EVALUATIE PKI

Rapportage

be brilliant together

Colofon
Versie 1.0, 8 maart 2012

Logica Business Consulting

Opgesteld door:
Ir. J.N. (Niek) IJzinga (Principal Consultant Security)
Ir.drs. A.E. (Albert) Vlug (Principal Consultant Public Sector)

Review:
Drs. A.E. (Alex) Klaassen RE (Principal Consultant IT-Auditing & Security)
F.H.B. (Frans) Kersten RE RA (Principal Consultant IT-Auditing & Security)

Ter attentie van
Mw. Drs. B. (Bertine) Steenbergen, Directeur Burgerschap en Informatiebeleid, ministerie van BZK
Mw. Dr. L.M.N. (Nicole) Kroon, Directeur Regeldruk en ICT-beleid, ministerie van EL&I

INHOUDSOPGAVE

1 MANAGEMENT SAMENVATTING

Beveiliging van elektronische communicatie is van eminent belang in de huidige informatie-samenleving. Partijen die de betrouwbaarheid van digitale beveiliging vormgeven moeten vertrouwd kunnen worden. DigiNotar was zo'n partij, maar is toch gecompromitteerd. Een hacker was in staat om in te breken in de omgevingen van DigiNotar en op afstand valse digitale certificaten te produceren die onder andere konden worden misbruikt om vertrouwelijke communicatie af te luisteren.

De gefalsificeerde certificaten werden in het private domein geproduceerd en uitgegeven. Controle hierop is ook privaat geregeld door een consortium van leveranciers van onder andere webbrowsers. Deze 'eigen merk' certificaten van DigiNotar werden gebruikt door burgers, private partijen en overheden. De overheid heeft geen invloed op de gang van zaken bij dergelijke private partijen, behalve in de rol van afnemer.

DigiNotar gaf naast de certificaten voor beveiligde websites, ook certificaten uit onder twee stelsels met een vorm van overheidstoezicht. Het ene stelsel is dat van *PKIoverheid* en het andere stelsel betreft de zogenaamde '*gekwalificeerde certificaten*'. Het stelsel PKIoverheid is primair bedoeld om veilige elektronische communicatie door en tussen overheden te faciliteren. Het stelsel gekwalificeerde certificaten is opgezet om elektronische handtekeningen in Nederland, in lijn met een Europese Richtlijn, een solide juridische basis te geven. Ten aanzien van PKIoverheid heeft het ministerie van BZK een (niet-wettelijke) toezichtstaak. Voor het stelsel van gekwalificeerde certificaten is wettelijk toezicht geregeld en belegd bij de Opta. Een inbraak in de omgeving waar DigiNotar de website-certificaten aanmaakte, betekent niet automatisch dat de omgevingen waar een vorm van overheidstoezicht op geregeld is ook gecompromitteerd zijn. Begin september 2011 rapporteerde Fox-IT tijdens een technisch forensische analyse echter dat dit bij DigiNotar niet kon worden uitgesloten: de hacker was ook actief geweest in de omgevingen waar PKIoverheid certificaten en gekwalificeerde certificaten worden geproduceerd.

De primaire verantwoordelijkheid voor een deugdelijke informatiebeveiliging van DigiNotar lag bij het management van de certificatiedienstverlener. Van eindverantwoordelijken voor een bedrijf dat haar bestaansrecht ontleent aan het leveren van diensten op het gebied van vertrouwensinfrastructuur mag worden verwacht dat informatiebeveiliging een topprioriteit krijgt. Het management van DigiNotar is hierin tekortgeschoten. De organisatie rond certificatie-dienstverleners, de normen waaraan ze moeten voldoen en het toezichtsarrangement hebben dit niet kunnen voorkomen terwijl ze hiervoor wel bedoeld waren.

De compromittering van DigiNotar heeft in ernstige mate het vertrouwen in veilige digitale communicatie geschaad en vroeg om een gedegen evaluatie van de stelsels die zijn bedoeld om deze veiligheid op basis van certificaten zeker te stellen. Het ministerie van BZK, dat verant-woordelijk is voor het beheer en toezicht op het PKIoverheid stelsel, en het ministerie van EL&I, dat beleidsverantwoordelijk is voor het stelsel van de gekwalificeerde certificaten, hebben

gezamenlijk opdracht gegeven tot het onderzoek waarvan de rapportage voor u ligt. Het doel van het onderzoek was om vast te stellen welke *risico's* de beide stelsels bevatten, of het *normenstelsel* nog toereikend is en of het *toezichtsarrangement* adequaat functioneert. Een analyse van het DigiNotar incident op zich zelf maakte geen deel uit van de opdracht. Verder is advies gevraagd over mogelijke alternatieven en over de eventuele implicaties voor de *Europese Richtlijn* op de elektronische handtekeningen die in 2012 wordt herzien.

Om de aanpak en de werking van de stelsels in de praktijk te kunnen analyseren zijn er, naast een documentatieonderzoek, 20 interviews gehouden en zijn er waarnemingen gedaan bij certificatiedienstverleners. Het onderzoek heeft plaatsgevonden in de maanden oktober 2011 tot en met januari 2012. De belangrijkste conclusies worden hieronder samengevat.

De stelsels hebben tot doel het vertrouwen te bewerkstelligen, dat nodig is voor veilige elektronische communicatie. Uit de opzet van de stelsels blijkt dat men dit vertrouwen destijds consciëntieus heeft willen borgen. Volledige zekerheid over beveiliging is nooit te geven, het gaat om *gerechtvaardigd vertrouwen*. Er kan worden geconcludeerd dat er geen sprake is van falen van de stelsels op één enkel aspect (de 'silver bullet'). Er blijkt licht te zitten tussen de verwachte betrouwbaarheid en de feitelijk gerealiseerde betrouwbaarheid. De normenstelsels, de toezichthouders, de auditors, en de accreditering zijn bedoeld om een deugdelijke grondslag te leveren voor het vertrouwen, maar op al deze aspecten zijn aanscherpingen en verbeteringen nodig. Op hoofdlijnen gaat het om de volgende zaken.

- Het toezichtsarrangement is niet ingericht om het beoogde vertrouwen te rechtvaardigen.
- De normenstelsels zijn te complex en op onderdelen onvoldoende concreet, met name als het gaat om bijvoorbeeld het aspect informatiebeveiliging.
- De uitvoering en opvolging van risicoanalyses spelen in de stelsels niet de rol die op grond van snel veranderende dreigingsprofielen zou mogen worden verwacht. Risicobeheersing van de maatschappelijke risico's is stelseloverstijgend en niet structureel ingericht.
- Voor belanghebbenden is de feitelijk geleverde betrouwbaarheid onvoldoende transparant.
- De stelsels zijn primair nationaal georiënteerd en in de praktijk is er vrijwel geen grensoverschrijdende Europese markt voor deze diensten.

Hieronder worden de hoofdconclusies nader beschreven.

Door de opkomst en het wereldwijde gebruik van internet is de *dreiging* van een digitale inbraak de afgelopen jaren aanzienlijk toegenomen. De Nederlandse stelsels zijn hierin niet meegegroeid. De leveranciers van webbrowsers maken deel uit van een netwerk waarin het internet 24 uur per dag en 7 dagen per week op verdachte gebeurtenissen wordt gemonitord.

De toezichthouders zijn mede afhankelijk van signalen die derde partijen afgeven, maar dit is binnen de stelsels niet geborgd. In Nederland werken we met het toezicht zoals dat 10 jaar geleden bedoeld was. Ook speelt *risicoanalyse* niet de centrale rol in de stelsels, die het gezien de snel veranderende dreigingen, wel verdient. Registratie bij de Opta is in beide stelsels verplicht, en er is destijds gekozen voor een lichte vorm van toezicht. Daarbij mag worden vertrouwd op een conformiteitsverklaring van een auditor. De auditrapporten met verbeterpunten voor certificatiedienstverleners worden door de Opta één keer per jaar opgevraagd. Afwijkingen van de norm worden door auditors beschreven, maar leiden in de praktijk niet tot het intrekken van een conformiteitsverklaring. In de stelsels zijn weken tot maanden de tijd om afwijkingen op te lossen. In de praktijk heeft het soms enkele jaren geduurd voordat een belangrijke systeemcomponent goed geconfigureerd was.

In Nederland is het mogelijk dat de partijen die certificatiedienstverleners auditen, zich laten accrediteren. De Raad voor Accreditatie realiseert hiermee extra kwaliteitsborging van de auditors. Conform de Europese Richtlijn mag certificatiedienstverleners niet worden verplicht zich te laten auditen door geaccrediteerde auditors, maar in Nederland hebben alle dienstverleners tot op heden vrijwillig voor deze route gekozen. De Raad voor Accreditatie maakt een onderscheid tussen het certificeren van producten en van management systemen. Bij het accrediteren van partijen die certificatiedienstverleners mogen auditen, is gekozen voor *management systeem audits*, en niet voor IT-audits. In de praktijk wordt er door de auditors wel steekproefsgewijs gekeken naar de IT, maar dit is niet structureel en volgt niet eenduidig uit de eisen die aan de auditors worden gesteld. De audits hebben bovendien betrekking op een periode in de toekomst en niet in het verleden. Over de toekomst kan door auditors minder zekerheid worden afgegeven dan over het verleden. De wijze van auditen van de eisen in het stelsel PKIoverheid, is gelijk aan die voor het stelsel voor gekwalificeerde certificaten. In de praktijk worden deze audits doorgaans gecombineerd. De auditrapporten dienen twee doelen, hetgeen niet zichtbaar is in de structuur van de rapporten. Voor beide stelsels geldt dat conformiteit van het management systeem op procesniveau wordt beoordeeld, terwijl conformiteit in de praktijk tegen alle concrete eisen wordt verwacht. Door het uitvoeren van IT-audits en door onafhankelijke operationele monitoring zou de feitelijke betrouwbaarheid van de dienstverlening kunnen worden versterkt.

Gekwalificeerde certificaten kunnen in Nederland, in tegenstelling tot bijvoorbeeld in Duitsland, ook onder het stelsel PKIoverheid vallen. De normen die voor beide stelsels gelden kennen een *onderlinge afhankelijkheid*. Het Programma van Eisen van het PKIoverheid stelsel verwijst naar het normenstelsel van de gekwalificeerde certificaten. Daarbij worden de normen geconcretiseerd, vaak strenger gemaakt. Ook worden er aanvullende eisen beschreven. Opname van een certificatiedienstverlener in het stelsel PKIoverheid vindt plaats op basis van een auditrapport waaruit blijkt dat conformiteit met de overlappende normen en met de aanvullende PKIoverheid normen aangetoond kan worden. Op basis van hetzelfde auditrapport wordt door de auditors een conformiteitsverklaring in het kader van de gekwalificeerde certificaten afgegeven. Dit komt de *transparantie en eenduidigheid* in de toepassing van de

normenkaders niet ten goede terwijl dat essentieel is voor de verstrekte zekerheid en het daarop gebaseerde vertrouwen.

Conformiteit met wet- en regelgeving ten aanzien van elektronische handtekeningen is voor beide stelsels noodzakelijk. Het is opmerkelijk dat deze conformiteit slechts indirect wordt getoetst. Verklaringen van externe auditors bevatten geen verwijzing naar het wettelijk kader. Er wordt verwezen naar bepaalde Europese normen, omdat verondersteld wordt dat deze normen de *wettelijke eisen toetsbaar maken*. In de Nederlandse wet- en regelgeving is op basis van deze veronderstelling een zogenaamd 'rechtsvermoeden' vastgelegd waarin bepaald wordt dat conformiteit met deze Europese normen gelijk staat aan conformiteit met bepaalde wettelijke eisen. Er zit echter licht tussen de wettelijke bepalingen in Nederland en de veronderstelde uitwerking ervan in de Europese normen. Zo zijn er bepalingen uit de Europese Richtlijn, bijvoorbeeld ten aanzien van de privacybescherming, die niet in het normenstelsel en ook niet in de Nederlandse wet terecht zijn gekomen. Andere wettelijke bepalingen, zoals die over de *informatiebeveiliging*, zijn niet toetsbaar uitgewerkt in de normen. Certificatiedienstverleners dienen zich aan bepaalde wettelijke bepalingen te houden, maar dit wordt tijdens de audit niet expliciet onderzocht en registratie bij de Opta geeft geen zekerheid ten aanzien van *'conformiteit met de wet'*. Daarnaast is het niet duidelijk wie er in de praktijk verantwoordelijkheid neemt om de normenstelsels in lijn te brengen met de wettelijke bepalingen.

De rol van de Opta als toezichthouder is bedoeld om vast te stellen welke certificatiedienst-verleners gekwalificeerde certificaten mogen uitgeven. Voor het uitgeven van certificaten onder PKIoverheid is ook een registratie bij de Opta vereist. Bovendien is de Opta gemandateerd om de dienstverlening te beëindigen indien er niet meer conform de wettelijke eisen gewerkt wordt. Door deze centrale rol van de Opta ontstaat het vertrouwen dat de overheid kritisch meekijkt met de commerciële dienstverleners. De wijze van het houden van wettelijk toezicht is in Nederland doelbewust licht ingevuld. Er bestond al een zelfreguleringssysteem met audits. Daarnaast speelde het argument van de veronderstelde extra kostendruk van het toezichts-arrangement bij de certificatiedienstverleners, die ontstaat bij een zwaardere rol voor de Opta. Hierdoor is er in de praktijk sprake van een *passieve werking van het toezicht*. De Opta onderneemt in de praktijk pas actie na signalen dat er mogelijk iets mis is. Onafhankelijke en adequate signalering op basis van continue monitoring is niet geregeld.

De rol van de auditors in de stelsels is bedoeld om te borgen dat een certificatiedienstverlener blijft voldoen aan het normenstelsels. Indien de auditor geaccrediteerd is, vertrouwen beide toezichthouders in de praktijk op de conformiteitverklaring van deze auditor. De onderliggende auditrapportage is niet voor iedereen in te zien. Auditors doen hun werk in opdracht van de certificatiedienstverleners. Hierbij wordt contractueel vastgelegd dat de betreffende informatie vertrouwelijk wordt behandeld. Of de auditors de verlangde zekerheid bieden is op grond van de conformiteitsverklaring niet vast te stellen. Slechts in hun verwijzing naar de Europese norm zijn de verklaringen onderling vergelijkbaar en eenduidig. Verwijzing naar conformiteit met de

wet- en regelgeving ontbreekt in alle verklaringen. Een expliciete verwijzing naar het TTP.NL schema, dat de feitelijke basis voor een audit door geaccrediteerde auditors zou moeten zijn, ontbreekt soms. Alle verklaringen vermelden dat 'het management systeem' object van toetsing was, maar voor de afnemers van de diensten blijft onduidelijk welke zekerheid daar feitelijk mee geboden wordt.

De complexiteit van de onderlinge verwijzingen, de *ondoorzichtigheid* als het op concrete punten aankomt en de onnodige interpretatieverschillen maken de stelsels voor belang-hebbenden niet helder. Betrouwbaarheid is echter gebaat bij heldere procedures en afspraken.

De Europese Richtlijn Elektronische Handtekeningen is eind jaren 1990 ontstaan vanuit de doelstelling om elektronische handel in Europa te stimuleren. De omvang van de markt voor gekwalificeerde certificaten is achtergebleven bij de toenmalige verwachtingen. De Richtlijn is door lidstaten op verschillende manieren geïmplementeerd waardoor er in de praktijk *drempels* bestaan voor certificatiedienstverleners om diensten in het buitenland te leveren. Wanneer een gerationaliseerd overkoepelend normenstelsel gerelateerd aan certificatiedienstverlening in Europees verband tot stand komt, en dit voor alle lidstaten normatief wordt, zal de eenduidigheid toenemen. Wanneer de rol van commerciële partijen binnen de stelsels ongewijzigd blijft, kan verbreding van de Richtlijn naar certificaten voor andere doeleinden, in het bijzonder voor authenticatie, dienstverleners nieuwe prikkels geven. Op dit moment zorgt het *verbod op toetsing* van certificatiedienstverleners voorafgaand aan registratie voor complicaties en voor onbedoelde risico's in de stelsels. Naburige landen (België en Duitsland) hebben om dezelfde reden als Nederland ook een tweede registratieroute zonder voorafgaande toetsing geïntroduceerd. Uiteindelijk zou het agenderen van geharmoniseerd toezicht en geharmoniseerde schema's waaraan certificatiedienstverleners moeten voldoen, kunnen leiden tot een hogere betrouwbaarheid van PKI-stelsels in Europees verband.

Alternatieven die momenteel worden uitgewerkt voor PKI, zoals DANE en Convergence, verkeren nog in een experimentele fase. Deze alternatieven zijn bedoeld om verbeteringen aan te brengen in aspecten van het vertrouwensmodel van PKI en niet om PKI als zodanig door een nieuw paradigma te vervangen. Voor zover deze verbeteringsmogelijkheden breed zullen worden geadopteerd valt te verwachten dat eerder sprake zal zijn van een geleidelijke selectieve adoptie, dan van een revolutie. Op dit moment zijn ook al enkele verbeteringen door te voeren in de wijze waarop PKI in de praktijk functioneert en waarvoor fundamentele veranderingen in het vertrouwensmodel niet nodig zijn.

De *menselijke factor* bij beveiliging is vaak de zwakste schakel. Dit aspect is in het onderzoek slechts beperkt naar structurele risico's onderzocht. Toch is de indruk ontstaan dat deze ook in de opzet en de werking van de stelsels een wezenlijke rol vervult. Deels is deze factor geobjectiveerd binnen de stelsels. Aan auditors worden bijvoorbeeld eisen gesteld ten aanzien van kennis, competentie en onafhankelijkheid. Echter, niet alle stakeholders hebben de benodigde kennis, een proactieve houding waarbij over formele grenzen heen wordt gekeken, en alertheid om signalen op basis van informele relaties op te pakken. Wanneer op meerdere

niveaus persoonlijke relaties tussen stakeholders zouden worden onderhouden en er actief op de attitude van mensen zou worden gestuurd, zouden kwetsbaarheden in de stelsels mogelijk eerder aan het licht komen.

Op korte termijn kunnen een aantal verbeteringen worden doorgevoerd. Het ligt verder voor de hand om de geconstateerde weeffouten structureel aan te pakken. Bij het vaststellen welke verbeteringen in de stelsels daadwerkelijk worden doorgevoerd dienen een aantal samen-hangende beleidsmatige keuzes te worden gemaakt. Bij deze keuzes kunnen fundamentele discussies een rol spelen waaronder die van de rol van de overheid versus de rol van de markt, de gewenste vorm van handhaving, de rol van Europa en de verantwoordelijkheid van de overheid voor beveiliging binnen vitale sectoren. Een *scenarioanalyse* op basis van de in dit rapport getrokken conclusies zou kunnen helpen bij verdere besluitvorming.

2 INLEIDING

2.1 Achtergrond

Elektronische communicatie is tegenwoordig essentieel voor het functioneren van de Nederlandse samenleving. Dit geldt zowel voor het economisch verkeer als voor het functioneren van de overheid. Om te komen tot betrouwbare elektronische communicatie wordt veelvuldig gebruik gemaakt van digitale certificaten. Misbruik van digitale certificaten kan ernstige maatschappelijke gevolgen hebben waaronder (identiteits)fraude, privacyschendingen, diefstal van goederen en vertrouwelijke gegevens, en het verstoren van de continuïteit van vitale infrastructuren.

Digitale certificaten zijn verbonden aan personen, systemen of aan elektronische diensten. Persoonsgebonden certificaten worden bijvoorbeeld gebruikt om in te kunnen loggen of om een elektronische handtekening te kunnen zetten. Systeemcertificaten maken het voor internet-gebruikers bijvoorbeeld mogelijk om zekerheid te krijgen over de identiteit van een website (zoals die van een overheidsinstelling of van een webwinkel). Organisaties die geautomatiseerd informatie met elkaar uitwisselen maken ook veel gebruik van (zogenaamde dienstgebonden) certificaten. Deze certificaten worden dan ingezet voor het beveiligen van elektronische diensten.

Digitale certificaten kunnen op verschillende wijzen worden ingezet:

1. In een commerciële situatie waarbij private partijen de betrouwbaarheid van hun digitale communicatie willen zekerstellen kunnen ‘eigen merk’ certificaten worden gebruikt. Dit kunnen consumenten zijn die communiceren met bedrijven, maar ook bedrijven onderling. Dit betreft zowel certificaten voor personen, systemen als diensten. De overheid heeft geen zeggenschap over dit marktstelsel, maar kan wel gebruik maken van dergelijke certificaten. Diverse overheidsinstanties gebruiken deze ‘eigen merk’ certificaten van commerciële partijen.

2. Voor het elektronisch ondertekenen van documenten of berichten met een rechtsgeldige digitale handtekening kunnen zogenaamde ‘gekwalificeerde certificaten’ worden gebruikt. Deze persoonsgebonden certificaten hebben een sterkere juridische bewijskracht dan andere certificaten. Voor deze certificaten bestaat een wettelijk kader en de leveranciers ervan vallen onder wettelijk geregeld overheidstoezicht. Certificatiedienstverleners moeten zich laten registreren door de Opta om deze certificaten in Nederland te mogen uitgeven. Voorwaarde voor registratie is dat ze kunnen aantonen dat ze voldoen aan de minimale wettelijke eisen en aan de bijbehorende normen.

3. Voor communicatie met de overheid en tussen overheden heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) het zogenaamde stelsel PKIoverheid in het leven geroepen waaronder ook certificaten worden uitgegeven. Deze PKIoverheids-

certificaten worden uitgegeven voor verschillende toepassingen, en kunnen zowel persoonsgebonden als systeem- of dienstgebonden zijn. Het verschil met de bovengenoemde certificaten is dat de overheid zelf eisen stelt aan deze certificaten om aanvullende betrouwbaarheid te waarborgen. Certificatiedienstverleners die deze certificaten willen uitgeven, dienen te voldoen aan het Programma van Eisen van PKIoverheid, zoals dat wordt beheerd door Logius.

Een certificatiedienstverlener, die voor deze drie verschillende doelen certificaten uitgeeft, zal rekening moeten houden met deze drie verschillende werelden, de bijbehorende eisen en de verschillende wijzen van toezicht. De laatste twee werelden, die van gekwalificeerde certificaten en van PKIoverheid, zijn de stelsels die onderwerp zijn van dit onderzoek.

2.2 Aanleiding: De DigiNotar affaire

In de eerste week van september 2011 werd Nederland opgeschrikt door een digitale inbraak in de beveiligde omgeving van DigiNotar. Dit commerciële bedrijf leverde certificaten binnen elk van de drie stelsels zoals beschreven in paragraaf 2.1. Omdat na de ontdekking van de inbraak niet kon worden uitgesloten dat, behalve de productie van 'eigen merk' certificaten, ook de certificaten van PKIoverheid gecompromitteerd waren, heeft de Minister van BZK in een nachtelijke persconferentie het vertrouwen in DigiNotar opgezegd. Ook de door DigiNotar uitgegeven certificaten konden toen niet meer worden vertrouwd. De gevolgen hiervan werden groot: alle elektronische communicatie die gebruik maakte van deze certificaten zou stil komen te liggen. In de crisissituatie die toen is uitgeroepen is een snelle en beheerste afbouw van het gebruik van DigiNotar certificaten gerealiseerd.

De vraag die velen heeft beziggehouden is: hoe kan een bedrijf dat niet alleen commerciële certificaten uitgeeft, maar ook opereert in twee stelsels met overheidstoezicht toch zoiets overkomen? Is het toezicht wel goed geregeld? Worden de audits wel grondig genoeg aangepakt? Zijn de regels wel duidelijk?

De achterliggende vraag die aanleiding is voor dit onderzoek luidt: was de DigiNotar affaire een incident of bestaan er zwaktes in de benoemde twee certificatenstelsels waardoor een dergelijke situatie zich opnieuw kan voordoen?

2.3 Onderzoeksopdracht

Het doel van dit onderzoek is het verschaffen van inzicht in de risico's van de stelsels waar de overheid een verantwoordelijkheid in heeft: het stelsel van de gekwalificeerde certificaten en het stelsel PKIoverheid. Het gaat niet over een analyse van het DigiNotar incident als zodanig, maar om de analyse van de zwakheden in de stelsels die naar aanleiding van de inbraak bij DigiNotar naar boven zijn gekomen.

De inbraak bij DigiNotar vond plaats binnen het stelsel van de commerciële certificaten die onder eigen merknaam werden uitgegeven. Deze certificaten vallen onder de eerste toepassing,

zoals beschreven in paragraaf 2.1. Als zodanig valt dat, strikt genomen, buiten de reikwijdte van dit onderzoek, aangezien het noch het stelsel van gekwalificeerde certificaten noch het stelsel PKIoverheid betrof. Fox-IT heeft echter aangetoond dat de inbraak niet beperkt is gebleven tot deze omgeving, maar dat ook activiteiten van de inbreker gevonden zijn in de omgevingen die onder een vorm van overheidstoezicht staan. Daarom zal de analyse van de toereikendheid van de stelsels starten met de DigiNotar casus en gericht zijn op de stelselmatige zwakheden en risico's.

De onderzoeksopdracht zoals deze door de ministeries van BZK en EL&I aan Logica is verstrekt omvat het opleveren van een evaluatie en een advies teneinde inzicht te verkrijgen in

- opzet, aard en werking van het PKIoverheidstelsel, met inbegrip van het TTP-certificatieschema, en de overige gekwalificeerde certificaten, naar aanleiding van de inbreuk bij DigiNotar, de gevolgen ervan ook in bredere zin;
- richtinggevende conclusies ten aanzien van de stelsels om risico's te beperken, en
- richtinggevende conclusies ten aanzien van de herziening van de EU Richtlijn voor zover de analyse van betrouwbaarheid van de stelsels daar aanleiding toe geeft.

Concreet zijn de volgende onderzoeksvragen gedefinieerd:

1. Welke risico's bevat het PKIoverheidstelsel (met inbegrip van het TTP.NL-certificatieschema) en het stelsel van de overige gekwalificeerde certificaten, zowel in opzet, inrichting en werking?
2. Is het huidige normenkader nog toereikend voor het doel waarvoor het ontworpen is?
3. Biedt het toezichtarrangement (inclusief audits) een adequaat inzicht in de feitelijke situatie, ingerichte procedures en genomen maatregelen door de aangesloten certificatiedienstverleners? In hoeverre worden de risico's hiermee afgedekt?
4. Welke sterktes en zwaktes bestaan er in het Nederlandse PKIoverheidstelsel en in het toezicht op de gekwalificeerde certificaten ten opzichte van twee op dit punt met Nederland vergelijkbare landen?
5. Welke alternatieven voor het PKIoverheidstelsel worden in de serieuze media aangedragen, in welke mate zijn deze vergelijkbaar met PKIoverheid en welke lessen kunnen hier voor PKIoverheid uit worden getrokken?
6. Welke richtinggevende conclusies kunnen hieruit worden getrokken?
7. Wat betekent dit voor de eisen aan nieuwe EU e-signature regelgeving?

2.4 Onderzoeksaanpak

2.4.1 Object van onderzoek

Gezien de onderzoeksvraag wordt als objecten van onderzoek gedefinieerd het PKIoverheidstelsel en het stelsel van gekwalificeerde certificaten. De stelsels bestaan voor dit onderzoek vervolgens uit de volgende deelgebieden:

- De bij het stelsel betrokken partijen met hun taken, bevoegdheden en verantwoordelijkheden;
- De eisen waaraan betrokken partijen binnen het stelsel dienen te voldoen;
- De verschillende soorten certificaten die door het stelsel worden ondersteund.

Een meer gedetailleerde beschrijving van deze deelgebieden, is opgenomen in hoofdstuk 3.

Het onderzoek richt zich hiermee dus primair op de stelsels en bijvoorbeeld niet specifiek op één certificatiedienstverlener, één certificerende instelling of één incident (de DigiNotar affaire).

2.4.2 Aspecten van Onderzoek

De analyse is uitgevoerd vanuit het perspectief van betrouwbaarheid van elektronische communicatie. Hierbij stonden twee vragen centraal:

- Is het stelsel ‘volledig’?
- Is het stelsel ‘juist’?

Deze bepalen als het ware de bril die tijdens het onderzoek is opgezet. Hiermee worden twee begrippen vanuit de accountancy gebruikt die onderdeel zijn van het begrip ‘betrouwbaarheid’. Het derde aspect van betrouwbaarheid, tijdigheid, valt buiten dit onderzoek.

2.4.3 Meetlat

Om de geformuleerde onderzoeksvragen te kunnen beantwoorden, is een ‘meetlat’ nodig. Wanneer is iets ‘volledig’ en ‘juist’? Wanneer is het normenkader toereikend voor het doel waarvoor het is ontworpen?

Voor het onderzoek naar het stelsel van gekwalificeerde certificaten hanteren we Europese en Nederlandse wet- en regelgeving als uitgangspunt. Een overzicht van deze wet- en regelgeving is opgenomen in [1-5, 10-14]. Dit uitgangspunt is echter niet absoluut aangezien de wet- en regelgeving ook zal worden getoetst aan de oorspronkelijk bedoelingen zoals die zijn verwoord in de toelichtingen op de wet. Hierbij wordt alleen gekeken of aanpassingen van wet- en regelgeving de betrouwbaarheid van de stelsels zou kunnen versterken.

Voor het onderzoek naar het stelsel PKIoverheid hanteren we de doelstellingen van PKIoverheid als meetlat. Deze zijn onder andere verwoord in het Programma van Eisen PKIoverheid [17]. Deze doelstellingen worden in dit rapport niet geëvalueerd maar als een gegeven beschouwd.

2.4.4 Diepgang en tijdvenster

Het onderzoek beschouwt zowel de opzet, als het bestaan en de werking van de stelsels. Onderzoek naar de opzet van de stelsels beschouwt de volledigheid en juistheid van gedocumenteerde vastlegging van stelsels. Dit gaat dus over het ontwerp van de stelsels, over hoe ze zijn bedacht.

Onderzoek naar het bestaan van de stelsels gaat over de vraag of vastgesteld kan worden dat daadwerkelijk gebeurt, wat volgens de opzet zou moeten gebeuren. Onderzoek naar de werking kijkt naar de vraag of dit ook gebeurt. Het bestaan wordt beschouwd als het begin van de werking. Het onderzoek heeft plaatsgevonden in de maanden oktober, november en december 2011, maar omvat geen in de tijd herhaalde observaties. De periode is te kort om de werking volledig te kunnen evalueren. In de rest van dit rapport wordt onderzoek naar bestaan en werking samengenomen. In het vervolg zullen slechts de termen ‘opzet’ en ‘werking’ worden gehanteerd.

Het onderzoek betreft het structureel analyseren van de stelsels en een evaluatie in termen van richtinggevende conclusies. Aanbevelingen met betrekking tot beleid vallen niet binnen de reikwijdte van dit onderzoek.

2.4.5 Aanpak van het onderzoek

Er zijn drie onderzoeksinstrumenten gehanteerd: desk research, interviews en waarneming.

Op basis van desk research is een analyse gemaakt van de te hanteren ‘toetssteen’ en van documentatie over de opzet van de stelsels (zie hoofdstuk 8). De volledigheid van bestudeerde documentatie is geverifieerd tijdens de interviews en op basis van de onderliggende referenties van de documentatie zelf.

Recente vertrouwelijke rapporten van certificerings- en inspectie-audits zijn ingezien voor drie certificatiedienstverleners inclusief DigiNotar.

