



CACert Zertifikatserstellung



Henrik Heigl

Cacert@gmx.net



Key ID: 0x042B3EE5

Key fingerprint = 1847 C70A 88ED 8C73 E866 F607 33B5 B05C 042B 3EE5

- Allgemeiner Überblick
- Zertifikat erstellen
- Zertifikat downloaden
- Einbinden
- Exportieren
- weiterverwenden

Was ist eine CA?

- Zertifizierungsdiensteanbieter“
- Eine CA bestätigt die Identität von Personen und Organisationen auf digitalem Wege („Personenbindung“)
- Ausstellung von digitalen Zertifikaten



Was ist CAcert?

- CAcert Inc. ist ein eingetragener Non-Profit Verein mit Sitz in Australien, der die Regeln definiert, und die zentralen Server betreibt
- Start www.CAcert.org: 2002
- Gründung CAcert Inc.: 2003
- Verifizierte User: > 23.000 (über 50.000 in 2006)
- Ausgestellte Zertifikate: > 39.000 (über 67.000 in 2006)
- Assurer: > 1800 (über 4000 in 2006)
- in über 29 Ländern weltweit
- in 14 Sprachen übersetzt
<http://www.cacert.org/stats.php>



Praktische Anwendung

- Webserver mit HTTPS absichern
- Unterschreiben und Verschlüsseln von Emails und Dokumenten
 - SSL/TLS Serverprogramme
 - Anmeldung bei Webseiten
 - Anmeldung bei VPN's

Assurance

- Assurance ist die Dienstleistung, bei der ein Assurer die Identität einer Person mittels amtlichen Lichtbildausweis kontrolliert
- gegenüber CAcert bestätigt, und dafür Punkte auf das lebenslange Konto bei CAcert vergeben werden
- Freier Markt
- Mittlerweile über 1800 Assurer weltweit (Stand 2004/2005)
- Lebenslanger Account bei CAcert, Zertifikate müssen spätestens alle 2 Jahre erneuert werden
- Zertifikate jederzeit selbst im Internet ausstellen
- Zertifikate sind kostenlos
- beliebige Menge von Zertifikaten
- dadurch nur Initialkosten, keine Folgekosten

Punkteschema

- Ab **50** Punkten kann man personalisierte Zertifikate ausstellen (***assured***)
- Ab **100** Punkten ist man Assurer, kann andere Personen Assuren, kann 10 Punkte vergeben, bekommt selber 2 Punkte für jede Assurance bis man auf 150 Punkte gekommen ist; Code Signing Zertifikat möglich (***assurer***)
- Bis **150** Punkte, da kann man 35 Punkte vergeben (***full assured***)
- Alle Serverzertifikate ab 50 Punkten sind 24 Monate gültig (bis 50 Punkte nur 6 Monate)

Eigene Punkte	Vergebbare Punkte
100	10
110	15
120	20
130	25
140	30
150	35

The screenshot shows the CAcert website interface. At the top left is the CAcert logo. To the right, the text "Free digital certificates!" is displayed. Below the logo is a warning message: "Warning! This site requires cookies to be enabled to ensure your privacy and security. This site uses session cookies to store temporary values to prevent people from copying and pasting the session ID to someone else exposing their account, personal details and identity theft as a result." In the center is a "Login" form with fields for "Email Address:" and "Pass Phrase:", and a "Login" button. On the right side, there is a navigation menu with sections: "Join CAcert.org" (with a "Join" link), "My Account" (with links for "Normal Login", "Cert Login", and "Lost Password"), "Miscellaneous" (with links for "CAcert News", "Howto Information", "CAcert Logos", "CAcert Statistics", "Root Certificate", "CRL", "RSS News Feed", "Credits", and "CAcert Board"), and "Translations" (with links for "العربية", "Български", "Čeština", "Dansk", "Deutsch", and "Ελληνικά"). A large number "1" is placed below the "Miscellaneous" section, with an arrow pointing to the "Root Certificate" link.

Unter www.cacert.com anmelden und einloggen

Ggf. vorher das Root Zertifikat (1) einbinden. Sofern nicht schon geschehen.



