

CACert Zertifikatserstellung



Henrik Heigl
cert@ivamp.de



Key ID: 0x042B3EE5
Key fingerprint = 1847 C70A 88ED 8C73 E866 F607 33B5 B05C 042B 3EE5

Überblick

- Zertifikat erstellen

Hierzu wird Beispielhaft Mozilla Firefox und Thunderbird verwendet.

- Zertifikat downloaden

- Einbinden

- Exportieren

- weiterverwenden

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 "Miscellaneous" section, with an arrow pointing to the "Root Certificate" link.

Unter www.cacert.com anmelden und einloggen

Ggf. das Root Zertifikat (1) einbinden. Dies ist wichtig für spätere Aktionen.

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, there is a form titled "E-Mail hinzufügen" (Add Email). The form contains a label "E-Mail Adresse:" followed by a text input field containing "test@Domain.com" and a "Hinzufügen" (Add) 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." To the right of the main content area is a vertical 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

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](#)

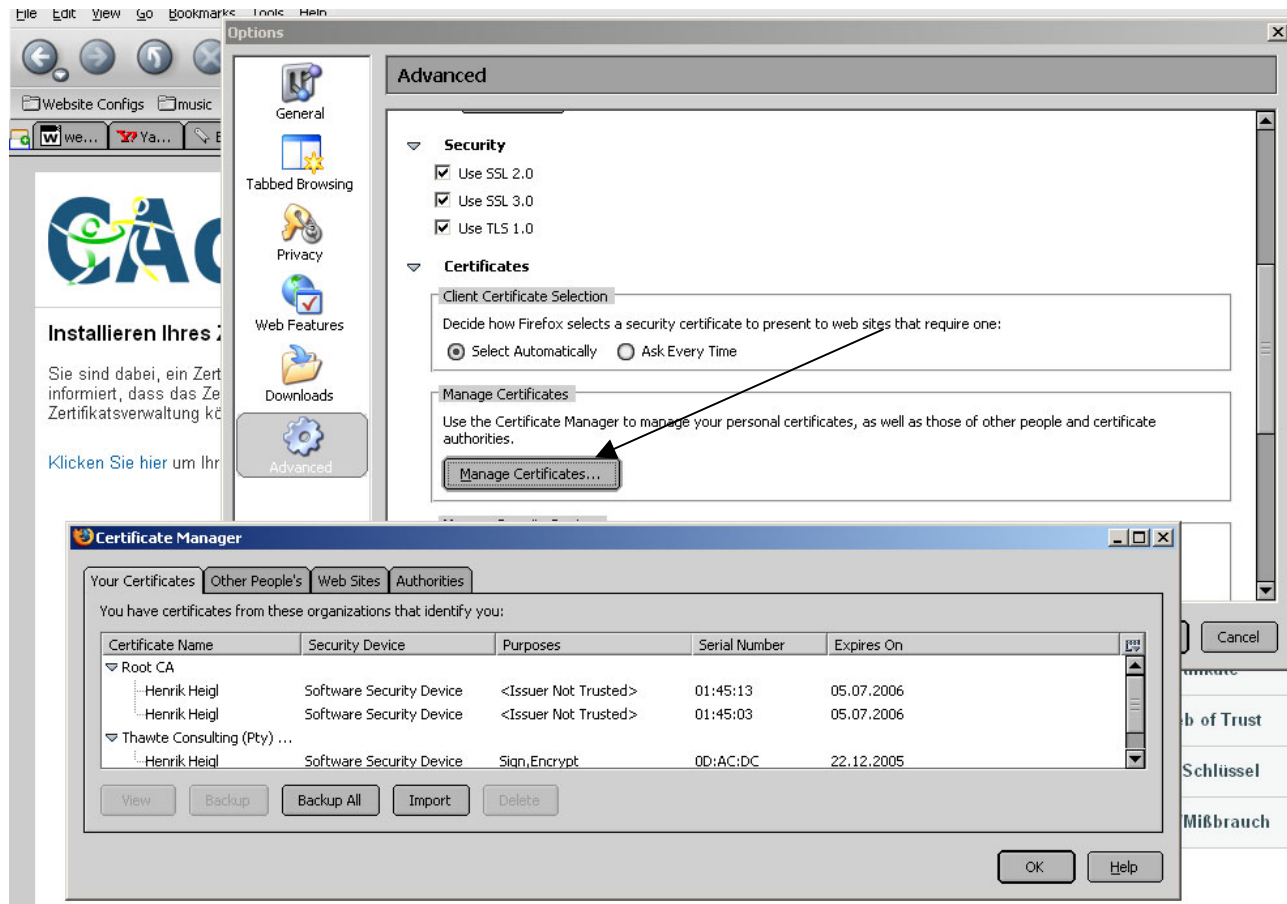
- + Meine Details
- + E-Mail Konto
- + Client Zertifikate
 - [Neu Anzeigen](#)
- + Domains
- + Server Zertifikate
- + CAcert Web of Trust
- + GPG/PGP Schlüssel
- + Streitfälle/Mißbrauch

Für die angelegte Mailadresse das Zertifikat anlegen (1)

Achtung: Es ist wichtig den Browser zu wissen bzw. alle Handlungen in ein und demselben Browser zu machen!

Hiernach mit „klicken Sie hier“ (2) das eben erstellte Zertifikat per Browser einbinden.

Zertifikat aus Browser sichern



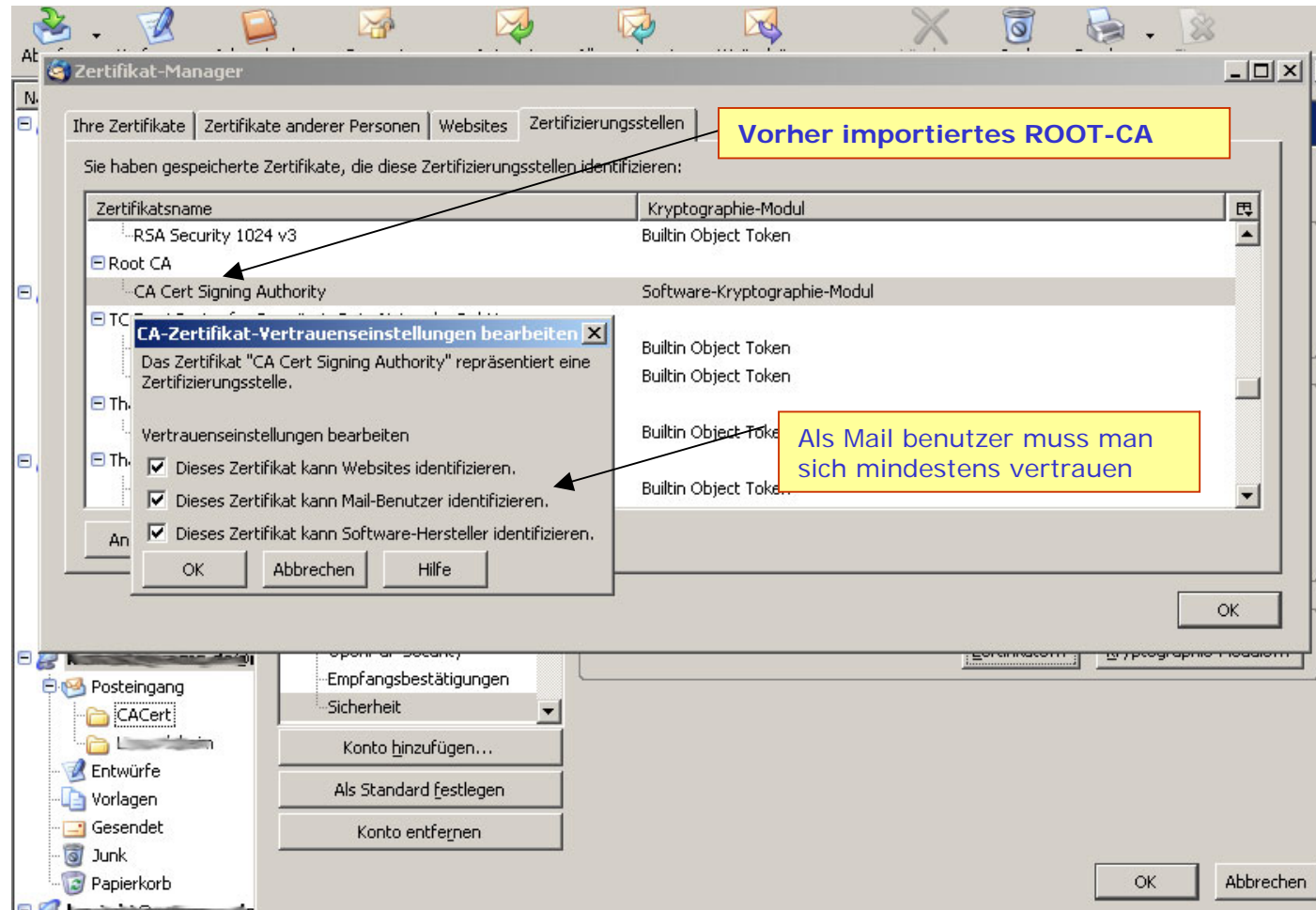
Nun kann das im Browser eingefügte Zertifikat unter den *Optionen – Sicherheit – Zertifikats Manager* (oder ähnlich, je nach Browser) gesichert werden.

Internet Explorer: *Optionen – Internet Optionen – Inhalt (Content) - Zertifikate*

Zertifikat in Mail einbinden

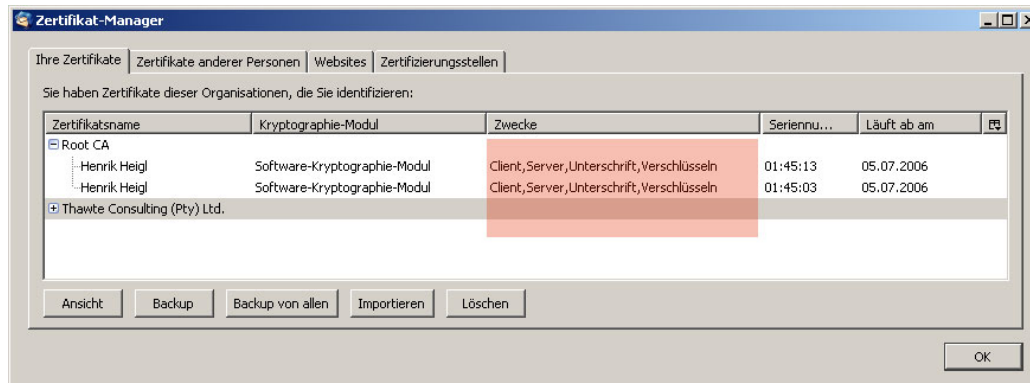
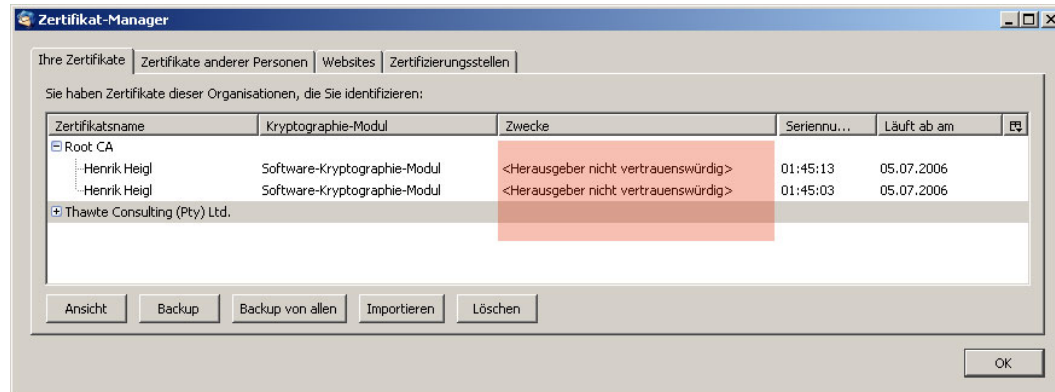
Nachdem man dieses dann z.B. im Thunderbird zur mail Signierung wieder importiert hat geht man in die Sicherheitseinstellungen im Zertifikatsmanagement (Eigenschaften des *Postfaches – Sicherheit – Zertifikate – Zertifizierungsstellen* runter bis CA Root erscheint) und bearbeitet das Root Zertifikat so, mindestens als mail Zertifikat vertraut wird.

Zertifikat in Mail einbinden /2



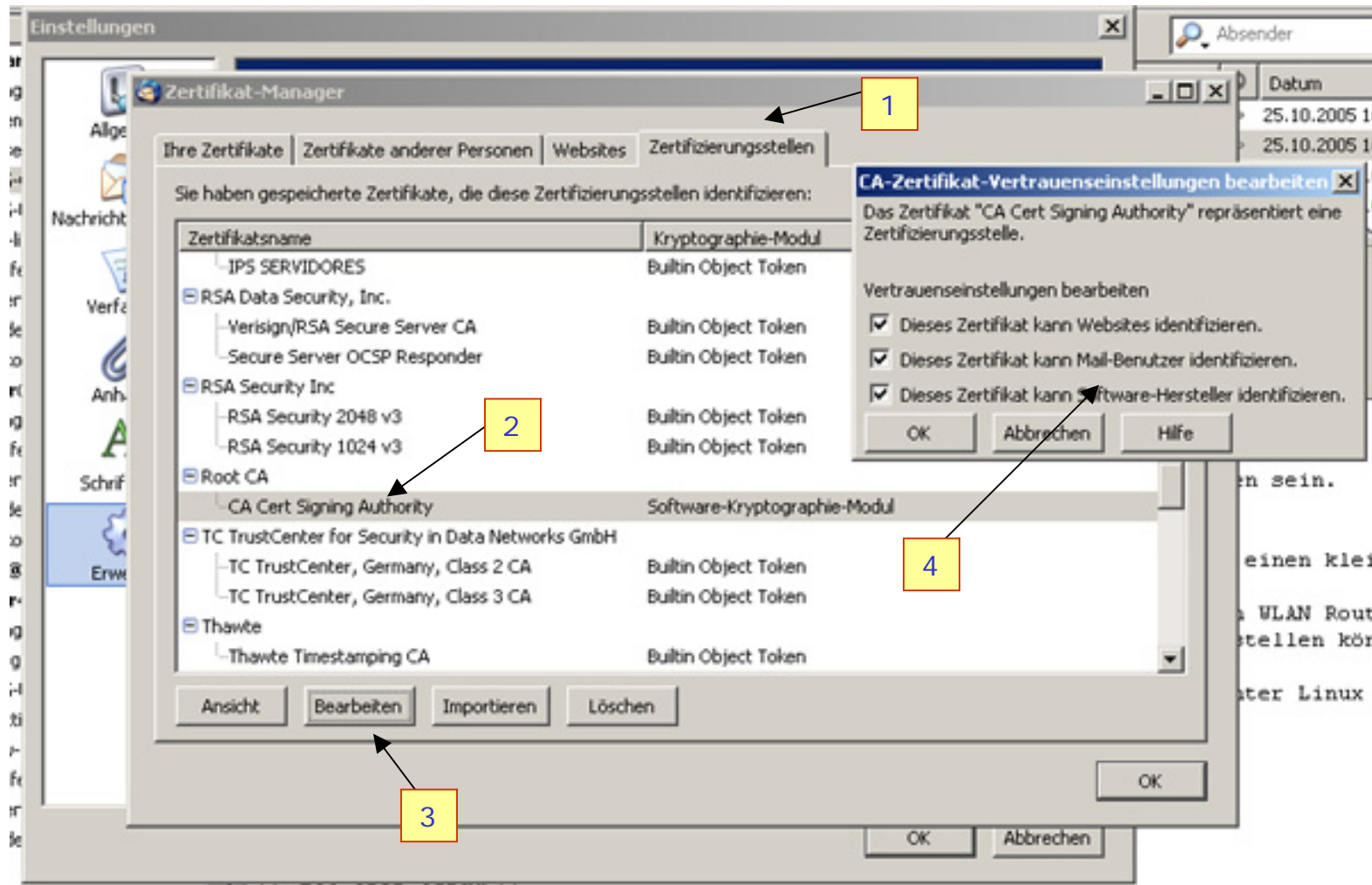
Es muss der Zertifikatsstelle vertraut werden, denn sonst können keine mails verschickt werden.

Zertifikat in Mail einbinden /3



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

Root CA vertrauen



Zertifikat eingebunden

- Überprüfung einer empfangenen Mail -

The screenshot shows an email client interface with a message from H. Heigl - LUG-GG dated 27.10.2005 09:59. The subject is 'Linuxinfotag Dresden'. A yellow callout box points to a question mark icon in the top right corner of the email header, with the text 'Kennzeichnung einer digital unterschriebenen E-Mail'. Below the email content, a 'Nachrichten-Sicherheit' dialog box is open. It contains the following text: 'Nachricht ist unterschrieben', 'Obwohl die digitale Signatur gültig ist, ist unbekannt, ob der Absender und der Unterzeichner die selbe Person sind. Die E-Mail-Adresse im Zertifikat des Unterzeichners stimmt nicht mit jener Adresse überein, von der aus die Nachricht geschrieben wurde. Bitte sehen Sie sich die Details des Unterschrifts-Zertifikats an, um zu sehen, wer die Nachricht unterschrieben hat.', 'Unterschrieben von: Henrik Heigl', 'E-Mail-Adresse: kontakt@ivamp.de', and 'Zertifikat herausgegeben von: CA Cert Signing Authority'. A yellow callout box points to the 'E-Mail-Adresse' field in the dialog, with the text 'Überprüfung des Zertifikates anhand eines Abgleichs zwischen Zertifikat und CA'. At the bottom of the dialog, there is a button labeled 'Unterschriftszertifikat ansehen'. Below the dialog, there is a warning: 'Nachricht wurde nicht verschlüsselt. Diese Nachricht wurde vor dem Senden nicht verschlüsselt. Informationen, die ohne Verschlüsselung über das Netzwerk / Internet gesendet werden, können von anderen Personen eingesehen werden, während sie übertragen werden.' At the bottom right of the email client, there are buttons for 'Ungelesen: 0' and 'Gesamt: 42'.

Weitere Infos

- Weitere Infos unter
<http://www.ivamp.de/cert>
<http://wiki.cacert.org/wiki/ClientCerts>

Danke und Fragen

- Henrik Heigl – cert@ivamp.de

