Organisations-Assurance

Für Firmen und andere Organisationen bietet CAcert ein Organisations-Assurance-Programm an.
Wenn die Organisation assured wurde, können nach belieben Zertifikate die den Organisationsnamen enthalten ausgestellt werden. Mitarbeiter können Zertifikate, die im Namen der Organisation ausgestellt wurden, erhalten.

Was kostet CAcert?

Die Zertifikate sind für Sie kostenlos. Dank vieler Freiwilliger, die CAcert betreiben, und hoch-automatisierten Diensten kann CAcert sehr kostengünstig arbeiten. Ihre Spenden helfen die Betriebskosten zu decken und sind jederzeit willkommen.

Wie kann ich CAcert unterstützen?

- Werden Sie Mitglied der CAcert-Gemeinschaft und benutzten Sie CAcert-Zertifikate
- Nehmen Sie am Assurer-Test teil und werden Sie CAcert-Assurer
- Helfen Sie CAcert auf Veranstaltungen und erzählen Sie anderen von CAcert
- Unterstützen Sie CAcerts Kernprozesse, z.B. in der Systemadministration oder im Support

http://wiki.cacert.org/HelpingCAcert

Wo finde ich weitere Informationen?

Mehr Informationen:
http://www.cacert.or
http://wiki.cacert.org

CAcert hat ein paar IRC-Chat-Kanäle auf irc.cacert.org (SSL-Port: 7000). Dort können Sie Kommentare zu den CAcert-Diensten abgeben, Support erhalten oder einfach nur mit Mitgliedern der CAcert-Gemeinschaft plaudern.

Kanäle:
#cacert (Englisch)
#cacert.ger (Deutsch)
#cacert.fr (Französisch)

Oder Webchat auf http://irc.cacert.org.

Support E-Mail: cacert-support@lists.cacert.org

Support-Informationen:
http://wiki.cacert.org/GettingSupport

http://www.cacert.org

Support

E-Mail: cacert-support@lists.cacert.org

IRC-Server: irc.cacert.org
Kanäle: #cacert, #cacert.ger or #cacert.fr

Fingerabdrücke

CAcert Root-Zertifikat

```
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
```

CAcert Class-3-Root-Zertifikat

```
SHA1: AD:7C:3F:64:FC:44:39:FE:F4:E9:0B:E8:F4:7C:6C:FA:8A:AD:FD:CE
MD5:  F7:25:12:82:4E:67:B5:D0:8D:92:B7:7C:0B:86:7A:42
```


Digitale Zertifikate für Personen und Organisationen

- Client-Zertifikate
- Server-Zertifikate
- Code-Signatur

SSL/TLS
S/MIME
PGP/GnuPG/OpenPGP

http://www.cacert.org

Digitale Zertifikate

Was ist CAcert?

CAcert ist ein community-basierter, eingetragener non-profit Verein mit Sitz in Australien.

Die Ziele von CAcert sind:
- Steigerung der Sicherheit im IT-Zeitalter
- Unterstützung unserer Benutzer in ihren Sicherheitsbestrebungen
- Bereitstellung von Tools und Mechanismen im Bereich der IT-Sicherheit

Anwendungsgebiete sind u.a.:
- Absichern von Webservern mittels HTTPS
- Signieren und Verschlüsseln von E-Mails
- SSL/TLS Serverdienste
- Kommunikation mit Webseiten
- VPN-Verbindungen
- digitales Signieren von Programmcode (z.B. Java)
- digitales Signieren von Dokumenten

CAcert ist bestrebt, Sicherheit für die IT-Welt frei verfügbar zu machen und die Mittel dafür für jeden erschwinglich zu gestalten. CAcert ist eine offene Gemeinschaft und nutzt den Open-Source-Gedanken, um ihre Ziele zu erreichen.

Warum sollte man mitmachen?

Sicherheit:
Steigern der eigenen und der allgemeinen Sicherheit bei der Verwendung des Internets.

Privatsphäre:
CAcert unterstützt Sie darin, Ihre Privatsphäre im Internet zu bewahren.

