PKI: vloek of zegen?
(if PKI is the answer, then what was the question?)*

dr. Jaap-Henk Hoepman[1]

Faculteit Informatica, Universiteit Twente
hoepman@cs.utwente.nl

Samenvatting In het bedrijfsleven en binnen de overheid wordt een Public Key Infrastructure (PKI) steeds vaker gezien als een noodzakelijke basis voor het beveiligen van interne netwerken en systemen, en voor het faciliteren van veilige en 'vertrouwbare' communicatie met externe partijen (klanten, toeleverantiers, burgers). Het beeld is ontstaan van een PKI als panacee voor alle beveiliginsproblemen. De vraag is of dit terecht is. Tijd voor een kritische analyse: wat is een PKI? Wat zijn haar sterke en zwakke kanten? Als het gaat om het beveiligen van systemen en het opbouwen van vertrouwen over het Internet, biedt een PKI dan een adequate oplossing, of zijn er andere, betere, oplossingen denkbaar?

1 Wat is een PKI?

Een Public Key Infrastructure (PKI) is in essentie gebaseerd op public key cryptografie. Hoewel de meeste lezers hiermee wel bekend zullen zijn, wil ik hier toch kort op ingaan. Bij deze versleutelingstechniek heeft iedere gebruiker twee sleutels: een geheime *privé* sleutel en een *publieke* sleutel. De publieke sleutel wordt gebruikt om een bericht te vercijferen of om een digitale handtekening te controleren. De privé sleutel wordt gebruikt om een bericht te ontcijferen of om een document van een digitale handtekening te voorzien. Hiervoor is de publieke sleutel onbruikbaar. Reden waarom deze dus niet geheim gehouden hoeft te worden.

Om iemand een vercijferd bericht te sturen (of om zijn digitale handtekening te controleren) heb je dus zijn publieke sleutel nodig. De vraag is dan: hoe kom ik aan iemand's publieke sleutel? Persoonlijk uitwisselen is zelden een optie, versturen via het Internet geeft geen garantie over de afzender, en zoeken in een grote public-key database al evenmin.

De oplossing van dit probleem wordt geboden door *certificaten*. Een certificaat wordt uitgegeven door een Certification Authority (CA) en bindt de naam van een persoon of entiteit aan een publieke sleutel. In feite is het een document van de vorm

De eigenaar[1] *van publieke sleutel K is J. Jansen.*

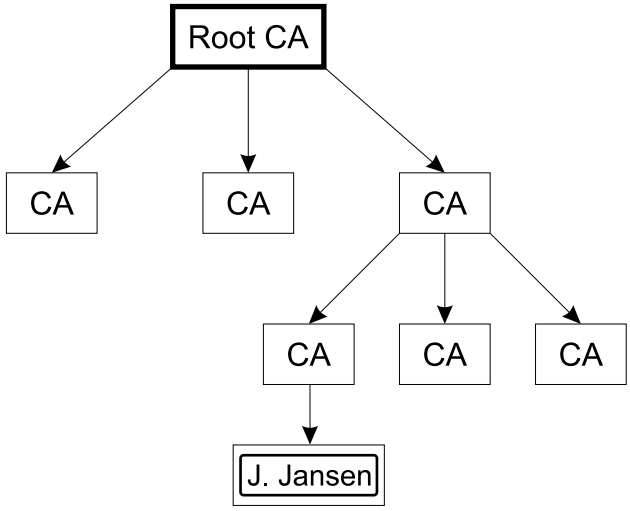
* Id: pki-answer.tex,v 1.1 2002/03/19 15:15:49 hoepman Exp

[1] Met eigenaar van een publieke sleutel bedoelen we hier de houder van de overeenkomstige privé sleutel, die het bezit hiervan met een authenticatie protocol moet aantonen.

voorzien van de handtekening van de CA. Een betrouwbare CA zal op één of andere manier gecontroleerd hebben dat K ook inderdaad de publieke sleutel van J. Jansen is. Door te vertrouwen op de CA, is de publieke sleutel van J. Jansen algemeen bekend.

Voor controle van een certificaat moet iedereen de publieke sleutel van de CA kennen. Als er op de hele wereld maar één CA zou zijn, was dat niet zo'n probleem. Maar voor het kunnen uitgeven van vele miljoenen certificaten is één CA een bottleneck.

