kostenlose Zertifikate
http://www.CAcert.org
FAQ Deutsch

Was ist CAcert?
CAcert wurde als Organisation gegründet, zum Zweck die erste Non-Profit Certificate Authority zu etablieren. Denn bis dahin wurden global verifizierbare Zertifikate nur von kommerziellen CAs ausgestellt, die dafür Geld verlangen. Zu teuer für die meisten Anwender, weshalb der Grossteil der Kommunikation im Internet unverschlüsselt und unverifiziert übertragen wird.
CAcert will die Open-Source-Philosophie auf die IT-Sicherheitswelt übertragen, und Sicherheit somit für jeden erschwinglich und verfügbar machen. Hier wird von CAcert die Möglichkeit angeboten, ihre Identität festzustellen und sich so gratis Zertifikate ausstellen zu können.

Was kann man damit machen?
Die Zertifikate ermöglichen Ihnen, Ihren Webserver mit HTTPS abzusicheren, Ihre E-Mails mit S/MIME digital zu unterschreiben und zu verschlüsseln. Sie sind somit nicht mehr auf selbstsignierte Zertifikate angewiesen. Die Zertifikate sind sowohl für private als auch für Organisationen einsetzbar.

Wo bekomme ich mein Zertifikat?
CAcert-Assurer überprüfen lediglich ihre Identität an Hand von zwei öffentlichen Lichtbildausweisen (Personalausweis/Führerschein/Reisepass). Zertifikate können Sie sich dann nach belieben selber über ein Webinterface ausstellen, wobei nur die Daten übernommen werden, die CAcert überprüft hat.

Kann ich mehrere E-Mail-Adressen/Domains haben?
Ja, selbstverständlich und unbegrenzt viele. Für jede E-Mail oder Domain bekommt man eine Bestätigungs-E-Mail an die E-Mail-Adresse bzw. eine offizielle E-Mail-Adresse der Domain geschickt (z.B. postmaster@domain).

Wann läuft mein Account ab?
Der CAcert Account ist unbegrenzt zeitlich gültig und gilt somit auf Lebenszeit. Lediglich die einzeln hierunter erstellten Zertifikate müssen spätestens alle 2 Jahre erneuert werden. Hierzu ist selbstverständlich keine erneute Assurance notwendig.

Wo ist das Wurzel-Zertifikat von CAcert schon integriert?
Unser Zertifikat ist bereits in verschiedenen Linux-Distributionen enthalten. Leider verwenden viele Browser (Microsoft Internet Explorer, Mozilla Firefox) eigene Zertifikatsspeicher.

Wann seid ihr in den Browsern?
Das ist unser größtes Ziel, welches wir schnellstmöglich erreichen werden. Voraussetzung dafür ist ein sogenannter WebTrust oder WebTrust kompatibler Audit, welcher ca. 70.000 Euro kostet und somit für eine non-profit Organsiation wie CAcert nicht ohne weiteres zu bewältigen ist. *Ihre Spende ist herzlich Willkommen!*

Was ist bis dahin?
Bis dahin muss man unser Rootzertifikat einmal selbst hinzufügen um allen durch CAcert.org ausgestellten Zertifikaten (zur Zeit über. 100.000) vertrauen zu können.

Warum soll ich CAcert vertrauen?
Wir prüfen die Identität alle unserer Benutzer anhand mindestens eines staatlichen Lichtbildausweises und jeder Benutzer wird in der Regel von mehreren Assuren geprüft.

Sind meine Daten sicher?
Wir speichern keine Ausweisdaten wie Ausweisnummer oder Ausweiskopien um dem "Identitätsklau" der in den Vereinigten Staaten zu stark verbreitet ist, vorzubeugen. Außer Ihrem vollen Namen, Ihrem Geburtsdatum und einer E-Mail-Adresse geben Sie keine weiteren

Daten Preis.

Wie funktioniert das Punktesystem?
CAcert beurteilt an Hand von Punkten wie gut die Identität bereits überprüft wurde. Man benötigt 100 Punkte um CAcert vollständig nutzen zu können. Auf großen Events erhalten sie in der Regel direkt 100 Punkte und dürfen selber andere assuren. Weitere Details finden Sie auf unserer Homepage und im Wiki.

Punkte	***Status***	***persönliche Client-Zertifikate***	***Code-Signing Zertifikate***	***PGP/GPG Signatur***	***Gültigkeit der Server-Zertifikate***	***max. Punkte vergabe***
0 to 49	unassured				6 Monate	
50 to 100	assured	Ja	Ja		24 Monate	
Assurer Prüfung: CATS Test						
100 to 149	Assurer	Ja	Ja	Ja	24 Monate	10 bis 30
150	fully assured	Ja	Ja	Ja	24 Monate	35

Können Punkte verfallen oder sich vermindern?
Nein. Punkte sind derzeit lebenslang gültig, solang derjenige der sie vergeben hat nicht unglaubwürdig wird. Es ist daher sinnvoll sich von möglichst vielen anderen Assuren zu lassen, um das Web of Trust so eng wie möglich zu gestalten.

Darf ich die Zertifikate für kommerzielle Anwendungen nutzen?
Selbstverständlich! Darüber hinaus gibt es bei CAcert sogar die Möglichkeit, seine Organisation assuren zu lassen und somit auch den Namen der Organisation im Zertifikat zu tragen. Bitte fragen Sie dazu unseren Organisationsberater am Stand.

Worauf muss ein Assurer achten?
Zustimmung zur CCA. Befolgung der Assurance Policy.
http://wiki.cacert.org/AssuranceHandbook2 (englisch) gibt Basisinformationen.

Wo bekomme ich Support?
E-Mail: support@cacert.org
Chat: irc.cacert.org #cacert (englisch) oder #cacert.ger (deutsch)
Wiki: http://wiki.cacert.org

Ich habe mein Passwort vergessen, was muss ich tun ?
Es gibt vier Möglichkeiten:

- Login mit einem persönlichem Client-Zertifikat
- Sie können die 5 Fragen beantworten, die Sie angegeben haben, als Sie Ihren Account erstellt haben.
- Sie erstellen einen neuen Account und verlieren alle Ihre Punkte. Sie können die E-Mail-Adressen und Domänen aus dem alten Account mit dem Disput System übernehmen.
- Sie zahlen 10,- EUR an CAcert, damit ein Admin ihr Passwort zurücksetzt.

Wie lautet der Fingerprint des Root Zertifikates?
SHA1: 13:5C:EC:36:F4:9C:B8:E9:3B:1A:B2:70:CD:80:88:46:76:CE:8F:33
MD5: A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B

Wie kann ich helfen?
http://wiki.cacert.org/HelpingCAcert

This document is signed by

	**Signatory**	EMAILADDRESS=ulrich@cacert.org, CN=Ulrich Schroeter
	Date/Time	Fri Feb 19 17:58:45 CET 2010
	Issuer-Certificate	EMAILADDRESS=support@cacert.org, CN=CA Cert Signing Authority, OU=http://www.cacert.org, O=Root CA
	Serial-No.	434828
	Method	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)
Note	This signature can be verified, if you open the document with Adobe Reader!	