). Daarnaast zijn ook hier kosten die de CAB in rekening brengt van toepassing: deze kosten worden geschat op €6.000 tot €12.000.

Totale periodieke kosten voor het behouden van gekwalificeerde status bedragen dus ongeveer €26.000 tot €37.000 per jaar, afhankelijk van de grootte van het bedrijf en de betreffende vertrouwensdienst (zie **Figuur *34***).

Figuur 34: Periodieke audit kosten voor QTSP's liggen tussen de tussen de €26.000 en €37.000 (illustratief).

Beschrijving	Aannames kosten	Totaal
Interne ondersteuning	30 – 40 persoonsdagen (0,2 FTE) Gemiddeld uurtarief: €77[59]	€ 20.000 - € 25.000
Externe kosten audit CAB	5 – 10 persoonsdagen[60] Gemiddeld uurtarief: €150	€ 6.000 - € 12.000
Totaal kosten periodieke audit per jaar		**€ 26.000 - € 37.000**

Verschillende QTSP's hebben echter aangegeven dat deze kosten voor een groot bedrijf met complexe vertrouwensdiensten of processen snel kunnen oplopen tot meer dan €100.000 per jaar.

Inclusief de initiële investering komen de totale certificeringskosten voor het aanbieden van een gekwalificeerde vertrouwensdienst over een periode van vijf jaar daarmee uit op ongeveer €150.000 tot €240.000.

Er is een risico op vertragingen waardoor QTSP's niet op tijd gecertificeerd kunnen worden
Het aantal auditors dat gekwalificeerd is om de vereiste audits voor QTSP's uit te voeren, is beperkt. Dit kan leiden tot mogelijke vertragingen omdat auditors niet onmiddellijk beschikbaar zijn om op aanvragen te reageren. Als gevolg hiervan kunnen QTSP's genoodzaakt zijn te wachten voordat ze nieuwe diensten kunnen lanceren. Dit kan ook een voorsprong bieden aan QTSP's die als eerste gecertificeerd worden, waardoor zij een voortrekkersrol kunnen spelen in nieuwe markten, zoals die van (Q)EAA's.

Daarnaast kunnen vertragingen verergeren door de gelijktijdigheid van het in kracht treden van de eIDAS revisie, het schrijven van de uitvoeringshandelingen, het auditen van QTSP's en het accreditatie proces van de auditor zelf. De eIDAS revisie gaat naar verwachting halverwege april 2024 van kracht[61]. De uitvoeringshandelingen, waarin nadere technische specificaties voor certificering zijn opgenomen, zijn op dit moment nog niet bekend. De uitvoeringshandelingen zijn nodig voor auditors om een adequate audit uit te voeren. Er ontstaat een overbruggingsperiode waarin zaken naast elkaar plaatsvinden waardoor vertragingen kunnen oplopen:

1. Auditors moeten zelf geaccrediteerd worden bij de RvA[62] voor de nieuwe vertrouwensdiensten terwijl er tegelijkertijd ook organisaties gecertificeerd willen worden voor deze nieuwe vertrouwensdiensten.

[59] Handboek Meting Regeldrukkosten, 2023
[60] EY, 2021
[61] Afhankelijk van EU tijdslijnen
[62] Raad voor Accreditatie

2. Auditors en toezichthouders moeten de uitvoeringshandelingen interpreteren om een goede audit en assessment uit te voeren. Echter zijn de uitvoeringshandelingen waarschijnlijk nog niet klaar terwijl de eIDAS revisie al wel van kracht is.

Door deze overbruggingsperiode kunnen QTSP's vertraging oplopen in het certificeringsproces.

6.1.2. Regeldruk gerelateerd aan specifieke gekwalificeerde vertrouwensdiensten

Voor specifieke vertrouwensdiensten neemt de druk om aan regelgeving te voldoen verder toe. Dit is deels te wijten aan de nieuwe vereisten die worden geïntroduceerd door de eIDAS revisie en deels doordat deze vertrouwensdiensten zich niet alleen onder eIDAS moeten certificeren, maar ook moeten voldoen aan eisen van andere partijen.

De verwachting is dat alleen SAM certificering extra kosten met zich meebrengt voor QES

De eIDAS revisie introduceert nieuwe eisen voor QSCDs die op afstand beheerd worden. QTSP's geven aan dat de compliance druk gaat stijgen omdat niet alleen de Hardware Security Module (HSM) gecertificeerd moet worden, maar ook de Signature Activation Module (SAM). De inschatting van QTSP's is dat de additionele kosten van dergelijke certificering op kan lopen tot honderdduizenden euro's. Een QTSP kan ervoor kiezen een dergelijke module te kopen, maar dit is eveneens zeer kostbaar.

Daarnaast gelden er nog extra vereisten in de eIDAS revisie voor gekwalificeerde elektronische handtekeningen:

- QESigs moeten informatie bevatten over de geldigheid van het certificaat, of een locatie aangeven waar deze status opgevraagd kan worden
- Voor 'advanced electronic signatures based on qualified certificates' moeten er additionele checks gedaan worden, zoals: 'was het certificaat echt gekwalificeerd', 'was het certificaat geldig op het moment van ondertekenen', 'komt de data overeen met wat je tekent', etc.
- Voor handtekeningen in de wallet gelden er specifieke eisen aan het format waarin de data uitgegeven wordt (bijv. JOSE (JWT) en COSE)

De verwachting is dat dat deze eisen niet tot extra kosten leiden, omdat veel QTSP's al voldoen aan deze eisen of eenvoudig aanpassingen kunnen doorvoeren.

Kosten stijgen voor QTSP's die nog niet op het Level of Assurance (LoA) hoog zitten voor de identiteitsvaststelling bij QWAC's, QES en QESeals

Artikel 24 in de eIDAS revisie schrijft voor dat de identiteit van degene aan wie de gekwalificeerde vertrouwensdienst (voor QEAA's, QWAC's, QES, en QESeals) geleverd wordt en hun attributen moet geverifieerd worden met LoA hoog. Dit betekent dat QTSP's, die momenteel een substantieel LoA hanteren, extra inspanningen en kosten moeten leveren om hun niveau te verhogen naar hoog. Het voordeel van deze eis is dat het zorgt voor harmonisatie binnen Europa, waardoor er een gelijker speelveld ontstaat. LoA hoog kan behaald worden met een van de volgende methodes:

- EDI Wallet of een eID-scheme
- QESig/QESeal certificaat
- Ander LoA High identificatiemiddel, mits goedgekeurd door de CAB
- Fysieke aanwezigheid van de persoon/vertegenwoordiger van de rechtspersoon

Voor bestaande processen waar nog veel gebruik gemaakt wordt van face-to-face controle is de introductie van de wallet (als identificatie middel op afstand) een wijziging waarmee operationele kosten kunnen worden beperkt. Daarnaast zorgen deze EU-breed geaccepteerde middelen ervoor dat men niet voor elk land een nieuw proces hoeft op te tuigen afhankelijk van wat lokaal beschikbaar is (bijv. iDIN in NL, Itsme in België). Momenteel kunnen toezichthouders in verschillende EU-lidstaten uiteenlopende eisen stellen aan de verificatie. De verwachting is daarmee dat de regeldrukkosten door deze eis juist zullen dalen voor bepaalde operationele processen. Dit is wel afhankelijk van de operationele kosten voor bijvoorbeeld het gebruik van de EDIW. Als de kosten voor een QTSP om gebruik te maken van de authenticatie met de EDIW te kostbaar wordt, is het mogelijk niet rendabel voor dienstverleners.