Zertifikat erstellen

The screenshot shows the CAcert website interface. At the top left is the CAcert logo. To the right, the text 'Kostenlose Digitale Zertifikate!' is displayed. Below the logo is a form titled 'E-Mail hinzufügen' with an input field for 'E-Mail Adresse' containing 'test@Domain.com' and a 'Hinzufügen' button. Below the form, a paragraph of text reads: 'Momentan werden Zertifikate für Punycode Domains nur ausgestellt, wenn die beantragende Person bereits die "Code-Signing"-Berechtigung (besonderes Assurance-Level) hat, da diese Domains ein etwas höheres Sicherheitsrisiko mit sich bringen.' On the right side, there is a sidebar menu with the following items: 'CAcert.org' (with links for 'Gehe zur Startseite' and 'Ausloggen'), '+ Meine Details', '+ E-Mail Konto' (with links for 'Hinzufügen' and 'Anzeigen'), '+ Client Zertifikate', '+ Domains', '+ Server Zertifikate', '+ CAcert Web of Trust', '+ GPG/PGP Schlüssel', and '+ Streitfälle/Mißbrauch'.

Danach ein neues E-Mail Konto anlegen

Zertifikat erstellen /2

CAcert Kostenlose Digitale Zertifikate!

Installieren Ihres Zertifikats

Sie sind dabei, ein Zertifikat zu installieren. Wenn Sie Mozilla/Netscape/Firefox basierte Browser verwenden, werden Sie nicht informiert, dass das Zertifikat erfolgreich installiert wurde. Sie können in die Einstellungen gehen, unter Security und Zertifikatsverwaltung können Sie sehen, ob das Zertifikat korrekt installiert wurde.

[Klicken Sie hier](#) um Ihr Zertifikat zu installieren.

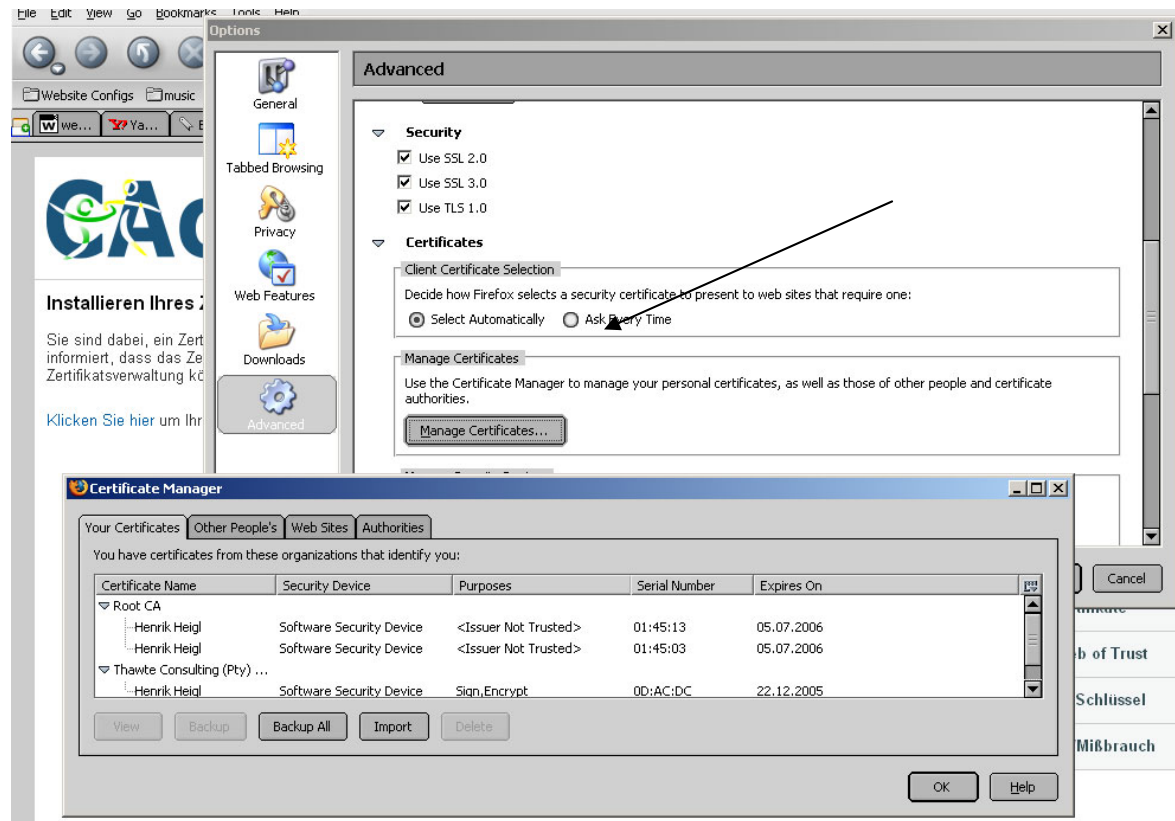
CAcert.org
[Gehe zur Startseite](#)
[Ausloggen](#)

