Invoering van één toegangspas

Op weg naar één corporate identiteit

Ir. A.J.M. Veltmeijer CISA
is de Information Security Officer voor KPMG Nederland. Vanuit de Office of the CIO heeft hij vanaf 2003 ook de rollen van IT Security Manager en IT Security Officer vervuld. Van 1999 tot 2003 was hij werkzaam als IT-Audit Manager bij KPMG IT Advisory. Tevens doceert hij colleges cryptografie en sleutelbeheer aan de post-academische EDP-Audit opleiding van de VU.

veltmeijer.amand@kpmg.nl

Ir. Amand Veltmeijer CISA

In 2008 is binnen KPMG Nederland een nieuwe identiteitspas ingevoerd voor de fysieke toegangscontrole. Na de invoering van persoonsgebonden certificaten op de contactchip van de pas, de corporate identiteitspas, zijn daar begin 2009 IT-beveiligingstoepassingen aan toegevoegd.
De invoering van de kaart is nagenoeg uniek door de landelijke invoering voor alle medewerkers en voor alle kantoren. De leermomenten uit de praktijk bij invoering van deze hybride corporate identiteitspas met persoonsgebonden certificaten en met gebruikmaking van een Managed PKI, worden in dit artikel met u gedeeld.

Inleiding

In dit artikel wordt ingegaan op de invoering van de corporate identiteitspas binnen KPMG Nederland. Deze kaart is voor medewerkers zowel de fysieke toegangspas tot gebouwen en ruimten alsook de elektronische identiteitspas voor gebruik van IT-beveiligingsfuncties.
Voor de IT-beveiligingsfuncties is de kaart voorzien van een contactchip met certificaten en is een Managed Public Key Infrastructuur gerealiseerd ([Getro5]). Vanuit de IT Security dienstverlening van KPMG is dit artikel deels een voorbeeld van 'Drinking Your Own Champagne' ([KPMG07]).

Ten aanzien van de corporate identiteitspas verschilt KPMG niet van andere organisaties, met dezelfde interne issues bij het streven naar en de realisatie van verbeteringen in de interne bedrijfsvoering door inzet van informatietechnologie en door integratie van processen en diensten.
De interne beschikbaarheid van de juiste kennis en ervaring op dit gebied heeft de afgelopen jaren bijgedragen aan het huidige succesvolle resultaat, een geïntegreerde aanpak voor één identiteitspas voor fysieke én IT-beveiligingstoepassingen.

Afzonderlijke business cases waren te klein om de noodzakelijke investering te rechtvaardigen

Allereerst wordt in dit artikel kort de voorgeschiedenis geschetst die leidde tot de uiteindelijke ontwikkeling en realisatie van de Public Key Infrastructuur (PKI) met de corporate identiteitspas als drager. Daarna wordt de ontwikkeling beschreven, eerst door kenmerkende werkwijzen en achtereenvolgens aan de hand van het invoeringstraject, de processen en de technologie. Enkele belangrijke leermomenten uit het interne ontwikkelingstraject volgen dan onder de kop 'Lessons learned'. Afgesloten wordt met conclusies voor ontwikkelingen van vergelijkbare corporate identiteitspassen.

Historie en uiteindelijke business case

In het begin van dit millennium werd binnen KPMG al gewerkt aan de opzet van een eigen PKI. Net als de jaren daaropvolgend waren echter de business cases ieder afzonderlijk te klein om de noodzakelijke investering te rechtvaardigen en konden verschillende potentiële PKI-toepassingen – zoals de interne verwerking van gevoelige (HR-) gegevens, communicatie met externe partijen waaronder banken en de AFM en gebruik van extranetten – onvoldoende worden samengevoegd tot één sluitende overall business case.

Behalve de kosten beperkte ook het geringe aantal toepassingen waarbinnen gebruik kon worden gemaakt van certificaten de invoering. Ook de PKI-technieken en -diensten waren minder uitontwikkeld dan tegenwoordig, waardoor te veel specifieke aanpassingen nodig waren om applicaties eenvoudig geschikt te maken voor eindgebruikers.

