

# *CAcert – an overview and practical working*

---

**H. Heigl**

CAcert Public Relations

**CAcert@gmx.net**

## *overview*

---

- Who can we trust?
- You often send „postcards“ in times of phishing, SPAM and viruses ...
- Why use people passwords and send them in clear text over the internet?
- What can I do for my personal privacy?

## *Longterm goals*

---

- Privacy with PKI for everyone
- Security through authentication
- Trust in the Internet

## *What is a CA?*

---

- „Certification service provider“
- Confirmation of identity on a digitaly way
- Exhibition of digital certificates

## *Where to find?*

---

- Webservers with https://
- Digitaly signed and / or encrypted E-mails and Documents
- Signing of Programmcode

## *What is the CAcert.Inc ?*

---

- CAcert Inc. is a registered non-profit organization based in Australia which defines the rules and operates the central servers
- Founded ca. 2002
- CAcert.Inc 2003



## *Person relationship*

---

- Till now: Control of the identity for every certificate by costing per certificate of 200. € per annum
- However what the rest of the world, it doesn't help me if I can afford a certificate?
- CAcert separates the Assurance confirmation of the identity by means of official ( The transparency cards) of Edition of the certificates

## *Assurance*

---

- Assurance is the service an Assurer „controls“ the identity a person, at which an official transparency card checks by means of wanting to allocate points on the lifelong account with CAcert opposite CAcert confirmed and for this
- Free market
- About 7000 (1800 in 2004) Assurers worldwide



## *points*

Punkte	Status	Punktevergabe (maximal)
0 – 49	unassured	–
50 – 99	assured	–
100 – 109	assurer	10
110 – 119	assurer	15
120 – 129	assurer	20
130 – 139	assurer	25
140 – 149	assurer	30
150	fully assured	35
200	super assurer	150

## *certificates*

---

- Lifelong account at Cacert
- Issuing certificates even on the Internet any time
- Certificates are free
- arbitrary amount of certificates
- only Initial costs, no subsequent costs

## *technology*

---

- X.509
  - Server Certs
  - Client Certs
  - Codesigning (java, ActiveX, cellphones, etc.)

## *security*

---

- CAcert is checked by a web trust of compatible audit
- General 4 eyes principle
- Open and transparent structures
- Source code is available for audits
- Immediate revocation lists

## *success*


---

- Over 50,000 assured users
- More then 67,000 certificates
- Over 4000 Assurers worldwide
- In over 29 countries available and translated in over 14 languages
- Root Certificate implemented in many Applikations and Distributions as e.g. Knoppix, FreeBSD, Nokia 770, CentOS, Debian, gentoo, HGK Zuerich, etc.
- <http://www.cacert.org/stats.php>

---

# *How to build and implement the CAcert Certificates in Applications*

*join*



## Free digital certificates!

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.

**Login**  
Email Address:   
Pass Phrase:

- Join CACert.org**
  - [Join](#)
- My Account**
  - [Normal Login](#)
  - [Cert Login](#)
  - [Lost Password](#)
- Miscellaneous**
  - [CACert News](#)
  - [Howto Information](#)
  - [CACert Logos](#)
  - [CACert Statistics](#)
  - [Root Certificate](#)
  - [CRL](#)
  - [RSS News Feed](#)
  - [Credits](#)
  - [CACert Board](#)
- Translations**
  - [العربية](#)
  - [Български](#)
  - [Čeština](#)
  - [Dansk](#)
  - [Deutsch](#)
  - [Ελληνικά](#)

1

First of all you have to „join“ under [www.cacert.org](http://www.cacert.org) - Note: if the Root Certificate from CACert isn't already in your browser (1) please do this manually.