- + Meine Details
- + E-Mail Konto
- + Client Zertifikate
 - Neu Anzeigen
- + Domains
- + Server Zertifikate
- + CAcert Web of Trust
- + GPG/PGP Schlüssel
- + Streitfälle/Mißbrauch

Für die angelegte Mailadresse das Zertifikat anlegen

Achtung: die Arbeitsschritte sind im selben Browser (z.B. Firefox ODER Internet Explorer) durchzuführen.

Das Zertifikat wird im Browser hinterlegt.



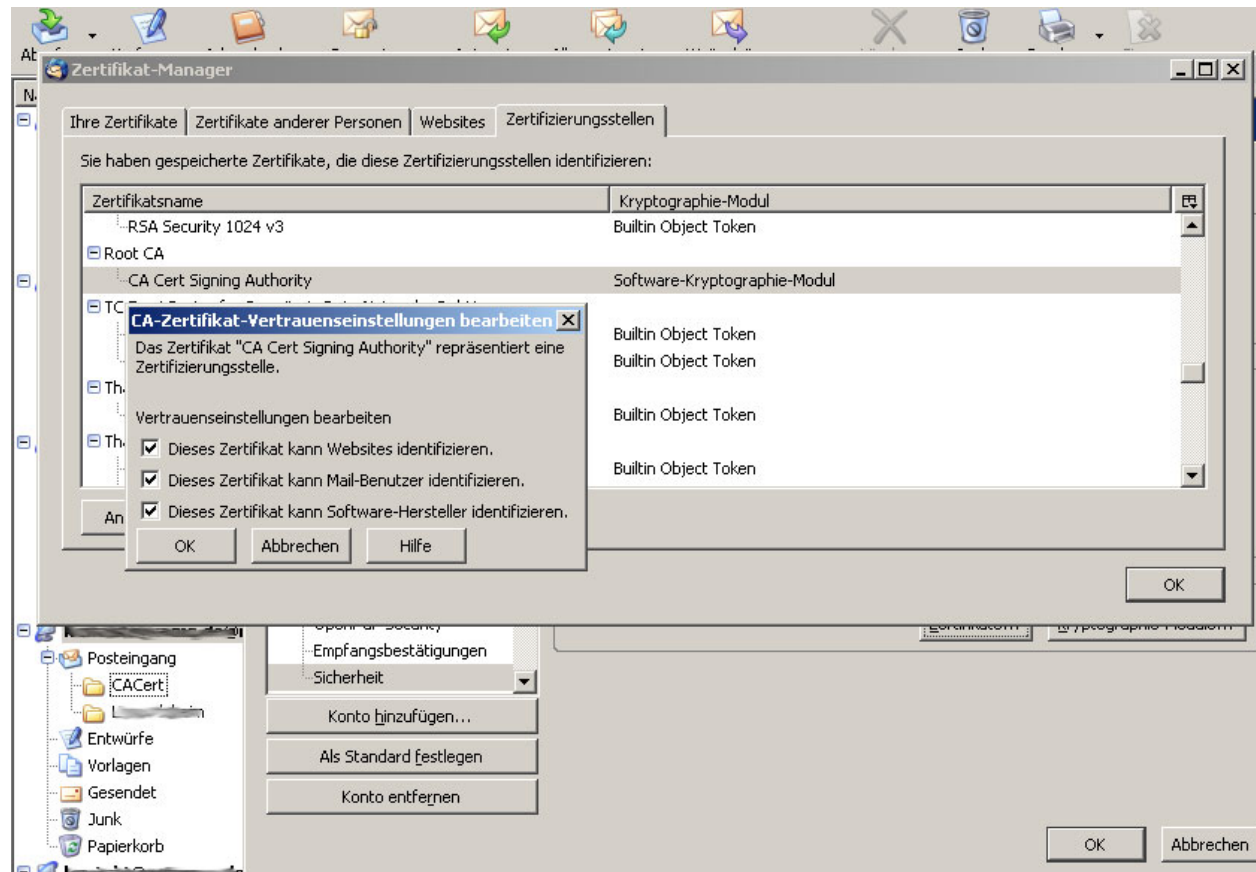
Nun kann das im Browser eingefügte Zertifikat unter den Optionen – Sicherheit – Zertifikats Manager (oder ähnlich, je nach Browser) gesichert werden.



