



SSL-Zertifikate und S/MIME

Sicher surfen und verschlüsseln

Philipp Gühring philipp@cacert.org

Zertifikat?

Digitaler Personalausweis,
mit dem sich
Personen und Computer
im Internet ausweisen können

Anwendungen

- ◆ Serverzertifikate
 - ◆ Webserver mit https:// (SSL) absichern
 - ◆ Mailserver
 - ◆ VPN
- ◆ Clientzertifikate
 - ◆ S/Mime: Unterschreiben und Verschlüsseln von Emails
 - ◆ Anmeldung bei Webseiten
 - ◆ Software/Makros/Applets signieren
 - ◆ Kostenloser Internetzugang bei Funkfeuer

Client Zertifikate in der Praxis

- ◆ Firefox
 - ◆ Login
 - ◆ Email Adressen freischalten
 - ◆ Client Zertifikat beantragen
 - ◆ Zertifikat installieren
 - ◆ Sicherung des Zertifikats
 - ◆ auf <https://secure.cacert.org/> verwenden



CAcert.org Webseite

Willkommen bei CAcert.org - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/

News Reference Maps and Directions CAcert NEWS Blog heise online News



Einleitung

Es hat lange gedauert, aber das Warten hat sich gelohnt! Endlich bekommt man Sicherheit zum richtigen Preis... Kostenlos!

Jahrelang musste jeder im Internet hohe Gebühren für Sicherheit bezahlen, die in Wirklichkeit gar nicht so teuer sein müsste und schon gar nicht sein sollte.

Die primären Ziele sind:

- Aufnahme des CAcert Zertifikats in die wichtigsten Browser!
- Einen Vertrauens-Mechanismus bereitzustellen, der die Sicherheitsanforderungen von Verschlüsselung erfüllt.

For general documentation and help please see our [Wiki Dokumentation](#) site.

Bei CAcert.org


- [Mitmachen](#)
- [Community Agreement](#)
- [Root-Zertifikat](#)

Mein Konto

- [Passwort Login](#)
- [Passwort Vergessen](#)
- [Net Cafe Login](#)
- [Zertifikats-LOGIN](#)

+ Über CAcert.org

+ Übersetzungen

Fertig [www.cacert.org](#) S  AS ready

Einloggen, E-Mail Adresse



Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php?id=1

News Reference Maps and Directions CAcert NEWS Blog heise online News

CAcert

E-Mail hinzufügen

E-Mail Adresse:

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

+ GPG/PGP Schlüssel

Fertig www.cacert.org AS35492


E-Mail Adresse verifiziert

Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php?id=2

News Reference Maps and Directions CAcert NEWS Blog heise online News



E-Mail Konto			
Standard	Status	Löschen	Adresse
<input checked="" type="radio"/>	Verifiziert	nicht verfügbar	pg@futureware.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	p.guehring@futureware.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	pg@futureware.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	www@futureware.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	postmaster@cacert.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	ph@cacert.org
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	ph@p.guehring@futureware.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	www@futureware.at
<input type="radio"/>	Verifiziert	<input type="checkbox"/>	ph@p.guehring@futureware.at

Setze als Standardwert Löschen

CAcert.org






[Gehe zur Startseite](#)
[Ausloggen](#)

+ Meine Details

+ E-Mail Konto
[Hinzufügen](#)
[Anzeigen](#)

+ Client Zertifikate

+ GPG/PGP Schlüssel

Fertig www.cacert.org      AS n/a

Zertifikat erzeugen ...

Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php?id=3

Neues Client-Zertifikat

Hinzufügen	Adresse
<input checked="" type="checkbox"/>	pg@futureware.at
<input type="checkbox"/>	p.guehring@futureware.at
<input type="checkbox"/>	...
<input type="checkbox"/>	...
<input type="checkbox"/>	...
<input type="checkbox"/>	...
<input type="checkbox"/>	...
<input type="checkbox"/>	...
<input type="checkbox"/>	...

