



Digitale Zertifikate für Jedermann

- **Client-Zertifikate**
(für Mail-Signatur und -Verschlüsselung (s/mime), Web-Browser Authentication, ..)
- **Server-Zertifikate**
(für den Web-Server, Mail-Server, etc..)
- **Web-Of-Trust**
- **kostenfrei**

CACert - denn Autorisierungsverfahren, Sicherung der Privatsphäre oder vertraulicher Daten durch Verschlüsselung sind ein Grundbedürfnis in der digitalen Welt, das nicht vom Geldbeutel abhängen sollte.

Cacert ist eine nicht-kommerzielle (und nicht-Regierungs-) Organisation, ist eine sog. Zertifizierungs-Authority (Root-CA) für X.509 Zertifikate (nach RFC 2519).

CACert unterschreibt die von ihr ausgegebenen Zertifikate. Damit ist z.B. vertrauenswürdige und sichere („government strength“) email-Kommunikation möglich, auch mit Personen mit denen man zuvor noch nicht kommuniziert hat – und dabei übrigens kinderleicht zu bedienen.

Die Unterschrift durch CACert kostet nichts und wird auch nichts kosten: freie Verschlüsselung für jedermann ist ein Ziel von CACert.

Das Verfahren beruht darauf, dass ein Nutzer nur Kenntnis der Root-CAs benötigt die ein fragliches Zertifikat unterschrieben hat. Schenkt man dieser Root-CA vertrauen, kann man dies auch gegenüber Zertifikaten die von dieser CA unterschrieben wurden.

Das Root-Zertifikat von CACert liegt gängigen Browsern und Email Programmen noch nicht bei. Genauer: es liegen nur Root-Zertifikate von kommerziellen Zertifizierungs-Authorities vor, die für ihre Unterschriften Geld verlangen.

Das will CACert ändern und arbeitet intensiv daran - denn Verschlüsselung allen verfügbar und kostenfrei zu machen ist ein Ziel von CACert.

Sind „Selbstunterschriebene Zertifikate“ eine Alternative?

Ja, wenn Anonymität wichtiger ist als Vertrauen in die Authentizität eines unbekanntem Kommunikationspartners.

Nur bedingt, weil man selbst den Aufwand treiben muss zu prüfen, ob der „Fingerprint“ des Zertifikates genau zu dem privaten Schlüssel des Ausstellers passt. Es muss also eine vorherige Kommunikation stattfinden vor dem eigentlichen Akt der Signatur oder Verschlüsselung.

Solange CACert noch nicht mit dem Browser mitkommt: Woher weiss ich, dass das Wurzel-Zertifikat von CACert das richtige ist?

- *Durch einen persönlichen Besuch bei CACert in Australien*
- *Auf <https://www.cacert.org/index.php?id=3> findet sich das Wurzelzertifikat. Dessen PKI-Fingerprint ist mit GPG signiert. Der gpg-Schlüssel liegt auf den PGP-Keyservern und wurde unterschrieben von anderen, deren Schlüssel wiederum von anderen unterschrieben wurden. Von denen man vielleicht jemanden persönlich kennt (Web-Of-Trust)*
- *MD5 Fingerprint: A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B*
- *SHA1 Fingerprint: 13:5C:EC:36:F4:9C:B8:E9:3B:1A:B2:70:CD:80:88:46:76:CE:8F:33*

Eine CA darf ein Zertifikat nur unterschreiben, wenn sie sich von der Richtigkeit der Daten (z. B. dass eine fragliche Person wirklich die ist die sie vorgibt zu sein) überzeugt ist.

Ist das Vertrauen in CACert gerechtfertigt?

Gegenfrage: wie sieht das bei einer kommerziellen CA aus? Immerhin ist da viel Geld im Spiel. Und man muss sich auf die dokumentierten Prozesse zum Schutz des Verfahrens verlassen.

CACert setzt auf ein „Web Of Trust“ (Netz des Vertrauens), ähnlich wie bei GPG/PGP: man weist sich gegenüber mehreren „Assurern“ aus. Der Assurer vergibt dafür Punkte. Mit genug Punkten erhält man ein personenbezogenes Zertifikat (**50**). Mit noch mehr Punkten kann man selbst Assurer werden (**100**), um andere zu beglaubigen. Mit steigender Erfahrung als Assurer (Zahl geleisteter Unterschriften) steigt wiederum das Vertrauen in den Assurer, der dann auch mehr Punkte vergeben kann (bis zu 35).

CACert unterschreibt also nach Gewichtung des Vertrauensverhältnisses in diesem punktebasierten Bewertungssystem.

Vertrauenspunkte im Web-Of-Trust bekommt man, indem man sich persönlich mit einem Assurer trifft und sich diesem mit einem gültigen amtlichen Dokument (Personalausweis oder Reisepass mit Lichtbild) ausweist. Nur wenn kein Zweifel über die Identität besteht, darf der Assurer beglaubigen. Die Unterlagen seiner Beglaubigungen muss der Assurer aufbewahren und bei Nachfragen durch CACert vorlegen können. Die erhobenen personenbezogenen Daten dürfen nicht anderweitig verwendet oder veröffentlicht werden (gem. BDSG, und gem. der Regeln von CACert).

Beglaubigungen im Rahmen des WOT-Programms von CACert

Wer sich beglaubigen lassen möchte, kann dies hier und jetzt tun. Andere Assurer finden sich auf den CACert Web-Seiten.

Schön wäre, wenn Sie sich auch aktiv in das Projekt mit einbringen würden, z. B. indem Sie sich selbst als Assurer zur Verfügung stellen (so dass das Web-Of-Trust größer wird, es mehr Orte gibt wo man sich beglaubigen lassen kann), CACert und seine Möglichkeiten und Ziele bekannter machen (Einladung zu Keysigning, Mithilfe bei / Organisation von Veranstaltungen), etc.. Auf dass die existierenden Möglichkeiten zur Sicherung der Privatsphäre besser wahrgenommen werden und bald wie selbstverständlich zum täglichen Umgang mit unserem Computer gehören.