Vertrouwen in vrije digitale X.509 certificaten

Koot, M.

Publication date
2008
Document Version
Final published version
Published in
Informatiebeveiliging

augustus 2008 nummer 5

special Privacy

INFORMATIEBEVEILIGING

Juridische aspecten van informatie-beveiliging vaak onderbelicht

Milton Mueller stelt privacy en security op internet centraal

Revocable privacy slaat brug tussen veiligheid en privacybelang

CAcert bouwt aan web-of-trust met X.509 certificaten

Privacy na 9/11, zoektocht naar de juiste balans

ib

PvIB
Platform voor
InformatieBeveiliging

Vertrouwen in vrije digitale X.509 certificaten

Auteur: Matthijs Koot > Matthijs Koot is werkzaam bij de Universiteit van Amsterdam en doet onderzoek naar privacy en technische informatiebeveiliging. Hij schrijft dit artikel op persoonlijke titel. E-mail: matthijs@koot.biz.

Public Key Infrastructuren (PKIs) worden vanwege hun gecentraliseerde karakter waarschijnlijk eerder geassocieerd met inbreuk op privacy dan met privacybescherming. Dit artikel laat PKIs van een andere kant zien door een beschouwing van CAcert, een non-profit vereniging die kosteloos digitale X.509 certificaten aanbiedt voor persoonlijke security en met name kijkt naar de privacy. We geven een korte opfrissing van PKI, beschrijven hoe CAcert afwijkt van commerciële PKI-aanbieders en benoemen enkele problemen en perikelen waar CAcert mee te maken heeft.

Een blijvend probleem bij versleuteling en digitale ondertekening van gegevens en communicatie is de vraag welke sleutel je wanneer kunt gebruiken en voor welk doel. Het gebruik van verkeerd, verouderd of gecompromitteerd sleutelmateriaal ondermijnt de functie van cryptografische algoritmen en beveiligingsprotocollen, hoe sterk die zelf ook zijn. Digitale certificaten kunnen worden gebruikt om te weten welk sleutelmateriaal bij welke persoon/organisatie hoort, of het sleutelmateriaal 'vers' is en niet is ingetrokken (bijvoorbeeld als gevolg van compromittering). Het doel van een digitaal certificaat is om sleutelmateriaal te koppelen aan een met voldoende zekerheid geïdentificeerde persoon of organisatie, d.i. om aan te tonen dat de genoemde identiteit in het bezit is van het genoemde sleutelmateriaal (er wordt verondersteld dat niemand anders dat sleutelmateriaal bezit en dat de genoemde identiteit het sleutelmateriaal beschermt). Indien nodig kunnen certificaten ook als bewijsmiddel worden gebruikt waarmee de certificaathouder kan aantonen over bepaalde eigenschappen te beschikken, zoals leeftijd (bijvoorbeeld 18+), werknemer te zijn bij een bepaalde organisatie, daar een bepaalde functie te hebben, et cetera.

Opfrissing digitale certificaten

Digitale certificaten worden toegepast bij versleutelings- en authenticatietechniek en elektronische handtekeningen. Voorbeelden zijn veilige e-mailcommunicatie (S/MIME), SSL/TLS-verbindingen (SSL-VPN, HTTPS, IMAPS) en verificatie van de authenticiteit/integriteit van software en documenten. Om een certificaat te krijgen, registreert een persoon of organisatie zich bij een Registration Authority (RA), die de identiteit van de aanvrager controleert conform een procedure die past bij het beoogde gebruik van het certificaat (is de persoon wel wie hij zegt dat hij is? Controle middels identiteitsbewijs, bankoverschrijving, waarborging door derden, et cetera). Bij acceptatie stuurt de RA de aanvraag door naar een Certificate Authority (CA). De CA stelt een certificaat op, vaak conform de X.509 standaard, met de naam en de publieke sleutel van de aanvrager (en een aantal andere details zoals geldigheidsduur, een serienummer en een verwijzing naar de uitgevende CA), ondertekent het, en stelt het beschikbaar. De ondertekening door de CA heeft de intuitieve betekenis: "ik, de CA, verklaar dat de identiteit van deze persoon/organisatie is vastgesteld en dat hij/zij over dit sleutelmateriaal beschikt".