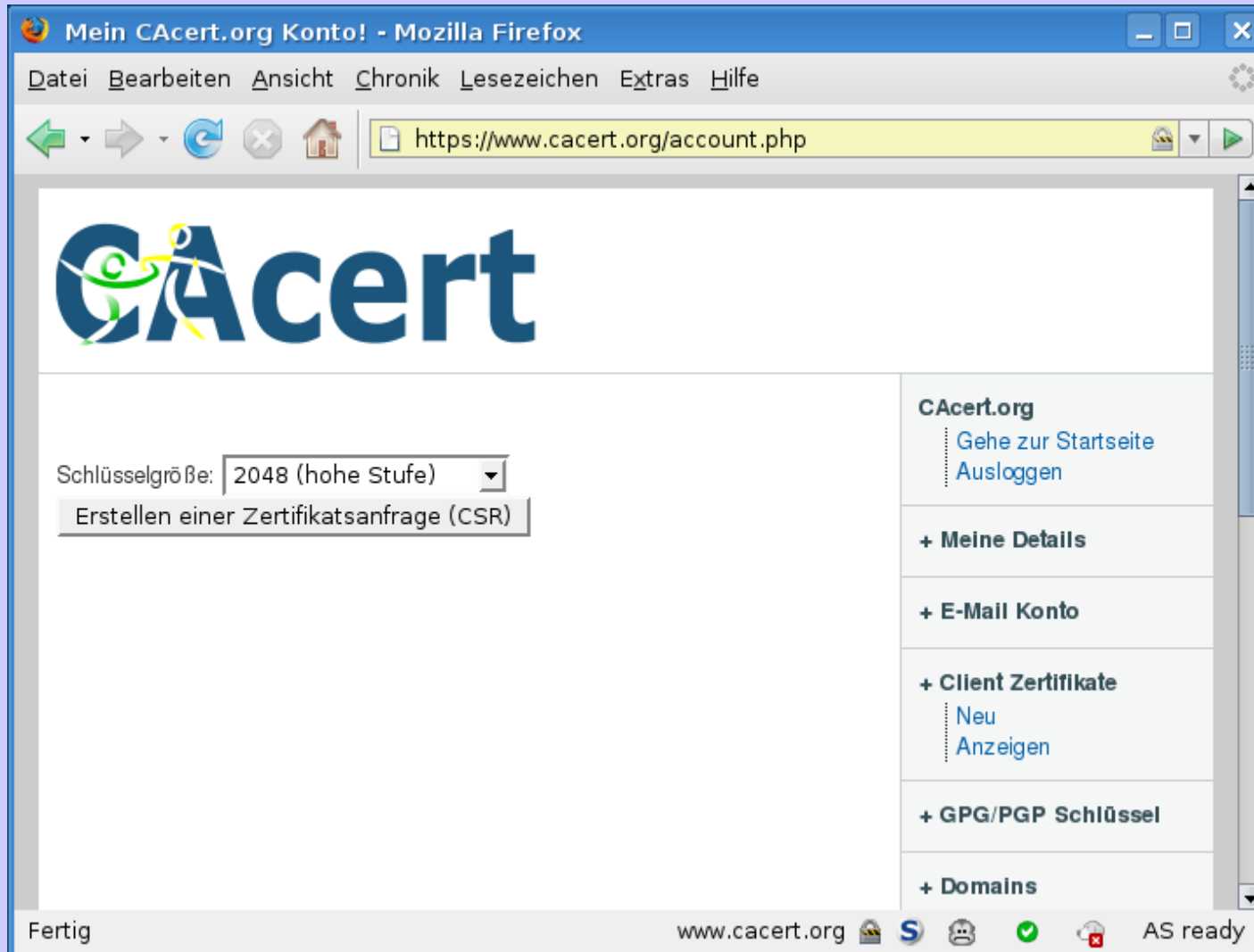
- + CAcert Vertrauensnetzwerk
- + CAP/TTP Formulare
- + System Administrator
- + Streitfälle/Mißbrauch
- + Werbung

Signieren mit dem Klasse 1 Root Zertifikat
 Signieren mit dem Klasse 3 Root Zertifikat
 Bitte beachten Sie: Das Klasse 3 Root Zertifikat und das Klasse 1 Zertifikat müssen beide in Ihr E-Mail-Programm installiert/importiert werden, damit das Programm den vollständigen Vertrauenspfad (Trust-Path) überprüfen kann. Bis in Zukunft das CAcert Zertifikat von den Browserherstellern vorinstalliert wird, dürfte das für die meisten Benutzer eine weniger wünschenswerte Option sein.

Kein Name
 Einfügen 'Philipp Gühring'
 Einfügen 'Philipp Michael Gühring'

Fertig www.cacert.org

Schlüssel Parameter



The screenshot shows a Mozilla Firefox browser window titled "Mein CAcert.org Konto! - Mozilla Firefox". The address bar displays "https://www.cacert.org/account.php". The main content area features the CAcert logo and a form for generating a Certificate Signing Request (CSR). The form includes a dropdown menu for "Schlüsselgröße:" set to "2048 (hohe Stufe)" and a button labeled "Erstellen einer Zertifikatsanfrage (CSR)". On the right side, there is a sidebar with navigation links: "CAcert.org", "Gehe zur Startseite", "Ausloggen", "+ Meine Details", "+ E-Mail Konto", "+ Client Zertifikate" (with sub-links "Neu" and "Anzeigen"), "+ GPG/PGP Schlüssel", and "+ Domains". The status bar at the bottom shows "Fertig", "www.cacert.org", and "AS ready".

Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php

CAcert

Schlüsselgröße: 2048 (hohe Stufe)

Erstellen einer Zertifikatsanfrage (CSR)

CAcert.org

- Gehe zur Startseite
- Ausloggen

+ Meine Details

+ E-Mail Konto

+ Client Zertifikate

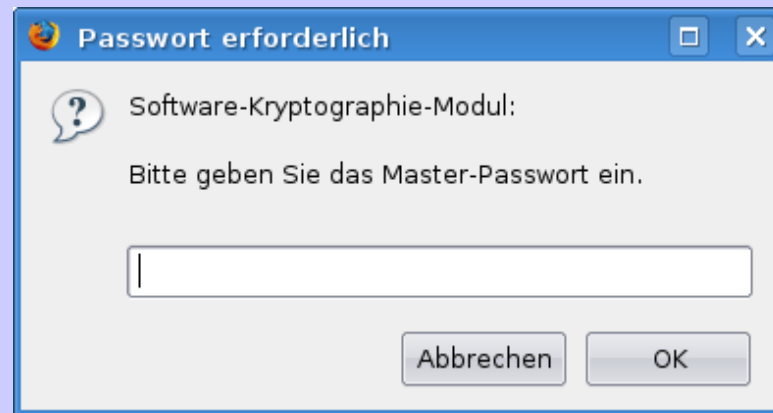
- Neu
- Anzeigen

+ GPG/PGP Schlüssel

+ Domains

Fertig www.cacert.org AS ready

Firefox Master-Passwort zur Aufbewahrung der Schlüssel



Schlüssel wird erzeugt

Zertifikat wird erzeugt



Zertifikat wurde erzeugt



Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php

CAcert

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](#) Ihr Zertifikat zu installieren.

CAcert.org
Gehe zur Startseite
Ausloggen

+ Meine Details

+ E-Mail Konto

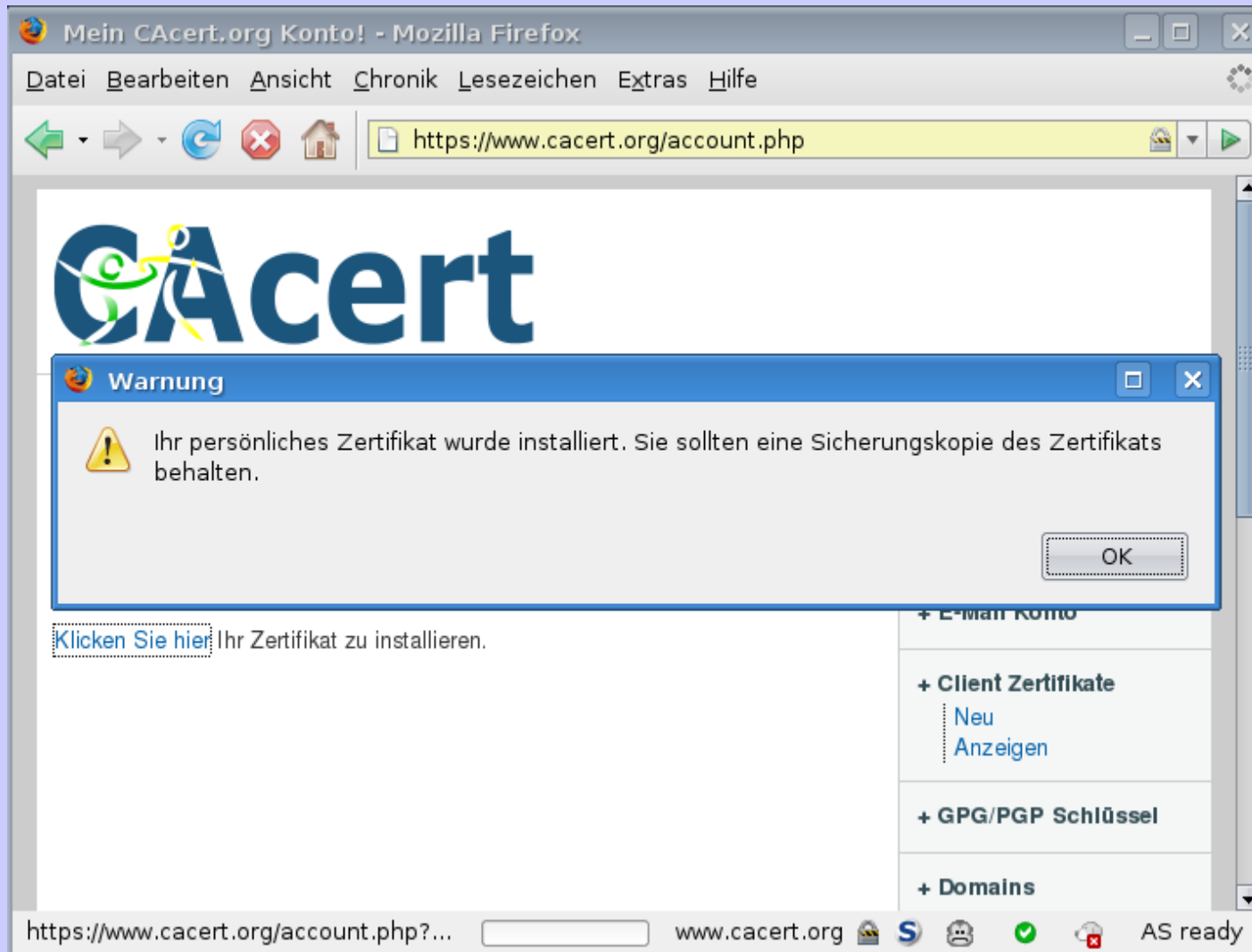
+ Client Zertifikate
Neu
Anzeigen

+ GPG/PGP Schlüssel

+ Domains

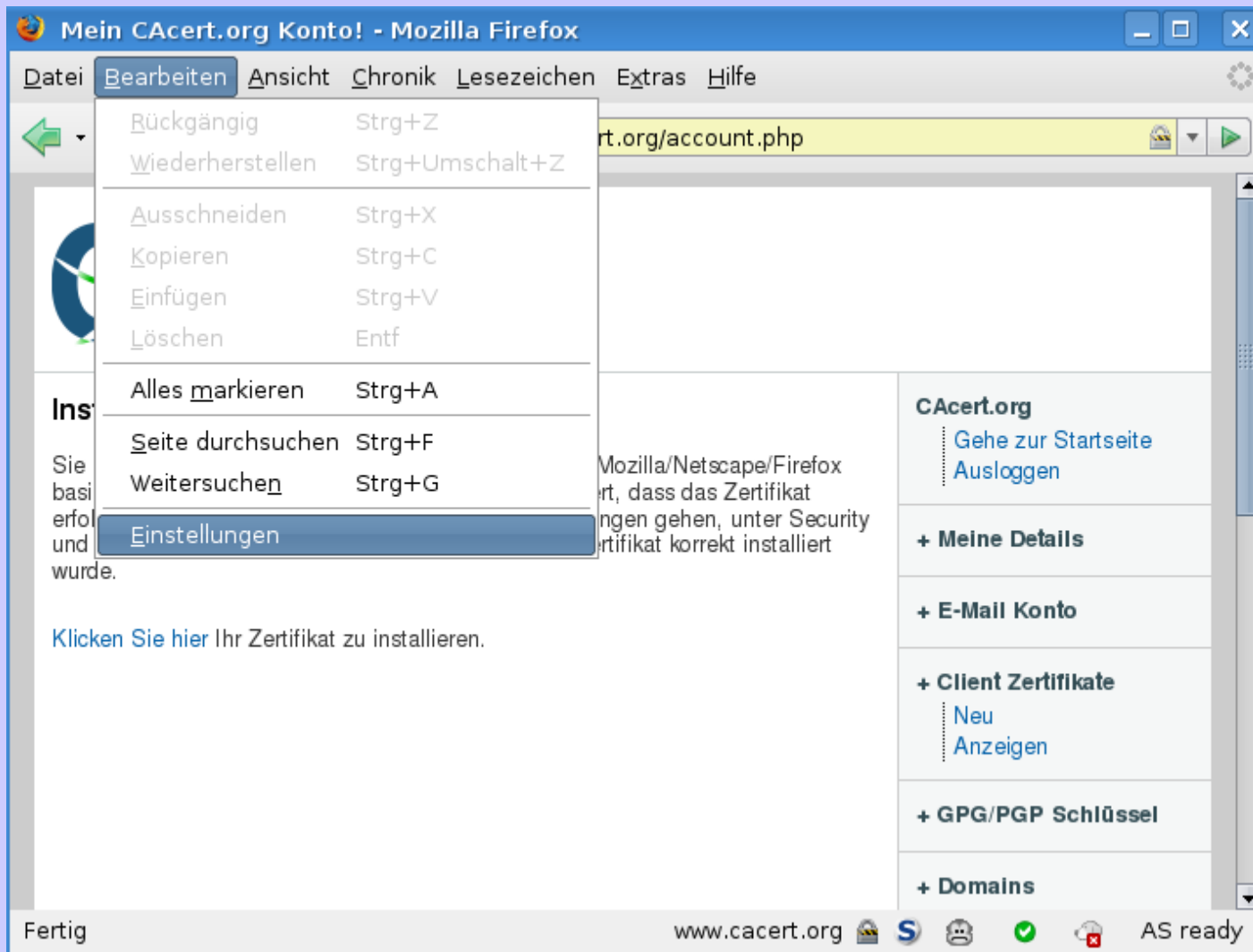
Fertig www.cacert.org AS ready

Zertifikat installiert



The screenshot shows a Mozilla Firefox browser window titled "Mein CAcert.org Konto! - Mozilla Firefox". The address bar displays "https://www.cacert.org/account.php". The main content area shows the CAcert logo and a warning dialog box. The warning dialog box has a blue header with the word "Warnung" and a yellow warning icon. The text inside the dialog reads: "Ihr persönliches Zertifikat wurde installiert. Sie sollten eine Sicherungskopie des Zertifikats behalten." Below the text is an "OK" button. Below the warning dialog, there is a blue link that says "Klicken Sie hier" followed by the text "Ihr Zertifikat zu installieren." On the right side of the page, there is a sidebar with several sections: "+ E-Mail Konto", "+ Client Zertifikate" (with sub-links "Neu" and "Anzeigen"), "+ GPG/PGP Schlüssel", and "+ Domains". The status bar at the bottom shows the address "https://www.cacert.org/account.php?...", the website name "www.cacert.org", and the text "AS ready".

Wo ist das Zertifikat nun?



The screenshot shows a Mozilla Firefox browser window titled "Mein CAcert.org Konto! - Mozilla Firefox". The address bar displays "rt.org/account.php". A context menu is open over the "Bearbeiten" menu item, listing options such as "Rückgängig", "Wiederherstellen", "Ausschneiden", "Kopieren", "Einfügen", "Löschen", "Alles markieren", "Seite durchsuchen", "Weitersuchen", and "Einstellungen". The main content area of the browser displays the CAcert.org account page, which includes a message about certificate installation and a sidebar with navigation links like "Gehe zur Startseite" and "Ausloggen".

Mein CAcert.org Konto! - Mozilla Firefox

rt.org/account.php

Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

- Rückgängig Strg+Z
- Wiederherstellen Strg+Umschalt+Z
- Ausschneiden Strg+X
- Kopieren Strg+C
- Einfügen Strg+V
- Löschen Entf
- Alles markieren Strg+A
- Seite durchsuchen Strg+F
- Weitersuchen Strg+G
- Einstellungen

Ins
Sie basi
erfol
und
wurde.

Klicken Sie hier Ihr Zertifikat zu installieren.

Mozilla/Netscape/Firefox
rt, dass das Zertifikat
ngen gehen, unter Security
rtifikat korrekt installiert

CAcert.org
Gehe zur Startseite
Ausloggen

+ Meine Details

+ E-Mail Konto

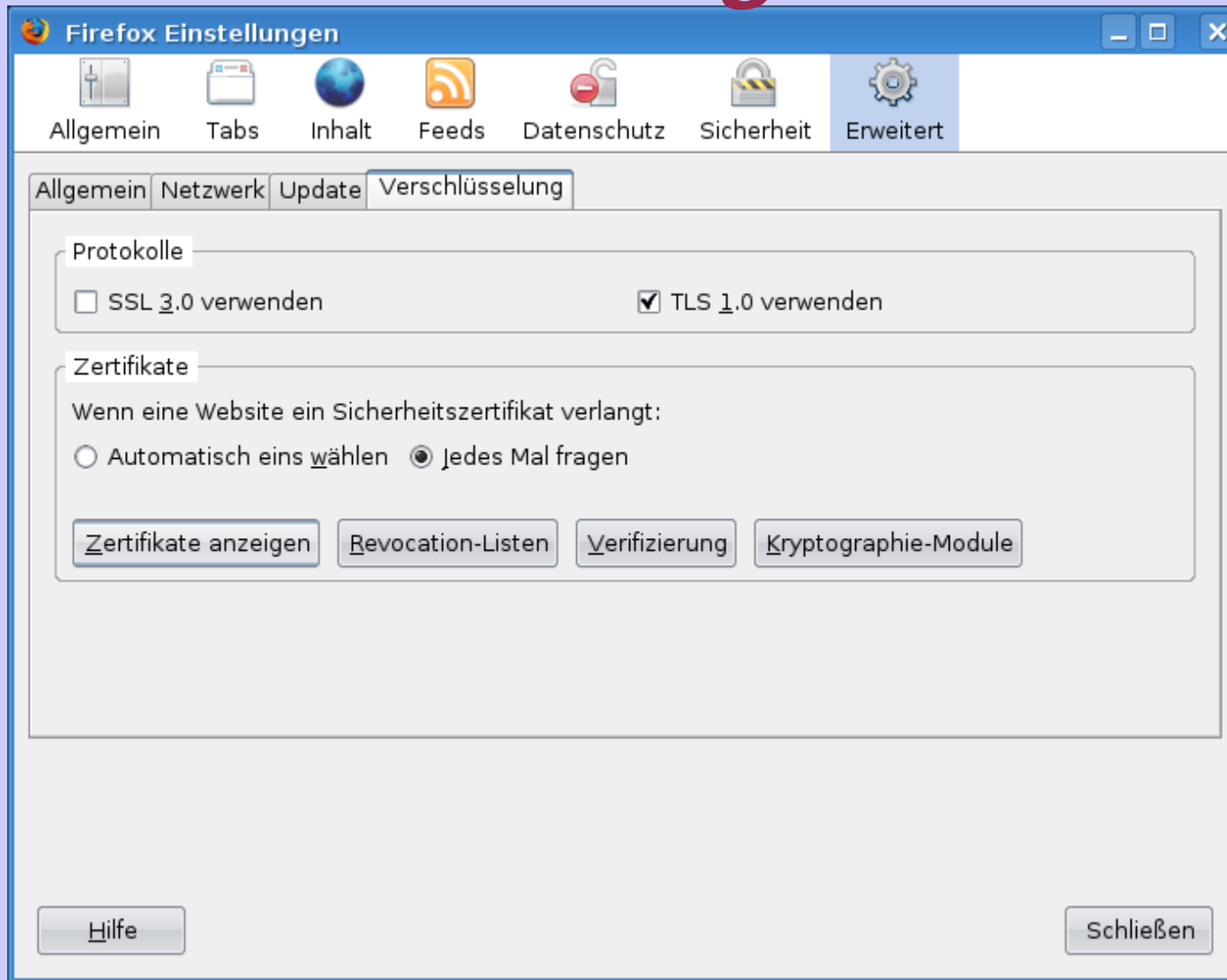
+ Client Zertifikate
Neu
Anzeigen

+ GPG/PGP Schlüssel

+ Domains

Fertig www.cacert.org AS ready

Einstellungen ...



Hier ist das Zertifikat

Zertifikat-Manager

Ihre Zertifikate | Zertifikate anderer Personen | Websites | Zertifizierungsstellen

Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

Zertifikatsname	Kryptograp...	Zwecke	Seriennummer	Herausgegeben...	Läuft ab am	
[-] CAcert Inc.						
[-] Philipp Gühring	Software-Kr...	Client,Server,U...	27:04	09.04.2007	08.04.2009	
[-] Internet Widgits Pty Ltd						
[-] CAcert WoT User	Software-Kr...	<Abgelaufen>	00:E8	13.10.2006	13.10.2007	
[-] CAcert WoT User	Software-Kr...	<Abgelaufen>	00:E4	12.10.2006	12.10.2007	
[-] Root CA						
[-] Philipp Gühring	Software-Kr...	Client,Server,U...	04:CC:50	08.03.2008	08.03.2010	
[-] Test Certificate	Software-Kr...	Client,Server,U...	04:6F:B0	19.12.2007	18.12.2008	
[-] Philipp Gühring	Software-Kr...	Client,Server,U...	04:6F:AC	19.12.2007	18.12.2009	
[-] Test Certificate	Software-Kr...	Client,Server,U...	04:6F:A8	19.12.2007	18.12.2008	
[-] Philipp Gühring	Software-Kr...	Client,Server,U...	04:6A:2C	14.12.2007	13.12.2009	
[-] Philipp Gühring	Software-Kr...	Client,Server,U...	04:03:E2	09.09.2007	08.09.2008	
[-] CAcert WoT User	Software-Kr...	Client,Server,U...	03:DB:CA	30.07.2007	29.07.2009	
[-] Signaturzertifikat für elektronisc...	Software-Kr...	<Abgelaufen>	03:29:30	28.01.2007	28.01.2008	
[-] CAcert WoT User	Software-Kr...	<Abgelaufen>	03:25:8C	24.01.2007	24.01.2008	
[-] Philipp Gühring	Software-Kr...	<Abgelaufen>	03:06:4A	19.12.2006	19.12.2007	
[-] Philipp Gühring	Software-Kr...	<Abgelaufen>	02:FF:98	12.12.2006	12.12.2007	
[-] Philipp Gühring	Software-Kr...	<Abgelaufen>	02:C8:AD	16.10.2006	16.10.2007	
[-] Philipp Gühring	Software-Kr...	<Abgelaufen>	02:A0:CF	01.09.2006	01.09.2007	

Ansicht | Backup | Backup von allen | Importieren | Löschen

OK

Zertifikat und Schlüssel sichern

The screenshot shows the Windows Certificate Manager interface with a 'Dateiname für Backup' dialog box open. The dialog is used to specify the name and location for a backup of certificates and keys.

Dialog: Dateiname für Backup

- Name:** