CAcert – die Community CA

Chancen und Grenzen einer gemeinnützigen Certificate Authority (CA)

Der Einsatz digitaler Zertifikate zur Absicherung von Web-Anwendungen und der Unternehmenskommunikation ist auf dem Vormarsch. Gerade in kleineren und mittelständischen Unternehmen scheitern entsprechende Projekte jedoch oftmals aus Budgetgründen. Sind kostenlose digitale Zertifikate eines gemeinnützigen, Community basierten Anbieters eine Alternative für den Unternehmenseinsatz?

Von Jens Paul, Pirmasens

Authentizität, Integrität und Vertraulichkeit bilden die Grundlage jeglicher interner und externer Kommunikation eines Unternehmens. Durch den Einsatz digitaler Zertifikate nach dem X.509 Standard kann diese Anforderungen mit minimalem Aufwand und ohne Beeinträchtigung der Anwender erreicht werden.

In der Praxis scheitert ein Unternehmensweiter Einsatz von digitalen Zertifikaten zur Absicherung der Web-Server und der email-Kommunikation gerade im Bereich der kleinen und mittelständischen Unternehmen jedoch häufig am begrenzten Budget der IT-Abteilung. Bei einem typischen mittelständischen Unternehmen mit einem Bedarf von 100 email-Zertifikaten für die Mitarbeiter, 3 SSL-Zertifikaten für die Absicherung der Web-Server und 2 Code-Signing Zertifikaten für die Entwickler entsteht bereits ein jährlicher Kostenblock von ca. € 5.000 alleine für die Bereitstellung der Zertifikate. Ein Investment, welches häufig nicht getätigt wird.

Dazu ergänzend sollte auch der Bereich der privaten Anwender betrachtet werden. In diesem Umfeld haben digitale Zertifikate kommerzieller Anbieter kaum eine Bedeutung. Ein Investment von € 20 pro Jahr ist für die meisten Anwender nicht akzeptabel, mehrere hundert Euro für ein SSL-Zertifikat schlichtweg nicht tragbar.

Wenn man diese Marktbetrachtung zu Grunde liegt, stellt sich die Frage, wie eine deutliche Steigerung der Sicherheit der Internet-Kommunikation erreicht werden kann, wenn ein Großteil der Anwender sich die dazu notwendigen digitalen Zertifikate nicht leisten kann oder leisten möchte.

Die Idee einer Community basierten Certificate Authority

Vor genau dieser Situation stand im Jahr 2002 der Australier Duane Groth. Er suchte nach einem Weg zur sicheren Kommunikation im Internet ohne auf ein kostenpflichtiges Zertifikat zurückgreifen zu müssen. Es entstand die Idee, anstelle einer bei kommerziellen Anbietern üblichen zentralen Identitätsüberprüfung (z.B. anhand des PostIdent Verfahrens), ein so genanntes Web of Trust (WoT) zu setzen. Bei einem WoT ergibt sich die Vertrauensstellung der Kommunikationspartner durch die gegenseitige Identitätsüberprüfung bei einem persönlichen Treffen. Je mehr Überprüfungen erfolgen, desto höher ist die erzielte Vertrauensstellung.

Aus dieser Idee wurde 2002 von Duane Groth das Projekt www.cacert.org ins Leben gerufen. Ein Jahr darauf wurde der gemeinnützige Verein CAcert Inc. gegründet.

Wichtigstes Ziel des Projektes und des Vereins ist die Bereitstellung beliebig vieler email-, SSL- und Code-Signing-Zertifikaten, unabhängig von der Art des Benutzers (Privatperson, Unternehmen, Organisation, etc.) und seiner Herkunft.

Registrierung und Identitätsüberprüfung einer Privatperson

Es muss zunächst die Homepage www.cacert.org aufgerufen und sich registriert werden. Zur Registrierung werden Name, Geburtsdatum, primäre email Adresse und Kennwort abgefragt. Zusätzlich können noch Fragen zur Kennwort Wiederherstellung hinterlegt werden. Nach erfolgter Registrierung wird eine vom System generierte email an die angegebene Adresse gesendet. Darin ist ein Link enthalten, durch welchen die angegebene email-Adresse validiert wird. Ab diesem Zeitpunkt kann der Anwender auf seinen Account zugreifen und sich Zertifikate ausstellen. Aufgrund der noch nicht erfolgten Identitätsüberprüfung ist zu diesem Zeitpunkt jedoch noch keine Aufnahme des Namens in das Zertifikat möglich.