Zertifikat in Mail einbinden

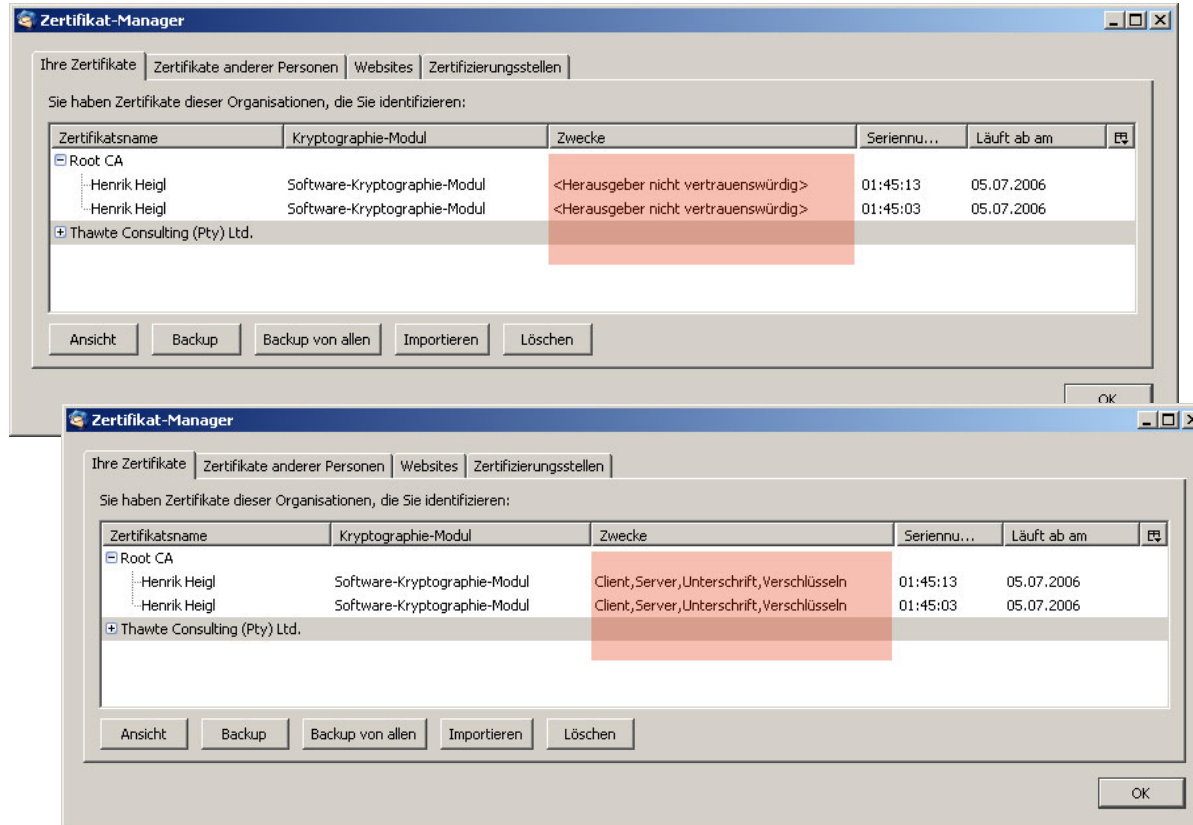
Nachdem man dieses dann z.B. im Thunderbird zur Mail Signierung wieder importiert hat (selber Weg wie beim exportieren im Browser) geht man in die Sicherheitseinstellungen im Zertifikatsmanagement (Eigenschaften des Postfaches – Sicherheit – Zertifikate – Zertifizierungsstellen runter bis *CA Root* erscheint) und bearbeitet das Root Zertifikat so, das am besten alle Häkchen angehakt sind.

