Het beoordelen van een Public Key Infrastructure (PKI)

Normenkaders en werkwijze

Drs. P.A. van Walsem

Het uitvoeren van onderzoek naar de implementatie, exploitatie en het beheer van Public Key Infrastructures (PKI's) en het gebruik van digitale certificaten krijgen steeds meer aandacht, zeker nu er in Nederland een voorstel voor de Wet Elektronische Handtekening en een Certificeringsschema zijn opgesteld. Om EDP-audit vaktechnische redenen is het relevant om te weten op welke wijze een onderzoek naar de betrouwbaarheid, beschikbaarheid, controleerbaarheid en beheersbaarheid van een PKI wordt uitgevoerd. In dit artikel wordt een overzicht gegeven van de verschillende normenkaders die zijn opgesteld, hun onderlinge relaties en de wijze waarop een onderzoek naar de betrouwbaarheid, beschikbaarheid, controleerbaarheid en beheersbaarheid moet worden uitgevoerd.

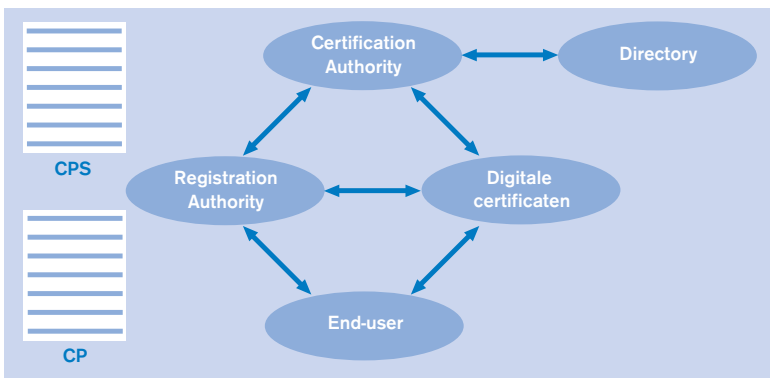
Inleiding

Bijna elk artikel over een Public Key Infrastructure (PKI) begint met de vergelijking tussen de papieren wereld en de elektronische/digitale wereld. De voordelen zijn legio en de risico's van elektronische handel over het internet kunnen door gebruik te maken van digitale certificaten en cryptografische sleutels worden beperkt.

Na de implementatie van een PKI zit het management vaak met vragen omtrent de kwaliteit van de inrichting van een PKI. Is een implementatie juist uitgevoerd? Zijn de geïmplementeerde PKI-processen betrouwbaar? Deze vragen hebben een relatie met het feit dat voor het implementeren en beheren van een PKI specialistische kennis nodig is. Deze kennis is vaak niet voldoende aanwezig binnen de organisatie. De behoefte om de inrichting en de werking van een PKI te toetsen wordt steeds groter, niet alleen vanuit de interne organisatie, ook extern worden steeds meer vragen gesteld. Is deze organisatie te vertrouwen? Zijn de procedures van een voldoende niveau? Kortom, zijn de certificaten wel blijvend betrouwbaar?

1) American Bar Association, *PKI Assessment Guidelines PAG v0.30*, public draft for comment, June 18, 2001.

Figuur 1. PKI-componenten en -processen.



Het management van de organisatie waarbinnen de PKI is geïmplementeerd, vraagt zich af op welke wijze zo'n onderzoek moet worden uitgevoerd, welke normen moeten worden gehanteerd en welke onderzoeksobjecten bij een dergelijk onderzoek horen. Moet de inrichting van de PKI gecertificeerd worden om zodoende een hogere mate van vertrouwen te wekken bij klanten van de organisatie?

Het doel van dit artikel is antwoord te geven op de genoemde vragen. Onderwerpen die aan bod komen zijn: de onderzoeksobjecten, technische standaarden, publieke en private PKI-normenkaders, het verschil tussen beide, de wijze van uitvoering, Third Party Mededelingen en certificering.

PKI-componenten en -processen

Een Public Key Infrastructure[1] (PKI) wordt in de literatuur omschreven als een opsomming van het totaal van hardware, software, mensen, processen en beleidsdocumentatie die samen gebruikmakend van de technologie van asymmetrische cryptografie, de creatie van een verifieerbare associatie tussen een publieke sleutel (het publieke gedeelte van een asymmetrisch sleutelpaar) en de identiteit van de houder van de private sleutel (het private gedeelte van een asymmetrisch sleutelpaar) faciliteren. Dit voor onder andere de authenticatie van de identiteit van een persoon of organisatie, het waarborgen van de integriteit van informatie, het zorgen voor ondersteuning bij het bepalen van onweerlegbaarheid en het tot stand laten komen van een versleutelde communicatiesessie.

