Consultatie van het voorontwerp van de

Uitvoeringswet eidas-verordening

Reactie van KPN

KPN
Contactpersoon: mr. P.C. Knol
Postbus 30 000
2500 GA Den Haag
paul.knol@kpn.com

Kenmerk: GCO/15/U/056

7 augustus 2015

Algemeen

KPN heeft kennis genomen van het voorontwerp voor een wetsvoorstel 'Uitvoeringswet eidas-verordening'. Hoewel het wetsvoorstel voornamelijk de bevoegdheidsverdeling regelt die vanaf 1 juli 2016 – bij de inwerkingtreding van een groot deel van de rechtstreekse werkende verordening – moet ingaan, komen bij lezing van het ontwerp en de toelichting daarbij nog enkele vragen en opmerkingen op, die in deze reactie worden aangegeven.

Algemene opmerkingen

Zoals uit de ontwerp memorie van toelichting op veel plaatsen blijkt gaat het bij zowel elektronische identificatie als vertrouwensdiensten om één centraal begrip: vertrouwen. Het spreekwoord zegt: 'vertrouwen komt te voet en gaat te paard' en daarmee is precies blootgelegd dat het hier gaat om een gevoelig onderwerp. Een goed werkend systeem van e-identificatie en beschikbaar stellen van elektronische handtekeningen, zegels en tijdstempels is noodzakelijk voor een goed functionerend elektronisch berichtenverkeer, maar als zich incidenten voordoen is het vertrouwen in die middelen snel geschaad en zal dat een grote weerslag hebben op (het gebruik van) het elektronisch berichtenverkeer.

De materiële normen betreffende de erkenning van elektronische identificatie in de EU en vertrouwensdiensten zijn vanaf de inwerkingtreding nog meer dan voorheen niet meer nationaal vast te leggen. Het past bij het streven naar een Europese Digitale Interne markt om binnen de EU erkenning en gebruik van nationale stelsels na te streven en normen alleen nog op communautair niveau vast te stellen. Tegelijkertijd moet daarbij bedacht worden dat in deze keten van spelers en verantwoordelijkheden het na te streven 'vertrouwen' wordt bepaald door de zwakste schakel. Hoewel de Verordening al is vastgesteld en Nederland daarmee geen rechtstreekse invloed meer heeft op de inhoudelijke vaststelling van normen blijft het van belang dat de overheid op alle terreinen nastreeft om een zo hoog mogelijk niveau van betrouwbaarheid van de informatie-uitwisseling en beveiliging na te streven. Dat kan betekenen dat Nederland invloed aanwendt om eventueel gesignaleerde gebreken in het niveau van betrouwbaarheid van andere lidstaten aan de orde te stellen. Dat kan echter alleen als Nederland zelf een adequaat niveau heeft van deskundigheid om – waar mogelijk in overleg met betrokken marktpartijen – de vinger aan de pols te kunnen houden en de technische ontwikkelingen bij te houden.

In dat opzicht is van het voorliggende wetsvoorstel veel meer van belang hoe de invulling van de (toezichts-)taken zal worden ingevuld dan de formele bevoegdheidstoedeling die hiermee wordt geregeld. In de toelichting wordt beschreven dat het meer inhoudelijke toezicht dat ter naleving van de bepalingen van de Verordening beter past bij de taken en functies van het Agentschap Telecom, dan bij ACM, waar tot op heden het toezicht is neergelegd. KPN gaat ervan uit dat binnen het departement en in overleg met ACM die conclusie is getrokken en neemt dat graag aan. Van belang is dan wel dat binnen het Agentschap voldoende deskundigheid kan worden opgebouwd en dat de middelen daarvoor in voldoende mate ter beschikking worden gesteld.

In het navolgende komen we op deze algemene opmerkingen terug.

