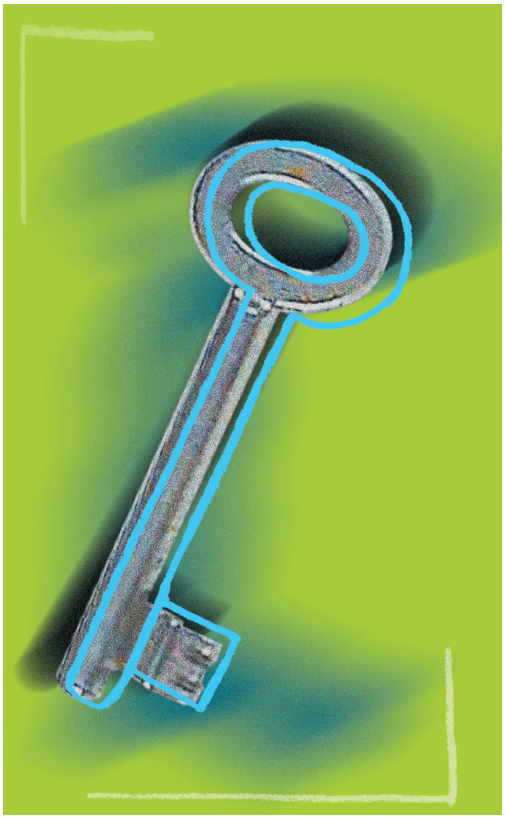


CAcert – die Community CA

Chancen und Grenzen einer gemeinnützigen Certificate Authority (CA)

Digitale Zertifikate helfen bei der Absicherung von Applikationen, Web-Anwendungen und der Unternehmenskommunikation. Gerade in kleineren und mittelständischen Unternehmen scheitern entsprechende Projekte jedoch oftmals aus Budgetgründen. Sind kostenlose digitale Zertifikate eines communitybasierten Anbieters eine Alternative für den Unternehmenseinsatz?

Von Jens Paul, Pirmasens

X.509-Zertifikate helfen Authentizität, Integrität und Vertraulichkeit zu sichern und bilden somit eine wichtige Grundlage interner und externer Kommunikation. In der Praxis scheitert ein unternehmensweiter Einsatz von digitalen Zertifikaten zur Absicherung von Servern und E-Mail-Kommunikation – gerade bei kleinen und mittelständischen Betrieben – jedoch häufig am begrenzten Budget der IT-Abteilung.

Bereits bei einem Bedarf von 100 E-Mail-Zertifikaten für Mitarbeiter, drei SSL-Zertifikaten für Web-Server und zwei Code-Signing-Zertifikaten für Entwickler können leicht jährliche Kosten von rund 5.000 € alleine für die Bereitstellung der Zertifikate anfallen – eine Investition, die häufig unterbleibt. Private Anwender scheuen erst recht Ausgaben für Zertifikate kommerzieller Anbieter, deren Nutzen sich ihnen heute ohnehin kaum erschließt – auch geringe jährliche Ausgaben erscheinen den weitaus meisten nicht akzeptabel, mehrere hundert Euro für ein Server-Zertifikat auch Enthusiasten schlichtweg als nicht tragbar.

Es stellt sich die Frage, wie man ohne entsprechende Bereitschaft zu Investitionen in eine Public-Key-Infrastruktur eine deutliche Steigerung der Sicherheit von Internet-Kommunikation erreichen kann. 2002 hatte der Australier Duane Groth auf der Suche nach einem Weg hierfür die Idee, auch bei X.509-Zertifikaten die zentralisierte Identitätsprüfung kommerzieller Anbieter durch ein Web of Trust (WoT) zu ersetzen, wie man es in ähnlicher Form von PGP kennen mag.

Web of Trust

In einem solchen Netzwerk folgt das Vertrauen in die Authentizität eines Zertifikats aus dem „verketteten" Vertrauen in die Überprüfung durch üblicherweise mehrere, möglicherweise unbekannte Dritte, deren Identität wiederum von Dritten überprüft worden ist. Hierbei kann (im allgemeinen Fall) eine Reihe festzulegender Parameter ins Spiel kommen, etwa ein Mindestmaß an unabhängigen Identitäts-Checks, eine maximale Zahl von Intermediären oder Bedingungen für die Vertrauenswürdigkeit der Aussagen bestimmter Personen(gruppen).

Aufgrund dieser Idee hat Groth das Projekt CAcert ins Leben gerufen (www.cacert.org); 2003 wurde der gemeinnützige Verein CAcert Inc. gegründet. Wichtigstes Ziel von Projekt und Verein ist weiterhin die Bereitstellung beliebig vieler E-Mail-, SSL- und Code-Signing-Zertifikate, unabhängig von der Art des Benutzers (Privatleute, Unternehmen, Organisationen etc.) und seiner Herkunft.

Während bei PGP jeder Anwender die Parameter für „sein" Web of Trust selbst festlegen kann (und muss), erfordert die streng hierarchische X.509-Welt ein anderes Vorgehen: Hier legt die „Vertrauensgemeinschaft" die Regeln für alle Teilnehmer eindeutig fest (s. u.) und erstellt auf dieser Basis „allgemeingültige" Zertifikate. Wie bei jeder Certificate Authority (CA) muss man sich auch hier die Frage stellen, ob diese Zertifizierungsrichtlinien (Certification Policy bzw. Certification Practice Statement – CPS) dem

geplanten Einsatz- beziehungsweise Nutzungszweck gerecht werden.

Mit höchster Gewissheit kann man letztlich einem digitalen Zertifikat nur dann vertrauen, wenn man sich persönlich von der Identität seines Kommunikationspartners überzeugt hat – und hinreichend fundierte Kenntnisse zur Prüfung von Ausweispapieren besitzt. Der Prüfung einer CA zu vertrauen, egal ob kommerziell oder gemeinnützig, birgt immer ein gewisses Restrisiko.

Die meisten Personen und Organisationen werden dieses Restrisiko tragen, da die Alternative der persönlichen Identitätsüberprüfung jedes Kommunikationspartners schlichtweg nicht praktikabel ist. Es stellt sich also letztlich die Frage nach dem Prozess der Identitätsprüfung: Im Rahmen des Web of Trust von CAcert erfolgt sie prinzipiell durch mehrere so genannte Assurer. Die Identität aller Assurer wurde ebenfalls mehrfach überprüft – persönlich und unmittelbar anhand von Ausweispapieren durch bestehende Assurer (eine bis vor Kurzem mögliche Prüfung durch Beglaubigung mindestens zweier „Trusted Third Parties" wie Notare oder öffentliche Stellen ist in Deutschland und einigen weiteren Ländern mittlerweile nicht länger verfügbar).

Assurance

Konnte bislang jeder ausreichend identitätsgeprüfte Community-Teilnehmer selbst (in zunächst begrenztem Umfang, s. u.) als Assurer auftreten, so sind ab September 2007 hierfür zusätzlich die Bearbeitung von Schulungsunterlagen (E-Learning) und ein erfolgreicher Online-Test erforderlich (siehe http://wiki.cacert.org/wiki/EducationCampus). Behandelte Themen sind dabei Zertifikate und ihre Nutzungsmöglichkeiten sowie die Kontrolle von Ausweisen.

Um die als Vorbedingung notwendigen „Prüfpunkte" zu erhalten, muss ein Assurer in spe im Normalfall von mindestens zehn unerfahrenen Prüfern oder mindestens drei top-erfahrenen Prüfern erfolgreich „assured" worden sein (vgl. Tab. 1). Eine Ausnahme bilden lediglich Identitätsprüfungen und Punktezuweisungen durch so genannte Super-Assurer, die von besonders befähigten und (temporär) ermächtigten CAcert-Teilnehmern im Rahmen von Messen und Veranstaltungen durchgeführt werden.