Vanaf 2005/2006 werd één toepassing, beveiligd e-mailen, in toenemende mate een drijfveer voor ontwikkeling van de certificaatinfrastructuur binnen KPMG Nederland ([Meen01]). Deeloplossingen voor beveiligd e-mailen waren wel al voorhanden, maar aspecten als gebruiksgemak, digitale ondertekening en beveiliging tot en met de mailbox werden hiermee onvoldoende ingevuld.
In verschillende achtereenvolgende pilots is vervolgens kennis en ervaring opgebouwd over beveiligd e-mailen met verschillende technieken, wijzen van implementeren en het gebruik van certificaatdiensten binnen de eigen IT-omgeving. Daarbij werden behalve ondersteuning van de gebruikers voor naleving van het e-mailbeleid ook andere toepassingen bekeken, met name het ondertekenen van (pdf-)documenten en verbetering van interne processen waarbinnen strikt vertrouwelijke informatie wordt verwerkt.

IT-ontwikkelingen

Verschillende IT-ontwikkelingen vormden uiteindelijk – gecombineerd met beveiligde e-mail – de aanzet tot de finale ontwikkeling, de realisatie van de Managed PKI-dienstverlening met gebruikmaking van de toegangspas als drager voor de certificaten.

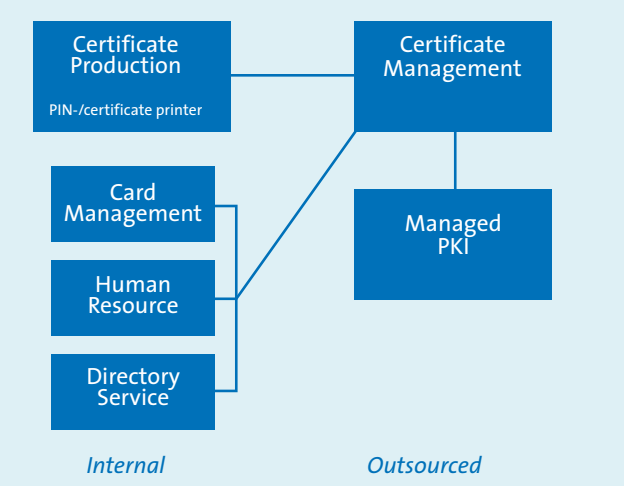
Belangrijke ontwikkelingen waren de invoering van draadloze netwerken en de uitvoering van het ICT/communicatiebeleid. Voor het gebruik van draadloze netwerken binnen kantoren is het gebruik van certificaten een vereiste vanuit dit beleid. Uitvoering van het communicatiebeleid – connectivity at any place, any where en Single Sign-On voor de werkplek – resulteerde in de wens tot één uniform authenticatiemiddel.
Door de toegenomen kennis van en ervaring met andere Managed PKI-diensten, zoals voor SSL/TLS-servicecertificaten voor beveiliging van e-mail tussen organisaties, was de jaren daarvoor ook de kennis en ervaring in de organisatie over PKI in de breedte toegenomen.
Een overkoepelend programma ter algehele verbetering van de IT-infrastructuur vormde tenslotte het organisatorische en financiële vehikel waarbinnen de plannen uiteindelijk werden uitgevoerd. Binnen dit programma werd de samenwerking tussen facilitaire dienst en de IT-organisatie verankerd binnen verschillende deelprojecten. De nieuwe dienst is duidelijk neergezet als onderdeel en uitbreiding van de basis IT-infrastructuur.

Als laatste, maar zeker niet de minst belangrijke reden voor de uiteindelijke ontwikkeling van de dienstverlening moeten de acceptabele prijsstelling voor de certificaten en de daling van de kosten voor realisatie worden genoemd. Dit laatste in het bijzonder door gebruik van zo veel mogelijk standaardsystemen en outsourced en/of managed services. In figuur 1 zijn de interne en uitbestede systeemcomponenten aangegeven.

Ontwikkeling

Zowel voor de ontwikkeling van een bedrijfsbrede PKI alsook voor de ontwikkeling van een identiteitspas waren de risico's bekend ([Naza01], [Velt01]). Om bekende risico's bij de ontwikkeling zoveel mogelijk te vermijden werden eerst de ervaringen uit voorgaande pilots vastgelegd in uitgangspunten, randvoorwaarden en verdere afbakening van de scope.

Deze werden vooraf besproken met de potentiële leverancier van de certificaatdiensten. Daarbij werden ook de visie en te volgen werkwijze definitief afgestemd. Hierdoor kon worden



Figuur 1. **Belangrijkste systemen voor productie van certificaten op de corporate identiteitspas.**

gewerkt met een ambitieuze tijdsplanning. Kernpunten van de gevolgde werkwijze daarbij zijn:

- De toepassingen waarbinnen certificaten de eerste twee jaar zouden (kunnen) worden ingezet, werden expliciet benoemd. Tijdens de gehele ontwikkeling werd rekening gehouden met het (toekomstige) gebruik binnen deze toepassingen. Elk ander mogelijk gebruik werd resoluut buiten het project geparkeerd.
- Enkel het volledige gebruik en beheer voor de eerste toepassing, beveiliging van e-mail, werd volledig uitgewerkt in het project. Ten aanzien van andere initieel bepaalde toepassingen werd in zoverre gekeken naar het gebruik en beheer dat de tijdens de ontwikkeling te maken keuzen daar geen negatieve invloed op zouden hebben.
- Er werd een strakke fasering aangehouden waarin na realisatie van het ontwerp snel een basisinfrastructuur aanwezig moest zijn om certificaten op de identiteitspas geplaatst te hebben. Dit diende gerealiseerd te zijn voordat de nieuwe pas ten behoeve van de fysieke toegangscontrole aan gebruikers zou worden verstrekt.
- Ten aanzien van het waarborgen van het betrouwbaarheidsniveau van de gehele PKI is het altijd bepalend geweest dat de uit te geven certificaten eenvoudig zouden moeten zijn op te waarderen tot gekwalificeerde certificaten (certificaten die voldoen aan eisen die vanuit de Wet Elektronische Handtekening worden gesteld om een elektronische handtekening te kunnen plaatsen die dezelfde rechtsgevolgen heeft als een handgeschreven handtekening).

Duidelijk was dat een definitieve keuze voor gekwalificeerde certificaten financieel niet haalbaar zou zijn voor de beoogde brede uitrol. Afhankelijk van andere externe ontwikkelingen zouden gekwalificeerde certificaten in de toekomst wel een eis kunnen zijn voor bepaalde doelgroepen en nog te realiseren gebruik.
Voorbeelden van keuzen die hieruit voortkomen zijn de keuze van de smartcard als SSCD (Secure Signature Creation Device) en de keuze van een provider die tevens gekwalificeerde certificaten kan leveren conform de eisen van de PKI-Overheid ([Walso2]).

Invoering

Toegangspas

Binnen het programma ter verbetering van de IT-infrastructuur waren onder andere de volgende twee deelprojecten gedefinieerd: 1. invoering van een nieuw toegangscontrolesysteem met de nieuwe toegangspas, en 2. invoering van de elektronische identiteitspas. Hierdoor konden op het juiste moment de eisen en wensen binnen de separate ontwikkelingstrajecten worden afgestemd. Voorbeelden waarbij de afstemming essentieel was zijn: de keuze om alle medewerkers te voorzien van de nieuwe kaart, de keuze voor embedding van de contactchip op de kaart en de initieel batchgewijze productie van de kaart en de certificaten.

Gedurende 2008 werd de nieuwe toegangspas per locatie uitgerold. De basisinfrastructuur was nog niet gereed op het moment dat de passen voor de eerste drie locaties werden uitgerold. Hierdoor waren separate terugroepacties nodig om de passen te voorzien van certificaten en sleutels.

Elektronische corporate identiteitspas

Op grond van eerdere ervaringen bij invoering van PKI voor beveiliging van e-mail, is er veel aandacht besteed aan de invoering bij de eindgebruikers. Voor gebruikers diende de invoering van de beveiligingsfuncties zo transparant mogelijk plaats te vinden, met een absoluut minimum aan verstoring van werkzaamheden en zo gebruiksvriendelijk mogelijk.

Zo is al in een zeer vroeg stadium een smartcardlezer toegevoegd aan de eisen voor nieuwe laptops. Hierdoor waren ruim voor de invoering de meeste gebruikers in stilte – via reguliere vervangingen van laptops – voorzien van een kaartlezer. Overige pc's werden naderhand voorzien van losse smartcardlezers.

Bij de uitrol van de fysieke toegangspas – eventueel via separate terugroepacties – was deze pas (de nieuwe corporate identiteitspas) voorzien van persoonlijke certificaten. Pas nadat alle gebruikers waren voorzien van de nieuwe elektronische identiteitspas en nadat de laatste aanpassingen in de infrastructuur hadden plaatsgevonden, werden de pincodes verstuurd en werd breed gecommuniceerd over de 'Corporate ID-Smartcard' en de eerste toepassing, het beveiligen van e-mail.

Toepassingen

De uitrol vond plaats in het kader van de nieuwe functionaliteit, het beveiligd e-mailen met gebruikmaking van de certificaten op de corporate identiteitspas. De overige geplande toepassingen werden daarbij enkel kort benoemd.

De beveiligde e-mailapplicatie bepaalde het gezicht, en daarmee voor een groot deel de acceptatie, van de identiteitspas bij de gebruikers. Om een zo breed mogelijke acceptatie te realiseren

Het is mogelijk om in één jaar tijd een volledige public key infrastructuur op te zetten en in gebruik te nemen

is bij invoering veel aandacht uitgegaan naar ondersteuning van het gebruik voor de applicatie. Aspecten die daartoe bijdroegen waren:

- Vrijwillig gebruik van de pas bij invoering en gebruik voor de eerste applicatie. Het accent lag op het ondersteunen van gebruikers bij invulling van het beleid ten aanzien van het beveiligd versturen van e-mail.
- Gerichte communicatie over de nieuwe mogelijkheden met doelgroepen waarvan bekend was dat ze er veel voordeel bij konden hebben in hun dagelijkse werkzaamheden en voor verbetering van de interne processen.
- Ondersteuning door het hoogste management in de vorm van een voortrekkersrol bij daadwerkelijk brede verspreiding van beveiligde interne e-mail.
- Verbeterde communicatie over de verschillende mogelijkheden om e-mail te beveiligen. De pas is niet in alle situaties de optimale oplossing voor beveiliging van e-mail. Door per situatie alternatieven aan te reiken wordt voorkomen dat de pas als het nieuwe verplichte IT-middel of 'speeltje' van de IT-organisatie wordt gezien.

Door de wijze van geleidelijke invoering van de kaart is deze invoering in zekere zin pas afgerond als er binnen alle geplande toepassingen gebruik van kan worden gemaakt. Het begeleiden en stimuleren van gebruik binnen processen en toepassingen gaat tot die tijd door.

Processen

Het tijdspad bij invoering van de persoonlijke certificaten werd in grote mate bepaald door de invoering van de fysieke toegangspas. Dit was weliswaar voortgekomen uit de noodzaak om tot één identiteitspas te komen, maar bood in praktijk het voordeel van de juiste tijdsdruk om op tijd de basisinfrastructuur gereed te hebben (zie ook 'Lessons learned').

Daardoor was er onvoldoende tijd om de processen in detail uit te werken en te integreren in bestaande levenscyclusprocessen van de toegangspas. De processen voor de certificaatdiensten werden separaat opgezet – met kennis over de bestaande smartcard levenscyclusprocessen – en naderhand gecombineerd met de reeds bestaande processen binnen de facilitaire dienst. Door de centrale benadering van beide processen en fysiek nabije huisvesting van beide organisatieonderdelen verliep dit zonder al te veel problemen. Hierdoor is wel – uit noodzaak – een gescheiden ontwikkeling van de productie en processen voor de fysieke toegangspas en voor de certificaten ontstaan. In de praktijk is dit een succesfactor gebleken voor een efficiënte en effectieve opzet, realisatie en invoering van de gecombineerde CID-Smartcard. Voor regulier beheer van de gecombineerde kaart is dit echter geen wenselijke situatie.