Een PKI bestaat uit verschillende componenten en processen (zie figuur 1). Een organisatie die een PKI heeft geïmplementeerd, wordt ook wel een Certificaat Uitgevende Organisatie (CUO) genoemd. Voor het uitgeven

van de certificaten wordt gebruikgemaakt van een Certification Authority (CA). De digitale certificaten die binnen PKI-componenten en -processen worden gehanteerd, zijn gebaseerd op de X509-standaard. Gegevens die in een certificaat zijn opgenomen, betreffen (afhankelijk van de versie) onder andere de naam van de persoon, functionaris of organisatie, de naam van de CA, uitgifte- en vervaldata, uniek serienummer van het certificaat, digitale handtekening van de CA, de verificatie- of encryptiesleutel, velden (waarin wordt verwezen naar de toepasselijke Certificate Policy (zie uitleg verderop in dit artikel) of bevoegdheden van de persoon of functionaris) en unieke naam van de bijbehorende CRL[2]. Voordat de certificaten kunnen worden uitgegeven, moet in eerste instantie een koppeling worden gelegd tussen de identiteit van een persoon of organisatie en zijn of haar publieke sleutel. Dit proces wordt uitgevoerd door een Registration Authority (RA). Om berichten te kunnen versleutelen en ondertekend te kunnen versturen en te kunnen ontvangen moeten de publieke sleutels bekend en toegankelijk zijn voor andere partijen. Dit wordt gerealiseerd door gebruik te maken van een directory.

2) CRL staat voor Certificaten Revocatielijst of Certificate Revocation List en geeft de status weer van de certificaten (bijvoorbeeld ingetrokken, opgeschort, ongeldig).

In toenemende mate worden de CA-functionaliteit en het beheer van de directory uitbesteed aan een derde partij.

Deze is via het internet (on line) voor iedereen toegankelijk. Voor het beheer van een PKI zijn alle algemene IT-beheerprocessen relevant, zoals change management en problem management. Tevens zijn er twee PKI-specifieke beheerprocessen, namelijk:

* CA-sleutelmanagement (sleutelbeheer). Hieronder worden alle beheerprocessen rondom het genereren, het distribueren, het vernieuwen en het vernietigen van CA-sleutels verstaan.
* certificaatmanagement (certificaatbeheer). Hieronder worden alle beheerprocessen rondom het genereren, het distribueren, het vernieuwen en het vernietigen van digitale eindgebruikercertificaten verstaan.

Waar certificaten voor kunnen worden gehanteerd en welke eisen hieraan worden gesteld, wordt veelal gepubliceerd in een Certificate Policy (CP). De bijbehorende geïmplementeerde procedures en maatregelen worden veelal gepubliceerd in een Certification Practice Statement (CPS). Om te zorgen dat eindgebruikers en vertrouwende partijen inzicht kunnen krijgen in de wijze waarop certificaten worden gegenereerd en welke controles en maatregelen een CA heeft genomen om betrouwbare certificaten uit te geven, worden de beide documenten voor het publiek via het internet toegankelijk gemaakt.

Het niveau van de geïmplementeerde maatregelen en procedures is afhankelijk van de toepassing van de digitale certificaten. Deze kan verschillend zijn. Zo worden certificaten gehanteerd om vertrouwelijke informatie via het internet te versturen, maar kunnen digitale certificaten ook worden gehanteerd om een Virtual Private Network (VPN)[3] te realiseren.

3) Door middel van het gebruik van een VPN kan het openbare internet gezien worden als een privaat netwerk. Hiervoor moet informatie tussen partijen versleuteld worden uitgewisseld. Tevens dient tijdens de uitwisseling van informatie de juiste identiteit van de verschillende netwerknodes te worden bepaald. Dit wordt door middel van het gebruik van digitale certificaten gerealiseerd. Over het algemeen worden ook eindgebruikercertificaten in een VPN toegepast.
4) Internet Engineering Task Force Request For Comment 2527.
5) Federal Information Processing Standard.
6) Public-key Infrastructure (X509) (IETF-Working group).
7) International Organization for Standardization.
8) British Standards Institution, Code voor Informatiebeveiliging.

Onderzoeksobjecten bij het beoordelen van een PKI

Voor het beoordelen van de kwaliteit (betrouwbaarheid, beschikbaarheid, controleerbaarheid en beheersbaarheid) van de getroffen maatregelen binnen een PKI kunnen vier onderzoeksobjecten worden onderscheiden:

* *ontsluiting van CA-beheer en -beleidsdocumentatie*. Denk hierbij aan de wijze waarop de CA-organisatie gegevens betreffende het gebruik en het beheer van certificaten aan eindgebruikers en vertrouwende partijen bekendmaakt.
* *algemene IT-beheermaatregelen*. Denk hierbij aan beheerprocessen zoals change management, problem management, het opstellen en beheren van ICT/PKI-beleid, alsook de beveiliging van de ICT-infrastructuur (routers, firewalls).
* *CA-sleutelmanagement*. Denk hierbij aan de beheerprocessen en maatregelen aangaande de levenscyclus van de cryptografische CA-sleutels (genereren, vernietigen en vernieuwen).
* *certificaatmanagement*. Denk hierbij aan de beheerprocessen en maatregelen rondom de levenscyclus van de digitale certificaten (uitgifte, intrekken, vernieuwen).