Er zijn 20 interviews gehouden met in totaal 28 personen vanuit verschillende organisaties en met een verschillende achtergrond (rol of positie). Tijdens de interviews is inzicht verkregen in zowel de opzet als het functioneren van de bij de stelsels betrokken partijen – en daarmee dus ook van de stelsels. Voor een representatief inzicht in opzet en werking, is er voor gezorgd dat alle betrokken partijen (beleidsverantwoordelijken, toezichthouders, tactisch beheerder, certificerende instellingen, certificatiedienstverleners) zijn geraadpleegd voor dit onderzoek. De lijst met te interviewen entiteiten/personen is in onderlinge afstemming tussen opdrachtgever en opdrachtnemer vastgesteld. Vervolgens is tijdens de interviews met de respondenten

geverifieerd of de onderzoeksgroep diende te worden uitgebreid. Een overzicht van geïnterviewde personen is opgenomen in Bijlage A.

Drie representatieve certificatiedienstverleners zijn in het onderzoek betrokken. Eén hiervan is DigiNotar omdat zij de aanleiding vormde voor het onderzoek. Bij DigiNotar zijn geen waarnemingen gedaan maar hiervoor wordt gesteund op onderzoek van Fox-IT. Met de verantwoordelijken van DigiNotar heeft geen interview plaats kunnen vinden. Wel zijn twee andere representatieve certificatiedienstverleners geïnterviewd. Dit met het oogmerk om vast te stellen of de problemen zoals deze zijn opgetreden bij DigiNotar een stelselmatige oorzaak hebben.

Bovendien zijn er in het kader van dit onderzoek waarnemingen bij deze certificatie-dienstverleners gedaan. Hiermee is niet beoogd een 'certificerende audit' uit te voeren. De doelstelling hiervan was het verkrijgen van een indruk ten aanzien de mate waarin geformuleerde eisen aan certificatiedienstverleners in de praktijk toetsbaar zijn gerealiseerd (bestaan), om zodoende een meer onderbouwd beeld te verkrijgen over de werking van de stelsels. De waarnemingen hebben zich dan ook slechts op drie gebieden geconcentreerd (logging, logische toegangsbeveiliging en scheiding van systemen). Deze gebieden zijn gekozen omdat Fox-IT op deze zaken kwetsbaarheden bij DigiNotar heeft geconstateerd.

2.5 Leeswijzer

Hoofdstuk 1 bevat de management samenvatting. Deze geeft een samenvatting van het gehele rapport met een bijzondere nadruk op de hoofdconclusies. Dit hoofdstuk is van belang voor lezers die in korte tijd kennis willen nemen van de essentie van dit rapport.

Hoofdstuk 2 Beschrijft de achtergrond van het onderzoek, de onderzoeksvragen en onderzoeksaanpak. Lezers die geïnteresseerd zijn in de grondslag voor dit onderzoek kunnen die in dit hoofdstuk vinden.

In hoofdstuk 3 wordt een overzicht gegeven van de PKI-stelsels die het primaire onderwerp van onderzoek vormen. Dit hoofdstuk is primair van belang voor lezers die het domein van onderzoek willen leren kennen.

Hoofdstuk 4 geeft de analyse van de opzet van de PKI-stelsels. Het bevat detailbevindingen en –analyses, ook als ze niet het gewicht hebben van een hoofdconclusie. Met 'opzet' wordt hier de manier bedoeld waarop de stelsels zijn ontworpen. Bij de analyse wordt primair naar risico's voor de betrouwbaarheid van de stelsels gekeken. Dit hoofdstuk gaat over onderzoeksvraag 1 ('risico's van de stelsels') voor zover het de 'opzet en inrichting' betreft. Bovendien wordt onderzoeksvraag 2 ('toereikendheid van het normenkader') hier behandeld.

In hoofdstuk 5 wordt gekeken naar de werking van de PKI-stelsels in de praktijk. Dit gaat dus niet om hoe het is bedacht, maar hoe het in de praktijk functioneert en welke risico's voor de betrouwbaarheid daarmee gepaard gaan. Het hoofdstuk gaat in op het tweede deel van onderzoeksvraag 1 ('de werking') en behandelt onderzoeksvraag 3 ('adequaatheid van het

toezichtsarrangement') . Net als het vorige hoofdstuk is dit hoofdstuk bedoeld voor lezers die geïnteresseerd is in details van de werking van de stelsels.

Hoofdstuk 6 beschrijft observaties vanuit een vergelijking van de beide-PKI stelsels met die in België en Duitsland. Bovendien is een beknopte beschouwing opgenomen van eventuele alternatieven voor de huidige PKI-stelsels. Onderzoeksvraag 4 ('vergelijking met het buitenland') en 5 ('alternatieven voor PKI') komen in dit hoofdstuk aan de orde.

In hoofdstuk 7 volgen de belangrijkste conclusies die kunnen worden getrokken uit de hoofdstukken 4, 5 en 6. Dit hoofdstuk is zelfstandig leesbaar voor een lezer die enigszins bekend is met de problematiek en bedoeld voor lezers die slechts geïnteresseerd zijn in de eindresultaten van het onderzoek. Onderzoeksvraag 6 ('mogelijkheden voor verbetering') en 7 ('lessen t.a.v. herziening EU Richtlijn') worden hierin behandeld.

Hoofdstuk 8, tenslotte, geeft de lijst met geraadpleegde documenten.

3 OVERZICHT VAN DE STELSELS

3.1 Invalshoeken

Een digitaal certificaat kan worden gezien als het digitale equivalent van een paspoort. Wanneer ze worden getoond, kan daarmee de identiteit van de eigenaar worden vastgesteld en kan op basis hiervan worden bepaald wat deze mag. Er moet dan wel zijn geverifieerd dat het een echt paspoort is. Paspoorten worden door een vertrouwde partij uitgeven. Certificaten worden ook door vertrouwde partijen uitgegeven: certificatiedienstverleners. Waar bij overheden vertrouwen in het algemeen besloten ligt in de aard van hun rol, geldt dit niet voor commerciële certificatiedienstverleners. Zijn moeten aan een stelsel van normen voldoen zodanig dat hen vertrouwen kan worden geschonken.

DigiNotar was zo'n certificatiedienstverlener. Het vertrouwen in DigiNotar viel weg omdat er digitaal was ingebroken, er valse certificaten waren aangemaakt en DigiNotar dit niet tijdig in de openbaarheid had gebracht. Ook andere door dit bedrijf uitgegeven certificaten werden toen niet meer vertrouwd. Daarmee ontstond het probleem dat alle elektronische communicatie die beveiligd was met certificaten van DigiNotar niet meer kon worden vertrouwd.

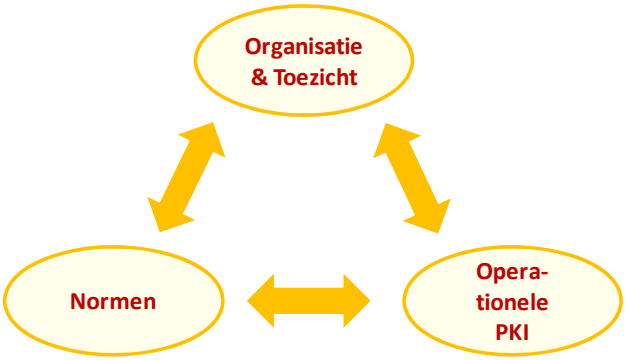
De afspraken, diensten en technologieën die het beveiligen van elektronische communicatie met geheime en publieke sleutels mogelijk maken worden samen ook wel 'Public Key Infrastructure' (PKI) genoemd. Vandaar de titel van dit rapport. Certificaten staan niet op zichzelf, maar hebben een plaats in een PKI. Vanwege de verschillende dimensies van PKI, spreken we van een 'PKI-stelsel'. We beschouwen PKI in dit rapport vanuit drie complementaire invalshoeken.

1. Organisatie en toezicht:
   De organisatie omvat de verschillende partijen die een rol spelen in het stelsel met hun verantwoordelijkheden, taken, bevoegdheden en onderlinge relaties. Het aspect toezicht omvat de wijze waarmee binnen het stelsel wordt geborgd dat iedereen zich aan de afspraken houdt.

2. Normen:
   Het geheel van wetgeving, regelgeving, standaarden en richtlijnen waaraan partijen zich committeren.

3. Operationele PKI:
   De PKI zoals deze vorm krijgt in de systeemtechnische werkelijkheid (operators, fysieke locaties, hardware, software, protocollen en formaten).

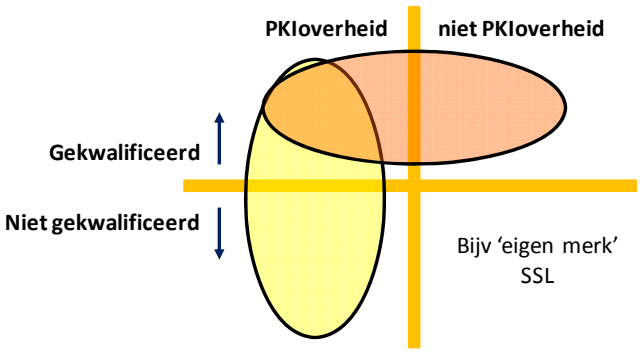
Deze drie invalshoeken zijn gekozen omdat ze elke een fundamenteel aspect van PKI afdekken en gezamenlijk de essentie van PKI weergeven. Ze vormen bovendien een bruikbaar vertrekpunt voor de analyse van de stelsels. Dit is samengevat in Figuur 1.



Figuur 1: Drie complementaire gezichtspunten op de stelsels

In dit rapport richten we ons op de evaluatie van twee PKI-stelsels. Het eerste stelsel is het 'PKIoverheidstelsel' en het tweede stelsel is dat van de 'gekwalificeerde certificaten'. Het stelsel PKIoverheid is eigendom van het ministerie van BZK en heeft tot doel om veilige elektronische communicatie van en met de overheid te ondersteunen. Het tactisch beheer van PKIoverheid is belegd bij Logius, een agentschap van het ministerie van BZK. Het tactisch en operationeel beheer van het decentrale deel van PKIoverheid ligt bij meerdere commerciële- en overheidspartijen: de certificatiedienstverleners. Logius stelt in overleg met het ministerie van BZK de eisen op waaraan de certificatiedienstverleners moeten voldoen.

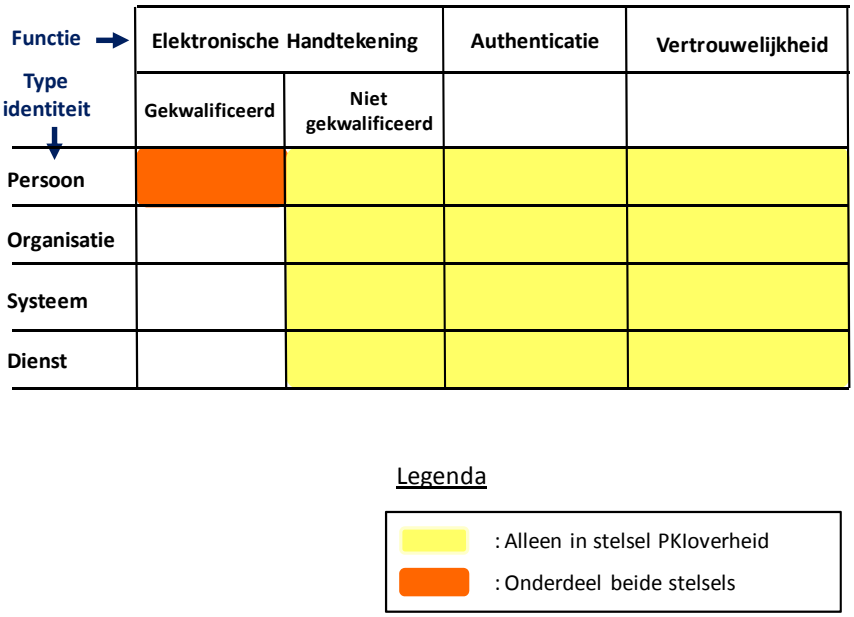
Het andere stelsel dat we in dit rapport beschouwen, het stelsel 'gekwalificeerde certificaten' heeft een ander karakter. Het omvat uitsluitend een specifiek soort certificaten. Bovendien verschilt het achterliggende doel van dan dat van PKIoverheid. Het stelsel gekwalificeerde certificaten is ontstaan vanuit de intentie om elektronische handel te bevorderen en een digitale of elektronische handtekening te creëren waaraan dezelfde juridische waarde kan worden toegekend als aan de 'klassieke' handgeschreven handtekening. Hiervoor werden betrouwbare elektronische handtekeningen van een wettelijke grondslag voorzien. In 1999 werd de Europese Richtlijn op de elektronische handtekeningen van kracht. In 2003 is deze Richtlijn in Nederland geïmplementeerd via de Wet op de Elektronische Handtekeningen (WEH). De WEH valt voor zover het betrekking heeft op certificatiedienstverleners onder verantwoordelijkheid van het ministerie van EL&I. De Opta is aangewezen om het wettelijk toezicht op certificatie-dienstverleners die gekwalificeerde certificaten uitgeven uit oefenen.



Figuur 2: Overlap stelsels

Er bestaat een overlap tussen beide onderzochte stelsels zoals te zien is in Figuur 2. Certificaten die buiten beide stelsels vallen zijn geen onderwerp van dit onderzoek. Aangezien certificatiedienstverleners in de praktijk in meerdere van de kwadranten in Figuur 2 certificaten leveren, zijn er afhankelijkheden die wel zullen worden beschouwd.

Het stelsel PKIoverheid omvat vier typen certificaten waarvan de gekwalificeerde certificaten er één zijn (zie Figuur 3). Elektronische handtekeningen kunnen worden gezet op basis van gekwalificeerde certificaten, maar ook met niet gekwalificeerde certificaten. Deze handtekeningen hebben dan een verschillende juridische status. Naast elektronische handtekeningen worden certificaten ook gebruikt voor authenticatie (vaststelling van identiteit) en vertrouwelijkheid (versleuteling van gegevens). Binnen het stelsel PKIoverheid bestaat voor elk van deze drie functies een apart certificaat. Gekwalificeerde certificaten zijn per definitie persoonsgebonden zoals te zien is in Figuur 3. Certificaten die worden uitgegeven voor organisaties, voor



Figuur 3: Typen Certificaten

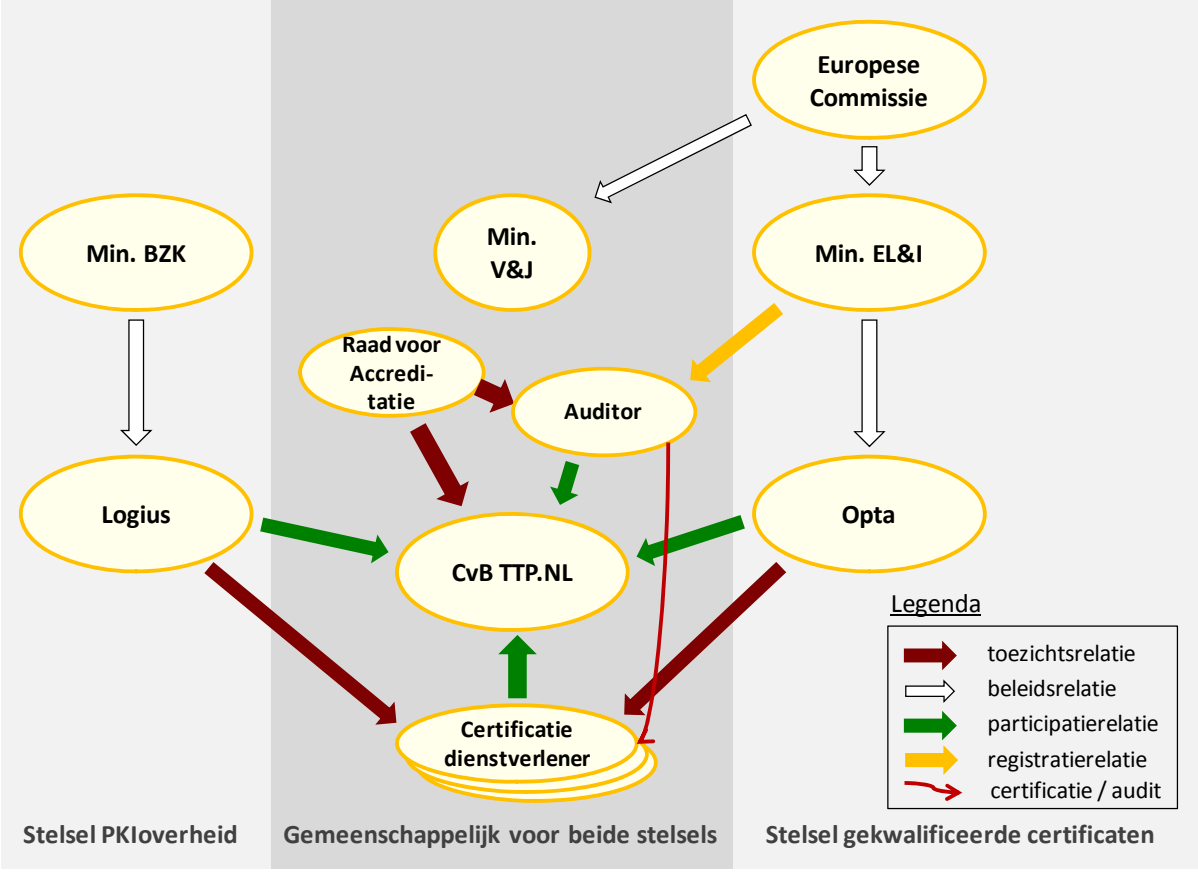
systemen of voor diensten vallen niet onder het stelsel gekwalificeerde certificaten, maar kunnen wel onder PKIoverheid vallen. Niet gekwalificeerde certificaten kunnen ook buiten beide onderzochte stelsels vallen en als 'eigen merk' door certificatiedienstverleners op de markt worden gebracht. Het meest bekende type 'eigen merk' certificaten zijn systeemgebonden SSL-certificaten voor de authenticatie van websites.

3.2 Organisatie & Toezicht

De organisatie van de stelsels omvat de participerende partijen en hun onderlinge relaties. Er zijn partijen met een uitvoerende verantwoordelijkheid, met een beleidsverantwoordelijkheid, en partijen met een toezichthoudende verantwoordelijkheid. De relevante partijen zijn schematisch weergegeven in Figuur 4. In het vervolg van dit rapport zal de term toezichthouder

worden gehanteerd voor zowel de wettelijk toezichthouder voor het stelsel van gekwalificeerde certificaten als voor de niet wettelijk toezichthouder voor het stelsel PKIoverheid, tenzij expliciet anders aangegeven.

De verantwoordelijkheid voor het beleid en de strategie voor PKIoverheid ligt bij het *ministerie van BZK*. De tactische uitvoering is belegd bij Logius. Een certificatiedienstverlener die onder PKIoverheid certificaten wil uitgeven moet voldoen aan het Programma van Eisen (PvE) van PKIoverheid [17]. Het ministerie van BZK is hiervan de eigenaar en accordeert wijzigingen erop. Conformiteit van certificatiedienstverleners met het PvE wordt vastgesteld door auditors en de door hen opgestelde conformiteitsverklaringen worden door *Logius* gebruikt als basis voor toelating tot het stelsel. Naast haar rol als tactisch beheerder van het afsprakenstelsel PKIoverheid (deze rol wordt aangeduid als 'Policy Authoriteit') is Logius verantwoordelijk voor de inrichting van de operationele PKI onder PKIoverheid voor zover het niet de dienstverlening aan afnemers en 'vertrouwende partijen' betreft. Het beheer van deze operationele PKI is grotendeels uitbesteed aan een commerciële partij.



Figuur 4: Organisatie en toezicht

Toezicht binnen het stelsel PKIoverheid is nodig om te waarborgen dat een geregistreerde certificatiedienstverlener blijft voldoen aan de eisen. Ten behoeve van het toezicht worden de

auditrapporten aangeleverd aan Logius zodra deze gereed gekomen zijn. Certificatie-dienstverleners hebben ook de plicht om beveiligingsincidenten bij Logius te melden. Handhaving door Logius kan plaatsvinden op basis van door een overeenkomst die wordt afgesloten tussen de certificatiedienstverlener en het ministerie van BZK.

De verantwoordelijkheid voor het beleid ten aanzien van het stelsel van de gekwalificeerde certificaten ligt primair bij het *ministerie van EL&I*. Op basis van de Europese Richtlijn Elektronische Handtekeningen [1] heeft Nederland de Wet op de Elektronische Handtekening ingevoerd [10, WEH]. Hierin wordt onder andere bepaald wat de verantwoordelijkheden van certificatiedienstverleners zijn wanneer ze gekwalificeerde certificaten uitgeven. Dit deel van de WEH is vastgelegd in de Telecommunicatie Wet.

De WEH betreft ook aanpassingen in het Burgerlijk Wetboek. Deze hebben vooral betrekking op de juridische grondslag voor het gebruik van gekwalificeerde certificaten en bevat bijvoorbeeld voorschriften over de betrouwbaarheid van verschillende niveaus van handtekeningen. Dit deel van de WEH valt onder de verantwoordelijkheid van het *ministerie van VenJ*. Het ministerie van VenJ heeft bovendien een coördinerende verantwoordelijkheid voor de veiligheid in Nederland. Dit omvat ook de digitale veiligheid. Begin 2011 is onder verantwoordelijkheid van de minister van VenJ de Nationale Cyber Security Strategie gelanceerd. Dit heeft onder andere geleid tot de installatie van de Cyber Security Raad op 30 juni 2011 en de oprichting van het Nationaal Cyber Security Centre (NCSC) op 1 januari 2012. Het ministerie van VenJ is niet eindverantwoordelijk voor alle digitale veiligheid in Nederland maar coördineert nationale beleidsaspecten, nationale crisissituaties en monitort risico's en incidenten op nationale schaal.

In een publiek – private samenwerking is het zogenaamde TTP.NL schema tot stand gekomen. Het TTP.NL schema [20] legt normen vast waar certificatiedienstverleners die zich aan het schema willen conformeren aan moeten voldoen. Het legt ook vast op welke wijze conformiteit dient te worden getoetst. Het schema is eigendom van ECP-EPN en wordt beheerd door een college van participerende instanties: het *College van Belanghebbenden (CvB) TTP.NL*. In dit College zijn onder andere de auditors, de certificatiedienstverleners, de Opta en Logius vertegenwoordigt.

De *Raad voor Accreditatie* (RvA) is in Nederland de enige instelling die accreditaties mag uitvoeren. In het kader van TTP.NL heeft deze Raad goedkeuring verleend aan het TTP.NL schema, aan de beheerder (ECP-EPN) en aan de instellingen die certificeringen tegen het schema uitvoeren (de auditors). Accreditatie heeft een aparte wettelijke grondslag.

De *auditors* die conformiteitsverklaringen tegen het TTP.NL schema mogen verstrekken zijn door de RvA geaccrediteerd. Daarnaast specificeert de Wet op Elektronische Handtekeningen dat ze door de Minister van EL&I worden aangewezen. Auditors worden ook wel aangeduid met de term 'certificerende instellingen' (in dit rapport zullen we de term 'auditors' hiervoor gebruiken; wanneer het om individuele personen gaat geven we dit expliciet aan). De eisen waaraan auditors moeten voldoen zijn nader gespecificeerd in een beleidsregel [14]. De

conformiteitsverklaringen van deze auditors worden door de Opta gebruikt als basis voor registratie van de certificatiedienstverleners.

Het toezicht op certificatiedienstverleners die gekwalificeerde certificaten uitgeven is in Nederland belegd bij de *Opta*. Het ministerie van EL&I is beleidsverantwoordelijk en vult de randvoorwaarden in die het de Opta mogelijk maken om haar toezichthoudende taak uit te oefenen. Het ministerie van EL&I is ook betrokken bij aanpassingen in de Europese Richtlijn en de Beschikkingen op dit terrein. Toezicht ten aanzien van andere aspecten van de WEH (zoals op leveranciers van 'veilige middelen') is in Nederland niet expliciet geregeld.

3.3 Normen

We maken onderscheid tussen drie typen normen. Ten eerste is er de Europese en Nederlandse wet- en regelgeving. Ten tweede zijn er meer specifieke normen die toezichthouders opleggen aan partijen wanneer ze willen toetreden tot een stelsel. Tenslotte zijn er de normen die partijen aan zichzelf opleggen. We zullen elk van deze typen normen in de volgende paragrafen behandelen. Een detailschema van de onderlinge samenhang tussen de eerste twee vormen van normen is opgenomen in Bijlage D.

3.3.1 Wet en regelgeving

Ondanks het feit dat PKI al langer bestaat, heeft de Europese richtlijn Elektronische Handtekeningen uit 1999 [1] ervoor gezorgd dat normenstelsels in Europees verband verder zijn uitgewerkt. De Richtlijn is nader geconcretiseerd in een aantal besluiten van de Europese Commissie [2, 3, 4, 5]. De Richtlijn, en de op basis daarvan uitgewerkte nationale wetten, kennen een bijzondere status toe aan de gekwalificeerde elektronische handtekening. De Nederlandse Wet Elektronische Handtekeningen [10, WEH] omvat aanpassingen van de Telecomwet en het Burgerlijk Wetboek. De WEH is nader geconcretiseerd in een Besluit [12], een Regeling [13] en een Beleidsregel [14]. Elke lidstaat is verplicht een passend systeem toezicht in te stellen op certificatiedienstverleners die gekwalificeerde certificaten uitgeven. In Nederland is deze toezichthoudende taak aan de Opta toegewezen. De taken en bevoegdheden van de Opta zijn vastgelegd in de Telecomwet.

Om gekwalificeerde certificaten te mogen verstrekken dient een certificatiedienstverlener geregistreerd te zijn bij de Opta. Voor deze registratie zijn twee mogelijke routes: 'directe registratie' en registratie via 'vrijwillige accreditatie'. De eerste route houdt een volledig zelfstandige beoordeling door de Opta in. Dit heeft echter tot op heden nooit plaatsgevonden. De 'vrijwillige accreditatie' route houdt in de praktijk in dat een externe door de Raad van Accreditatie geaccrediteerde auditor (de 'certificerende instelling') op basis van een onderzoek bepaalt of een certificatiedienstverlener voldoet aan het TTP.NL schema. De Opta voert dan geen aanvullend onderzoek uit, maar registreert de partij op basis van de door de auditor afgegeven conformiteitsverklaring (welke ook wel een 'certificaat' wordt genoemd).

De term ‘vrijwillige accreditatie’ behoeft enige toelichting. Het duidt een kader aan waarbinnen certificatiedienstverleners vrijwillig kunnen opereren. De term komt voort uit de Europese Richtlijn en wordt ook door de Opta gehanteerd in lijn met de Richtlijn. De RvA gebruikt de term accreditatie echter alleen voor de formele acceptatie van auditors. Het gebruik van de term ‘accreditatie’ in de Richtlijn is anders. In dit rapport hanteren we de definitie van de RvA aangezien zij autoriteit op het gebied van accreditatie in Nederland. Wanneer in het rapport wordt verwezen naar de ‘vrijwillige accreditatie route’ van de Opta, gebruiken we deze term tussen apostrofs en zonder de formele accreditatie van de RVA te bedoelen. De term ‘certificeren’ is verwarrend, omdat certificatiedienstverleners zelf ook gecertificeerd worden. Om verwarring met digitale certificaten te voorkomen, hanteren we de term conformiteits-beoordeling voor het certificeren van de certificatiedienstverleners door auditors (zie verder de verklarende woordenlijst in Bijlage B).

3.3.2 Internationale standaarden

Gezaghebbende technische normen voor PKI zijn in de jaren 1990 ontwikkeld door de Internet Engineering Task Force (IETF) [53-55]. Deze hebben onder andere betrekking op de structuur van verklaringen van certificatiedienstverleners omtrent hun dienstverlening, formaten voor certificaten en protocollen. Met de implementatie van de Europese Richtlijn elektronische handtekeningen zijn door de Europese standaardiserende organisaties CEN en ETSI normen opgesteld die specifieker toe zijn gesneden op het gebruik van PKI in het kader van elektronische handtekeningen. De veelheid aan normen en de complexiteit van de stelsels is onderzocht in opdracht van de Europese Commissie [70, 73-77]. Als gevolg hiervan heeft de Europese Commissie in 2009 de Europese standaardisatie organisaties de opdracht gegeven om het raamwerk van normen op het gebied van elektronische handtekeningen te rationaliseren [72]. Hier wordt momenteel aan gewerkt [46].

We onderscheiden vijf domeinen waarop internationale standaarden in het kader van de PKI-stelsels zijn gedefinieerd:

1. Eisen aan certificatiedienstverleners;
2. Eisen aan ‘betrouwbare systemen’ die door certificatiedienstverleners worden gebruikt voor de productie van certificaten;
3. Eisen aan ‘veilige middelen’ waarmee gekwalificeerde handtekeningen dienen te worden gezet;
4. Eisen aan protocollen en formaten voor certificaten;
5. Eisen aan auditors.

Elk van deze domeinen heeft een relatie met wettelijke eisen. Voor een gedetailleerd overzicht van relevante normen verwijzen we naar Bijlage D.

Centraal in beide stelsels die in dit rapport worden geëvalueerd staat de ETSI 101 456 norm [42] die eisen formuleert aan certificatiedienstverleners die gekwalificeerde certificaten uitgeven. Deze standaard heeft een equivalent voor niet-gekwalificeerde certificaten die voor PKIoverheid en voor TTP.NL ook van toepassing is [44]. De Europese Richtlijn schrijft gebruik van de ETSI 101 456 norm niet voor. In Nederland is hij echter wel opgenomen in de Regeling [13]. Wanneer een certificatiedienstverlener er aan voldoet wordt deze vermoed te voldoen aan een deel van de Wet.

3.3.3 PKIoverheid

Het stelsel PKIoverheid heeft, in tegenstelling tot het stelsel gekwalificeerde certificaten, geen wettelijke grondslag. Het dient om betrouwbare elektronische communicatie binnen de overheid en tussen overheid en burgers/organisaties mogelijk te maken. Het stelsel van gekwalificeerde certificaten was toen men met PKIoverheid startte (1999) nog niet ingericht. PKIoverheid is ook ontstaan vanuit de behoefte aan PKI ten behoeve van een Nationale Elektronische Identiteitskaart (eNIK). De invoering van eNIK in Nederland is destijds uitgesteld, maar is momenteel weer in onderzoek bij het ministerie van BZK. Later zijn daar andere doeleinden aan toegevoegd zoals het beveiligen van communicatie via overheidswebsites (SSL) en veilige communicatie met tachograaf systemen (Autonome Apparaten). De normen van PKIoverheid zijn vastgelegd in een Programma van Eisen [17, PvE]. Het PvE PKIoverheid vereist van een certificatiedienstverlener dat deze geregistreerd is bij de Opta. Ook vereist PKIoverheid certificering van certificatiedienstverleners volgens het TTP.NL schema. Er zijn in het PvE PKIoverheid bovendien expliciete eisen gesteld aan het voldoen aan standaarden en aan het toezichtsarrangement.

Een aantal eisen aan certificatiedienstverleners zijn tussen het ministerie van BZK en de certificatiedienstverlener contractueel vastgelegd. Er is een standaard contract wat alle certificatiedienstverleners onder PKIoverheid dienen te ondertekenen.

3.3.4 Het TTP.NL Schema

Het TTP.NL schema beschrijft de vereisten voor de certificatie van het management systeem van certificatiedienstverleners. Het TTP.NL schema heeft niet alleen betrekking op gekwalificeerde certificaten, maar ook op niet-gekwalificeerde certificaten en op diensten voor het betrouwbaar dateren van elektronische informatie (‘time stamping’). Het bevat afspraken over welke normen van toepassing zijn en over het toezichtsarrangement. ECP-EPN beheert een register van organisaties die zijn gecertificeerd volgens het schema [20].

Het schema is onder andere bedoeld om invulling te geven aan wettelijke eisen ten aanzien van de gekwalificeerde elektronische handtekening.

