

CAcert - ein Überblick und Anwendung

Powered by

H. Heigl

CAcert Public Relations, Germany

CAcert@gmx.net

Fragen

- Warum verwenden die meisten Leute noch immer das elektronische Gegenstück der Postkarte obwohl Themen wie Viren, Spam und Phishing in aller Munde sind?
- Warum verwenden die Leute noch immer Passwörter, und schicken sie im Klartext?
- Was kann ich tun, um mich und meine Privatsphäre zu schützen?

Grundlagen Sicherheit



Sichere Daten-Kommunikation: Was gehört dazu?

- **Authentizität**
Wie stelle ich sicher, daß die Nachricht, die ich erhalte, wirklich von der Person kommt, von der ich es glaube, das Sie es ist?
- **Integrität**
Wie stelle ich sicher, daß die Nachricht, nachdem sie abgesandt wurde, von niemandem verändert wurde?

Grundlagen /2



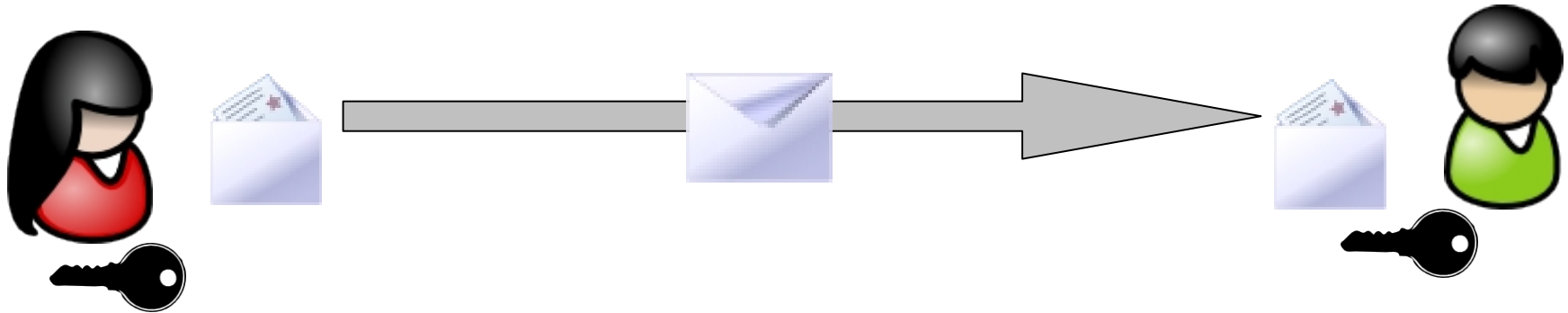
- **Verbindlichkeit**
sicherstellen, daß der Urheber und Absender einer Nachricht nachträglich nicht bestreiten kann, diese Nachricht verfasst zu haben
- **Vertraulichkeit**
Wie stelle ich sicher, dass die Nachricht nur vom Empfänger und keinem dritten gelesen wird?

Grundlegender Lösungsansatz

- Verschlüsselung (GPG)
 - PGP entwickelt von Werner Koch und Phil Zimmermann
 - Eigene Schlüssel und Zertifikate
 - Web-of-Trust
- Signierung (S/Mime)
 - Auch für Verschlüsselung anwendbar
 - Alternativer Standard
 - X.509