In sommige gevallen worden deze processen en het beheer van de PKI-componenten niet door een en dezelfde partij uitgevoerd. In toenemende mate worden de CA-functionaliteit en het beheer van de directory uitbesteed aan een derde partij. De certificaten worden dan nog wel onder verantwoordelijkheid van de certificaatuitgevende organisatie gegenereerd, alleen wordt deze activiteit uitgevoerd door een derde partij. De koppeling van de identiteit van een persoon of organisatie aan het certificaat (de RA-functie) wordt dan nog wel binnen de certificaatuitgevende partij uitgevoerd. Reden van uitbesteding zijn vaak de kostbare technische investeringen die voor fysieke beveiliging door de certificaatuitgevende organisatie moeten worden gemaakt.

Het onderzoek naar de kwaliteit van de in opzet, bestaan en werking getroffen PKI-maatregelen dient goed afgebakend te zijn. Indien de bovenstaande situatie zich voordoet moet extra aandacht aan de onderlinge werkafspraken en contracten tussen de verschillende partijen worden besteed.

PKI-normenkaders (publiek en privaat)

Voor het inrichten en beoordelen van de bovenstaande onderzoeksobjecten kunnen bestaande technische standaarden worden gehanteerd. Zo kan voor het beoordelen van de ontsluiting van de CA-bedrijfsdocumentatie gebruik worden gemaakt van de RFC 2527-standaard[4]. Voor het beoordelen van de inrichting van de CA-sleutelmanagementprocessen kan gebruik worden gemaakt van de FIPS 140-1-standaard[5]. Voor het inrichten en beoordelen van de certificaatmanagementprocessen kunnen de PKIX-standaarden[6] en de ISO 15782-standaard[7] worden gehanteerd. Voor het beoordelen van de algemene omgevingsmaatregelen kan de BS 7799[8] worden gehanteerd. Hierbij dient natuurlijk wel te worden opgemerkt dat aan deze technische standaarden nog specifieke PKI-eisen moeten worden toegevoegd. Vanuit

vaktechnische en praktische overwegingen is het eenvoudiger als tijdens zo'n onderzoek gebruik kan worden gemaakt van een integraal PKI-normenkader.

In 1998-1999 heeft binnen KPMG Information Risk Management (IRM) een internationale werkgroep een aantal PKI-controledoelstellingen geformuleerd waarbij gebruik is gemaakt van verschillende bestaande technische standaarden. De ontwikkeling van deze controledoelstellingen is onderdeel geweest van het opzetten van een KPMG-brede PKI Audit Methodologie. Deze PKI-controledoelstellingen zijn als input gehanteerd voor een ANSI/ASSC-werkgroep (X9F5). Deze werkgroep was verantwoordelijk voor het opstellen van de X9.79 PKI Policies and Procedures Guidelines, die later als input zijn gehanteerd voor het Webtrust for Certification Authorities Program en nu zijn voorgedragen als potentiële ISO-standaard.

De ANSI X.9.79-standaard[9] is voor vele andere PKI-standaarden als basis gehanteerd. Het ETSI-normenkader[10] en het Identrus-normenkader zijn hiervan voorbeelden. Binnen de verscheidene PKI-normenkaders die opgesteld zijn, kan een onderscheid worden gemaakt in publieke en private normenkaders. Publieke PKI-normenkaders zijn normenkaders die openbaar zijn en waar iedereen kennis van kan nemen. Soms moet hier een kleine vergoeding voor worden betaald. Verschillen tussen de publieke normenkaders kunnen liggen in de bewoordingen, definities van de verschillende onderzoeksobjecten en de doelgroepen waarbinnen deze normenkaders worden gehanteerd (financiële industrie).

Private PKI-normenkaders zijn normenkaders die gehanteerd worden in een gesloten gemeenschap. Deze normenkaders zijn niet openbaar en worden alleen verspreid binnen een gemeenschap (vertrouwens/trust-netwerk) waarop ze van toepassing zijn. Verschillen tussen deze normenkaders hebben te maken met de product- en dienstspecifieke onderdelen. Verder verschillen de scope en onderzoeksobjecten van die van de publieke normenkaders. Voorbeelden hiervan zijn gegeven in tabel 1.

Auditactiviteiten

Voor het uitvoeren van een onderzoek naar de kwaliteit (betrouwbaarheid, beschikbaarheid, controleerbaarheid en beheersbaarheid) van de getroffen maatregelen binnen een PKI kunnen drie fasen worden onderscheiden, namelijk planning, uitvoering en rapportage. Hieronder wordt van elke fase een korte beschrijving gegeven.

Planning

Als eerste dient te worden bepaald welk normenkader tijdens het onderzoek zal worden gehanteerd. Dit wordt in overleg met de opdrachtgever bepaald en is enerzijds afhankelijk van het onderzoeksobject en anderzijds van het doel van het onderzoek. De opdrachtgever is over het algemeen diegene die verantwoordelijk is voor het beheer en de exploitatie van de PKI-systemen en -componenten, maar steeds vaker worden opdrachten voor het beoordelen van de PKI-systemen en -componenten gegeven door de klanten die gebruikmaken van de PKI-dienstverlening (CA- en RA-services). De internationale status van het normenkader speelt bij de keuze hiervan een grote rol.

Indien het onderzoeksobject deel uitmaakt van een Trust Netwerk, zoals VeriSign Trust Netwerk, en het onderzoek als doel heeft vast te stellen in hoeverre de CUO voldoet aan de door VeriSign vastgestelde normen, dan heeft het door VeriSign opgestelde normenkader de voorkeur. Indien het onderzoeksobject geen deel uitmaakt van een Trust Netwerk en het onderzoek tot doel heeft de CUO te certificeren tegen de Europese richtlijn Elektronische Handtekening, dan heeft de ETSI TS 101456-standaard de voorkeur. Kortom, de keuze van een normenkader houdt verband met het onderzoeksobject en de opdrachtformulering, en dient in goed overleg met de opdrachtgever te worden bepaald.

Eén van de belangrijkste activiteiten tijdens de planningsfase is het analyseren en wegen van risico's die de CUO loopt. Hiervoor dient inzicht te worden verkregen

9) American National Standard Institute.
10) European Telecommunications Standards Institute.

Nr.	Organisatie	Standaard	Publiek/Privaat
1.	American National Standard Institute (ANSI)	X9.79, maart 2001	Publiek
2.	American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (AICPA/CICA)	Webtrust principles for Certification Authorities, v1.0 2001	Publiek
3.	European Electronic Signature Standardisation Initiative (EESSI)	ETSI TS 101456v1.1.1, 2000	Publiek
4.	American Bar Association	PKI Assessment Guidelines v0.30, public draft for comment, June 18, 2001	Publiek
5.	VISA	Certificate processor requirements v1.6, July 1998	Privaat
		Certificate Authority principles and procedures v1.0, March 1998	
6.	Mastercard	Security Requirements for Certificate Authorities and Payment Gateways, v1.0	Privaat
7.	Identrus	Compliance and Controls Assessment Guidelines for Express Partners, 12-8-2000	Privaat
8.	VeriSign	VeriSign Trust Network Affiliate Audit Program Guide, version 2000	Privaat

Tabel 1. Overzicht van PKI-normenkaders.

in onder andere het aantal certificaten dat in omloop is gebracht, de geldigheidsduur van een certificaat, de omgeving waarin de PKI-componenten worden geëxploiteerd, het businessmodel, het gebruik van de certificaten, het gehanteerde trustmodel, de technische inrichting van de PKI alsook de relevante PKI-componenten en -processen. Hoe meer certificaten in omloop, des te groter het risico dat hier frauduleuze handelingen mee kunnen worden uitgevoerd. Ook een risico is dat de kracht van cryptografische sleutels met lange geldigheidsduur wordt afgezwakt door nieuwe technologische ontwikkelingen. Maakt de CUO-organisatie deel uit van een gemeenschap van CUO's, een soort 'Community of Trust', dan worden beleidsdocumentatie en procedures en richtlijnen centraal beheerd en bestaat er toezicht op de handhaving van deze procedures en richtlijnen. Is er sprake van een alleenstaande CUO, dan kan deze niet gebruikmaken van de centrale beheer- en toezichtfaciliteiten die een gemeenschap van CUO's wel heeft.
Risicobepalend is tevens het businessmodel van een CUO-organisatie. Hierbij kan een onderscheid worden gemaakt in een open en een gesloten CUO-model. In een gesloten model (privaat model) kunnen procedures en richtlijnen voor eindgebruikers op een relatief eenvoudige wijze worden afgedwongen. Er kan dan bijvoorbeeld sprake zijn van een werknemer-werkgeverrelatie. In een open model (publiek model) dienen gebruikersovereenkomsten te worden opgesteld en is het afdwingen dat de eindgebruikers zich aan de procedures en richtlijnen houden moeilijker uitvoerbaar. Verder dient de IT-auditor tijdens deze fase een goed beeld te verkrijgen van de wijze waarop de certificaten worden toegepast. Worden de certificaten toegepast voor het vertrouwelijk versturen van e-mailberichten of worden zij toegepast om juridische documentatie te ondertekenen en te versturen (bijvoorbeeld een koopakte). De toepassing van de certificaten bepaalt tevens de mate van risico.

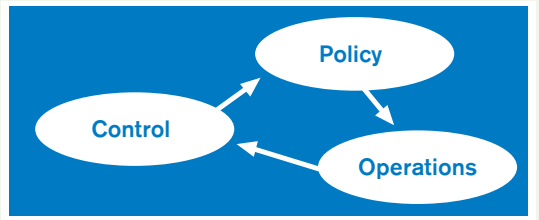
Tevens is het van belang om een goed beeld van de ICT-infrastructuur te verkrijgen. De bestaande normenkaders behandelen op dit moment nog onvoldoende de controlemaatregelen voor het beheer van firewalls, routers en webservers. Verder wordt onvoldoende aandacht besteed aan maatregelen die gericht zijn op het beheer van Unix en Windows NT. Het beoordelen van deze ICT-onderdelen dient alsnog in een onderzoek te worden meegenomen. Inzicht in de wijze waarop het trustmodel is ingericht is van belang om te kunnen bepalen op welke wijze de koppeling tussen de eindgebruiker en zijn publieke sleutel plaatsvindt en of het beheer van PKI-onderdelen van de CUO bij derden is belegd. In sommige gevallen is het RA-proces belegd bij een derde partij. Indien de afspraken tussen deze partijen niet goed zijn gespecificeerd en geïmplementeerd, ontstaat een verhoogd risico.

Sommige CUO's hebben bepaalde processen niet ingericht, zoals bijvoorbeeld key escrow[11]. Tijdens de planningsfase is het van belang te bepalen in hoeverre bepaalde PKI-processen van toepassing zijn op de inrichting van de CA-omgeving.

11) Key escrow is het opslaan van cryptografische sleutels bij derden.

Tijdens de planningsfase kan door gebruik te maken van een vragenlijst die door het management van de CUO zelf is ingevuld, al een globaal inzicht in de getroffen maatregelen worden verkregen. Voor elk onderzoeksobject dient het management aan te geven welke documentatie aanwezig is (beleidsdocumentatie en/of procedures). De Certification Practice Statement (CPS) kan worden gehanteerd ter controle op de verklaring die het management geeft.

De wijze waarop gerapporteerd wordt omtrent de betrouwbare inrichting van de PKI hangt af van de vraag of de bevindingen van het onderzoek voor intern gebruik worden gehanteerd (om de kwaliteit van de inrichting te bepalen) of dat de resultaten van het onderzoek naar externe partijen worden gecommuniceerd (het verkrijgen van vertrouwen). Zie hiervoor figuur 2.



Intern om de kwaliteit te waarborgen
- Het beoordelen van de beleidsdocumentatie ten opzichte van het normenkader.
- Het beoordelen in hoeverre de geïmplementeerde maatregelen voldoen aan de beleidsdocumentatie en internationale standaarden.

Extern om vertrouwen te realiseren
- Door middel van een Third Party Statement.
- Door middel van certificering tegen de Europese richtlijn Elektronische Handtekening.

Figuur 2. Interne rapportage en externe rapportage.

Resultaat van de planningsfase is een auditplan waarin activiteiten voor het uitvoeren van de audit worden beschreven.

Uitvoering

Om de kwaliteit (betrouwbaarheid, beschikbaarheid, controleerbaarheid en beheersbaarheid) van de getroffen maatregelen binnen een CUO te kunnen beoordelen, is het van belang dat tijdens de uitvoering van de audit inzicht wordt verkregen in de opzet en het bestaan van de door de CUO-organisatie geïmplementeerde maatregelen en procedures. Bij het beoordelen van de opzet wordt onderzocht in hoeverre de procedures volledig zijn en of de kwaliteit van alle procedures en maatregelen voldoende is. Vervolgens moet het bestaan van deze maatregelen en procedures worden bepaald. Hierbij wordt onderzocht in hoeverre ook volgens de in opzet beschreven procedures en maatregelen wordt gewerkt. Indien met de opdrachtgever is afgesproken om ook de werking van de maatregelen te beoordelen, dient over een bepaalde periode te worden onderzocht in hoeverre de ingerichte maatregelen toereikend zijn om aan de doelstellingen te kunnen voldoen. Hieronder is een overzicht van de uit te voeren auditactiviteiten gegeven.

Om inzicht in de opzet van de gehanteerde maatregelen en procedures te verkrijgen, moeten de volgende activiteiten worden verricht:
* Stel vragen aan het CUO-management en operationeel CA/RA-personeel omtrent de inrichting van de geïmplementeerde maatregelen.
* Bekijk de selfassessment vragenlijst die door het CA/RA-personeel is ingevuld en vergelijk deze met de toepasselijke onderdelen in de CPS, CP's en CA/RA operationele documentatie.
* Beoordeel de CPS, CP en CA/RA operationele documentatie op onderdelen daar waar het CA-personeel de selfassessment vragenlijst niet heeft ingevuld.
* Beoordeel de leveranciersdocumentatie van de CA-software.

Om inzicht in het bestaan van de maatregelen en procedures te verkrijgen, moeten de volgende activiteiten worden verricht:
* Neem de uitvoering van de maatregelen en procedures waar en bepaal in hoeverre deze maatregelen en procedures worden uitgevoerd zoals beschreven in de CPS, CP en CA/RA operationele documentatie.
* Indien een waarneming van de uitvoering van de CA/RA-maatregelen en -procedures niet mogelijk is, bepaal dan door middel van het uitvoeren van interviews met CA/RA-personeel in hoeverre de maatregelen en procedures worden uitgevoerd zoals beschreven in de CPS, CP en CA/RA operationele documentatie.

Om te kunnen bepalen in hoeverre de in opzet en bestaan gehanteerde maatregelen en procedures van voldoende niveau zijn, dienen de volgende activiteiten te worden uitgevoerd:
* Vergelijk de gehanteerde CA/RA-maatregelen en -procedures met de normen zoals die in het gehanteerde normenkader staan vermeld.
* Bespreek het niveau van de aangetroffen maatregelen binnen het auditteam.
* Raadpleeg indien noodzakelijk referentiemateriaal om het niveau van de gehanteerde CA/RA-maatregelen en -procedures te kunnen beoordelen.

Om de werking van de maatregelen en procedures te kunnen bepalen, moeten binnen een vastomlijnde tijdsperiode de volgende activiteiten worden uitgevoerd:
* Ontwikkel testprocedures om de werking van de maatregelen en procedures te kunnen testen.
* Verzamel documentatie, rapportages en gespreksverslagen.
* Neem de uitvoering van de maatregelen en procedures waar.
* Herhaal binnen de tijdsperiode controleactiviteiten.

Voor de dossiervorming is het van belang om tijdens de beoordeling voldoende bewijsmateriaal te verzamelen. Denk hierbij onder andere aan papieren registraties van aanvragen voor certificaten en vastlegging van de CA-sleutelceremonie die heeft plaatsgevonden. Voor elk van de onderzoeksobjecten en bijbehorende processen (zie tabel 2) moeten in opzet en bestaan de ingerichte maatregelen op hun kwaliteit worden beoordeeld.

CA-omgevingsmaatregelen
* Beveiligingsbeleid
* Beveiligingsorganisatie
* Classificatie en beheer van bedrijfsmiddelen
* Beveiligingseisen t.a.v. personeel
* Fysieke beveiliging
* Systeem- en netwerkmanagement
* Logische toegangsbeveiliging
* Systeemontwikkeling en -onderhoud
* Continuïteitsmanagement
* Naleving

CA-sleutelbeheer
* CA-sleutelgeneratie
* CA-sleutelopslag en herstel
* CA-sleuteldistributie
* CA-sleutelvernietiging
* CA-cryptobeheer

Certificaatmanagement
* Certificaatregistratie
* Certificaatvernieuwing
* Certificaatintrekking en Certificate Revocation List (CRL)-verwerking

Ontsluiting van beheer en beleidsdocumentatie
* Certification Practise Statement
* Certificate Policy

Tabel 2. Onderzoeksobjecten.

Indien op bepaalde onderdelen geen organisatiespecifieke beleidsdocumentatie en/of procedures aanwezig zijn, kan de documentatie van de softwareleverancier wellicht uitkomst bieden.

Belangrijke documenten om inzicht te verkrijgen in de getroffen maatregelen zijn onder andere:
* overzicht van de PKI ICT-architectuur;
* Certification Practice Statement/Certificate Policy;
* beschrijving van het beveiligingsbeleid;
* overzicht van fysieke beveiligingsmaatregelen;
* contracten tussen de CA en externe partijen;
* beschrijving van incidentmanagementprocedures;
* continuïteitsplannen en scenario's (CA-dienst beëindigingsmaatregelen);
* functie- en taakomschrijving (CA vertrouwelijke rollen en verantwoordelijkheden);
* beschrijving van certificaataanmeldings- en registratieprocedures;
* beschrijving van CA-sleutelbeheerprocedures.

Rapportage

Rapportages voor intern gebruik ter bepaling van de kwaliteit van de inrichting zijn bestemd voor het management van de CUO-organisatie. In geval van het uitbesteden van het beheer van onderdelen van de PKI is deze rapportage bestemd voor de organisatie die juridisch de eindverantwoordelijkheid draagt voor het uitgeven van de digitale certificaten. De bevindingen gaan gepaard met een management letter waarin eventuele aanbevelingen omtrent de inrichting worden beschreven. Indien de inrichting van de PKI voldoende betrouwbaar wordt geacht, zal een verklaring worden afgegeven.

Voor rapportage voor extern gebruik (het verkrijgen van vertrouwen) kan een Third Party Mededeling worden afgegeven. Deze verklaring kan naar alle relaties van de CUO-organisatie worden gecommuniceerd. Tevens kan een deel van de rapportage op de website van de CUO worden geplaatst. Verder bestaat nog de mogelijkheid om een gedeelte van de dienstverlening van de CUO te certificeren tegen de Europese richtlijn Elektronische Handtekening. Welke vorm van rapportage wordt gekozen, is afhankelijk van het businessmodel van de CUO-organisatie en het doel van het onderzoek. Hieronder worden beide vormen van externe rapportage kort toegelicht.

Third Party Mededeling

Een Third Party Mededeling (TPM) is een verklaring van een onafhankelijke derde partij omtrent de kwaliteit van de door de serviceorganisatie getroffen interne maatregelen ten behoeve van haar IT-dienstverlening, zoals CA-services en RA-services van een CUO-organisatie. De normen die worden gehanteerd, kunnen uit diverse normenkaders zijn samengesteld en zijn in de bijlage van de TPM-rapportage opgenomen. Onderdelen van een TPM[12] zijn minimaal het oordeel en een bijlage met een beschrijving van de dienstverlening en de internecontrolestructuur, inclusief een beschrijving van de gehanteerde controledoelstellingen.

12) P. Veltman RE RA, *Third party review en -mededeling bij uitbesteden van IT-services*, Compact, september 1995.

De OPTA zal verantwoordelijk worden voor het registreren van Certificaat Uitgevende Organisaties die gekwalificeerde certificaten uitgeven.

Bij eventuele vragen of externe onderzoeken van klanten en vertrouwende partijen kan door de serviceorganisatie worden verwezen naar deze TPM-verklaring. Hierdoor wordt de belasting van het meewerken aan vele externe onderzoeken voor de serviceorganisatie verminderd. Dit heeft een positief effect op medewerkers én klanten van de serviceorganisatie. Periodiek dienen onderhoudsaudits te worden gepleegd, dit om de naleving van TPM-eisen te kunnen toetsen.

Certificering van CUO's

Heel actueel is op dit moment het certificeren van Certification Service Providers (CSP's)[13] ofwel Certificaat Uitgevende Organisaties (CUO's) tegen de Europese richtlijn Elektronische Handtekening. Deze richtlijn is in 1999 binnen de Europese Unie opgesteld om elektronische handel te stimuleren en het gebruik van elektronische handtekeningen te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. Hierbij wordt een onderscheid gemaakt tussen een 'gewone' en een geavanceerde elektronische handtekening. De richtlijn stelt dat een geavanceerde elektronische handtekening een gelijke mate van rechtskracht bezit als een handgeschreven handtekening. De gewone elektronische handtekening (denk hierbij aan een gescande handtekening) mag tijdens een juridisch dispuut geen rechtsgeldigheid worden ontzegd omdat zij niet aan de voorwaarden voor een geavanceerde elektronische handtekening voldoet.

13) CSP's zijn organisaties die gekwalificeerde digitale certificaten uitgeven en hierbij gebruikmaken van een PKI. De verschillende PKI-componenten kunnen bij verschillende organisaties in beheer zijn.

14) Mw. A.C. Gräve, *Consequenties van de Wbp voor de bestuurlijke informatievoorziening*, Compact 2001/4.

Met welke methodiek een geavanceerde elektronische handtekening dient te worden gegenereerd, is niet beschreven in de Europese richtlijn. Wel worden eisen gesteld aan het genereren van een geavanceerde elektronische handtekening. Deze eisen zijn geformuleerd in de bijlage van de richtlijn. Indirect wordt ervan uitgegaan dat digitale (gekwalificeerde) certificaten bij het genereren van geavanceerde elektronische handtekeningen worden gehanteerd. Gekwalificeerd wil zeggen dat deze certificaten met meer waarborgen zijn gegenereerd. In bijlage I van de richtlijn zijn eisen gedefinieerd aan de opbouw van gekwalificeerde certificaten. Bijlage II stelt eisen aan de certificatiedienstverleners die gekwalificeerde certificaten afgeven en bijlage III stelt eisen aan de veilige middelen (smartcards/tokens) voor het aanmaken van elektronische handtekeningen.

Elk land binnen de Europese Unie moet wetgeving opstellen waarmee aan de Europese richtlijn wordt voldaan. Sommige landen hebben al wel certificeringsschema's opgesteld. In Nederland zal de OPTA verantwoordelijk worden voor het registreren van CSP's die gekwalificeerde certificaten uitgeven. Een certificeringsschema is door ECP.nl/TTP.nl opgesteld. Als toetsingskader wordt hierbij de door de EESSI-werkgroep opgestelde ETSI TS 101456-standaard gehanteerd.

KPMG is één van de certificerende instellingen die een dergelijk ECP.nl compliance-certificaat kan gaan uitgeven. Er is op dit moment geen verplichting tot certificering tegen de Europese richtlijn, maar door het verkrijgen van een certificaat wordt wel uiting gegeven aan het voor klanten en vertrouwende partijen zo belangrijke vertrouwensniveau van een CUO.

Praktijkervaringen

Veel CUO's zijn nog niet klaar voor certificering. Vaak schort het nog op het vlak van continuïteitsmaatregelen, het vastleggen van procedures en richtlijnen en de implementatie van de beveiligings- en risicomanagementprocessen. Procedures en maatregelen voor het geval dat een CA-sleutel wordt gecompromitteerd of dat de CA-dienstverlening wordt beëindigd, zijn veelal niet gedocumenteerd. Hierdoor ontstaat het risico dat de betrouwbaarheid en de continuïteit van de dienstverlening in gevaar komen, wat eventueel kan leiden tot het verlies van klanten of tot rechtszaken van gebruikers van oude certificaten.

In PKI-normenkaders is er onvoldoende aandacht voor het beoordelen van de ICT-infrastructuur waarvan de PKI gebruikmaakt. Hierbij moet worden gedacht aan penetratietests en aan het beoordelen van baselines en configuraties van firewalls, routers en besturingssystemen als Windows NT.

Verder dient tijdens het onderzoek rekening te worden gehouden met de Wet bescherming persoonsgegevens (Wbp). De verwerking van persoonsgegevens uit hoofde van het uitgeven van certificaten valt onder de privacywetgeving. Betrokkenen waarvan de gegevens zijn geregistreerd hebben rechten[14], zoals het recht op informatie of en zo ja welke gegevens worden verwerkt, het recht

op informatie omtrent het doel van de gegevensverwerking, en het recht op correctie en verwijdering van gegevens indien de gegevens niet juist of onvolledig zijn. Organisaties die persoonsgegevens verwerken hebben op hun beurt weer plichten, zoals de plicht om mee te werken zodat betrokkenen hun rechten kunnen uitoefenen, en de plicht om betrokkenen in kennis te stellen van het doel waarvoor gegevens worden verwerkt. Deze rechten en plichten hebben organisatorische en procedurele consequenties voor organisaties die bij het uitgeven van digitale certificaten persoonsgegevens verwerken.

Samenvatting en conclusie

Geconcludeerd kan worden dat er voor het uitvoeren van een onderzoek naar de kwaliteit (betrouwbaarheid, beschikbaarheid, controleerbaarheid en beheersbaarheid) van de binnen een CUO-organisatie (CA en RA) getroffen maatregelen een grote verscheidenheid aan PKI-normenkaders bestaat. Het onderzoeksobject, het doel van het onderzoek en de status van het normenkader bepalen in grote mate de keuze van het te hanteren PKI-normenkader. Inzicht verkrijgen in de opbouw van de CUO-organisatie is van groot belang voor het opzetten van het auditplan. De verschillende PKI-processen en het beheer van de PKI-componenten kunnen zijn verdeeld over meerdere organisaties. Hierdoor gaat tijdens het onderzoek de beoordeling van opgestelde contracten en het waarborgen van het nakomen van de gemaakte afspraken tussen deze partijen een grotere rol spelen. Door het toenemende financiële belang van internettransacties zal het doel van het uitvoeren van een onderzoek naar de kwaliteit van maatregelen binnen een CUO-organisatie naar verwachting steeds meer verschuiven richting het verstrekken van vertrouwen naar externe partijen, waardoor het uitvoeren van TPM- en certificeringsonderzoeken aan populariteit zal winnen.

Literatuur

Carlisle Adams en Steven Lloyd, *Understanding the Public Key Infrastructure*, 31 december 1999.

American Bar Association (ABA), *PKI assessment Guidelines v0.30*, public draft for comment, June 18, 2001.

American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants (AICPA/CICA), *Webtrust principles for Certification Authorities, v1.0*, 2001.

American National Standard Institute (ANSI), *X9.79*, March 2001.

BS 7799: 1995 *Code of Practise for Information Security Management*.

S. Chokhani en W. Ford, *Internet Public Key Infrastructure Certificate Policy and Certification Practise Statement Framework*, Internet Draft, 1997.

European Electronic Signature Standardisation Initiative (EESSI), *ETSI TS 101456v1.1.1*, 2000.

W. Ford en M. Baum, *Secure Electronic Commerce, Building the infrastructure for digital signatures of encryption*, Upper Saddle River, New Jersey, Prentice Hall PTR 1997.

Mw. A.C. Gräve, *Consequenties van de Wbp voor de bestuurlijke informatievoorziening*, Compact 2001/4.

Identrus, *Compliance and Controls Assessment Guidelines For Express Partners*, 12-08-2000.

Mastercard, *Security Requirements for Certificate Authorities and Payment Gateways, v1.0*.

Andrew Nash, William Duance, Celia Joseph en Derek Brink, *PKI implementing and managing e-security*, RSA press, 2001.

P. Veltman RE RA, *Third party review en -mededeling bij uitbesteden van IT-services*, Compact, september 1995.

VeriSign, *VeriSign Trust Network Affiliate Audit Program Guide, version 1.0*, 2000.

VISA, *Certificate Authority principles and procedures v1.0*, March 1998.

VISA, *Certificate processor requirements v1.6*, July 1998.

Drs. P.A. van Walsem is als IT-auditor werkzaam bij KPMG Information Risk Management. Zijn aandachtsgebied ligt bij het advies voor en de audit van e-businessprocessen en -systemen. Daarnaast heeft hij zich gespecialiseerd in het beoordelen en certificeren van Public Key Infrastructures (PKI). Uit dien hoofde is hij betrokken geweest bij het opzetten van de Internationale KPMG PKI Rapid Deployment Methodologie en de Internationale KPMG PKI Audit Methodologie.