Durch dieses „Viele-Augen"-Prinzip und die gesteigerten Anforderungen an das Sachverständnis von Community-Teilnehmern, die selbst

Was CAcert nicht kann...

CAcert sieht sich nicht als Konkurrenz zu kommerziellen Anbietern, sondern vielmehr als sinnvolle Ergänzung, vor allem dort, wo PKI „nichts kosten darf". Durch die Community-basierte Struktur und die Zielsetzung, kostenlose Zertifikate anzubieten, ergeben sich prinzipbedingt einige Einschränkungen gegenüber kommerziellen Zertifizierungsdiensten:

_____ Support-Anfragen werden durch das Freiwilligen-Team von CAcert und durch die Community bearbeitet. Auch wenn das oft schneller und umfassender als bei einem kommerziellen Anbieter erfolgt, kann CAcert keinerlei Garantie für eine Bearbeitung geben oder bestimmte Reaktionszeiten gewährleisten. Sofern ein Unternehmen bei Problemen definierte Antwortzeiten benötigt, ist von einem Einsatz der CAcert-Zertifikate abzuraten.

_____ CAcert bietet keinerlei Versicherung für den Einsatz der Zertifikate an und übernimmt keinerlei Haftung für entstandene Schäden. Dies sollte insbesondere bei einem Einsatz im E-Commerce-Umfeld berücksichtigt werden.

_____ CAcert ist keine durch die Bundesnetzagentur akkreditierte Zertifizierungsinstanz. Mit den ausgestellten Zertifikaten können daher keine qualifizierten Signaturen im Sinne des deutschen Signaturgesetzes (SigG) erstellt werden.

_____ Das CAcert-Root-Zertifikat ist zwar bereits in einigen Linux-Distributionen integriert, *nicht* jedoch standardmäßig in den verbreiteten Browsern. Aktuell unterzieht sich CAcert einer Auditierung der Mozilla Foundation, nach deren Abschluss die Integration in die Browser angestrebt ist. Bis dahin ist zur Nutzung der CAcert-PKI in aller Regel eine einmalige Prüfung und Aufnahme der Class-1- und Class-3-Root-Zertifikate in den Zertifikatspeicher vonnöten:

```
Class 1 PKI Key
Fingerprint SHA1:
13:5C:EC:36:F4:9C:B8:E9:
3B:1A:B2:70:CD:80:88:46:
76:CE:8F:33
Fingerprint MD5:
A6:1B:37:5E:39:0D:9C:36:
54:EE:BD:20:31:46:1F:6B

Class 3 PKI Key
DB:4C:42:69:07:3F:E9:C2:
A3:7D:89:0A:5C:1B:18:C4:
18:4E:2A:2D
Fingerprint MD5:
73:3F:35:54:1D:44:C9:E9:
5A:4A:EF:51:AD:03:06:B6

GPG Key
1024D/65D0FD58 2003-07-11 CA
CertSigningAuthority(RootCA)
Fingerprint:
A31D 4F81 EF4E BD07 B456
FA04 D2BB 0D01 65D0 FD58
```

Download der X.509-Zertifikate und GPG-Schlüssel über www.cacert.org/index.php?id=3

als Assurer mitarbeiten möchten, sieht sich CAcert dem Vergleich mit kommerziellen Angeboten durchaus gewachsen, auch wenn es mit diesen nicht konkurrieren möchte. Man bedenke, dass bei vielen Angeboten die Identitätsüberprüfung in Deutschland häufig über das so genannte PostIdent-Verfahren erfolgt, bei dem ein Mitarbeiter einer Postfiliale oder -agentur oder der Zusteller die Personalien eines Antragstellers überprüfen. Eine zusätzliche Prüfung durch weitere Personen erfolgt üblicherweise ebensowenig wie eine Schulung der Post-Mitarbeiter bezüglich der Thematik digitaler Zertifikate.