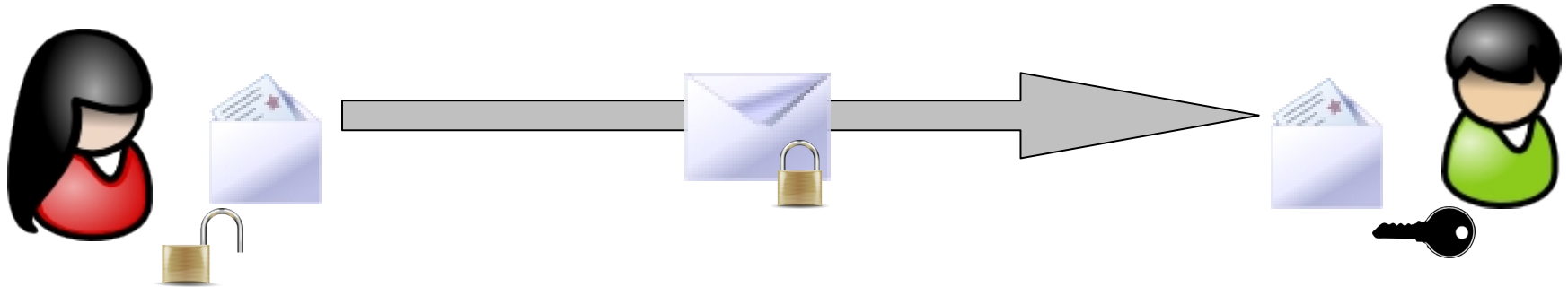
Symmetrische Verschlüsselung



Beide Benutzer haben den **gleichen** Schlüssel, der durch einen **geheimen** Kanal ausgetauscht werden muss.

Nur wie bekomme ich einen sicheren Kanal?

Asymetrische Verschlüsselung



Jeder Benutzer hat einen geheimen und einen öffentlichen Schlüssel. Der öffentliche Schlüssel muss vorher durch einen **authentischen** Kanal verteilt werden.

Nur wie bekomme ich einen authentischen Kanal, wenn ich meinen Kommunikationspartner nie persönlich getroffen habe?

Vertrauenswürdigkeiten

Home made identity cards



Foto des
Vortragenden hier
einfügen

Name: Linus Torvalds

Date of Birth: December 28, 1969

Wieso glaubt niemand, dass ich Linus Torvalds bin?
Aber (fast) jeder glaubt, was auf meiner Identitätskarte steht!

Was ist eine CA

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

Cacert Inc

- 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



Praktische Anwendungen

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

Personenbindung

- Bisher: Kontrolle der Identität für jedes Zertifikat, dadurch Kosten pro Zertifikat von 200,- € pro Jahr bei vielen kommerziellen Anbietern
- Was hilft es mir, wenn ich mir ein Zertifikat leisten kann, aber der Rest der Welt nicht?
- CAcert trennt die **Assurance** (Bestätigung der Identität mittels amtlichen Lichtbild Ausweisen) von der Ausgabe der X.509 Zertifikate (technische Seite)

X.509

- Bindung zwischen dem öffentlichen Schlüssel und einer E-Mail Adresse, einer Webserver Domäne oder einem Personennamen.
- Zertifizierungsstellen (Cacert, VeriSign, TC Trustcenter usw.) garantieren, dass der Besitzer des privaten Schlüssels auch der Inhaber der entsprechenden E-Mail Adresse, Domäne, etc. ist.
 - Klasse 1 Zertifikat: automatisch verifizierte Angaben
 - Klasse 3 Zertifikat: eingehende Prüfung von staatlich ausgestellten Dokumenten
- Die Zertifizierungsstellen oft verlangen viel Geld für ein Zertifikat, sind aber oft nicht ganz vertrauenswürdig...
- Alternativer Ansatz von PGP/GPG: Web of Trust
Der Benutzer entscheidet, welche Zertifikate er für valide hält und welchen Benutzer er als vertrauenswürdigen Signierer einstuft.

CAcert Zertifikate

- Lebenslanger Account bei CAcert
- Zertifikate jederzeit selbst im Internet ausstellen
- Zertifikate sind kostenlos
- beliebige Menge von Zertifikaten
- dadurch nur Initialkosten, keine Folgekosten

Verfügbare Zertifikate

- Client certificates (unassured)
Gültigkeit 12 Monate. Nur E-Mail Adresse im Zertifikat.
- Assured client certificates
Gültigkeit 12 Monate. Ab 50 Punkte.
- Code signing certificates
Zum signieren von Java Applets usw. Erst ab 100 Punkte und mit
zusenden einer Kopie des Ausweises.
- Server certificates (unassured)
Gültig für 6 Monate.
- Assured server certificates
Gültig für 24 Monate. Ab 50 Punkte.