Aanpassingen hoofdstukken 1, 2 en 15 Tw: verschuiving van toezicht

De voorgestelde wijzigingen vloeien voort uit de Verordening zelf en de keuze om het toe-

zicht van ACM over te dragen naar het AT. Zoals bij de algemene opmerkingen al aangegeven heeft KPN op zich geen bezwaar tegen deze wijzigingen, maar hangt veel ervan af hoe die rol door het AT wordt ingevuld en hoeveel ruimte het AT krijgt om de daarvoor benodigde specifieke kennis te verwerven. In de toelichting is meermalen aangegeven dat de 'Diginotar affaire' aanleiding om tot een andere vorm van toezicht te komen. Dat hiertoe echter pas bijna vier jaar na die affaire een grondslag voor wordt gecreëerd – en in de tussenliggende tijd het toezicht niet wezenlijk is aangepast – geeft echter niet de indruk van grote urgentie.

De Diginotar affaire heeft – volgens KPN – mede geleerd dat de toezichthoudende rol niet alleen moet toezien op het toezicht op de naleving van structurele verplichtingen, maar ook dat er voldoende deskundigheid en praktische (markt)kennis bij de toezichthouder moet zijn om indien zich een incident of crisis voordoet met voldoende gezag en overlegvaardigheden (vaak ook met overige marktpartijen en instanties) snel te kunnen acteren.

Een andere belangrijke vraag die als zodanig niet in het wetsvoorstel wordt geregeld is hoe de beveiliging van de informatie bij de toezichthouders (ACM en AT) is geregeld en hoe de overdracht van die uiterst vertrouwelijke informatie op een voldoende beveiligde manier wordt geregeld. Zonder enig wantrouwen ten aanzien van de inzet van betrokkenen uit te spreken wil KPN wel benadrukken dat hierbij niet alleen hoge eisen aan betrokken eigen personeel moet worden gesteld, maar ook aan de gebruikte systemen, communicatiemiddelen en eventueel in te schakelen derden. Het zou wenselijk zijn als in de toelichting op het wetsvoorstel wordt aangegeven welke waarborgen de Minister daarvoor opneemt.

Meerdere toezichthouders

Aanbieders van vertrouwensdiensten (TSP's), hun toezichthouders (College bescherming persoonsgegevens, art 11.5c, het Agentschap Telecom, Onderdeel L, artikel 18.2a) en in mindere mate het NCSC hebben te maken met verschillende normen uit verschillende bronnen. De bronnen voor normen betreffen EU regelgeving, ETSI-normen, aanvullende of specifieke nationale regelgeving (hetzij van de Minister, hetzij van AT), specifieke regelgeving vanuit de hiërarchie waarbinnen de certificaten worden uitgegeven (bijvoorbeeld het Symantec Trust Network Certificate Policy of PKI-overheid Programma van Eisen) en tot slot de CAB-forum-normen (bepaalde ETSI-normen verwijzen hiernaar). Dat resulteert voor een gemiddelde TSP op dit moment in globaal 1000 tot 1500 normen waaraan moet worden voldaan. Daarbij zij gezegd dat deze normen ook nog redelijk frequent aan verandering onderhevig zijn, dat het aantal toeneemt en dat verschillende normen die bijvoorbeeld betrekking hebben op hetzelfde proces niet helemaal eensluidend zijn of elkaar in een enkel geval zelfs tegenspreken.

Los van het feit dat daar zeer veel tijd en energie in gaat zitten en dat dat allerlei praktische problemen met zich mee brengt (bijvoorbeeld op het gebied van de kostprijsberekening) leidt dit binnen elke TSP tot een discussie over wat elke individuele norm nu precies betekent. Dat zal het geval ook zijn bij de toezichthouder als ook bij de certificerende instelling.

De vraag is nu hoe voorkomen gaat worden dat een TSP gezien de normen – die op grond van haar eigen risicoanalyse, gewikt en gewogen hebbende, komend tot een bepaalde set maatregelen en die implementeert (met hoge kosten) – geconfronteerd wordt met onenigheid tussen certificerende instelling en/of (één van) de toezichthouders of tussen toezichthouders onderling. Het lijkt gewenst dat er in het algemeen meer en betere afstemming gaat plaats vinden tussen normenstellers (bijvoorbeeld binnen en met ETSI) en het lijkt ge-

wenst in de MvT richting te geven aan coördinatie en afstemming tussen certificerende instelling en toezichthouders.