6.2. Boetes gerelateerd aan eIDAS

Een significante wijziging in eIDAS is gerelateerd aan boetes voor het niet voldoen aan de wetgeving. In de eIDAS revisie stelt de Commissie de ondergrens voor de maximum boetebedragen vast[63]:

- Voor natuurlijke personen: maximumboete minimaal € 5.000.000
- Voor rechtspersonen als vertrouwensdienstverlener: maximumboete minimaal € 5.000.000 of 1% van wereldwijde omzet

Een minimaal maximum betekent dat lidstaten zelf kunnen besluiten een hoger maximum boetebedrag vast te stellen, maar dat deze minimaal zo hoog moet zijn als aangegeven door de Commissie. In eIDAS1 waren geen sancties opgenomen bij niet voldoen aan de wetgeving, nationale overheden zijn vrij die zelf te bepalen. In de praktijk worden nu nauwelijks sancties opgelegd. Uit de vergelijking met AVG/ blijkt dat de vrees voor hoge boetes een sterk zelfregulerend effect heeft, en dat met name grote partijen in zaken met veel media-aandacht stevige boetes krijgen om dit effect te versterken.
In veel gevallen is er bij het bekend worden van overtreding van de wetgeving al grote schade ontstaan aan het vertrouwen in de dienstverlener, met bijbehorende grote gevolgen op de marktpositie.

Naast het opvoeren van sancties wordt in de eIDAS revisie ook specifiek aangegeven dat klanten van QTSP's bij het niet nakomen van de regelgeving het recht hebben de door hen geleden materiele en immateriële schade op QTSP's te verhalen[64]. Het introduceren van deze boeterichtlijnen kan potentieel grote gevolgen hebben voor vertrouwensdienstverleners.

6.3. Marktadaptatiekosten

In hoofdstuk 5 is beschreven welk effect de eIDAS-revisie heeft op de vertrouwensdiensten, waaronder het effect op de vraag. Als de vraag voor deze diensten toe- of afneemt, heeft dit waarschijnlijk ook gevolgen voor de kosten voor het aanbieden voor vertrouwensdienstverleners. De verwachting is dat, onder de huidige situatie, een toename van de vraag niet direct zal leiden tot extra disproportionele kosten of grote noodzakelijke investeringen. Het merendeel van de diensten is schaalbaar ingericht en zal een normale vraagstijging goed aankunnen. Daarnaast is de stijging van kosten evenredig met de stijging in omzet.

Echter, bij een echt significante vraagstijging (certificaten voor handtekeningen) zullen er wel significante investeringen en herinrichting (denk aan hardware, kennis, cloudcapaciteit en automatisering) van de organisaties nodig zijn. Op dit moment is er een beperkt aantal partijen op de markt actief die voorbereid zijn op een dergelijke schaalvergroting. Een aantal kleinere partijen hebben beperkte teamcapaciteit of maken gebruik van handmatige processen en zijn dus minder goed voorbereid op een grote verandering van de vraag. Dit betekent dat zij significante investeringen zullen moeten doen om te kunnen schalen, bijvoorbeeld in extra hardware of klantenservice. Het is onduidelijk of dit haalbaar is voor deze partijen.

Daarnaast is er een onderscheid in de marktadaptatiekosten tussen verschillende bestaande diensten.

QTimestamps, QERDS, QEArchiving

Voor deze diensten wordt geen grote verandering in vraag verwacht (zie hoofdstuk 5) en zullen er dus zeer waarschijnlijk geen extra kosten gemaakt hoeven te worden. Vertrouwensdienstverleners van deze diensten moeten echter wel blijven investeren om relevant te blijven en ook een veranderende vraag in de toekomst te kunnen blijven leveren.

QESeals, QWAC's

Voor deze diensten zijn de marginale kosten relatief hoog, wat betekent dat de schaalbaarheid laag is en extra investeringen/kosten benodigd zijn om het potentieel van de extra vraag te kunnen realiseren. Dit is met name omdat identificatieproces voor deze diensten nog grotendeels fysiek voltrokken wordt. Zoals eerder besproken is in de eIDAS-revisie wel toegevoegd dat deze processen ook ondersteund kunnen worden door bijvoorbeeld de EDIW, waarbij de verwachting is dat dit tot operationele kostenbesparingen zal leiden.

[63] eIDAS, artikel 16
[64] eIDAS, art 13.1

QESigs

Voor deze diensten is de verwachting dat de schaalbaarheid ervoor zorgt dat de gemiddelde kosten zullen afnemen, doordat er grotere volumes zullen ontstaan en de kosten dus verspreid kunnen worden. De operationele kosten zullen evenredig meestijgen met de stijgende omzet. Daarnaast is de verwachting van vertrouwensdienstverleners dat er beperkte extra investeringen benodigd zijn om potentieel van toegenomen vraag te realiseren.

Nieuwe diensten

Voor de implementatie van nieuwe diensten moeten bestaande (Q)TSP's extra investeringen doen. QTSP's nemen een terughoudende houding aan vanwege de onduidelijkheid doordat de uitvoeringshandelingen nog niet klaar zijn. Daarnaast is de businesscase voor QTSP's om de (Q)EAA dienst aan te bieden afhankelijk van de adoptiegraad van de EDIW, wat op dit moment nog erg onzeker is.

7. Verdienmodellen & Concurrentieanalyse

Voor (Q)Timestamps en (Q)ERDS zijn er geen noemenswaardige specifieke gevolgen voor de verdienmodellen door de eIDAS revisie. Voor (Q)ESeals en (Q)WAC's kunnen er nieuwe omzetstromen ontstaan rondom de EDIW, waardoor bestaande verdienmodellen meer duurzaam worden. De verdienmodellen komen mogelijk wel onder druk te staan door hoge regeldrukkosten, zie hoofdstuk 6.

Voor elektronische handtekeningen ontstaan nieuwe verdienmodellen door de eIDAS revisie. Van de nieuwe vertrouwensdiensten zullen de verdienmodellen voor elektronische attesteringen van attributen de meeste impact hebben op de markt. Daarnaast is de verwachting dat er veel concurrentie op deze markt zal ontstaan.

In zijn algemeenheid ontstaat er steeds meer concurrentie op de markt voor vertrouwensdiensten, onder andere door het ontstaan van een Europese markt. Deze trend is al zichtbaar en zal zich in de komende jaren doorzetten.