Zur Identitätsüberprüfung ist es notwendig, sich mit mehreren Assurern (Personen, welche die Überprüfung durchführen) zu treffen. Dies kann auf IT Messen erfolgen oder im Rahmen von lokalen Anwendertreffen. Alternativ besteht auch die Möglichkeit über die Funktion „Finde einen Assurer“ mit lokalen Assurern Kontakt aufzunehmen.

Im Rahmen des persönlichen Treffens überprüft der Assurer die Identität des Antragstellers anhand eines amtlichen Lichtbildausweises (Personalausweis, Reisepass, Führerschein). Es wird jedoch empfohlen zwei Dokumente vorzuweisen, da gerade ältere Bilder auf Führerscheinen eine eindeutige Überprüfung erschweren.

Nach erfolgter Überprüfung vergibt der Assurer zwischen 10 und maximal 35 Vertrauenspunkten (die Anzahl der Punkte die ein Assurer vergeben kann hängt von seiner Erfahrung in der Arbeit als Assurer ab). Diese überträgt er nach dem Treffen (bei einer Messe kann es einige Tage in Anspruch nehmen) in das System, der Anwender erhält eine Benachrichtigung, sobald die Übertragung erfolgt ist.

Sobald ein Anwender mindestens 50 Punkte erreicht hat (d.h. mindestens 2 Assurer haben unabhängig voneinander seine Identität überprüft), kann der Name in das Zertifikat aufgenommen werden, ein vollwertiger Einsatz der SSL- und email Zertifikate ist möglich. Ab 100 erreichten Punkten kann der Anwender auch ein Code Signing Zertifikat erhalten und selbst Assurer werden (mehr dazu im weiteren Verlauf des Artikels)

Ausstellung von Zertifikaten für Unternehmen

Der Prozess der persönlichen Assurance ist ab einer gewissen Unternehmensgröße keine praktikable Vorgehensweise mehr. Im Jahr 2006 hat CAcert ein Pilotprojekt zur Organisations-Assurance (OA) gestartet. Bei einer OA stellt das Unternehmen einen Antrag auf Zertifizierung. Hierzu wird ein Antragsformular (u.a. mit Namen des Unternehmens, Rechtsform, Administratoren, etc.) vom Unternehmen ausgefüllt und zusammen mit weiteren Dokumenten (z.B. beglaubigter Handelsregisterauszug) an einen Organisations Assurer von CAcert gesendet.

Nach erfolgreicher Überprüfung des Antrages (Name des Unternehmens, Rechtsform, Vertretungsberechtigung, Domain-Rechte, etc.) und der eingereichten Dokumente erfolgt die Freigabe durch den Organisations Assurer.

Ab diesem Zeitpunkt stehen dem angegebenen Administrator (dieser muss bereits einen Account bei CAcert besitzen und assured sein, d.h. über mindestens 50 Vertrauenspunkte verfügen) weitere Möglichkeiten in seinem Account zur Verfügung. Er kann Zertifikate für das Unternehmen sowie die Mitarbeiter des Unternehmens ausstellen. Die Identitätsüberprüfung der Mitarbeiter obliegt ihm.

Alle durch den Administrator des Unternehmens ausgestellten Zertifikate enthalten immer zwingend den Namen des Unternehmens.

Das Pilotprojekt der OA (primär in Deutschland und Österreich) wurde im Sommer 2007 erfolgreich abgeschlossen. Die zugrunde liegende Policy wird zur Zeit von CAcert für die internationale Verwendung ergänzt, die weltweite Freigabe wird für Herbst 2007 erwartet. Alle im Rahmen des Pilotprojekts durchgeführten Unternehmens Assurances behalten Ihre Gültigkeit.

Aktuelle Verbreitung von CAcert

Nach 161 Benutzern im Gründungsjahr und knapp 3.000 im Folgejahr, konnten vier Jahre nach Projektstart im Jahre 2006 bereits über 75.000 Benutzer mit über 200.000 Zertifikaten bei CAcert begrüßt werden. Die größte Verbreitung von CAcert liegt in Deutschland und den Niederlanden, gefolgt von Österreich, den USA und Australien.

Im Jahre 2007 werden deutliche Veränderungen im Bereich der Infrastruktur und der Personalstruktur durchgeführt, wodurch die notwendigen Kapazitäten für ein weiterhin exponentielles Wachstum geschaffen werden. Nach Abschluss dieser Umstellungen will CAcert sein Engagement in diesen Ländern weiter verstärken und insbesondere auch in den osteuropäischen, amerikanischen und asiatischen Ländern eine stärkere Präsenz aufbauen.