(Siehe auch <http://www.cacert.org/index.php?id=19>)

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
- Mittlerweile über 1800 Assurer (über 6500 im Jahre 2006) weltweit

Pflichten des Assurers

- Assurance nur bei einem persönlichen Treffen.
 - Zwei Ausweise müssen kontrolliert werden.
 - CAP Formular (CAcert Assurance Programm) muss ausgefüllt und unterschrieben werden.
 - Der Assurer muss das CAP-Formular 7 Jahre lang aufbewahren.
-
- Alle Infos für Assurer im Assurance Handbook:
<http://wiki.cacert.org/wiki/AssuranceHandbook>

Punkteschema

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

Wie sicher ist Cacert?

- CACert wird durch einen WebTrust kompatiblen Audit überprüft
- Durchgängiges 4 Augen Prinzip bei Assurances
- Offene und transparente Strukturen
- Sourcecode steht für Audits zur Verfügung
- Sofortige Widerrufslisten

Erfolg

- 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>

Quo Vadis

- 60'000 registrierte Benutzer (davon über 6'000 Assurer und 3'500 Benutzer mit 1-99 Punkten).
- Root-Zertifikat schon eingebaut in:
FreeBSD, Nokia 770, Knoppix 3.8, Debian, Gentoo, MirBSD, CentOS 4, Wildfire, HGK-Zürich
- Root-Zertifikat bald in:
Grml 0.5, Fedora Core, Mozilla, ...
- über 71.000 verifizierte Benutzer
- über 40.000 verifizierte Domains und über 90.000 verifizierte E-Mail Adressen
- über 7000 Assurer (6500 Mitte 2006)
- Pro Monat durchschnittlich 2000-3000 neue Benutzer, 5000 neue Zertifikate
- 2003 waren rund 2700 neue benutzer zu verzeichnen. Bis 2006 hat sich diese Zahl verzehnfacht

CAcert HowTo

Zertifikatserstellung mit CAcert

The screenshot shows the CACert website interface. At the top left is the CACert logo. To the 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", "My Account", "Miscellaneous", and "Translations". An arrow points from a red "1" to the "Root Certificate" link in the "Miscellaneous" section.

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:

Login

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

Unter www.cacert.org anmelden und einloggen

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

anmelden

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"/>
<p>*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.</p>	
<p>Lost Pass Phrase Questions - Please enter five questions and your responses to be used for security verification.</p>	
1)	<input type="text"/>
2)	<input type="text"/>
3)	<input type="text"/>
4)	<input type="text"/>
5)	<input type="text"/>
<p>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.</p>	
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"/>	

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. A note below the form states: '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

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.

Zertifikat erstellen

The screenshot shows a web form titled "New Client Certificate". It has a table with two columns: "Add" and "Address". The "Add" column contains a checked checkbox. The "Address" column contains a blurred email address. Below the table, there are two radio button options: "Sign by class 1 root certificate" (selected) and "Sign by class 3 root certificate". A note follows: "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". Below this, there are two more radio button options: "No Name" and "Include Name" (selected). A text box for "Optional Client CSR, no information on the certificate will be used" is empty. At the bottom right, there is a "Next" button.