## Join form

My Details		
First Name:		<input type="text"/>
Middle Name(s) (optional)		<input type="text"/>
Last Name:		<input type="text"/>
Suffix (optional)		<input type="text"/>
Date of Birth (dd/mm/yyyy)	<input type="text" value="1"/>	<input type="text" value="January (1)"/> <input type="text" value="19XX"/>
Email Address:		<input type="text"/>
Pass Phrase*:		<input type="text"/>
Pass Phrase Again*:		<input type="text"/>
<small>*Please note, in the interests of good security, the pass phrase must be made up of an upper case letter, lower case letter, number and symbol.</small>		
<small>Lost Pass Phrase Questions - Please enter five questions and your responses to be used for security verification.</small>		
1)	<input type="text"/>	<input type="text"/>
2)	<input type="text"/>	<input type="text"/>
3)	<input type="text"/>	<input type="text"/>
4)	<input type="text"/>	<input type="text"/>
5)	<input type="text"/>	<input type="text"/>
<small>It's possible to get notifications of up and coming events and even just general announcements, untick any notifications you don't wish to receive. For country, regional and radius notifications to work you must choose your location once you've verified your account and logged in.</small>		
Alert me if:	<input checked="" type="checkbox"/> General Announcements <input checked="" type="checkbox"/> Country Announcements <input checked="" type="checkbox"/> Regional Announcements <input checked="" type="checkbox"/> Within 200km Announcements	
<input type="button" value="Next"/>		



## Add E-mail



### Kostenlose Digitale Zertifikate!

E-Mail hinzufügen

E-Mail Adresse:

Hinzufügen

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.

CACert.org

[Gehe zur Startseite](#)

[Ausloggen](#)

+ Meine Details

+ E-Mail Konto

[Hinzufügen](#)

[Anzeigen](#)

+ Client Zertifikate

+ Domains

+ Server Zertifikate

+ CACert Web of Trust

+ GPG/PGP Schlüssel

+ Streitfälle/Mißbrauch

You have to „add“ the E-Mail addresses for the Certificates you want to build.

## Building cert

New Client Certificate

Add	Address
<input checked="" type="checkbox"/>	[blurred email address]

☒ Sign by class 1 root certificate  
☐ Sign by class 3 root certificate

Please note: The class 3 root certificate needs to be imported into your email program as well as the class 1 root certificate so your email program can build a full trust path chain. Until we are included in browsers this might not be a desirable option for most people

☐ No Name  
☒ Include Name [blurred name]

Optional Client CSR, no information on the certificate will be used

Next

The name can be included if the assurance was made and you got >50 points.

More infos about CSR (**C**ertificate **S**igning **R**quest):  
<http://wiki.cacert.org/wiki/CSR>

## *Deliver to the browser*

**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.

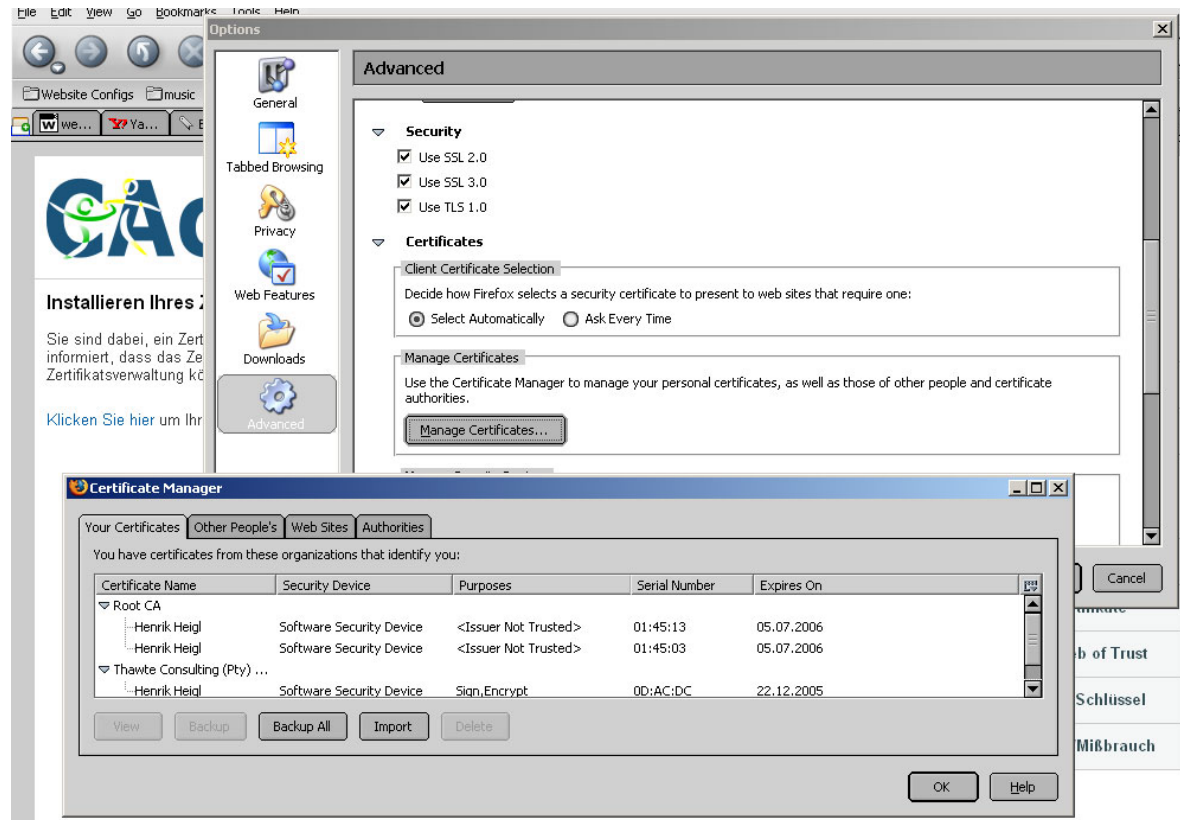
[Klicken Sie hier](#) um Ihr Zertifikat zu installieren.