Vertrouwen in de dienstverlener

De certificaathouder kan het certificaat alleen gebruiken indien andere betrokkenen de certificaathouder en de CA vertrouwen (een 'betrokkene' is bijvoorbeeld een server aan wie een certificaat ter authenticatie wordt voorgelegd, een persoon die de ondertekening van een ontvangen mailtje wil verifiëren of een persoon die een vertrouwelijk mailtje wil sturen aan de certificaathouder). De CA heeft dus een rol als een Trusted Third Party (TTP), en verlangt dat er wordt vertrouwd op wat hij via zijn ondertekeningen 'zegt'. De CA kan niet garanderen dat de certificaathouder zijn geheime sleutel goed beschermt, alleen 'dat hij z'n best heeft gedaan'. Betrokkenen moeten ervan uit kunnen gaan dat het de CA is die een certificaat tekent, en niet iemand die zich voordoet als die CA. Ter (gedeeltelijke) rechtvaardiging van dat vertrouwen worden CAs op een zeer hoog beveiligingsniveau gebracht, met sterke technische (waaronder fysieke) en procedurele/organisatorische beveiliging. Het periodiek ondergaan van audits op procedures en beleid door (soms meerdere) accountancykantoren is een belangrijk onderdeel van het beveiligingsproces van een CA.

De betrouwbaarheid van een certificaat hangt in eerste instantie af van de juistheid in vaststelling van de identiteit van de aanvrager. Het vaststellen van een identiteit is de taak van de RA('s). Deze dient van elke nieuwe aanvrager te controleren of de overlegde identiteitsbewijzen[1] authentiek zijn (=niet vervalst), te beoordelen of ze inderdaad toebehoren aan de aanvrager (bijvoorbeeld door controlevragen te stellen en te letten op discrepanties in fysieke kenmerken), en te verifiëren dat de gegevens in overeenstemming zijn met de Certificate Signing Request (CSR) en met wat bekend is bij de CA. Na acceptatie staat de RA in voor de identiteit van de aanvrager.

CAcert: kosteloze certificaten

Waar PKIs vroeger vooral gebruikt werden binnen financiële instellingen en overheidsorganisaties, zijn er met de opkomst van internet in de vrije markt commerciële partijen ontstaan die tegen betaling digitale certificaten uitgeven aan iedereen die er behoefte aan heeft en ervoor wil betalen. Enerzijds door de hoge kosten die gepaard gaan met het beveiligingsproces van CAs, anderzijds door commerciële overwegingen van de aanbieders, blijven de kosten per certificaat relatief hoog. PKI-technologie vindt mede daardoor nog beperkt toepassing

[1] Bij CAcert wordt altijd gewerkt met officiële identiteitsbewijzen, zoals paspoorten en rijbewijzen. Veel commerciële CAs bieden ook certificaten op basis van alleen een bankoverschrijving cq het betalen van abonnementsgeld. In dat geval is sprake van andere en misschien 'vagere' gegevens als basis voor vaststelling van identiteit.

in niet-commerciële domeinen, terwijl daar dezelfde veiligheidsbehoeften zijn.

CAcert is een Australische non-profit vereniging die als doel heeft om iedereen, ongediscrimineerd, te faciliteren bij het beschermen van privacy op internet *[CAcert]*. Daartoe bieden ze kosteloos X.509 certificaten aan iedereen die er behoefte aan heeft. Bij CAcert is het niet een centrale[2] organisatie, maar zijn het de certificaathouders zèlf die elkaars identiteit vaststellen. Dit proces wordt *waarmerken* genoemd. Er wordt gewerkt met een puntensysteem, waarbij de certificaathouders elkaar na identificatie (in levende lijve, met controle van paspoort of rijbewijs, conform voorgeschreven procedures) *waarmerkingspunten* kunnen toekennen voor de mate van vertrouwen die zij hebben in hun vaststelling van de identiteit van de ander. Er is dus sprake van een web-of-trust, in tegenstelling tot de enkelvoudige vertrouwensrelatie bij de meeste commerciële CAs. Het idee is: hoe hoger het aantal verzamelde web-of-trust punten, hoe groter de kans dat een certificaathouder inderdaad is wie hij zegt te zijn (uiteraard blijven het uiteindelijk de certificaathouders en andere betrokkenen zelf die bepalen/voelen of er voldoende vertrouwen is om de certificaten te accepteren voor gebruik). Een nieuwe certificaathouder kan zelfs pas *waarmerker* waarmerkingspunten toekennen na voldoende punten te hebben verzameld en aangetoond te hebben over voldoende kennis te beschikken over de procedures. Het aantal punten dat wordt gegeven is afhankelijk van de getoonde documenten en de ervaring van de waarmerkers. In veel landen is een groeiend netwerk van lokale waarmerkers die zich aanbieden om op afspraak te waarmerken, zo ook Nederland. In Nederland bestaat sinds vorig jaar zelfs een onafhankelijke stichting die het gebruik van vrije digitale certificaten (voor privacy en security) stimuleert, en daarbij ook CAcert promoot *[Oophaga]*.

Vertrouwen in de community

Direct na registratie bij CAcert, nog voordat enige identificatie heeft plaatsgevonden, kunnen al certificaten worden aangevraagd. Zolang geen punten zijn verzameld via waarmerkers, is de enige zekerheid die aan een certificaat kan worden ontleend, dat de genoemde sleutel hoort bij iemand die e-mail kan verzenden en ontvangen op het genoemde e-mailadres. Er is verder geen zekerheid over de werkelijke identiteit van die persoon. Het beleid van CAcert is dan ook dat pas bij een web-of-trust van 50 punten (ongeveer twee tot vijf waarmerken) de volle naam van een individu of organisatie gekoppeld is (en dus gecheckt door RA/CA) aan een certificaat. Onder die drempel kunnen alleen *naamloze* certificaten worden aangevraagd (waarbij geldt: "CN = CAcert WoT User"). Zodra de drempel is bereikt kan het certificaat worden vervangen door een certificaat op naam (bijvoorbeeld: "CN = Teus Hagen"[3]).

Hoewel de certificaten bij CAcert nog steeds door een centrale CA worden uitgegeven, en deze centrale CA nog steeds vertrouwen verlangt, is er geen centrale organisatie die over kopieën van de identiteitsbewijzen van alle aanvragers beschikt. Bij commerciële CAs is dat vaak wèl het geval. Bij CAcert vertrouwt de CA (en daarmee ook de eindgebruikers) nog steeds op de RA-functie, maar is de RA-functie belegd bij de eindgebruikers, de CAcert Community Members, die via de CAcert Community Agreement onderhevig zijn aan interne arbitrage bij geschillen. De betrouwbaarheid van de certificaten hangt af van de zorgvuldigheid waarmee waarmerkers de andere eindgebruikers waarmerken. Of dit aanvaardbaar is, hangt af van het beoogde gebruik van certificaten: het lijkt in elk geval eerder aanvaardbaar bij persoonlijk gebruik en in minder hiërarchische sectoren dan in sectoren waarin vertrouwen vooral hiërarchisch is bepaald en waarin aansprakelijkheid belangrijk is (industriële, militaire en bancaire applicaties). Er valt ook iets te zeggen voor de wet van de grote getallen: hoe meer waarmerkers er zijn, des te groter de kans dat eventuele fouten worden gecompenseerd ('miracle of aggregation').

Ter versterking van het (te rechtvaardigen) vertrouwen van eindgebruikers in de certificaten wordt nagedacht over aanvullende maatregelen. Zo wordt overwogen om toegekende punten na een bepaalde periode te laten vervallen, zodat periodieke her-waarmerking nodig is en het web-of-trust 'vers' blijft. Ook wordt overwogen om de identificatieprocedure uit te breiden tot (optionele) wederzijdse identificatie, waarbij de waarmerker zichzelf ook identificeert aan de gewaarmerkte. De gewaarmerkte kan dan *ervaringspunten* toekennen aan de waarmerker (zoals gezegd, de waarmerker kent de gewaarmerkte *waarmerkingspunten* toe). Bij registratie van een nieuwe deelnemer wordt het e-mailadres gecontroleerd via een e-mailbevestiging. Bij aanvraag van servercertificaten wordt via e-mailbevestiging gecontroleerd of de aanvrager e-mail kan ontvangen op de domeinnaam waarvoor het certificaat wordt aangevraagd.