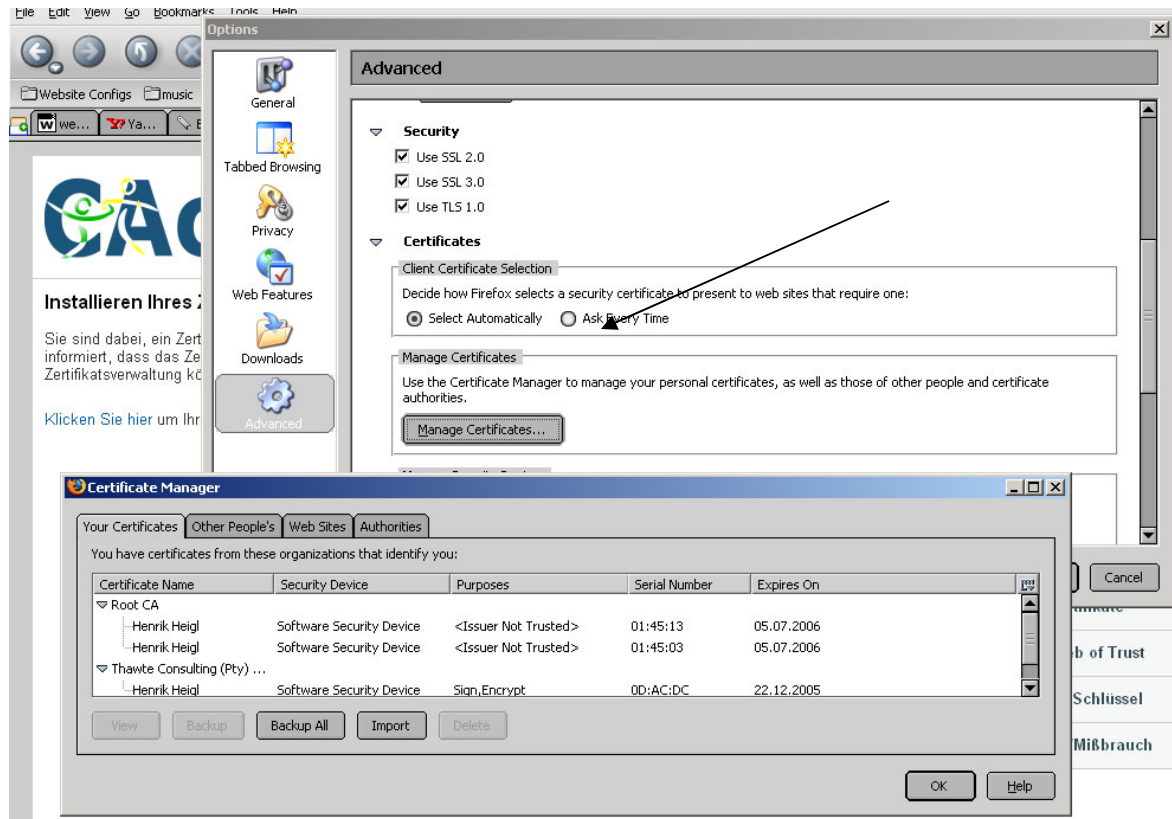
Die Auswahl ob der eigene Name im Zertifikat enthalten sein soll oder nicht taucht erst nach der Assurance (Punktezahl > 50) auf.

Weitere Infos zu CSR (**C**ertificate **S**igning **R**equ**e**st):

