CAcert FAQ *(deutsch)*

http://cacert.org

- ***Was ist CAcert?***

CAcert wurde als Non-Profit-Organisation gegründet, mit dem 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 OpenSource Philosophie auf die IT Sicherheitswelt übertragen, und Sicherheit somit für jeden erschwinglich und verfügbar machen. Auf der CeBit 2006 wird von CAcert die Möglichkeit angeboten, Ihre Identität festzustellen und sich so gratis Zertifikate ausstellen zu können.

Die Zertifikate ermöglichen Ihnen, ihren Weberver mit HTTPS abzusichern und Ihre Emails mit S/MIME digital zu unterschreiben und zu verschlüsseln. Sie sind somit nicht mehr auf selbstsignierte Zertifikate angewiesen. Die Zertifikate sind sowohl privat als auch für Organisationen einsetzbar.

- ***Was kann man damit machen?***

Man kann sich Server-/Client-zertifikate ausstellen, S/MIME nutzen, Codesigning betreiben und sich seinen PGP/GPG Key signieren lassen, ohne dafür (wie bei anderen großen kommerziellen CAs) hunderte von Euro pro Jahr zu bezahlen.

- ***Wo bekomme ich mein Zertifikat?***

CAcert-Assurer überprüfen lediglich ihre Identität an Hand von zwei öffentlichen Lichtbildausweisen (Personalausweis/Pass/Führerschein). Zertifikate können Sie sich dann nach Belieben selber über ein Webinterface ausstellen, wobei alle Daten entfernt werden, die CAcert nicht überprüft hat.

- ***Kann ich mehrere Emailadressen/Domains haben?***

Ja. Selbstverständlich und unbegrenzt. Für jede Email oder Domain bekommt man eine "Pingmail" an die Emailadresse bzw eine offizielle Emailadresse 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 Rootcert von CAcert schon integriert?***

Wir sind bereits bei verschiedenen Linuxdistributionen im Standardcache. Leider verwenden viele Browser (IE, Firefox) eigene Zertifikatsspeicher.

- ***Wann seid ihr in den Browsern?***

Das ist unser größtes Ziel, welches wir aller Voraussicht nach im Laufe von 2006 erreichen werden. Voraussetzung dafür ist ein sogenannter Webtrustaudit nach ONR 17700, welcher ca. 70.000 Euro kostet und somit für eine Non-profit Organisation 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 ca. 80.000) vertrauen zu können.

- ***Warum soll ich CAcert vertrauen?***

Wir prüfen die Identität aller unserer Benutzer an Hand mindestens eines staatlichen Lichtbildausweises und jeder Benutzer wird in der Regel von mehreren Assuren geprüft.

- ***Sind meine Daten sicher?***

Wir speichern keine Ausweisdaten wie z.B. Ausweisnummern und sind damit für keinen "Identitätsklau" wie in den Vereinigten Staaten anfällig. Außer Ihrem vollen Namen, Ihrem Geburtsdatum und einer E-Mailadresse geben Sie keine weiteren Daten preis.

CAcert FAQ *(deutsch)*

http://cacert.org

- ***Was ist CAcert?***

CAcert wurde als Non-Profit-Organisation gegründet, mit dem 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 OpenSource Philosophie auf die IT Sicherheitswelt übertragen, und Sicherheit somit für jeden erschwinglich und verfügbar machen. Auf der CeBit 2006 wird von CAcert die Möglichkeit angeboten, Ihre Identität festzustellen und sich so gratis Zertifikate ausstellen zu können.

Die Zertifikate ermöglichen Ihnen, ihren Weberver mit HTTPS abzusichern und Ihre Emails mit S/MIME digital zu unterschreiben und zu verschlüsseln. Sie sind somit nicht mehr auf selbstsignierte Zertifikate angewiesen. Die Zertifikate sind sowohl privat als auch für Organisationen einsetzbar.

- ***Was kann man damit machen?***

Man kann sich Server-/Client-zertifikate ausstellen, S/MIME nutzen, Codesigning betreiben und sich seinen PGP/GPG Key signieren lassen, ohne dafür (wie bei anderen großen kommerziellen CAs) hunderte von Euro pro Jahr zu bezahlen.

- ***Wo bekomme ich mein Zertifikat?***

CAcert-Assurer überprüfen lediglich ihre Identität an Hand von zwei öffentlichen Lichtbildausweisen (Personalausweis/Pass/Führerschein). Zertifikate können Sie sich dann nach Belieben selber über ein Webinterface ausstellen, wobei alle Daten entfernt werden, die CAcert nicht überprüft hat.