Om het gebruik van certificaten uitgegeven door CAcert in de hand te houden wordt gebruik gemaakt van copyright op de CAcert root key en CAcert handtekening. De voorwaarden van gebruik zijn hiervoor vastgelegd in een special licentie: CAcert Non-Related Persons Disclaimer and License en Contributor License Agreement. De licenties moeten het vrije gebruik garanderen. De voorwaarden zijn vergelijkbaar met de licenties zoals die in de Open Source wereld gehanteerd worden.

Problemen en perikelen

Internationaal

Lokale wetten en regels. De huidige eindgebruikers van CAcert zitten wereldwijd verspreid over nationale en juridische grenzen en hebben te maken met verschillende lokale wetten en regels. In sommige regio's bestaan wetten en regels die invloed hebben op de manier waarop CAcert haar diensten mag (moet) aanbieden. Zo zijn er in sommige Europese landen regels over digitale handtekeningen, waarbij wordt voorgeschreven wat er in het Common Name-veld van een Distinguished Name moet staan. Italiaanse wetgeving vereist bijvoorbeeld dat het CN-veld wordt gevuld als "<achternaam> / <voornaam> / <sofinummer> / <uniek nummer>" *[Lioy06]*, terwijl het gebruik van certificaten voor servers voorschrijft dat de CN alleen de domeinnaam bevat. De Europese richtlijn over elektronische handtekeningen, 99/93/EC, is nog niet in alle Europese landen geïmplementeerd. Een andere eigenaardigheid is dat sommige landen CAs verplichten om ook de *geheime* sleutels te

[2] Omwille van verduidelijking van het onderscheid tussen CAcert en traditionele PKI-aanbieders worden RAs hier gekenmerkt als "centrale organisatie". In werkelijkheid is vaak sprake van één of meer semi-decentrale kantoren die allemaal een contract hebben met de CA.

[3] Genoemd persoon heeft toestemming gegeven voor dit voorbeeld.

archiveren, bijvoorbeeld voor escrow (of spionage).

Persoonsgegevens. De Europese privacyrichtlijnen en Nederlandse regelgeving schrijven voor dat zodra persoonsgegevens in EU-jurisdictie worden geïmporteerd, er een lokaal persoon moet worden aangewezen als verantwoordelijke voor die gegevensverwerking en voor handhaving van privacyregels. Bij verwerking van persoonsgegevens door CAcert-waarmerkers in Nederland zou een Nederlander verantwoordelijk moeten worden gesteld. Met een wereldwijd gedistribueerd systeem met toegang op afstand tot services en servers is dit lastig, omdat je bijvoorbeeld niet wilt dat die persoon (als gewezen verantwoordelijke) zou kunnen beschikken over de geheime sleutel van CA. Daarnaast moet bij verwerking van persoonsgegevens voor elk persoonsgegeven kunnen worden gerechtvaardigd/aangetoond dat dat gegeven echt noodzakelijk is voor de operationele dienstverlening van CAcert. Voor bijvoorbeeld de geboortedatum die bij CAcert wordt gebruikt voor unieke identificatie van certificaathouders (daarover straks meer) is dat lastig.