**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

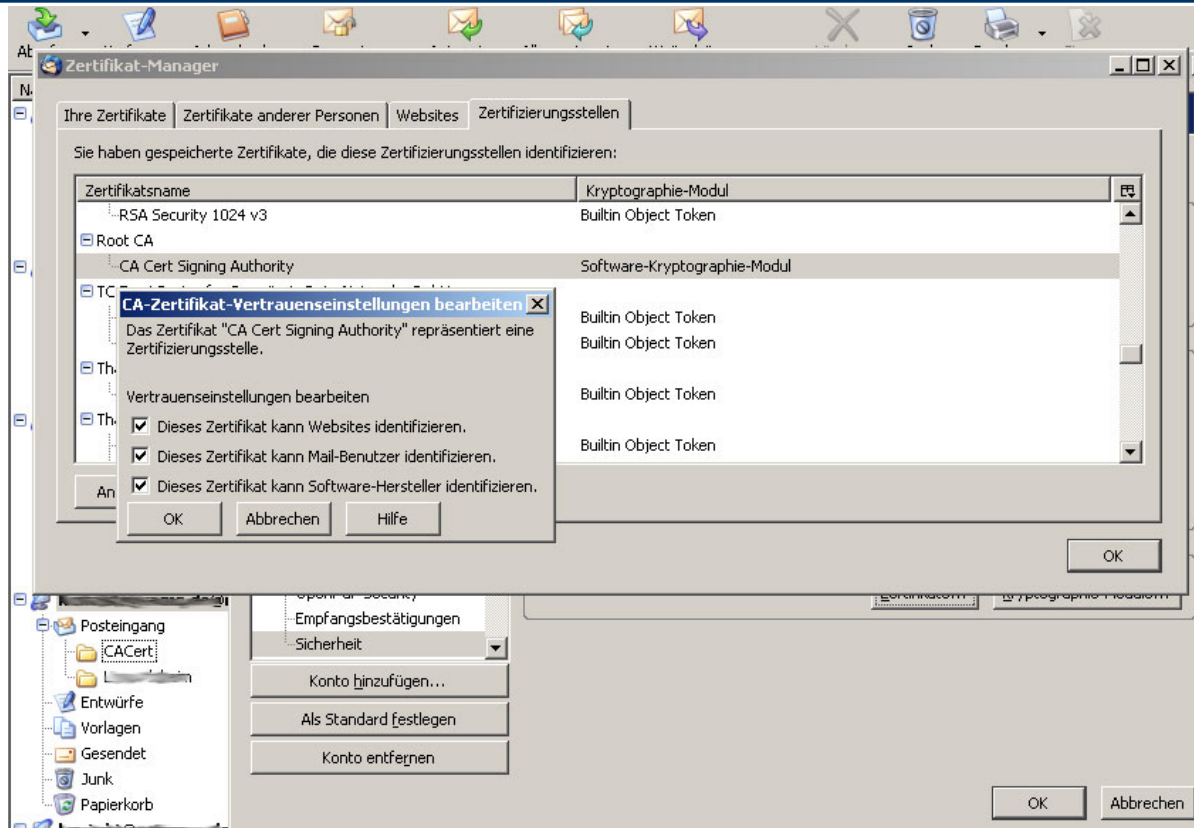
Then finish this part to add (1) the Certificate through the browser in it (2).

## Extract from Browser



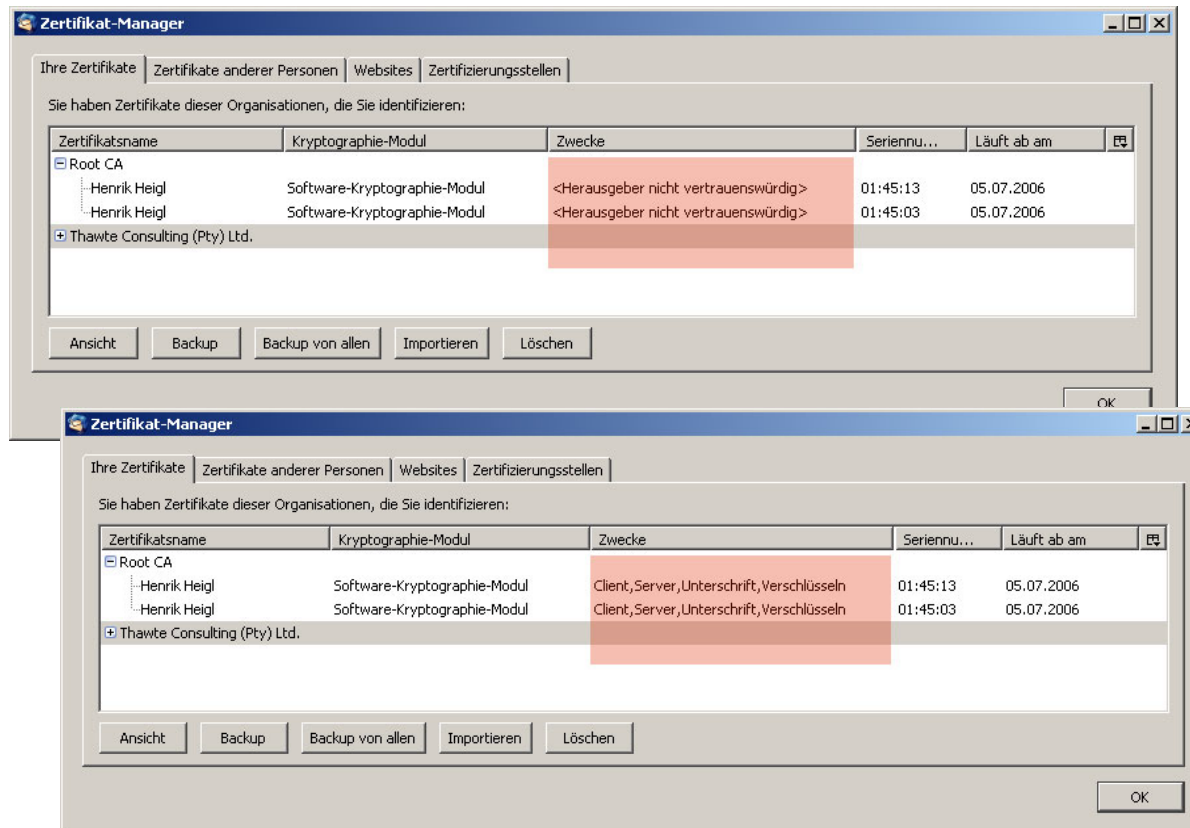
Over the point „backup all“ in the security options in your browser you can „extract“ the Certificate out of the browser into a single encrypted File (PKCS).

## Import in another app (e.g. Thunderbird E-mail Client)

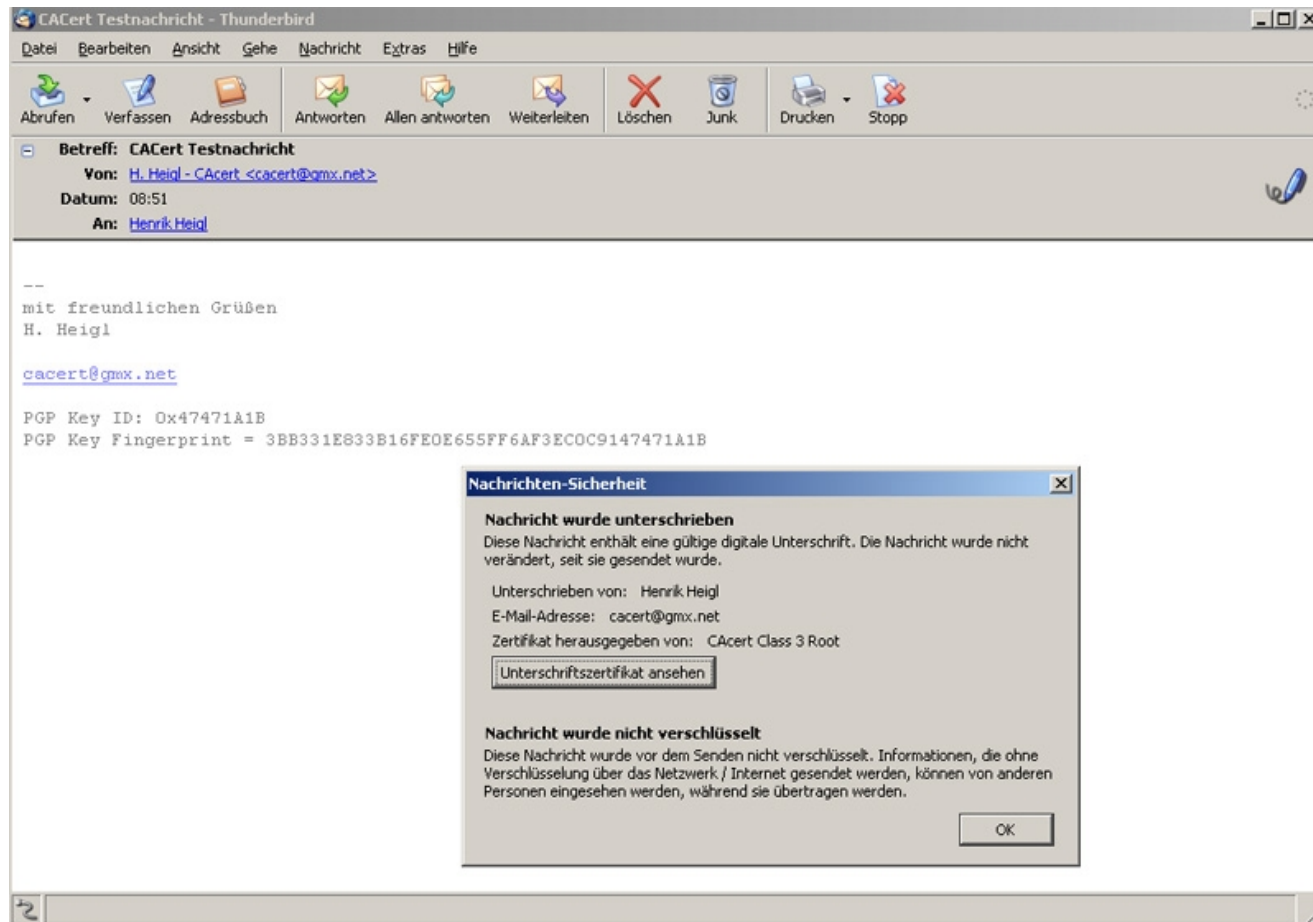


After importing the Certificate you have to „trust“ your own certificate. Otherwise you cannot write signed E-mails with it.

# *With and without trusting*



## *How it looks like*



## *More information*

---

- **Cacert**  
<http://www.cacert.org>  
<http://www.cacert.org/wiki>
- <http://www.ivamp.de/cert>
- CACert im irc
  - Server: [irc.cacert.org](http://irc.cacert.org)
  - Chanel: [#cacert](#) oder [#cacert.ger](#)