Consultatieverslag

Van 8 juli tot en met 8 augustus 2015 is een conceptversie van de uitvoeringswet bij Europese verordening 910/2014 over elektronische identiteiten en vertrouwensdiensten (eIDAS) openbaar gemaakt in een internetconsultatie (www.internetconsultatie.nl/eidas). In totaal zijn er acht reacties ontvangen.
Deze reacties zijn afkomstig van de Stichting ITrustfoundation, KPN, PWC, Connectis, Arthur's Legal B.V., Rijksdienst voor het Wegverkeer, Unie van Waterschappen en een burger. De reacties van de internetconsultatie zijn gegroepeerd naar de onderstaande vier hoofdpunten:
• Samenhang met aanverwante ontwikkelingen;
• Toezicht en certificering;
• Aanvraag gekwalificeerde vertrouwensdienst;
• Kosten en compensatie.

Samenhang met aanverwante ontwikkelingen
Verschillende respondenten hebben gewezen op de samenhang van de verordening met andere onderwerpen, ontwikkelingen, stelsels en voorzieningen. PKI-overheid, Idensys, privacy, informatiebeveiliging, het CAB-forum, Internet of Things, data analytics en constant evoluerende cybersecurity technologieën, zijn genoemd. Daarbij wordt opgemerkt dat wetgeving niet altijd de meest effectieve manier is om spanningsvelden tussen security en privacy op te lossen.

Reactie
De onderwerpen van de verordening en het wetsvoorstel vertonen nauwe samenhang met PKI-overheid en Idensys, het in ontwikkeling zijnde Nederlandse stelsel van elektronische identiteiten voor burgers en bedrijven. Vaak worden de diensten op het gebied van elektronische identificatie door bedrijven aangeboden die ook vertrouwensdiensten leveren. Het is wenselijk dat normering, certificering, toezicht en financiering daarvan zoveel mogelijk hetzelfde wordt geregeld, zodat leveranciers niet voor iedere voorziening te maken hebben met net weer andere eisen, toezicht en bijbehorende financieringsstructuren. Bij de inrichting van het toezicht op Idensys en de mogelijke herinrichting van het toezicht op PKI-overheid zal zoveel mogelijk worden aangesloten op de normen en structuren die uit de verordening en deze uitvoeringswet voortvloeien. Daarbij moet worden onderkend dat verschillen tussen genoemde stelsels en voorzieningen kunnen leiden tot andere eisen en inrichting. Deelnemers zijn bijvoorbeeld op grond van een privaatrechtelijk contract verbonden aan de normen van PKI-overheid. Voor staatstoezicht op deze normen is een wettelijke basis nodig. Omdat het wetsvoorstel minimum-uitvoering van de verordening beoogt, is dit niet het

juiste wetsvoorstel om regelingen te treffen voor Idensys of PKI-overheid. Voornoemde punten zijn onderdeel van het beleid of andere in voorbereiding zijnde wetgeving van de Ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijkrelaties. De samenhang van het wetsvoorstel met privacy en informatiebeveiliging wordt onderkend. Een informatiebeveiligingsincident met een elektronische identiteit of vertrouwensdienst kan leiden tot een inbreuk op de bescherming van persoonsgegevens. De bescherming van persoonsgegevens en het toezicht is geregeld in de Wet bescherming persoonsgegevens (Wbp), die wordt vervangen door een voorstel van de Europese Commissie voor een Algemene verordening gegevensbescherming (COM (2012)11 def). De eidas-verordening en dit wetsvoorstel zijn onderdeel van een juridisch kader dat mede tot doel heeft informatiebeveiligingsincidenten en inbreuken op de bescherming van persoonsgegevens te voorkomen en, ingeval deze zich toch voordoen, te bestrijden. Bij de totstandkoming van de eidas-verordening is de relatie met het CAB-Forum en de wereldwijde dimensie van internet en certificaten meerdere keren aan de orde geweest. De relatie is zowel de Nederlandse overheid als de Europese Commissie bekend. Het is juist dat de verordening noch dit wetsvoorstel van toepassing zijn op het CAB-Forum of Amerikaanse leveranciers van browsers. Dit is een complexe aangelegenheid die wordt veroorzaakt door de territoriale werking van wetgeving enerzijds en de mondiale eisen en technische werking van certificaten anderzijds. Middels handelsverdragen wordt geprobeerd om afspraken te maken over verplicht overleg tussen browserleveranciers, die buiten de Europese Unie zijn gevestigd, en een lidstaat die met een ernstig incident met certificaten te kampen heeft. Op aanverwante ontwikkelingen zoals het Internet of Things en data analytics is ondermeer het voornoemde juridisch kader voor de bescherming van persoonsgegevens van toepassing. Los van de vraag of nadere regulering van deze aanverwante ontwikkelingen wenselijk is, is het wetsvoorstel niet de geëigende plaats om dit te doen.

Toezicht en certificering
Een aantal respondenten geeft aan dat verschillende toezichthouders en het NCSC een rol hebben bij het toezicht op de verordening en de melding en opvolging van incidenten. Respondenten wijzen op de risico's van uiteenlopende informatieverzoeken, onenigheid tussen toezichthouders bij normuitleg en tegengestelde eisen bij het optreden in geval van een crisis. Respondenten pleiten voor eenduidigheid in normering, informatie-inwinning en een gecoördineerd optreden van toezichthouders en NCSC bij een crisis. Een respondent stelt voor om in de uitvoeringswet te bepalen dat betrokken instanties samenwerkingsprotocollen moeten afsluiten waarin wordt aangegeven welk van de toezichthouders bij een crisis het initiatief neemt in de richting van betrokken vertrouwensdienst-verlener(s) en hoe de gezamenlijke verantwoordelijkheden daarbij worden ingevuld. Enkele

respondenten vragen om verduidelijking van de rol en werkzaamheden van de toezichthouder ten opzichte van certificerende instellingen. Respondenten kunnen zich vinden in de in het wetsvoorstel beschreven wijziging van de rol van de toezichthouder, waarbij deze zelf een inhoudelijk oordeel vormt over het voldoen van de vertrouwensdienstverleners aan de eisen van de verordening. Respondenten geven aan dat de toezichthouder hiervoor voldoende middelen, inhoudelijke kennis en gezag moet hebben. Het toezicht dient meerwaarde te hebben en belangrijker dan de bevoegdheidstoedeling is de wijze van invulling van (toezichts-)taken. Daarbij is het belangrijk dat de toezichthouder het werk van de certificerende instellingen niet over gaat doen. Een respondent merkt op dat de frequentie van conformiteitsbeoordelingen in ISO-normen is voorgeschreven en vraagt wat de impact is wanneer buitenlandse vertrouwensdienstverleners op de Nederlandse markt verschijnen die een lagere frequentie hanteren dan in Nederland gebruikelijk is. De respondent pleit voor harmonisatie via de vast te stellen norm voor conformiteitsbeoordelingen (ETSI EN 319 103).

Reactie
Bij het toezicht op de verordening en het voorkomen en verhelpen van crisis zijn AT, het CBP en het NCSC betrokken. AT is primair verantwoordelijke voor het toezicht op de vertrouwensdienstverleners. Het CBP heeft een rol indien de bescherming van persoonsgegevens in het geding is, terwijl het NCSC hulp en ondersteuning biedt bij het verhelpen van cybersecurityincidenten. Dit zijn verschillende rollen die partijen op grond van verschillende wettelijke bevoegdheden uitoefenen. Samenwerking tussen de partijen en eenduidigheid bij optreden ingeval van een crisis is zowel in het belang van de vertrouwensdienstverleners als het oplossen van de crisis. Het voorstel om in het wetsvoorstel op te nemen dat er samenwerkingsprotocollen worden afgesloten tussen toezichthouders en het NCSC om die samenwerking beter te kunnen waarborgen wordt overgenomen (onderdeel M). De rol van de toezichthouder is het toezien op de naleving van de verordening. Daarbij maakt de toezichthouder gebruik van risico- en dreigingsanalyses. Indien de verordening en het bepaalde in het wetsvoorstel niet wordt nageleefd kan de toezichthouder handhavend optreden. Het conformiteitbeoordelingsverslag van de conformiteitsbeoordelingsinstantie, dat gebaseerd wordt op ISO 17065, vormt de basis van het toezicht door Agentschap Telecom. Dit verslag biedt inzicht in het voldoen van de gekwalificeerde vertrouwensdienstverlener en de door hem gekwalificeerde vertrouwensdiensten aan de eisen van de verordening. Het verslag biedt geen rechtsvermoeden dat aan eisen uit de verordening is voldaan. De toezichthouder kan zelfstandig aanvullend onderzoek doen naar deelaspecten, specifieke eisen of thematisch controleren. Daarbij zal de toezichthouder dubbele inspanningen en lasten