Die Manipulation einer Identitätsüberprüfung ist bei beiden Verfahren theoretisch denkbar – beide Verfahren versuchen jedoch Manipulationsmöglichkeiten zu vermeiden. Die Frage, welchem Verfahren mehr Vertrauen entgegengebracht werden kann, lässt sich nicht pauschal abhandeln; jeder PKI-Nutzer muss sie letztlich für sich selbst beantworten. Bei Bedenken gegenüber einem verteilten communitybasierten Prüfansatz möge man sich jedoch auch vergegenwärtigen, dass die praktische Alternative zu kostenlosen CAcert-Zertifikaten heute oft darin bestünde, überhaupt kein Zertifikat – und somit keinerlei Identitätsprüfung – zur Verfügung zu haben. Einige prinzipbedingte Einschränkungen von CAcert-Zertifikaten gegenüber kommerziellen Angeboten beschreibt der Kasten auf Seite 55.

Einzelpersonen

Wer für sich selbst und für eigene Domains die Möglichkeiten von CAcert nutzen möchte, muss zunächst ein Konto auf www.cacert.org anlegen. Zur Registrierung werden Name, Geburtsdatum, primäre E-Mail-Adresse und ein Kennwort abgefragt; zusätzlich können noch Fragen zur Kennwort-Wiederherstellung hinterlegt werden. Das System verschickt dann eine Challenge-E-Mail mit einem speziellen Link an die angegebene Adresse, um zu verifizieren, dass der frisch Registrierte auch tatsächlich Inhaber des angegebenen Mail-Accounts ist. Bereits nach Bestätigung dieses Links kann der Anwender Zertifikate ausstellen, die aber mangels erfolgter Identitätsüberprüfung noch keine Aufnahme des Namens ermöglichen.

Zur Identitätsüberprüfung ist es notwendig, sich mit mehreren verschiedenen Assurern persönlich zu treffen. Dies kann auf IT-Messen wie der SYSTEMS (s. S. 58) oder im Rahmen lokaler Anwendertreffen erfolgen (siehe http://blog.cacert.org/). Alternativ besteht die Möglichkeit,

Tabelle 1: Assurance-Punkte und ihre Auswirkung im CAcert-Bewertungssystem

Punkte / Status	Bedeutung
0–49 Punkte „not assured"	– die angegebene E-Mail-Adresse wurde validiert – es kann ein Client-Zertifikat mit einer Gültigkeit von 12 Monaten ausgestellt werden – es kann ein Server-Zertifikat mit einer Gültigkeit von 6 Monaten ausgestellt werden – keine Aufnahme des Namens in das Zertifikat möglich
50–99 Punkte „assured"	– der Name des Anwenders kann in das Zertifikat aufgenommen werden – Server-Zertifikate sind 24 Monate lang gültig – vorhandene PGP-Schlüssel können durch CAcert signiert werden
100 Punkte	– maximale Punktzahl im Rahmen von Identitätsüberprüfungen des Web of Trust – Beantragung eines Code-Signing-Zertifikats möglich – Möglichkeit, Assurer zu werden: Hierzu ist die Bearbeitung der Schulungsunterlagen mit anschließender Online-Prüfung erforderlich (ab Herbst 2007)
100–149 Punkte + Prüfung „Assurer"	– Assurer können bei Überprüfungen Dritter maximal folgende Punkte vergeben: ab 100 Punkten: 10 Punkte ab 110 Punkten: 15 Punkte ab 120 Punkten: 20 Punkte ab 130 Punkten: 25 Punkte ab 140 Punkten: 30 Punkte ab 150 Punkten: 35 Punkte – für jede durchgeführte Überprüfung (Assurance) steigt der Punktestand eines Assurers um 2 Punkte.
150 Punkte „fully assured" – maximale Punktzahl durch Tätigkeit als Assurer	– maximale Punktzahl im Rahmen des Trusted-Third-Party-(TTP)-Programms (TTP war eine Sonderform der Assurance, bei der die Identitätsprüfung durch einen vertrauenswürdigen Dritten – z. B. einen Notar – durchgeführt wurde; diese Variante ist in Deutschland und einigen weiteren Ländern nicht länger verfügbar)
200 Punkte	„Super Assurer" – temporärer Status, der nur in Gebieten mit sehr geringer Assurer-Dichte vergeben werden kann – erfordert eingehende Überprüfung der Person und kann nur vom CAcert-Vorstand erteilt werden – ein Super Assurer kann auch über 35 Punkte vergeben – die Weiterführung des „Super Assurer"-Programms wird derzeit geprüft