Conformiteit aan het schema vereist conformiteit aan een aantal normen. Daarnaast zijn er ook normen die expliciet worden genoemd, maar waarvan het schema aangeeft dat conformiteit met 'vergelijkbare normen' ook tot conformiteit aan TTP.NL kan leiden.

Eens per drie jaar dient een certificeringsaudit plaats te vinden door een geaccrediteerde auditor. Tussentijds vindt jaarlijks een inspectie-audit plaats. Het schema specificeert hoe er door auditor en certificatiedienstverlener dient te worden gehandeld in het geval van grote of klein afwijkingen van de normen. De wijze van auditen is op hoofdlijnen aangeven. Er zijn richtlijnen ten aanzien van het tijdsbeslag van de audit gespecificeerd.

3.3.5 Operationele normen van certificatiedienstverleners

De productvoorwaarden van een certificatiedienstverlener worden vastgelegd in een certificatiebeleidsdocument (de 'Certificate Policy'). Onder het stelsel gekwalificeerde certificaten stellen certificatiedienstverleners dit document zelf op om afnemers duidelijk te maken welke techniekonafhankelijke voorwaarden verbonden zijn die aan de afname van hun certificatie-diensten. Onder PKIoverheid is dit certificatiebeleidsdocument onderdeel van het Programma van Eisen en daarmee gelijk voor alle certificatiedienstverleners: iedereen houdt zich daarmee aan dezelfde voorwaarden.

Elke certificatiedienstverlener stelt daarnaast een certificatiepraktijkdocument op (de 'Certificate Practice Statement'), waarin vastgelegd wordt op welke manier de certificatiediensten precies worden geleverd. Ook staat hierin de meest concrete uitwerking van beheersmaatregelen. Dit geldt voor beide stelsels. Afhankelijk van het type certificaten kunnen beide documenten verschillen.

Zowel het certificatiebeleidsdocument als het certificatiepraktijkdocument is onderdeel van het normenstelsel al zijn het de certificatiedienstverleners zelf die ze definiëren. Beide documenten zijn publiek zodat afnemers van certificaten en vertrouwende partijen kunnen beoordelen welke diensten worden geleverd, welke aansprakelijkheden gelden en welk vertrouwen kan worden gegeven.

3.4 Operationele PKI

3.4.1 Processen

In deze paragraaf gaan we beknopt in op de processen voor het leveren van certificatiediensten om in de volgende hoofdstukken de operationele PKI nader te kunnen analyseren.

Certificatiedienstverlening omvat meer dan het uitgeven van certificaten alleen. Meer specifiek vallen de volgende processen onder certificatiedienstverlening:

- Registratie / aanvraag
- Certificaatgeneratie

- Certificaatuitgifte
- Uitgifte van ‘veilige middelen’
- Herroepen van certificaten
- Statusmelding van certificaten

Deze processen zijn onder andere benoemd in ETSI-norm 101 456 [42]. Verder bestaan er verschillende vormen van uitbesteding door certificatiedienstverleners. Het kan daarbij een deel, maar ook alle processen betreffen. Een typisch voorbeeld hiervan is een certificatie-dienstverlener die certificatenaanvraag en -uitgifte uitbesteedt aan een partij die daar vanwege haar fysieke locaties beter toe in staat is.

Het is ook mogelijk dat een partij die formeel de rol van certificatiedienstverlener bekleedt, het grootste deel van de processen uitbesteedt aan een partij die de operationele processen uitvoert.

Tenslotte maken certificatiedienstverleners ook gebruik van leveranciers van gespecialiseerde IT-infrastructuurdiensten waardoor (een deel van) de certificatenproductiestraat niet direct onder hun controle staat.

3.4.2 Systemen

In deze paragraaf geven we een aantal kenmerken weer van de systemen die een certificatie-dienstverlener gebruikt om de processen uit de volgende paragraaf te kunnen uitvoeren. Het gaat hierbij om een beschrijving van de relevante systemen en hun samenhang bij certificatiedienstverlening.

De gehele levenscyclus van een certificaat wordt beheerst door één vertrouwensknooppunt (een zogenaamde ‘Certificate Authority’) in een PKI. Een certificatiedienstverlener kan meerdere vertrouwensknooppunten beheren ten behoeve van haar dienstverlening. Het is daarbij voor certificatiedienstverleners mogelijk om voor de implementatie van meerdere vertrouwens-knooppunten dezelfde systemen te gebruiken.

De systemen die de processen van certificatiedienstverleners ondersteunen, bestaan onder andere uit specifieke hard- en software. Afhankelijk van het type certificaten en de certificatiepraktijk van een certificatiedienstverlener, worden certificaten al dan niet via een online webapplicatie aangevraagd. Wanneer voor de uitgifte van een certificaat een specifiek register moet worden geraadpleegd (zoals de GBA of een professioneel register voor personen), kan hiermee tijdens registratie een verbinding worden gemaakt.

Voor de productie van een certificaat is een verbinding met een derde partij onwenselijk omdat dit proces op geen enkele manier extern mag worden beïnvloed. Dit geldt ook voor het plaatsen van het certificaat op een ‘veilig middel’ zoals een USB-token of een chipkaart.

Voor het proces van uitgifte van certificaten, al dan niet in combinatie van veilige middelen, is afhankelijk van de certificatiepraktijk van de certificatiedienstverlener, direct fysiek contact tussen uitgever en afnemer nodig.

Wanneer certificaten niet meer betrouwbaar zijn of anderszins uit het systeem dienen te worden verwijderd, worden ze herroepen. Daarmee worden ze door het vertrouwensknooppunt op een ‘zwarte lijst’ geplaatst. Deze ‘zwarte lijst’ met statusinformatie over certificaten dient te allen tijde online te kunnen worden geraadpleegd door partijen die van een certificaat gebruik willen maken (‘vertrouwende partijen’).

De Europese Richtlijn stelt eisen aan ‘betrouwbare systemen’ van certificatiedienstverleners.

4 ANALYSE VAN DE OPZET VAN DE STELSELS

In dit hoofdstuk worden risico's in de stelsels van de gekwalificeerde certificaten en van PKIoverheid, geanalyseerd voor zover ze gerelateerd zijn aan de opzet van de stelsels. We behandelen achtereenvolgens risico's gerelateerd aan de organisatie van de stelsels, aan het toezicht en aan het normenkader.

4.1 Organisatie

4.1.1 Stelsel gekwalificeerde certificaten

Het primaire doel van de Wet op de Elektronische Handtekening (WEH) is het borgen van vertrouwen in elektronische communicatie. Door dit vertrouwen wordt de elektronische handel tussen de Europese lidstaten ondersteund. Handtekeningen zijn van belang voor de betrouwbaarheid van de handel, en elektronische handtekeningen zijn hiervan het logische equivalent in de digitale wereld. Ze vereisen gemeenschappelijke randvoorwaarden die zorgen voor betrouwbaarheid. Vertrouwen als primair doel wordt genoemd in de toelichting op de WEH [11], maar is verder niet expliciet in het stelsel vormgegeven. In bijvoorbeeld de Verkeerswet zijn gedragsbepalingen opgenomen waarin het verboden is zich op de weg zodanig te gedragen dat een ander gehinderd wordt of er gevaar voor een ander kan ontstaan. In de wet- en regelgeving over de elektronische handtekening staat niet dat men vertrouwen moet borgen, maar vooral hoe dat dient te gebeuren: bijvoorbeeld door professioneel en zorgvuldig om te gaan met geheime sleutels en certificaten. Het risico van een doel uitwerken in middelen zonder het doel daarin steeds mee te nemen, is dat het oorspronkelijke doel ('vertrouwen borgen') dat leidend was voor de opzet van het stelsel, in de werking van de stelsels verloren gaat of tegengewerkt wordt door regels op de concretere abstractieniveaus. De zogenaamde 'checks and balances' waarmee voorkomen kan worden dat dit effect optreedt, zijn niet in de opzet van het stelsel aanwezig. Het stelsel van de gekwalificeerde certificaten is gebaseerd op impliciet vertrouwen. De afwezigheid van expliciet vertrouwen en van gezond wantrouwen richting partijen die de regels mogelijk niet zo nauw nemen, is een omissie in de opzet.

Certificaten worden niet alleen gebruikt voor elektronische handtekeningen, maar ook voor het borgen van de vertrouwelijkheid van informatie tijdens uitwisseling. In toenemende mate is er vanuit de markt behoefte aan grensoverschrijdende normen voor authenticatie. De verwachting is nu dat het sociaaleconomische verkeer gestimuleerd zal worden indien binnen Europa op eenzelfde wijze vastgesteld kan worden of personen, systemen of diensten daadwerkelijk zijn wie ze zeggen te zijn [69, 77]. Deze 'authenticatie'-functie van certificaten is nu geen onderdeel van het stelsel.

4.1.2 Stelsel PKIoverheid

In 1999 is er een besluit genomen door de ministerraad om met PKIoverheid te starten met als doel om overheidscommunicatie veilig te maken. Onder overheidscommunicatie werd verstaan communicatie tussen overheden, tussen overheid en burger en tussen overheid en bedrijven. Hieronder viel dus niet specifiek communicatie tussen burgers of tussen bedrijven. Er waren toen ook ideeën voor het introduceren van een kaart voor alle burgers waarmee ook een elektronische handtekening kan worden gezet (de eNIK). Daartoe is een persoonlijk certificaat nodig voor de elektronische handtekening.

Omdat men voor de beveiliging van elektronische communicatie niet afhankelijk wilde zijn van één commerciële partij, is besloten PKIoverheid in te richten volgens een markmodel. Door het opstellen van normen en het organiseren van een vorm van toezicht werd de benodigde betrouwbaarheid gerealiseerd. Het ministerie van BZK en Logius zijn gezamenlijk verantwoordelijk voor PKIoverheid. De toepassingen van PKIoverheid zijn breder dan een persoonlijke chipkaart. Ook certificaten voor het beveiligen van websites en voor machine-naar-machine communicatie zijn bijvoorbeeld onderdeel van het PKIoverheidstelsel geworden. Het oorspronkelijke doel om communicatie met de overheid te faciliteren is nog steeds van toepassing. PKIoverheid beperkt zich niet tot communicatie met de overheid. Bedrijven kunnen ook onderling met certificaten van PKIoverheid werken. Dit wordt door Logius gedoogd. De aansturing en het beheer van PKIoverheid is publiek gebleven om betrouwbare communicatie met en tussen overheden te kunnen blijven faciliteren. Het risico van een politiek gestuurde governance is dat de private partijen die de certificaten uitgeven geconfronteerd kunnen worden met maatregelen die gebaseerd zijn op politieke dreigingen zonder dat de wenselijkheid en haalbaarheid getoetst is in de praktijk. Dit risico wordt beperkt doordat maatregelen altijd vooraf met certificatiedienstverleners worden besproken.

Er is geen wettelijke basis voor de opzet van het stelsel PKIoverheid en er is geen wettelijke verplichting om PKIoverheid te gebruiken. De Rijksoverheid sluit steeds meer aan bij een architectuur waar de diensten van Logius gebruikt moeten worden. Logius stelt voor aansluiting op haar diensten het gebruik van PKIoverheid verplicht. Vanuit het Rijk is er geen verplichting richting bijvoorbeeld de lagere overheden. Met respect voor het huis van Thorbecke zijn bijvoorbeeld de gemeentes vrij om al dan niet te kiezen voor PKIoverheid certificaten. Het gebruik van commerciële certificaten die niet onder PKIoverheid vallen, bijvoorbeeld voor gemeentelijke websites, brengt het risico met zich mee dat de kans op incidenten groter is dan noodzakelijk en dat deze niet via het PKIoverheidstelsel maar pas in een crisissituatie beheersbaar kunnen worden gemaakt. Het feit dat PKIoverheid certificaten voor bijvoorbeeld vitale sectoren niet verplicht zijn, brengt het risico met zich mee dat elektronische communicatie binnen deze sectoren niet de beveiliging krijgt die vanuit het maatschappelijk belang wenselijk is. De overheid kan bovendien niet gemakkelijk ingrijpen om de maatschappelijke impact te beperken.

De sturing op stelsels zoals PKIoverheid wordt door het mondiale karakter van internet beperkt. Of de Nederlandse certificaten in het PKIoverheidstelsel worden geaccepteerd door de webbrowsers van de Nederlandse burger, wordt in de praktijk bepaald door de internationale browserleveranciers. In het nationale stelsel hebben zij geen formele rol, maar hun besluiten kunnen wel vergaande implicaties hebben. De afhankelijkheid van wereldwijd opererende browserleveranciers brengt het risico met zich mee dat zij PKIoverheidscertificaten als onbetrouwbaar aanmerken terwijl Logius ze nog betrouwbaar acht. Afstemming op bovennationaal niveau kan dit risico beperken.

4.1.3 Beide stelsels

4.1.3.1 Registratie bij de Opta

Certificatiedienstverleners mogen uitsluitend gekwalificeerde certificaten uitgeven, indien ze geregistreerd zijn bij de Opta. In de toelichting bij de wet [11] is aangegeven dat er geen drempel mag zijn om geregistreerd te worden. Het aanleveren van een informatiepakket of een verklaring van een geaccrediteerde auditor volstaat. De Europese Richtlijn bepaalt dat certificatiedienstverleners hun diensten vrij zonder voorafgaande machtiging moeten kunnen aanbieden. Onder een voorafgaande machtiging wordt niet alleen elke vergunning verstaan waarvoor de certificatiedienstverlener een besluit van de nationale autoriteiten moet verkrijgen voordat hij zijn certificatiediensten mag verlenen, maar ook alle andere maatregelen met hetzelfde effect. In Nederland wordt dit ruim geïnterpreteerd. Registratie bij de Opta mag niet beschouwd worden als een vergunning. De Opta wilde ten tijde van de invoering van de WEH de situatie voorkomen dat een certificatiedienstverlener die zich niet aan de normen hield en wiens registratie door de Opta beëindigd was zich (zonder drempel) toch weer zou kunnen laten registreren terwijl men nog steeds niet aan de normen voldeed. Daarom is er een wettelijk verbod gekomen om gekwalificeerde certificaten uit te geven zonder registratie bij de Opta.

De wet legt eisen op aan certificatiedienstverleners die gekwalificeerde certificaten uitgeven en de Opta houdt hierop wettelijk toezicht. De Opta houdt geen toezicht op de auditors die in opdracht van de certificatiedienstverleners worden ingezet. De Opta houdt wel toezicht op de naleving van de wettelijke eisen voor certificatiedienstverleners, maar deze naleving kan niet uit de registratie bij de Opta worden afgeleid. De Opta geeft op haar website aan dat de registratie bij de Opta niet mag worden beschouwd als een bewijs dat de betreffende certificatiedienst-verlener voldoet aan de wettelijke eisen. Registratie bij de Opta geeft de Opta de bevoegdheid om nader onderzoek te doen en de registratie te schrappen.

Toetreding tot het stelsel PKIoverheid vereist een registratie bij de toezichthouder van het stelsel voor de gekwalificeerde certificaten (de Opta). Wanneer een certificatiedienstverlener alleen SSL-certificaten onder PKIoverheid wil uitgeven, dient ze ook aan de eisen voor gekwalificeerde certificaten te voldoen: zo dient ze o.a. tegen het TTP.NL schema te worden gecertificeerd en door de Opta geregistreerd te worden. De Opta zou zo'n registratieverzoek naast zich neer kunnen leggen, aangezien ze alleen gekwalificeerde certificatiedienstverleners

registreert. Wanneer ze een dergelijke certificatiedienstverlener wel registreert, zou haar toezichthoudende taak in dit geval zonder betekenis zijn. De wettelijke rol van de Opta om toezicht te houden op de certificaten betreft namelijk alleen de gekwalificeerde certificaten. Hier vallen de SSL-certificaten van PKIoverheid niet onder.

4.1.3.2 Afhankelijkheden en verschillen tussen de stelsels

In het stelsel van de gekwalificeerde certificaten is de rol van de overheid relatief beperkt gehouden ten gunste van de marktwerking, in het PKIoverheid stelsel bepaalt de overheid het programma van eisen. In het stelsel PKIoverheid kan de overheid rechtstreeks de normen bepalen, in het stelsel van de gekwalificeerde handtekeningen kan de Opta dat niet. Wederzijdse afhankelijkheden en onduidelijke verantwoordelijkheden in stelsels met verschillende doelstellingen brengen risico's met zich mee. Verschillende uitgangspunten, bijvoorbeeld ten aanzien van de rol van de markt, een andere juridische basis (privaatrechtelijk versus publiekrechtelijk) en een andere visie op handhaving kunnen in concrete situaties strijdig blijken te zijn. Dat schept onduidelijkheid en leidt niet tot versterking van het vertrouwen. Wanneer een certificatiedienstverlener er bijvoorbeeld voor zou kiezen om uitsluitend gekwalificeerde certificaten onder PKIoverheid uit te gaan geven wordt zij in het stelsel van PKIoverheid verplicht om zich, conform het TTP.NL schema, vooraf te laten auditen door een geaccrediteerde partij. Deze verplichting staat op gespannen voet met het verbod uit de Europese Richtlijn die verplichte certificering vooraf niet toestaat.

4.1.3.3 Overlap tussen de stelsels

Nederland heeft geen strikte scheiding doorgevoerd in de opzet van de beide stelsels. Gekwalificeerde certificaten voor elektronische handtekeningen kunnen zowel binnen het stelsel van de elektronische handtekeningen worden uitgegeven, als in het stelsel PKIoverheid. Een ogenschijnlijk heldere verdeling van verantwoordelijkheden binnen beide stelsels, kan ondoorzichtig worden als beide stelsels een overlap vertonen. Wanneer bijvoorbeeld een certificatiedienstverlener die gekwalificeerde certificaten onder PKIoverheid uitgeeft, gecompromitteerd raakt, kunnen er verschillen van inzicht bestaan tussen Logius en de Opta over hoe te handelen. Logius zou al dan niet kunnen beslissen om de dienstverlener operationeel uit PKIoverheid te verwijderen. De Opta zou al dan niet kunnen beslissen om de registratie van de dienstverlener te beëindigen. Als deze beslissingen tegenstrijdig zijn is onduidelijk wie het voortouw neemt.

Een ander voorbeeld van complicaties die kunnen optreden als gevolg van de overlap in de stelsels is het feit dat de toezichtsregimes in beide stelsels niet gelijk zijn, terwijl eerstelijns controle (audits) door de auditors wel gelijktijdig wordt uitgevoerd. De auditors hebben te maken met de ETSI-norm waarvoor de Opta een conformiteitsverklaring verlangt, het TTP.NL schema, dat voor PKIoverheid een vereiste is, en met de aanvullende PKIoverheidsnormen. Hierdoor ontstaat onduidelijkheid over welke zekerheid wordt geboden voor welk toezichtsregime en welk deel van de conformiteitsverklaringen en auditrapporten hier betrekking op hebben.

4.1.3.4 Expertise gedreven stelsels versus maatschappelijk belang

De PKI-stelsels, inclusief de wet- en regelgeving en standaarden, zijn in eerste instantie het domein van experts gebleven. De stelsels zijn vooral technisch en procedureel opgezet, terwijl de risico's en de gevolgen als het mis gaat, de maatschappij als geheel betreffen. Dit is ook aangetoond door het DigiNotar incident. De PKI-stelsels zijn niet formeel aangemerkt als 'vitale infrastructuur'. Het is aan de 'vertrouwende partijen' en aan de afnemers van certificaten om passende maatregelen te nemen in hun bedrijfsprocessen die gebruik maken van certificaten. Er worden binnen de stelsels geen risicoanalyses uitgevoerd op het niveau van kritische bedrijfsprocessen (in vitale sectoren) en bedrijfscontinuïteitsmaatregelen zijn in beide stelsels beperkt aanwezig. Het is daardoor niet zeker dat de stelsels optimaal zijn ingericht zodat certificatiedienstverleners leveren wat vertrouwende partijen en afnemers nodig hebben voor het beveiligen van kritische bedrijfsprocessen.

Crisismanagement op nationaal niveau is wel geregeld, maar beide stelsels zijn daar in hun opzet niet mee verbonden. Relatiebeheer tussen stakeholders op operationeel, tactisch en strategische niveau zou er voor zorgen dat signalen dat er iets mis is sneller leiden tot correctie. Bovendien kan er in geval van calamiteiten worden geëscaleerd naar mensen die elkaar al kennen. Het risico van de kloof tussen expertgedreven stelsels en de maatschappelijke diensten die er van afhankelijk zijn, is dat in de praktijk van de stelsels niet geregeld is wat in het maatschappelijk belang is.

4.1.3.5 Stelseloverstijgende risico's

Beide stelsels hebben een eigen afbakening en houden geen rekening met opschaling van een probleem. Het calamiteitenplan van PKIoverheid overstijgt bijvoorbeeld niet de grenzen van Logius en sluit slechts beperkt aan op het calamiteitenplan bij nationale crises, doordat het laatste niet specifiek ingaat op PKI. Binnen beide stelsels wordt wel geregeld wat een certificatiedienstverlener moet doen om continuïteit te garanderen wanneer hijzelf failliet gaat, maar de verantwoordelijkheid voor de continuïteit van de dienstverlening aan de maatschappij is niet ingericht. Interdepartementale coördinatie is nodig waar meer dan één ministerie betrokken is. Deze coördinatie is niet geregeld in de stelsels.

De beide PKI-stelsels zijn niet geclassificeerd als nationale vitale infrastructuur. De DigiNotar affaire heeft echter aangetoond hoe belangrijk PKI tegenwoordig is binnen vitale sectoren. In de opzet van beide stelsels zijn de maatregelen en tijdslijnen die voorgeschreven worden niet in lijn met de snelheid waarmee gehandeld moet worden als een vitale infrastructuur bedreigd wordt. Zo is er in het TTP.NL schema dat in beide stelsels gebruikt wordt, sprake van weken en maanden om bepaalde geconstateerde afwijkingen op te lossen. Het risico van een maatschappelijke ontwrichting, veroorzaakt door het wegvallen van het vertrouwen in een certificatiedienstverlener, ontstaat doordat de rol van de overheid bij het beschermen van vitale infrastructuren niet expliciet geregeld is in de stelsels.

4.2 Toezicht

4.2.1 Stelsel gekwalificeerde certificaten

In het stelsel van gekwalificeerde certificaten zijn de certificatiedienstverleners verantwoordelijk voor het (blijven) voldoen aan de eisen. Conform de wet- en regelgeving moeten zij dit kunnen aantonen. Uitgangspunten in dit stelsel, zoals beschreven in de toelichting op de WEH [11], zijn dat certificatiedienstverleners geen hoge toetredingsdrempel mogen ervaren, dat ze verantwoordelijk zijn voor hun eigen dienstverlening en dat auditors hen desgewenst helpen om de betrouwbaarheid van de dienstverlening te verbeteren. Geaccrediteerde auditors zijn niet te beschouwen als toezichthouder in de zin van de wet, maar kunnen door hun borgende rol wel een belangrijke functie vervullen bij de invulling van het toezicht. De Opta mag steunen op het rapport van een geaccrediteerde auditor, maar is er niet van afhankelijk. De Opta kan zelfstandig besluiten nemen op basis van eigen onderzoek dat men uitvoert of heeft laten uitvoeren.

Verplichte conformiteitsbeoordelingen van certificatiedienstverleners worden door de Europese Richtlijn verboden, omdat dit een te hoge toetredingsdrempel zou kunnen vormen. Europese lidstaten hebben niet de mogelijkheid om een conformiteitsbeoordeling door geaccrediteerde auditors te verplichten. Het risico hiervan is dat een certificatiedienstverlener in het huidige stelsel kan besluiten om zelf een (bevriende) niet geaccrediteerde auditor te selecteren. De Opta moet in dat geval bepalen of deze auditor competent genoeg is en of de dienstverlener in aanmerking komt voor directe registratie. Daartoe is de Opta niet ingericht.

Beide toezichthouders zijn afhankelijk van signalen om adequaat te kunnen ingrijpen. Er bestaat voor certificatiedienstverleners geen verplichting om kwetsbaarheden en incidenten te melden aan de Opta in tegenstelling tot de meldplicht aan de auditor en aan Logius.

4.2.2 Stelsel PKIoverheid

Het toezicht op het stelsel PKIoverheid wordt uitgevoerd door Logius. Dit toezicht is niet wettelijk geregeld. De juridische basis voor het toezicht wordt gevormd door de privaatrechtelijke contracten die het ministerie van BZK sluit met certificatiedienstverleners. Hierin staat onder andere dat de certificatiedienstverlener verplicht is zich te houden aan het Programma van Eisen (PvE) van PKIoverheid, dat zij BZK onverwijld op de hoogte stelt van een eventuele compromittering of risico's die afbreuk doen aan de betrouwbaarheid van de dienstverlening, en dat zij onmiddellijk alle redelijke medewerking verlenen aan een onderzoek dat BZK te allen tijde gerechtigd is uit te laten voeren. In het PvE is onder andere opgenomen dat een certificatiedienstverlener geregistreerd moet zijn bij de Opta. Het is in het stelsel van PKIoverheid niet duidelijk of de Opta hiermee ook toezichthouder wordt van niet gekwalificeerde certificaten onder PKIoverheid. Wettelijk gezien heeft de Opta deze taak niet, maar welke vorm van toezicht hiermee wel of niet geregeld wordt, is niet beschreven. Ook is niet duidelijk of de wijze van auditen die bedoeld is in het stelsel van de gekwalificeerde certificaten, voldoende is

voor de zekerheid die men in het stelsel PKIoverheid beoogt. Het risico van 'meeliften' op wat in het stelsel van de gekwalificeerde certificaten geregeld is aan toezicht, is dat er onbedoeld een andere zekerheid wordt gerealiseerd dan voor het PKIoverheid stelsel nodig is. Zoals uit paragraaf 4.3.3 blijkt, bevat het toezichtsarrangement voor het stelsel gekwalificeerde certificaten kwetsbaarheden.

In het PvE is onder meer opgenomen dat een certificatiedienstverlener moet kunnen aantonen conform te zijn met het TTP.NL schema. Er wordt gesteld dat met een verklaring van TTP.NL conformiteit aangetoond wordt dat de certificatiedienstverlener voldoet aan de betreffende Europese norm [42], de WEH [10], het Besluit Elektronische Handtekeningen [12] en de bijbehorende Regeling [13]. Zo wordt een TTP.NL conformiteitsverklaring gepositioneerd door PKIoverheid. De verplichting tot conformiteit met TTP.NL, hetgeen bij het stelsel van de gekwalificeerde certificaten niet verplicht is, zorgt ervoor dat de conformiteit door een geaccrediteerde auditor moet worden vastgesteld. Voor de eisen van PKIoverheid die een nadere specificatie geven van de TTP.NL eisen en die aanvullend zijn op het TTP.NL schema, kan de conformiteit niet onder accreditatie worden vastgesteld, aangezien hiervoor geen schema is opgesteld. PKIoverheid geeft aan dat auditors die de conformiteit tegen de specifieke PKIoverheid eisen vaststelt dezelfde competenties moet hebben als benodigd voor TTP.NL certificatie [17]. In opzet zou de situatie zich voor kunnen doen dat een niet-geaccrediteerde auditor conformiteit met de PKIoverheid eisen vaststelt. Het beoordelen of een dergelijke auditor de vereiste competenties heeft, dient dan door de beheerder van PKIoverheid zelf te worden uitgevoerd.

In het contract tussen het ministerie van BZK en een certificatiedienstverlener worden een aantal eisen aan certificatiedienstverleners gesteld. Deze contracten geven een juridische basis voor handhaving en in het uiterste geval kan het contract worden ontbonden. De expliciet opgenomen verplichtingen zijn voor een deel een selectie uit het PvE, voor een ander deel zijn het nieuwe eisen. Het risico van twee typen 'afspraken' is dat juridisch gezien alleen handhaving door contractopzegging kan plaatsvinden. Handhaving door het operationeel afkoppelen van certificatiedienstverleners van de PKIoverheid hiërarchie die niet aan de alle eisen van PKIoverheid voldoen, is door Logius mogelijk en sneller uit te voeren dan de ontbinding van een contract.

4.2.3 Beide stelsels

4.2.3.1 Audits

De wijze waarop het toezicht in beide stelsels gebruik kan maken van auditors is gelijk indien certificatiedienstverleners de route van de vrijwillige accreditatie kiezen en de geaccrediteerde auditor een dubbele opdracht geven: conformiteit vaststellen met TTP.NL en met de eisen van PKIoverheid. Zowel de Opta als Logius hanteren de verklaringen van een geaccrediteerde auditor als basis voor toelating tot de respectievelijke stelsels. De Raad voor Accreditatie heeft het schema waarmee auditors een certificatiedienstverlener kunnen auditen (TTP.NL) op

verzoek van het College van Belanghebbenden TTP.NL geaccepteerd. Audits vinden plaats op verzoek van de certificatiedienstverlener zelf. De reikwijdte van een dergelijke audit is afgebakend in het TTP.NL schema: het gaat om een audit van het management systeem. Voor het auditen van de 'betrouwbare systemen' en 'veilige middelen' verwijst het TTP.NL schema naar andere normen en afspraken. Feitelijk wordt bij een management systeem audit geen directe zekerheid gegeven over de betrouwbaarheid van de technische systemen. De RvA maakt een principieel onderscheid tussen een productcertificatie en een management systeem certificatie [16]. Eisen aan auditors die management systemen beoordelen worden gebaseerd op de internationale standaard hiervoor [57]. In deze norm is beschreven welke zekerheid een dergelijke certificering oplevert: 1) de conformiteit van het management systeem met de audit criteria, 2) of het management systeem in staat is om zeker te stellen dat de organisatie aan zijn beleid en doelstellingen kan voldoen, 3) of het management systeem effectief genoeg is om zeker te stellen dat de organisatie blijvend kan voldoen aan haar doelstellingen. Met een certificering tegen het TTP.NL schema wordt dus zekerheid gegeven over het functioneren van het management systeem van de certificatiedienstverlener.

4.2.3.2 Ruimte in normenstelsels

De normenstelsels laten op punten ruimte voor verschillende invullingen. Er is ruimte nodig om certificatiedienstverleners de mogelijkheid te geven om hun eigen keuzes te maken en zich te kunnen onderscheiden in de markt. De verschillende invullingen kunnen echter leiden tot niet bedoelde verschillen in gerealiseerde betrouwbaarheidsniveaus in de praktijk. De ruimte in de normenstelsels wordt onder andere veroorzaakt doordat sommige normen binnen de stelsels zijn gepositioneerd als (prescriptieve) eisen, terwijl andere normen richtinggevend of optioneel zijn. Het TTP.NL schema vereist voor wat betreft gekwalificeerde certificaten bijvoorbeeld conformiteit aan de ETSI-norm [42] maar stelt dat voor conformiteit aan de norm met eisen voor betrouwbare systemen [49] en voor de norm voor veilige middelen [51] alternatieven mogelijk zijn. In Nederland zijn geen instellingen aangewezen die deze veilige middelen kunnen certificeren. De Minister van EL&I heeft deze mogelijkheid om dergelijke instellingen aan te wijzen volgens de wet wel [10, 18.17a]. Bovendien is er geen toezichthouder op de conformiteit van veilige middelen met de wettelijk eisen [11, par. 2.8]. In Duitsland wordt formele certificering van de betrouwbare systemen van certificatiedienstverleners als eis gesteld bij vrijwillige accreditatie. De ETSI-norm [42] kent ook een toelichting [43] die echter geen formele status is toegekend.

Het zou de eenduidigheid van het beoogde betrouwbaarheidsniveau ten goede komen wanneer optionele normen óf een verplicht karakter zouden krijgen óf uit de stelsels zouden worden verwijderd.

