Ministerie van Economische Zaken

Informatiegids vertrouwensdiensten eIDAS

Dit is een informatiegids voor vertrouwens-diensten van de eIDAS-verordening. In deze verordening worden kwaliteitseisen voor en toezicht op elektronische vertrouwensdiensten geregeld. De verordening is onlangs gereviseerd. Er zijn nieuwe vertrouwensdiensten toegevoegd.

Deze gids is bedoeld voor bedrijven, overheids-instanties en alle personen die elektronische transacties uitvoeren in de EU en zich moeten houden aan de eIDAS-verordening.

Inhoudsopgave

1. Elektronische vertrouwensdiensten

Vertrouwen is essentieel voor de digitale economie. Om dit vertrouwen te realiseren, spelen zogeheten elektronische vertrouwens-diensten een belangrijke rol. Dit zijn diensten die via digitale versleuteling (encryptie) zorgen voor de echtheid van websites, elektronische handtekeningen en andere digitale berichten.

Wat kunnen vertrouwensdiensten voor mij als organisatie betekenen?

Omdat digitalisering toeneemt, worden vertrouwensdiensten steeds belangrijker. Digitaal kan namelijk veel worden nagemaakt en kan iemand zich relatief makkelijk als iemand anders voordoen. Vertrouwensdiensten zorgen ervoor dat dit lastiger wordt gemaakt. Met behulp van een vertrouwensdienst, zoals een elektronische handtekening, kunnen we er meer op vertrouwen dat de boodschap die we zien ook echt van de veronderstelde afzender is en de boodschap onderweg niet veranderd is. Dit is niet alleen prettiger, maar heeft belangrijke economische gevolgen doordat het transactiekosten vermindert en processen stroomlijnt. Door meer gebruik te maken van (gekwalificeerde) vertrouwensdiensten verkleinen we de misbruikrisico's en kunnen we gebruik-maken van de efficiëntie die digitalisering ons biedt.

Welke vertrouwensdiensten zijn er?

Ondanks dat veel mensen onbekend zijn met de term 'vertrouwensdiensten' gebruiken we ze toch al vaak. Elke keer als we naar een website gaan, maken we ongemerkt gebruik van een vertrouwensdienst, namelijk *certificaten voor websiteauthenticatie*. Deze certificaten herken je aan het 'slotje' naast de URL-balk bij de meeste websitebrowsers. Een andere vertrouwensdienst is het uitgeven van elektronische handtekeningen. Net als bij een 'natte' handtekening is een elektronische handtekening een wilsuiting door een natuurlijke persoon en kan daarmee een rechtsgevolg hebben. Oftewel, als u een elektronische handtekening zet onder een koopcontract van een huis, dan bent u de koper van dat huis. Het is in het digitale verkeer mogelijk om zowel e-mails als andere digitale berichten als digitale documenten te ondertekenen met elektronische handtekeningen. Iets vergelijkbaars geldt voor *elektronische zegels*, maar dan met het verschil dat het verzegelen namens een organisatie gebeurt in plaats van door een natuurlijke persoon. Daarnaast bestaan er vertrouwensdiensten als elektronische tijdsstempels en elektronische bezorgdiensten.

Welke wetgeving bestaat er al?

In de Europese eIDAS-verordening zijn kwaliteitseisen voor en toezicht op elektronische vertrouwensdiensten geregeld. De eIDAS-verordening verduidelijkt ook dat een elektronische handtekening, zegel of tijdsstempel even rechtsgeldig is als de niet-elektronische variant. Daarnaast maakt de eIDAS-verordening onderscheid tussen gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. De eisen aan gekwalificeerde vertrouwensdiensten zijn zwaarder en het toezicht daarop is uitgebreider. De verordening geeft aan dat een gekwalificeerde vertrouwensdienst zondermeer rechtsgeldig is.

Wat verandert er in de nieuwe wetgeving?

In 2024 is de eIDAS-verordening herzien.[1] Er is nu een verplichting voor overheden bijgekomen om Europese Digitale Identiteitswallets (hierna: EDI-wallets) beschikbaar te stellen voor burgers en organisaties. Daarnaast is het aantal vertrouwensdiensten uitgebreid én kan een aantal vertrouwensdiensten via EDI-wallets gebruikt worden. Omdat het toezicht op vertrouwensdiensten naar tevredenheid werkt, is dit niet veranderd.

EDI-wallets zijn applicaties waarmee burgers of organisaties hun digitale identiteit aan kunnen tonen. De gebruiker kan er echter ook gegevens mee bewaren, beheren en delen. Dit delen gebeurt met gegevens, die gekoppeld kunnen zijn aan een identiteit, zoals een rijbewijs, treintickets, vergunningen, lidmaatschappen, werkpasjes en toegangskaarten. Ook kun je via de EDI-wallet een (gekwalificeerde) elektronische handtekening of zegel maken, zodat dit soort diensten ook makkelijk toepasbaar zijn in het EDI-wallet-ecosysteem.

Introductie EDI-Wallets

Nieuwe vertrouwensdiensten

Elektronische handtekeningen op afstand

Archiefdiensten & registerdiensten

Elektronische attesteringen

1 Verordening (EU) nr. 2024/1183 die aanpassingen bepaalt ten aanzien van verordening nr.910/2014

De EDI-wallets zijn de verantwoordelijkheid van nationale overheden maar moeten wel voldoen aan Europese (veiligheids)eisen zodat ze overal in Europa gebruikt kunnen worden. Ook kan een overheid ervoor kiezen om EDI-wallets die door bedrijven of andere organisaties zijn gemaakt, te erkennen als wallet in dat land als ze aan de eisen voldoen.

In de herziening van de verordening zijn ook nieuwe vertrouwensdiensten gedefinieerd. Het gaat dan om *elektronische handtekeningen op afstand, archiefdiensten*, *registerdiensten* en het leveren van *elektronische attesteringen van attributen*. Daarnaast regelt de verordening dat burgers gratis een gekwalificeerde handtekening moeten kunnen zetten via de EDI-wallet, als dat voor niet-professioneel gebruik is. Dat betekent dat de overheid ervoor moet zorgen dat deze handtekening beschikbaar is én ook echt gratis is voor de burgers. De overheid mag maatregelen nemen om te voorkomen dat deze gratis handtekening wordt gebruikt voor professionele doeleinden.

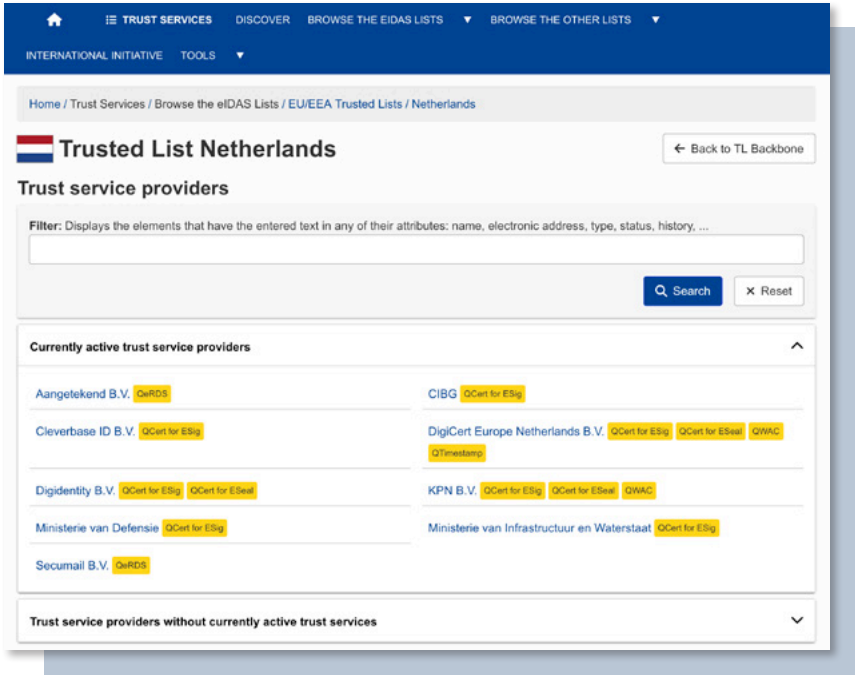
Hoe ziet de Nederlandse markt voor vertrouwensdiensten eruit? En hoe gaat de herziening van de verordening die beïnvloeden?

De markt voor vertrouwensdiensten is in Nederland een duidelijke groeimarkt. Het aantal aanbieders is nu nog beperkt, maar uit onderzoek blijkt dat de vraag naar vertrouwensdiensten door de herziening in de komende jaren gaat toenemen.[2] Vertrouwensdiensten zijn een fundamenteel onderdeel van een innovatieve sector die noodzakelijk is voor een betrouwbare en toekomstbestendige digitale economie in Nederland. Ook de introductie van EDI-wallets gaat het voor zowel burgers als bedrijven makkelijker maken om vertrouwensdiensten te gebruiken en om data met elkaar te delen.

2 https://www.rijksoverheid.nl/documenten/kamerstukken/2024/06/21/kamerbrief-onderzoeksrapport-de-marktimpact-van-de-eldas-revisie-op-vertrouwensdiensten

De onderzoekers schatten in dat in een volwassen markt 11,6 miljoen Nederlandse burgers gebruikmaken van de gekwalificeerde elektronische handtekening via de Wallet. Het gebruik van gekwalificeerde certificaten zal volgens die schatting 462,5% groter zijn dan nu. Ook voor andere vertrouwensdiensten verwachten ze dat er nog veel groeipotentieel is. Deze groei heeft dan niet alleen directe positieve effecten op deze sector, maar zorgt er ook voor dat Nederlandse burgers en het Nederlandse bedrijfsleven minder kwetsbaar zijn voor online fraude, misinformatie en onderbrekingen van online dienstverlening.

De markt voor elektronische handtekeningen voor niet-professioneel gebruik is naar schatting klein. Toch willen we de verplichting om een gratis handtekening aan te bieden aan burgers als een kans zien om de markt in Nederland te versterken en niet te verstoren. Daarom onderzoeken we hoe we marktpartijen kunnen inzetten om de gratis handtekening voor burgers te realiseren.



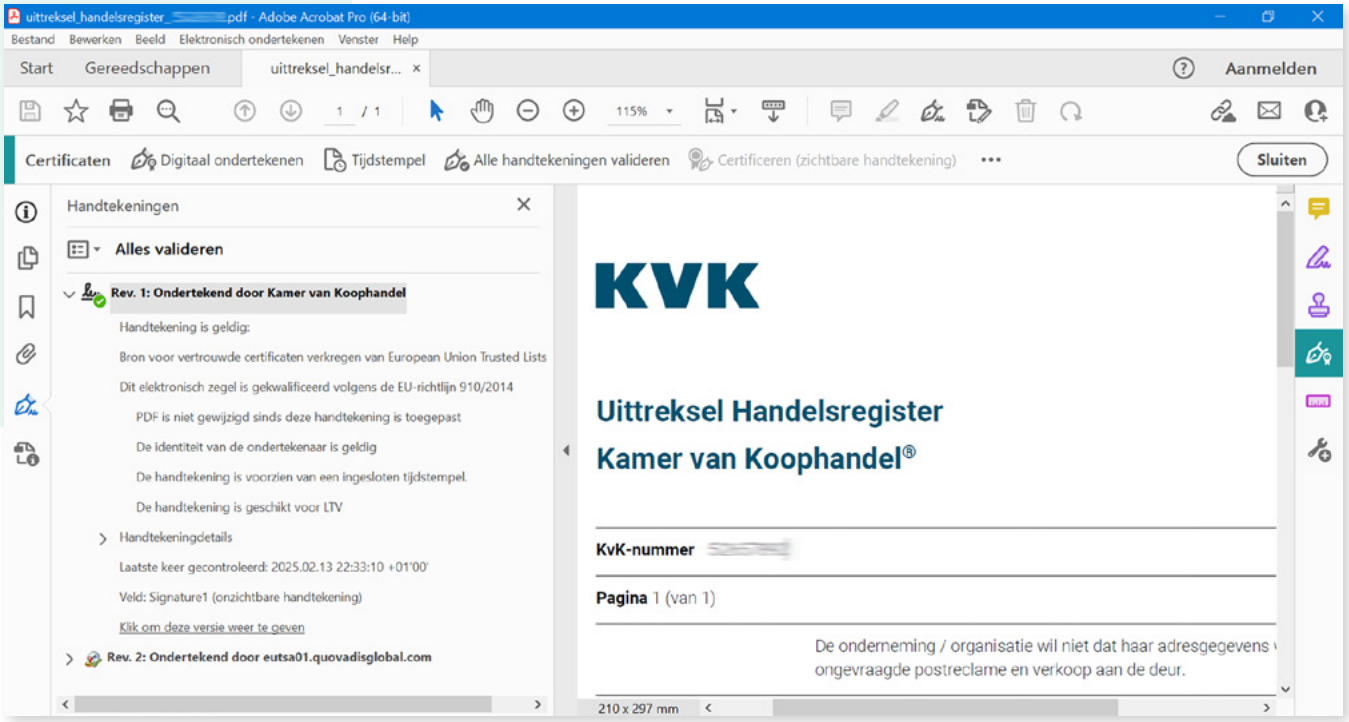
2. Waar kun je vertrouwensdiensten voor gebruiken?

Elektronische handtekening

Elektronische handtekeningen zijn steeds gebruikelijker bij het ondertekenen van allerlei documenten. Met name bij belangrijke documenten waarvan je wilt dat er later niet mee geknoeid wordt. Organisaties en burgers kunnen door middel van ondertekensoftware en een fysieke digitale sleutel met gemak vanaf de computer of laptop documenten ondertekenen. Een digitale sleutel kan bijvoorbeeld beveiligd zijn opgeslagen in een smartcard of een speciale USB-stick. Het document is na ondertekenen direct beschermd door een unieke manier van versleuteling. Elke wijziging na ondertekening wordt direct ontdekt. Dat is dus anders dan in de papieren wereld waar het makkelijker kan zijn om iets te wijzigen ná de ondertekening. Een elektronische handtekening is rechtsgeldig als deze 'voldoende betrouwbaar' is, volgens bepalingen in artikel 3:15a van het Burgerlijk Wetboek. Gekwalificeerde elektronische handtekeningen zijn dermate veilig dat ze automatisch rechtsgeldig zijn.

Voorbeeld

Een voorbeeld waar gekwalificeerde handtekeningen kunnen worden gebruikt, zijn het ondertekenen van contracten, bijvoorbeeld bij autohuur, of bij gebruikersvoorwaarden bij het openen van een bankrekening.



Elektronisch zegel

Bedrijven kunnen voor het ondertekenen van documenten ook kiezen voor elektronische zegels. Dit gebeurt met name bij grote aantallen documenten. De ondertekening gebeurt dan op de bedrijfsnaam. Bij een grootschalig gebruik wordt een hardware security module (HSM) in het netwerk geïntegreerd. Een HSM is een fysiek computerapparaat dat digitale sleutels beveiligt en beheert. Blijft het bij kleinschalig gebruik dan zou net als bij een elektronische zegel een losse smartcard gebruikt kunnen worden.

Voorbeeld

Een voorbeeld zijn de elektronische uittreksels uit het handelsregister die door de Kamer van Koophandel van gekwalificeerde zegels worden voorzien. In het ondertekende document zien ze er net zo uit als een elektronische handtekening, maar ze verwijzen naar een organisatie en niet naar een natuurlijke persoon.

Elektronische handtekeningen/zegels op afstand

Elektronische handtekeningen of zegels op afstand kunnen in exact dezelfde situaties worden gebruikt als waar “gewone” elektronische handtekeningen en zegels worden toegepast. Op dit moment worden ze door het gemak voor de gebruiker steeds vaker gebruikt. Zo heeft de gebruiker geen smartcardlezer, extra software of USB-stick nodig. Omdat je geen fysieke sleuteldrager krijgt overhandigd, is ook een fysieke identificatie niet nodig. Dit maakt de kostprijs fors lager. De elektronische handtekening op afstand wordt door commerciële bedrijven ook aangeboden aan natuurlijke personen. In dit geval wordt een HSM in het netwerk geïntegreerd. De eindgebruiker heeft zijn eigen digitale kluisje met daarin zijn sleutel, die alleen hij kan ontsluiten. Hoewel dus de dienst elektronische handtekening “op afstand” heet, kan hij zowel in online gevallen gebruikt worden als in gevallen waarbij de partijen bij elkaar staan of zitten. Het gaat er meer om dat het device waar de sleutels in zitten niet fysiek in de buurt is, maar op afstand staat.

Voorbeeld

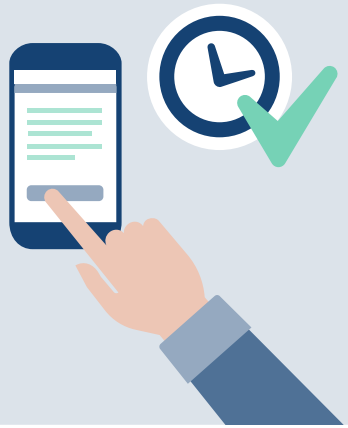
Bij elektronische handtekeningen op afstand zijn dezelfde voorbeelden van toepassingen als bij “gewone” elektronische handtekeningen zoals het ondertekenen van contracten of documenten. In het ondertekende document zien ze er ook hetzelfde uit.

Elektronisch tijdsstempel

Bij een *elektronische tijdsstempel* wordt het moment waarop documenten of andere gegevens zijn ontstaan of verzonden onweerlegbaar vastgelegd. Dit kan bijvoorbeeld belangrijk zijn als er zekerheid moet zijn over een keten van bewijs. Zo kan het bij een inschrijving voor een online veiling of aanbesteding van belang zijn dat het precieze tijdstip waarop de inschrijving is gedaan bekend is. Met een tijdsstempel wordt dat tijdstip ondubbelzinnig vastgelegd.

Voorbeeld

Bij het gekwalificeerde elektronisch tijdsstempel hieronder wordt ondubbezinnig de tijd aangegeven die hoort bij de betreffende handeling. Door gebruik te maken van het EU Trustmark (het blauwe slotje met het gele vinkje) en expliciete vermelding kan iedereen zien dat het een gekwalificeerd tijdsstempel is en de aangegeven tijd juist is.



Elektronische geregistreerde bezorgdiensten

Elektronische bezorgdiensten worden gebruikt in situaties waarbij het van belang is om zeker te weten dat een document veilig aankomt bij de juiste ontvanger en je daar een bewijs van wilt hebben. Deze dienst is te vergelijken met een elektronische tegenhanger van een aangetekende brief. Dat zal vooral zijn in gevallen waarbij (grote) financiële of juridische gevolgen met het bericht zijn gemoeid, zoals bij contracten, aanmaningen en bezwaren of beroepen. De vorm van zo'n bezorgdienst kan een e-mail zijn maar bijvoorbeeld ook een portaal.

Voorbeeld

Een voorbeeld in Nederland is de verzending van gerechtelijke stukken binnen de rechtspraak, waar het gebruik van gekwalificeerde elektronische bezorgdiensten inmiddels verplicht is.

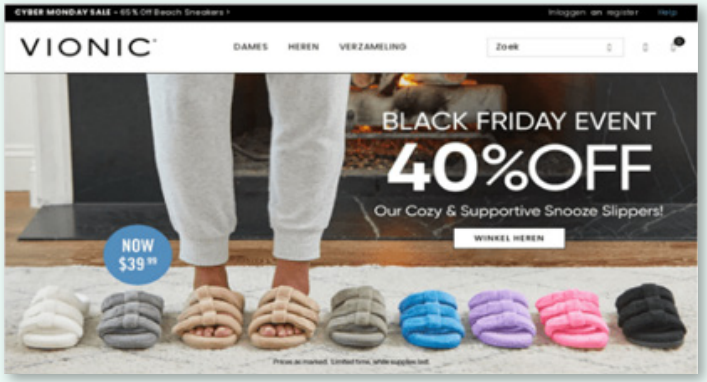
Certificaat voor websiteauthenticatie

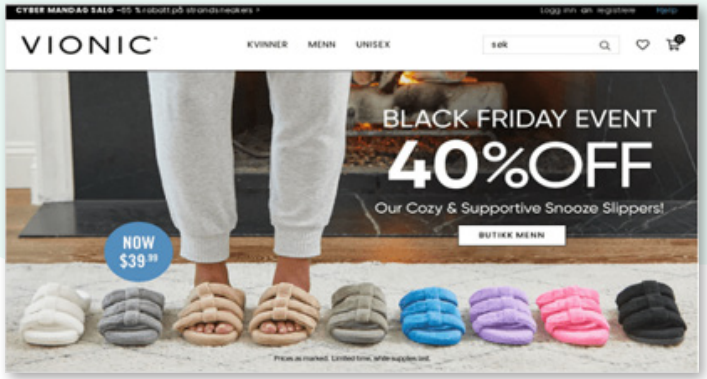
De certificaten voor websiteauthenticatie zijn bij de meeste websitebrowsers te vinden via het ‘slotje’ naast de URL-balk. De eigenaar van een website schaft zo’n certificaat aan. Dit betekent dat de verbinding veilig is. De meest gebruikte websitebrowsers zijn Chrome (van Google), Safari (van Apple) en Edge (van Microsoft). De uitgevers van door de browsers toegelaten certificaten voor websiteauthenticatie kun je terugvinden in hun zogeheten root store. Wanneer een uitgever van een websitecertificaat niet (meer) in de rootstore van een browser zit, krijg je de melding dat de website niet vertrouwd wordt.

Gekwalificeerd certificaat voor websiteauthenticatie

Certificaten voor websiteauthenticatie zijn bedoeld om de identiteit van een website aan te geven. Een gewoon certificaat voor websiteauthenticatie zegt niet veel meer dan dat degene die zegt dat hij het websitedomein bezit, heeft aangetoond dat hij daadwerkelijk het websitedomein bezit. Dat kan dus ook een nepwebsite zijn.

De bedoeling van een gekwalificeerd certificaat voor websiteauthenticatie (QWAC) is daarentegen dat de gebruiker de echte website beter kan identificeren. Nepwebsites worden door de browsers niet automatisch geweerd en de uitgevers van de certificaten kunnen dan toch in de root stores, die het vertrouwen van de browser bepalen, zitten. Eigenaars van nepwebsites kunnen namelijk een gewoon websitecertificaat krijgen (in veel gevallen gratis) waarvoor je alleen hoeft aan te tonen dat je een bepaald domein bezit. Dit is ook een certificaat voor websiteauthenticatie, maar dus eigenlijk van een laag niveau. Dat certificaat is voor de browsers genoeg om de website normaal te laten functioneren, maar niet om een nepwebsite te weren. Om een QWAC te kunnen ontvangen, moet de eigenaar van de website ook documenten zoals een uittreksel uit het handelsregister en een door de directeur ondertekende goedkeuring van de aanvraag meeleveren om de binding tussen de bedrijfsnaam en de website aan te tonen. In de herziening van de eIDAS-verordening moeten browsers ervoor zorgen dat websites voorzien van een QWAC’s makkelijk te identificeren zijn voor bezoekers van die websites. Het symbool daarvoor is nog in ontwikkeling.





Voorbeeld

Nepwebsites zijn momenteel veel in omloop bij criminelen om via deze websites mensen illegaal geld afhandig te maken. Daarbij lijkt de website als twee druppels water op de echte website. Bijvoorbeeld ten tijde van Black Friday. Veel mensen zijn dan op koopjesjacht en de gretigheid kan daarbij ten koste gaan van beveiligingsbewustzijn. In die periode zie je een enorme toename van dergelijke frauduleuze websites.

De bovenste twee afbeeldingen zijn van nepwebsites:

- De bovenste nepwebsite (**vionicsneakersnederland.com**) is gericht op gebruikers in Nederland;
- De middelste nepwebsite (**vionicskonorge.com**) is gericht op gebruikers in Noorwegen;
- Alleen de onderste (**vionicshoes.com**) is van Vionic.

Elektronische attesteringen van attributen

Een elektronische attestering van een attribuut (EAA) is een gegeven in elektronisch formaat. Aan de hand van een EAA kan een eigenschap, hoedanigheid, recht of toestemming van een natuurlijke of rechtspersoon of van een object worden geauthentiseerd. Dat kunnen bijvoorbeeld diploma's, leeftijdsbewijzen, machtigingen, vergunningen, factuurgegevens, duurzaamheidscertificaten en zelfs concertkaarten zijn. Deze attributen kunnen zowel bij publieke als private bronhouders in beheer zijn. Als je een online bestelling doet, wil de webwinkel graag weten wat je adres is. Als je ergens solliciteert, wil je aanstaande werkgever graag weten welke relevante diploma's je hebt gehaald en welke opleidingen je hebt afgerond.

Bezitters van EDI-wallets kunnen straks de elektronische attesteringen van attributen allemaal via deze wallets delen. De verordening bepaalt de eisen waaraan de uitgevers van elektronische attesteringen van attributen moeten voldoen. Bij het hoogste niveau van betrouwbaarheid, de gekwalificeerde EAA's en publieke EAA's, zal de ontvanger een hoge mate van zekerheid hebben van dat wat hem getoond wordt. Dit verbetert de datakwaliteit en de dienstverlening en draagt daarnaast bij aan het verminderen van administratieve lasten en fraude. Uiteindelijk zal het maatschappelijk verkeer bepalen welke (Q)EAA's het meest zullen worden gebruikt via de EDI-wallets.

Voorbeeld

Een EAA helpt bijvoorbeeld financiële instellingen. Zij moeten in verband met de wet – ter voorkoming van witwassen en financieren van terrorisme – onder meer nagaan wie de uiteindelijke eigenaar van een bedrijf is. Die gegevens moet een bedrijf aanleveren bij de financiële instellingen. Bij bedrijfsmatige handelingen is het belangrijk om te weten of degene die ze wil uitvoeren daartoe gemachtigd is. In al deze voorbeelden zal de persoon de gegevens momenteel in veel gevallen schriftelijk of door middel van zelfverklaringen aanleveren.

Elektronische archivering en elektronische registerdiensten

Elektronische *archiefdiensten* en *registerdiensten* zijn betrekkelijk nieuwe vertrouwensdiensten. Zij hebben als doel het vertrouwen in het juist bewaren van gegevens over een langere periode te vergroten. De toepassing van de verordening op deze diensten en de verdere uitwerking hiervan zullen zich in de komende jaren verder ontwikkelen.

De verwachting is dat elektronische archivering met name van belang is bij documenten en contracten die elektronisch zijn ondertekend of verzegeld zijn. De sleutels daarvan verlopen na een aantal jaren. De archiveringsdienst kan zorgen dat na die looptijd toch nog kan worden nagegaan wie heeft getekend en kan worden vastgesteld dat het document niet veranderd is.

3. Conformiteit / Compliancy

Verschillende niveaus van vertrouwensdiensten

Vertrouwensdiensten zijn er op verschillende niveaus, waarvan “geavanceerd” en “gekwalificeerd” de belangrijkste zijn. Het hoogste niveau van betrouwbaarheid zijn de gekwalificeerde vertrouwensdiensten. De eIDAS-verordening bepaalt dat deze diensten per definitie rechtsgeldig zijn. Nationale toezichthouders in de EU-lidstaten verlenen deze gekwalificeerde status. In Nederland verleent de Rijksinspectie Digitale Infrastructuur (RDI) deze status. Gekwalificeerde vertrouwensdiensten zijn herkenbaar aan het EU-trustmark, dat ook alleen door de gekwalificeerde vertrouwensdiensten mag worden gebruikt voor de door hen geleverde gekwalificeerde diensten.

De gekwalificeerde en geavanceerde vertrouwensdiensten moeten aantoonbaar voldoen aan de eisen vanuit de eIDAS-verordening. Voor geavanceerde handtekeningen zijn die eisen onder meer dat de handtekening alleen gekoppeld is aan de ondertekenaar, deze de ondertekenaar kan identificeren en dat de handtekening is gemaakt met behulp van gegevens met een hoge mate van zekerheid. Voor gekwalificeerde handtekeningen komt er nog bij dat er gebruik gemaakt moet worden van certificaten die geproduceerd zijn met gekwalificeerde, hoogbeveiligde apparaten, zoals bijvoorbeeld smartcards of HSM’s. Daarmee geven gekwalificeerde vertrouwensdiensten een zeer hoog niveau van betrouwbaarheid en ligt die juridische gelijkschakeling voor de hand.

Wanneer een gekwalificeerde vertrouwensdienst gebruiken?

Een gekwalificeerde dienst heeft het voordeel van een juridische zekerheid. Een gekwalificeerde elektronische handtekening is bijvoorbeeld gelijkgeschakeld aan een handgeschreven handtekening. Van een website die beveiligd is met een gekwalificeerd certificaat, weet je dat de website ook echt toebehoort aan de partij die je veronderstelt. En van een gekwalificeerde elektronische attestering weet je dat deze gelijk is aan de authentieke bron. Dat geeft voordelen bij het gebruik van gekwalificeerde diensten. Bij gebruik van een niet-gekwalificeerde dienst is er dus een risico dat de handtekening niet van de persoon is die je veronderstelt.

Een ander voordeel van een gekwalificeerde vertrouwensdiensten is dat de vertrouwensdienstverlener op grond van de eisen van de verordening moet kunnen aantonen dat hij geschoold personeel in dienst te heeft, dat gebruikmaakt van betrouwbare en beveiligde systemen. Om de continuïteit te garanderen moet de dienstverlener borgen dat de dienstverlening overgedragen kan worden naar een andere gekwalificeerde vertrouwensdienstverlener.

Daartegenover staat dat de kosten hoger zullen zijn dan bij het gebruik van geavanceerde of lagere niveaus van vertrouwensdiensten. Organisaties moeten daarom zelf een risico-afweging maken en beslissen welk niveau vertrouwensdienst het best past bij hun proces. Een hulpmiddel bij deze risico-afweging is de Handreiking Betrouwbaarheidsniveaus van Forum Standaardisatie, die in maart 2024 is herzien. Voor sommige partijen zal de rechtszekerheid een belangrijk element zijn, voor andere partijen, zoals in de vitale sectoren, de gegarandeerde continuïteit. Voor die laatste groep, de vitale sectoren, is er een extra aspect om rekening mee te houden bij die risicoafweging: in de Europese NIS2-richtlijn staat dat lidstaten het gebruik van gekwalificeerde diensten dienen aan te moedigen bij essentiële en belangrijke entiteiten.

Rechtsgeldig of niet?

Diverse aanbieders van vertrouwensdiensten schermen met termen als “rechtsgeldig” of met “voldoet aan de eisen van de eIDAS-verordening”. Wat wil dat zeggen? Eigenlijk niet veel! De eIDAS-verordening geeft namelijk eisen voor alle vertrouwensdiensten, zowel voor gekwalificeerde als niet-gekwalificeerde. Voor niet-gekwalificeerde diensten zijn dat uiteraard minder zware eisen dan voor gekwalificeerde. Dit houdt in dat de garanties en betrouwbaarheid van niet-gekwalificeerde diensten ook van een lager niveau zijn. “Voldoet aan de eisen van de eIDAS-verordening” kan dus ook betekenen dat slechts aan die minimale eisen is voldaan en geeft dus geen kwaliteitsgarantie.
Nog niet alles rondom de rechtsgeldigheid van vertrouwensdiensten is duidelijk. In de eIDAS-verordening is de gelijkschakeling van gekwalificeerde elektronische handtekeningen met natte handtekeningen opgenomen en die zijn daarmee zonder meer rechtsgeldig. Er staat echter ook in de verordening dat van lagere niveaus zoals een ingescande handtekening, de rechtsgeldigheid niet van tevoren mag worden ontkend. Dit zal afhangen van de omstandigheden en het doel waarvoor het wordt gebruikt. Mocht daar in individuele gevallen onenigheid over ontstaan, dan zal een rechter de kwestie beoordelen.
Waar de term “rechtsgeldigheid” op zichzelf weinig zegt, geldt dit niet voor de termen “gekwalificeerd” en “geavanceerd”. Het gebruik van “gekwalificeerd” geeft waarborgen, zoals per definitie rechtsgeldigheid. De termen “gekwalificeerd” en ook “geavanceerd” zijn beschermd en mogen – net als het EU-trustmark – niet worden gebruikt door partijen die hier niet aantoonbaar aan voldoen. De Nederlandse toezichthouder RDI mag optreden en boetes opleggen wanneer partijen deze termen of dit logo ten onrechte gebruiken.

Conformiteitsbeoordelingsinstanties

Een conformiteitbeoordelingsinstantie – ook wel Conformity Assessment Body (CAB) – stelt de conformiteit van vertrouwensdienstverleners met de eisen van de verordening vast. Een CAB in het kader van de eIDAS-verordening moet zelf ook aan zware eisen voldoen. Hiervoor worden ze geaccrediteerd door de nationale accreditatie-organisatie. In Nederland is dat de Raad voor Accreditatie (RvA). Zo’n accreditatie zelf is vier jaar geldig. De CAB wordt jaarlijks getoetst door de RvA. Er zijn binnen de eIDAS-verordening vier gebieden waarop CAB’s actief zijn:

1. Beoordeling van conformiteit van EDI-wallets;
2. Beoordeling van conformiteit van gekwalificeerde vertrouwensdiensten;
3. Beoordeling van conformiteit van publieke vertrouwensdiensten die elektronische attesteringen van attributen uitgeven;
4. Beoordeling van conformiteit van gekwalificeerde middelen om elektronische handtekeningen of elektronische zegels mee uit te geven.

Een CAB kan op elk van deze deelgebieden afzonderlijk actief zijn en wordt hiervoor dus ook apart geaccrediteerd. Om conformiteitsbeoordelingen voor de onderdelen onder 1 en 4 uit te mogen voeren, moet de organisatie niet alleen een accreditatie bezitten, maar ook zijn aangewezen door de lidstaat. Voor onderdeel 4 betekent dit in Nederland een aanwijzing door de minister van Economische Zaken. CAB's zijn terug te vinden in een vertrouwenslijst die wordt bijgehouden door de Europese Commissie.

Omdat het leveren van vertrouwensdiensten – gekwalificeerd of niet – binnen de interne markt van de EU valt, betekent dit onder andere dat een gekwalificeerde dienst in de ene lidstaat ook een gekwalificeerde dienst – inclusief de rechtsgevolgen – in een andere lidstaat is. Daarom zijn de eisen van de eIDAS-verordening vertaald in internationale standaarden die door de industrie gehanteerd kunnen worden. De CAB's kunnen deze geharmoniseerde standaarden goed hanteren bij de conformiteitbeoordeling. De meeste standaarden voor de vertrouwensdiensten worden door het European Telecommunications Standards Institute (ETSI) opgesteld.

eIDAS Dashboard

Het eIDAS Dashboard van de Europese Commissie is een belangrijk hulpmiddel waarop iedereen kan zien of ze met gekwalificeerde dienstverleners, gekwalificeerde middelen of met geaccrediteerde CAB's te maken hebben. In dit dashboard zijn de vertrouwenslijsten voor elk van deze deelgebieden opgenomen. Het eIDAS Dashboard is opgebouwd per lidstaat en is daarmee een compilatie van nationale vertrouwenslijsten. De lidstaten zorgen ervoor dat de nationale lijsten up-to-date zijn. De vertrouwenslijsten in het eIDAS Dashboard voldoen zelf aan internationale standaarden en zijn in XML-formaat beschikbaar zodat ze in IT-systemen te verwerken zijn.

Begrippenlijst

- **eIDAS-verordening** – Europese wetgeving (Electronic Identification and Trust Services) die regels stelt voor elektronische identificatie en vertrouwensdiensten.
- **Encryptie** – Het versleutelen van gegevens om deze te beveiligen tegen ongeautoriseerde toegang.
- **EDI-wallets** – Europese Digitale Identiteitswallets, digitale applicaties waarmee burgers en organisaties hun identiteit en documenten kunnen beheren en delen.
- **Elektronische handtekening** – Digitale variant van een handgeschreven handtekening die rechtsgevolgen kan hebben.
- **Elektronisch zegel** – Digitaal alternatief voor een stempel of zegel, gebruikt door organisaties.
- **Elektronische tijdsstempel** – Een methode om onweerlegbaar vast te leggen wanneer een document of bericht is verzonden of aangemaakt.
- **Elektronische geregistreerde bezorgdiensten** – Digitale variant van een aangetekende brief, waarbij ontvangst en verzending juridisch worden vastgelegd.
- **Certificaat voor websiteauthenticatie** – Digitale certificaten die de authenticiteit van een website bevestigen en een veilige verbinding garanderen.
- **QWAC** (Qualified Website Authentication Certificate) – Gekwalificeerd certificaat voor websiteauthenticatie dat extra zekerheid biedt over de identiteit van een website-eigenaar.
- **EAA** (Elektronische Attestering van Attributen) – Een digitaal bewijs van een eigenschap, recht of toestemming, zoals een diploma of rijbewijs.
- **HSM** (Hardware Security Module) – Een fysiek apparaat dat digitale sleutels beveiligt en beheert.
- **CAB** (Conformity Assessment Body) – Een instantie die beoordeelt of vertrouwensdiensten voldoen aan regelgeving.
- **RvA** (Raad voor Accreditatie) – Nederlandse organisatie die toeziet op de certificering van conformiteitsbeoordelingsinstanties en ze hiervoor accrediteert.
- **EU-trustmark** – Een keurmerk dat aangeeft dat een vertrouwensdienst gekwalificeerd is en voldoet aan de eIDAS-eisen.
- **eIDAS Dashboard** – Online platform beheerd door de Europese Commissie waar men kan controleren of een dienstverlener gekwalificeerd is.

Deze brochure is een uitgave van:

Ministerie van Economische Zaken
Postbus 20401 | 2500 EK Den Haag

Ontwerp: VormVijf

Februari 2025