Voor alle vertrouwensdiensten geldt dat de waarde van gekwalificeerd t.o.v. niet-gekwalificeerd beperkt wordt herkend. Het gebruik van gekwalificeerde diensten wordt niet juridisch afgedwongen en er is veel ruimte voor niet-gekwalificeerde diensten. Hierdoor staan de verdienmodellen voor gekwalificeerde diensten in zijn algemeenheid onder druk.

7.1. Nieuwe verdienmodellen voor elektronische handtekeningen

Het verdienmodel voor het zetten van handtekeningen is aan het verschuiven van een procesgerichte aanpak naar een middelgerichte aanpak. Hierin is het onderscheid tussen geavanceerde en gekwalificeerde handtekeningen belangrijk. Zoals beschreven is de huidige markt voor gekwalificeerde handtekeningen in Nederland beperkt tot beroepscertificaten. De verdienmodellen hiervoor zullen beperkt veranderen.

In het huidige verdienmodel voor geavanceerde handtekeningen betalen bedrijven een QTSP voor het gehele proces van het zetten van geavanceerde handtekeningen. Bij de introductie van de EDIW met een certificaat voor elektronische handtekeningen is dit proces niet meer nodig en komt er hiervoor een ander verdienmodel voor in de plaats. Het huidige verdienmodel zal dan gedeeltelijk wegvallen.

Hiernaast ontstaat er een nieuw verdienmodel voor QTSP's voor de uitgifte van certificaten voor elektronische handtekeningen aan de EDIW. Vanwege de verplichting dat elke lidstaat een EDIW moet aanbieden zal de overheid waarschijnlijk de kosten hiervan op zich nemen. Omdat dit een bestaande markt is, is het moeilijk voor de overheid om te beargumenteren dat zij zelf QTSP moeten worden om deze certificaten uit te geven. De overheid zou dan optreden als marktpartij en om concurrentievervalsing te voorkomen, moet de overheid zich aan gedragsregels houden[65]. Als de overheid niet optreedt als QTSP zijn er globaal twee opties:

1. De overheid voert een aanbestedingsprocedure uit en selecteert één leverancier. Hiermee ontstaat er afhankelijkheid van één partij die deze dienst op zeer grote schaal moet aanbieden. Het is onduidelijk of dit voor alle huidige partijen in de markt haalbaar is.
2. De overheid voert één of meerdere aanbestedingsprocedures uit en selecteert meerdere leveranciers. Hierbij is standaardisatie en interoperabiliteit (zowel technisch als operationeel) een belangrijke randvoorwaarde.

Het winnen van één of meerdere aanbestedingen is daarmee waarschijnlijk het voornaamste verdienmodel voor vertrouwensdienstverleners voor de uitgifte van certificaten voor elektronische handtekeningen (voor burgers). Omdat er nu nog nauwelijks markt is voor burgercertificaten, is dit een nieuw verdienmodel voor vertrouwensdienstverleners.

Het gebruik van QES voor burgers voor niet professioneel gebruik moet gratis zijn. Er ontstaan verdienmodellen rondom het professioneel gebruik van QES. QTSP's kunnen dit waarschijnlijk goedkoper aanbieden, aangezien de kosten voor onboarding dalen (omdat de EDIW wallet hiervoor benut kan worden). Een neveneffect van de introductie van de EDIW is dat burgers vertrouwder raken

[65] Rijksoverheid

met het zetten van elektronische handtekeningen. Dit zal naar verwachting ook het gebruik van elektronische handtekeningen voor professioneel gebruik stimuleren.

7.2. Verdienmodellen voor elektronische attesteringen van attributen

De verwachting is dat er veel concurrentie op de markt voor de uitgifte van (Q)EAA ontstaat. De verwachting is dat veel authentieke bronnen dit proces zullen uitbesteden aan QTSP's. Op deze markt voor (Q)EAA's ontstaan twee soorten verdienmodellen: 1) Verdienmodellen voor authentieke bronnen die (Q)EAA's uitgeven en 2) verdienmodellen voor QTSP's die (Q)EAA-diensten leveren.

7.2.1. Concurrentie voor uitgifte van elektronische attesteringen van attributen

Vertrouwensdienstverleners die (Q)EAA-diensten leveren zullen deze diensten aanbieden aan authentieke bronnen om (Q)EAA's uit te geven. Authentieke bronnen hebben drie opties op (Q)EAA's uit te geven:

Authentieke bron als QTSP: Een authentieke bron besluit om zelf QTSP te worden om (Q)EAA's zelf uit te geven.

Authentieke bron met hulp van een QTSP: Een authentieke bron geeft (Q)EAA's uit met de hulp van een QTSP die (Q)EAA's mag uitgeven. Dit kan bijvoorbeeld via een uitbesteding of door de diensten van een QTSP in te kopen.

Vrije markt voor QTSP's: Een authentieke bron stelt de data beschikbaar en meerdere QTSP's kunnen (Q)EAA's uitgeven op basis van de beschikbaar gestelde data.

Voor overheidsinstanties is er een extra optie. Een overheidsinstantie kan, zolang ze de eisen van eIDAS volgen, zelf QEAA's uitgeven zonder QTSP te zijn (zogenoemde Public EAA's).

Het is onduidelijk welke optie voor welke overheidsinstantie het meest gewenst is. Het voordeel van het uitbesteden is dat aanvraag- en auditprocessen worden uitgevoerd door de QTSP en dat heel specifieke regeldrukkosten niet bij de overheid komen te liggen. Hierin is ook onderscheid mogelijk tussen de keuze voor het centraal uitgeven van alle (Q)EAA's door de overheid of om elke overheidsinstantie dit zelf te laten bepalen.

Wanneer bedrijven de beheerder zijn van een bron is het waarschijnlijk dat zij de uitgifte van (Q)EAA's uitbesteden, bijvoorbeeld een bank als bron voor de financiële data van klanten. In de meeste gevallen wordt verwacht dat de kosten voor het verkrijgen van de QTSP-status, enkel om eigen data uit te geven, niet opwegen tegen de voordelen. Een uitzondering op die regel kan zijn wanneer de beheerder van de bron zelfstandig de veiligheid en privacy van de gegevens wil handhaven en dus de controle erover niet afstaat.

Het is de verwachting dat er veel concurrentie op de markt voor QTSP's zal ontstaan. Op basis van de uitgevoerde interviews ontstaat het beeld dat veel partijen de intentie hebben om QTSP voor (Q)EAA's te worden. Hierdoor zullen QTSP's met elkaar concurreren om (Q)EAA-diensten te leveren aan authentieke bronnen.

De aansprakelijkheid voor de uitgifte van (Q)EAA's is onduidelijk en het is wachten op de Uitvoeringshandelingen voor meer helderheid. Desondanks blijft ook na deze nadere bepalingen een verschil bestaan tussen de juridische werkelijkheid en de dagelijkse praktijk. Het eigenhandig handelen van de betrokken partijen en het toezicht op die partijen zijn een grote factor in hoeverre de dagelijkse praktijk afwijkt van de juridische werkelijkheid.