über die Funktion „Finde einen Assurer“ mit Community-Teilnehmern in der Nähe Kontakt aufzunehmen, die als Assurer tätig sind. Im Rahmen des persönlichen Treffens überprüft der Assurer die Identität des Antragstellers anhand mindestens eines, besser zweier amtlicher Lichtbildausweise (Personalausweis, Reisepass, Führerschein). Nach erfolgter Überprüfung vergibt er zwischen 10 und maximal 35 Vertrauenspunkte und schreibt diese dem CAcert-Account des Überprüften gut.

Sobald ein Anwender mindestens 50 Punkte erreicht hat, kann er auch seinen Namen in Zertifikate aufnehmen und erhält so vollwertige SSL- und E-Mail-Zertifikate. Ab 100 erreichten Punkten kann der Teilnehmer auch ein Code-Signing-Zertifikat erhalten und selbst Assurer werden. Es bleibt festzuhalten, dass bei der Assurance keine einzelnen Zertifikate geprüft werden, sondern die persönliche Identität des Teilnehmers. Dieser kann sich anschließend über die Web-Oberfläche beliebig viele Zertifikate von CAcert signieren lassen. Für jede erstmals zugeordnete E-Mail-Adresse und Domain prüft das System zuvor, dass diese auch tatsächlich dem „Herrschaftsbereich“ des Teilnehmers unterstehen.

Zertifikate für Unternehmen

Der Prozess der persönlichen Assurance ist ab einer gewissen Unternehmensgröße jedoch keine praktikable Vorgehensweise mehr. Im Jahr 2006 hat CAcert daher ein Pilotprojekt zur Organisations-Assurance (OA) gestartet. Bei einer OA stellt *das Unternehmen* einen Antrag auf Zertifizierung und benennt mindestens einen Administrator, der über einen CAcert-Account verfügen und „assured“ sein muss. Hierzu wird ein Antragsformular vom Unternehmen ausgefüllt und zusammen mit weiteren Dokumenten (z. B. beglaubigter Handelsregisterauszug) an einen speziell benannten Organisations-Assurer von CAcert gesendet oder diesem übergeben.

Nach erfolgreicher Überprüfung des Antrags (Name des Unternehmens, Rechtsform, Vertretungsberechtigung, Domain-Rechte etc.) erfolgt die Freigabe durch den Organisations-Assurer. Ab diesem Zeitpunkt stehen dem angegebenen Administrator die im Folgenden genannten zusätzlichen Möglichkeiten in seinem Account zur Verfügung – alle durch den Administrator des Unternehmens ausgestellten Zertifikate enthalten dabei immer zwingend den Namen des Unternehmens:

_____ Hinzufügen einer Domain mit anschließender Verifizierung mittels einer E-Mail Anfrage,
_____ Aufnahme einzelner Organisations-Einheiten (OU),
_____ Signieren von Server-Zertifikaten für das Unternehmen,
_____ Ausstellen von Client-Zertifikaten für die Mitarbeiter des Unternehmens, ohne die Notwendigkeit den normalen Assurance-Prozesses durchlaufen zu müssen,
_____ Aufnahme weiter gehender Informationen in das Zertifikat (z. B. Name des Unternehmens, Adresse,...),
_____ Nutzung der CAcert-API, um die Ausstellung von Zertifikaten zu automatisieren.

Das Pilotprojekt der OA (primär in Deutschland und Österreich) wurde im Sommer 2007 nach der Aufnahme von rund 130 Organisationen erfolgreich abgeschlossen. Die zugrunde liegende Policy wird zurzeit von CAcert auf Basis der gesammelten Erfahrungen für die internationale Verwendung ergänzt, die weltweite Freigabe wird für den Herbst 2007 erwartet.

Das Projekt hat dabei auch gezeigt, dass bei den teilnehmenden Unternehmen ein hoher Beratungsbedarf hinsichtlich der Möglichkeiten der OA und dem Einsatz digitaler Zertifikate besteht. Es wurde daher angedacht, für erfahrene Assurer eine Zusatzqualifikation und Ausbildung zum „Organisation Assurance Consultant“ anzubieten. Entsprechende Umsetzungsmöglichkeiten werden derzeit innerhalb des Projekts erörtert.

Einsatzmöglichkeiten im Unternehmen

Die Einsatzmöglichkeiten im Unternehmenseinsatz sind PKI-typisch vielfältig. Einige Beispiele sind die Absicherung von Web-Server-Verbindungen (SSL/TLS), die Verschlüsselung von E-Mail-Kommunikation (S/MIME, PGP/GPG) und die zertifikatsbasierte Authentifizierung von Clients an Web-Servern (anstelle von Kennwörtern). Die zulässigen Einsatzmöglichkeiten der Zertifikate sind im Certification Practice Statement (CPS) geregelt, das auf http://wiki.cacert.org/wiki/CPS eingesehen werden kann. Mit den von CAcert bereitgestellten Zertifikaten kann jedoch *keine* qualifizierte Signatur im Sinne des deutschen Signaturgesetzes (SigG) erzeugt werden; von einer Verwendung zur Signatur elektronischer Rechnungen ist daher abzuraten.

Chancen für ISPs und Systemhäuser

Neben dem steigenden Interesse bei Endanwendern ist seit der diesjährigen CeBIT auch eine verstärkte CAcert-Integration in das Portfolio von Systemhäusern und Internet Service Providern (ISP) festzustellen. Die Einsparungen des Kostenblocks „Zertifikate“ ermöglicht dann den Kunden, verstärkt in ein professionelles PKI-Rollout oder die Benutzerschulung zu investieren. Die Aufnahme von CAcert-Zertifikaten in das Angebotsportfolio eines Systemhauses bedeutet daher keineswegs den Wegfall eines Umsatzgaranten, sondern führt vielmehr zu einer Verschiebung der Umsätze in den deutlich lukrativeren Bereich der Dienstleistungen.

Im Privatkundenvertrieb könnte ein Mehrwert geschaffen werden, indem die Identität eines Kunden beim Kauf eines Systems direkt überprüft und das passende Zertifikat in seine E-Mail-Umgebung eingebunden wird. Und im Bereich des Webhostings stellen ISPs zunehmend ihren Kunden kostenfreie SSL-Zertifikate zur Absicherung des Web-Auftritts zur Verfügung; durch die Verwendung von Community-Zertifikaten kann dieses Angebot besonders kostengünstig realisiert werden.

Nachhaltigkeit

Nach 161 Benutzern im Gründungsjahr und knapp 3000 im Folgejahr, hat CAcert 2006, vier Jahre nach Projektstart, bereits über 75000 Benutzer mit über 200000 Zertifikaten erfasst. Die größte Verbreitung findet man in Deutschland und den Niederlanden, gefolgt von Österreich, den USA und Australien. Das Jahr 2007 ist von deutlichen Veränderungen im Bereich der Infrastruktur und der Personalstruktur geprägt, wodurch der Verein die notwendigen Kapazitäten für ein weiterhin exponentielles Wachstum schaffen will.