Privacy

Minimum persoonsgegevens, geen open directory. Een certificaat is een bewijs dat het sleutelmateriaal in het bezit is van een geïdentificeerde persoon of organisatie, en het ligt voor de hand te denken dat een certificaat dan ook een weergave moet bevatten van die identiteit. In dat geval bevat het certificaat waarschijnlijk persoonsgegevens en is de certificaathouder traceerbaar tot het individu. Certificaten zijn in principe openbaar (binnen de scope en bereikbaarheid van de PKI), en soms bieden CAs een zoekfunctie aan om in hun interne repository (in meer of mindere mate gericht) te zoeken naar certificaten. Hoewel certificaten kunnen worden gebruikt ten gunste van bepaalde privacydoelen (immers, certificaten kunnen beschermen tegen schending van vertrouwelijkheid door het gebruik van de verkeerde, verouderde of gecompromitteerde sleutels), vormen ze zelf ook een risico voor *andere* privacydoelen: afhankelijk van de inhoud van de certificaten en de vrijgevigheid van de zoekfunctie kan iedereen met toegang tot de zoekfunctie en de certificaten persoonsgegevens verzamelen. De certificaateigenaren hebben daar dan doorgaans geen controle over en geen inzage in. Tegen deze dreiging bestaan twee simpele maatregelen: het verwijderen of beperken van de zoekfunctie en het beperken van de hoeveelheid persoonsgegevens die op een certificaat staat vermeld. Het beleid van CAcert is expliciet dat er géén zoekfunctie beschikbaar is en dat een certificaathouder niet traceerbaar mag zijn (bijvoorbeeld qua locatie) op basis van zijn certificaten. Een certificaat wordt uitgegeven op basis van controle van identiteitsbewijzen en bewijst dat de identiteit van de certificaathouder (als het goed is) is vastgesteld, maar *is* zelf geen identiteitsbewijs en hoeft dus ook geen persoonsgegevens te bevatten. Op de CAcert-clientcertificaten (voor personen) staan alleen de volledige naam (CN-veld) en het e-mailadres (E-veld). De CAcert-servercertificaten (voor personen) bevatten alleen een domeinnaam. CAcert-certificaten voor organisaties bevatten de naam van de organisatie (OU-veld) en wèl een locatie (L-veld) (deze worden gewaarmerkt via het KvK-register).

Geen archief van kopieën en nummers van paspoort/rijbewijs. Bij de oprichting in 2002 schreef CAcert voor dat waarmerkers een archief moesten bijhouden met kopieën van de identiteitsbewijzen van gewaarmerkte personen en dat dat archief zeven tot tien jaar moest worden bewaard. In 2006 is dat voorschrift omwille van privacybescherming gewijzigd en hoefden alleen nog de nummers/codes van de identiteitsbewijzen te worden gearchiveerd, met dezelfde termijn van zeven tot tien jaar. In lijn met nieuwe Europese privacyregels heeft CAcert recentelijk besloten om ook de laatste eis te laten vallen en zijn de waarmerkers opgeroepen om alle resterende archieven van kopieën van identiteitsbewijzen en nummers/codes van identiteitsbewijzen (veilig) te vernietigen. Er worden dus geen kopieën van identiteitsbewijzen van personen meer gearchiveerd en de gegevens over een persoon zijn geminimaliseerd tot de naam (of namen) van die persoon, geboortedatum (onderdeel van de Distinguished Name, zie volgende paragraaf), geregistreerde e-mailadressen en domeinnamen van de persoon.

Wat wèl (centraal) wordt opgeslagen. Tijdens registratie van een nieuwe deelnemer wordt gevraagd naar de volledige naam (zoals vermeld op een geldig identiteitsbewijs uitgegeven door de overheid met een pasfoto met de betreffende (exacte) naam), de geboortedatum (idem, zie volgende paragraaf), het primaire e-mailadres en een vijftal vrij te kiezen challenge-response controlevragen voor de wachtwoord-resetfunctie; wanneer op een later moment servercertificaten worden aangevraagd, zullen ook domeinnamen worden gevraagd. Gedurende het gebruik van de CAcert diensten worden geregistreerd: certificaat requests, vervallen verklaarde certificaten, de opgedane ervaringspunten en of de deelnemer waarmerkingsadministrateur is voor een organisatie. Deze gegevens, en alleen die gegevens die technisch noodzakelijk zijn voor de dienstverlening, staan centraal opgeslagen in de sterk beveiligde CAcert gebruikersdatabase[4]. Toegang tot de database is (alleen) mogelijk voor wie onderdeel uitmaakt van de CAcert-keten, en elke toegang wordt gelogd. Verantwoordelijkheid (en aansprakelijkheid) voor deze gegevens ligt uiteindelijk bij CAcert Inc. en contracten (CAcert Third Party Disclaimer and License) met tussenliggende providers.