7.2.2. Verdienmodellen voor QTSP's

Het meest voor de hand liggende verdienmodel voor de QTSP is een maandelijkse/jaarlijkse prijs die authentieke bronnen betalen voor het gebruik maken van de dienst van de QTSP, met mogelijk een variabele component voor het aantal attesteringen. Een QTSP zal waarschijnlijk Software Development Kits (SDKs) aanbieden aan authentieke bronnen om ervoor te zorgen dat de (Q)EAA-dienst naadloos aansluit op bestaande applicaties en producten van de authentieke bron. Dit vereist waarschijnlijk een

integratie (met maatwerk) tussen QTSP's en authentieke bronnen waar de QTSP. Het verdienmodel zal waarschijnlijk verschillen per authentieke bron omdat het ontsluiten van de data verschilt per bron. In sommige gevallen is er sprake van verplichte ontsluiting en in andere gevallen is het slechts een additionele dienst of compliance gedreven.

Een alternatief verdienmodel betreft een gedeelde inkomstenstructuur tussen QTSP's en authentieke bronnen. Een voorbeeld hiervan is dat de omzet per uitgegeven (Q)EAA tussen de QTSP en authentieke bron wordt gedeeld.

Een derde verdienmodel betreft een afspraak tussen QTSP en authentieke bronnen waarbij de QTSP het recht koopt om de data van de authentieke bron te ontsluiten aan de wallet. Vervolgens dient de QTSP een verdienmodel te organiseren voor het gebruik van deze data door de relying party. Hiertoe moet de leesbaarheid van de attestering worden beperkt tot een set gecontracteerde relying parties. In dit model fungeert de QTSP als een reseller van gegevens van de authentieke bron. Dit inkomstenmodel is vooral geschikt voor waardevolle gegevens.

7.2.3. Verdien- en kostenmodellen voor authentieke bronnen

Afhankelijk van het type authentieke bron is er sprake van een verdienmodel of een kostenmodel. Het openstellen van de data van de authentieke bron brengt kosten met zich mee, voornamelijk in het opzetten en onderhouden van dit extra kanaal. Voor authentieke bronnen zijn er drie mogelijk verdien/kostenmodellen.

Optie 1: De holder/burger betaalt

Een optie voor authentieke bronnen is dat de holder/burger betaalt voor het verkrijgen van een (Q)EAA. Dit concept is niet nieuw. Burgers betalen momenteel al voor verschillende (overheids)diensten zoals het aanvragen van een *Verklaring Omtrent Gedrag* (VOG), een KVK-uittreksel, of een rijbewijs, zie **Figuur *35*** [66] [67].

Figuur 35: Burgers betalen momenteel ook al voor verschillende 'attesteringen'.

Hoewel dit geen innovatief verdienmodel is, kan het voor authentieke bronnen in de toekomst potentieel tot extra inkomsten leiden. Er kunnen nieuwe attesteringen ontstaan die waardevol genoeg zijn voor burgers, dat zij bereid zijn ervoor te betalen. Ook is het mogelijk dat deze attesteringen belangrijk genoeg zijn voor een relying party, waardoor deze partij bereid is de kosten te dekken voor de burger die de (Q)EAA aanvraagt. Dit laatste scenario komt vaak voor bij VOG-aanvragen die worden gedaan voordat werknemers in dienst treden, waarbij de werkgever uiteindelijk de kosten vergoedt.

Optie 2: De relying party betaalt

Een andere optie is dat de relying party betaalt voor het gebruik van attesteringen van authentieke bronnen. Hiertoe moet de leesbaarheid van de attestering worden beperkt tot een set gecontracteerde

[66] KVK, Justis, CBR
[67] N.B. Kosten voor rijbewijzen verschillen per gemeente, gemiddeld is dit €44,65

relying parties. De technische invulling van dit model is nog niet definitief. Waar het op neerkomt is dat een QTSP (zelf of in naam van een authentieke bron) iets uitgeeft dat alleen door gecontracteerde relying parties gebruikt kan worden.

In deze optie kan een authentieke bron ervoor kiezen om (Q)EAA's kosteloos aan holders/burgers uit te geven, maar een vergoeding te vragen aan relying parties die de (Q)EAA's van burgers willen gebruiken.

Optie 3: De authentieke bron betaalt
In dit scenario draagt de authentieke bron de kosten zelf of zijn deze kosten verwerkt in de prijs van een ander product. Een voorbeeld hiervan is wanneer de kosten voor een (Q)EAA van een diploma zijn opgenomen in het collegegeld.

7.3. Verdienmodellen voor elektronische grootboeken

Door de brede definitie van eLedgers worden er meerdere type verdienmodellen gehanteerd voor die dienst. Dit loopt van decentrale blockchains, als Bitcoin, Ethereum en Solana, die een fee rekenen per transactie, tot aan de traditionele financiële sector die onder andere werkt met subscriptiemodellen. Er valt voor eLedgers om die reden geen generiek verdienmodel aan te wijzen.

Zeer waarschijnlijk worden alleen permissioned netwerken geclassificeerd als QELedger. Voor die type grootboeken liggen periodieke verdienmodellen meer voor de hand. Permissioned netwerken zijn centrale grootboeken en zijn als dienst goed te vergelijken met andere SaaS-diensten in het feit dat je de dienst of software kan inkopen bij een centrale partij die vervolgens het beheer op zich neemt. Dit geldt niet voor decentrale grootboeken waar de veiligheid en bruikbaarheid van een netwerk wordt afgedwongen op basis van incentives en game-theorie op protocolniveau, denk bijvoorbeeld aan de beloningen voor het mijnen van een Bitcoin blok en de invloed van de halveringsperiodes[68] op het netwerk. Naast periodieke verdienmodellen kan ook een door de overheid gesubsidieerde QELedger een mogelijkheid zijn om de kosten ervan te dekken.

7.4. Verdienmodellen voor elektronische archiefdiensten

Voor (Q)EArchiving is een verdienmodel op basis van abonnement het meest logisch. Omdat hierbij een langere bewaarplicht speelt is een jaarlijkse fee, eventueel met een korting voor abonnementen met een langere tijdspanne.

Een andere mogelijkheid is dat er geen apart verdienmodel ontstaat voor (Q)EArchiving, maar dat er juist een aantal QTSP's ontstaan die fungeren als een one-stop-shop voor meerdere vertrouwensdiensten voor gebruikers. Hierbij is (Q)EArchiving een aanvullende dienst om de levensduur, leesbaarheid, integriteit en oorspronkelijkheid te waarborgen voor een langere periode. Hierin zal de schaal waarop QTSP's deze diensten aanbieden resulteren in schaalvoordelen en daarmee lage kosten.

7.5. Waarde van gekwalificeerde diensten wordt beperkt erkend

De waarde van gekwalificeerde diensten worden in Nederland nog beperkt erkend, zowel bij publieke als private partijen. Hierdoor zijn ook de huidige verdienmodellen voor gekwalificeerde diensten zeer beperkt met een zeer lage vraag naar deze diensten.