Melding van incidenten

Uit de toelichting (par. 5.4) blijkt dat naast het AT als toezichthouder de facto ook het CBP en NCSC een rol spelen bij het melden van incidenten en de facto daarmee ook als (een soort) toezichthouder optreden. Ieder van deze drie instanties ontleent zijn bevoegdheid aan een andere grondslag en kent eigen bevoegdheden. Ze zullen elk eigen opslag van informatie en eigen beveiligingssystemen hebben. Mogelijk zullen zij ook elk eigen externe deskundigen betrekken. Het is uiterst onwenselijk dat in het midden blijft hoe praktisch het toezicht zal gaan lopen indien zich situaties als hier bedoeld met overlappende bevoegdheden zullen voordoen. Voor marktpartijen zou het – juist in 'crisis' situaties – niet doenlijk zijn om met drie verschillende instanties tegelijkertijd in gesprekken, toezicht en informatieverzoeken betrokken te raken. Minimaal zou in de wet bepaald moeten worden dat voor deze situaties de betrokken instanties samenwerkingsprotocollen zullen moeten afsluiten waarin wordt aangegeven welk van de toezichthouders het initiatief neemt in de richting van betrokken ondernemingen en hoe de gezamenlijke verantwoordelijkheden dan daarbij worden ingevuld. In de Tw is dat in andere gevallen van samenlopende bevoegdheden al veel vaker toegepast. Voorkomen moet worden dat ondernemingen zelfs zouden kunnen worden geconfronteerd met tegengestelde eisen ten aanzien van oplossingen, verstrekking van gegevens met telkens andere doorsnijdingen, meermalen overleg over dezelfde onderwerpen met andere deskundigen, etc.

Het in het midden laten hiervan kan meebrengen dat bij concrete incidenten de aandacht meer uitgaat naar het 'managen' van drie toezichthouders dan aan het oplossen van het incident. Daarbij is niemand gebaat.

De meer materiële bepalingen van hoofdstuk 18 Tw

Hoewel KPN erkent dat een groot deel van de wijziging van de bepalingen van hoofdstuk 18 Tw noodzakelijk wordt door inwerkingtreding van de Verordening, heeft KPN wel een aantal vragen en opmerkingen bij de tekst of (vooral) toelichting bij de nieuw voorgestelde bepalingen. Hoewel het daarbij misschien lijkt te gaan om details, meent KPN dat de genoemde punten een rol kunnen spelen bij de noodzakelijke betrouwbaarheid van de gehele keten, zoals bij de algemene opmerkingen benoemd.

- In artikel 18.15c, zesde lid, wordt gesproken van een 'soortgelijk buitenlands register'. In de toelichting wordt niet aangegeven aan welke kwaliteitseisen buitenlandse registers moeten voldoen om als 'soortgelijk' aan het Nederlands handelsregister te kunnen kwalificeren. Moet bijvoorbeeld een dergelijk register berusten op publiekrechtelijke (wettelijke) grondslag? Zo niet, hoe wordt dan bewaakt dat de opgenomen informatie adequaat en moeilijk vervalsbaar is? Het zou wenselijk zijn hieraan in de toelichting aandacht te besteden.

- Artikel 18.15d geeft aan dat identificatie op afstand 'kan' plaatsvinden met een identificatiemiddel met een betrouwbaarheidsniveau 'substantieel of hoog'. Dit levert een aantal bedenkingen en vragen op:

- Uit de MvT blijkt dat aan een gekwalificeerde vertrouwensdienst een hoog niveau van betrouwbaarheid kan worden toegekend. Dat blijkt uit:
    - Het MvT onderdeel 2.3 Certificaten onderdeel van vertrouwensdiensten stelt het volgende 'In de verordening worden specifieke eisen gesteld aan het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen, voor elektronische zegels en voor website-authenticatie (artikel 3, vijftiende lid, dertigste lid en achtendertigste lid). Dit zijn certificaten waaraan door de daarvoor geldende specifieke eisen en het toezicht daarop een hoog betrouwbaarheidsniveau wordt toegekend.'.
    - MvT Onderdeel A, artikel 1.1, onderdeel tt: De verordening maakt onderscheid tussen gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. Aan gekwalificeerde vertrouwensdiensten kan door de daaraan in de verordening gestelde eisen een hoog niveau van betrouwbaarheid worden toegekend.
- Aannemende dat voor de Vertrouwensdiensten eenzelfde definitie geldt als voor identificatiediensten (zie artikel 8 van de Verordening) dan is het moeilijk te begrijpen dat voor het aanvragen van een Vertrouwensdienst, met een klaarblijkelijk hoog betrouwbaarheidsniveau, gesteund mag worden op een identificatiemiddel van het niveau substantieel.
- Te meer daar
    - Elektronische identificatie wordt geregeld in nationale stelsels (zie hoofdstuk II van de Verordening). Daartussen zijn dus allerhande verschillen mogelijk. Dat heeft Richtlijn 1999/93/EG wel geleerd.
    - Het toezicht op deze stelsels (mogelijk) binnen de stelsels (op nationaal niveau) geregeld (artikel 9, lid 1b van de Verordening) wordt.
    - De definities van de termen laag, substantieel en hoog tamelijk vaag zijn (art 8 van de verordening). Substantieel verschilt van laag qua definitie alleen in de woorden 'beperkt' (betrekkelijk klein) versus 'substantieel' (aanzienlijk, belangrijk, wezenlijk). Dat zijn relatieve termen.
      De definities van de termen 'Substantieel' verschilt van 'hoog' op het punt van dat het risico van misbruik of wijziging van identiteit dient te worden 'verkleind', dan wel dient te worden 'voorkomen'. Verkleinen is een relatieve term en het voorkomen van risico's is niet mogelijk.
- Omdat de keten zo sterk is als de zwakste schakel lijkt het erop dat identificatie op basis van een identificatiemiddel van het niveau 'substantieel' wel een hele zwakke schakel gaat vormen voor het betrouwbaarheidsniveau van een gekwalificeerde vertrouwensdienst met dus het betrouwbaarheidsniveau 'hoog'. Ten eerste omdat de Verordening het mogelijk maakt, ten tweede omdat elektronische identificatie op nationaal niveau wordt geregeld en ten derde omdat de definities ruimte bieden voor verschillende interpretaties.
- Bovendien lijkt het erop dat alle andere bepalingen, eisen, normen en regels daarmee in bepaalde mate overdone worden en daarmee alle door alle TSP's genomen/te nemen maatregelen in meer of minder mate inefficiënt worden.
- Uit de 'kan' formulering blijkt dat de gekwalificeerde verlener er niet toe over hoeft te gaan en zou kunnen bepalen dat alleen bij een betrouwbaarheidsniveau 'hoog' hiertoe zou kunnen overgaan. Dat roept de vraag op of de Verordening het ook mogelijk maakt dat dit in Nederland algemeen wordt toegepast en het niveau 'substantieel' onvoldoende is?

- Uiteindelijk gaat het er hier niet om welke kwalificatie wordt toegekend aan een betrouwbaarheidsniveau, maar hoe dit op een noodzakelijk kwaliteitsniveau zal worden vastgesteld. Het zou zeer wenselijk zijn als in de memorie van toelichting wordt aangegeven op welke manier de Nederlandse overheid denkt dat dit bereikt kan worden.

- Artikel 18.15e, eerste lid, geeft aan dat indien in een gekwalificeerd certificaat andere specifieke gegevens bevat dan volgens de Verordening vereist, de dienstverlener dient te zorgen voor dat de juistheid van die gegevens, vastgesteld op een niveau dat past bij de betrouwbaarheid die aan de status gekwalificeerd wordt toegekend. In de MvT wordt v.w.b. persoonsgegevens gesteld dat verificatie dient plaats te vinden overeenkomstig Nationale wetgeving, daar waar dat niet mogelijkheid wordt volstaan met de mededeling dat dat moet gebeuren op een passende wijze. Dit geeft wel erg weinig indicatie over de eisen die daaraan gesteld worden. Het zou wenselijk zijn dit te verduidelijken.

- Artikel 18.15e, tweede lid, bepaalt dat indien specifieke gegevens in een openbaar toegankelijk register zijn opgenomen, ten aanzien van die gegevens aan dat lid wordt voldaan indien de gekwalificeerde verlener van vertrouwensdiensten voorafgaand aan de uitgifte van het gekwalificeerd certificaat de juistheid van die gegevens door raadpleging van dat register vaststelt. Er lijken geen eisen te worden gesteld aan de kwaliteit van de inhoud van dat openbare register. Dient het een betrouwbaar register te zijn? Dient dat vastgesteld te worden? Dient het een wettelijke basis te hebben? Dient het een zekere internationale status te hebben?

Vragen naar aanleiding van de Memorie van Toelichting

Enkele passages uit de toelichting bij het voorontwerp roepen nadere vragen op:

- Op p. 3, 2e alinea, staat: '*De controle over het gebruik van persoonsidentificatiegegevens berust bij de persoon van wie de identiteit is*.' De context hiervan is dat persoonsidentificatiegegevens die zijn opgeslagen in een chip die is geïntegreerd in een pasje of aanwezig zijn in een beveiligde omgeving binnen een informatiesysteem. Het is duidelijk dat de gegevens bij die persoon behoren, maar vanuit de context (en de Wbp) is duidelijk dat ook de bewerker van die gegevens een bepaalde rol heeft. Als het gaat om opslag van deze gegevens in een beveiligde omgeving, is dan niet de Verantwoordelijke, degene die de gegevens verzamelt en bewerkt en opslaat, die verantwoordelijk is voor (de controle over) het gebruik ervan, voor zover het gebruik van deze gegevens binnen het domein van de Verantwoordelijke gebeurt?

- Op p. 3, 2e alinea, staat: '*Het is gericht op het creëren van gewaarborgd vertrouwen bij een ander.*' Moet in die zin 'gewaarborgd' niet 'gerechtvaardigd' zijn? In een bepaalde onzekere situatie wil men op iets kunnen vertrouwen. Het vertrouwen dient gerechtvaardigd te zijn. Als het vertrouwen gewaarborgd moet zijn is geen sprake meer van een onzekere situatie.

- Op p. 6 (par 3.1, 2e alinea) staat: '*De verordening is tevens van toepassing op vertrouwensdiensten die aan het publiek worden aangeboden (zie hiervoor verder de toelichting bij artikel I, onderdeel F)*.' Artikel 2 van de verordening (Toepassingsgebied) stelt in lid 2: '*Deze verordening is niet van toepassing op de verlening van vertrouwensdiensten die uitsluitend in systemen die gesloten zijn als gevolg van nationaal recht of overeenkomsten tussen een welbepaalde groep deelnemers*.' Is daarmee 'niet aan het publiek' synoniem met 'die gesloten zijn als gevolg van nationaal recht of overeenkomsten tussen een welbepaalde groep deelnemers'?

- In par. 5.4 (p. 12, 2e alinea) staat aangegeven: '*Vanuit oogpunt van duidelijkheid, voorzienbaarheid en kenbaarheid kan het noodzakelijk zijn omstandigheden en criteria aan te duiden waaronder een melding vereist is. De Minister van Economische Zaken kan hierin door middel van beleidsregels en/of richtsnoeren voorzien uit hoofde van het toezicht op de naleving van de verordening en de Minister van Veiligheid en Justitie voor een melding aan het NCSC*.' KPN zou graag benadrukken dat het niet alleen wenselijk is, maar zelfs noodzakelijk om hierover tevoren duidelijkheid te verkrijgen.

- In par. 5.6 Uitvoeringsmaatregelen staat aan het eind (p. 16) de volgende alinea: '*De verordening bepaalt dat lidstaten regelgeving kunnen vaststellen over de tijdelijke schorsing van gekwalificeerde certificaten voor gekwalificeerde elektronische handtekeningen en gekwalificeerde elektronische zegels. In de internationale ETSI standaarden wordt de mogelijkheid van het opschorten van certificaten – naast het intrekken- feitelijk nu al geboden, maar het ondersteunen daarvan door gekwalificeerde vertrouwensdienstverleners is optioneel. De gedachte achter het opschorten is dat iemand de status van een certificaat niet vertrouwt en de vertrouwensdienstverlener daarover inlicht. De vertrouwensdienstverlener wil deze melding verifiëren bij de certificaathouder en gedurende die tijd schort de vertrouwensdienst-verlener het certificaat op. Wanneer er niets aan de hand blijkt te zijn dan wordt het certificaat weer geldig gemeld en anders definitief ingetrokken. In Nederland wordt van de mogelijkheid tot het opschorten van certificaten geen gebruik gemaakt. Er is geen behoefte om deze lijn te wijzigen. In het (private) programma van eisen PKI-overheid is vastgelegd dat het niet toegestaan is certificaat-opschorting te ondersteunen.*' Deze passage is niet goed te plaatsen na de voorafgaande alinea, waarin het gaat over de relatie tussen de beschikbaarheid van een verslag/verklaring van een conformiteitsbeoordelingsinstantie en de overeenstemming met de in de verordening genoemde eisen. Deze alinea gaat over de mogelijkheid tot schorsing van gekwalificeerde certificaten. Dat lijkt heel wat anders.

- In par. 5.8 Uitvoeringsmaatregelen (p. 17, 1e alinea) wordt vermeld: '*Zoals hiervoor is toegelicht biedt de verordening in tegenstelling tot de richtlijn geen basis meer voor vrijwillige conformiteitsbeoordeling met toekenning van een wettelijk vermoeden dat aan eisen is voldaan*.' Toch dienen conformiteitsbeoordelingen te worden uitgevoerd en dient bijvoorbeeld een verslag of rapport van een dergelijke conformiteitsbeoordeling te worden meegestuurd. Toekenning van een wettelijk vermoeden is te veel, maar toch dient een toezichthouder er wat mee te doen, er op te steunen. De toezichthouder mag er zijn oordeel niet op baseren, maar hij mag en moet het wel gebruiken. Daartussen lijkt een soort van vacuüm te ontstaan. De vraag is wat gaat de toezichthouder nu precies wel doen met zo'n rapport? Het zou wenselijk zijn om hieraan in de toelichting meer aandacht aan te besteden.

- In par. 5.8 Uitvoeringsmaatregelen (p. 17, 2e alinea) wordt vermeld: '*In opdracht van de Europese Commissie wordt gewerkt aan een conformiteitbeoordelingsschema voor de verordening*.' Is dat Draft ETSI EN 319 403 V2.1.1 (2014-12) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers? Als dat schema er komt, is er dan nog ruimte voor een Nederlands schema? Is er dan nog een schemabeheerder nodig?

- In de toelichting op onderdeel F, artikel 2.5b, wordt beschreven dat de procedure voor registratie van een dienstverlener van vertrouwensdiensten, die gekwalificeerd wil worden, bepaalt dat eerst een conformiteitsverslag ingediend dient te worden, dat daarna de toezichthouder het rapport bestudeert, aanvullend onderzoek verricht (daar drie maanden de tijd voor heeft) en – bij welbevinden – de status toekent. Formeel betekent dit dat het in te dienen conformiteitsverslag alleen een beoordeling van de opzet van het managementsysteem kan bevatten. Betekent dit dat op een zeker moment, maximaal twee jaar later, de bestaan en werking van het management systeem worden gecontroleerd? Het lijkt wellicht verstandig om aan dit proces meer richting te geven.

  Daar komt bij dat de drie maanden termijn wel erg lang is. Dat kan ertoe leiden dat een dienstverlener een behoorlijke investering doet om te kunnen produceren, met goed gevolg een conformiteitsaudit doorloopt, maar daarna maximaal drie maanden moet stilzitten voordat het kan produceren. Is het niet mogelijk deze termijn te bekorten? In het voortraject kan het proces worden afgestemd, capaciteit worden gereserveerd etc. Daarenboven wordt volgende gesteld 'Indien de verificatie door het toezichthoudend orgaan niet binnen die drie maanden is afgerond, brengt het toezichthoudend orgaan de verlener van vertrouwensdiensten op de hoogte van de redenen voor de vertraging en van de termijn waarbinnen de verificatie zal zijn afgerond'. Er zijn voor KPN maar weinig acceptabele redenen voor een eventuele vertraging aan te geven.

KPN is graag bereid de voorgaande vragen en opmerkingen desgewenst toe te lichten.