4.2.3.3 Richtlijnen voor Register EDP-auditors

De beroepsorganisatie van Register EDP Auditors (NOREA) geeft haar leden een raamwerk en een richtlijn mee voor het uitvoeren van zogenaamde 'assurance opdrachten' [61]. Hierbij wordt onder andere aangegeven welke eisen worden gesteld aan de diepgang van een dergelijke

opdracht. Het feit dat de audit is gebaseerd op een formeel kader en dat er zekerheid wordt geboden aan een derde partij zijn wel noodzakelijke maar geen voldoende voorwaarden om een opdracht te classificeren als een 'assurance opdracht'. Assurance opdrachten zijn namelijk altijd opdrachten die zekerheid geven over het verleden (retrospectief), terwijl certificeringsaudits betrekking hebben op de toekomst (zie geldigheidsduur van de conformiteitsverklaring). Over de toekomst kan minder zekerheid worden afgegeven dan over het verleden. Daarom geldt hiervoor een ander regime voor geregistreerde auditors. Assurance opdrachten dienen door Register EDP-auditors of Register Accountants te worden uitgevoerd. Certificeringsaudits hoeven niet door bij NOREA geregistreerde auditors plaats te vinden. In het geval van certificerings-audits, welke dus niet onder de NOREA-richtlijn vallen, is in het algemeen niet iets te zeggen over de geleverde mate van zekerheid.

Wanneer een door NOREA geregistreerde auditor betrokken is bij een certificeringsopdracht dienen het Reglement Gedragscode en het Reglement Kwaliteitsbeheersing van NOREA te worden gevolgd, maar niet het NOREA-raamwerk en de -richtlijn voor assurance opdrachten. NOREA heeft geen specifieke richtlijnen opgesteld voor het uitvoeren van (in de tijd vooruitkijkende) certificeringsaudits. Geregistreerde IT-auditors kunnen volgens hun professionele normen en opleiding geen audits uitvoeren op een management systeem zonder de IT-implementatie, die de processen die binnen de opdracht vallen ondersteunt, expliciet te beoordelen. Bij een deugdelijk uitgevoerde management systeem audit hoort bijvoorbeeld ook het beoordelen van firewall-instellingen. Een geregistreerde auditor kan zich niet beperken tot de vaststelling of de verantwoordelijkheden en processen hiervoor adequaat zijn ingericht.

Certificering van certificatiedienstverleners tegen de ETSI normen / het TTP.NL schema valt volgens NOREA in de categorie 'overeengekomen specifieke werkzaamheden'. Een ISO 27001 certificering is een ander voorbeeld van zulke certificeringen. Voorbeelden van (retrospectieve) assurance opdrachten zijn Third Party Mededelingen en ISAE 3402 verklaringen.

4.2.3.4 Zekerheid van 'management systeem' audits

De management systeem audit benadering die de auditors hanteren en die door de Raad voor Accreditatie wordt aangereikt, biedt niet de zekerheid die toezichthouders en andere 'vertrouwende partijen' mogen verwachten. Richtlijnen van de Raad waarborgen niet dat geaccrediteerde auditors de implementatie van de onderliggende IT moeten beoordelen en laten dus een enge interpretatie van het begrip 'management systeem audit' toe. Het is opmerkelijk dat de ontoereikendheid van de 'management systeem audit' benadering binnen het College van Deskundigen TTP.NL niet is besproken, dat het niet aan de orde is geweest bij accreditaties door de RvA en dat de auditors er tijdens audits in de praktijk wel mee worstelen, maar dat het geen reden is om een opdracht niet te aanvaarden.

Kijkend naar de assurance die feitelijk beoogd wordt – zekerheid over de betrouwbaarheid van certificaten en van een certificaatdienstverlener – kan een onderzoek van enkel het management systeem als te beperkt worden aangemerkt. Het risico van een certificering die zich alleen richt op het management systeem, is dat de verwachting van eindgebruikers niet

overeen komt met de feitelijke betekenis van de afgegeven conformiteitsverklaring. Gebruikers van certificaten verwachten dat een certificatiedienstverlener die geaudit is, een keurmerk heeft ontvangen dat zijn systemen en processen betrouwbaar zijn.

In het TTP.NL schema wordt van auditors conformiteit met de ISO 17021 norm vereist. In de eisen waartegen zij certificatiedienstverleners die gekwalificeerde certificaten uitgeven dienen te toetsen staat de Europese ETSI 101 456 norm centraal. Deze eisen betreffen de systemen en diensten van de certificatiedienstverlener. Het is niet duidelijk hoe door de auditor omgegaan moet worden met de normen in het TTP.NL schema met betrekking tot technische systemen en bijvoorbeeld het goed beveiligd zijn van deze systemen. De verwijzing naar het certificeren van de 'betrouwbare systemen' die de processen van de certificatiedienstverlener ondersteunen, dient een auditor volgens de handleiding van het schema wel te controleren. De betekenis van deze handreiking in het kader van een management systeem certificering is niet helder. In de richtlijn van de RvA voor de beoordeling van schema's [16] wordt wel aangegeven dat bij productcertificering de normen die betrekking hebben op een kwaliteitssysteem getoetst moeten worden, maar dat leidt niet tot een management systeem certificering. Een vergelijkbare bepaling bij de management systeem certificering, namelijk dat normen die betrekking hebben op een product of dienst wel getoetst moeten worden zonder dat er dan sprake is van productcertificering, is niet opgenomen. Het is niet duidelijk hoe een aantal specifieke eisen uit de ETSI 101 456 norm getoetst zouden moeten worden. Enerzijds staat er bijvoorbeeld in eis 7.4.10 van deze norm dat een certificatiedienstverlener zich er van zal verzekeren dat aan alle wettelijke verplichtingen wordt voldaan. Anderzijds stelt de ISO 17021 standaard dat een management systeem certificering niet leidt tot de vaststelling dat aan alle wettelijke verplichtingen is voldaan. Er zit een spanning tussen de eisen van het TTP.NL schema (in het bijzonder de ETSI-normen) en de wijze waarop conformiteit met deze eisen vastgesteld moet worden (de management systeem certificering van de RvA). Het wordt aan de auditors overgelaten hoe met deze spanning om te gaan. Het risico hiervan is dat er in de praktijk verschillende benaderingen worden gehanteerd die verschillende niveaus van zekerheid bieden. Auditors kunnen zich formeel beperken tot een vaststelling dat het management systeem voldoet aan de eisen, terwijl bij afnemers van certificaten en certificatiediensten de indruk gewekt kan worden dat conformiteit op de producten en diensten wordt gerealiseerd.

Het aangeven van het aantal dagen dat een audit mag duren in het TTP.NL schema heeft (in de opzet) als risico dat het onbedoeld een beperking van de diepgang van de audit aangeeft. Er is ook een spanning met de eis uit de standaard voor auditors [57, artikel 9.1.4.1], dat zij bij het vaststellen van het aantal dagen onder meer rekening moeten houden met de risico's die horen bij de specifieke producten, processen en activiteiten van de certificatiedienstverlener. Na een vastgestelde dreiging of geconstateerde inbraak zal het aantal dagen van de audits die vervolgens plaatsvinden significant verhoogd moeten zijn.

4.2.3.5 Verslaglegging van audits en conformiteitsverklaringen

De normen waar de RvA naar verwijst, schrijven ook de wijze van verslaglegging voor. Naast een samenvatting van de conformiteit, dienen de afwijkingen in detail te worden vastgelegd [57, artikel 9.1.9.6.1]. Het auditrapport bevat in opzet geen gedetailleerde beschrijving van de zaken waarvan de auditor heeft vastgesteld dat ze voldoen, noch hoe het normenstelsel is geoperationaliseerd of hoe er getest is, maar alleen de zaken die niet voldoen. Het risico van een dergelijke verslaglegging is dat de diepgang van de audit en de daarmee gepaard gaande zekerheid voor de lezer niet duidelijk zijn. Ook kan na een incident niet vastgesteld worden of de auditor de oorzaak van het incident expliciet beoordeeld heeft.

Afwijkingen die in een auditrapport staan hoeven niet te leiden tot het intrekken van een TTP.NL conformiteitsverklaring. Het uitgangspunt van het TTP.NL schema is dat conformiteitsverklaring niet hoeven te worden ingetrokken zolang het management van de certificatiedienstverlener tijdig een plan opstelt om de afwijkingen te verhelpen. Het uitgangspunt is dat een conformiteitsverklaring niet ingetrokken hoeft te worden wanneer de auditor eist dat de afwijkingen binnen een bepaalde termijn worden opgelost en wanneer door het management van de certificatiedienstverlener een plan van aanpak hiervoor wordt opgeleverd. Het onderscheid tussen grote afwijkingen en kleine afwijkingen wordt wel gemaakt, maar er is in het TTP.NL schema ook een bepaling opgenomen dat grote afwijkingen worden behandeld als kleine afwijkingen zodra er een door de auditor goedgekeurd plan van aanpak ligt om de grote afwijkingen op te lossen. In het licht van de rol van een auditor die helpt om de dienstverlening te verbeteren, is dat te billijken. In het licht van de rol van de auditor die beoordeelt of het management de aanpak onder controle heeft, is dit wellicht ook consistent. In het licht van de rol van een auditor die een conformiteitsverklaring afgeeft op basis waarvan de toezichthouder bepaalt of een certificatiedienstverlener gekwalificeerde certificaten mag verstrekken, is dit opmerkelijk. Het risico dat grote afwijkingen van de norm geen impact hoeven te hebben op de conformiteitsverklaring en daarmee op de registratie, is dat er (tijdelijk) diensten die niet voldoen aan de norm worden verleend aan mogelijk maatschappelijk belangrijke sectoren. Indien geconstateerde afwijkingen geen repercussies hoeven te hebben voor de registratie, ontstaat ook het risico dat de minder strenge handhaving leidt tot minder strenge naleving.

4.2.3.6 Transparantie accreditatieproces

Een schema dat de RvA accepteert, dient de competenties te beschrijven die nodig zijn voor de auditors die andere partijen tegen dat schema certificeren. De Raad toetst auditors tegen deze eisen via documentatie en via observaties tijdens audits. De Raad heeft de bevoegdheid om bij twijfel onderzoek te doen of een auditor zich houdt aan de afspraken en normen waartegen ze geaccrediteerd zijn. Er is een contractuele relatie tussen de Raad en de auditors en op basis van die privaatrechtelijke overeenkomst zijn de observaties en bevindingen van de Raad ten aanzien van de auditor vertrouwelijk. Het risico van deze opzet is dat er onvoldoende balans van belangen is aangebracht, als het gaat om een inhoudelijke beoordeling van een specifieke accreditatie. Het stelsel laat toe dat een certificatiedienstverlener zelf een auditor kiest, maar er

zijn geen prikkels om iedereen scherp te houden, zoals in de situatie waarin de registrerende partij of een onafhankelijke toezichthouder (of een concurrent) de auditor uit mag kiezen. In paragraaf 5.5.4 wordt nader ingegaan op de marktwerking tussen auditors.

4.3 Normen

Een normenstelsel biedt een samenhangend geheel van normen waaraan partijen moeten voldoen. Eerst zullen de normen van het stelsel voor de gekwalificeerde certificaten worden geanalyseerd, daarna dat voor het stelsel van PKIoverheid. Vervolgens zal het normenstelsel dat voor beide geldt worden beschouwd. Afgesloten wordt met een analyse van de normen die betrekking hebben op enkele specifieke thema's die naar aanleiding van DigiNotar naar boven zijn gekomen.

4.3.1 Stelsel gekwalificeerde certificaten

In het stelsel van gekwalificeerde certificaten vormen de bijlagen van de Europese Richtlijn de basis voor de normen waaraan een certificatiedienstverlener moet voldoen. De meeste technische specificaties die op Europees niveau zijn opgesteld, hebben in Europa geen wettelijke status. Het risico hiervan is dat lidstaten verschillende normenkaders hanteren waardoor er verschillen in betrouwbaarheid kunnen ontstaan en de beoogde interoperabiliteit niet gerealiseerd wordt. Een gerationaliseerd raamwerk van normen [zoals 48], waar de Richtlijn naar verwijst, kan dit risico beperken. Zeker wanneer dit raamwerk alle eisen uit de Richtlijn en bijbehorende beschikkingen invult.

In de Nederlandse Wet [10], het bijbehorende Besluit [12] en de Regeling [13] over Elektronische Handtekeningen worden de eisen uit de bijlage van de Richtlijn geïnterpreteerd. De ruimte die de Richtlijn biedt kan door de wetgever op verschillende manieren worden ingevuld. Hierbij zijn destijds beleidsmatige keuzes gemaakt. In de Regeling wordt verwezen naar bepaalde Europese specificaties. Zo zijn de eisen aan gekwalificeerde certificaten (bijlage I van de Richtlijn) uitgewerkt in artikel 3 van het Besluit. De Regeling stelt vervolgens dat vermoed mag worden dat voldaan wordt aan de eisen uit dit artikel, indien voldaan wordt aan de Europese specificatie [46]. Op vergelijkbare wijze worden de 12 eisen die gesteld worden aan certificatiedienstverleners (bijlage II van de Richtlijn) uitgewerkt in artikel 2 van het Besluit. Hier maken ook de eisen voor het domein van de betrouwbare systemen die certificatiedienstverleners dienen te gebruiken deel van uit. De Regeling bepaalt dat voldaan wordt aan de meeste eisen uit dit artikel, indien voldaan wordt aan de (bijna 200 eisen van de) Europese specificatie ETSI TS 101 456. Vervolgens worden ook de eisen aan een veilig middel (bijlage III van de Richtlijn) beschreven in artikel 5 van het Besluit en in artikel 4 van de Regeling via een rechtsvermoeden gelijkgesteld aan de Europese Afspraak CWA 14169 [51] als het gaat om de conformiteitbepaling. Tenslotte worden in het Besluit in artikel 4 ook de eisen aan auditors benoemd die wordt geconcretiseerd in een separate Beleidsregel [14].

Nadere beschouwing van deze 'rechtsvermoedens' laat zien dat de volledigheid en de juiste formulering van de eisen onderling niet geborgd is. Zo zijn er zaken die in de Nederlandse wet- en regelgeving vereist worden, maar niet terugkomen in de ETSI 101 456 specificatie. De Regeling geeft bijvoorbeeld aan dat conformiteit met ETSI 101 456 een conformiteit inhoudt met artikel 2.1 a..m, o en r van het Besluit. De artikelen 2.1 n, p, q en s worden hier kennelijk beschouwd als niet gedekt door de ETSI-norm. Deze door de Nederlandse wetgever van belang geachte aspecten betreffen de aanwezigheid van procedures voor klachtenafhandeling en geschillenbeslechting, over de verplichtingen om overdracht en continuïteit te borgen als de dienstverlening van een certificatiedienstverlener stopt en over de integriteit van de medewerkers: ze mogen niet voor 6 maanden of langer veroordeeld zijn. Een audit tegen het TTP.NL schema die naar de ETSI 101 456 norm verwijst, lijkt geen conformiteit vast te stellen met deze zaken. Analyse van deze ETSI-norm laat zien dat sommige zaken echter wel beschreven worden. Zo bevat eis 7.5.f de verplichting om procedures te hebben voor het afhandelen van klachten en geschillen. In eis 7.4.9 is de overdracht en continuïteit opgenomen, met een aanvullende bepaling over een financiële regeling bij faillissement.

Het TTP.NL schema verwijst naar de ETSI-norm, maar stelt ook aanvullende eisen als het gaat om de auditaanpak. De Opta accepteert een TTP.NL certificering, maar andersom geldt in de opzet niet dat op basis van een registratie bij de Opta verondersteld mag worden dat er voldaan wordt aan TTP.NL (dit is immers niet verplicht). Het risico van al deze verwijzingen is dat de zekerheid die met een audit verkregen wordt niet duidelijk is. Een ander risico betreft het beheer van de ETSI-normen waarnaar verwezen wordt: als die worden veranderd of juist jarenlang niet bijgehouden, heeft Nederland daar slechts indirect invloed op.

De ETSI-norm is bedoeld om uitwerking te geven aan de meer abstracte eisen van de Richtlijn. Voor de procedures met betrekking tot productie en uitgifte van certificaten is dat het geval. Voor de zaken die de beveiliging van systemen en informatie betreffen is dat zeer beperkt het geval. Het risico van weinig concreet uitgewerkte normen voor de informatiebeveiliging, is dat er een grote mate van diversiteit kan ontstaan in de wijze waarop de diensten en producten beveiligd zijn en in de wijze waarop audits de beveiliging toetsen.

4.3.2 Stelsel PKIoverheid

Het Programma van Eisen (PvE) van PKIoverheid rust op het TTP.NL schema, maar voegt daar eisen aan toe. Vaak is dit een aanscherping van een eis uit het schema. Zo wordt er van de procedures rondom klachten en geschillen bepaald dat ze het instellen van procedures bij de gewone rechter niet mogen beletten. Van de 80 eisen en sub-eisen zijn er 30 nieuw [17, deel 3a bijlage B]. Deze eisen gaan onder andere over de backup en archivering van geheime sleutels, en over de aansprakelijkheid. Met het PvE neemt de Rijksoverheid de ruimte om los van Europese regelgeving en normering eisen te stellen aan certificatiedienstverleners onder PKIoverheid. De ETSI-eisen met betrekking tot informatiebeveiliging in het PvE worden nauwelijks verder uitgewerkt.

4.3.3 Beide stelsels

De overlap in beide stelsels betreffen de gekwalificeerde certificaten. De overlap van normen die in de beide stelsels gelden is niet eenvoudig vast te stellen. In het stelsel van de gekwalificeerde certificaten die niet onder PKIoverheid vallen, gelden de normen uit de wet- en regelgeving voor de elektronische handtekeningen. Voor de gekwalificeerde certificaten die onder PKIoverheid vallen, geldt ook het normenkader van PKIoverheid. In het geval van vrijwillige accreditatie is de overlap datgene wat is vastgelegd in het TTP.NL schema, in het geval van directe registratie bij de Opta is de overlap onduidelijk. De exacte relatie tussen TTP.NL en de wet is in de stelsels niet transparant gemaakt. Daarbij blijkt er licht te zitten tussen TTP.NL en de ETSI-norm: het schema TTP.NL bevat diverse bepalingen over de wijze van auditen die in ETSI niet genoemd worden. Ook zijn er wat dit betreft bepalingen in de ETSI-norm die geen deel uitmaken van TTP.NL. Zo is de reikwijdte van de audit in de ETSI-norm: alle eisen uit het ETSI-document en het van toepassing zijnde beleid inzake gekwalificeerde certificaten. De reikwijdte is TTP.NL is alleen het management systeem.

Ook blijkt er licht te zitten tussen TTP.NL en de Europese Richtlijn. Zo is artikel 8 van de Richtlijn heel concreet en vergaand als het gaat om de bescherming van de privacy. In de ETSI-eis 7.4.10 wordt conformiteit met de nationale privacywetgeving vereist. Artikel 8.2 van de Richtlijn gaat veel verder. Zoals de Rekenkamer al in 2001 aangaf [64], zijn certificatie-dienstverleners aan veel strengere eisen zijn gebonden dan anderen die persoonsgegevens verwerken: de enige rechtmatige grond waarop zij persoonsgegevens mogen verwerken is de uitdrukkelijke toestemming van de betrokkene. Het begrip ‘uitdrukkelijke toestemming’ houdt meer in dan een handtekening onder een contract dat verwijst naar algemene voorwaarden. De toestemming moet gebaseerd zijn op juiste, duidelijke en volledige informatie over de beoogde verwerking. Ook moet de toestemming vrijwillig gegeven zijn. Indien het niet geven van een dergelijke toestemming tot gevolg heeft dat de conformiteitsverklaring niet verkregen wordt, kunnen vragen gesteld worden in welke mate toestemmingen vrijwillig gegeven kunnen worden. De genoemde eis komt in deze vorm niet terug in TTP.NL, niet in de betreffende Europese norm, en ook niet in het PvE van PKIoverheid.

4.3.4 Specifieke thema’s

In deze paragraaf analyseren we het normenstelsel op enkele inhoudelijke zaken die als zwaktes van de stelsels aan het licht zijn gekomen door de DigiNotar affaire.

4.3.4.1 Informatiebeveiliging

In Bijlage II van de Europese Richtlijn worden de eisen gespecificeerd waaraan een dienstverlener moet voldoen om gekwalificeerde certificaten uit te mogen geven. Onderdeel van deze eisen zijn beveiligingseisen, zoals

- bekendheid van het personeel met goede beveiligingsprocedures (e),

- de bescherming van systemen tegen wijzigingen (f),
- het nemen van maatregelen tegen het vervalsen van certificaten (g), en
- het garanderen van de vertrouwelijkheid van het proces (g).

Deze beveiligingseisen komen terug in de twee uitwerkingen van de Richtlijn: de Europese ETSI-norm en de nationale wet- en regelgeving met betrekking tot gekwalificeerde certificaten.

In het Besluit, wordt in artikel 2.1 beschreven aan welke eisen een certificatiedienstverlener zich moet houden. Zo dient het personeel dat in dienst is, deskundig te zijn op het gebied van de beveiligingsprocedures en er dienen adequate maatregelen getroffen te worden tegen het vervalsen van de gekwalificeerde certificaten. Deze twee eisen komen overeen met de Wet.

Het Besluit vereist dat een gekwalificeerd certificaat is aangemaakt met een 'betrouwbaar systeem' [12, artikel 2.1.c]. De norm die hiervoor volgens de EU Richtlijn gehanteerd dient te worden is echter niet in de Nederlandse wet- en regelgeving opgenomen. Wel wordt hierin aan de certificatiedienstverlener een eis gesteld dat deze met de ontwikkeling van de techniek mee dient te lopen. Van de auditor wordt verwacht dat hij dit steeds weer opnieuw vaststelt.

Volgens het TTP.NL schema moet betrouwbaarheid van gebruikte systemen worden vastgesteld volgens een Europese afspraak [49] of een vergelijkbare norm. Door de beperkte verankering in de Nederlandse wet- en regelgeving bestaat in opzet het risico dat er in Nederland minder betrouwbare systemen worden gebruikt door certificatiedienstverleners dan in sommige andere lidstaten (waaronder België en Duitsland). In het bijzonder wanneer zij kiezen voor directe registratie bij de Opta.

De Minister van EL&I kan volgens de WEH een instelling aanwijzen die belast is met het beoordelen van de overeenstemming van 'veilige middelen' met de wettelijk eisen [10, artikel 18.7-2]. Dit is echter in Nederland niet gebeurd. Andere lidstaten, waaronder Duitsland, hebben dit wel gedaan. Hierdoor bestaat in Nederland het risico dat auditors die certificatie-dienstverleners beoordelen in beide stelsels minder zekerheid kunnen bieden ten aanzien van het uitleveren van certificaten op veilige middelen.

In de ETSI 101 456 norm staan in hoofdstuk 7.2.1 de eisen waar de omgeving aan moet voldoen waar de certificaten worden gemaakt om vervalsing te voorkomen. Hierbij wordt verwezen naar andere normen, en die bepalen dat er voor voldoende beveiliging gezorgd moet zijn. 7.4.1 bevat de eisen voor security management. In 7.4.4 wordt in abstracte termen gesteld dat de personen adequaat geautoriseerd moeten worden en dat diefstal van informatie tegengegaan moet worden. In 7.4.5 wordt bescherming tegen virussen, kwaadaardige en ongeautoriseerde software genoemd. In 7.4.6 wordt aanbevolen om firewalls zodanig te configureren dat op protocol niveau de toegang tot de servers wordt beschermd. Ook worden als voorbeeld intrusion-detection-systems genoemd, continue monitoring en alarm faciliteiten. Sommige eisen zijn in de ETSI-norm iets concreter gemaakt, bij de meeste bestaat de uitwerking vooral uit herformuleren op hetzelfde abstractieniveau. Daar waar de normen wel

concreter zijn uitgewerkt, zijn dit voorbeelden of informatieve verwijzingen, waarvan de status minder duidelijk is.

Het TTP.NL schema bevat, naast eisen over de wijze van auditen, geen uitwerking van de ETSI normen. Ook op het gebied van de informatiebeveiliging voegt het TTP.NL schema niets specifieks toe. De toegevoegde waarde van TTP.NL als het gaat om een meer concrete uitwerking van de normen, zit vooral in de bijbehorende handreikingen [21, 22]. Daarin is soms nauwkeuriger geformuleerd wat vereist wordt, soms worden aanwijzingen voor de auditors gegeven en er wordt vaak een 'best practice' beschreven. Het toevoegen van 'eigen' normen aan het TTP.NL schema is door het CvB TTP.NL nooit beoogd.

Voor de beveiliging van het sleutelgeneratie proces wordt in het TTP.NL schema, net als in de ETSI-norm, verwezen naar drie mogelijke normen. In aanvulling hierop geeft TTP.NL de handreiking: 'de auditor dient na te gaan of de betreffende module geïnstalleerd is volgens de gekozen norm'. Dit verhoudt zich moeilijk met de context van een management systeem audit. Een risico van de handreikingen is de onduidelijke positionering: het is niet duidelijk of ze normatief of informatief van aard zijn.

Binnen het normenstelsel bevat alleen de ETSI-norm een informatieve verwijzing naar de voorloper van de nu algemeen erkende beveiligingsnorm ISO 27001. Ook deze norm heeft als object een management systeem en is weinig concreet. De ETSI-norm kent bijvoorbeeld geen verplichting tot reguliere penetratietesten om de daadwerkelijke beveiliging te testen. Er wordt gemeld dat toezichthouders bij signalen van misbruik of inbraak kunnen ingrijpen, maar er is niet geregeld hoe die signalen bij de betreffende instantie terecht moeten komen, anders dan vanuit de certificatiedienstverleners zelf. Rapportage op basis van continue monitoring door een onafhankelijke betrouwbare partij wordt nergens genoemd.

Het PvE van PKIoverheid geeft geen aanvullingen of verscherpingen van de informatie-beveiligingseisen die voortvloeien uit het TTP.NL schema.

Samengevat kan geconcludeerd worden dat er op het punt van informatiebeveiliging voor de auditor, door de vele verwijzingen en interpretatiemogelijkheden, geen eenduidig en concreet normenkader is voor het uitvoeren van audits.

4.3.4.2 Risicoanalyse

De basis voor risicobeheersing is het uitvoeren van een deugdelijke risicoanalyse. Deze wordt in de WEH niet genoemd. Door de ETSI-standaard (7.4.1.a) en in het TTP.NL schema (hoofdstuk 3 stap 3) wordt een risicoanalyse wel vereist. In de opzet van de stelsels is echter niet geborgd dat de risicoanalyse regelmatig geactualiseerd wordt. Afgaand op de formeel beschreven rollen van de Opta, speelt de toezichthouder hierin geen rol. In opzet komt het College van Belanghebbenden TTP.NL in aanmerking voor een bespreking van de gedeelde risico's gebaseerd op een actueel dreigingsbeeld. Het is binnen de stelsels immers de plicht van certificatiedienstverleners en van auditors om de marktontwikkelingen in te brengen bij dit College.

In de beveiligingswereld is het gebruikelijk om beveiligingsmaatregelen te ontlenen aan twee bronnen: een verzameling verplichte minimum maatregelen (‘de baseline’), en additionele maatregelen die voortvloeien uit een specifieke risicoanalyse. De risicomanagement cyclus in het algemeen en de rol van risicoanalyses in het bijzonder heeft in de ETSI-standaard niet de prominente plaats die het in andere gezaghebbende beveiligingsstandaarden wel heeft (zoals ISO 27002). Bovendien is in de ETSI-standaard risicoanalyse niet gepositioneerd als aanvullend op de minimum maatregelen die de rest van de standaard vereist.

4.3.4.3 Meldplicht

Een certificatiedienstverlener is verplicht om onregelmatigheden direct te melden. Dat staat in de ETSI-norm, in het TTP.NL schema, in het PvE van PKIoverheid en in de contracten met de auditor en Logius. Het belang hiervan is kennelijk onomstreden, maar als certificatiedienst-verleners redenen hebben om hier geen gevolg aan te geven, is het niet duidelijk wat de sancties zullen zijn. Zo is het onduidelijk of er voor de Opta verschil is tussen ETSI-normen die een uitwerking zijn van wettelijke bepalingen en ETSI-normen die dat niet zijn. De meldplicht valt in de laatste categorie.

Bovendien zullen auditors en toezichthouders eerst de afwijkingen benoemen en de certificatiedienstverlener tijd geven om ze op te lossen wanneer andere partijen onregel-matigheden ontdekken en dat melden.

5 ANALYSE VAN DE WERKING VAN DE STELSELS

In dit hoofdstuk worden risico's in de stelsels van de gekwalificeerde certificaten en van PKIoverheid geanalyseerd, voor zover ze gerelateerd zijn aan de werking van de stelsels. We behandelen achtereenvolgens risico's gerelateerd aan de organisatie van de stelsels, aan het toezicht binnen de stelsels, in het normenkader en gerelateerd aan de marktwerking. Daar waar relevant is aangegeven welk van beide stelsels het betreft.

5.1 DigiNotar

5.1.1 Consequenties

De compromittering van DigiNotar heeft velen verrast. Voordien was niet inzichtelijk hoe afhankelijk vitale sectoren waren geworden van certificaten van dienstverleners als DigiNotar. Ook de afhankelijkheid van (Amerikaanse) browserleveranciers werd pas goed duidelijk toen zij op het punt stonden de certificaten van DigiNotar onbruikbaar te maken. Dit zou er toe leiden dat er geen betrouwbare communicatie meer zou kunnen plaatsvinden op basis van DigiNotar certificaten.

Certificaten van DigiNotar werden onder andere gebruikt voor het beveiligen van elektronische communicatie tussen overheidsorganen onderling, tussen overheidsorganen en burgers en bedrijven, maar ook in de private sector. Voorbeelden van processen die hierdoor tot stilstand bleken te kunnen komen waren de communicatie tussen de rechterlijke macht en de advocatuur, het inklaren van goederen in de haven van Rotterdam en het uitwisselen van informatie tussen overheidsinstellingen en de belastingdienst. Nadat deze mogelijke gevolgen bekend waren geworden, heeft de Minister van BZK ingegrepen om het effect te beperken. Een onderdeel hiervan was het maken van een afspraak met Microsoft, om een patch van hun browsers waarmee DigiNotar certificaten ongeldig zouden worden, in Nederland later te distribueren. Uit het Fox-IT onderzoek [62] is gebleken dat DigiNotar vanaf 19 juni 2011 op de hoogte was van de compromittering van hun systemen terwijl al op 6 juni een eerste verkenning door de hacker had plaatsgevonden. De beschikbare informatie gaf toen aan dat deze compromittering de 'eigen merk' certificaten betrof, en niet de certificaten die onder overheidstoezicht staan. DigiNotar heeft in juli 2011 zelfstandig een extern onderzoek laten doen naar de compromittering. De resultaten werden aan het management van DigiNotar gerapporteerd op 27 juli 2011. Hieruit kwam naar voren dat de webservers en de systemen die de certificering ondersteunen gecompromitteerd waren. Deze resultaten zijn niet gecommuniceerd met de auditor, Logius of de Opta. Pas toen Govcert door haar Duitse zusterorganisatie geattendeerd werd op een mogelijk gefalsificeerd certificaat dat was uitgegeven door DigiNotar en DigiNotar hierover werd geïnformeerd, heeft het bedrijf een nader onderzoek laten uitvoeren door Fox-IT. Fox-IT stelde vast dat niet uitgesloten kon worden dat de compromittering ook de door de overheid gereguleerde PKI-stelsels betroffen.