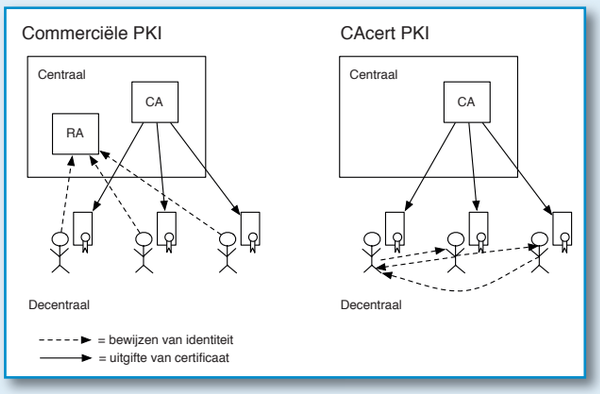
Unieke namen

Ondubbelzinnige identificatie via geboortedatums. Hoewel het deelnemers in een PKI is toegestaan om meerdere certificaten, (e-mail)adressen en namen[5] te hebben, moeten ze binnen de scope van in de PKI ondubbelzinnig identificeerbaar zijn. Het streven van CAcert is dat certificaten uitsluitend namen bevatten zoals die op officiële identiteitsbewijzen staan vermeld. Omdat verschillende personen dezelfde voor- en achternaam kunnen hebben is het nodig om aanvullende onderscheidende attributen te registreren. Zulke attributen moeten betekenisvol zijn: een volgnummer volstaat

niet (welke Teus is “Teus Hagen 1”? Welke is “Teus Hagen 2”?). Medewerkers in kantooromgevingen kunnen vaak worden onderscheiden aan de hand van de businessunit en afdeling waar ze werken; zorgverleners in medische instellingen kunnen vaak worden onderscheiden aan de hand van nummers uit het BIG-register. De scope en doelgroep van CAcert zijn echter zo ruim dat zich niet gemakkelijk gemeenschappelijke attributen laten aanwijzen. Bij CAcert wordt daarom de geboortedatum als onderscheidend attribuut gebruikt. Een geboortedatum is een relatief sterk onderscheidend en de technische noodzakelijkheid van de registratie en opslag ervan is/wordt daarom ook uitvoerig bediscussieerd en betwist op de CAcert-policy mailinglist. Voorlopig is er nog geen werkbaar alternatief om gelijknamige personen te kunnen onderscheiden en blijft de geboortedatum een centraal geregistreerd (persoons)gegeven. De geboortedatum kan alleen worden opgevraagd door waarmerkers, tijdens het waarmerkingsproces.

Handtekeningen

Betrouwbare tijdstempels. Het doel van een digitale handtekening is om een persoon of organisatie onweerlegbaar te verbinden aan een bepaalde handeling op een bepaalde tijd. De factor tijd is belangrijk: het moet niet mogelijk zijn om de tijdstempel van de handtekening te beïnvloeden naar een tijdstip in de toekomst of in het verleden. In een PKI kan daartoe een Time Stamping Authority (TSA) worden gebruikt, een betrouwbare tijdserver. Net als RAs wordt ook een TSA zelf gecertificeerd door de CA. De TSA genereert en ondertekent tijdstempels bij een gegeven handeling; andere partijen in de PKI kunnen de integriteit en authenticiteit van de tijdstempel (en van de handeling) controleren door verificatie van de handtekening[6]. CAcert heeft zelf geen TSA, en daardoor beschouwen sommigen CAcert ongeschikt voor het gebruik van digitale handtekeningen. Er bestaat een CAcert-gecertificeerde publieke TSA onder de naam OpenTSA(.org), maar de status en betrouwbaarheid daarvan is onbekend bij uw auteur. In algemene zin geldt dat de betrouwbaarheid van TSAs afhangt van de precisie en accuratesse van de klok, de betrouwbaarheid en beveiliging van de timestamping service (net zo zwaar als die van de CA) en de beveiliging en kwaliteit van de software.



Conclusie

Zijn de certificaten van CAcert en die van een commerciële PKI-aanbieder even betrouwbaar? Dat hangt af van het beoogde gebruik/doel van het certificaat, de eindgebruikers, de factoren die in een bepaalde situatie bepalen of een certificaat ‘betrouwbaar’ wordt geacht en de commerciële aanbieder waarmee wordt vergeleken. Beide soorten hebben voor- en nadelen en vanwege enkele vrij fundamentele verschillen lijkt deze vraag een “appels met peren”-vergelijking te verwoorden.

CAcert geeft certificaten kosteloos uit en heeft een focus op toepassing van certificaten voor persoonlijke security en privacy. De (beperkte) zekerheid die aan een certificaat kan worden ontleend wordt in eerste instantie bepaald door de zorgvuldigheid waarmee certificaathouders elkaars identiteit vaststellen. Nadelen van CAcert: het waarmerken is voor de meeste waarmerkers geen dagelijkse routine, ze hebben relatief klein eigenbelang bij zorgvuldigheid en vooral bij ad hoc processen is er dan een grotere kans op fouten/vergissingen; de relatieve onbekendheid van CAcert is een drempel (men vertrouwt een onbekende niet zomaar). Voordelen van CAcert: na verloop van tijd raken meestal meerdere waarmerkers betrokken bij de identificatie, waardoor eventuele fouten vanzelf worden gecompenseerd en het vertrouwen kan groeien (ook in punten); CAcert streeft uitdrukkelijk en merkbaar naar het privacyvriendelijk faciliteren van privacy en security (geen adresgegevens, geen centrale archieven, et cetera); certificaathouders worden altijd vis-à-vis gewaarmerkt en altijd op basis van officiële identiteitsbewijzen (in tegenstelling tot bijvoorbeeld een bankpas of geldtransactie); CAcert groeit wereldwijd met 25.000-30.000 nieuwe leden per jaar.

De meeste commerciele aanbieders vragen geld voor certificaten en hebben een focus op e-commerce. De (beperkte) zekerheid die aan een certificaat kan worden ontleend wordt in eerste instantie bepaald door de zorgvuldigheid waarmee de aanbieder zelf de identiteit van de certificaathouders vaststelt. Nadelen van commerciële aanbieders: certificaathouders worden vaak op afstand gewaarmerkt en soms alleen op basis van een geldtransactie; er is geen corrigerend systeem wanneer een RA (of de beperkte groep RAs) procedures onzorgvuldig naleeft (“single-point(s)-of-failure”); er wordt niet altijd zorgvuldig rekening gehouden met privacy. Voordelen van commerciële aanbieders: veel van de commerciële aanbieders zijn al ‘well-established’ en genieten naamsbekendheid; het centrale waarmerkingsmodel en enkelvoudige vertrouwen is duidelijk en overzichtelijk; er is een relatief groot eigenbelang bij zorgvuldige waarmerking (imagoschade is fataal voor TTPs).

Qua techniek, beleidsraamwerk en aansprakelijkheid is geen of nauwelijks verschil: voor zowel CAcert als commerciële PKI-aanbieders kunnen dezelfde vragen en twijfels worden opgeworpen. Welke procedures zijn er? Worden ze gecheckt? Is er een security handboek? Is er een RA handboek? Hoe openbaar is deze informatie (‘public scrutiny’ helpt niet alleen bugs uit software, maar ook bugs uit procedures)? Hoe zit het met technische beveiliging van de CA en de geheime sleutel van de CA? Aansprakelijk-

[4] Ter informatie (niet ter overtuiging): deze databaseserver draait op een versleuteld bestandssysteem, en toegang tot de server is beperkt tot SSH-verbindingen vanaf een aantal IP-adressen. De server staat fysiek in een hoog beveiligde ruimte (soort bunker) en achter een aparte firewall.

[5] De naam van een individu kan op verschillende manieren zijn weergegeven op verschillende identiteitsbewijzen. Soms staan op het ene bewijs alleen voorletters (bankpas: “T.E. Hagen”), volledige namen op een ander bewijs (paspoort: “Teunis Evert Hagen”) en iets daartussen op weer een ander bewijs (rijbewijs: “Teunis E. Hagen”). Het beleid van CAcert is dat punten alleen worden toegekend voor namen die precies overeenkomen, er moeten dus apart vertrouwenspunten worden verzameld voor elke weergave van een naam.

[6] Verondersteld wordt dat de ondertekening van de TSA geschiedt met zijn interne tijd.

vervolg volgende pagina>>

heid is bij zowel CAcert als commerciële aanbieders gebaseerd op 1) statements van de CA, 2) de overeenkomst tussen gebruikers en de CA, en 3) de claim voor de 'lezers' van certificaten die zelf geen deel uitmaken van de PKI (Non-Related Persons).
Met de kosteloze PKI-diensten voor persoonlijke security en privacy levert CAcert een dienst die nodig is en waarvoor steeds meer belangstelling komt. Privacy is bij uitstek een persoonsgebonden onderwerp en het web-of-trust waarmerkingsmodel en privacyvriendelijke dienstverleningsmodel van CAcert lijkt daar beter bij aan te sluiten dan een hiërarchisch model van 'opgelegd' vertrouwen. Uw auteur is in elk geval zelf tevreden eindgebruiker van CAcert.
Geïnteresseerde lezers worden verwezen naar *[Schneier03]* (over gebreken in certificaten) en *[Schneier00]* (over vertrouwen en schijnveiligheid).

Met dank aan Teus Hagen voor zijn waardevolle suggesties en feedback.

Vergelijking tussen commerciële CAs en CAcert (versimpeld overzicht)

	Commerciële CA	CAcert
Vaststelling van identiteit		
Door wie	Dienstverlener (centraal)	Certificaathouders (decentraal)
Op afstand / vis-a-vis	Vaak op afstand, soms vis-a-vis	Altijd vis-a-vis
Bewijsvoering	Vaak officieel ID-bewijs, soms alleen geldtransactie	Altijd officieel ID-bewijs
Vertrouwen nodig	In dienstverlener	Tussen certificaathouders
Voordelen	Gestroomlijnd dagelijks proces, veel kennis/ervaring	Geen centraal archief kopie-identiteitsbewijs
	Groot eigenbelang bij zorgvuldigheid	Geen single-point-of-failure, want meerdere RAs
Nadelen	Evt. centraal archief kopie-identiteitsbewijs	Geen dagelijks proces (ad-hoc)
	Single-point-of-failure bij onzorgvuldige RA	Klein eigenbelang bij zorgvuldigheid
Kosten		
Kosten	Per certificaat en/of entree- en abonnementskosten	Geen
Certificaatsoorten		
Server (bijv. HTTPS, SSL-VPN)	Ja	Ja, maar <50pt max 6.mnd geldig
Client (bijv. S/MIME, SSL-VPN)	Ja	Ja, maar <50pt niet op naam
Techniek		
Certificaten	X.509	X.509
Smartcards mogelijk	Ja	Ja
Beleidsstukken		
Beleidsstukken	CP, CPS	CP, CPS, Community Agreement, NRP
Toepassingen		
"Veel gezien"	E-commerce	Persoonlijke privacy
"Minder gezien, ook mogelijk"	Persoonlijke privacy	E-commerce

Bronnen

[CAcert] CAcert (website), www.cacert.org
[Lioy06] "PKI past, present and future" (artikel); Lioy, Marian, Moltchanova en Pala; International Journal of Information Security (2006) 5: 18–29
[Oophaga] Oophaga Foundation (website), www.oophaga.nl
[Schneier00] "Secrets and Lies" (boek), Bruce Schneier, 2000, John Wiley & Sons, ISBN 0-471-25311-1
[Schneier03] "Practical Cryptography" (boek), Niels Ferguson en Bruce Schneier, 2003, Wiley, ISBN 0-471-22357-3