

CACert Zertifikatserstellung



Henrik Heigl
Pforzheim2005@ ivamp. de



Key ID: 0x042B3EE5

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

Überblick

- Zertifikat erstellen
- Zertifikat downloaden
- Einbinden
- Exportieren
- weiterverwenden

Einleitung

- Die hier gezeigte HowTo Anleitung ist Beispielhaft für den Browser Mozilla Firefox und den E-Mail Client Thunderbird durchgeführt.
- Bei anderen Browsern/E-Mail Clients entsprechend der Menustruktur die Vorgehensweise einfach abwandeln.

1.) Account erstellen

The screenshot shows the CAcert website interface. At the top left is the CAcert logo. At the top right, it says "Free digital certificates!". Below the logo is a warning message about cookies. 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 "Root Certificate" link, with an arrow pointing to it.

Unter www.cacert.com anmelden und einloggen.

Ggf. vorher das Root Zertifikat (1) einbinden.

2.) Zertifikat erstellen



The screenshot shows the CAcert.org website interface. At the top left is the CAcert logo. At the top 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 is a paragraph of text: '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 sub-links 'Gehe zur Startseite' and 'Ausloggen'), '+ Meine Details', '+ E-Mail Konto' (with sub-links '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 (muss nicht das Account Konto sein) für das später das Zertifikat gelten soll.

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.

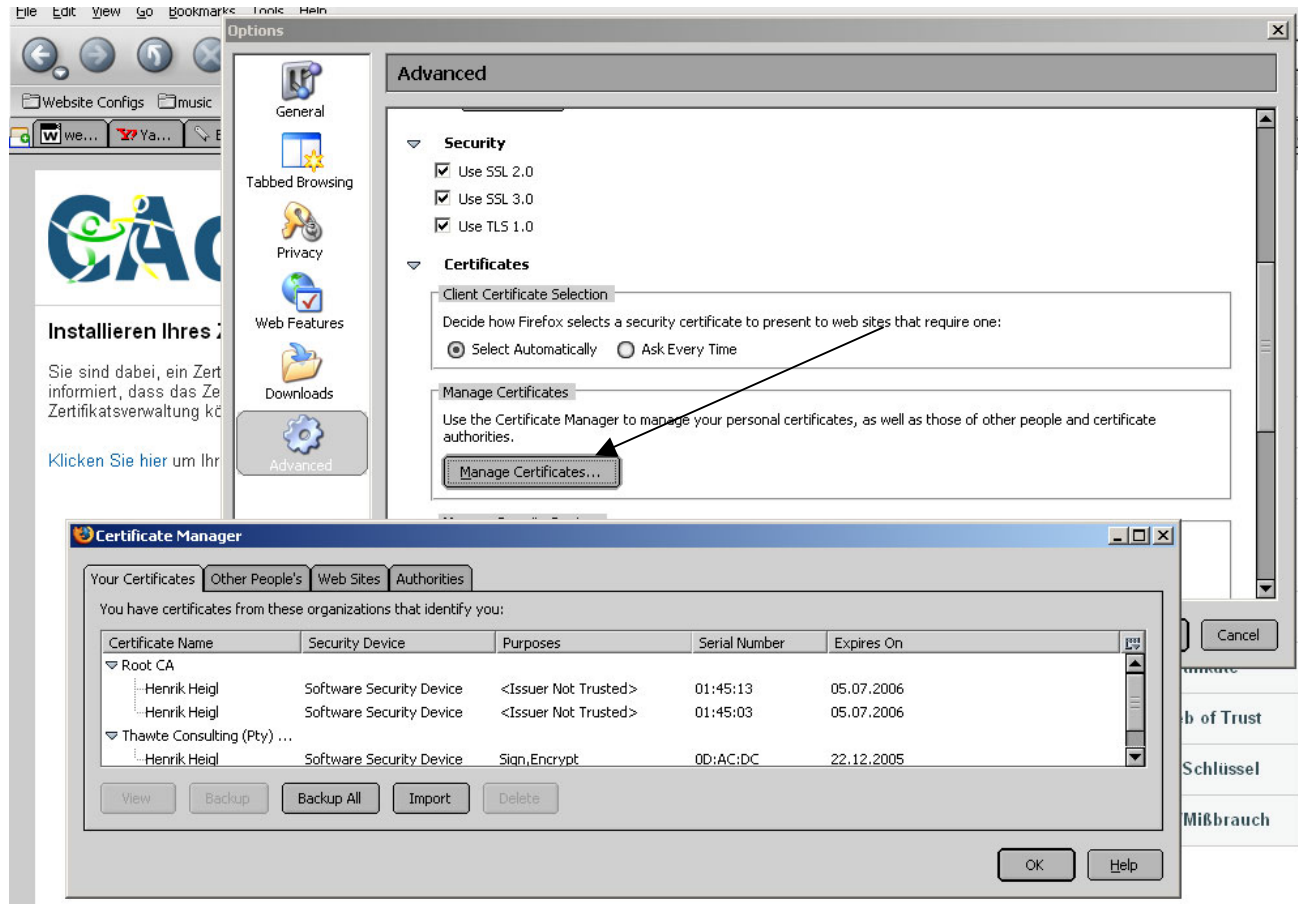
[Klicken Sie hier](#) um Ihr Zertifikat zu installieren.