Welnu, een PKI is een hiërarchische ordening van verschillende Certification Authoroties (CAs), waarmee dit dilemma wordt opgelost (zie figuur 1). Bovenaan de hiërarchie staat de *Root* CA. Deze geeft certificaten uit met de naam en publieke sleutel van direct ondergelegen CAs (welke, op hun beurt hetzelfde doen voor lager gelegen CAs). De CAs op het laagste nivo tenslotte geven certificaten uit die identiteiten aan publieke sleutels bind. Voor het controleren van het cer-



Figuur 1. PKI hiërarchie

tificaat van J. Jansen uit het voorbeeld is nu de publieke sleutel van de Root CA nodig, *plus* alle certificaten van de tussenliggende CAs op het pad van de Root CA naar de CA van J. Jansen. De tussenliggende certificaten zijn nodig om de publieke sleutel van J. Jansen's CA te kunnen achterhalen en te verifiëren.

2 Toepassingen

We zien dat een PKI primair bedoeld is om een identiteit aan een publieke sleutel te koppelen. Wat zou je verder met deze functionaliteit kunnen doen?

De meest voor de hand liggende toepassing is identificatie en authenticatie over een netwerk als het Internet. Een gebruiker identificeert zich met een certificaat. Vervolgens wordt hij geauthenticeert door te controleren of hij inderdaad eigenaar is van de privé sleutel horend bij de publieke sleutel in het certificaat.

Een vergelijkbare toepassing van een PKI is het beveiligen van e-commerce. Hier koppelen certificaten internet domein namen als `www.rabobank.nl` aan een publieke sleutel. Als met een dergelijke web site via SSL een veilige verbinding wordt opgezet, wordt automatisch het certificaat gecontroleerd en vervolgens de site met behulp van de publieke sleutel geauthenticeerd.

Voor het sturen van beveiligde email kan via een PKI eerst het certificaat met het email adres van de ontvanger achterhaald en gecontroleerd worden, en vervolgens met de gevonden publieke sleutel het bericht vercijferd worden. Op een vergelijkbare manier is ook van een digitaal getekend contract eenvoudig te achterhalen of de handtekeningen valide zijn en door wie ze gezet zijn.

Toegangscontrole (voor gebouwen, systemen, of opgeslagen digitale documenten) gebaseerd op een PKI verloopt als volgt. Iemand die toegang wil tot een document, wordt eerst via certificaat en publieke sleutel geauthenticeerd, en vervolgens wordt op basis van de bewezen identiteit toegang al dan niet verleend.

3 Werkt een PKI?

Theoretisch gezien lijkt een PKI een groot aantal beveiliginsproblemen op te lossen. Maar is dit in de praktijk ook het geval? Er blijken toch een aantal problemen met een PKI te bestaan, waardoor het implementeren van bovenstaande toepassingen minder eenvoudig is dan men op het eerste gezicht zou denken.

3.1 Wat is identiteit?

Essentieel voor een goed werkende PKI is dat ieder individu een globaal unieke naam binnen de PKI heeft. Zo'n unieke naam (gebaseerd op de X.500 standaard voor directory services als LDAP) is bijvoorbeeld

J. Jansen, Faculteit Informatica, Universiteit Twente, Nederland.

We zien dat aan een naam attributen (zoals adres of werkgever) worden toegevoegd, om de naam uniek te maken.

Hiermee is wel gegarandeerd dat de namen uniek zijn, het is volstrekt onduidelijk hoe men op grond van onvolledige gegevens de unieke naam van een persoon kan achterhalen. Immers, mensen kennen elkaars unieke naam niet. Sterker nog, verschillende mensen kunnen één en dezelfde persoon onder een andere 'naam' kennen:

- J. Jansen, de secretaris van de voetbalvereniging,
- Jan, de buurman, of
- Jan Jansen, de collega.

Een ander probleem is dat bij reorganisaties binnen een bedrijf dergelijke unieke namen van medewerkers kunnen veranderen. Dit betekent dat ook alle certificaten moeten worden veranderd. Bovendien moet er een mapping tussen oude en nieuwe namen bewaard worden: anders zouden personen onder de 'oude' naam niet meer herleidbaar zijn tot personen onder de 'nieuwe' naam.