Die einzelnen CAcert-Fachbereiche (Support, Ausbildung, PR, Systemadministration, Audit etc.) werden jeweils durch einen so genannten Officer verantwortet, der ein den Anforderungen angepasstes Team leitet. Diese Officer arbeiten eigenverantwortlich in ihrem Bereich, berichten jedoch regelmäßig an den Vereinsvorstand, der seit den Wahlen im Mai 2007 aus dem Präsidenten Greg Rose (USA), dem Schatzmeister Robert Cruikshank (Australien) und dem Sekretär Evaldo Gardenali (Brasilien) besteht.

Parallel zu dieser „Führungshierarchie“ existiert noch die Advisory Group, welche den Vereinsvorstand bezüglich der strategischen Ausrichtung berät. Zudem dient die Advisory Group auch als Bindeglied zwischen der Community und dem Vorstand; sie besteht zurzeit aus Teus Hagen (Niederlande), Ian Grigg (Australien) und Jens Paul (Deutschland).

Die wichtigste personelle Grundlage von CAcert sind natürlich die Assurer. Heuer wurde daher im Sinne der Qualitätssicherung der bereits erwähnte Education Campus aufgebaut, der angehenden Assurern als Grundlage für ihren „Zulassungstest“ einen Ausbildungsworkshop zur Verfügung stellt. Für Bearbei-

CAcert auf der SYSTEMS

Auf der diesjährigen SYSTEMS (München, 2007-10-23/26) führt CAcert auf der IT-SecurityArea in Halle B3 (wie immer kostenlose) persönliche Assurances durch. Für die Vorbereitung von Organisation-Assurances (OA) werden kompetente Ansprechpartner vor Ort sein, um Möglichkeiten und Erfordernisse zu besprechen und gemeinsam die Anträge weitgehend vorzubereiten. Da der oder die vorgesehenen Administratoren für eine OA aber auch selbst überprüfte CAcert-Teilnehmer sein müssen, ist ein persönliches Erscheinen empfehlenswert.

Checkliste persönliche Assurance

vorab: Anlegen persönlicher CAcert-Accounts auf www.cacert.org

_____ zwei gültige amtliche Lichtbildausweise

_____ (möglichst vorausgefüllte) persönliche Antragsformulare

_____ persönliches Erscheinen ist notwendig!

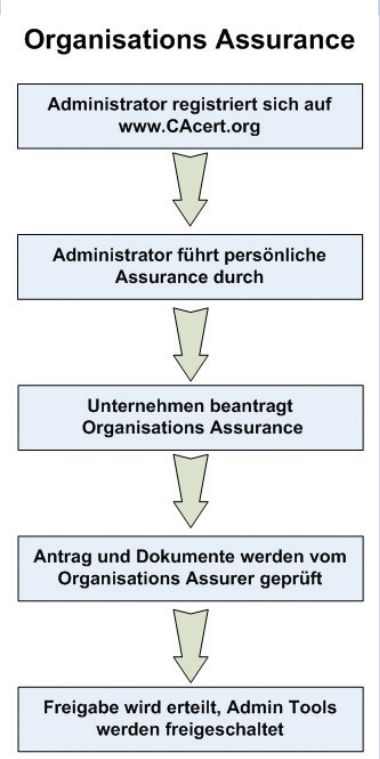
Organisations-Zertifizierung

Da die OA-Policy sich zum Redaktionsschluss noch in Überarbeitung befand, kann an dieser Stelle nur auf das CAcert-Blog verwiesen werden (http://blog.cacert.org/), das zu gegebener Zeit über die neuen Richtlinien berichten wird. Für spezifische Rückfragen vor der Messe wenden Sie sich bitte per E-Mail an:

CAcert Organisation Review Germany
c/o Dipl. -Rpfl. (FH)
Michael Grigutsch
E-Mail: michael@cacert.org

CAcert Organisation Review Austria
c/o Mag. Georg Markus Kainz
E-Mail: kainz@cacert.at

für alle anderen Länder:
support@cacert.org



Auch eine Organisations-Assurance erfordert überprüfte Administratoren – persönliche Assurance und Beratung sowie Vorbereitung des OA-Antrags können auf der SYSTEMS erfolgen.

tung der Organisations-Assurance ist angesichts der notwendigen Überprüfungen nicht zuletzt eine intensive Kenntnis der Rechtsformen von Organisationen notwendig. Im Rahmen des Pilotprojekts war daher neben der individuellen Schulung und der CAcert-Erfahrung auch eine juristische Ausbildung die Voraussetzung für Organisations-Assurer.