Er is vast komen te staan dat van het vervalste Google-certificaat actief misbruik is gemaakt [62]. Of dat voor andere vervalste certificaten eventueel ook geldt, is niet zeker. In Nederland is in ieder geval schade veroorzaakt doordat niet alle DigiNotar certificaten onmiddellijk konden worden vervangen en als gevolg daarvan bepaalde elektronische communicatie tijdelijk tot stilstand kwam. Er is een nationale crisis uitgeroepen waardoor, voor het eerst, het Nationaal Crisis Centrum de regie voerde over de afhandeling van een IT-beveiligingscalamiteit. Vele overheidsinstellingen, certificatiedienstverleners, ICT-dienstverleners en anderen zijn zeer intensief in touw geweest om de gevolgen, met succes, beheersbaar te maken.

Toen DigiNotar de compromittering ontdekte, verkeerde ze in de veronderstelling dat de compromittering slechts 'eigen merk' certificaten betrof. De meldplicht aan de auditor en aan Logius is niet alleen van toepassing op certificaten binnen de stelsels, maar ook op 'eigen merk' certificaten indien er een risico voor de stelsels ontstaat. Het contract tussen DigiNotar en het ministerie van BZK maakt melding van een meldplicht in geval van 'compromittering van geheime sleutels en andere relevante incidenten'. Fox-IT constateerde dat DigiNotar gebruik maakte van gedeelde infrastructuur, procedures en personeel voor 'eigen merk' certificaten en voor door de overheid gereguleerde certificaten. Het incident kan daarmee als relevant voor de door de overheid gereguleerde stelsels worden gekwalificeerd. Hiermee heeft DigiNotar in ieder geval laten blijken de mogelijke consequenties van de compromittering voor de stelsels te onderschatten. De feitelijke reden waarom DigiNotar het incident niet heeft gemeld, is tijdens het onderzoek niet vast komen te staan. Het is niet mogelijk geweest om de betrokkenen van DigiNotar op dit punt te horen.

DigiNotar was niet de eerste certificatiedienstverlener die in 2011 werd gecompromitteerd. Er zijn aanwijzingen dat het dezelfde hacker was die in maart 2011 een grotere certificatie-dienstverlener (Comodo) compromitteerde. Comodo is geen onderdeel van de door de Nederlandse overheid gereguleerde PKI-stelsels. Indien de informatie over de Comodo-hack samen met mogelijke risicomitigerende maatregelen direct aan de certificatiedienstverleners binnen de Nederlandse stelsels was gecommuniceerd, eventueel direct gevolgd door een audit, dan was het risico op compromittering van DigiNotar verkleind. Dat is niet gebeurd. In versie 3.1. van het PvE PKIoverheid van 1 juli 2011 heeft Logius, mede naar aanleiding van de Comodo-hack, wel enkele aanvullende eisen opgenomen. Deze hebben echter niet onmiddellijk effect op de operatie van certificatiedienstverleners gehad.

5.1.2 Primaire oorzaak

Het management van DigiNotar was in de eerste plaats zelf verantwoordelijk voor het leveren van een deugdelijke en betrouwbare dienst die overeenkomt met de door hen gecommuni-ceerde verwachtingen. Doordat het technisch forensisch onderzoek van Fox-IT heeft aangetoond, dat sommige elementaire informatiebeveiligingsmaatregelen niet aanwezig waren of niet adequaat functioneerden, mag worden gesteld dat de leiding van DigiNotar zich

onvoldoende rekenschap heeft gegeven van de daaraan verbonden risico's voor hun bedrijfsvoering, voor hun klanten en voor de samenleving als geheel.

De feitelijke verklaring waarom DigiNotar preventief niet heeft gedaan wat nodig was om de hacker buiten de deur te houden is tijdens ons onderzoek niet vast komen te staan.

5.1.3 Eerstelijns controle

DigiNotar was geregistreerd bij de Opta via 'vrijwillige accreditatie' en was opgenomen in het stelsels PKIoverheid. Ze beschikte over een verklaring van conformiteit met TTP.NL van een geaccrediteerde auditor, die was afgegeven op 1 november 2010 en drie jaar geldig was. Waar tijdens de certificeringsaudit in oktober 2010 door de auditor naar gekeken is, en of daar afwijkingen van de normen zijn geconstateerd is onderdeel van een vertrouwelijk auditrapport.

Naast Logius is ook de auditor van DigiNotar niet door het management van DigiNotar op de hoogte gebracht toen de compromittering was geconstateerd. Zij ontvingen pas een signaal toen ze eind augustus voor andere auditwerkzaamheden ter plekke waren. Toen ze direct daarna een onderzoek wilde starten bij DigiNotar werden ze ingehaald door het Fox-IT onderzoek dat net was gestart.

De conformiteitsverklaring is door de auditor niet expliciet ingetrokken omdat zij toen niet in de gelegenheid werden gesteld om zelf onderzoek te doen. Met het failliet verklaren van DigiNotar is het contract ontbonden en de conformiteitsverklaring ongeldig geworden.

Of de maatregelen die door Fox-IT als zwak zijn bevonden, ten tijde van de certificeringsaudit in oktober 2010 door de auditors expliciet als adequaat zijn beoordeeld, is door de partijen die toegang hebben tot de rapporten van deze certificeringsaudits niet vast te stellen. Een belangrijke oorzaak daarvan is dat auditrapporten alleen afwijkingen van de norm beschrijven. Er wordt niet expliciet aangeven welke zaken afdoende zijn bevonden.

5.1.4 Tweedelijns controle

5.1.4.1 Stelsel gekwalificeerde certificaten

Toen de Opta werd geïnformeerd over de compromittering van DigiNotar heeft zij de laatste auditrapporten bij de auditor opgevraagd. Op basis van het Fox-IT rapport en een verklaring van DigiNotar heeft ze geconcludeerd dat DigiNotar niet meer voldeed aan de in de wet gestelde eisen. Daarop heeft de Opta besloten de registratie van DigiNotar in te trekken [63]. Zij achtte het op dat moment voldoende bewezen dat niet aan de wettelijke eisen werd voldaan. Op dat moment was de conformiteitsverklaring door de auditor niet ingetrokken. De werking van de tweedelijns controle (in casu de Opta) heeft de werking van de eerstelijns controle ingehaald.

Wanneer incidenten in een crisissituatie worden opgelost, bestaat er het risico dat er zwaardere maatregelen worden ingezet dan op grond van het feitelijke probleem nodig is. De bijeffecten die zich als gevolg van het publiekelijk en krachtdadig ingrijpen van het Ministerie van BZK en

van de Opta hebben gemanifesteerd zijn dat er voor DigiNotar nauwelijks meer een mogelijkheid was om de problemen op te lossen. Het vertrouwen in het hele bedrijf was verdampt, het bedrijf ging failliet en er werden gerechtelijke procedures met betrekking tot het besluit van de Opta gestart.

5.1.4.2 Stelsel PKIoverheid

Logius had voor de DigiNotar crisis de rapporten van de laatste certificeringsaudit van DigiNotar ontvangen. Deze zijn, voorafgaand aan het incident, geen aanleiding geweest om richting DigiNotar actie te ondernemen.

Toen op vrijdag 2 september 2011 op basis van het tijdelijke Fox-IT rapport bleek dat niet kon worden uitgesloten dat certificaten onder PKIoverheid gecompromitteerd waren, wilde Logius DigiNotar in eerste instantie operationeel van PKIoverheid afkoppelen. Toen echter bleek dat dit een groot maatschappelijk risico betekende, is deze actie gestaakt. Logius heeft daarna samen met Govcert actief overleg gevoerd met browserleveranciers om te voorkomen dat zij het vertrouwen in DigiNotar certificaten onmiddellijk zouden intrekken.

Ondanks het feit dat DigiNotar failliet is verklaard draait het bedrijf op kleine schaal door onder regie van het ministerie van BZK totdat een belangrijk proces van de Belastingdienst over is gegaan op niet-DigiNotar certificaten.

Door de plotselinge grootschalige migratie naar certificaten van andere certificatiedienst-verleners, moesten deze snel opschalen. Hierop waren ze niet voorbereid.

Het risico, wat in opzet bestond, dat de continuïteit van bedrijfsprocessen in vitale sectoren als gevolg van het wegvallen van vertrouwen in een certificatiedienstverlener in gevaar zou komen, heeft zich tijdens de DigiNotar crisis ook daadwerkelijk gemanifesteerd.

5.1.4.3 Beide stelsels

De Raad voor Accreditatie die de auditor van DigiNotar had geaccrediteerd, heeft ten tijde van de crisis onderzocht of de accreditatie van de auditor terecht was verleend. Dit onderzoek heeft niet geleid tot het intrekken van de accreditatie van de auditor. Het maken van een keuze om de conformiteitsverklaring van DigiNotar in te trekken werd ingehaald door het feit dat DigiNotar failliet ging.

5.2 Organisatie

5.2.1 Opta registratieroutes

In opzet zijn er twee manieren om als certificatiedienstverlener geregistreerd te kunnen worden bij de Opta, voor het leveren van gekwalificeerde certificaten: ‘vrijwillige accreditatie’ en ‘directe registratie’. In de praktijk is echter nog nooit een dienstverlener via de ‘directe registratie’ bij de Opta geregistreerd. Dit wordt veroorzaakt doordat de ‘vrijwillige accreditatie’ route voor certificatiedienstverleners in de praktijk een paar voordelen biedt. De markt van gekwalificeerde

certificaten is een relatief kleine markt. Deze potentiële markt wordt vergroot wanneer de certificatiedienstverlener ook gekwalificeerde certificaten binnen het stelsel PKIoverheid kan leveren. Alle commerciële certificatiedienstverleners die bij de Opta zijn geregistreerd hebben er dan ook voor gekozen om zich bovendien bij PKIoverheid aan te sluiten. Voor beide stelsels geldt een toezichtsregime dat audits vereist.

Wanneer is gekozen voor een 'vrijwillige accreditatie' bij de Opta is de overlap in het normenstelsel gelegen in het TTP.NL schema. Conformiteit aan het TTP.NL schema en aan de additionele eisen van het PvE PKIoverheid kan binnen één conformiteitsaudit door een certificerende instelling worden vastgesteld. In het geval van 'directe registratie' bij de Opta zou de certificatiedienstverlener ook conformiteit moeten aantonen aan wettelijke eisen. Bovendien zou voor PKIoverheid ook dan een audit tegen het TTP.NL schema benodigd zijn. Vrijwillige accreditatie is dus voor een certificatiedienstverlener die moet voldoen aan PKIoverheid het meest kosteneffectief.

De bij de Opta beschikbare capaciteit voor het houden van toezicht op het stelsel was tot 1 januari 2011 0,3 FTE. Dit werd voldoende geacht vanuit de keuze voor het houden van 'licht toezicht'. Er is daarna een uitbreiding gekomen als gevolg van de invoering van additionele regelgeving [4, 5]. Bovendien beschikt de Opta niet over diepgaande technische expertise of auditexpertise op het gebied van gekwalificeerde elektronische handtekeningen. Daarmee is de Opta momenteel kwantitatief en kwalitatief onvoldoende toegerust om directe registratie-verzoeken correct af te handelen.

Een risico van de huidige manier van toezicht is dat voor het toezicht op de juiste werking van de wettelijke eisen, in de praktijk volledig wordt vertrouwd op een conformiteitsverklaring van de auditor. Het is moeilijk voor de Opta om het werk van de auditor op waarde te schatten en de consistentie en geschiktheid van het normenkader kan niet goed worden beoordeeld. Het passieve toezicht dat de Opta in de praktijk uitoefent, dat overeenstemt met de opzet, brengt het risico met zich mee dat signalen niet tijdig worden ontvangen en dat eventueel benodigde verbeteringen in het toezicht niet worden geïdentificeerd.

5.2.2 Opdrachtgeverschap audits

De opdrachtgever van de auditors zijn de certificatiedienstverleners. Ze hebben doorgaans een langdurige relatie met de auditor. Een doorlopend contract dekt doorgaans de certificerings- en inspectieaudits. De vergoedingen daarvoor, worden betaald door de certificatiedienstverleners.

Het TTP.NL schema geeft richtlijnen voor het aantal dagen dat voor de uitvoering van beide soorten audits aangewend dient te worden. Deze richtlijnen zijn al enkele jaren geleden, op verzoek van de certificatiedienstverleners tot stand gekomen. Gebleken was toen dat de ramingen voor het aantal benodigde dagen tussen de auditors zeer sterk uiteen liepen.

De auditors geven aan geen invloed te ervaren op de kwaliteit van hun werkzaamheden vanuit commerciële prikkels of vanuit de richtlijn ten aanzien van het aantal beschikbare dagen.

Volgens hen offreren zij het aantal benodigde dagen dat noodzakelijk is voor het leveren van kwaliteit.

In de praktijk blijkt dat het noemen van een aantal dagen in het schema, werkzaam is in het bepalen van de wijze en diepgang van de audit. Er zijn auditors die hierin een bevestiging zien van het feit dat de management systeem audit geen IT-audit diepgang hoeft te hebben.

Het voordeel van een langdurige relatie met dezelfde auditor is dat deze de systemen, processen en klanten van de certificatiedienstverlener goed kent. Hij kan daarmee in korte tijd gerichter zijn werk doen. Het risico hiervan is dat mogelijk blinde vlekken bij de auditor ontstaan of dat er niet geheel onbevooroordeeld meer wordt geaudit. Er is niet vastgesteld dat het risico zich in de praktijk heeft gemanifesteerd. Er kan echter ook niet worden uitgesloten dat dat nog zal gebeuren.

In Europees verband wordt momenteel gewerkt aan een Europese standaard voor conformiteits-beoordelingen van certificatiedienstverleners [47] waarin de toezichthouders directer betrokken zijn dan momenteel voor de Opta geldt. De verantwoordelijkheden voor aansturing van het auditproces worden volgens het voorstel gedeeld tussen de certificatiedienstverlener en de toezichthouder. Met deze benadering wordt de toezichthouder in staat gesteld directer invloed uit te oefenen op de audits waardoor pro-actiever toezicht kan ontstaan.

5.2.3 Doelbinding TTP.NL schema

Het TTP.NL schema werd al ontwikkeld toen men begon met het opstellen van de Europese Richtlijn. Het beeld was destijds dat de handel via internet gekwalificeerde handtekeningen nodig had. Terugkijkend kan worden gesteld dat het belang van een juridisch geldige handtekening is overschat. Op dit moment kiest de markt vaak voor lagere niveaus van beveiliging. In Nederland was de initiële insteek bij TTP.NL niet vanuit het realiseren van adequaat toezicht en borging van vertrouwen, maar vanuit het faciliteren van de elektronische handel.

Het College van Belanghebbenden TTP.NL beheert het schema en agendeert mogelijke interpretatieverschillen en marktontwikkelingen. Een doel daarbij is om invulling te geven aan de wettelijke eisen. Het is een breed samengesteld overlegorgaan waarbij niet één partij de regie voert. Het ministerie van EL&I heeft geen zitting in het College en de Opta vervult een passieve rol in het College. Het College is bovendien beperkt doordat ze bijvoorbeeld geen inzage heeft in de rapporten van de auditors. Het is derhalve lastig voor het College om daadkrachtig en proactief op te treden.

Met betrekking tot het TTP.NL schema mag in eerste instantie van het College van Belanghebbenden verwacht worden dat aangegeven wordt hoe het schema adequaat invulling geeft aan de wettelijke eisen voor de elektronische handtekening. Als beleidsverantwoordelijke is het ministerie van EL&I eindverantwoordelijk om te bepalen of het middel (het TTP.NL schema) tegemoet komt aan het doel. De Opta houdt zich niet actief bezig met het toetsbaar

maken van de wettelijke vereisten zodat vastgesteld kan worden of daaraan wordt voldaan. Zij voert slechts het toezicht uit.

Na een actieve periode in de begin jaren van het eerste decennium van deze eeuw, toen de WEH en diverse Europese normen tot stand kwamen, is de aandacht voor het elektronische handtekeningen dossier bij het ministerie van EL&I verminderd. Het ministerie vervult op dit dossier momenteel vooral een faciliterende rol richting de Opta.

De Raad voor Accreditatie heeft het TTP.NL schema geaccepteerd. Het beoordelen of een schema geschikt is voor het beoogde doel, is geen onderdeel van acceptatie door de Raad.

Het risico dat niet één partij zich primair verantwoordelijk voelt om te borgen dat het TTP.NL schema een complete en correcte invulling geeft van de wettelijke eisen, is dat bepaalde wettelijke eisen bij conformiteitsbeoordelingen niet aan de orde komen. Dat risico is in de opzet besloten zoals uit de analyse van hoofdstuk 4 gebleken is.

Ook in door de auditors afgegeven conformiteitsverklaringen is een verwijzing naar wet en regelgeving geen standaard element. De auditors nemen dat niet expliciet mee in hun conformiteitbeoordelingen. Zij toetsen conformiteit aan het TTP.NL schema en/of de ETSI 101 456 norm. Het daarmee gepaard gaande risico is dat de wettelijk toezichthouder (de Opta) en anderen die vertrouwen op de conformiteitsverklaring baseren, menen dat deze verklaringen conformiteit met de wet impliceert, terwijl dat niet noodzakelijkerwijs het geval is.

5.3 Toezicht

5.3.1 De rol van risicoanalyse

In opzet van het TTP.NL schema is de uitvoering van een risicoanalyse die basis is voor selectie van maatregelen bij een certificatiedienstverlener een belangrijke stap. Bij conformiteits-beoordelingen van management systemen voor beveiliging (zoals bij ISO 27001) speelt risicobeheer in het algemeen en de risicoanalyse in het bijzonder vaak een prominente rol.

De risicoanalyse die certificatiedienstverleners volgens het normenstelsel worden geacht te maken voor hun dienstverlening wordt door de auditors als belangrijk gezien, maar vormen in de praktijk geen leidraad voor een audit. Zoals aangegeven in paragraaf 4.3.4.2 is de rol die de risicoanalyse in de stelsels zou moeten spelen ook niet geheel helder. In de praktijk zou deze moeten leiden tot selectie of aanscherping van specifieke maatregelen die van toepassing zijn.

In de praktijk is de risicoanalyse vaak van onvoldoende kwaliteit of diepgang om leidend te kunnen zijn tijdens een audit. De door de certificatiedienstverlener concreet geselecteerde beveiligingsmaatregelen zijn vaak niet terug te voeren op een gedocumenteerde risicoanalyse. De actualiteit van het dreigingsprofiel waarop de risicoanalyse van de certificatiedienstverlener is gebaseerd is geen expliciet onderwerp van onderzoek.

Bij het beoordelen van de risicoanalyse maken de auditors geen gebruik van een standaard methode of best practice voor het beoordelen van de aanwezige risicoanalyses. De auditors

beoordelen de aanwezige risicoanalyses op basis van hun 'professional judgement'. Mogelijke specifieke externe dreigingen krijgen daarin niet expliciet aandacht.

Het risico van het ontbreken van een adequate risicoanalyse, is dat met de maatregelen niet aangesloten wordt bij de daadwerkelijke betrouwbaarheidsrisico's van een certificatiedienst-verlener.

5.3.2 Concreetheid van het toezicht

5.3.2.1 Diepgang van de Conformiteitsaudit

In de praktijk beoordelen de auditors, conform de opzet, het management systeem van de certificatiedienstverlener en voeren ze geen volledige IT-audit uit. De diepgang van een audit van het management systeem is in de praktijk minder dan bij een IT-audit. Een management systeem certificeringsaudit zich richt in eerste instantie op de vraag of het management 'de zaak' in de greep heeft. Hieronder valt onder andere de beoordeling van processen, beleid en interne controle. Bij een IT-audit zou het daarnaast ook gaan over bijvoorbeeld de daadwerkelijke implementatie van de technische maatregelen. Daarnaast wordt aangegeven, dat de diepgang van de werkzaamheden naar de daadwerkelijke inrichting en van de werking van deze geïmplementeerde maatregelen bij een IT-audit groter is. Er worden meer detail testwerkzaamheden uitgevoerd bij een IT audit. In auditrapporten worden in de praktijk afwijkingen gerapporteerd die er op duiden dat er wel steekproefsgewijs concreet naar bestaan en werking van technische maatregelen is gekeken. De auditors gaan dus soms dieper dan een management systeem audit vereist. Er bestaan voorbeelden dat is gekeken naar de daadwerkelijke instellingen van de firewall of naar de configuratie van monitoring tooling.

Er zijn normen die voortvloeien uit Nederlandse wet- en regelgeving die door de auditors niet kunnen worden beoordeeld, omdat het niet binnen hun expertisegebied valt. Een voorbeeld is de eis van financiële soliditeit van de certificatiedienstverlener [12 artikel 2.1e, 52 artikel 7.5e]). Deze eis is overgenomen in het normenkader, maar niet geconcretiseerd, bijvoorbeeld naar toetsbare eisen aan liquiditeit, solvabiliteit of de omvang van aansprakelijkheid. Daar waar door auditors zulke normen wel zijn meegenomen bij audits, werd hierover in de praktijk minder zekerheid afgegeven dan over andere normen.

Het aantal dagen dat gebruikt kan worden voor een certificatie-audit of inspectie-audit, zoals aangeven in het TTP.NL, schema wordt door de auditors niet als beperking gezien. In de praktijk wordt de richtlijn van dit aantal dagen in grote lijnen gevolgd. De auditors geven aan primair te worden gedreven te worden door het leveren van kwaliteit. Wel wordt aangegeven dat met een reguliere IT-audit een grotere diepgang kan worden bereikt in de testwerk-zaamheden.

5.3.2.2 Frequentie en detaillering rapportage

De Opta vraagt jaarlijks de laatste auditrapporten van de auditors. Ook bij een initiële certificeringsaudit registreert de Opta een certificatiedienstverlener uitsluitend op basis van de

afgegeven conformiteitsverklaring. Soms wordt naar aanleiding van auditrapportage aanvullende informatie opgevraagd of worden aanwijzigen gegeven om onvolkomenheden op te lossen. De reden waarom de Opta de auditrapporten niet direct ontvangt bij het beschikbaar komen daarvan, of directer toezicht uitvoert, is een gevolg van het feit dat wettelijk niet is geregeld dat de Opta kan eisen dat de rapporten direct worden opgestuurd. Het uitgangspunt is het goed functioneren van en vertrouwen in de auditors.

Logius krijgt een afschrift van de auditrapporten direct nadat deze beschikbaar komen. Dit is geregeld via het Programma van Eisen PKIoverheid. Logius bestudeert de rapporten om te beoordelen of de verbeterplannen serieus zijn opgepakt. Zij heeft wel eens aanvullende testen of een actieplan geëist. Als het gaat om de wijze waarop een auditor een audit uitvoert, vertrouwt Logius op het TTP.NL schema en op de accreditatie van de auditors door de RvA.

5.3.3 Handhaving door toezichthouders

De Opta heeft eens, voor de DigiNotar affaire, een partij gedwongen om aanpassingen door te voeren onder dreiging van beëindiging van registratie. Tot voor de DigiNotar affaire is door de Opta nog nooit een registratie van een certificatiedienstverlener beëindigd noch een boete opgelegd. Daardoor is de preventieve werking van repressieve handhaving in de praktijk beperkt. De Opta heeft deze mogelijkheid volgens de Telecommunicatiewet wel. Het elimineren van een certificatiedienstverlener uit de stelsels als ultieme sanctie heeft consequenties die de toezichthouder in het algemeen zal willen vermijden. Een actief sanctiebeleid zoals boetes zouden een onderdeel van het uitgebreide toezichtarrangement kunnen vormen. Daarnaast zou de toezichthouder onder alle omstandigheden vertegenwoordigers van de certificatiedienstverlener kunnen horen.

Handhaving door de Opta is zowel repressief als preventief wettelijk geregeld. Cruciaal is de signalering op basis waarvan de Opta kan of moet ingrijpen. Er is niet geregeld dat signalen vanuit onafhankelijke bronnen of vanuit de certificatiedienstverleners aan de Opta worden doorgegeven. Iemand die een digitale inbraak professioneel uitvoert, zal als eerste de signalering van de gecompromitteerde partij om de tuin proberen te leiden. Dit is te vergelijken met een inbreker die eerst de beveiligingscamera's van een mooi beeld voorziet. Het risico van een beperkte signalering die bij de partij vandaan moet komen waar toezicht op gehouden wordt, is dat de signalering niet tijdig doorkomt.

Logius voert tweedelijns controle uit voor wat betreft certificaten binnen het stelsel PKIoverheid. Logius is tactisch beheerder van PKIoverheid en besluit, in overleg met de beleidsverantwoordelijke (het ministerie van BZK), tot acceptatie of verwijdering van certificatiedienstverleners binnen het stelsel PKIoverheid. Het eigenaarschap van PKIoverheid en van het PvE is belegd bij het ministerie van BZK. In de praktijk wordt het beheer van en het toezicht op het stelsel primair door Logius uitgevoerd. Hierdoor bestaat het risico dat keuzes ten aanzien van de strategische richting waarop PKIoverheid zich ontwikkelt in de praktijk worden gestuurd vanuit tactisch of operationeel niveau ook al worden ze formeel op beleidsniveau geaccordeerd.

5.4 Normen

5.4.1 Concreetheid informatiebeveiliging

In hoofdstuk 4 is gebleken dat in opzet er ten aanzien van normen van informatiebeveiliging nog verbeteringen mogelijk zijn. Dit is in het College van Belanghebbenden TTP.NL voor zover bekend niet expliciet besproken.

Het actueel houden van risicoanalyses hoort een belangrijk onderdeel te zijn van het management systeem van de certificatiedienstverleners. In de praktijk hebben we niet kunnen vaststellen dat dit bij het auditen van het management systeem expliciete aandacht krijgt. Het kan effectief zijn om een gemeenschappelijke risicoanalyse aanvullend uit te voeren. Aanscherping van het normenkader met concrete informatiebeveiligingseisen kan het best plaatsvinden op basis van een risicoanalyse die actuele bedreigingen en de gemeenschappelijke processen en systemen van de certificatiedienstverleners tot uitgangspunt neemt. Wanneer ogenschijnlijk effectieve concrete beveiligingsmaatregelen worden geselecteerd bestaat het risico dat ze niet gerelateerd zijn aan feitelijke dreigingen en/of niet goed kunnen worden geïmplementeerd in de praktijk van certificatiedienstverleners.

Het uitvoeren van een risicoanalyse heeft geen deel uitgemaakt van dit onderzoek. Wel zijn tijdens het onderzoek op een aantal punten verbeteringsmogelijkheden naar voren gekomen.

We geven enkele voorbeelden van gebieden die in de risicoanalyse specifieke aandacht zouden kunnen krijgen:

- Er wordt in het normenkader relatief veel aandacht geschonken aan preventieve maatregelen. Detectie, monitoring en een snelle response kunnen ook zeer effectief zijn. Zeker in het licht van het feit dat uiteindelijk nagenoeg alle systemen kunnen worden gecompromitteerd. Hier zou in het normenstelsel meer aandacht voor kunnen zijn.

- Concrete eisen ten aanzien van de scheiding tussen de front-office systemen (registratieproces) en de back-office systemen (certificaatproductieproces) van certificatiedienstverleners zijn niet opgenomen in het normenstelsel. Hierdoor is niet zeker of het fysiek onmogelijk is dat een vertrouwensknooppunt (backoffice systeem) vanaf internet kan worden benaderd.

- Eisen aan sterke authenticatie voor alle medewerkers van een certificatiedienstverlener die toegang hebben tot systemen die de primaire processen ondersteunen zijn niet erg concreet.

- Een eis dat een certificatiedienstverlener een zodanige registratie zou moeten voeren dat na compromittering direct met zekerheid kan worden vastgesteld welke certificaten vervalst zijn is niet aangetroffen.

Het tweede en derde punt hierboven zijn geadresseerd in het PvE PKIoverheid vanaf versie 3.1 (juli 2011), maar zijn in het TTP.NL schema nog niet opgenomen.

5.4.2 Dynamiek dreigingen en beheer stelsels

De dreigingen op internet veranderen snel. Vrijwel dagelijks worden nieuwe kwetsbaarheden in software bekend. In de periode dat de Europese standaarden, die zijn opgenomen in de stelsels, ontstonden waren hackers veelal nog individuen die hun activiteiten primair ontplooiden om zichzelf een status binnen hun gemeenschap te verschaffen. Tegenwoordig zijn professionele criminele organisaties, hacktivisten en zeer goed geëquipeerde buitenlandse overheden actief [65].

De huidige stelsels zijn nog niet ingericht op het regelmatig bijstellen van actuele dreigingsbeelden en het op basis daarvan snel aanpassen van de eisen. In de praktijk is veel overleg nodig voordat een Europese norm, het TTP.NL schema of het PvE PKIoverheid kan worden aangepast. Het doorvoeren van wijzigingen kan in het stelsel PKIoverheid relatief snel gebeuren, maar toch kost het ook bij kritische incidenten zoals Comodo en DigiNotar enige maanden en geen weken, laat staan dagen, om het PvE hierop aan te passen. Daarna duurt het weer tot de volgende reguliere audit voordat er op getoetst wordt (wanneer het dan in het aandachtsgebied van de auditor zit).

Het risico van het niet tijdig actualiseren van de eisen waaraan certificatiedienstverleners moeten voldoen, is dat zij concrete maatregelen om nieuwe dreigingen tegen te gaan niet tijdig implementeren.

5.4.3 Verbreding EU-richtlijn

De groei van de markt van gekwalificeerde certificaten is achtergebleven bij de verwachtingen ten tijde van de invoering van de Europese Richtlijn. Dit wordt bevestigd door internationale onderzoeken [73, 74, en 77] en de marktconsultatie voor de herziening van de EU Richtlijn [78].

In deze onderzoeken worden geen harde cijfers over de verwachte groei en huidige status van gekwalificeerde certificaten in Nederland gegeven. Het beeld dat de verwachtingen ten aanzien van de markt voor gekwalificeerde certificaten oorspronkelijk overschat zijn, wordt ook voor Nederland bevestigd door verschillende geïnterviewden.

Er is echter een toenemende behoefte aan betrouwbare elektronische authenticatie vanuit de overheid en het bedrijfsleven. In Nederland wordt dit in het publieke domein gedemonstreerd door het gebruik van DigID en van eHerkenning voor bedrijven. In Europees verband wordt via het STORK-project aan interoperabiliteit tussen vier niveaus van authenticatie gewerkt [69].

5.5 De rol van de markt

5.5.1 Aantal certificatiedienstverleners

Er zijn op 1 januari 2012 zes leveranciers op de Nederlandse markt van gekwalificeerde certificaten geregistreerd bij de Opta:

a) KPN Corporate Market

b) Digidentity B.V.

c) QuoVadis Trustlink B.V.

d) ESG de Electronische Signatuur B.V.

e) Ministerie van Defensie

f) Agentschap CIBG

De eerste vier hiervan zijn commerciële certificatiedienstverleners. Dit zijn dezelfde bedrijven die ook certificatiediensten leveren binnen de PKIoverheid. De vier commerciële certificatiedienstverleners kennen op nationale schaal grote onderlinge verschillen. Niet alleen qua schaalgrootte, maar ook qua dienstenpakket. Er zijn leveranciers die uitsluitend certificatiediensten leveren en hier dus hun bestaansrecht er aan ontlenen. Andere leveranciers onderscheiden zich door innovatieve oplossingen. Sommige leveranciers zijn onderdeel van grote organisaties die andersoortige diensten leveren.

Op basis van het beperkte aantal dienstverleners, kan niet gesteld worden dat er géén marktwerking is. Het gaat echter om een beperkt aantal aanbieders die geen gelijkwaardige positie in de markt innemen. Daarbij komt dat er ook onderling certificatiediensten worden geleverd. De marktwerking is derhalve beperkt.

