Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1198

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 21 juni 2024

Vertrouwen is essentieel voor de digitale economie. Om dit vertrouwen te realiseren, spelen zogeheten elektronische vertrouwensdiensten een belangrijke rol. Dit zijn diensten die via digitale versleuteling (encryptie) zorgen voor de echtheid van websites, elektronische handtekeningen en andere digitale berichten. Om ervoor te zorgen dat deze diensten ook echt betrouwbaar zijn, stelt de Europese eIDAS-verordening[1] (hierna: de verordening) eisen aan vertrouwensdienstverleners en regelt het toezicht hierop. In Nederland is dit uitgewerkt in de Telecommunicatiewet.

De verordening is dit jaar herzien. De herziening[2] introduceert niet alleen een Europese Digitale Identiteitswallets (hierna: EDI-wallets), maar breidt ook het aantal vertrouwensdiensten uit én zorgt ervoor dat een aantal vertrouwensdiensten via EDI-wallets gebruikt kunnen worden. Omdat het toezicht op vertrouwensdiensten naar tevredenheid werkt, is dit niet veranderd.

Om een optimale uitvoering van deze verordening en specifiek mijn beleid ten aanzien van vertrouwensdiensten te kunnen borgen, heb ik aan Innopay opdracht gegeven om te onderzoeken welke gevolgen de herziening van de verordening heeft op de markt van vertrouwensdiensten. In de bijlage vindt u het resultaat van dit onderzoek.

In deze brief ga ik in op de aanbevelingen uit het onderzoek, waarover een nieuwe bewindspersoon eventuele keuzes kan maken. Vervolgens geef ik aan waarom vertrouwensdiensten steeds belangrijker worden en ten slotte leg ik uit hoe deze vertrouwensdiensten zijn gereguleerd in de verordening.

[1] Verordening (EU) nr. 910/2014
[2] Verordening (EU) nr. 2024/1183

kst-26643-1198
ISSN 0921 - 7371
's-Gravenhage 2024

De aanbevelingen uit het onderzoek

De onderzoekers geven aan dat het belang van vertrouwensdiensten zal toenemen door de herziening van de verordening, dat er ten gevolge van de herziening ook toenemende regeldrukkosten zijn en dat er nog veel vragen leven bij marktpartijen. Deze vragen gaan vooral over de beleidskeuzes ten aanzien van vertrouwensdiensten. De onderzoekers doen de volgende aanbevelingen:

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

De inzichten uit het onderzoek kunnen in de komende tijd gebruikt worden door de volgende bewindspersoon om beleidskeuzes te maken die onder andere in de uitvoeringswet voor de herziene verordening worden uitgewerkt (de verwachting is dat de conceptwet in 2025 naar uw Kamer wordt gestuurd). Hieronder staat in hoofdlijnen wat de belangrijkste aandachtspunten zijn ten aanzien van de aanbevelingen.

Beleid over vertrouwensdiensten

Het uitgangspunt voor het vertrouwensdienstenbeleid is dat de overheid als marktmeester optreedt voor een goedwerkende markt van vraag naar en aanbod van vertrouwensdiensten. Het wettelijk kader en kwalitatief hoogwaardige toezicht zorgen ervoor dat gebruikers van vertrouwensdiensten ervan uit kunnen gaan dat een gekwalificeerde vertrouwensdienstverlener ook echt veilige en betrouwbare vertrouwensdiensten levert. De herziening van de verordening verandert niets aan dit uitgangspunt.

De herziene verordening laat wel een aantal vragen open waarvoor het volgende kabinet een aantal beleidskeuzes moet maken die van invloed zijn op de markt voor vertrouwensdiensten. De belangrijkste beleidskeuzes betreffen:

- De wijze waarop het verschaffen van een gratis gekwalificeerde elektronische handtekening voor burgers in een EDI-wallet plaatsvindt;
- Welke maatregelen kunnen worden genomen om te voorkomen dat de gratis gekwalificeerde elektronische handtekening voor burgers voor professionele doeleinden wordt gebruikt;
- Een vergoedingenstructuur voor elektronische attesteringen van attributen (het afgeven van digitale verklaringen over het eigenaarschap en juistheid van eigenschappen of rechten gekoppeld aan de identiteit van een natuurlijk of rechtspersoon).

Bij het maken en uitvoeren van deze beleidskeuzes is het van belang dat er samenwerking wordt gezocht met de volgende bewindspersoon van Binnenlandse Zaken en Koninkrijksrelaties die verantwoordelijkheid draagt voor digitale identiteiten, waaronder EDI-Wallets. Omdat de beleidskeuzes niet los kunnen worden gezien van de Europese context, is het ook van belang dat hierbij ook nauw zal worden samengewerkt met andere lidstaten.

Randvoorwaarden

Bij het ontwikkelen van het Nederlandse stelsel rondom EDI-wallets en bij de Nederlandse inzet voor de Europese Large Scale Pilots in het kader van de eIDAS verordening wordt in nationaal verband met belanghebbenden, andere departementen en uitvoeringsinstanties samengewerkt. Bij deze

Large Scale Pilots neemt mijn Ministerie op ambtelijk niveau aan twee consortiums deel. De resultaten van het onderzoek helpen om weloverwogen keuzes te maken waarbij de markt voor vertrouwensdiensten zich verder kan ontwikkelen.

Communicatie

Veel burgers en organisaties zijn niet goed bekend met vertrouwensdiensten en wat deze voor hen kunnen betekenen. Naar aanleiding van de herziening van de verordening komen vertrouwensdiensten echter dichterbij, onder andere vanwege de uitgifte van attributen en de gratis gekwalificeerde elektronische handtekeningen voor alle burgers. Daarom is het van belang dat er een plan wordt opgesteld voor communicatie over vertrouwensdiensten. Hierbij dient rekening te worden gehouden met de communicatie over andere Europese wetgeving over de digitale economie die onlangs tot stand is gekomen. Hierbij is het van belang dat wordt samengewerkt met de volgende bewindspersoon van Binnenlandse Zaken en Koninkrijksrelaties die verantwoordelijkheid draagt voor digitale identiteiten.

Achtergrond: Het toenemend belang van vertrouwensdiensten

Vertrouwensdiensten zijn belangrijk voor de digitale economie en worden door de toenemende digitalisering steeds belangrijker. Digitaal kan namelijk veel worden nagemaakt en kan iemand zich relatief makkelijk als iemand anders voordoen. Vertrouwensdiensten zorgen er voor dat dit lastiger wordt gemaakt. Als iets elektronisch is ondertekend of een andere vertrouwensdienst is verleend op «gekwalificeerd niveau», kunnen we er meer op vertrouwen dat de boodschap die we zien ook echt van de veronderstelde afzender is. Dit is niet alleen prettiger, maar heeft belangrijke economische gevolgen doordat het transactiekosten verminderd en processen stroomlijnt. Door meer gebruik te maken van (gekwalificeerde) vertrouwensdiensten worden de risico's van misbruik verlaagd en kunnen we gebruik maken van de efficiëntie die digitalisering ons biedt.

Ondanks dat veel mensen niet bekend zijn met de term «vertrouwensdiensten» gebruiken we ze vaak. Elke keer wanneer we naar een website gaan, maken we ongemerkt gebruik van een vertrouwensdienst, namelijk *certificaten voor websiteauthenticatie*. Deze 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 en, wanneer het ook nog eens een gekwalificeerde vertrouwensdienst is, dat je kunt zien van wie de website is die je op dat moment bezoekt en dat je te maken hebt met de legitieme website en niet met een nepwebsite. Daarmee wordt de kans op online fraude verkleind. Het is van belang in het kader van de herziening van de verordening, dat bezoekers van websites geholpen worden om te weten wanneer een website betrouwbaar is. Hieraan zal worden bijdragen door het genoemde communicatieplan.

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, andere digitale berichten als digitale documenten te ondertekenen met elektronische handtekeningen. Dit gebeurt door aan het document met behulp van een geheime sleutel die bij de ondertekenaar hoort, een versleutelde code toe te voegen. Hierdoor wordt ervoor gezorgd dat elke poging tot verandering

van het document ontdekt wordt. Als de elektronische ondertekening gekwalificeerd is, dan wordt dit gedaan met behulp van hoogwaardige hardware, zoals smartcards en Hardware Security Modules (HSM's). Conformiteitsbeoordelingsinstanties die in Nederland door mij zijn aangewezen stellen vast of deze hardware aan de eisen van de verordening voldoet. 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.

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.

Bij een *elektronische geregistreerde bezorgdienst* wordt zekerheid verkregen over de afzender en de ontvanger van een bericht. De afzender weet daarmee dat de juiste persoon het bericht heeft ontvangen. Het is daarmee te zien als een elektronische tegenhanger van een aangetekende brief. De vorm van zo'n bezorgdienst kan een e-mail zijn maar bijvoorbeeld ook een portaal. Deze bezorgdiensten zijn momenteel al in diverse sectoren in gebruik, zoals de zorg en de rechtspraak.

In de herziening worden daarnaast nieuwe vertrouwensdiensten zoals *archiefdiensten*, *registerdiensten* en het leveren van *elektronische attesteringen van attributen* geïntroduceerd. Bij dit laatste valt te denken aan bijvoorbeeld het rijbewijs, diploma's, bankrekeningnummers, adressen, leeftijd, certificaten, tickets. Deze attributen kunnen dus zowel bij publieke als private bronhouders in beheer zijn. De verordening bepaalt de eisen waaraan de uitgevers van elektronische attesteringen van attributen dienen te voldoen, zodat de uiteindelijke ontvanger – bijvoorbeeld via EDI-wallets – een hoge mate van zekerheid heeft dat wat hem getoond wordt, ook zo in de authentieke bron is opgenomen en de attestering ook echt toebehoort aan degene die deze toont.

De markt voor vertrouwensdiensten is in Nederland een duidelijke groeimarkt, het aantal aanbieders is nu nog beperkt maar het onderzoek duidt op een toenemende ontwikkeling van de vraag. Het gaat bovendien om een innovatieve sector die een fundamenteel onderdeel voor een betrouwbare digitale economie in Nederland verzorgt. De onderzoekers geven aan dat de markt voor vertrouwensdiensten flink zal toenemen als gevolg van de herziening. Niet alleen vanwege de introductie van nieuwe vertrouwensdiensten maar ook omdat voor het delen van data via EDI-wallets vertrouwensdiensten gemakkelijk kunnen worden gebruikt door burgers en bedrijven. Zo schatten de onderzoekers in dat in een volwassen markt 11,6 miljoen Nederlandse burgers gebruik zullen maken van de gekwalificeerde elektronische handtekening via de Wallet. Ook schatten ze in dat het gebruik van gekwalificeerde certificaten voor websiteauthenticatie in een volwassen markt 462,5% groter zal zijn dan nu. Ook voor andere vertrouwensdiensten verwachten ze dat er nog veel groeipotentieel is. Als deze groei verwezenlijkt wordt, dan heeft dat niet alleen directe positieve effecten op deze sector, maar zorgt het er ook voor dat Nederlandse burgers en het Nederlandse bedrijfsleven minder kwetsbaar zullen zijn voor online fraude, misinformatie en onderbrekingen van online dienstverlening.

Achtergrond: de eIDAS-verordening

De in 2016 in werking getreden eIDAS-verordening heeft als doel om ervoor te zorgen dat vertrouwensdiensten ook echt te vertrouwen zijn. Een belangrijke aanleiding voor deze verordening was een groot

cyberincident in Nederland in 2011: de hack bij Diginotar. Door de hack bij dit Nederlandse bedrijf werden nep-certificaten voor websiteauthenticatie via Diginotar uitgegeven. Hierdoor kon een kwaadwillende derde partij inlognamen, wachtwoorden en andere gevoelige informatie verkrijgen. Met de introductie van de eIDAS-verordening zijn er, op initiatief van Nederland, zwaardere eisen gesteld aan vertrouwensdienstverleners en is het toezicht op het voldoen aan die eisen verscherpt. In Nederland is de Rijksdienst voor Digitale Infrastructuur de toezichthouder.

De eIDAS-verordening verduidelijkt ook dat een elektronische handtekening, zegel of tijdsstempel even rechtsgeldig is als de niet-elektronische variant. Daarnaast brengt de eIDAS-verordening een onderscheid aan tussen gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. De eisen aan gekwalificeerde vertrouwensdiensten zijn zwaarder dan aan niet-gekwalificeerde vertrouwensdiensten én het toezicht is *ex ante*, oftewel de toezichthouder controleert of de vertrouwensdienstverlener voldoet aan de eisen voordat deze dienstverlener zijn diensten mag aanbieden. Dat gebeurt nadat de vertrouwensdienstverlener al een audit heeft ondergaan door een geaccrediteerde conformiteitsbeoordelingsinstantie. Een gekwalificeerde vertrouwensdienstverlener is dus al (dubbel) gecontroleerd wat bijdraagt aan het vertrouwen in deze dienstverlener. De verordening geeft aan dat een gekwalificeerde vertrouwensdienst zondermeer rechtsgeldig is. In de herziening van de verordening is er aan dit kader niets fundamenteels veranderd.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens