

ARTIKEL

auteur Ing. Jacques A. Cazemier, Ir. Bart M.P. Giesbers MSIT
tijdschrift Digitaal Bestuur

26 maart 2009

PKI: EERST TOT 10 TELLEN...

PKI is geen oplossing op zichzelf, het succes wordt bepaald door de bredere context.

Al sinds 1996 zijn er technische oplossingen beschikbaar en het is inmiddels 10 jaar geleden dat de overheid het startsein gaf voor een nationale PKI-voorziening. Maar toch is er voornamelijk sprake van geïsoleerde of kleinschalige implementaties die gelukt zijn.

Nu echter stimuleert de Dienstenrichtlijn vanuit de Europese Unie het gebruik van PKI. Deze richtlijn stelt dienstverleners vanaf 2010 in staat om eenvoudiger activiteiten te ontplooiën binnen de Europese Unie, onder meer door het elektronisch kunnen afhandelen van procedures en formaliteiten. Eén van de onderliggende eisen is het gebruik van op PKI gebaseerde elektronische handtekeningen. Dit zal de noodzaak tot adoptie van PKI in heel Europa vergroten.

Tijd om te laten zien hoe het wel moet.

We willen wel, maar het lukt niet?

In Digitaal Bestuur 2008 nummer 4 heeft u in het artikel ["Informatiebeveiliging als hoofdpijndossier"](#) kunnen lezen dat de invoering van PKI nog steeds duur en complex is. Ook citeert het artikel PKIloverheid: "PKI komt langzaam maar zeker van de grond". De beperkte realisatie wordt ondersteund door voorbeelden vanuit de Justitie-omgeving. Eerder is ook in de media en publicaties melding gemaakt van vertraging van het project Defensiepas, de PKI-kaart van Defensie. Daarnaast zijn er bij de auteurs nog andere niet met name te noemen voorbeelden van niet gelukte, vertraagde of onvolwassen implementaties van PKI.

Toch blijft de behoefte aan PKI-oplossingen aanwezig en worden vanuit de Europese Unie ook keuzes gemaakt die deze noodzakelijk maken. Voor programma's als de Dienstenrichtlijn, e-Procurement en e-Invoicing wordt gezocht naar oplossingen voor elektronische identificatie en elektronische handtekening. Daarbij zijn al keuzes gemaakt om op PKI gebaseerde elektronische handtekeningen te gebruiken.

Kortom, PKI is nog steeds een goede oplossing voor het invullen van beveiligingsvereisten, maar de implementatie leidt nog vaak tot problemen. Dit artikel beoogt een handreiking te geven hoe de slaagkans van de invoering van PKI vergroot wordt.

Waarom ook alweer PKI als oplossing?

PKI gebruikt u om betrouwbaar informatie uit te wisselen. U kunt met PKI een aantal beveiligingsfuncties realiseren, zoals het plaatsen van elektronische handtekening, het veilig versturen van informatie of het aanmelden op een toepassing. Gelet op de ontwikkelingen in Europees verband richten de voorbeelden in dit artikel zich op de toepassing van de elektronische handtekening. De strekking van de oplossing geldt ook voor de andere beveiligingsfuncties van PKI.

De elektronische handtekening is juridisch gelijkwaardig aan de "natte" (handgeschreven) handtekening, mits deze voldoet aan een aantal eisen. Deze eisen zijn vastgelegd in de Europese Richtlijn Elektronische handtekeningen en in Nederland verankerd in de Wet Elektronische handtekeningen. Deze eisen voor een elektronische handtekening brengen het gebruik van PKI met zich mee. Met name in het kader van Europese digitalisering, zoals wordt voorzien in de Europese Dienstenrichtlijn en e-Procurement voorzieningen, vindt de elektronische handtekening zijn toepassing om deze digitalisering mogelijk te maken. Echter, ook in nationaal verband brengt digitalisering de behoefte aan de elektronische handtekening met zich mee.

Wellicht werkt u al aan de implementatie van PKI of werkt u met de elektronische handtekening? Of wellicht bent u vanuit wet- en regelgeving of organisatiebehoefte voornemens dat te gaan doen? Dan is het zeer waarschijnlijk dat er verschillende implementatie scenario's de revue gepasseerd zijn, of dat u praktische drempels bent tegen gekomen. Kortom, misschien herkent u zich in de hieronder beschreven voorbeelden.

Herkent u zich in de volgende situaties?

... De PKI is initieel opgezet in een autonome beheersbare pilotvorm om kleinschalig ervaring op te doen met PKI zelf of met een daadwerkelijke toepassing in uw bedrijfsvoering. Het zal niet de eerste keer zijn dat een pilot evolueert tot een permanente oplossing. Is dan de business case nog geldig? Is de implementatie dan nog voldoende schaalbaar? Is de oplossing toepasbaar voor andere processen in de bedrijfsvoering? Is de oplossing geschikt voor een uitbreiding naar een grotere en meer diverse doelgroep? Zo nee, is volledige nieuwbouw haalbaar met de inmiddels in gebruik genomen pilotomgeving of zijn processen al te veel afhankelijk van de pilotinfrastructuur? En ook voor deze situatie dient rekening gehouden te worden met de juridische en organisatorische borging bij de opschaling van de pilot.

... De PKI is vanuit een technische invalshoek door uw ICT-afdeling gerealiseerd, mogelijk volledig geïntegreerd met uw Microsoft omgeving. Of misschien als separate oplossing, al of niet met toepassing van diensten van externe commerciële dienstverleners. Nu is het tijd geworden om de PKI-dienstverlening en kwaliteit daadwerkelijk te borgen aan de hand van de bijbehorende juridische aspecten, organisatorische inrichting en beveiligingsmaatregelen. Dan zou het kunnen zijn dat bij de realisatie van de technische invulling keuzes zijn gemaakt die niet passen bij de juridische en organisatorische borging of het kennisniveau van gebruikers. Dit kan betekenen dat de technische implementatie geheel of gedeeltelijk vernieuwd of aangepast dient te worden, met de daarbij behorende inspanning en kosten.

... De PKI is bedoeld om één elektronische identiteit te introduceren als basis voor meerdere toepassingen. Daarbij is zekerheid over de betrouwbaarheid van deze identiteit van belang voor uw organisatie. Kan deze zekerheid geleverd worden op basis van een betrouwbare basisregistratie zoals uw personeelsadministratie? Of zijn daar additionele (handmatige) handelingen voor nodig? Hoe betrouwbaar acht u een elektronische identiteit van een partij met wie u communiceert, zeker in het geval van een buitenlandse partij?

... De PKI maakt gebruik van een veilig middel, zoals een smartcard, om gekwalificeerde handtekeningen mogelijk te maken. Dat middel wordt ook toegepast voor andere toepassingen die geen relatie met de PKI hebben. Te denken valt aan toepassingen zoals toegangscontrole, betalen en telefonie. Is rekening gehouden met de gevolgen van de andere toepassingen voor de PKI? Wat gebeurt er indien overgestapt wordt op een andere telefonieaanbieder? Wat zijn de gevolgen van nieuwe vereisten voor toegangscontrole voor het middel waarmee een handtekening wordt gezet? Had dit voorzien kunnen worden?

... De PKI is in volle omvang en adequaat opgezet voor toepassing bij meerdere interne processen. Nu ontstaat een behoefte waar een uitbreiding van het toepassingsgebied aan de orde is. De PKI-functionaliteit, bijvoorbeeld de handtekening, dient toegepast te worden in een keten met andere organisaties. Echter, is de uitbreiding mogelijk, is rekening gehouden met een afdoende schaalbare oplossing? Zijn herkenbare betrouwbaarheidsniveaus toegepast die bestand zijn tegen organisatieoverschrijdende koppeling? Aansluiting van processen en techniek is vereist en aansprakelijkheid dient geregeld te worden.

Wat is nu de kern van het probleem?

Uit de bovenstaande situaties zijn de volgende fundamentele oorzaken voor niet succesvolle implementaties van PKI af te leiden:

1. Er is een onvoldoende brede kijk op het toepassingsgebied van de PKI.
2. Er wordt kleinschalig gestart, zoals ook vaak vanuit de praktijk wordt aanbevolen. Echter, er wordt onvoldoende rekening gehouden met de bredere context en toekomstige ontwikkelingen.
3. De implementatie wordt teveel vanuit een technische invalshoek aangevlogen, met onvoldoende oog voor de business case en organisatorische en juridische aspecten.
4. Gebrek aan inzicht in afhankelijkheden van onderliggende voorzieningen en de continuïteit bij wijzigingen daarin.

Hoe valt dit op te lossen?

Het kennen van het probleem is het begin van de oplossing. Uit bovenstaande opsomming blijkt dat voor het merendeel van de oorzaken voor mislukking, er sprake is van problemen uit de context van de feitelijke PKI oplossing. Het lijkt correct te veronderstellen dat de techniek zelf goed werkt, de toepassing ervan in de organisatie(s) is het zwakke punt. Oftewel dat aan de oplossing in relatie tot zijn omgeving problemen overblijven.

Deze gevolgtrekking wijst erop dat naast het installeren van techniek er ook aandacht moet zijn voor omgeving en organisatie. Denken aan een PKI oplossing betekent dan ook het onderzoeken van alle mogelijke raakpunten tussen organisatie, techniek, toepassing in processen met de bijbehorende juridische aspecten en de voorziene oplossing. De uiteindelijke beslissing om PKI toe te passen, is afhankelijk van de uitkomsten van het onderzoek; de onderzoeksresultaten dienen om oplossingen te vinden voor de eerder genoemde problemen.

Aanbevolen wordt de volgende stappen te ondernemen:

1. Indien het gebruik van PKI niet voorgeschreven is (door bijvoorbeeld de dienstenrichtlijn), is het opstellen van een objectieve, overtuigende business case noodzakelijk. Daarmee worden de argumenten voor PKI als oplossing zichtbaar gemaakt. Net als iedere andere

beveiligingsmaatregel mag PKI alleen worden toegepast als daar een zakelijk te verantwoorden reden voor is.

2. Het onderzoeken van risico's voor de succesvolle implementatie van de PKI-oplossing. De volgende aandachtsgebieden zijn daarbij van belang:
 - a) **Inventarisatie van raakpunten** van PKI aan organisatie, processen en infrastructuur. Het doel is een zo compleet mogelijke lijst te hebben van de typische situatie. Eén van de problemen met PKI is dat het gebruik ervan zich verder in de organisatie of processen uitstrekt dan voorheen voorzien was. Die lijst dient als basis voor de hiernavolgende aandachtsgebieden.
 - b) De **afhankelijkheid van bedrijfsprocessen** van de goede werking van de PKI oplossing. Daarmee wordt de kwetsbaarheid van de betreffende processen zichtbaar. Of die kwetsbaarheid risico's oplevert, zal moeten worden onderzocht. Als de risico's te groot zijn is duidelijk waar maatregelen nodig zijn en welk effect die maatregelen dienen te hebben.
 - c) **Ketenwerking**: de processen in de keten die ook of juist geen PKI toepassen, inclusief parallel uitgevoerde processen zijn onderwerp van onderzoek. Onderzocht moet worden hoe in die processen omgegaan wordt met PKI. Indien er bijvoorbeeld op het gebied van kennis en achtergrond niveauverschil bestaat bij de deelnemende processen, zal daarvoor een oplossing gevonden moeten worden.
 - d) De **roadmap van deze processen**: organisaties en processen veranderen. Er moet nagegaan worden of op termijn veranderingen te voorzien zijn en hoe die er dan uit gaan zien. De kernvraag is: blijft PKI in de huidige vorm dan de beste oplossing? Indien er aanpassingen van PKI nodig zijn, is het goed dat vroegtijdig te signaleren. Dit aandachtsgebied is al vanaf het prille begin van toepassing, ook bij het initiëren van een pilot- of testomgeving dient rekening gehouden te worden met toekomstige ontwikkelingen.
 - e) **Kennis en achtergrond van de gebruikers**: dit onderwerp is een groter struikelpunt dan verwacht. Cryptografie is een onderwerp dat niet toegankelijk is. Alleen wanneer de techniek totaal onzichtbaar is, zal gebruik zonder problemen verlopen. Het aangeven dat een handtekening gezet moet worden of dat een bestand in een envelop gedaan moet worden, mag geen technische kennis bij de gebruiker vereisen. Training en informatieverschaffing zijn vaak succesfactoren gebleken bij implementatie.
 - f) **Continuïteitseisen** van het toepassen van PKI tijdens normale omstandigheden en tijdens calamiteiten – oftewel wat te doen als sleutels, algoritmen of implementatie zijn gecompromitteerd. Archivering verdient eveneens bijzondere aandacht. Daar moet aandacht zijn voor blijvende, vertrouwde toegang tot informatie, zie ook het [artikel "Cryptografie beperkt houdbaar"](#) van december 2008. Zelfs onder niet normale omstandigheden. Het is vervelend om informatie kwijt te raken door niet werkende ondersteunende techniek of cryptografie.
 - g) **Ontwikkelingen in de infrastructuur**: indien er veranderingen zijn in de infrastructuur waar PKI gebruik van maakt, zal er aandacht zijn voor de effecten op de PKI oplossing. Helaas vinden ook veranderingen plaats in de infrastructuur buiten de directe omgeving van PKI. Zoals het aanpassen van een firewall configuratie of een virusscanner. Het is mogelijk dat dan de ingerichte PKI oplossing niet meer werkt – en daarmee ook het zetten van een handtekening onmogelijk wordt.
 - h) **Juridische aspecten**: zoals wie is er aansprakelijk als het gebruik van PKI niet het gewenste effect heeft? Of als het verkeerd gebruikt wordt? Maar ook de juridische

Fout! Geen tekst met opgegeven opmaakprofiel in document.

consequenties van gebruik buiten de grenzen van de eigen organisatie of in internationaal verband dienen onderzocht te worden.

Bovenstaande punten hebben weinig met de PKI techniek te maken. Die werkt in het algemeen wel: de organisatie eromheen en met name de verzameling van afhankelijkheden zijn bepalend voor succes of falen.

Wat kan ik hier morgen aan doen?

Bovenstaande tekst is geen vrijbrief om besluitvorming langer uit te stellen. Beslissen over oplossingen op het gebied van beveiliging mogen hoge prioriteit hebben omdat uitstel in veel gevallen de onveilige situatie laat voortduren of het invoeren van een veilige situatie belemmert.

Met het onderzoek dat in dit artikel genoemd is, is het mogelijk om PKI morgen al meer integraal te beschouwen. PKI is immers niet een onderdeel dat toegevoegd kan worden. Toegepaste PKI is onlosmakelijk verbonden aan zijn omgeving, met name processen en organisatie. Een benadering vanuit een beperkte blik leidt tot processen die niet het juiste resultaat opleveren. Kortom, begin morgen eerst met tellen tot 10 voordat u een vliegende start maakt.