Personelle Struktur von CAcert

Der wichtigste personelle Bestandteil von CAcert sind die Assurer, welche die Identitätsüberprüfungen im Rahmen eines persönlichen Treffens durchführen. Ab 100 Vertrauenspunkten kann ein Anwender bei Interesse Assurer werden. Im Jahr 2007 wurde im Sinne der Qualitätssicherung ein Education Campus aufgebaut. Im Rahmen des Education Campus steht allen angehenden Assurern ein Ausbildungsworkshop zur Verfügung. Dieser kann als Online Training bearbeitet oder im Rahmen eines Workshops auf einer Messe durchgeführt werden. Nach Bearbeitung der Ausbildungsunterlagen kann der angehende Assurer eine Online Zertifizierung ablegen. Anschließend erfolgt eine Freigabe für seine Tätigkeit als Assurer.

Die Bearbeitung der Organisations Assurance erfolgt durch die Organisations Assurer. Für die im Rahmen dieser Tätigkeit notwendigen Überprüfungen ist insbesondere eine intensive Kenntniss der Rechtsformen von Organisationen notwendig. Im Rahmen des Pilotprojekts wurde als Voraussetzung für einen Organisations Assurer neben der individuellen Schulung und der Erfahrung als Assurer auch eine juristische Ausbildung festgeschrieben. Die allgemein gültige, weltweite Policy wird gerade erarbeitet.

Die einzelnen Fachbereiche (Support, Ausbildung, PR, Systemadministration, Audit, etc.) werden jeweils durch einen Officer verantwortet, welcher ein den Anforderungen angepasstes Team leitet.

Die Officer arbeiten eigenverantwortlich in Ihrem Bereich, berichten jedoch regelmäßig an den Vereinsvorstand. Dieser besteht seit den Wahlen im Mai 2007 aus dem Präsidenten Greg Rose (USA), dem Schatzmeister Robert Cruikshank (Australien) und dem Sekretär Evaldo Gardenali (Brasilien).

Parallel zur Führungshierarchie existiert noch die Advisory Group, welche den Vorstand bzgl. der strategischen Ausrichtung von CAcert berät. Weiterhin dient die Advisory Group als Bindeglied zwischen der Community und dem Vorstand und kann in allen Bereichen auf Antrag der Community untersuchend und beratend tätig werden. Sie besteht zur Zeit aus Teus Hagen (Niederlande), Ian Grigg (Australien) und Jens Paul (Deutschland).

Infrastruktur

Das Hosting der CAcert Infrastruktur erfolgt ab 2007 in einem Hochsicherheitsrechenzentrum in den Niederlanden, weiterhin steht ein Backup-Rechenzentrum in Österreich zur Verfügung. Der physikalische Zugang zu den Servern erfolgt nach den üblichen Verfahrensweisen eines Hochsicherheitsrechenzentrums, weiterhin ist eine zwei Personen Regelung in Kraft. Alle Administratoren im Bereich der primären Systeme (Datenbank, Zertifikatsprozesse, etc.) werden einer Sicherheitsüberprüfung unterzogen.

Die Datenspeicherung erfolgt ausschließlich auf Servern innerhalb der EU unter Berücksichtigung der europäischen Datenschutzrichtlinien.

Einsatzmöglichkeiten im Unternehmenseinsatz

Die Einsatzmöglichkeiten im Unternehmenseinsatz sind vielfältig. Dies umfasst, ist jedoch nicht beschränkt auf:

- Absicherung von Web Servern, z.B. https Verbindungen, Webmail, Chat Foren, etc.
- Verschlüsselung von email Kommunikation.
- Zertifikats-basierte Authentifizierung an Web Servern anstelle einer Kennwort-basierten.

Die einzelnen zulässigen Einsatzmöglichkeiten der Zertifikate sind im Certificate Practice Statement (CPS) geregelt, welches auf der Homepage von CAcert eingesehen werden kann.

Mit den von CAcert bereitgestellten Zertifikaten kann keine qualifizierte Signatur im Sinne des deutschen Signaturgesetzes (SigG) erzeugt werden. Von einer Verwendung zur Signatur elektronischer Rechnungen ist daher abzuraten.