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

H. Heigl – cacert@gmx.net

www.Cacert.org

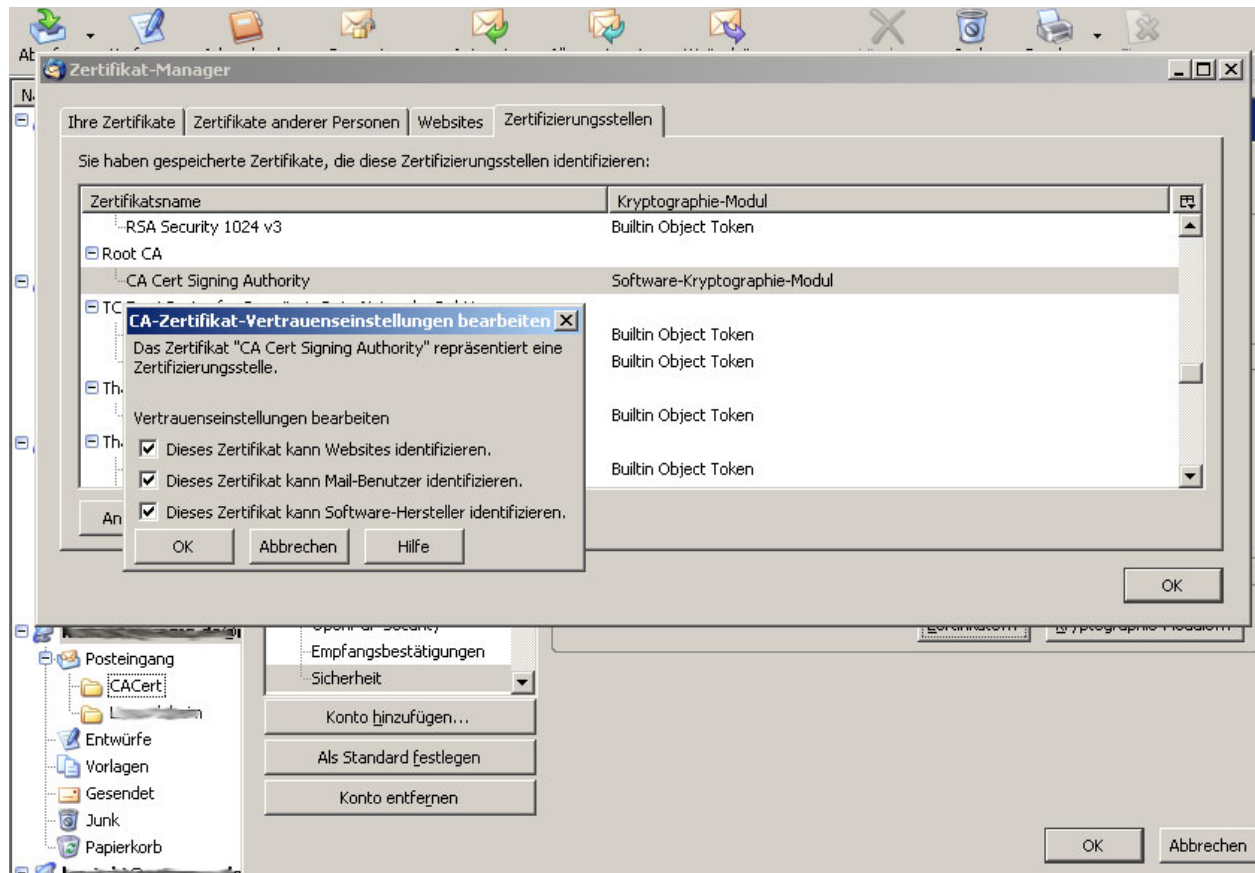


Nun kann das im Browser eingefügte Zertifikat unter den Optionen – Sicherheit – Zertifikats Manager (oder ähnlich, je nach Browser) gesichert werden. Im Verlauf des Exports müssen sie zwei Passwörter wählen. Dieses kann, muss aber nicht dasselbe wie bei Cacert.org sein.

Zertifikat in Mail einbinden

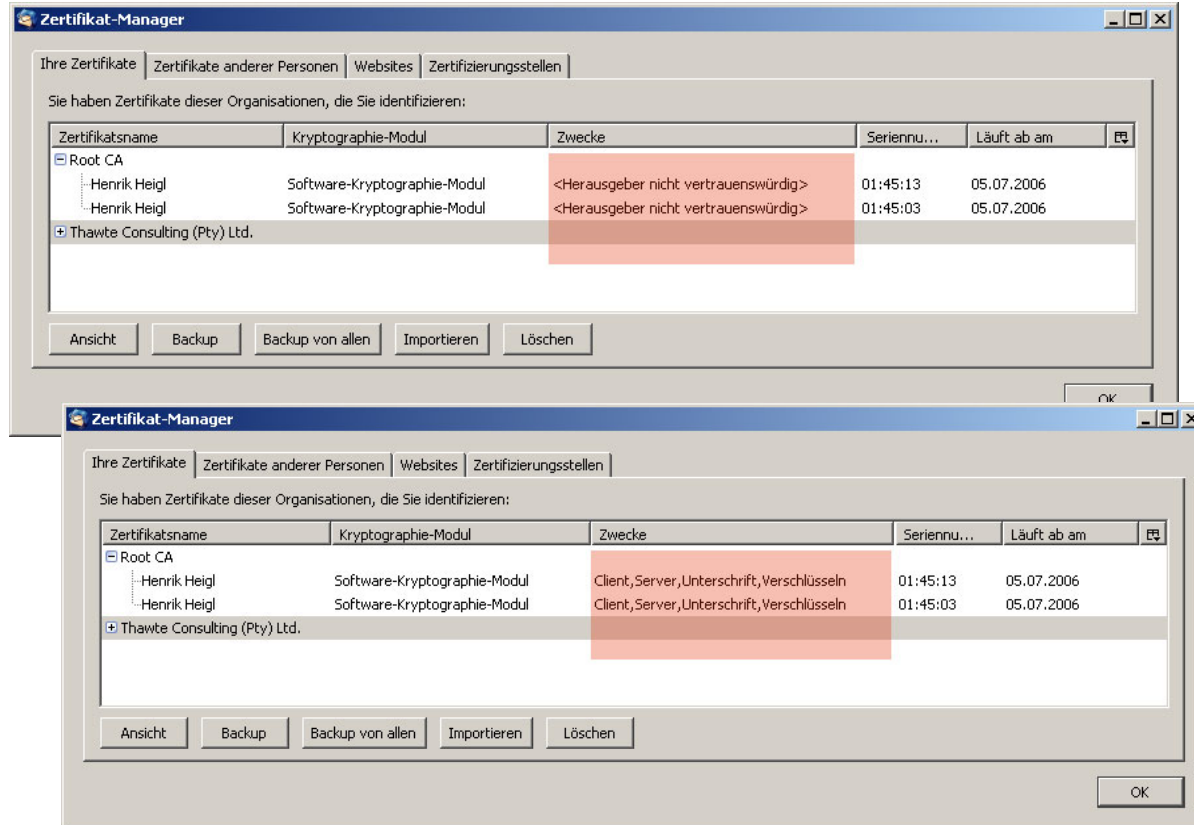
Nachdem man dieses dann z.B. im Thunderbird zur Mail Signierung wieder importiert hat (selber Weg wie beim exportieren im Browser) geht man in die Sicherheitseinstellungen im Zertifikatsmanagement (Eigenschaften des Postfaches – Sicherheit – Zertifikate – Zertifizierungsstellen runter bis *CA Root* erscheint) 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

The screenshot shows a Thunderbird email client window titled "CACert Testnachricht - Thunderbird". The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Gehe", "Nachricht", "Extras", and "Hilfe". The toolbar contains icons for "Abrufen", "Verfassen", "Adressbuch", "Antworten", "Allen antworten", "Weiterleiten", "Löschen", "Junk", "Drucken", and "Stopp".

The email header shows:

- Betreff:** CACert Testnachricht
- Von:** H. Heigl - CACert <cacert@gmx.net>
- Datum:** 08:51
- An:** Henrik Heigl

The email body contains the following text:

--
mit freundlichen Grüßen
H. Heigl
cacert@gmx.net
PGP Key ID: 0x47471A1B
PGP Key Fingerprint = 3BB331E833B16FEOE655FF6AF3ECOC9147471A1B

A "Nachrichten-Sicherheit" dialog box is overlaid on the email content. It contains the following information:

- Nachricht wurde unterschrieben**
Diese Nachricht enthält eine gültige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde.
Unterschrieben von: Henrik Heigl
E-Mail-Adresse: cacert@gmx.net
Zertifikat herausgegeben von: CACert Class 3 Root
[Unterschriftszertifikat ansehen](#)
- 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.

Weiterführendes ...

- **Cacert**
<http://www.cacert.org>
<http://www.cacert.org/wiki>
- **Signaturgesetz:**
http://bundesrecht.juris.de/bundesrecht/sigg_2001/
<http://www.netlaw.de/gesetze/sigg.htm>
- **Kleine Secure-Mail und –Messaging FAQ**
<http://www.ivamp.de/sig.pdf>
<http://www.ivamp.de/cert>
- CACert im irc
 - Server: `irc.cacert.org`
 - Chanel: `#cacert` oder `#cacert.ger`

Statistics

- über 71.000 verifizierte Benutzer
- über 40.000 verifizierte Domains und über 90.000 verifizierte E-Mail Adressen
- über 7000 Assurer (6500 Mitte 2006)
- Pro Monat durchschnittlich 2000-3000 neue Benutzer, 5000 neue Zertifikate
- 2003 waren rund 2700 neue benutzer zu verzeichnen. Bis 2006 hat sich diese Zahl verzehnfacht