Auch die technische Infrastruktur wurde erneuert: Das Hosting für CAcert erfolgt seit diesem Jahr in einem Hochsicherheitsrechenzentrum in den Niederlanden, darüber hinaus steht ein Backup-Rechenzentrum in Österreich zur Verfügung. Der physische Zugang zu den Servern erfolgt nach den üblichen Verfahrensweisen eines Hochsicherheits-RZ, weiterhin ist eine Vier-Augen-Regelung in Kraft; alle Administratoren im Bereich der primären Systeme (Datenbank, Zertifikatsprozesse etc.) werden einer Sicherheitsüberprüfung unterzogen.

Weitere technische Rahmenbedingungen: Im Einsatz sind Sun-Server und Firewall-Lösungen von TUNIX; als Betriebssystem arbeitet eine angepasste Debian-Linux-Distribution. Alle internen Kommunikationsverbindungen sind verschlüsselt, weitestgehend kommen hierbei OpenSSL sowie GnuPG zum Einsatz. Das gesamte Benutzerfrontend von CAcert ist in PHP entwickelt und wird getrennt von den Signatur-Servern gehostet; die Anbindung an diese erfolgt über eine serielle Verbindung. Die Datenspeicherung erfolgt ausschließlich auf Servern innerhalb der EU unter Berücksichtigung der europäischen Datenschutzrichtlinien.

Das Projekt CAcert kann wohl nach fünf Jahren und mit heute rund 100 000 Benutzern guten Gewissens als etabliert bezeichnet werden. Der Community-Aspekt bedeutet auf der einen Seite zwar die Abhängigkeit von freiwilligen Helfern, auf der anderen Seite jedoch auch die Sicherheit eines riesigen Expertenpools, auf den zurückgegriffen werden kann.

Der Finanzbedarf von CAcert ist im Vergleich zu einem kommerziellen Anbieter drastisch reduziert: Verbleibende Kostenblöcke sind vor allem der Betrieb der Infrastruktur, Ausgaben im Rahmen von Messeauftritten sowie Reisekostenerstattungen. Diese Kosten werden ausschließlich durch individuelle Spenden von Privatleuten und Unternehmen sowie durch Zuwendungen von Stiftungen gedeckt.

Dass CAcert ein „ernsthaftes“ Projekt ist, sollten diese Ausführungen hinreichend untermauert haben. Wird es langfristig existieren? Durch die 2007 durchgeführten strukturellen Veränderungen, eine starke Community und bestehende Finanzierungszusagen spricht alles dafür! ■

Elemente eines CAcert-Zertifikats

Je nach Art des Zertifikats (Client Server) und Art des Antragstellers (Privatperson / Organisation) können über die Web-Oberfläche oder (mit Einschränkungen) über die API unterschiedliche Informationen in die CAcert-Zertifikate integriert werden:

Client-Zertifikate
_____ Name
_____ E-Mail-Adresse

Persönliche Server-Zertifikate
_____ (Host-)Name
_____ SubjectAlternativeName

Organisations-Zertifikate
Organisationszertifikate enthalten zusätzlich
_____ Name der Organisation
_____ Adresse
_____ Abteilung (OU)

Jens Paul (j.paul@paul-dv.de) ist geschäftsführender Gesellschafter des IT-Systemhauses Paul-Datenverarbeitung GmbH in Pirmasens. Innerhalb des Projektes CAcert (www.cacert.org) ist er Mitglied der Advisory Group und als Education Officer verantwortlich für alle Ausbildungsfragen.