Zertifikat in Mail einbinden /2

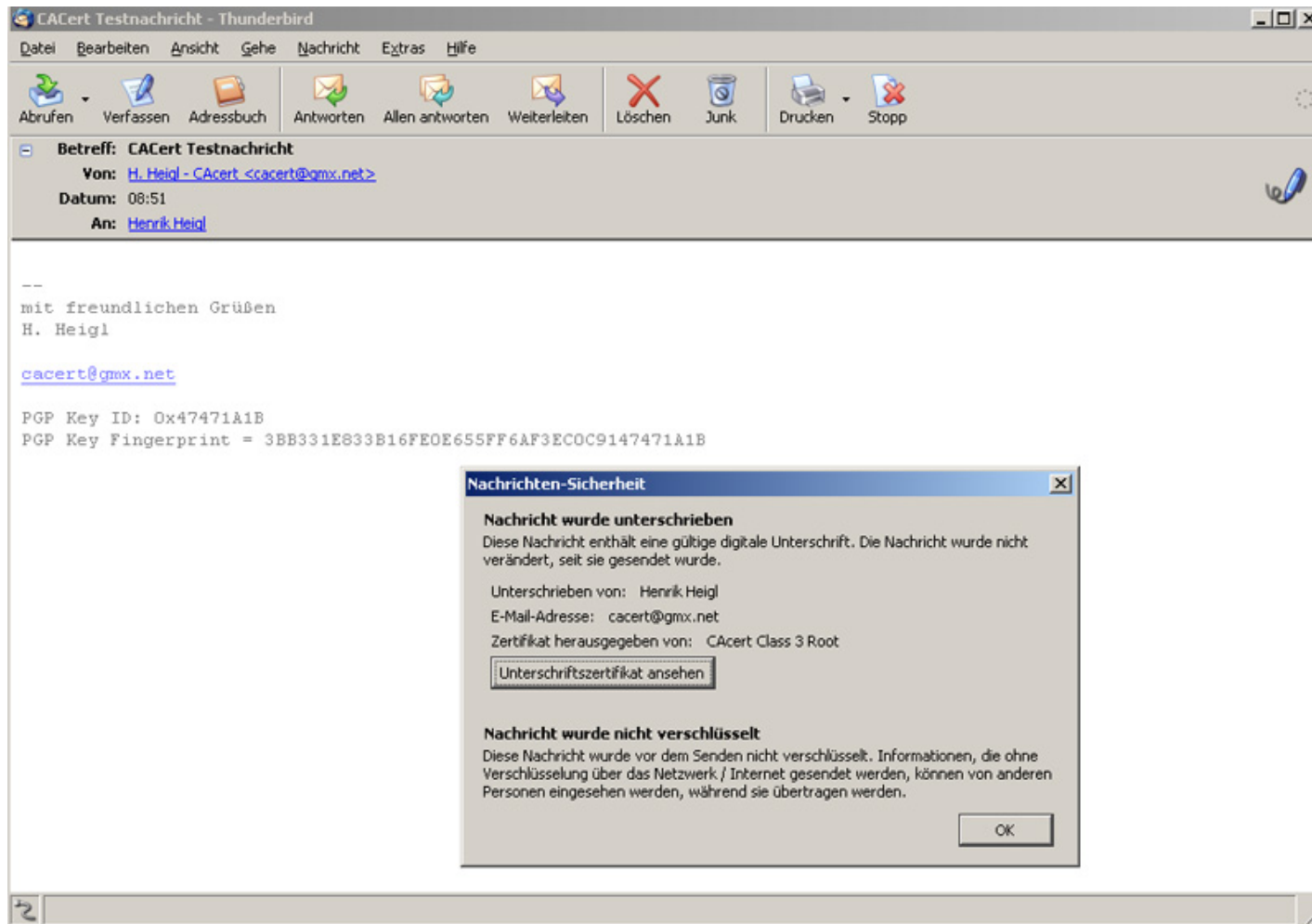


Es muss der Zertifikatsstelle vertraut werden.

Zertifikat in Mail einbinden /3



Ansicht





Weitere Infos

- Weitere Infos unter
 - <http://www.cacert.org>
 - <http://wiki.cacert.org>
 - <http://wiki.cacert.org/wiki/ClientCerts>
 - <http://blog.cacert.org>
 - <http://www.ivamp.de/cert>
- CACert im irc
 - Server: irc.cacert.org
 - Chanel: #cacert oder #cacert.ger



Danke und Fragen

- Henrik Heigl – CAcert@gmx.net
- CACert im irc
 - Server: irc.cacert.org
 - Chanel: #cacert oder #cacert.ger