Een voorbeeld. Binnen de UT zullen hoogste waarschijnlijk de faculteiten Informatica en Elektrotechniek fuseren tot één ICT faculteit. Is

J. Jansen, Faculteit Informatica, Universiteit Twente, Nederland.

dezelfde persoon als

J. Jansen, ICT Faculteit, Universiteit Twente, Nederland.

En als bij Elektrotechniek ook een J. Jansen werkzaam was, hoe onderscheiden we beiden dan, en hoe weten we dan welke van de twee oorspronkelijk bij Elektrotechniek werkte?

Als ik een beveiligde email naar de secretaris van de voetbalvereninging wil sturen, heb ik zijn publieke sleutel nodig. Ik weet toevallig dat hij werkzaam is op de UT. Helaas vind ik nu *twee* J. Jansen's, beide werkzaam aan de UT. Als ik de verkeerde kies, komt het vertrouwelijke bericht bij de verkeerde persoon terecht!

Er wordt vaak gezegd dat zonder een PKI de identiteit van een persoon in de virtuele wereld niet vast te stellen is. Uit bovenstaande voorbeelden blijkt dat *met* een PKI dat niet veel makkelijker is geworden. Weliswaar bindt een PKI een publieke sleutel aan een unieke naam, de vertaalslag van gewone naam naar unieke naam is nog steeds onbeveiligd, met alle gevolgen van dien.

3.2 Validiteit van een certificaat

Eerder is al opgemerkt dat een CA bij het uitgeven van een certificaat geacht wordt te controleren of de publieke sleutel en de opgegeven naam inderdaad bij elkaar horen. Deze controle is lastig, en duur als ze goed moet worden uitgevoerd. Meestal is de controle dus zwak, en het uitgegeven certificaat minder valide. Zo kreeg een hacker het vorig jaar voor elkaar om een certificaat voor zijn publieke sleutel te krijgen, met daarin Microsoft als 'zijn' naam!

Voor het controleren van de identiteit van server-side certificaten - zoals die voor de authenticatie van website adressen door SSL gebruikt worden - wordt vaak gebruik gemaakt van informatie in het Domain Name System (DNS). Dit is echter geen goed idee: informatie in het DNS is eenvoudig door hackers te veranderen. Bovendien worden server-side certificates juist gebruikt om te *beschermen* tegen dergelijke DNS-hacks. Een vicieuze beveiligins-circel dus eigenlijk!

Erg veel redenen om ultra-valide certificaten uit te geven zijn er ook niet voor een CA. De enige echt belangrijke is het in stand houden van een betrouwbaar imago. Maar aansprakelijk voor een fout in een certificaat is een CA niet of slechts in beperkte mate. Het Certification Practice Statment (CPS) van een CA, waarin wordt vastgelegd welke garanties de CA op alle door haar uitgegeven certificaten geeft, legt het risico simpelweg bij de gebruiker van het certificaat.

3.3 PKI of PKI's?

Het oorspronkelijke idee was dat er één globale PKI zou ontstaan. Dit is echter geenszins het geval. Er zijn verschillende globaal opererende CA's als Verisign en Thawte. In Internet Explorer zijn standaard tientallen root certificaten van dergelijke CA's beschikbaar. Bovendien zijn er verschillende lokale initiatieven voor het opzetten van nationale PKI's (in Nederland bijvoorbeeld PKI Overheid), en zetten ook bedrijven ieder voor zich een PKI op voor de beveiliging van hun informatiesystemen.

De certificaten van elk van deze PKI's zijn onderling onvergelijkbaar en niet uitwisselbaar. Het is bijvoorbeeld onduidelijk hoe certificaten uitgegeven door de Nederlandse overheid in het buitenland gebruikt zouden kunnen worden. Cross-certificering blijkt in de praktijk een lastig probleem te zijn. Ook de naam van één persoon kan tussen verschillende PKI's verschillen. Er bestaat binnen de PKI-filosofie geen methode om vast te leggen dat twee verschillende namen naar hetzelfde individu verwijzen. Andersom kan ook: twee verschillende personen die (elk in een andere PKI) dezelfde naam krijgen. Het wordt dan wel erg lastig te bepalen wie wie is.