Het ontbreken van erkenning en herkenbaarheid leidt tot verwarring in de markt, wat misbruik van het eIDAS-vertrouwensicoon in de hand werkt. Ondanks dat het icoon beschermd is merken QTSP's dat er niet gekwalificeerde partijen zijn die het icoon gebruiken. Sommige organisaties tonen op hun website het 'trust services-icoon' en vermelden dat ze 'eIDAS-compliant' zijn. Eindgebruikers kunnen het verschil niet onderscheiden, waardoor gekwalificeerde diensten niet hun volledige potentieel bereiken.

In andere EU lidstaten worden gekwalificeerde diensten meer erkend, mede doordat het gebruik in sommige gevallen volgens nationale wetgeving verplicht is. Zo moeten in Italië alle facturen met een

[68] Om en nabij iedere 4 jaar halveert het aantal bitcoins dat in omloop wordt gebracht tot het maximum van 21 miljoen is bereikt. Elke vier jaar wordt de helft van de nog niet in omloop gebrachte bitcoins in omloop gebracht.

gekwalificeerde elektronische handtekening ondertekend zijn en moeten in Oostenrijk en Duitsland alle betaalterminals een gekwalificeerde elektronische zegel hebben. Door deze verplichting ontstaat er meer erkenning van gekwalificeerde diensten bij de meeste mensen, ook in zijn algemeenheid.

In Nederland wordt er op dit moment samengewerkt om deze erkenning en herkenning te verhogen via het samenwerkingsplatform Trusted Information Partners (TIP). TIP stelt partijen in staat om diensten te ontwikkelen waarmee alle burgers, bedrijven en overheden eenvoudig en betrouwbaar digitaal zaken met elkaar doen. Binnen TIP werken publieke en private partners samen en maken ze afspraken over het gebruik van open standaarden. De Belastingdienst en het Ministerie van BZK betrokken bij TIP[69].

7.6. Concurrentie neemt toe door het ontstaan van een Europese markt

Verwacht wordt dat er, mede door de verhoogde interoperabiliteit door de eIDAS revisie, een Europese markt voor vertrouwensdiensten ontstaat. Hierdoor wordt het voor Nederlandse vertrouwensdienstverleners eenvoudig om diensten aan te bieden in andere lidstaten. Daarnaast wordt het ook eenvoudig voor vertrouwensdienstverleners uit andere lidstaten om diensten aan te bieden in Nederland, wat leidt tot een toename van concurrentie op de Nederlandse markt. Er zullen waarschijnlijk minder nieuwe partijen proberen marktaandeel te veroveren in de verschillende vertrouwensdienstmarkten, omdat de hoge compliance druk ook werkt als een toetredingsbarrière.

Voor in ieder geval de markten voor QESeals en QES hebben dienstverleners uit andere lidstaten een voordeel ten opzichte van Nederlandse dienstverleners. Deze partijen kunnen dezelfde diensten aanbieden voor een fractie van de prijs van Nederlandse dienstverleners. Dit komt door de schaalvoordelen die deze partijen hebben behaald in andere lidstaten, sterke concurrentie in andere lidstaten, eenvoudigere wettelijke verplichtingen en meer duidelijkheid door toezichthouders. In Zuid-Europese landen is het gebruik van QESeals en QES in veel gevallen al verplicht.

Voor een deel komt dit voordeel te vervallen door strengere eisen onder de eIDAS revisie, zoals de noodzaak voor Level of Assurance hoog waaraan deze partijen uit andere lidstaten in veel gevallen nog niet voldoen. De verwachting is dat dit voordeel voor Nederlandse partijen te beperkt is voor het beperken van dit concurrentievoordeel van partijen uit andere lidstaten. De prijzen van deze partijen in andere lidstaten liggen in sommige gevallen 15 keer lager dan in Nederland.

In de Europese markt neemt het risico op 'shoppen' door QTSP's toe. Dit betekent dat QTSP's strategisch kiezen in welk land ze zich laten certificeren/kwalificeren om de kosten en inspanningen te verlagen, waardoor ze een sterkere concurrentiepositie in Europa kunnen opbouwen. Meerdere factoren kunnen deze strategische keuze beïnvloeden (niet uitputtend):

- **Kosten van een auditor:** Auditors moeten zelf ook geaccrediteerd zijn in Europa, en deze accreditatie verschilt per land en per raad van accreditatie. Hoe langer de accreditatieprocedure duurt, hoe meer het de auditor heeft gekost om geaccrediteerd te worden. Dit kan leiden tot hogere audit kosten voor QTSP’s.
- **Rol van de toezichthouder:** De wetten en normen bieden ruimte voor interpretatie, wat leidt tot verschillen in hoe toezichthouders deze normen interpreteren. Dit is vooral het geval wanneer er in normen, zoals ETSI, wordt verwezen naar 'Industry Best Practice'. Dit laat de beoordeling over aan zowel de industrie als de toezichthouders. Verschillen in inzicht tussen toezichthouders kunnen ertoe leiden dat het in sommige landen moeilijker en dus duurder is om als QTSP gecertificeerd te worden.

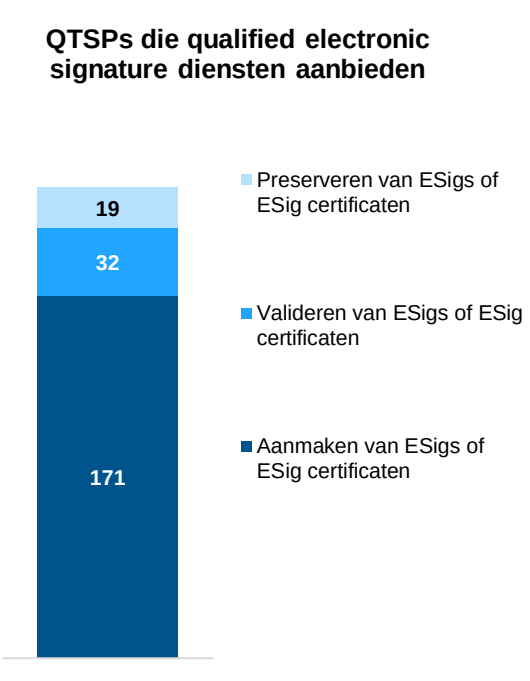
[69] Trusted Information Partners

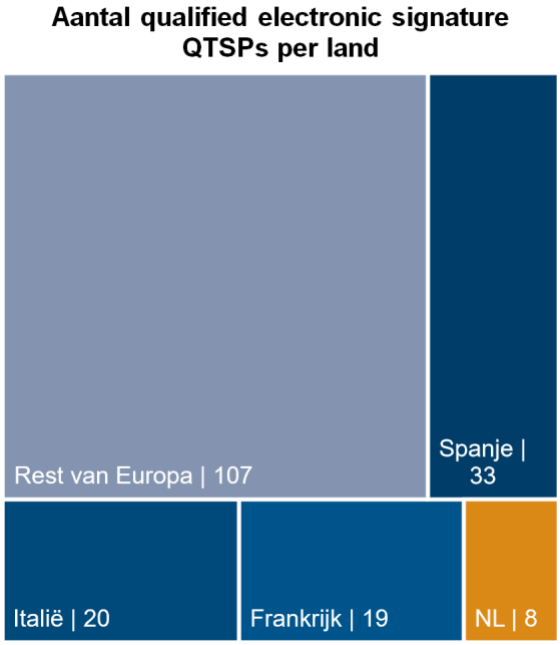
8. Appendix

8.1. Gekwalificeerde vertrouwensdiensten 1-pagers

8.1.1. Electronic signatures 1-pager

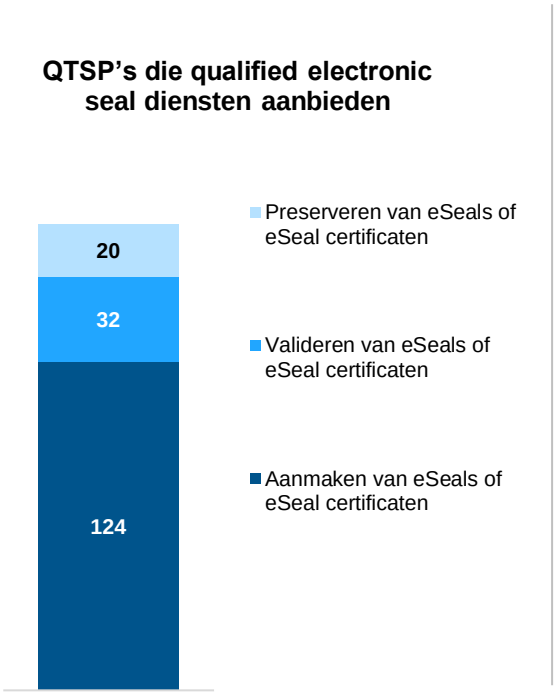
Naam	(qualified) electronic signatures
Afkorting	(Q)ES
eIDAS artikelen	3, 25 – 32, 32a, 33, 34, ANNEX I, ANNEX II
Deeldiensten	1. Aanmaken van eSig of eSig certificaat 2. Valideren van eSig of eSig certificaat 3. Preserveren van eSig of eSig certificaat 4. Beheer van middelen voor het zetten van elektronische handtekeningen op afstand
Definitie in eIDAS	'Elektronische handtekening zijn gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die dor de ondertekenaar worden gebruikt om te ondertekenen'
Doel	Het doel van een eSig is het scheppen van vertrouwen door de mogelijkheid van het digitaal ondertekenen van een document om daarmee de instemming van de ondertekenaar of specifiek de authenticiteit en integriteit van het document zelf te onderschrijven.
Nederlandse QTSP's die QES diensten aanbieden	1. CIBG 2. Cleverbase ID B.V. 3. Digidentity B.V. 4. KPN B.V. 5. Ministerie van Defensie 6. Ministerie van Infrastructuur en Waterstaat 7. NotarisID B.V. 8. QuoVadis Trustlink B.V.

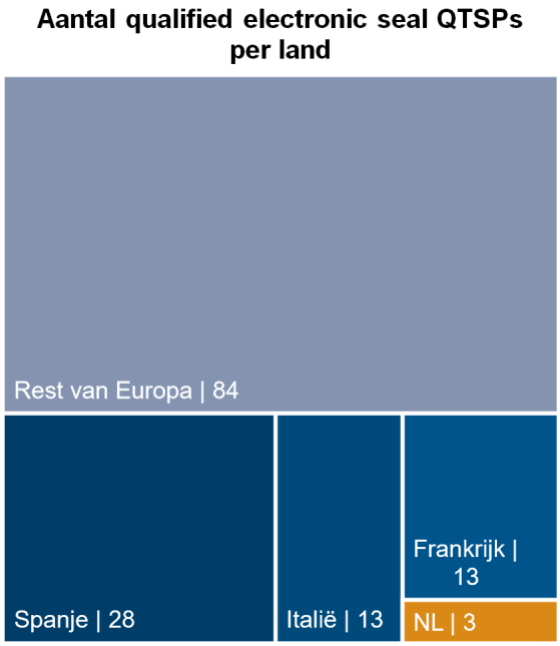




8.1.2. (Q)ESeal 1-pager

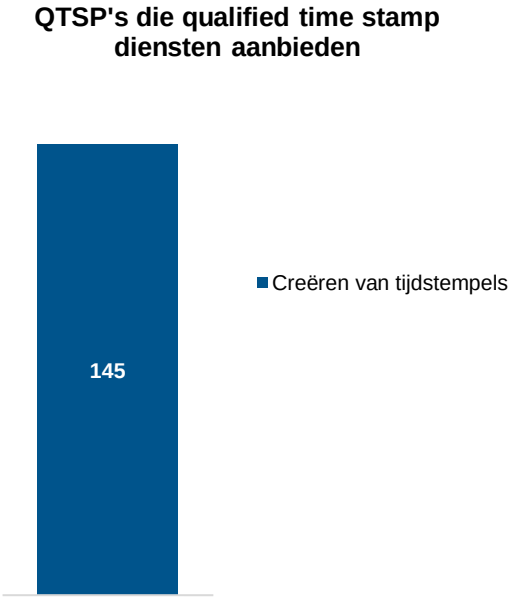
Naam	(qualified) electronic seals
Afkorting	(Q)ESeal
eIDAS artikelen	3, 35 – 39, 39a, 40, ANNEX III
Deeldiensten	1. Aanmaken van eSeal of eSeal certificaat 2. Valideren van eSeal, of eSeal certificaat 3. Preserveren van eSeal of eSeal certificaat 4. Beheer van middelen voor het zetten van elektronische zegels op afstand
Definitie in eIDAS	'Elektronische zegels zijn gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen'
Doel	Het doel van een eSeal is het scheppen van vertrouwen door de mogelijkheid van het digitaal ondertekenen van een document om daarmee de instemming van een rechtspersoon of specifiek de authenticiteit en integriteit van het document zelf te onderschrijven.
Nederlandse QTSP's die QESeal diensten aanbieden	1. Digidentity B.V. 2. KPN B.V. 3. QuoVadis Trustlink B.V.

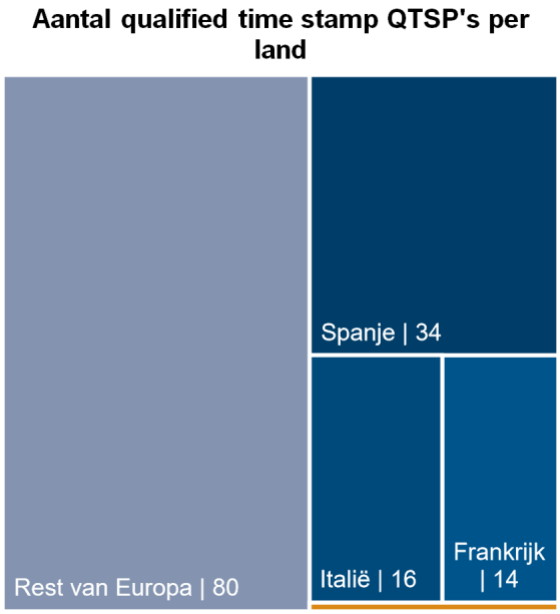




8.1.3. (Q)Timestamp 1-pager

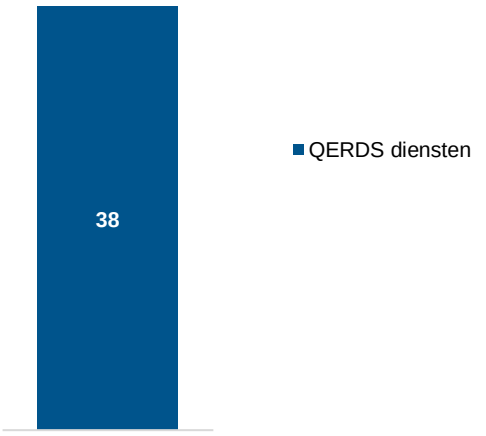
Naam	(qualified) electronic timestamp
Afkorting	(Q)Timestamp
eIDAS artikelen	Artikelen: 3, 41, 42
Deeldiensten	1. Creëren van tijdstempels 2. Validatie van tijdstempels
Definitie in eIDAS	‘Elektronische tijdstempels zijn gegevens in elektrische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden’
Doel	Het doel van een elektronische tijdstempel is het scheppen van vertrouwen door elektronische gegevens te voorzien van een tijd en datum die daarmee bewijs is voor hun bestaan of de vereiste versie.
Nederlandse QTSP’s die QTimestamp diensten aanbieden	1. QuoVadis Trustlink B.V.

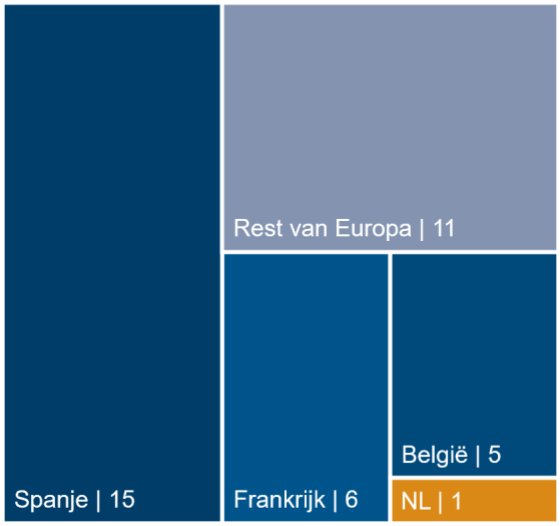




8.1.4. (Q)ERDS 1-pager

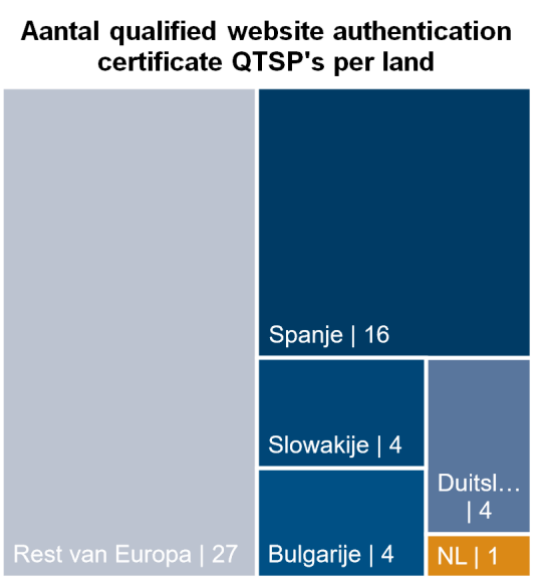
Naam	(qualified) electronic delivery service
Afkorting	(Q)ERDS
eIDAS artikelen	Artikelen: 3, 43, 44
Deeldiensten	1. Leveren van diensten voor elektronische aangetekende bezorging 2. validatie van gegevens die verstuurd zijn via diensten voor elektronische aangetekende bezorging
Definitie in eIDAS	'Diensten voor elektronische aangetekende bezorging zijn diensten die het mogelijk maken gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen'
Doel	Het doel van een ERDS is het scheppen van vertrouwen door het garanderen van het veilige versturen van data tussen verschillende partijen.
Nederlandse QTSP's die QERDS diensten aanbieden	1. Aangetekend B.V.





8.1.5. (Q)WAC 1-pager

Naam	(qualified) website authentication certificates
Afkorting	(Q)WAC
eIDAS artikelen	3, 45, 45a, ANNEX IV
Deeldiensten	1. Uitgeven certificaten voor websiteauthenticatie 2. Validatie certificaten voor websiteauthenticatie
Definitie in eIDAS	'Certificaat voor websiteauthenticatie is een attestering die het mogelijk maakt de authenticiteit van een website vast te stellen en die de website verbindt aan de natuurlijke personen of rechtspersoon aan wie het certificaat is afgegeven'
Doel	Het doel van een (Q)WAC is het scheppen van vertrouwen door het garanderen van een veilige verbinding tussen een natuurlijk persoon of rechtspersoon en een website. Hiernaast schept een (Q)WAC vertrouwen over de identiteit van de entiteit achter de website.
Nederlandse QTSPs die QWAC diensten aanbieden	1. QuoVadis Trustlink B.V.



8.1.6. (Q)EAA 1-pager

Naam	**(qualified) electronic attestation of attributes**
Afkorting	(Q)EAA
eIDAS artikelen	Artikelen: 3, 45b, 45c, 45d, 45e, 45f, 45g, 45h ANNEX V, ANNEX VI, ANNEX VII
Deeldiensten	1. Het uitgeven van elektronische attestering van attributen 2. Validatie van de uitgegeven elektronische attestering van attributen
Definitie in eIDAS	‘Elektronische attestering van attributen is een attestering in elektronisch formaat aan de hand waarvan attributen kunnen worden geauthenticeerd’
Doel	Het doel van een (Q)EAA is het scheppen van vertrouwen door digitaal bewijs te leveren over een bepaald attribuut dat een natuurlijk- of rechtspersoon bezit.

8.1.7. (Q)E-Archiving 1-pager

Naam	(qualified) electronic archiving
Afkorting	(Q)E-Archiving
eIDAS artikelen	Artikelen: 3, 45i, 45j
Deeldiensten	1. Elektronisch archiveren van data
Definitie in eIDAS	‘Een dienst die de ontvangst, opslag, opvraging en verwijdering van elektronische gegevens en elektronische documenten verzorgt om de duurzaamheid en leesbaarheid ervan te garanderen alsook de integriteit, de vertrouwelijkheid en het bewijs van de oorsprong ervan gedurende de volledige bewaartermijn te behouden’
Doel	Het doel van elektronische archiveringsdiensten is het scheppen van vertrouwen door het waarborgen van de integriteit en oorspronkelijkheid van digitale data voor langere periode.

8.1.8. (Q)ELedger 1-pager

Naam	(qualified) electronic ledger
Afkorting	(Q)ELedger
eIDAS artikelen	Artikelen: 3, 45k, 45l
Deeldiensten	1. Opslaan van data in elektronische grootboeken
Definitie in eIDAS	‘Een opeenvolging van elektronische gegevensbestanden die de integriteit van die bestanden en de nauwkeurigheid van de chronologische volgorde van die bestanden waarborgt’
Doel	Het doel van een elektronisch grootboek is het scheppen van vertrouwen door een manipulatiebestendig digitale registratie van data te faciliteren die haar authenticiteit en integriteit op het gebied van datum, tijd en chronologische volgorde verzekerd

8.2. Begrippenlijst EN – NL

Engelse Term	Nederlandse Term
(Qualified) Certificate for electronic seals	(Gekwalificeerd) Certificaat voor elektronische zegels
(Qualified) Certificate for electronic signature	(Gekwalificeerd) Certificaat voor elektronische handtekening
(Qualified) Certificate services for website authentication	(Gekwalificeerde) Certificatendiensten voor websiteauthenticatie
(Qualified) Electronic archiving	(Gekwalificeerde) Elektronische archivering
(Qualified) Electronic attestation of attributes	(Gekwalificeerde) Elektronische attestering van attributen
(Qualified) Electronic ledgers	(Gekwalificeerde) Elektronische grootboeken
(Qualified) Electronic registered delivery services	(Gekwalificeerde) Diensten voor elektronische aangetekende bezorging
(Qualified) Electronic seals	(Gekwalificeerde) Elektronische zegels
(Qualified) Electronic signatures	(Gekwalificeerde) Elektronische handtekeningen
(Qualified) Electronic time stamps	(Gekwalificeerde) Elektronische tijdstempels
(Qualified) Management of remote electronic signature and seal creation devices	(Gekwalificeerd) Beheer van middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand
(Qualified) Seal creation device	(Gekwalificeerde) Middel voor het aanmaken van elektronische zegels
(Qualified) Signature creation device	(Gekwalificeerde) Middel voor het aanmaken van elektronische handtekeningen
(Qualified) Trust services	(Gekwalificeerde) vertrouwensdiensten
(Qualified) Trust services providers	(Gekwalificeerde) Verlener van vertrouwensdiensten
Advanced electronic seals	Geavanceerde elektronische zegels
Advanced electronic signatures	Geavanceerde elektronische handtekeningen
Authentic source	Authentieke bron
Conformity assessment body	Conformiteitbeoordelingsinstantie
Creator of a seal	Aanmaker van een zegel
Credential	Inloggegevens
Cybersecurity scheme	Cyberbeveiligingsschema
Digital Identity Wallet	Wallet voor digitale identiteit
Electronic documents	Elektronische documenten
Electronic identification scheme	Stelsel voor elektronische identificatie
Electronic seal creation data	Gegevens voor het aanmaken van elektronische zegels
Electronic signature creation data	Gegevens voor het aanmaken van elektronische handtekeningen
EU Digital Identity Trust Mark	EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit
Level of assurance	Betrouwbaarheidsniveau
Preservation service for electronic signatures	Bewaringsdienst voor elektronische handtekeningen
Relying party	Vertrouwende partij
Signatory	Ondertekenaar
Strong user authentication	Sterke gebruikersauthenticatie
Zero-knowledge proof	Zero-knowledge proof

8.3. Lijst met afkortingen

Afkorting	Term
AES	Advanced Electronic Signature
AESeal	Advanced Electronic Seal
BZK	Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
DLT	Distributed Ledger Technology
DV	Domain Validation
e-archivering	Elektronisch archivering
e-Archiving	Electronic Archiving
e-handtekening	Elektronische handtekening
e-tijdstempel	Elektronische tijdstempel
e-zegel	Elektronische zegel
EAA	Electronic Attestation of Attributes
EDIW	European Digital Identity Wallet
eID	Elektronische identificatie
eIDAS	Electronic IDentification, Authentication and trust Services
eLedgers	Electronic Ledger
EPREL	European Product Registry for Energy Labelling
ERDS	Electronic Registered Delivery Service
eSeal	Electronic Seal
eSig	Electronic Signature
ETSI	European Technical Standard Institute
EV	Extended Validation
EZK	Het Ministerie van Economische Zaken en Klimaat
FIDA	Framework for FInancial Data Access
HSM	Hardware Security Module
NFC	Near Field Communication
NIS2	Network and Information Security directive
ODIW	Organisational Digital Identity Wallet
OV	Organisation Validation
PSD2	Payment Services Directive 2
PSD3	Payment Services Directive 3
PSR	Payment Services Regulation
QE-Archiving	Qualified Electronic Archiving
QEAA	Qualified Electronic Attestation of Attributes
QELedgers	Qualified Eectronic Ledgers
QERDS	Qualified Electronic Registered Delivery Service
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
QSCD	Qualified Signature Creation Device
QSealCD	Qualified Seal Creation Device
QTimestamp	Qualified Electronic Timestamp
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
RDI	Rijksinspectie Digitale Infrastructuur
RP	Relying Party
SAM	Signature Activation Module
SES	Simpel Electronic Signature
SESeal	Simple Electronic Seal
TIP	Trusted Information Partners
TS	Trust Services
TSP	Trust Service Providers
UZI	Unieke Zorgverlener Identificatie
VOG	Verklaring Omtrent Gedrag
WAC	Website Authentication Certificate
Wdo	Wet digitale overheid

Auteurs

Voor meer informatie over de gespecialiseerde expertise van INNOPAY op het gebied van vertrouwensdiensten, digitale identiteit of voor aanvullende informatie over dit rapport, kunt u contact opnemen met:

Vincent Jansen
Vice President
Vincent.jansen@innopay.com

Jorrit Penninga
Manager
Jorrit.penninga@innopay.com

Leon Kluiters
Senior consultant
Leon.kluiters@innopay.com

Jeroen van der Hoeven
Consultant
Jeroen.vanderhoeven@innopay.com

Maurits Mulder
Consultant
Maurits.mulder@innopay.com

Pieter Verhagen
Senior manager
Pieter.verhagen@innopay.com

INNOPAY
A business of Oliver Wyman

World Trade Center tower 3, floor 3
Strawinskylaan 381
1077 XX AMSTERDAM
The Netherlands
T: +31 20 65 80 651

INNOPAY DE GmbH
c/o TechQuartier
Platz der Einheit 2
60327 Frankfurt
Germany
T: +49 (0) 69 50 50 60 4350

info@innopay.com
www.innopay.com

About INNOPAY

INNOPAY is an international consultancy firm specialised in digital transactions. We help companies anywhere in the world to harness the full potential of the digital transactions era.

We do this by delivering strategy, product development and implementation support in the domain of Digital Identity, Data Sharing and Payments. Our services capture the entire strategic and operational spectrum of our client's business, the technology they deploy, and the way they respond to local and international regulations.

We have grown from strength to strength since our foundation in 2002 and operate from our offices in Amsterdam and Frankfurt. Our head office is located in The Netherlands, where we have the #1 market position.

We are a founding member of Holland FinTech, a financial technology hub with links to the rest of Europe, the US, the Middle East and Asia. Our team consists of over 60 experienced domain experts who regularly advise a wide range of global organisations.