Het uitgangspunt voor de Europese Richtlijn en het stelsel gekwalificeerde certificaten is geweest dat er marktwerking tussen de certificatiedienstverleners op gang gebracht moet worden. Indien het uitgangspunt van markwerking gehandhaafd wordt ligt het voor de hand om maatregelen in te voeren die de marktwerking intensiever stimuleren.

Voor de continuïteit van PKIoverheid is het van belang dat er meerdere aanbieders zijn. Er zijn een aantal mogelijkheden om dit te borgen. Een eerste mogelijkheid is om onder regie van de overheid de certificatiediensten aan te besteden over meerdere dienstverleners. Hierbij kan de gehele dienstverlening worden verdeeld over meerdere leveranciers, maar ook kan de dienstverlening per onderdeel worden verdeeld. Een tweede mogelijkheid is de huidige situatie continueren waarin commerciële en overheidspartijen certificatiediensten verlenen. Een derde mogelijkheid is om niets aan te besteden. De keuze voor een van deze scenario's vergt beleidsmatige afwegingen.

5.5.2 Nationale oriëntatie

De omvang van de nationale markten voor gekwalificeerde certificaten is achtergebleven bij verwachtingen die bestonden ten tijde van de introductie van de Europese Richtlijn op de elektronische handtekeningen. Voor certificatiedienstverleners is het bedrijfseconomisch wenselijk om diensten supranationaal aan te kunnen bieden. Hiervoor bestaan echter belemmeringen. De stelsels in de lidstaten zijn namelijk primair nationaal georiënteerd. Er bestaan significante verschillen tussen lidstaten ten aanzien van wet- en regelgeving, de gehanteerde standaarden en in het toezichtsarrangement. Samen met andere verbeterpunten in de Europese richtlijn worden deze punten nader toegelicht in een recent Europees rapport [77].

Voorbeelden van verschillen in de normenkaders betreffen eisen aan bewaartermijnen, de face-to-face uitgifte van certificaten en de verplichting tot conformiteit met de ETSI-norm. Verder kent elke lidstaat registratie bij een nationale toezichthouder, maar de registratievoorwaarden verschillen. Dit maakt het voor internationaal opererende certificatiedienstverleners noodzakelijk om kosten te maken om te voldoen aan de voorwaarden van toezichthouders in verschillende landen terwijl dat niet noodzakelijkerwijs tot meer betrouwbaarheid leidt. Ook moeten ze extra kosten maken om te voldoen aan het toezichtarrangement wat in de verschillende landen geldt.

Deze verschillen vormen een belemmering voor certificatiedienstverleners om diensten in andere lidstaten te leveren. Internationaal opererende certificatiedienstverleners hanteren liever internationale standaarden zoals Webtrust dan nationale implementaties van de Europese Richtlijn.

5.5.3 Transparantie

Transparantie en eenduidigheid ten aanzien van de betrouwbaarheid van de certificatie-dienstverleners is voor de afnemers van hun diensten en voor de vertrouwende partijen van groot belang.

Het beleid dat certificatiedienstverleners zelf hebben opgesteld voor hun diensten (certificatie-beleidsdocumenten) en de specificatie van de wijze waarop ze de diensten leveren (certificatie-praktijkdocumenten) zijn publiek toegankelijk en voor de meer dan geïntereseerde afnemer, naast de conformiteitsverklaring, de enige controleerbare basis waarop het vertrouwen in een certificatiedienstverlener berust. Van alle Nederlandse certificatiedienstverleners zijn deze documenten in een actuele versie daadwerkelijk aangetroffen [28-38]. Of een certificatie-dienstverlener zich ook in de praktijk houdt aan wat ze zelf hebben beschreven, wordt niet expliciet gecontroleerd tijdens audits.

In de praktijk is de verwachte transparantie en eenduidigheid op bijvoorbeeld de afgeven conformiteitsverklaringen niet altijd aanwezig. Verwijzingen naar gehanteerde normenkaders, naar van toepassing zijnde wet- en regelgeving en verwijzingen naar het TTP.NL-schema, en

naar certificatiebeleidsdocumenten en certificatiepraktijkdocumenten zijn niet eenduidig. Dit is conform het TTP.NL schema wel verplicht [20, artikel 6.11],

De auditrapporten zijn niet inzichtelijk voor de afnemers en vertrouwende partijen, maar uitsluitend voor de certificatiedienstverlener, voor de Opta en voor Logius. Voor zover het bedrijfsgevoelige informatie betreft is dit begrijpelijk, maar met betrekking tot de auditaanpak, de reikwijdte van de audit en de operationalisering van het normenkader mag transparantie worden verwacht.

Een eenduidig overzicht van wat het daadwerkelijke object van onderzoek is van deze audits (processen en procedures of ook werking van de maatregelen), welke eisen daadwerkelijk zijn getoetst en op welke wijze, is op basis van auditrapporten niet vast te stellen. De auditors geven in hun auditrapporten geen expliciete operationalisering van het normenkader en geen testplan. In auditrapportages wordt niet standaard gemeld welke normen men met welke diepgang of met welke prioriteit heeft getoetst. Ook wordt niet verantwoord op basis waarvan genomen steekproeven zijn samengesteld. Op welke zaken expliciet conformiteit is geconstateerd wordt niet gerapporteerd.

Afwijkingen worden gerapporteerd met referenties naar de normen waaraan niet wordt voldaan. De afwijkingen worden geclassificeerd als ‘groot’ of ‘klein’. De motivatie voor de classificatie ontbreekt en de definities die de auditors hanteren voor grote en kleine afwijkingen zijn niet identiek. Het is niet ongebruikelijk dat meerdere afwijkingen worden gevonden tijdens een audit. De afwijkingen verschillen zowel in het proces waar ze betrekking op hebben als in de mate waarin ze zijn gerelateerd zijn aan IT-beveiliging. De lead auditor verzoekt bij geconstateerde afwijkingen de certificatiedienstverlener om binnen een bepaalde termijn een verbeterplan ter beoordeling aan de auditor voor te leggen. Wanneer er geen ‘grote afwijkingen’ meer bestaan wordt de conformiteitsverklaring verlengd.

De eenduidigheid, transparantie en herkenbaarheid richting zowel gebruiker als ook de Opta en Logius, kunnen sterk worden verbeterd om de risico’s op een onvolledige en/of onjuiste nakoming van wettelijke eisen te mitigeren.

5.5.4 Marktwerking auditors

In Nederland zijn op dit moment twee auditors door de Raad van Accreditatie geaccrediteerd om conformiteits- en inspectieaudits te verrichten.

Er is dus slechts zeer beperkt sprake van marktwerking tussen auditors. Het wisselen van auditor is slechts beperkt mogelijk en komt in de praktijk niet voor. Met het wegvallen van één auditor, zou de marktwerking volledig verdwenen zijn.

Vanwege wijzigingen in de Europese wetgeving is het voor buitenlandse auditors per 1 januari 2014, niet meer mogelijk om in Nederland geaccrediteerd te worden, zonder vestiging in Nederland.

Op dit moment ervaren ook de auditors geen ‘commerciële prikkel’. De markt is daar te klein voor.

Geconcludeerd kan worden dat er op dit moment in de praktijk geen marktwerking voor de geaccrediteerde auditors is. De prikkel om de beste kwaliteit tegen de beste prijs te leveren, moet daarom voort komen uit de professionaliteit van de auditors. Volgens de opzet wordt de deskundigheid en onafhankelijkheid van de auditors bij accreditatie beoordeeld.

De vraag of de in opzet gekozen weg van marktwerking, in deze situatie, de beste waarborgen biedt is daarom gerechtvaardigd.

6 ANALYSE VAN ALTERNATIEVEN

In dit hoofdstuk worden de Nederlandse stelsels vergeleken met die in België en Duitsland met als doel om te zien of hier voor de Nederlandse situatie lessen uit kunnen worden getrokken. Verschillen tussen de lidstaten maakt vergelijking mogelijk. Bij de analyse van de stelsels, zijn twee landen beschouwd die voldoende vergelijkbaar zijn met Nederland om er iets van te leren, maar voldoende onderscheidend om te voorkomen dat er niets van kan worden geleerd.

België en Duitsland zijn landen die geschikt zijn om een vergelijking mee te trekken vanwege

- hetzelfde (Europese) wettelijke kader;
- vergelijkbare professionalisering van PKI bij de overheid;
- vergelijkbare bestuurlijke cultuur inzake rol van de overheid bij certificatiediensten.

In paragraaf 6.3, tenslotte, worden enkele alternatieve benaderingen van PKI geanalyseerd om de bepalen of PKI vervangen zou kunnen worden door een ander paradigma wat betrouwbaarder elektronische communicatie mogelijk maakt.

6.1 Het stelsel gekwalificeerde certificaten

De Europese Richtlijn is in diverse lidstaten geïmplementeerd, maar nog niet in alle landen volledig. De implementaties binnen de lidstaten leveren ook geen eenduidig beeld op.

Er zijn landen die in de praktijk werken zonder toezichthouder, hoewel de Richtlijn aangeeft dat iedere lidstaat een adequaat systeem van toezicht moet hebben [11, 77]. Van de landen die het toezicht hebben opgezet, zijn er die de toezichthouder mandaat hebben gegeven om externe auditors te kiezen. Er zijn landen die certificatiedienstverleners de mogelijkheid bieden om zelf een externe auditor te kiezen die zich heeft laten accrediteren. Zoals in beschreven in hoofdstuk 3 heeft Nederland in de WEH beide mogelijkheden opengehouden.

Er zijn landen die een eigen certificeringsschema hebben opgezet dat vergelijkbaar is met TTP.NL in Nederland, maar er zijn ook landen die werken zonder een geaccrediteerd schema. Er zijn landen waarbij de Minister bij gerede twijfel een onaangekondigd onderzoek kan starten bij een certificatiedienstverlener. In Nederland is dit mandaat bij de Opta als toezichthouder belegd. Er zijn landen, zoals in Nederland waarbij de juridische geldigheid van de elektronische handtekening bij wet is geregeld, maar er zijn ook lidstaten die de Richtlijn nog niet volledig hebben geïmplementeerd [77]. De normen en specificaties die op Europees niveau zijn gecreëerd, zijn voor een beperkt deel vereist vanuit de Europese Richtlijn of de bijbehorende beschikkingen. Sommige van deze normen zijn door lidstaten wel geadopteerd als invulling van de Richtlijn. Een voorbeeld hiervan is [42], wat door Nederland in regelgeving is verankerd. Het risico van een Richtlijn zonder Europese normen en specificaties is dat er verschillen ontstaan

tussen de landen en het doel van vrije handel met juridisch geldige handtekeningen niet gehaald wordt.

6.1.1 België

De Belgische Wet op de Elektronische Handtekening [6], die de nationale implementatie van de Europese Richtlijn is, werd op 9 juli 2001 aangenomen. Bovendien is er in 2002 een Koninklijk Besluit [7] van kracht geworden dat controle en toezicht regelt op certificatiedienstverleners die gekwalificeerde certificaten verstrekt.

Het federale ministerie van Economische Zaken (FOD Economie) is in België verantwoordelijk voor het registreren van en het uitoefenen van toezicht op certificatiedienstverleners die gekwalificeerde certificaten uitgeven. Dit is, anders dan in Nederland, niet uitbesteed aan een separate toezichthoudende instantie. In België zijn verantwoordelijkheden voor beleid en toezicht in één hand gehouden. Dit verkleint de kans dat beleid en de toezichtspraktijk onvoldoende op elkaar aansluiten.

In België bestaan, evenals in Nederland, feitelijk twee routes voor de registratie van certificatiedienstverleners bij de toezichthouder. De 'directe registratie' route in België vereist dat een certificatiedienstverlener zich bij FOD Economie aanmeldt. Hierbij dienen identificerende gegevens te worden overlegd. De 'directe registratie' in Nederland vereist bovendien het overleggen van informatie op basis waarvan de Opta conformiteit met de WEH kan vaststellen. De 'vrijwillige accreditatie route' in België vereist geen conformiteitsaudit door een geaccrediteerde auditor vooraf. Dit geldt wel voor de Nederlandse vrijwillige accreditatie route.

Voor registratie middels 'vrijwillige accreditatie' bij FOD Economie dient een certificatie-dienstverlener een aanvraag in te dienen waarin conformiteit aan het BE.SIGN schema wordt verklaard. In België dient binnen 6 maanden na registratie een audit door een geaccrediteerde auditor plaats te vinden [7, artikel 4.1]. De certificatiedienstverlener kan zelf een door de Belgische nationale accreditatie-instelling (BELAC) geaccrediteerde auditor kiezen. Het auditrapport en de conformiteitsverklaring moeten door de certificatiedienstverlener worden aangeleverd aan FOD Economie. In geval van twijfel kan FOD Economie om een aanvullende audit vragen. Direct nadat een certificatiedienstverlener wordt geregistreerd is in België dus sprake van een toezichtsarrangement dat verwijdering uit het stelsel, op basis van het uitblijven van een conformiteitsverklaring door een geaccrediteerde auditor, mogelijk maakt.

In België is het verbod op verplichte certificatie van certificatiedienstverleners voor registratie uit de EU Richtlijn, geïmplementeerd door dienstverleners die gekwalificeerde certificaten uitgeven twee routes voor registratie bij FOD Economie aan te bieden die echter wel iets anders worden ingevuld dan in Nederland. In beide gevallen kunnen ze gekwalificeerde certificaten uitgeven. Bij twijfel is het aan de rechter om te beoordelen of de dienstverlener en de certificaten aan de wet voldoen. De rechter mag daarbij op basis van hun registratie geen verschil maken tussen certificatiedienstverleners. Het is echter voor afnemers van

gekwalificeerde certificaten duidelijk dat het toezichtsarrangement van FOD Economie is bedoeld om betrouwbaarheid van certificatiedienstverleners te waarborgen.

Net als in Nederland zijn in België de auditkosten bij 'vrijwillige accreditatie' voor de certificatie-dienstverlener.

FOD Economie mag, op elk moment, onverwacht een controle uitvoeren bij een geregistreerde certificatiedienstverlener. Deze controles worden in het bijzonder uitgevoerd na een klacht of een vermoeden van afwijking van de eisen in de wet. De controles hebben een wettelijke grondslag in een Koninklijk Besluit [7, artikel 7]. In Nederland heeft de Opta deze mogelijkheid ook krachtens de Telecommunicatiewet (artikel 15 en 18.7).

De Belgische Wet op de Elektronisch Handtekeningen verwijst direct naar de EU Richtlijn voor normen waaraan 'veilige middelen' en 'betrouwbare systemen' moeten voldoen [6, artikel 6] zonder ze zelf in wetten of regelingen vast te leggen. Dit is anders dan in Nederland waar in de Regeling Elektronische Handtekeningen expliciet normen zijn opgenomen. Voor wat dit betreft is de Belgische Wet eenvoudiger te beheren en automatisch afgestemd op Europese keuzes voor normen. Hiermee is in België besloten om geen standaarden te adopteren die Europese keuzes aanvullen of vervangen.

Volgens [7, artikel 4.4] verleent FOD Economie een registratie wanneer alle elementen in het initiële auditverslag positief zijn. Over hoe dient te worden omgegaan met afwijkingen van de norm geconstateerd door auditors is in Nederland niets in wet- of regelgeving vastgelegd. De Opta heeft volgens de Telecomwet (artikel 2.2) wel de mogelijkheid om de registratie van certificatiedienstverleners te beëindigen bij gerede verdenking dat ze niet conform de wet opereren. Over hoe concreet moet worden omgegaan met afwijkingen die auditors constateren zijn regels opgenomen in het TTP.NL schema. Daarbij is het afgeven van conformiteitsverklaring terwijl kleine afwijkingen nog niet zijn opgelost toegestaan.

Volgens [7, artikel 4.8] moeten significante wijzigingen in het systeem of beheer door certificatiedienstverleners worden gemeld bij FOD Economie.

In België zijn bij FOD Economie per 1 januari 2012 drie vertrouwensknooppunten geregistreerd die allen worden beheerd door één commerciële organisatie (Certipost). Twee van deze vertrouwensknooppunten betreffen de Belgische overheid maar geven zelf geen certificaten uit aan afnemers (het gaat om de Belgische 'nationale root'). De derde betreft commerciële gekwalificeerde certificaten van Certipost. Er zijn voor zover bekend geen andere leveranciers van gekwalificeerde certificaten in België. Dit betekent dat er geen certificatiedienstverleners zijn die gekwalificeerde certificaten uitgeven zonder geregistreerd te zijn bij de Belgische toezichthouder. Dat is in Nederland ook het geval. Voor België geldt, in tegenstelling tot Nederland, dat er op het gebied van gekwalificeerde certificaten in de praktijk geen markt is met meerdere aanbieders waaruit kan worden gekozen.

6.1.2 Duitsland

In Duitsland wordt de wettelijke basis voor gekwalificeerde certificaten geregeld in de 'Signaturgesetz' [9] en bijbehorende regeling [8]. Dit vormt de Duitse implementatie van de Europese Richtlijn. Voorafgaand aan deze wet had Duitsland vanaf 1997 een wet die de elektronische handtekeningen regelde. Deze was gebaseerd op verplichte accreditatie. In 1999 werd de Europese Richtlijn van kracht en die verbood verplichte accreditatie. Toen is de verplichte route vrijwillig geworden. Op dit moment heeft Duitsland een schema voor vrijwillige accreditatie en een schema zonder accreditatie. In de praktijk kiezen certificatiedienstverleners voor 'vrijwillige accreditatie' omdat hun klanten dat vragen. In lijn met de Europese Richtlijn is de wettelijke status dezelfde. Momenteel zijn er 7 certificatiedienstverleners geregistreerd via de 'vrijwillige accreditatie' route (inclusief 2 onder de Duitse overheid), en 2 zijn geregistreerd via 'directe registratie'.

De Minister van Economische zaken is verantwoordelijk voor de wettelijke en strategische aspecten. Hij stuurt de Bundesnetzagentur aan, die op het tactische niveau de uitvoering van het stelsel coördineert. De Bundesnetzagentur is als uitvoeringsorganisatie van de overheid, eigenaar van het schema voor vrijwillige accreditatie en is de auteur van het schema waartegen certificatiedienstverleners gecertificeerd worden. De Bundesnetzagentur heeft het mandaat om in te grijpen: wanneer ze het nodig acht, kan ze certificatiedienstverleners bezoeken en alle informatie opvragen.

Bij een certificatiedienstverlener onder dit schema voor vrijwillige accreditatie, worden zowel de certificatieprocessen geaudit als de 'betrouwbare systemen' die deze processen ondersteunen. Dit laatste betreft een productaudit. Private auditors voeren deze evaluaties uit. De auditrapporten worden door Bundesnetzagentur gereviewd. Beide audits zijn een voorwaarde voor Bundesnetzagentur om een certificatiedienstverlener te registreren voor het verstrekken van gekwalificeerde certificaten. De Bundesnetzagentur is verantwoordelijk voor de accreditatie van procesauditors en van productauditors. De accreditatie wordt in de uitgevoerd door het agentschap voor informatiebeveiliging van de Rijksoverheid: Bundesambt für Sicherheid in der Informationstechnik (BSI).

De audits zijn voor rekening van de certificatiedienstverlener en de opdrachten worden door hen zelf gegeven. Een bedrag ter grootte van 250.000 euro is wettelijk vereist als een risicodekking bij de registratie.

In tegenstelling tot Nederland is er in Duitsland één nationaal vertrouwensknooppunt waar alle gekwalificeerde certificaten onder vallen. Hiermee wordt de interoperabiliteit geborgd en is er internationaal een eenvoudiger netwerk mogelijk, omdat ieder land maar één aanspreekpunt hoeft te hebben. In de praktijk is er hierdoor één nationale PKIoverheid voor gekwalificeerde certificaten, waar marktpartijen aan kunnen deelnemen.

6.2 PKI stelsels van de Overheid

6.2.1 België

In België worden onder regie van de overheid persoonsgebonden gekwalificeerde certificaten en ook certificaten voor systemen en overheidsdiensten uitgegeven. Ditzelfde geldt voor PKIoverheid in Nederland. De Belgische overheid zorgt bovendien ook voor software-integriteitscertificaten (zogenoemde 'code signing' certificaten) die in Nederland niet onder PKIoverheid vallen.

In België ligt de verantwoordelijkheid voor beleid en het strategisch beheer van de nationale PKI, evenals in Nederland, bij de Rijksoverheid. In België is dit belegd bij het Rijksregister en bij FedICT, een agentschap van de Rijksoverheid dat zich bezig houdt met overheidsbrede ICT. Terwijl in Nederland marktwerking binnen PKIoverheid is gecreëerd door commerciële certificatiedienstverleners de mogelijkheid te geven onder de regels van PKIoverheid hun diensten aan te bieden, is in België de PKI operationeel uitbesteed, maar volledig onder regie van de overheid gebleven. Binnen de Belgische overheidsPKI is dus geen sprake van marktwerking. Een commercieel bedrijf (Certipost) voert het tactisch en operationeel beheer uit terwijl FedICT en het Rijksregister de strategie en het beleid bepalen. Het ontbreken van marktwerking binnen de Belgische overheidsPKI ontneemt eventueel geïnteresseerde certificatiedienstverleners de mogelijkheid om de overheidsmarkt te veroveren. Zij kunnen alleen meedoen met de periodieke overheidsaanbesteding van certificatiedienstverlening. Dit maakt het voor certificatiedienstverleners ook moeilijker om een economisch rendabele bedrijfsvoering buiten de overheid te realiseren. Dit wordt geïllustreerd door het feit dat in België in de praktijk slechts één certificatiedienstverlener de markt domineert. In de Belgische situatie kan de overheid echter wel veel directer afspraken maken en toezicht houden op de activiteiten van de dienstverlener die via een overheidsaanbesteding werd gekozen.

Het risico dat een certificatiedienstverlener wordt gecompromitteerd (zoals DigiNotar overkwam) is nooit uit te sluiten, ook niet in België. Wanneer door de overheid volledig op één certificatiedienstverlener wordt gerust dienen vanwege de gevolgen van een eventueel incident meer preventieve maatregelen te worden getroffen. In het geval van een incident kan er immers niet direct naar andere leveranciers worden uitgeweken.

In België en Nederland zijn verschillende keuzes gemaakt ten aanzien van de manier waarop individuele gebruikers via de nationale PKI vertrouwen kunnen krijgen in bijvoorbeeld de identiteit van een systeem zoals een website. In België is er voor gekozen om dit te regelen via een commerciële leverancier (GlobalSign) terwijl in Nederland hiervoor wordt gerust op een vertrouwensknooppunt ('de root': De Staat der Nederlanden CA) dat eigendom is van de overheid.

Een belangrijk deel van de nationale PKI in België is opgezet ten bate van de Belgische eNIK. In tegenstelling tot Nederland kent België al geruime tijd een elektronische Nationale Identiteits Kaart (eNIK) waarop gekwalificeerde certificaten ten behoeve van het zetten van

gekwalificeerde handtekeningen zijn opgenomen. In België is daarmee een deel van de nationale PKI ontwikkeld dat in Nederland nog zal moeten worden ontwikkeld wanneer een vergelijkbare eNIK wordt geïntroduceerd. Het belang van de nationale PKI zou in Nederland dus nog significant kunnen toenemen, daar waar België deze groei al achter de rug heeft.

6.2.2 Duitsland

In Duitsland is er geen overlap tussen de stelsels voor de gekwalificeerde certificaten en de Duitse elektronische Nationale Identiteits Kaart: de Federal Identity Card (FIC). Voor de implementatie van deze kaart zijn 5 verschillende PKI's geïmplementeerd die vergelijkbaar zijn met die voor elektronische paspoorten: het gaat dan bijvoorbeeld om ondertekening van het identiteitsdocument, verificatie van het identiteitsdocument, toegang tot biometrische functies en de communicatie tussen de FIC en de Duitse Staatsdrukkerij. Deze PKI's zijn praktisch volledig onder controle van de overheid.

In tegenstelling tot in Nederland is er in Duitsland geen overlap tussen de PKI stelsels van de overheid en die van de gekwalificeerde certificaten. Er vallen geen gekwalificeerde certificaten onder de Duitse overheidsPKI. Het onderscheid tussen de domeinen van de nationale identiteitskaart voor de burgers enerzijds en die van een gekwalificeerde handtekeningen anderzijds, is organisatorisch, functioneel en technisch grondig doorgevoerd. De functionaliteit voor de gekwalificeerde handtekening die op de 'Duitse eNIK' staat, valt onder verantwoordelijkheid van het Duitse ministerie van economische zaken, terwijl de rest van de kaart onder verantwoordelijkheid valt van de Minister van Binnenlandse Zaken.

6.3 Overige alternatieven

6.3.1 Context

Bij DigiNotar zijn kwetsbaarheden van de traditionele PKI aan het licht gekomen. In deze paragraaf worden deze knelpunten kort geschetst en de aangedragen alternatieven besproken. We illustreren de knelpunten aan de hand van een voorbeeld waarbij een persoon via zijn webbrowser winkelt bij een webwinkel. De webwinkel heeft een SSL-certificaat aangeschaft bij een certificatiedienstverlener. Overigens geldt de argumentatie voor PKI in het algemeen, niet alleen voor deze voorbeeldsituatie met SSL-certificaten die van een eigen merk of van PKIoverheid kunnen zijn. Ook voor gekwalificeerde certificaten zijn de beschreven knelpunten relevant.

PKI-stelsels zoals die algemeen in gebruik zijn, worden gekenmerkt door onder andere de onderstaande eigenschappen.

- De betrouwbaarheid wordt in belangrijke mate gecreëerd door knooppunten in de vertrouwensinfrastructuur die certificaten uitgeven en intrekken. In het voorbeeld is het een vertrouwensknooppunt beheerd door de certificatiedienstverlener die het SSL-certificaat aan de webwinkel verstrekt.

- Een of meerdere vertrouwensknooppunten worden beheerd door certificatiedienstverleners. Dit kunnen commerciële partijen zijn, of onderdelen van overheden of bedrijven die ze gebruiken om eigen communicatie te beveiligen. In het voorbeeld kan de leverancier van het SSL-certificaat ook, middels andere vertrouwensknooppunten, andere soorten certificaten uitgeven (zoals persoonsgebonden certificaten).

- Vertrouwensknooppunten kunnen zelfstandig bestaan, maar zijn veelal ondergebracht in boomstructuren (hiërarchieën) waardoor de vertrouwensketen zich over organisatiegrenzen heen uitstrekt. In het voorbeeld kan het vertrouwensknooppunt wat het SSL-certificaat produceert een operationele relatie hebben met een vertrouwensknooppunt van een andere leverancier.

- Certificaten worden voor verschillende doeleinden verstrekt. Het vertrouwen dat afnemers aan certificaten ontlenen verschilt sterk. Niet alle certificaten hoeven derhalve hetzelfde betrouwbaarheidsniveau te bieden.

Een operationele 'traditionele PKI' kent als gevolg van het bovenstaande de volgende beperkingen:

- Bij het wegvallen van vertrouwen in een vertrouwensknooppunt of een certificatiedienstverlener moeten alle afnemers van certificaten van dit knooppunt naar andere certificaten alvorens ze weer beveiligd elektronische informatie kunnen uitwisselen. In het voorbeeld zou de webwinkel zo snel mogelijk een SSL-certificaat van een andere certificatiedienstverlener willen krijgen.

- 'Vertrouwende partijen' kunnen in de praktijk niet zelf direct kiezen welke certificatiedienstverlener ze al dan niet vertrouwen wanneer ze niet zelf de afnemer van certificaten zijn. Ze kunnen dan slechts kiezen om de aangeboden beveiliging te gebruiken of de aangeboden dienst niet (beveiligd) af te nemen. In het voorbeeld is de persoon die wil winkelen bij de webwinkel de 'vertrouwende partij'. Deze kan niet kiezen bij welke certificatiedienstverlener de webwinkel haar SSL-certificaat moet afnemen.

- Bij gebruik van generieke PKI-software (zoals een webbrowser) voor generieke doeleinden, dienen alle certificatiedienstverleners die actief zijn op het internet a priori te worden vertrouwd om beveiligde elektronische communicatie op te kunnen zetten met een willekeurige persoon, systeem of dienst op het internet. In het voorbeeld geldt dat de webbrowser van de persoon die wil webwinkelen, wanneer deze op een standaard manier is ingesteld, een groot aantal certificatiedienstverleners vertrouwt. Dit is nodig omdat de (gebruiker van de) webbrowser niet van te voren weet welke certificatiedienstverlener het SSL-certificaat aan de webwinkel heeft verstrekt.

- De leveranciers van generieke PKI-software (zoals een webbrowser) spelen een nog rol in de mate waarin certificaten worden vertrouwd. Hierbij wordt niet alleen vertrouwd op

wat de dienstverlener zelf aangeeft (de gepubliceerde 'zwarte lijst' met certificaten), maar houden de browserleveranciers ook een 'zwarte lijst' met certificatiedienstverleners bij.

Deze knelpunten in 'traditionele PKI' hebben zich bij het DigiNotar incident gemanifesteerd. In deze paragraaf schetsen we kort een aantal benaderingen van PKI die pogen bovenstaande knelpunten weg te nemen. Ook deze benaderingen zijn vormen van PKI en rusten grotendeels op dezelfde technische standaarden, alleen ze gaan uit van wijzigingen in aspecten van het achterliggende vertrouwensmodel.

Public Key Infrastructuur is een verzamelnaam voor diverse afspraken, diensten en technologieën. Het omvat afspraken over de organisatie van de vertrouwensinfrastructuur en over de technische uitwerking in implementatiestandaarden. De Internet Engineering Task Force (IETF), die veel mondiale internet standaarden beheert, heeft de afgelopen 20 jaar diverse algemeen geaccepteerde standaarden gepubliceerd. Binnen en buiten de IETF zijn uitbreidingen van de oorspronkelijke PKI-concepten en implementatiestandaarden voorgesteld die functionele uitbreidingen mogelijk maakten. Sommige hiervan worden in de praktijk ook gebruikt. Er bestaat echter geen compleet alternatief systeem met dezelfde functionele eigenschappen als PKI.

Alternatieven die momenteel worden uitgewerkt en waarmee wordt geëxperimenteerd zijn deels ingegeven door de compromittering van certificatiedienstverleners als Comodo en DigiNotar. Ze richten zich doorgaans niet op PKI in de brede zin van het woord, maar op het gebruik van systeemcertificaten ten behoeve van SSL. We geven in de volgende paragrafen een beknopt overzicht van een aantal van deze alternatieve benaderingen.

Gebruikers die met een webbrowser veilig willen communiceren met een website op basis van PKI moeten vertrouwen stellen in het certificaat van de website en daarmee in de certificatiedienstverlener die een certificaat heeft verstrekt aan de eigenaar van de website. Bovendien moeten ze vertrouwen stellen in de integriteit van de browsersoftware en de lijst met derde partijen die in hun browser zijn geconfigureerd. Bij het installeren van een browser bestaat deze lijst tegenwoordig standaard uit een groot aantal certificatiedienstverleners. Bij Microsoft Internet Explorer gaat het bijvoorbeeld om meer dan 100 certificatiedienstverleners met meer dan 300 vertrouwensknooppunten. De gebruiker kan deze lijst verkleinen, maar dit heeft tot gevolg dat veilige communicatie met bepaalde websites niet meer mogelijk is. Met dit aantal certificatiedienstverleners kan niet worden verwacht dat al deze partijen in de praktijk hetzelfde betrouwbaarheidsniveau hebben. Ook kan niet worden uitgesloten dat wel eens een certificatiedienstverlener wordt gecompromitteerd.

6.3.2 Web of Trust - PGP

In de jaren 1990 is naast PKI gebaseerd op een stelsel van vertrouwde derde partijen ook een PKI-concept ontstaan waarbij gebruikers elkaar direct vertrouwen schenken zonder tussenkomst

van een derde. Dit concept wordt wel een ‘web of trust’ genoemd en is onder andere geïmplementeerd door de softwareleverancier PGP.