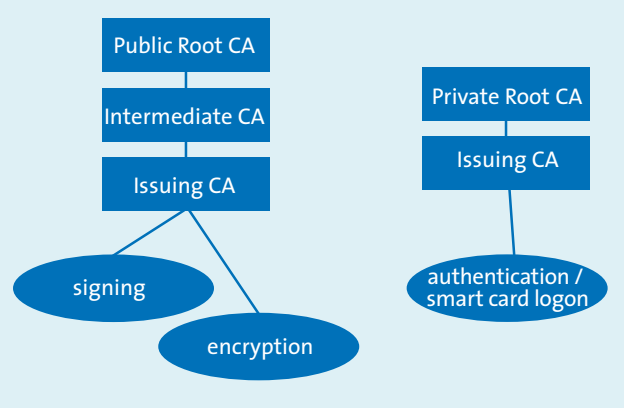
Met de toename van de kennis en ervaring van de processen en systemen bij beide organisatieonderdelen wordt daarom voorzien dat de reguliere kaartprocessen geheel door één dienst (facilitair) zullen worden uitgevoerd. Door de benodigde specialistische kennis van informatiesystemen en certificaatdiensten zal voor de tweedelijnsondersteuning de IT-organisatie verantwoordelijk blijven. Gepland staat dan ook een uitvoering van het gehele productieproces onder één verantwoordelijk organisatieonderdeel. Op termijn zal de volgende integratiestap, combinatie van de twee verschillende productiesystemen in één systeem, eenvoudig te realiseren zijn door de opgedane ervaring.

De afstemming binnen het gehele proces tussen alle betrokken partijen, intern en extern, zal de komende periode vooralsnog een belangrijk aandachtspunt blijven om het proces verder te verbeteren.

Technologie

In deze paragraaf worden de belangrijkste technische kenmerken van de geïmplementeerde corporate identiteitspas opgesomd. Enige basiskennis van PKI is daarbij handig maar niet noodzakelijk voor begrip van het gehele artikel.

- De identiteitspas is voorzien van twee antennes ter ondersteuning van diverse systemen voor fysieke toegangscontrole en een contactchip voor de IT-beveiligingsfuncties. De pas is verder voorzien van een pasfoto, de naam van de pashouder en een holografische laag.
- Op de contactchip van de identiteitspas bevinden zich drie certificaat/private key paren: voor digitaal ondertekenen (signing), voor versleutelen (encryption) en voor authenticatie (client authentication / smartcard-logon). In figuur 2 is de PKI-hiërarchie weergegeven.
- De signing- en encryptioncertificaten worden uitgegeven binnen één publieke PKI (Getronics/Verisign). Doordat de root Certificate Authorities (CA's) van deze PKI door de meeste systemen als trusted worden aangemerkt, is daarmee geborgd dat er voor externe uitwisseling van beveiligde e-mail en documenten geen extra trustrelaties hoeven te worden gerealiseerd. Het wel of niet functioneren van de externe uitwisseling wordt verder bepaald door de ondersteuning van (persoonlijke) certificaten binnen de specifieke toepassing in de externe IT-omgeving.
- Het authenticatiecertificaat wordt uitgegeven binnen een private PKI. Aanloggen met de corporate identiteitspas op wil-



Figuur 2. **De PKI-hiërarchie met signing- en encryptioncertificaten uitgegeven onder een public PKI en authentication/smart card-logoncertificaten uitgegeven onder een private PKI.**

lekeurige informatiesystemen is immers enkel wenselijk indien de trust expliciet is aangebracht. Publicatie van revocations (intrekking of herroeping van de geldigheid van een certificaat) voor externe partijen is ook niet noodzakelijk, in tegenstelling tot de onder een publieke PKI uitgegeven certificaten.

- De certificaat/sleutelparen worden alle drie in alle lifecycle- en beheerprocessen als één geheel verwerkt. Zo worden ze alle drie bij productie gelijk op de kaart geplaatst en heeft een intrekking van de kaart een revocation van alle drie de certificaten tot gevolg. Het enige punt waarbij een certificaat individueel wordt verwerkt, is de recovery van het encryptiecertificaat. Voor specifieke recoveryverzoeken kan het encryptiecertificaat op een blanco kaart worden geplaatst volgens strikte procedures.
- Bij vervanging van de pas worden de certificaten automatisch vernieuwd en worden oude encryptiecertificaten op de pas bijgeplaatst.
- De geldigheidstermijn van de certificaten is gelijkgesteld aan de vervangingsperiode van de fysieke pas om de overlast van extra verwerkingen voor gebruikers te minimaliseren.
- De essentiële PKI-componenten zoals alle CA's en het certificaatbeheersysteem worden gehost en beheerd door Getronics. KPMG heeft een Registration Authority (RA)-deelrol die technisch wordt ingevuld met een dedicated werkstation voor het certificaatbeheersysteem. Dit werkstation is verder voorzien van de nodige kaartlezers, een kaartprinter voor productie van de certificaten en een printer voor de pinmailers.
- Binnen het Certificaat Management Systeem zijn naast de gebruikersrol – voor productie van de certificaten – onder andere rollen gedefinieerd voor het resetten van pincodes door de helpdesk en rollen voor het verwerken van vertrouwelijke informatie en het uitvoeren van specifieke beheerhandelingen.

Lessons learned

Hieronder worden enkele leermomenten aangegeven uit het ontwikkelings- en invoeringstraject van de corporate identiteitspas bij KPMG.

Het feit dat op veel deelgebieden de kennis en ervaring binnen de organisatie aanwezig is betekent niet automatisch dat genoemde punten en gerelateerde risico's konden worden voorzien of konden worden voorkomen. Daarvoor zijn er te veel omgevingsfactoren en relaties met andere (interne) ontwikkelingen die niet konden worden beïnvloed, zoals het ontstaan van een economische crisis gedurende het project.

De totale opzet en invoering van de elektronische identiteitspas had uiteindelijk een doorlooptijd van ruim één jaar. Met de juiste aandacht voor de hieronder opgesomde punten is het zeker mogelijk om binnen één jaar tijd, vanaf scratch, een volledige public key infrastructuur – gecombineerd met een smartcard als drager van de certificaten – op te zetten en in gebruik te nemen.

Scoping

Definieer vooraf een duidelijke scope en baken deze verder af met duidelijke uitgangspunten en randvoorwaarden. Definieer ook de voorwaarden waaronder hiervan mag worden afgeweken. Dit punt is een grote open deur maar des te belangrijker gebleken door de wijze waarop het project voordeel heeft gehad bij de gezamenlijke visieontwikkeling met de leverancier, de duidelijke afspraken vooraf en de daardoor vliegende start.

Projectfasering, projectteam en samenwerking

Breng een projectfasering aan waarin eerst de basis-PKI wordt gerealiseerd waarin wel in grote lijnen de processen en toepassingen worden bepaald, maar waarin deze nog niet in detail worden uitgewerkt.
Voorwaarde voor succes hierbij is wel dat in het projectteam de juiste expertise – technisch, organisatorisch, en processen – aanwezig is om de (nadelige) gevolgen van keuzen in deze fase voor latere fasen te kunnen inschatten. Tevens dient het projectteam de juiste beslissingsbevoegdheid te hebben om snel adequate keuzen te kunnen maken.

Beschikbaarheid van de basisinfrastructuur was een noodzaak om de certificaten te kunnen produceren voordat deze werden verstrekt aan de gebruikers. Deze tijdsafhankelijkheid noodzaakte het project geheel te focussen op de technische realisatie en om op tal van punten snel keuzen te maken met de in het project beschikbare kennis.

Hierdoor werden discussies over onderling afhankelijke infrastructurele, proces- en applicatie-issues beperkt tot de essentie. In daaropvolgende fasen werden vervolgens de processen en het gebruik binnen de applicaties gedetailleerd ingevuld en geïmplementeerd.

De standaardisatie, en daarmee de koppeling van verschillende PKI-technieken is de laatste jaren sterk toegenomen. Desondanks vergde de ontwikkeling van de interfaces naar de ver-

schillende componenten op het laatst – vlak voor uitrol – meer tijd dan gepland. Korte beslissingslijnen waren daarbij essentieel voor goede communicatie naar het project, de beheerorganisatie en de gebruikers.

Uitbesteding / Managed dienstverlening

In de aanloop van het project in 2007 werd in andere internationale onderdelen van de organisatie gewerkt aan een interne PKI, voornamelijk voor gebruik binnen de eigen IT-infrastructuur. Met name door de bredere toepasbaarheid van de certificaten en snellere implementatiemogelijkheden is toch gekozen voor het uitbesteden van de PKI-diensten. Deze keuze, en de keuze voor de aanbieder van Managed PKI-diensten is essentieel geweest voor het succesvolle resultaat ([Getro5]).

Het binnen het project samenvoegen van de ervaring, expertise en kunde van eigen medewerkers en die van de leverancier in het project heeft geleid tot een managed service die met de beschikbare middelen niet binnen de eigen organisatie gerealiseerd en beheerd had kunnen worden. Net als bij outsourcing van andere IT-diensten dient de eigen organisatie wel over de juiste kennis te beschikken om de regie te blijven voeren tijdens de ontwikkeling en om in control te blijven over de beheerdiensten.

Behalve de voordelen van tijdwinst en kosten zijn de mogelijkheden voor aanpassingen en uitbreiding van de PKI-diensten, met behoud van betrouwbaarheidsniveau van certificaten, een voordeel gebleken van de uitbestede dienst.

Aanvraag-, uitgifte- en beheerprocessen

Niet nieuw, maar toch zinvol om hierbij te benoemen zijn de volgende, meest opvallende leermomenten:

- Blijf altijd streven naar een eenvoudig en uniform aanvraag- en distributieproces, ook als dit tijdelijk, tijdens ontwikkeling, niet zo kan worden opgezet.
- Ga ervan uit dat wat er in het gehele proces van aanleveren van kaarten en productie van kaart en certificaat mis kan gaan, ook een keer mis gaat.
- Blijf de kaart- en applicatieprocessen conceptueel altijd als separate processen beschouwen en breng scheiding en controles aan daar waar dat mogelijk is. Hoezeer de fysieke toegangscontrole ook is gekoppeld aan de identiteitspas, het blijft een applicatie net als bijvoorbeeld het beveiligen van e-mail.
- Richt de productie van de kaart en die van de certificaten in binnen één proces. Gescheiden opzet kan wenselijk zijn bij ontwikkeling maar voor het reguliere beheer is het inefficiënt en een bron van verstoringen.
- Doe de initiële uitrol en/of invoering in één keer. Eventueel noodzakelijke uitzonderingen blijven de beheerorganisatie zeer lange tijd achtervolgen, zijn een bron van verstoringen en een groot acceptatierisico.

Conclusies

Gerelateerd aan de in dit artikel genoemde aspecten en onze interne projectervaringen kunnen de volgende conclusies worden getrokken ten aanzien van de opzet, realisatie en invoering van een corporate identiteitspas en managed PKI voor persoonsgebonden certificaten op die kaart:

In een samenwerkingsverband met een Managed PKI-leverancier en met de juiste aandacht voor scoping en gefaseerde realisatie is het mogelijk binnen één jaar tijd, vanaf scratch, een volledige public key infrastructuur – gecombineerd met een smartcard als drager van de certificaten – op te zetten en in gebruik te nemen.

Door geleidelijke invoering van de elektronische corporate identiteitspas – geleidelijk in de zin van niet direct noodzakelijk voor gebruik van de IT-infrastructuur en niet direct toepasbaar voor alle uiteindelijk te ondersteunen toepassingen – is invoering mogelijk met een sterk beperkt budget.

Om tegen acceptabele kosten beveiligde uitwisseling van elektronische gegevens tussen organisaties op grote schaal mogelijk te maken, is er behoefte aan een ‘sub-qualified’ en/of de-facto PKI-standaard. Met deze standaard moet het voor organisaties eenvoudig zijn om bilateraal afspraken te maken over wat en hoe er informatie wordt uitgewisseld en met welke juridische betekenis.

Literatuur

[Getro5] Getronics PinkRoccade Nederland BV, *Managed PKI Service; Introduction*, 2005.

[KPMG07] KPMG IT Advisory, *Public Key Infrastructure Implementatie en Audit; Betrouwbare en veilige elektronische communicatie*, 2007.

[Meeno1] Drs. W.J.P. van de Meent, *Het ontwikkelen van e-mailconventies,* Compact 2001/5.

[Nazao1] Noel Nazario en Martijn van Oosten, *Real-world Application of Public Key Infrastructures Deployment Methodology*, Compact 2001/1.

[Velto1] Ir. A.J.M. Veltmeijer, *Beheeraspecten van technisch complexe omgevingen*, Compact 2001/2.

[Walso2] Drs. P.A. van Walsem en ir. A. van Zanten CISA, *Is ETSI TS 101456 geschikt voor gebruik bij een certificeringsonderzoek?*, Compact 2002/4.