voor de vertrouwensdienstverleners zoveel mogelijk voorkomen. Dit punt van respondenten wordt onderschreven en zal in de praktijk vorm moeten krijgen. Om zijn rol te kunnen vervullen en toegevoegde waarde te kunnen bieden, is de opbouw van inhoudelijke deskundigheid bij de toezichthouder een vereiste. Het gaat om kennis van een zeer specialistisch onderwerp die in Nederland in beperkte mate aanwezig is. Het is wenselijk dat de toezichthouder deze kennis zelf in huis heeft en niet afhankelijk wordt van externe inhuur. De verordening bepaalt dat gekwalificeerde verleners van vertrouwensdiensten ten minste eens in de 24 maanden aan een conformiteitsbeoordeling onderworpen moeten worden. Deze eis dient te worden verdisconteerd in de auditschema's die worden gehanteerd. De toezichthouder kan daarnaast op ieder moment zelf een (aanvullende) audit doen. De verordening verplicht tot acceptatie van alle vertrouwensdiensten uit andere lidstaten. Voor gekwalificeerde vertrouwensdiensten uit andere lidstaten geldt, net als voor Nederlandse vertrouwensdiensten, dat deze tenminste eens in de 24 maanden aan een conformiteitsbeoordeling moeten worden onderworpen. Een aanbieder van gekwalificeerde vertrouwensdiensten afkomstig uit een lidstaat waar de toezichthouder een andere audittermijn hanteert dan de Nederlandse toezichthouder, kan zijn diensten zonder belemmering op de Nederlandse markt aanbieden. Bij het bepalen van de audittermijn zal de Nederlandse toezichthouder rekening houden met de termijn die toezichthouders in andere lidstaten bepalen. Betrouwbaarheid gekwalificeerde vertrouwensdienst Een respondent legt de vraag voor of zogeheten gekwalificeerde vertrouwensdiensten kunnen worden aangevraagd met een elektronische identiteit dat een «substantieel» betrouwbaarheidsniveau heeft. Indien dit mogelijk is, beschouwt respondent dit als de introductie van een zwakke schakel in de keten. Respondent vraagt of de verordening het mogelijk maakt dat Nederland ervoor kiest om alleen een elektronische aanvraag met een elektronisch identificatiemiddel van betrouwbaarheidsniveau «hoog» toe te staan. Een andere respondent vraagt of elektronische identiteiten als vertrouwensdiensten in de zin van de verordening kunnen worden aangemerkt.

Reactie
Artikel 24, eerste lid, van de verordening bepaalt dat een gekwalificeerd certificaat kan worden verkregen met een elektronische identiteit van niveau» substantieel» of «hoog». Het gaat hier om een recht dat is gekoppeld aan verplichte erkenning in andere lidstaten. Nederland kan er dan ook niet voor kiezen om alleen een afgifte van een gekwalificeerd certificaat met een elektronisch identificatiemiddel van niveau «hoog» toe te staan. In artikel 24 eerste lid, onder b, is verder bepaald dat de fysieke aanwezigheid van de natuurlijke persoon of de gemachtigde afgevaardigde van de rechtspersoon wordt gewaarborgd voordat een gekwalificeerd certificaat wordt afgegeven. Deze waarborg zorgt ervoor dat de aanvraag en

afgifte van een certificaat niet alleen op een elektronisch identificatiemiddel van niveau «substantieel» of «hoog» kan worden gebaseerd. Hoewel elektronische identiteiten diensten zijn waaraan vertrouwen wordt ontleend, zijn het geen vertrouwensdiensten in de zin van verordening 910/2014 EC. De verordening geeft een limitatieve opsomming van wat vertrouwensdiensten zijn. Voor deze diensten geldt het regime van toezicht en wederzijdse erkenning, zoals in hoofdstuk 3 van de verordening is beschreven. Denkbaar is wel dat aan een elektronisch identificatiemiddel optioneel functionaliteit is toegevoegd, waardoor het tevens als een vertrouwensdienst moet worden aangemerkt. Bijvoorbeeld doordat het elektronisch identificatiemiddel naar keuze van gebruiker ook als elektronische handtekening gebruikt kan worden. In dat geval geldt hoofdstuk 2 van de verordening voor zover het middel als elektronisch identificatiemiddel geschikt is en is daarnaast het toezicht en wederzijdse erkenning uit hoofdstuk 3 van de verordening van toepassing, voor zover het middel tevens als een vertrouwensdienst kan worden gebruikt. Aangezien elektronische identiteiten nauw verwant zijn met vertrouwensdiensten en vaak door dezelfde partijen worden uitgegeven, is het wenselijk dat normering, certificering en toezicht en financiering daarvan zoveel mogelijk op dezelfde wijze vorm krijgt als bij de vertrouwensdiensten.

Kosten en compensatie
Twee respondenten vragen om in de memorie van toelichting in te gaan op de financiële gevolgen van de verordening voor uitvoeringsorganisaties en de waterschappen. De memorie van toelichting gaat volgens hen nu alleen in op de gevolgen voor het bedrijfsleven en de medeoverheden, terwijl uitvoeringsorganisaties en de waterschappen ook kosten moeten maken. Een respondent geeft aan dat de code interbestuurlijke verhouden voorschrijft dat de waterschappen, net als gemeenten en provincies, gecompenseerd dienen te worden voor de financiële gevolgen van de verordening.

Reactie
In het onderzoek naar de financiële gevolgen van de verordening zijn de waterschappen meegenomen. De financiële gevolgen van de verordening zijn per waterschap of uitvoeringsorganisatie niet anders dan voor een gemeente of provincie. De code interbestuurlijke verhoudingen stelt dat het Rijk bij beleidsvoornemens die relevant zijn voor gemeenten en provincies inzicht geeft in de financiële consequenties, de bestuurlijke, praktische en informationele gevolgen en dat dit ook geldt voor de waterschappen. De memorie van toelichting is aangepast, zodat die inzicht biedt in de kosten van de verordening voor de waterschappen. De waterschappen zijn niet genoemd in artikel twee van de Financiële Verhoudingswet. De code Interbestuurlijke verhouding bevat evenmin een verplichting om de

waterschappen te compenseren voor de kosten die implementatie van de verordening met zich meebrengt.