PGP wordt op het internet al vele jaren gebruikt voor het beveiligen van berichten tussen individuen die vooraf vertrouwen aan elkaar hebben geschonken doordat ze elkaar veelal persoonlijk kennen. Het fundamentele verschil met standaard PKI is de afwezigheid van certificatiedienstverleners in het PGP model. PGP is daarom niet geschikt voor het beveiligen van communicatie met een individu of systeem waaraan de gebruiker niet expliciet het vertrouwen heeft geschonken. Dit is de kracht van PGP, maar hierdoor is het PGP model, in tegenstelling tot ‘traditionele PKI’ met certificatiedienstverleners, beperkt schaalbaar. Het verifiëren van de identiteit van een website is ook binnen PGP niet zonder meer mogelijk.

6.3.3 DNS-Based Authentication of Named Entities (DANE)

Om het gebruik van unieke elektronische identiteiten op het internet mogelijk te maken is het ‘Domain Name System’ (DNS) in gebruik. Dit maakt het mogelijk om ongeacht de locatie van een gebruiker of van de te benaderen website aanduidingen als ‘www.overheid.nl’ of ‘www.DigiNotar.nl’ te hanteren. DNS is een mondiaal gedistribueerd systeem dat al decennia in gebruik is. Momenteel vindt een geleidelijke migratie plaats naar beter beveiligde onderlinge communicatie tussen elementen van dit systeem. Dit betreft de invoering van het zogenaamde DNSSEC protocol.

Het DANE initiatief is bedoeld om het mogelijk te maken DNSSEC te gebruiken bij het verifiëren van identiteiten van systemen op het internet. Momenteel vindt dit hoofdzakelijk met behulp van ‘traditionele PKI’ plaats. Het voordeel van DANE zou zijn dat het verifiëren van identiteiten beter wordt verankerd in de basis van het internet in plaats van de ‘traditionele PKI’. DANE gaat echter uit van een gedistribueerd systeem met vertrouwde derde partijen hetgeen als een van de risicofactoren van PKI wordt gezien. Daarbij hebben gebruikers in dit scenario minder keuzemogelijkheden ten aanzien het vertrouwen wat ze aan derde partijen schenken. Tenslotte is DANE niet bedoeld voor het brede toepassingsdomein van PKI (waaronder elektronische handtekeningen).

6.3.4 Convergence

Convergence is de naam van een in 2011 gelanceerde benadering van PKI die de gebruiker van een browser in staat stelt zelf te bepalen welke derde partijen op het internet hij vertrouwt. Bij de ‘traditionele PKI’ aanpak is het de website die aangeeft welke derde partij vertrouwd moet worden om een beveiligde verbinding op te kunnen zetten. Het voordeel van de convergence aanpak is dat de gebruiker zelf keuzes kan maken die binnen een ‘traditionele PKI’ benadering niet mogelijk zijn. Er zijn echter nog steeds vertrouwde partijen nodig. Dit kunnen ook andere partijen dan certificatiedienstverleners zijn, maar daarbij is nog niet duidelijk waaraan vertrouwen kan worden ontleend.

De doelstelling achter convergence is belangrijk: gebruikers nieuwe mogelijkheden in handen geven om vertrouwen op te kunnen baseren wanneer ze communiceren met websites. Echter de uitwerking is om verschillende redenen incompleet en onvolwassen. Ook is convergence geen alternatief voor PKI maar een alternatieve manier om PKI te gebruiken. Het aantal vertrouwde derde partijen hoeft daarbij niet kleiner te worden, maar ze veranderen wel van aard. Tenslotte is convergence primair bedoeld voor een situatie waarin een gebruiker via een browser een website benaderd, terwijl PKI een veel breder toepassingsgebied kent.

6.3.5 Samenvatting

Terwijl het gebruik van PKI de afgelopen 20 jaar een enorme vlucht heeft genomen zijn alternatieven en uitbreidingen voor delen van de algemeen geaccepteerde PKI-standaarden onderzocht. Dit heeft echter niet geleid tot een fundamentele herziening van PKI concepten. PKI wordt momenteel op zo'n grote schaal gebruikt dat, als er al een algemeen geaccepteerd gelijkwaardig alternatief zou bestaan, migratie van de huidige 'traditionele' PKI waarschijnlijk lange tijd in beslag zou nemen.

De alternatieven benaderingen genoemd in paragraaf 6.3.3 en 6.3.4 zijn nog in een onderzoeksfase en kennen geen grootschalige implementaties. Het alternatief genoemd in paragraaf 6.3.2 al geruime tijd in gebruik. Theoretisch en praktisch is aangetoond dat dit concept in sommige specifieke situaties voldoet, maar in het algemeen onvoldoende schaalbaar is om 'traditionele PKI' op het internet te vervangen.

Elk van de genoemde alternatieven zijn bedoeld om verbeteringen aan te brengen in aspecten van het vertrouwensmodel van PKI en niet om PKI als zodanig door een nieuw paradigma te vervangen. In essentie is vertrouwen ook subjectief: afhankelijk van je gezichtspunten, persoonlijke ervaringen en overtuigingen. Het laat zich niet voor iedereen in hetzelfde model vangen.

7 CONCLUSIES

In dit hoofdstuk trekken we conclusies op basis van de analyse uit de hoofdstukken 4, 5 en 6. Dit hoofdstuk is zelfstandig leesbaar door diegenen die redelijk zijn ingevoerd in de materie.

7.1 DigiNotar

7.1.1 Consequenties

De DigiNotar affaire heeft in binnen- en buitenland veel stof doen opwaaien bij zowel specialisten als beleidsmakers. De compromittering van de beveiliging van DigiNotar was voor menigeen een verassing, met name omdat DigiNotar juist een bedrijf was dat als 'vertrouwde derde partij' geacht werd al het nodige te doen om hackers buiten de deur te houden. Het DigiNotar incident groeide uit tot een nationale crisis toen bleek dat de certificatiedienst-verlening van DigiNotar essentieel was voor een aantal primaire processen van overheden en vitale sectoren. De (veelal Amerikaanse) browserleveranciers konden DigiNotar certificaten ongeldig verklaren. Hierdoor zouden websites van de overheid en van het bedrijfsleven niet meer goed functioneren. Vanwege de consequenties hiervan voor elektronische communicatie met de overheid heeft de Minister van BZK toen ingegrepen om de gevolgen van deze situatie te verkleinen. In de crisissituatie die toen is uitgeroepen is een snelle en beheerste afbouw van het gebruik van DigiNotar certificaten gerealiseerd.

7.1.2 Primaire oorzaak

De primaire verantwoordelijkheid voor een deugdelijke informatiebeveiliging ligt bij het management van de certificatiedienstverlener. Van eindverantwoordelijken voor een bedrijf dat haar bestaansrecht ontleent aan het leveren van diensten op het gebied van vertrouwens-infrastructuur mag worden verwacht dat informatiebeveiliging een topprioriteit krijgt. Het feit dat het DigiNotar incident niet is gemeld bij Logius of bij de auditor, terwijl daartoe wel een verplichting bestond, geeft aan dat het management van DigiNotar in gebreke is gebleven. Bovendien zijn bij het technisch forensisch onderzoek dat door Fox-IT is uitgevoerd, zaken aan het licht gekomen die zij typeren als strijdig met algemeen gebruikelijke maatregelen in de IT-beveiligingswereld. Het management heeft zich onvoldoende rekenschap heeft gegeven van de verantwoordelijkheid die men in de PKI-stelsels droeg. Interne controle maatregelen en interne audits bij DigiNotar hebben de tekortkomingen niet kunnen voorkomen.

7.1.3 Eerstelijns controle

Het beoordelen van alle technische beveiligingsmaatregelen in het kader van certificatie-dienstverlening is niet expliciet voorgeschreven. De auditors beoordelen wel steekproefsgewijs technische beveiligingsmaatregelen. Dit wordt door de auditors verstandig geacht om de gevraagde zekerheid rond de implementatie van het management systeem te beoordelen. Als

een achteraf gebleken kwetsbaarheid door auditors niet gerapporteerd wordt, kan dat betekenen dat zij deze niet hebben gecontroleerd, of dat zij deze wel hebben gecontroleerd maar dat ze geen afwijkingen hebben gevonden. Op basis van de auditrapporten is dit onderscheid niet te maken. De auditrapporten bevatten slechts afwijkingen van normen en geen beschrijvingen van uitgevoerde tests of van conformiteiten. Bovendien wordt door auditors een conformiteitsverklaring voor de komende drie jaar afgegeven. Tussentijds wordt jaarlijks een beperkte inspectie-audit uitgevoerd. Aangezien deze audits niet over het verleden gaan maar betrekking hebben op de toekomst, is slechts beperkte zekerheid te geven. Er bestaat een kloof tussen de verwachting van de afgegeven zekerheid en deze zekerheid die daadwerkelijk door de auditors geboden wordt.

Er vindt in het kader van eerstelijns controle geen continue en intensieve monitoring plaats. Er is nooit volledige zekerheid dat beveiligingsincidenten niet kunnen plaatsvinden. Echter, wanneer het eerstelijns controle zowel een IT-audit als technische testen en –monitoring omvat, neemt de kans op kwetsbaarheden, zoals die door Fox-IT bij DigiNotar zijn geconstateerd, af.

7.1.4 Tweedelijns toezicht

De compromittering van DigiNotar heeft plaatsgevonden ten aanzien van commercieel uitgegeven certificaten die buiten de beide onderzochte stelsels vallen. Toen door Fox-IT werd geconstateerd dat niet kon worden uitgesloten dat ook de productie van gekwalificeerde certificaten van PKIoverheid was gecompromitteerd, hebben zowel de Opta (als toezichthouder op certificatiedienstverleners die gekwalificeerde certificaten uitgeven) als Logius (als Policy Autoriteit van het PKIoverheidstelsel) geacteerd. Logius is geen toezichthouder met publiek rechtelijke grondslag, maar in de praktijk kunnen zowel Opta als Logius worden beschouwd als tweedelijns toezichthouders op certificatiedienstverleners.

De Opta heeft, na de rapporten van de laatste certificeringsaudit te hebben opgevraagd, van de bevindingen van Fox-IT te hebben kennisgenomen, en DigiNotar om een zienswijze te hebben gevraagd, de registratie van DigiNotar beëindigd. Het is moeilijk voor de Opta om het werk van de auditor op waarde te schatten en de consistentie en geschiktheid van het normenkader kan niet goed worden beoordeeld. Bij het besluit tot intrekking van de registratie van DigiNotar is wel een uitgebreide motivatie gevoegd. Logius had de mogelijkheid om DigiNotar operationeel van PKIoverheid af te koppelen, maar heeft in overleg met het nationaal crisisteam besloten dat niet te doen om te voorkomen dat primaire processen van de overheid tot stilstand zouden komen. Logius heeft technische beveiligingstests en zelfevaluaties laten uitvoeren bij de overige aangesloten certificatiedienstverleners om vast te stellen of hackers daar ook zouden kunnen binnendringen.

Logius heeft nauwer contact gehouden met de certificatiedienstverleners dan de Opta, onder andere door het organiseren van periodieke bijeenkomsten (het ‘CSP overleg’) waarin aanpassingen van het Programma van Eisen worden besproken. Zij zijn daar gezien hun rol en het karakter van hun werkzaamheden beter voor toegerust dan de Opta. Certificatie-

dienstverleners geven aan dat Logius suggesties en signalen uit de praktijk wel serieuzer zou kunnen oppakken.

7.2 Organisatie

7.2.1 Overlap tussen stelsels

De beide stelsels overlappen elkaar voor wat betreft de gekwalificeerde certificaten. Alle certificatiedienstverleners die bij de Opta zijn geregistreerd, maken ook deel uit van het stelsel PKIoverheid. De Opta en Logius hebben beide een vorm van zeggenschap over gekwalificeerde certificaten. Gekwalificeerde certificaten onder het PKIoverheidstelsel voldoen aan extra eisen bovenop gekwalificeerde certificaten buiten het PKIoverheidstelsel. Er bestaan in Nederland in de praktijk gekwalificeerde certificaten met twee verschillende betrouwbaarheidsniveaus en twee verantwoordelijke instanties, waarvan er één een toezichthouder met wettelijke grondslag is. De Europese Richtlijn heeft met de introductie van het begrip 'gekwalificeerde certificaten' één betrouwbaarheidsniveau voor certificaten in de Europese Unie willen bewerkstelligen.

In Duitsland zijn alle gekwalificeerde certificaten buiten de nationale overheids-PKI gehouden. Dit geldt ook voor optionele functionaliteit voor het zetten van elektronische handtekeningen middels de Duitse Nationale elektronische identiteitskaart.

Het feit dat zowel Logius als de Opta een vorm van zeggenschap hebben over certificatie-dienstverleners die gekwalificeerde certificaten onder PKIoverheid uitgeven compliceert de stelsels. PKIoverheid vereist ook een registratie bij de Opta en beide stelsels rusten op conformiteit met het TTP.NL schema. Er zijn echter geen afspraken tussen de beheerders van de stelsels die beschrijven wat er zou moeten gebeuren wanneer een certificatiedienstverlener uit een enkel stelsel wordt verwijderd. De onderlinge afhankelijkheden tussen de stelsels zijn niet operationeel uitgewerkt.

Wanneer beide stelsels in een overkoepelend stelsel zouden worden ondergebracht, zou dit het noodzakelijk maken om afhankelijkheden en overlap beter te organiseren. In zo'n overkoepelend stelsel zouden certificaten met verschillende betrouwbaarheidsniveaus kunnen bestaan.

7.2.2 Opta registratieroutes

Voor registratie van een certificatiedienstverlener bij de Opta bestaan twee routes. De ene route betreft zogenaamde 'directe registratie' waarbij de dienstverlener informatie aanlevert waaruit blijkt dat hij aan de wet voldoet. De manier waarop een aanvraag via deze route door de Opta wordt beoordeeld is niet bekend. Deze route is nog nooit bewandeld. De andere registratieroute is die van de 'vrijwillige accreditatie'. Hierbij wordt een certificatiedienstverlener door een door de Minister aangewezen en geaccrediteerde auditor op conformiteit met de ETSI-norm volgens het TTP.NL schema getoetst. De registratieaanvraag bij de Opta wordt dan vergezeld van een conformiteitsverklaring van de auditor.

De ‘vrijwillige accreditatie’ route bij de Opta wordt in de praktijk altijd gevolgd. Op deze manier zijn de kosten van het toezichtarrangement voor een certificatiedienstverlener relatief laag. Omdat verplichte certificatie vooraf niet is toegestaan volgens de Europese Richtlijn, zijn lidstaten genoodzaakt ook directe registratieroutes aan te bieden.

De feitelijke werking van de ’directe registratie’ route is onduidelijk en brengt dus onnodige onzekerheid met zich mee. Het verbod op conformiteitsbeoordelingen van certificatiedienst-verleners vooraf is in de EU Richtlijn opgenomen om te voorkomen dat lidstaten specifieke aanvullende eisen zouden stellen bovenop de wettelijke verplichtingen voor gekwalificeerde handtekeningen. Dit zou ongewenste belemmeringen voor elektronische handtekeningen in de Europese markt opwerpen doordat handtekeningen met verschillende betrouwbaarheidsniveaus zouden ontstaan. Het inrichten van een Europees certificeringsschema waardoor verschillen tussen lidstaten verdwijnen, zou dit verbod overbodig maken. Het verwijderen van dit verbod uit de Richtlijn zou wellicht ook op steun van andere lidstaten kunnen rekenen. Een vergelijkbare situatie doet zich namelijk voor in andere Europese landen waaronder Duitsland.

7.2.3 Opdrachtgeverschap audits

De auditor is, hoe professioneel ook, commercieel afhankelijk van de certificatiedienstverlener omdat deze zijn opdrachtgever is. De controle op de auditor wordt uitgevoerd door de Raad voor Accreditatie. Deze beoordeelt echter geen individuele audits maar de competentie, de onafhankelijkheid en de procesvoering van auditors over een periode. Aangezien de auditors uiteindelijk zekerheid bieden aan de Opta en aan Logius valt te overwegen om deze als opdrachtgever te laten fungeren. Ze kunnen dan directer invloed uitoefenen op de aandachtspunten, de timing en de diepgang van een audit. Wanneer de toezichthouder opdrachtgever zou zijn richting de auditors, heeft dat als voordeel dat er directer gestuurd kan worden op zaken die het stelsel versterken. Directere grip op de eerstelijns controle kan zorgen voor een alertere, beter geïnformeerde en meer betrokken toezichthouder. Bovendien kan de toezichthouder door wisselende allocatie van auditopdrachten, auditors scherp houden. Wanneer niet gekozen wordt voor direct opdrachtgeverschap door de toezichthouder, kan ook worden overwogen een tussenvorm te adopteren in lijn met de Europese conceptnorm op dit gebied die in ontwikkeling is [47].

Een aandachtspunt is dat de Opta en Logius financieel in staat zouden moeten worden gesteld om dit opdrachtgeverschap in te vullen. Een ander aandachtspunt is dat combineren van de audits ten behoeve van beide stelsels anders georganiseerd zou moeten worden. Bovendien dienen de toezichthouders dan te worden toegerust om hun rol als opdrachtgever professioneel te kunnen invullen.

Met het veranderen van het opdrachtgeverschap richting de auditors zou de rol van de overheid in de stelsels toenemen. Dat vergt een beleidsmatige afweging of de taken, verantwoordelijk-heden en bevoegdheden aangepast kunnen worden ten gunste van overheidstoezicht en ten koste van de oorspronkelijke opzet.

7.2.4 Doelbinding TTP.NL schema

Het TTP.NL schema vormt de basis voor certificatiedienstverleners in beide stelsels. Het schema en de beheerder ervan zijn door de Raad voor Accreditatie formeel 'geaccepteerd'. De Raad beoordeelt of een schema toetsbaar is, voldoende draagvlak heeft en of het een beheerder kent. Of het schema dekkend is voor wat een gebruiker beoogt, beoordeelt de Raad niet.

In het geval van TTP.NL zou het voor de hand liggen dat het College van Belanghebbenden TTP.NL waarborgt dat het schema invulling geeft aan privaatrechtelijke en wettelijke eisen voor de elektronische handtekening. In haar rol als eindverantwoordelijke voor de Wet op de Elektronische Handtekening mag van het ministerie van EL&I verwacht worden dat ze beoordeelt of het middel (waar onder TTP.NL certificering) tegemoet komt aan haar doel (toetsbaar maken van wettelijke eisen). Voor zover bekend hebben zowel het College van Belanghebbenden als het ministerie nooit een expliciete beoordeling van het schema gedaan in het licht van de Wet op de Elektronische Handtekening.

Conformiteitsverklaringen van geaccrediteerde auditors geven geen directe zekerheid over conformiteit betreffende wet- en regelgeving. Ze bevatten een verwijzing naar een enkele ETSI-norm en soms een verwijzing naar het TTP.NL schema. Ook de onderliggende auditrapporten bevatten niet altijd eenduidige verwijzing naar de betreffende wet- en regelgeving.

7.3 Toezicht

7.3.1 De rol van risicoanalyse

Certificatiedienstverleners dienen volgens de Europese normen over een actuele risicoanalyse te beschikken die richting geeft aan hoe ze risico's beheersen. Deze risicoanalyse is in de praktijk niet altijd actueel, specifiek en gekoppeld aan concrete maatregelen. De auditors valideren de risicoanalyse op basis van hun professionele bagage. De mate waarin de risicoanalyse leidend is voor de prioriteit, diepgang of de methode van de door de auditors uitgevoerde testen is onzeker.

Dreigingen veranderen snel. Wanneer risicoanalyse meer aandacht krijgt in de aanpak van certificatiedienstverleners, dan wordt zichtbaar welke risico's door het management worden onderkend en of passende risicobeperkende maatregelen zijn genomen. Indien de risicoanalyse niet een losse eis is in het normenstelsel, maar een verplicht uitgangspunt, worden door de implementatie ervan maatregelen genomen die corresponderen met feitelijke dreigingen. Wanneer de auditor actief toe gaat zien op de werking van de risicoanalyse in de daadwerkelijke besluitvorming, dan wordt de kans dat de certificatiedienstverlener ineffectieve maatregelen treft daardoor verkleind. De kwaliteit van de risicoanalyse kan gewaarborgd worden door deze inhoudelijk door de auditors te laten toetsen tegen algemeen aanvaarde methoden en dreigingsprofielen.

De maatschappelijke risico's van deze bedrijfstak is door recente incidenten duidelijk geworden. Risicobeheersende maatregelen zijn op dit stelseloverkoepelende niveau niet georganiseerd. Risicobeheersing binnen de stelsels kan verbeterd worden, risicobeheersing over de stelsels heen kan voorkomen dat elk incident met maatschappelijke impact een crisis wordt.

7.3.2 Concreetheid van het toezicht

De management systeem audits zoals bedoeld door de Raad voor Accreditatie, die binnen de stelsels momenteel worden uitgevoerd, bieden onvoldoende zekerheid ten aanzien van de betrouwbaarheid van certificatiedienstverleners die een belangrijke schakel vormen binnen vitale sectoren. De IT-audit die een certificatiedienstverlener op haar systemen conform het TTP.NL schema moet uitvoeren, is geen onderdeel van de management systeem audit die een geaccrediteerde auditor uitvoert. Indien deze IT-audit wel onderdeel wordt van de conformiteitsvaststelling, dan wordt het toezicht concreter. Wanneer de geregistreerde certificatiedienstverleners de verplichting zouden hebben (dreigende) incidenten bij de Opta te melden, zou door de Opta directer kunnen worden ingegrepen.

Penetratietesten vormen geen verplicht onderdeel van het toezichtsarrangement. Het periodiek laten uitvoeren van penetratietesten verkleint de kans dat technische kwetsbaarheden onopgemerkt blijven. Voor certificatiedienstverleners waarvoor het gezien hun rol in vitale sectoren nodig is om het toezichtarrangement verder aan te scherpen, kan frequente operationele rapportage aan de toezichthouder worden ingevoerd. Zulke systeemrapportage kan automatisch worden gegenereerd door betrouwbare systemen en indicatoren voor dreigende incidenten bevatten.

De toezichthouder kan het monitoren en beoordelen van deze rapportage desgewenst uitbesteden aan het Nationaal Cyber Security Centre (NCSC). Het NCSC zou in opdracht van de toezichthouder ook zelfstandig operationele monitoring kunnen uitvoeren. De toezichthouder dient in dit geval te worden toegerust om deze signalen ook daadkrachtig te kunnen afhandelen. Bovendien dient de eindverantwoordelijkheid voor toezicht bij één partij te blijven om ambiguïteit in verantwoordelijkheden te voorkomen.

7.3.3 Handhaving door toezichthouders

De auditrapporten worden door de wettelijk toezichthouder (Opta) eens per jaar opgevraagd waardoor er niet proactief kan worden ingegrepen mocht een auditrapport daar aanleiding toe geven. Wanneer de wettelijk toezichthouder zou zijn ingericht om intensiever en meer proactief toezicht te houden op certificatiedienstverleners, dan zou zij directer kunnen reageren op signalen van dreigingen. Een actieve rol van de toezichthouder past bij de toegenomen maatschappelijke gevolgen van beveiligingsincidenten in de digitale wereld.

Tot voor de DigiNotar affaire is door de wettelijk toezichthouder nog nooit een registratie van een certificatiedienstverlener beëindigd noch een boete opgelegd. Dit is voordien nooit nodig

geweest, maar dit brengt met zich mee dat de preventieve werking van repressieve handhaving in de praktijk minimaal is. Het elimineren van een certificatiedienstverlener uit de stelsels als ultieme enige en sanctie, heeft consequenties die de toezichthouder in het algemeen zal willen vermijden. Sancties zoals boetes zouden een onderdeel van het uitgebreide toezichts-arrangement kunnen vormen.

7.4 Normen

7.4.1 Onderlinge afhankelijkheden normensets

Normen waaraan certificatiedienstverleners dienen te voldoen worden beheerd door sterk van elkaar verschillende organisaties. Afhankelijk van het type certificaten hebben certificatie-dienstverleners te voldoen aan normen van Europese standaardisatieorganisaties (gekwalificeerde certificaten, [42, 44, 45]), aan aanvullende normen van PKIoverheid (certificaten onder PKIoverheid, [17]) en aan eisen van mondiaal opererende software-leveranciers (SSL en EV SSL-certificaten, [59, 60]). Er zijn bovendien onderlinge afhankelijk-heden en duplicaties tussen de normenstelsels. Het Programma van Eisen PKIoverheid [17] stelt voor gekwalificeerde certificaten onder andere conformiteit aan TTP.NL verplicht. TTP.NL vereist conformiteit aan de Europese norm [42]. Naast deze indirecte verwijzing, verwijst PKIoverheid ook expliciet naar de Europese norm en geeft er daarnaast op onderdelen ook concretere invulling aan. Sommige elementen van de norm zijn ook direct in het Programma van Eisen PKIoverheid overgenomen. Het normenstelsel waar certificatiedienstverleners die gekwalificeerde certificaten uitgeven aan moeten voldoen is complex (zie Bijlage D voor details). Dit komt de transparantie en eenduidigheid in de toepassing van de normenkaders niet ten goede terwijl dat essentieel is voor de verstrekte zekerheid en het daarop gebaseerde vertrouwen. Een aantal vereenvoudigingen zouden de normenstelsels eenduidiger en transparanter maken. Dit kan bijvoorbeeld door het vervangen van indirecte verwijzingen door directe verwijzingen (zoals tussen de norm voor ‘betrouwbare systemen’ [49] en de Wet, of tussen de norm voor accreditatie van certificerende instellingen [57] en de Wet).

7.4.2 Concreetheid informatiebeveiliging

Ruimte in de normenstelsels bestaat ook doordat de normen niet op alle punten even concreet zijn uitgewerkt. Dit geldt in het bijzonder voor het aspect informatiebeveiliging. In de centrale norm voor wat betreft eisen aan certificatiedienstverleners die gekwalificeerde certificaten uitgeven [42] worden een aantal controledoelstellingen op het gebied van informatiebeveiliging gespecificeerd. Deze controledoelstellingen zijn overgenomen uit een voorloper van de ISO 27001 standaard en daarom niet meer actueel. Dit kan worden opgelost door het verwijderen van deze controledoelstellingen uit de ETSI-norm en desgewenst naar de ISO 27001 standaard te verwijzen.

De ISO 27001 standaard is echter ook voor meerdere interpretaties vatbaar en minder concreet dan de meeste procescontroles in de ETSI-norm. De ISO 27001 standaard wordt in de stelsels ook niet aangevuld met meer concrete eisen aan informatiebeveiliging. De consequentie is dat de certificatiedienstverleners veel ruimte hebben ten aanzien van de invulling van beveiligingsmaatregelen en dat de auditors hun eigen interpretaties aan de norm geven om te kunnen toetsen. De ISO 27001 standaard biedt een bruikbaar algemeen raamwerk voor informatiebeveiliging, maar is onvoldoende toegesneden op de specifieke kenmerken van certificatiedienstverleners.

Het is aan te bevelen om het normenkader op een aantal punten aan te vullen met meer concrete eisen op het gebied van informatiebeveiliging. Met betrekking tot informatiebeveiliging zou beter vanuit wet- en regelgeving kunnen worden verwezen naar een internationaal gerespecteerde norm zoals ISO 27001 waar vergelijkbare, maar actuele, controledoelstellingen in zijn opgenomen. Deze norm is niet concreet en specifiek genoeg om minimale beveiligingsmaatregelen voor certificatiedienstverleners te specificeren. Analoog met de Nederlandse de norm voor informatiebeveiliging in de zorg (NEN 7510), die is uitgewerkt in toetsbare voorschriften, zou een specifiek op certificatiedienstverleners toegesneden norm als concretisering van de ISO 27001 standaard kunnen worden ontwikkeld.

7.4.3 Dynamiek dreigingen en beheer stelsels

Dreigingen op het internet veranderen snel. Nieuwe technologieën komen beschikbaar, nieuwe categorieën van aanvallers worden actief en de toegankelijkheid van internet in opkomende landen en via nieuwe apparaten neemt razendsnel toe. Dit snel veranderende dreigingsbeeld contrasteert met de wijze waarop de normen worden beheerd en met de wijze waarop toezicht op certificatiedienstverleners wordt uitgeoefend. Om de ‘wapenwedloop’ ten aanzien van certificaten niet in het voordeel van aanvallers te doen uitvallen, is het frequent evalueren van normen in het kader van actuele dreigingsbeelden benodigd. Het opstellen en beheren van een gemeenschappelijk actueel dreigingsbeeld zou bijvoorbeeld in het College van Belanghebbenden van het TTP.NL schema geagendeerd kunnen worden. Alle belanghebbenden zijn verplicht om alle relevante marktontwikkelingen in te brengen in het College van Belanghebbenden TTP.NL. Het dynamisch veranderende dreigingsbeeld is binnen het College de afgelopen jaren niet bediscussieerd.

7.4.4 Verbreding EU Richtlijn

De EU Richtlijn voor Elektronische Handtekeningen is ontstaan met het oogmerk om elektronische handel en elektronische overheidsdiensten te stimuleren. De verwachting ten tijde van de invoering van de Richtlijn was dat de elektronische handtekening dit zou bewerkstelligen. De omvang van de markt voor gekwalificeerde certificaten is achter gebleven bij deze verwachtingen. Op dit moment is er een toenemende behoefte aan betrouwbare

elektronische authenticatie. Certificaten worden in de praktijk veelvuldig gebruikt om sterke authenticatie te realiseren. In Europees verband is dit niet geregeld.

Het verbreden van de Europese Richtlijn voor elektronische handtekeningen zodat ook authenticatie er onder komt te vallen, zorgt voor een bredere wettelijke grondslag voor certificatiediensten en het bijbehorend toezicht. Dit zou naar verwachting zorgen voor meer zekerheid ten aanzien van de beveiliging van elektronische dienstverlening in Europa. Daarmee wordt beter voldaan aan de oorspronkelijke doelstellingen van de Richtlijn. Een bijkomend aspect is dat een andere doelstelling van de EU Richtlijn, het bevorderen van marktwerking tussen certificatiedienstverleners, bij een grotere omvang van de markt beter tot stand kan komen.

7.5 De rol van de markt

7.5.1 Aantal certificatiedienstverleners

In Nederland zijn op 1 januari 2012 zes certificatiedienstverleners door de Opta geregistreerd waarvan twee overheidsinstanties. Dit zijn dezelfde dienstverleners die certificatiediensten leveren onder PKIoverheid. De vier commerciële dienstverleners kennen onderling aanzienlijke verschillen voor wat betreft schaalgrootte, breedte van het certificatiedienstenpakket, en de core business van het bedrijf. Certificatiedienstverleners maken gebruik van derde partijen voor het leveren van hun diensten. Deze relaties bestaan ook tussen de zes certificatie-dienstverleners binnen de stelsels. Er is dus marktwerking tussen de certificatiedienstverleners binnen de stelsels maar deze is beperkt. Wanneer een certificatiedienstverlener zich terugtrekt kan deze beperkte marktwerking worden verstoord.

7.5.2 Nationale oriëntatie

Zoals aangegeven in paragraaf 7.4.4 is de omvang van de nationale markten voor gekwalificeerde certificaten achtergebleven bij verwachtingen die bestonden ten tijde van de introductie van de Europese Richtlijn op de elektronische handtekeningen. Voor certificatiedienstverleners is het bedrijfseconomisch wenselijk om diensten supranationaal aan te kunnen bieden. Hiervoor bestaan echter belemmeringen. De stelsels in de lidstaten zijn namelijk primair nationaal georiënteerd. Er bestaan significante verschillen tussen lidstaten ten aanzien van wet- en regelgeving, de gehanteerde standaarden en in het toezichtsarrangement.

De consequentie van deze nationale oriëntatie is dat de marktwerking voor certificatiediensten in Europa beperkt blijft. Bovendien is niet zeker of de betrouwbaarheid van certificaten afkomstig uit verschillende landen gelijk is. Wanneer op termijn de normenstelsels binnen Europa zouden worden geharmoniseerd, er één Europees (TTP.eu) schema zou bestaan, en er slechts één Europese toezichthouder zou worden aangewezen, dan zou gemakkelijker een pan-Europese markt voor gekwalificeerde certificatiediensten kunnen ontstaan.

7.5.3 Kosten toezichtsarrangement

Certificatiedienstverleners investeren in beveiligingsmaatregelen en het voldoen aan extern opgelegde eisen. De kosten om geregistreerd te worden, audits te ondergaan en de door auditors geconstateerde afwijkingen weg te nemen, zijn voor rekening van de certificatiedienstverlener. Voor commerciële certificatiedienstverleners zijn de kosten van dit toezichtsarrangement onderdeel van de bedrijfskosten die moeten worden terugverdiend met hun dienstenverlening. Toename in schaalgrootte van certificatiediensten verkleint per certificaat de kostencomponent voor het toezichtsarrangement. Wanneer wordt besloten tot het verzwaren van het toezichtarrangement, is aan te bevelen factoren die marktwerking belemmeren te verminderen of anderszins de markt te vergroten zodat dienstverleners gemakkelijker in schaalgrootte kunnen toenemen.

7.5.4 Transparantie

Voor afnemers van certificatiediensten en 'vertrouwende partijen' is het moeilijk om de betrouwbaarheid van certificatiedienstverleners en hun verantwoordelijkheden vast te stellen. De conformiteitsverklaringen die auditors afgeven zijn alleen begrijpelijk voor deskundigen en zijn onvergelijkbaar. De verwijzingen naar normenkaders, certificatiebeleidsdocumenten en het TTP.NL schema worden niet uniform opgenomen. Verklaringen van auditors over afwijkingen van de normen en de manier waarop zekerheid wordt gegeven zijn uitsluitend beschikbaar voor de betreffende certificatiedienstverlener, de Opta en Logius. Afnemers van certificaten kunnen kennis nemen van de verantwoordelijkheden en werkwijze van de certificatiedienstverleners via publieke documenten (het certificatiebeleidsdocument en het certificatiepraktijkdocument). Naleving van deze publiek beschikbare verklaringen wordt door de auditors in de praktijk niet expliciet getoetst en wat auditors wel toetsen is niet publiek beschikbaar.

Transparantie en eenduidigheid ten aanzien van de daadwerkelijk geleverde certificatiediensten en de kwaliteit ervan, verhoogt het gerechtvaardigde vertrouwen dat in de diensten kan worden gesteld. Herkenbaarheid kan bijvoorbeeld worden bevorderd door het invoeren van een eenduidig 'keurmerk' voor certificatiediensten waarbij auditors worden verplicht aanvullende informatie in conformiteitsverklaringen op te nemen zoals een expliciete beschrijving welke controles zijn uitgevoerd. Een keurmerk met een voor vertrouwende partijen duidelijke betekenis en zekerheid bestaat op dit moment in de praktijk niet. Om eenduidigheid van zo'n keurmerk te bevorderen is het aan te bevelen om tenminste alle door de overheid gereguleerde certificaten er onder te laten vallen, al kunnen er wel meerdere niveau's in het keurmerk worden aangebracht.

7.5.5 Marktwerking auditors

In Nederland zijn momenteel twee partijen geaccrediteerd om certificatiedienstverleners te auditen. Ze onderhouden doorgaans een langdurige relatie met hun klanten, de certificatie-

dienstverleners. Contracten tussen auditors en certificatiedienstverleners worden voor onbepaalde tijd afgesloten. In de praktijk wordt er niet tussen auditors gewisseld.

Vanaf 1 januari 2014 is het ook niet meer mogelijk voor geïnteresseerde auditors die in het buitenland gevestigd zijn, om in Nederland geaccrediteerd te worden voor het verstrekken van conformiteitsverklaringen aan Nederlandse certificatiedienstverleners.

De auditors geven aan niet op prijs te concurreren. Deze vorm van certificering maakt voor hen ook slechts een klein deel van hun omzet uit. Bij het wegvallen van één van beide auditors zou de marktwerking geheel wegvallen.

Wisselen van auditor heeft het voordeel dat een auditor de certificatiedienstverlener met een frisse blik beoordeelt. Een vaste auditor heeft als voordeel dat er telkens kan worden voortgebouwd op aanwezige kennis. Met periodiek wisselen van auditor kunnen beide voordelen worden gecombineerd. Hiervoor is het nodig dat er meerdere auditors zijn. Bij wijzigingen in het toezichtsarrangement is het daarom van belang om het risico van verdwijnen van marktwerking mee te wegen.

7.6 Operationele PKI

7.6.1 Alternatieven

PKI is een verzameling afspraken, diensten en technologieën waarvan het grootste deel beproefd is en niet ter discussie staat. De verbeteringsmogelijkheden in het onderliggende vertrouwensmodel zijn grotendeels nog niet goed uitgekristalliseerd en zijn nog niet volwassen genoeg voor brede toepassing. Recent naar voren gekomen ‘alternatieven’ waaronder DANE en Convergence kunnen op termijn waardevolle aanvullingen vormen, maar zijn nog in een onderzoeksstadium en zijn eerder aanpassingen op PKI dan volwaardige alternatieven. Voor zover deze verbeteringsmogelijkheden uiteindelijk breed zullen worden geadopteerd valt te verwachten dat eerder sprake zal zijn van een geleidelijke selectieve adoptie, dan van een revolutie.

Op dit moment zijn ook al enkele verbeteringen door te voeren in de wijze waarop PKI in de praktijk functioneert en waarvoor fundamentele veranderingen in het vertrouwensmodel niet nodig zijn.

Ten eerste is het zonder wijzigingen in het vertrouwensmodel mogelijk om een hoger betrouwbaarheidsniveau te realiseren met PKI in situaties waarin generieke software(configuraties) van vertrouwende partijen kan worden vervangen door specifieke software(configuraties). In deze situatie hoeft de vertrouwende partij niet te rusten op een groot aantal vertrouwensknooppunten, maar vertrouwen kan dan worden ontleend aan een enkel knooppunt of een enkel certificaat. Deze situatie bestaat bijvoorbeeld vaak wanneer twee organisaties die elkaar kennen een systeem-systeem koppeling willen beveiligen.

Ten tweede kunnen de consequenties van het wegvallen van vertrouwen in een vertrouwensknooppunt of certificatiedienstverlener worden beperkt door het uniformeren van abonneeregistratieprocedures. Hierdoor zouden afnemers zich gemakkelijker voor continuïteits-doeleinden bij meerdere certificatiedienstverleners kunnen registreren. Om een vervanging van certificaten afkomstig van een specifieke dienstverlener te vergemakkelijken is het bovendien verstandig om een actueel overzicht bij te houden van componenten die gebruik maken van certificaten.

Om, in geval vertrouwen in een certificatiedienstverlener wegvalt, te kunnen overstappen naar een andere dienstverlener, is het van belang dat er voldoende alternatieven bestaan en dat deze dienstverleners in staat zijn om hun productie en uitgifte processen tijdig op te schalen. Bovendien dienen de processen bij de dienstverlener daartoe zo te zijn opgezet dat aanpassingen ten behoeve van specifieke vereisten van nieuwe abonnees snel kunnen worden ingewilligd.

7.6.2 De menselijke factor

De menselijke factor bij beveiliging is vaak de zwakste schakel. Positief geformuleerd: niet het systeem van normen en afspraken, maar de menselijke aandacht en gedrevenheid maakt het verschil. Deze menselijke factor is in het onderzoek naar structurele risico's slechts beperkt onderzocht. Toch is de indruk ontstaan dat deze ook in de opzet en de werking van de stelsels een wezenlijke rol vervult. Gedeeltelijk is deze factor geobjectiveerd binnen de stelsels. Aan auditors worden bijvoorbeeld eisen gesteld ten aanzien van kennis, competentie en onafhankelijkheid. Echter, niet alle stakeholders hebben de benodigde kennis en overzicht, of een proactieve houding waarbij over formele grenzen heen wordt gekeken, of een alertheid om signalen op basis van informele relaties op te pakken. Wanneer op meerdere niveaus formele en persoonlijke relaties tussen stakeholders zouden worden onderhouden en er actief op de attitude van mensen zou worden gestuurd, zouden kwetsbaarheden in de stelsels mogelijk eerder aan het licht komen.

8 REFERENTIES

Juridisch kader - internationaal

[1] European Directive 1999/93/EC of the European Parliament and the Council of the 13 December 1999 on a Community framework for electronic signatures.

[2] EC decision 2003/511 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC, 14 July, 2003

[3] EC decision 2009/767 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC, 2009/767/EC, 16 October 2009

[4] EC decision 2010/425 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States, 28 July 2010

[5] EC decision 2011/130 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC, 25 February, 2011

[6] Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten (BS van 29.09.2001), België

[7] Koninklijk besluit van 6 december 2002 houdende organisatie van de controle en de accreditatie van de certificatiedienstverleners die gekwalificeerde certificaten afleveren. (BS 17.01.2003), België

[8] Verordnung zur elektronischen Signatur, 16/11/2001, Duitsland

[9] Gesetz über Rahmenbedingungen für elektronische Signaturen, 16/5/2001, Duitsland

Juridisch kader - Nederland

[10] Aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13), Wet Elektronische Handtekeningen, 8 mei 2003, Staatscourant

[11] Wet elektronische handtekeningen – Memorie van Toelichting

[12] Besluit Elektronische Handtekeningen met Nota van Toelichting, 8 mei 2003, Staatscourant

[13] Regeling Elektronische Handtekeningen, 6 mei 2003 nr. WJZ/03/02263

[14] Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen, 6 mei 2003 nr. WJZ/03/02264

De stelsels

[15] RvA-R13 "Regelement voor de Beoordeling en Acceptatie van Schemabeheerders", Raad voor Accreditatie, 1 januari 2008

[16] RvA-T33 "Beoordeling van Schema's voor Conformiteitsbeoordeling", Raad voor Accreditatie, juli 2008

[17] PKIoverheid Programma van Eisen, versie 3.1, 1 juli 2011.

[18] Certification Practice Statement (CPS) Policy Authority PKIoverheid voor Extended Validation certificaten uit te geven door de Policy Authority van de PKI voor de overheid, v1.1, 1 juli 2011

[19] Certification Practice Statement (CPS) Policy Authority PKIoverheid voor certificaten uit te geven door de Policy Authority van de PKI voor de overheid, v3.4, 1 juli 2011

[20] TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and / or Time-stamp tokens, version 8.1, ECP-EPN, June 2010.

[21] TTP.NL Scheme - Guidance Note 1, ECP-EPN, June 2010

[22] TTP.NL Scheme - Guidance Note 2, ECP-EPN, June 2010

[23] TTP.NL Schema Terms of Reference van het College van Belanghebbenden – TTP.NL, ECP-EPN, juni 2010

[24] Register van certificaten op basis van TTP.NL Schema, ECP-EPN, 18 oktober 2011

[25] Accreditatie van beheerder TTP.NL (ECP-EPN) op basis van ISO/IEC 17021, Registratienr S 388, Raad voor Accreditatie

[26] Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by Opta (Trusted Services List NL), Opta, 19 November, 2011

[27] Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by FPS Economy (Trusted Services List BE), FPS Economy, 1 September, 2011

Certificatiedienstverleners

[28] Certificate Policy DigiNotar Gekwalificeerd, v1.0, november 2003

[29] Certification Practice Statement DigiNotar Algemeen, v4.1, 28 juli 2010

[30] Certification Practice Statement DigiNotar Gekwalificeerd, v1.5.2, 28 januari 2010

[31] Certification Practice Statement DigiNotar PKIoverheid Domein Overheid en Bedrijven, v1.5.2, 12 februari 2010

[32] Certification Practice Statement DigiNotar PKIoverheid SERVICES Domein Overheid en Bedrijven, v1.2.2, augustus 2007

[33] Bijlage CPS DigiNotar, Techische Specificaties, v4.1, 15 juli 2010

[34] Bijlage CPS DigiNotar Gekwalificeerd, Technische Specificaties, v1.4, september 2008

[35] Certification Practice Statement, Digidentity, v1.0, 20 april 2011

[36] Certification Practice Statement, ESG de elektronische signatuur BV, v 4.10, 4 februari 2011

[37] Certification Practice Statement, Getronics Nederland BV, v4.1, 15 augustus 2011

[38] Certification Practice Statement, PKIoverheid, Quo Vadis Trustlink BV, v1.0, 30 juni 2009

[39] Certification Practice Statement, Belgium Root, v 1.1, 3 February 2006, FedICT

[40] Certification Practice Statement, Citizen CA Belgium, v1.3, CertiPost.

[41] Certification Practice Statement, For Qualified, Normalised and Lightweight Certificates, v 2.4, 12 January 2011, Certipost

Standaarden

[42] ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates, v 1.4.3, mei 2007

[43] ETSI TS 102 437: Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates), v1.1.1, oktober 2006

[44] ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates, v2.1.2, april 2004

[45] ETSI TS 102 023: Policy requirements for time-stamping authorities, v1.2.2, oktober 2008

[46] ETSI TS 101 862: Qualified Certificate Profile, v1.3.2, juni 2004

[47] ETSI TS draft Electronic Signatures and Infrastructures (ESI) – Trust Service Provider Conformity Assessment – General requirements and guidance, v0.0.3, November, 2011

[48] ETSI draft Special Report - Rationalised Framework for Electronic Signature Standardisation, August, 2011.

[49] CEN CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatur–s - Part 1: System Security Requirements, juni 2003

[50] CEN CWA 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP), mei 2004

[51] CEN prEN 14169 (draft): Protection profiles for Secure Signature Creation Device — 6 parts

[52] CWA 14172-3: EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures, maart 2004

[53] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. IETF, November 2003

[54] RCF 2560 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP. IETF

[55] RFC 5280 - X.509 Public Key Infrastructure Certificate - and Certificate Revocation List (CRL) Profile, IETF

[56] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, NIST

[57] ISO 17021 “Conformity Assessment – Requirements for bodies providing audit and certification of management systems”, februari 2011

[58] ISO 19011 “Guidelines for quality and environmental management systems auditing”, October 2002

[59] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.0, CA/Browser Forum, 22 november 2011.

[60] Trust Service Principles and Criteria for Certification Authorities v2.0, AICPA, March 2011

[61] Richtlijn Assurance-opdrachten door IT-auditors (3000), Norea

Overig Nederland

[62] Interim Report DigiNotar Certificate Authority breach “Operation Black Tulip” (public version), Fox-IT, September 5, 2011

[63] Besluit van het College van de Onafhankelijke Post en Telecommunicatie Autoriteit op grond van artikel 2.2, vierde lid, sub b van de Telecommunicatiewet tot het beëindigen van de registratie van DigiNotar B.V. als certificatiedienstverlener wegens verrichten van activiteiten en diensten in strijd met artikel 2 van het Besluit elektronische handtekeningen, Opta, 13 september 2011

[64] Sleutels van vertrouwen, TTP’s, digitale certificaten en privacy, Achtergrondstudies en Verkenningen, Registratiekamer, maart 2001

[65] Cybersecuritybeeld Nederland, Ministerie van Veiligheid en Justitie, December 2011

[66] Brief van de Ministers van BZK en VENJ aan de 2e kamer betreft de Digitale Inbraak DigiNotar, dd 5 september 2011

[67] Brief van de Ministers van BZK en VenJ aan de 2e kamer betreft de Digitale Inbraak DigiNotar, dd 16 september 2011

[68] Eindrapport "Een open tunnelvisie, Evaluatie van het TTP-beleid", Universiteit van Tilburg / Ordina Management Consulting, 30 juni 2004

[69] Adviescommissie Authenticatie en Autorisatie Bedrijven (A3 Bedrijven) – Eindadvies, 11 november 2011

Overig Europa

[70] Report from the Commission to the European Parliament and the Council on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, 15 March 2006

[71] Communication from the Council – Action Plan on e-signatures and e-identification to facilitate the provision on cross-border public services in the Single Market, 28 November 2008

[72] EC Standardisation Mandate M/460 to CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to Electronic Signatures, 22 December 2009

[73] Study on the standardisation aspects of eSignature, A Study for the European Commission (DG Information Society and Media), SEALED, DLA Piper, Final Report, 22/11/2007

[74] Study on Cross-Border Interoperability of eSignatures (CROBIES), Framework for Secure Signature Creation Devices cross-border recognition, A report to the European Commission from SEALED, time.lex and Siemens, 31/7/2010

[75] Secure Identity Across Borders Linked (STORK) Deliverable D2.3 - Quality authenticator scheme, 3 maart 2009

[76] IDABC EFVS Study – Completion of the framework for signature validation services, March 2010

[77] Study "Digital Internal Market", IP/A/IMCO/ST/2011-04, juni 2011

[78] Marktconsultatie elektronische identificatie, elektronische authenticatie en elektronische handtekeningen, afgesloten 15 april 2011, Europese Commissie

[79] Study for the European Commision, DG Information Society, "The Legal and Market Aspects of Electronic Signatures", Katholieke Universiteit Leuven, October 2003

[80] Important topics for the review of Directive 1999/93/EC from the supervisory authorities' point of view, Forum of European Authorities for Electronic Signatures (FESA), 30 June, 2003

[81] Belgium Country Report, ENISA, May 2011

[82] Germany Country Report, ENISA, May 2011

BIJLAGE A: LIJST MET GEÏNTERVIEWDE PERSONEN

Drs. C. (Carl) Adamse, coördinerend senior beleidsmedewerker, ministerie van BZK

Ir. J. (Jan) van den Akker, Teamleider, Raad voor Accreditatie

Drs. O. (Olaf) Andersen, plv. Directeur Informatiseringsbeleid Rijk, ministerie van BZK

Ir. R. (René) van den Assem, Principal Consultant en Partner, Verdonck, Klooster & Associates en Voorzitter College van Belanghebbenden TTP.NL

A. (Adri) de Bruijn RE RA, Partner, PWC

R.V. (Rob) Duiven, kwartiermaker Cyber Security, ministerie van VenJ

Prof.dr. P.W.A. (Peter) Eimers RA, Directeur, PWC

Drs. A. (Arjen) Haasnoot, Senior Beleidsmedewerker, ministerie van EL&I

Drs. D. (Dave) Hagenaars, Managing Director Benelux, BSI Group

Drs. M. (Mark) Hoevers, Secretaris College van Belanghebbenden TTP.NL

Drs. M.A. (Mark) Janssen, Tactisch Beheerder PKIoverheid, Logius

A. (Aart) Jochem, Manager security team, Govcert

Mr. R. (Raoul) Klein, Senior Jurist, Opta.

G. (Gerben) Klein Baltink, secretaris Cyber Security Raad

C. (Carlo) Luijten, Senior Beleidsmedewerker, ministerie van BZK

Ir. A. (Ard) Niesen RE, Voorzitter NOREA

Drs. W.J.A. (Wilfried) Olthof, Directeur NOREA

Mr. P.H. (Patrick) Paling RE, Senior Manager, KPMG

Ir. J. (Jan) van der Poel, Bestuurder / Algemeen Directeur, Raad voor Accreditatie

Ir. R. (Ronald) Prins, CEO Fox-IT

A. (Andreas) Reisen, Hoofd divisie “Paspoorten, identiteitsdocumenten en –systemen”, Federaal ministerie van Binnenlandse Zaken, Duitsland

Dr.ir. E.J. (Elbert Jan) van Veldhuizen, plv. Afdelingshoofd Consument, Nummers en Bestuur, Opta

R. (Renaat) Verschraeghen, Senior Security Analist, FedICT, België

Drs. H. (Hans) Verweij, Manager Productregie, Logius

Mw. Drs. M. (Maureen) van den Wijngaart, Relatiebeheerder, Raad voor Accreditatie

Product Manager, Certificatiedienstverlener

Consultant, Certificatiedienstverlener

Manager, Certificatiedienstverlener

BIJLAGE B: VERKLARENDE WOORDENLIJST

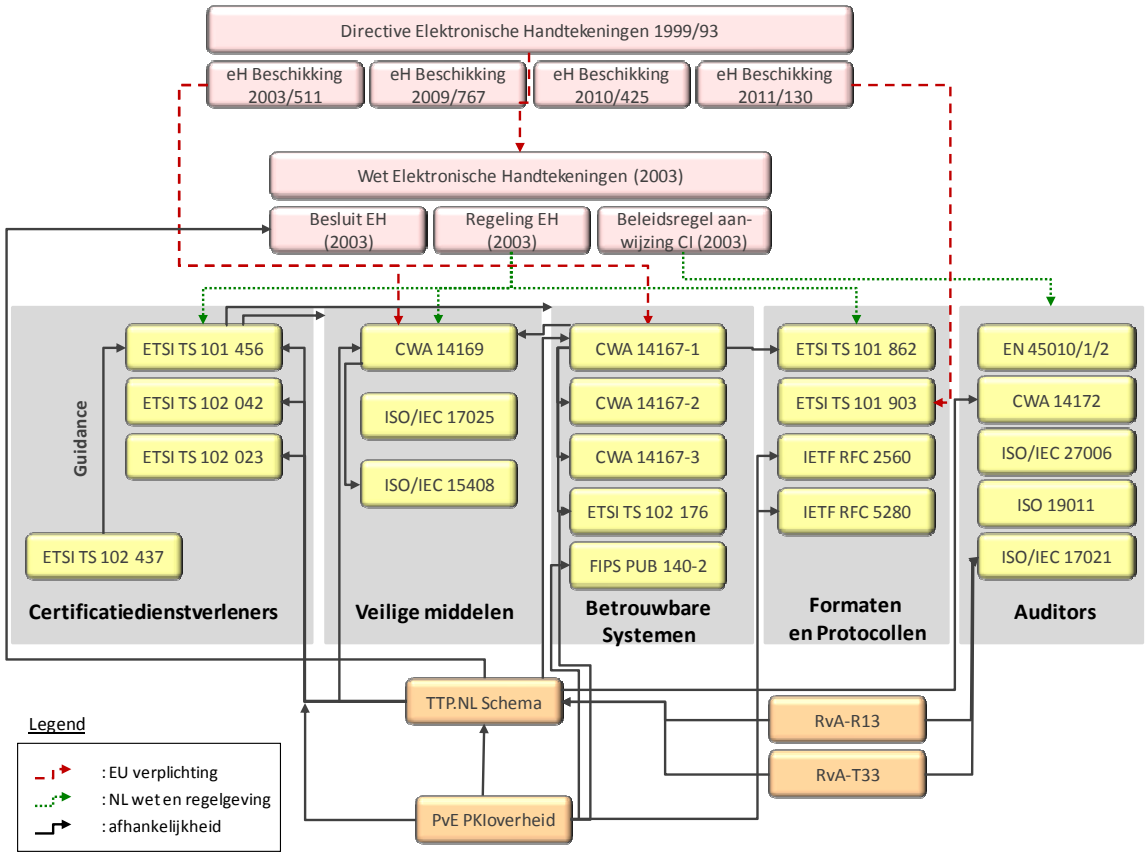
Accreditatie:	De activiteit waarmee een daartoe geautoriseerde onafhankelijke en onpartijdige instantie verklaart dat een conformiteits-beoordelende instantie voldoet aan specifieke eisen en daarmee competent is voor het uitvoeren van specifieke conformiteits-beoordelende activiteiten, zoals certificeren, inspecteren, kalibreren of testen.
Auditor:	Zie 'Certificerende Instelling'. Een auditor kan ook een individu zijn die al dan niet onder verantwoordelijkheid van een Certificerende Instelling audits uitvoert. Tenzij aangegeven, wordt deze betekenis in dit rapport niet gehanteerd.
Betrouwbaar systeem:	Een systeem dat beschermd is tegen wijziging en dat technische en cryptografische veiligheid garandeert van de processen die het ondersteunt.
Betrouwbaarheid:	Volledigheid, juistheid en tijdigheid
Certificaat:	De publieke sleutel van een entiteit (zoals een persoon of systeem) samen met een identificatie van de entiteit, en mogelijk andere informatie, onvervalsbaar cryptografisch aan elkaar verbonden met behulp van de geheime sleutel van het vertrouwensknooppunt dat het certificaat uitgeeft.
Certificatiebeleidsdocument:	Een verzameling regels die de toepasbaarheid van een certificaat voor een bepaalde groep gebruikers en/of toepassingen met gemeenschappelijke beveiligingseisen vastlegt.
Certificatiedienstverlener:	Een natuurlijke of een rechtspersoon die certificaten uitgeeft en/of gerelateerde diensten aanbiedt.
Certificatiepraktijkdocument:	Een verklaring van de praktijken die door een vertrouwensknooppunt worden gehanteerd bij het uitgeven, beheren, herroepen en vernieuwen van certificaten.
Certificerende instelling:	Een organisatie die conformiteitsbeoordelingen uitvoert en dat onderwerp van accreditatie kan zijn.
IT-audit:	Het deskundig en onafhankelijk vellen van een oordeel over de kwaliteit van de informatievoorziening en de veiligheid en betrouwbaarheid van informatiesystemen.
Gekwalificeerd certificaat:	Een certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een certificatiedienstverlener die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet.

Management systeem:	Een raamwerk van processen en procedures die worden gebruikt zodat een organisatie de taken kan uitvoeren die nodig zijn om haar doelstellingen te bereiken.
Public Key Infrastructuur:	De combinatie van hardware, software, mensen, beleidsregels en procedures die nodig zijn voor het creëren, beheren, distribueren, gebruiken, opslaan en herroepen van digitale certificaten.
PKI-stelsel:	Een combinatie van de volgende invalshoeken op een PKI: organisatie en toezicht, normenstelsel en operationele PKI.
Toezichthouder:	De wettelijk toezichthouder op het stelsel 'gekwalificeerde certificaten' (hier: Opta) houdt toezicht op basis van publiekrechtelijke taken. De niet wettelijk toezichthouder op het stelsel PKIoverheid (hier: Logius) houdt toezicht op privaatrechtelijke contracten.
Toezichtsarrangement:	Afspraken ten aanzien van toetsing en handhaving op naleving van normen.
Veilig middel:	Hardware en software die gebruikt wordt om elektronische handtekeningen mee te zetten, en dat voldoet aan de eisen in Bijlage III van de EU Richtlijn
Vertrouwensknooppunt:	Een organisatorisch verband, welk onderdeel is van een Certificatiedienstverlener of die onder verantwoordelijkheid van de Certificatiedienstverlener handelt en die door één of meerdere 'vertrouwende partijen' wordt vertrouwd om certificaten te creëren, toe te wijzen en in te trekken.
Vertrouwende partij:	De ontvanger van een certificaat die vertrouwen hierop baseert

BIJLAGE C: LIJST MET GEHANTEERDE AFKORTINGEN

BZK	Binnenlandse Zaken en Koninkrijksrelaties
EL&I	Economische Zaken, Landbouw en Innovatie
GBA	Gemeentelijke Basis Administratie
NIK:	Nationale Identiteits Kaart
Opta:	Onafhankelijke Post en Telecommunicatie Autoriteit
PKI:	Public Key Infrastructuur
PvE	Programma van Eisen
RvA:	Raad voor Accreditatie
SSL	Secure Socket Layer
TTP.NL:	Het samenwerkingsverband “trusted third parties” in Nederland
VenJ	Veiligheid en Justitie
WEH	Wet Elektronische Handtekeningen

BIJLAGE D: OVERZICHT NORMEN



Figuur 5: Normenstelsel

BIJLAGE E: OVER LOGICA EN OVER DE AUTEURS

Logica Nederland BV

Logica heeft meer dan 40 jaar ervaring met informatiebeveiliging voor klanten binnen de overheid en in het bedrijfsleven. Overheden en bedrijven over de gehele wereld vertrouwen Logica hun beveiligingsproblemen toe. Een geïntegreerd team van meer dan 600 security professionals, gevestigd in 12 landen van Europa, het Midden Oosten en Australië zorgt dat de beveiligingsdiensten aan locale klanten geleverd worden.

Daarmee heeft Logica unieke kennis en ervaring opgebouwd hoe complexe beveiligings-vraagstukken in de praktijk kunnen worden aangepakt. De oplossingen van Logica bestaan uit een combinatie van consultancy, systeemintegratie en managed services om mensen, processen en technologie in samenhang te adresseren.

Ir. Niek IJzinga, Principal Consultant en NL Security Practice Leader

Niek is sinds 1 februari 1995 in dienst bij Logica. Sindsdien heeft hij zich bijna uitsluitend met informatiebeveiliging beziggehouden. Als beveiligingsdeskundige heeft hij rollen vervuld als interim security manager, security architect, pre-sales consultant en beveiligingsadviseur in binnen- en buitenland. Niek heeft brede technische (security) kennis op zowel infrastructuur, software engineering en architectuur vlak. Hij is betrokken geweest bij PKI vanuit zowel de beleidsmatige als de implementatiekant. Niek opereert doorgaans op het snijvlak tussen bedrijfsprocessen en IT. Niek heeft ervaring met zowel consultancy, (fixed price) projecten als met managed services. Hij is actief geweest in verschillende marktsectoren.

Drs. Ir. Albert Vlug, Principal Consultant Public Sector

Albert Vlug is van 1992-2006 werkzaam geweest in de medische informatica van het ErasmusMC te Rotterdam. Eén van zijn belangrijkste projecten aldaar was het opzetten van een Zekerheidstructuur rondom de nationale verzameling van medische dossiers van artsen ten behoeve van wetenschappelijk onderzoek. Vanaf 2004 was Albert als adviseur verbonden aan Nictiz voor het ontwerpen van standaarden voor medisch inhoudelijke berichten en voor beveiliging van de gegevensuitwisseling. Vanaf 2007 was hij als hoofd van de afdeling Ontwerp en Onderhoud verantwoordelijk voor de eisen die gesteld worden aan landelijke gegevensuitwisseling. Dit omvatte ook de eisen aan identificatie en authenticatie oplossingen gebaseerd op PKI.

Sinds 2010 is Albert werkzaam bij Logica als Lead Consultant Public Sector. Hij adviseert in het bijzonder zorgaanbieders op bestuurlijk en directie niveau met betrekking tot informatie-voorzienings- en informatiebeveiligingsbeleid.

Logica Business Consulting Nederland, Prof. W.H. Keesomlaan 14, 1180 AD Amstelveen
Contact: Niek IJzinga, Security Practice Leader, T: +31 (0) 88 564 0000, niek.ijzinga@logica.com

Logica Business Consulting is de Business Consulting Divisie van de Logica Groep. Logica verleent zakelijke en technologische diensten. Wereldwijd telt Logica 41.000 medewerkers. Het bedrijf biedt zakelijke dienstverlening, systeemintegratie en outsourcing voor klanten over de hele wereld. Onder de klanten bevinden zich de grootste bedrijven van Europa.

Logica Business Consulting heeft een netwerk van ongeveer 3500 consultants in Europa. Onze consultants helpen klanten success te bereiken door middel van transformatietrajecten. Zij onderscheiden zich door hun Europese cultuur, hun vermogen om nauw met klanten samen te werken, en een unieke combinative van marktspecifieke, functionele en technologische expertise.

Logica staat genoteerd aan de beurs van Londen en aan Euronext in Amsterdam (LSE: LOG; Euronext: LOG)
Meer informatie is beschikbaar via www.logica.com/consulting