CAcert im Vergleich zu den kommerziellen Anbietern

CAcert sieht sich nicht als Konkurrenz zu den kommerziellen Anbietern, sondern vielmehr als sinnvolle Ergänzung, insbesondere in Kosten sensitiven Bereichen.

Durch die Community basierte Struktur und die Zielsetzung kostenlose Zertifikate anzubieten, ergeben sich einige Einschränkungen gegenüber den kommerziellen Anbietern:

- Alle Support Anfragen werden durch das Support Team von CAcert und der Community bearbeitet. Auch wenn die Bearbeitung oftmals schneller und umfassender als bei einem kommerziellen Anbieter erfolgt, kann CAcert keinerlei Garantie für eine Bearbeitung geben oder eine Reaktionszeit benennen. Sofern ein Unternehmen definierte Reaktionszeiten benötigt, ist von einem Einsatz der Zertifikate abzuraten.
- CAcert bietet keinerlei Versicherung für den den Einsatz der Zertifikate an und übernimmt keinerlei Haftung für entstandene Schäden. Dies sollte insbesondere bei einem Einsatz im eCommerce Umfeld berücksichtigt werden.
- CAcert ist keine durch die Bundesnetzagentur akkreditierte CA. Mit den ausgestellten Zertifikate können keine qualifizierte Signatur im Sinne des SigG erstellt werden.
- Das CAcert Root Zertifikat ist bereits in einigen Linux Distributionen integriert, jedoch noch nicht in den meisten Browsern (Internet Explorer, Firefox, Opera, etc.). Aktuell unterzieht sich CAcert einer Auditierung, nach deren Abschluss die Integration in die Browser angestrebt ist. Bis dahin muss die Vertrauensstellung von CAcert Zertifikaten noch vom Anwender akzeptiert werden.

Auditierung

Die Auditierung von CAcert stellt eine Herausforderung dar. Der Auditor trifft auf eine Kombination aus neuen Auditierungskriterien, kostenlosen Zertifikaten und einem ehrenamtlichen Engagement der Beteiligten. Diese Faktoren stellen eine Herausforderung für das herkömmliche Verständnis einer PKI dar.

Innerhalb von CAcert spielen Kosteneffizienz bei der Identitätsüberprüfung und Gewinnmaximierung keine Rolle. Dagegen liegt der Schwerpunkt auf den Risiken, Pflichten und Haftungsfragen der einzelnen Beteiligten. Die grundlegende Erwartungshaltung ist es, ein für alle Beteiligte fairen Prozess zu etablieren, welcher die Tatsache berücksichtigt, dass keine Produkte verkauft werden. CAcert empfindet es als wichtig, den Benutzern nicht nur zu sagen, was ein Zertifikat ist und kann, sondern auch wo die Einschränkungen einer Community basierten CA liegen. Diese Vorgehensweise ist deutlich umfangreicher als die im Rahmen einer klassischen Auditierung.

Ein entsprechendes Rahmenwerk zu erzeugen, welches diesen Anforderungen, und gleichzeitig auch den Anforderungen einer konventionellen PKI gerecht wird, ist ein enorme Herausforderung, welche CAcert Stück für Stück umsetzt.

Kann ich der Qualität eines Web of Trust (WoT) trauen?

Letztendlich kann man die Vertrauensfrage bei einem digitalen Zertifikat nur dann definitiv mit ja beantworten, wenn man sich persönlich von der Identität seines Kommunikationspartner überzeugt hat. 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.

Konzentrieren wir uns daher auf den Prozess der Identifikationsprüfung:

Im Rahmen des WoT von CAcert erfolgt die Identitätsüberprüfung durch die Assurer. Bei allen Assurern wurde die Identität mehrfach überprüft und sie durchlaufen eine Schulung in welcher u.a. die Themen Zertifikate und Ihre Nutzungsmöglichkeiten sowie die Kontrolle von Ausweisen behandelt werden. Das erlernte Wissen wird anschließend durch einen Test abgefragt. Erst mit zunehmender Erfahrung kann ein Assurer mehr Vertrauenspunkte vergeben. Weiterhin wird die Identität eines Antragstellers durch mehrere Personen überprüft.

Im Rahmen der kommerziellen Anbieter erfolgt die Identitätsüberprüfung normalerweise durch das so genannte PostIdent Verfahren, d.h. ein Mitarbeiter einer Postfiliale bzw. einer Postagentur überprüft die Identität eines Antragstellers. Eine Überprüfung durch weitere Personen erfolgt üblicherweise nicht, ebensowenig eine Schulung des Poststellenmitarbeiters bzgl. der Thematik digitale Zertifikate.

Eine Manipulation einer Identitätsüberprüfung ist bei beiden Verfahren theoretisch denkbar. Beide Verfahren versuchen jedoch eine Manipulation zu vermeiden.

Die Frage, welchem Verfahren mehr Vertrauen entgegengebracht werden kann, lässt sich nicht pauschal beantworten. Diese Frage sollte sich jeder Anwender selbst stellen.

Kann ein Community Projekt langfristig existieren ?

Das Projekt CAcert kann nach 5 Jahren und rund 100.000 Benutzern sicherlich als etabliertes Projekt bezeichnet werden. Der Community Aspekt birgt auf der einen Seite die Abhängigkeit von freiwilligen Helfern, auf der anderen Seite die Sicherheit eines riesigen Expertenpools auf den zurück gegriffen werden kann.

Der Finanzbedarf von CAcert konnte im Vergleich zu einem kommerziellen Anbieter drastisch reduziert werden. Als verbleibende Kostenblöcke sind insbesondere der Betrieb der Infrastruktur, Ausgaben im Rahmen von Messeauftritten sowie notwendige Reisekostenerstattungen zu nennen. Diese Kosten werden ausschließlich durch individuelle Spenden von Privatpersonen und Unternehmen sowie durch Zuwendungen von Stiftungen gedeckt.

Durch die 2007 durchgeführten strukturellen Veränderungen, einer starke Community und bestehenden Finanzierungszusagen, ist die langfristige Existenzfähigkeit von CAcert positiv zu beurteilen.

Chancen für Internet Service Provider (ISP) und Systemhäuser

Neben dem steigenden Interesse der Endanwender an dem von CAcert bereitgestellten Angebot ist insbesondere seit der diesjährigen CeBIT auch eine verstärkte Integration in das Portfolio der Systemhäuser und ISP festzustellen.

Die Einsparungen des Kostenblocks „Zertifikate“ erlaubt es den Kunden in ein professionelles Rollout der zertifikatsbasierten Infrastruktur oder eine 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, in dem ein Kunde beim Kauf eines Systems direkt assured, und das Zertifikat in seine Mailumgebung eingebunden wird. Gerade Neukunden können auf diese Weise einfach von der Servicequalität des Anbieters überzeugt werden.

Im Bereich des Webhostings stellen ISP zunehmend Ihren Kunden kostenfrei SSL Zertifikate zur Absicherung Ihres Web Auftritts zur Verfügung. Durch die Verwendung von Community Zertifikaten kann dieses Angebot kostengünstig realisiert werden.

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

((Hinweis an die Redaktion: Die folgenden Abschnitte sind vertiefende Informationen für die Darstellung in Textkästen. Sie beziehen sich auf den gesamten Artikel, Ihre Positionierung innerhalb des Artikels ist für das Leseverständnis nicht relevant))

X.509

X.509 ist ein ITU-T Standard für eine Public-Key-Infrastruktur (PKI). Er gilt als derzeit wichtigster Standard für digitale Zertifikate. X.509 setzt ein hierarchisches System von vertrauenswürdigen Zertifizierungsstellen voraus, welche die Zertifikate ausstellen.

Gemäß dem X.509 Standard muss ein entsprechendes Zertifikat immer an einen *Distinguished Name* oder einen *Alternative Name* wie beispielsweise eine email-Adresse gebunden sein.

Nahezu alle Browser besitzen im Lieferumfang ein vorkonfigurierte Liste vertrauenswürdiger Zertifizierungsstellen, welche durch die Benutzer um weitere ergänzt werden kann.

Weiterhin sieht X.509 vor, dass eine Zertifizierungsstelle ausgestellte Zertifikate ungültig machen kann, indem diese in die *Certificate Revocation List* (CRL, „Zertifikatssperrliste“) eingetragen werden.

Digitales Zertifikat

Ein Digitales Zertifikat (auch Zertifikat oder Public-Key-Zertifikat) sind strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen.

Durch ein digitales Zertifikat können Nutzer eines asymmetrischen Kryptosystems den öffentlichen Schlüssel einer Identität (z.B. einer Person, einer Organisation oder einem IT-System) zuordnen und seinen Geltungsbereich bestimmen.

Damit ermöglichen digitale Zertifikate den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch die korrekte Anwendung der öffentlichen Schlüssel.

Quelle: Wikipedia