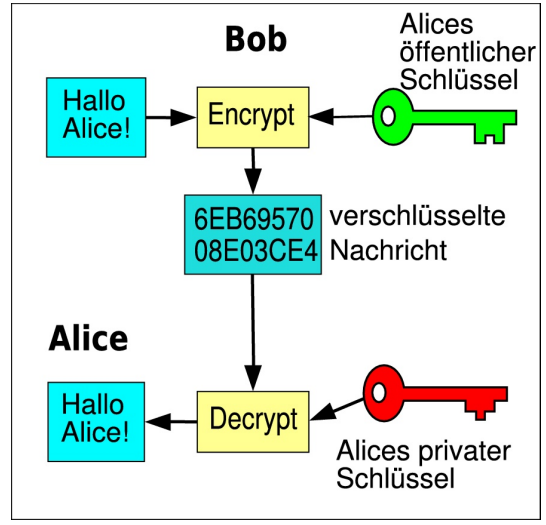
Authentizität:
Andere können sicher sein, dass Ihre Identität geprüft wurde und Sie wirklich derjenige sind, der Sie vorgeben zu sein.

Kostenlose E-Mail- und Serverzertifikate

X.509-Zertifikate finden Anwendung, um E-Mails mit S/MIME zu signieren und Servern - wie z.B. Web- und Mailservern - die Bereitstellung einer sicheren Verbindung zu ermöglichen.
Üblicherweise verlangen Firmen hohe Gebühren für die Wahrnehmung von Aufgaben eines Trustcenters: Das Überprüfen Ihrer Identität und ob Ihre Webseite oder E-Mail-Adresse auch wirklich Ihnen gehört. CAcert bietet dies kostenlos an.

Wie funktioniert CAcert?

Um bei CAcert mitzumachen, müssen Sie sich zunächst auf http://www.cacert.org anmelden. Anzugeben sind lediglich der ganze Name, Geburtsdatum und E-Mail-Adresse. Später können Sie beliebig viele E-Mail-Adressen für Client-Zertifikate und Domainnamen für Server-Zertifikate Ihrem Benutzerkonto hinzufügen.
Anschließend können Sie sich nach Belieben Zertifikate über die Web-Schnittstelle ausstellen.
Wenn Sie den Zertifikaten Ihren Namen hinzufügen wollen, müssen Sie zunächst Ihre Identität überprüfen lassen - nehmen Sie Kontakt zu Assurern auf (z.B. über die Assurer-Suche auf der Webseite) oder treffen Sie sie auf Veranstaltungen.



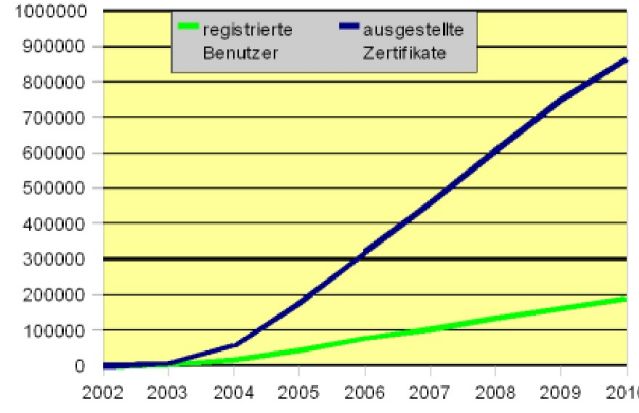
Wie Public-Key-Verschlüsselung funktioniert

Kostenlose PGP-/GnuPG-/OpenPGP-Signatur

Wenn Sie assured wurden, können Sie Ihren PGP-/GnuPG-/OpenPGP-Schlüssel vom CAcert PGP-Schlüssel signieren lassen.

Signatur von Programmcode

Als Programmierer können Sie Ihren Programmcode mit Ihrem CAcert-Zertifikat unterschreiben, diesen somit als den Ihren kennzeichnen und ihn vor Verfälschungen schützen.



Entwicklung von CAcert seit der Gründung in 2002

Mit welcher Software kann man CAcert-Zertifikate nutzen?

Sie können CAcert-Client-Zertifikate mit allen Anwendungen nutzen, die mit X.509-Zertifikaten umgehen können. Z.B.:

- Microsoft Outlook und Office
- Mozilla Thunderbird und Firefox
- OpenOffice.org

Sie können CAcert-Server-Zertifikate mit allen Programmen nutzen, die mit SSL-basierten Zertifikaten umgehen können. Z.B.:
- Apache Webserver
- Microsoft Internet Information Services
- Mail-Server (z.B. Postfix, Sendmail, Courier)
- OpenSSL / OpenVPN