3.4 Privacy

Het gebruik van een een PKI voor toegangscontrole heeft verder het grote nadeel dat de identiteit van de aanvrager telkens geregistreerd wordt. Vaak is dit handig, of uit beveiligingsoogpunt zelfs noodzakelijk, maar lang niet altijd. Uit privacy overwegingen is het beter om daar waar de identiteit er niet toe doet, er ook niet naar te vragen. Een PKI sluit deze mogelijkheid uit.

4 Wat is de vraag?

We hebben gezien dat een PKI een aantal tekortkomingen heeft. Laten we teruggaan naar de genoemde toepassingen van een PKI en kijken met welk doel een PKI daar wordt ingezet.

Het authenticeren van websites heeft als doel een gebruiker het vertrouwen te geven dat hij met de juiste website communiceert. In het geval van een virtuele winkel zou de informatie in het certificaat eventueel ook gebruikt kunnen worden voor juridische stappen bij problemen met een transactie. Deze mogelijkheid moet de consument ook meer vertrouwen in e-commerce geven.

In het geval van toegangscontrole tot gebouwen, systemen, of documenten gaat het eigenlijk om de vraag of een individu gerechtigd (geautoriseerd) is om een bepaalde handeling of actie uit te voeren.

Kort gezegd, het gaat om vertrouwen opbouwen en autorisaties controleren. In de rest van dit artikel zullen we alternatieve oplossingen hiervoor bekijken.

5 Alternatieven

De in de inleiding geschetste vorm van een certificaat wordt wel een *identiteits* certificaat genoemd, omdat zij een identiteit aan een publieke sleutel bindt. Er zijn echter zeer wel andere vormen van certificaten denkbaar. Zogenaamde *attribuut* certificaten binden een eigenschap aan een publieke sleutel. Voorbeelden van attribuut certificaten zijn bijvoorbeeld

> *De eigenaar van publieke sleutel K is ouder dan* 18 *jaar.*

of

> *De eigenaar van publieke sleutel K heeft toegang tot document xyz.*

5.1 Vertrouwen opbouwen

Een groot probleem op het internet is het opbouwen van vertrouwen. Hoe weet je met wie je handelt? Hoe weet je of de andere partij zich aan de afspraken zal houden? Als ik betaal voor een bestelling, hoe weet ik dan of ik mijn goederen geleverd krijg?

Het eerste probleem wordt, deels, door een PKI opgelost. Antwoord op de andere vragen geeft een PKI niet, of het moet de mogelijkheid zijn om *naderhand* met behulp van de identiteit van de 'valsspeler' via juridische wegen eventuele conflicten uit te vechten.

Vertrouwen is echter heel iets anders. Vertrouwen heeft te maken met de kennis die je op *voorhand* bezit, op basis waarvan je het risico op fraude of schade kunt inschatten. Het vertrouwen is hoog als het risico laag is. Er zijn in principe twee manieren om die kennis te verkrijgen.

De eerste manier is door het opbouwen van een (vertrouwens) relatie. Iemand die je kent, waar je vaker contact mee hebt gehad, of waar je vaker mee gehandeld hebt, kun je beoordelen op zijn betrouwbaarheid. Als ik regelmatig artikelen bij een bepaalde web-shop koop, en deze levert altijd keurig de artikelen af, en schrijft het juiste bedrag af van mijn credit card, dan vertrouw ik op deze web-shop. Ook als deze "B. de Haas ProductPaleis" heet. In dit geval is de naam van de persoon of het bedrijf niet van belang. Waar het om gaat is dat je de garantie hebt telkens met dezelfde persoon of hetzelfde bedrijf van doen te hebben. Certificaten zijn hier dus helemaal niet van belang. Het enige wat nodig is, is dat telkens één en dezeflde publieke sleutel voor alle communicatie gebruikt wordt.

De tweede manier is af te gaan op het deskundige oordeel van een ander. Een keurmerk dus, uitgedeeld door een ter zake kundige beroepsgroep of brancheverenigingbijvoorbeeld, of de Consumentenbond. Die een keurmerk ook intrekken als een lid niet of niet meer aan de criteria voldoet. Zo'n instantie fungeert dus als uitgever van certificaten met de volgende inhoud

> *De eigenaar van publieke sleutel K voldoet aan de eisen* abc *van instelling* xyz.

Zo zou de Consumentenbond, vergelijkbaar met haar vroegere Webtrader initiatief, certificaten uit kunnen geven met als inhoud

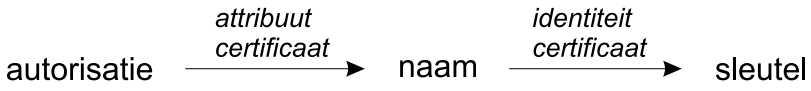
> *De Consumentenbond is van mening dat de eigenaar van publieke sleutel K een betrouwbare web-shop runt.*

Voordeel van een dergelijk certificatie systeem is dat certificaten (in tegenstelling tot logo's) niet te kopiëren zijn naar andere sites.

Dergelijke digitale keurmerken bieden wel vooraf garanties over de kwaliteit van de dienstverlening, en kunnen in belangrijke mate bijdragen aan het verhogen van het vertrouwen op het Internet.

5.2 Autorisaties controleren

In figuur 2 staat in een schema weergeven hoe middels een PKI autorisaties worden gecontroleerd. Middels een attribuut certificaat (of een access control list



Figuur 2. Autorisatie middels een PKI

(ACL)) wordt een bepaalde autorisatie aan een naam gekoppeld. Bij het controleren van de autorisatie wordt het certificaat bij de naam gevraagd, en vervolgens vindt authenticatie met behulp van de daarin gevonden sleutel plaats.

Nadeel van deze methode is dat het controleren van de autorisatie in twee stappen moet gebeuren, en dat beide schakels (van autorisatie naar naam en van naam naar sleutel) goed beveiligd moeten zijn.

SDSI (Simple Distributed Security Infrastructure) van Rivest en Lampson en SPKI (Simple Public Key Infrastructure) van Ellison maakt een eenvoudiger vorm van toegangscontrole mogelijk. SDSI (en SPKI) lossen met een zeer eenvoudige stap het basisprobleem van de naamgeving binnen een PKI op: er zijn eenvoudigweg geen namen. Of beter gezegd: publieke sleutels (die per definitie al uniek zijn) worden binnen SDSI als namen gebruikt. Eigennamen kunnen aan zo'n publieke sleutel gebonden worden, maar worden verder binnen SDSI niet gebruikt.

In figuur 3 staat schematisch weergegeven hoe het controleren van autorisatie binnen een systeem als SDSI te werk gaat. Middels een attribuut certificaat wordt voor de gewenste autorisatie de benodigde sleutel gevonden, welke direct voor authenticatie van de gebruiker gebruikt kan worden. Eventueel kan een bijbehorende eigennaam bij de sleutel gevonden worden (bijvoorbeeld voor het later afhandelen van een dispuut), maar deze is voor het verlenen van de toegang zelf niet nodig.

Figuur 3. Autorisatie middels een attribuut-certificaat

Als een dergelijk identiteits-certificaat niet bestaat, implementeerd deze methode een vorm van anoniem toegang verlenen. Wel is het natuurlijk zo dat verschillende verzoeken tot toegang door hetzelfde individu makkelijk herkenbaar zijn omdat hiervoor telkens dezelfde sleutel gebruikt wordt.

6 Conclusie

Een PKI wordt door de markt krachten toegedicht die zij maar in beperkte mate bezit. Grootste probleem is dat een PKI gebaseerd is op het concept van een unieke naamgeving van personen en entiteiten, welke in de praktijk lastig is te gebruiken. Bovendien is voor een groot aantal beveligingsproblemen een PKI gebaseerd op identiteiten overbodig. Voor het toegangscontrole ligt een directe koppeling tussen sleutels en toegangsrechten voor de hand. Voor het opbouwen van vertrouwen zijn digitale keurmerken veel waardevoller. Beide kunnen middels attribuut certificaten worden gerealiseerd.

Referenties

[1] C. M. ELLISON, *Establishing identity without certification authorities*, in 6th USENIX Sec. Symp., San Jose, CA, USA, July 1996, USENIX, pp. 67–76.

[2] ———, *The nature of a usable pki*, Computer Networks, 31 (1999), pp. 823–830.

[3] R. RIVEST AND B. LAMPSON, *SDSI – a simple distributed security infrastructure*. Apr. 1996.