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 (1) und es dann auch im Browser installieren (2)

3.) Zertifikat aus Browser sichern



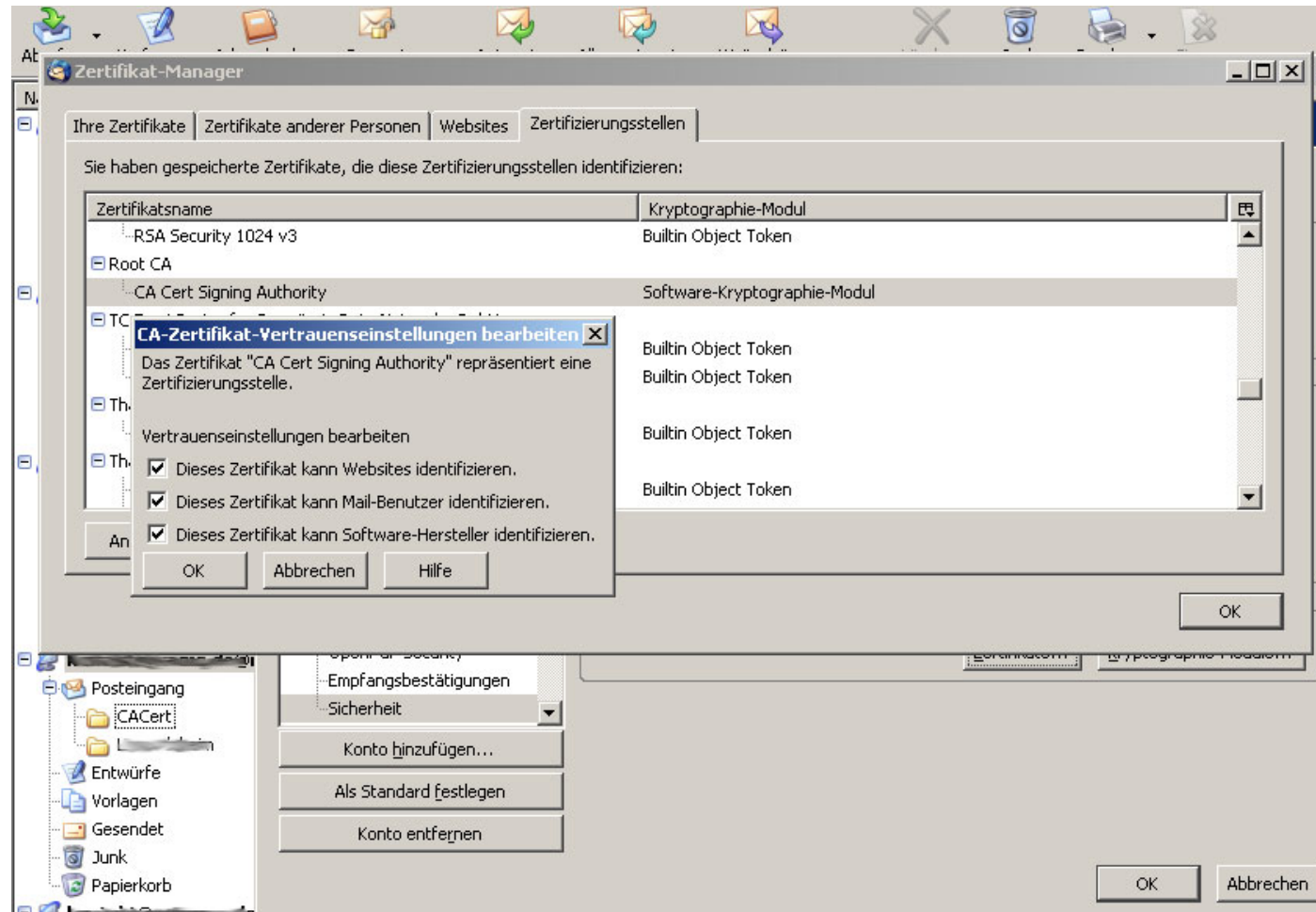
Nun kann das im Browser eingefügte Zertifikat unter den *Optionen – Sicherheit – Zertifikats Manager* (oder ähnlich, je nach Browser) gesichert werden. Einfach mit „Backup All“ anklicken und so das komplette Zertifikat im PKCS Format speichern.