- ***Kann ich mehrere Emailadressen/Domains haben?***

Ja. Selbstverständlich und unbegrenzt. Für jede Email oder Domain bekommt man eine "Pingmail" an die Emailadresse bzw eine offizielle Emailadresse 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 Rootcert von CAcert schon integriert?***

Wir sind bereits bei verschiedenen Linuxdistributionen im Standardcache. Leider verwenden viele Browser (IE, Firefox) eigene Zertifikatsspeicher.

- ***Wann seid ihr in den Browsern?***

Das ist unser größtes Ziel, welches wir aller Voraussicht nach im Laufe von 2006 erreichen werden. Voraussetzung dafür ist ein sogenannter Webtrustaudit nach ONR 17700, welcher ca. 70.000 Euro kostet und somit für eine Non-profit Organisation 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 ca. 80.000) vertrauen zu können.

- ***Warum soll ich CAcert vertrauen?***

Wir prüfen die Identität aller unserer Benutzer an Hand mindestens eines staatlichen Lichtbildausweises und jeder Benutzer wird in der Regel von mehreren Assuren geprüft.

- ***Sind meine Daten sicher?***

Wir speichern keine Ausweisdaten wie z.B. Ausweisnummern und sind damit für keinen "Identitätsklau" wie in den Vereinigten Staaten anfällig. Außer Ihrem vollen Namen, Ihrem Geburtsdatum und einer E-Mailadresse 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 unter http://www.cacert.org.

Punkte	Status	personalisierte Client-zertifikate	Code-Signing Zertifikat	PGP/GPG Signatur	Gültigkeit für Server Zertifikate	max. Punktevergabe
0 bis 49	unassured	-	-	-	6 Monate	-
50 bis 99	assured	ja	-	ja	24 Monate	-
100 bis 149	Assurer	ja	ja	ja	24 Monate	10 bis 30
150	fully assured	ja	ja	ja	24 Monate	35
200	super Assurer	ja	ja	ja	24 Monate	150

- ***Können Punkte verfallen oder sich vermindern?***

Nein. Punkte sind 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 Organistion assuren zu lassen und somit auch den Namen der Organisation im Zertifikat zu tragen. Bitte fragen Sie dazu unseren Organisationsberater vor Ort.

- ***Worauf muss ein Assurer achten?***

http://wiki.cacert.org/wiki/AssuranceHandbook (englisch) gibt Basisinformationen - ist allerdings noch in der Entwicklung.

- ***Wo bekomme ich Support***

E-mail: support@cacert.org

Chat: irc.cacert.org *#cacert* (englisch) oder *#cacert.ger* (deutsch)

- ***Ich habe mein Passwort vergessen, was muß ich tun ?***

- 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 Email 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?***

md5 = a6:1b:37:5e:39:0d:9c:36:54:ee:bd:20:31:46:1f:6b

sha1 = 135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33

- ***Wie kann ich helfen?***

http://wiki.cacert.org/wiki/HelpingCAcert

- ***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 unter http://www.cacert.org.

Punkte	Status	personalisierte Client-zertifikate	Code-Signing Zertifikat	PGP/GPG Signatur	Gültigkeit für Server Zertifikate	max. Punktevergabe
0 bis 49	unassured	-	-	-	6 Monate	-
50 bis 99	assured	ja	-	ja	24 Monate	-
100 bis 149	Assurer	ja	ja	ja	24 Monate	10 bis 30
150	fully assured	ja	ja	ja	24 Monate	35
200	super Assurer	ja	ja	ja	24 Monate	150

- ***Können Punkte verfallen oder sich vermindern?***

Nein. Punkte sind 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 Organistion assuren zu lassen und somit auch den Namen der Organisation im Zertifikat zu tragen. Bitte fragen Sie dazu unseren Organisationsberater vor Ort.

- ***Worauf muss ein Assurer achten?***

http://wiki.cacert.org/wiki/AssuranceHandbook (englisch) gibt Basisinformationen - ist allerdings noch in der Entwicklung.

- ***Wo bekomme ich Support***

E-mail: support@cacert.org

Chat: irc.cacert.org *#cacert* (englisch) oder *#cacert.ger* (deutsch)

- ***Ich habe mein Passwort vergessen, was muß ich tun ?***

- 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 Email 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?***

md5 = a6:1b:37:5e:39:0d:9c:36:54:ee:bd:20:31:46:1f:6b

sha1 = 135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33

- ***Wie kann ich helfen?***

http://wiki.cacert.org/wiki/HelpingCAcert