

## IN WELCHEN PROGRAMMEN KANN MAN CACERT ZERTIFIKATE EINBINDEN?

---

### 1. Client Zertifikate

In jedem Programm welches mit X.509 (S/Mime) Zertifikaten umgehen kann. Dazu gehören unter anderem

- Microsoft Outlook
- Adobe Acrobat
- OpenOffice

### 2. Server Zertifikate

Alle Serverprodukte, die mit SSL basierten Zertifikaten umgehen können.

Dazu gehören unter anderem

- Apache Webserver
- Microsoft Internet Information Server
- OpenSSL / OpenVPN

## WAS MUSS ICH SONST NOCH WISSEN?

---

Alle Infos sind entweder unter [www.cacert.org](http://www.cacert.org) oder <http://wiki.cacert.org> zu finden.

Desweiteren gibt es einen IRC Chat

IRC Server: [irc.cacert.org](irc://irc.cacert.org)

Channel: [#cacert](#) (in English)

[#cacert.ger](#) (in deutsch)

Weitere Supportinfos:

<http://wiki.cacert.org/wiki/GettingSupport>

Für Spenden besuchen Sie bitte

<http://www.cacert.org/index.php?id=13>



- **Client-Zertifikate**
- **Server-Zertifikate**
- **Web-Of-Trust**
- **Organisation-Assurance**

CACert.org

<http://www.cacert.org>

Support: [#cacert](irc://irc.cacert.org) oder [#cacert.ger](irc://irc.cacert.org)

For most software, the fingerprint is reported as:

A6: 1B: 37: 5E: 39: 0D: 9C: 36:  
54: EE: BD: 20: 31: 46: 1F: 6B

Under MSIE the thumbprint is reported as:

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

**SSL/TLS**  
**S/MIME**  
**OpenPGP**  
**Code-Signing**



CACert.org  
<http://www.cacert.org>



## DIGITALE ZERTIFIKATE

### WAS IST CACERT ?

---

CACert.Inc ist ein Communitybasierter, eingetragener Non-Profit Verein mit Sitz in Australien. Ziel ist der Betrieb eines kostenfrei arbeitenden Zertifizierungsdienst-Anbieters (CA) zur Ausstellung von elektronischen Zertifikaten nach dem X.509 Standard.

Die Anwendungsbereiche sind u.a. :

- Webserver mit HTTPS absichern
- Unterschreiben und Verschlüsseln von Emails
- SSL/TLS Serverprogramme
- Anmeldung bei Webseiten
- Anmeldung bei VPN's
- digitales unterschreiben von selbst erstelltem Programmcode (z.B. Java)

CACert.Inc will somit die OpenSource Philosophie auf die IT-Sicherheitswelt übertragen, und Sicherheit für jeden erschwinglich und verfügbar machen.

### KOSTENLOSE E-MAIL UND SERVER ZERTIFIKATE

---

Wer seinen E-Mail-Verkehr und/oder (Web)Server mittels S/MIME digital signieren oder sicheren Zugriff auf seine Online-Präsenz über HTTPS anbieten möchte, braucht -- mitunter sehr teure -- X.509-Zertifikate. Er zahlt dafür, dass eine Firma diese sogenannte Trustcenter-Aufgaben wahrnimmt: Sie prüft, ob dem Kunden wirklich die Webseite oder die E-Mail-Adresse

gehören (Identitätsüberprüfung). Dies kann je nach zu erwartendem Verwaltungsaufwand mehrere hundert Euro kosten.

### WIE GEHT DAS MIT CACERT

---

Interessierte Personen müssen eigentlich im ersten Schritt nichts weiter tun als sich kostenfrei und ohne jede weitere Verpflichtung bei [www.CAcert.org](http://www.CAcert.org) anzumelden. Anzugeben sind lediglich Ihre E-mail Adresse, Name und Geburtsdatum. In einem zweiten Schritt haben Sie z.B. bei Veranstaltungen oder auf Einzelanfrage die Möglichkeit sich beglaubigen zu lassen (Assurance) um Ihre Identität zu verifizieren. Danach können Sie Ihre eigenen Zertifikate über das gesicherte Webinterface ausstellen und weiterverwenden.

### KOSTENLOSE PGP/GNUPG KEYSIGNING

---

Auch Ihren PGP/GnuPG Key können Sie innerhalb des CACert Web-of-Trust beglaubigen lassen.

### CODESIGNING

---

Wenn Sie Programmierer sind und Ihren Code als Ihren eigenen kennzeichnen und Ihn ebenso digital unterschreiben möchten ist dies auch möglich.



### ORGANISATIONS ASSURANCES

---

Bei CACert. Inc. können auch im Handelsregister eingetragene Gesellschaften, Kaufleute und Vereine ebenso wie Hochschulen, Städte, Gemeinden, Ämter und andere siegelführende Körperschaften und Gesellschaften des bürgerlichen Rechts von einem CACert Organisations-Assurer abgenommen und beglaubigt werden.

### WIESO SOLLTE MAN MITMACHEN?

---

#### **Sicherheit:**

Sie erhöhen Ihre eigene Sicherheit und den sichereren Umgang im täglichen Umfeld des Internets.

**Authentisch:** Andere können sich sicher sein, das Sie auch wirklich *Sie* selbst sind.

### WIE KANN MAN MITMACHEN ?

---

Sie können sich zum einen natürlich einen CACert.org Account anlegen und aktiv Zertifikate zur Sicherstellung Ihrer Identität verwenden. Sie es im E-mail Verkehr, in Dokumenten oder auf Servern.

Desweiteren können Sie CACert natürlich auch selbst aktiv als Assurer unterstützen und andere Leute assuren (Identitäten beglaubigen).

### WAS KOSTET MICH NUN DAS GANZE?.

---

Dadurch, das der technische und organisatorische Teil getrennt ist und der organisatorische Teil von Freiwilligen und Interessierten übernommen wird, ist der administrative Aufwand sehr gering und somit werden hier keinerlei Kosten für Sie anfallen. Die Zertifikate kosten also rein garnichts.