4.) Zertifikat in Mail einbinden

(Bild grundsätzlich wie vorher)

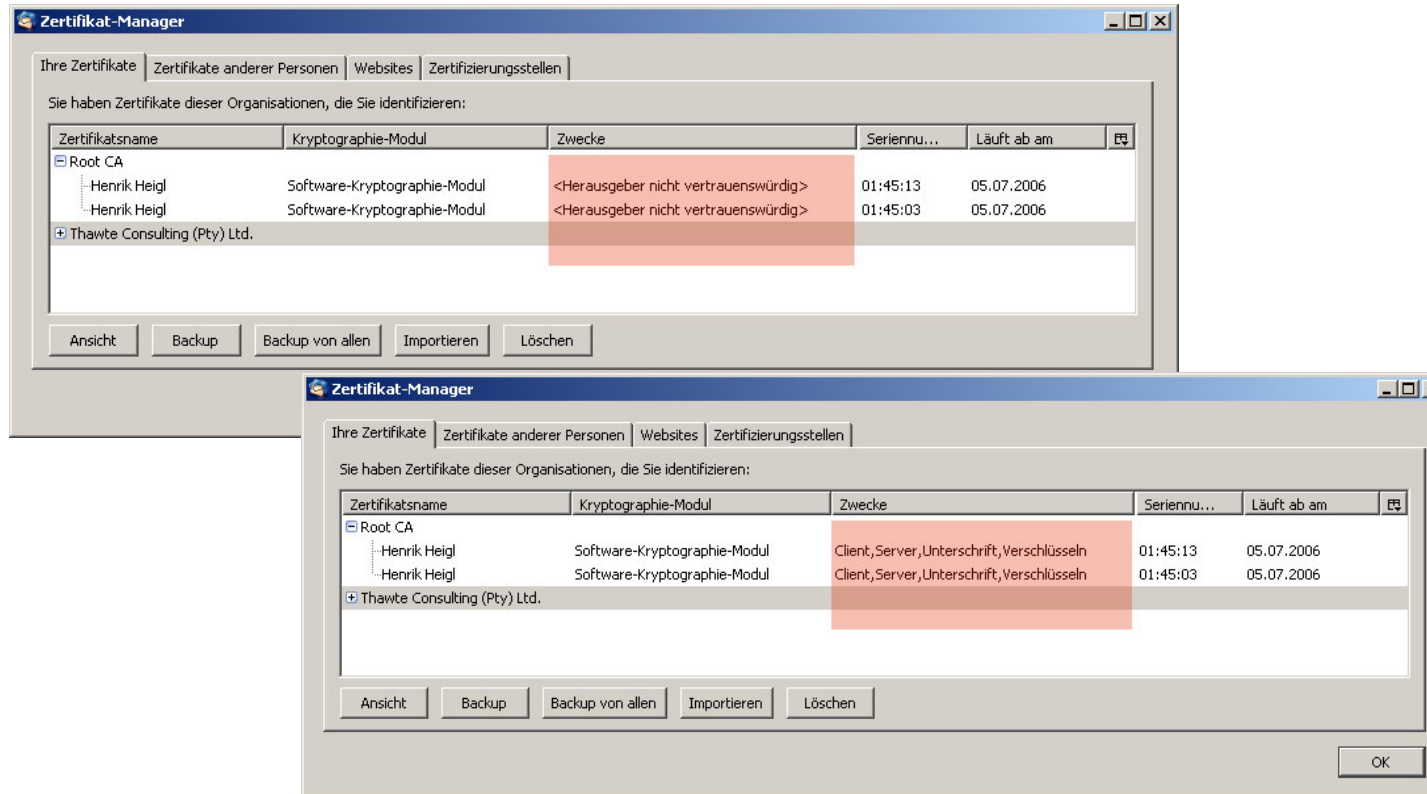
Nachdem man dieses dann z.B. im Thunderbird zur Mail Signierung wieder importiert hat (*Extras – Einstellungen – Erweitert Zertifikate – Importieren*) geht man in die Sicherheitseinstellungen im Zertifikatsmanagement (*Eigenschaften des Postfaches – Sicherheit – Zertifikate – Zertifizierungsstellen* 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, denn sonst können keine Mails verschickt werden.

Zertifikat in Mail einbinden /3



Es muss der Zertifikatsstelle vertraut werden, denn sonst können keine Mails verschickt werden.

Weitere Infos

- Weitere Infos unter <http://wiki.cacert.org/wiki/ClientCerts>

Danke und Fragen

- Henrik Heigl – kontakt@ivamp.de

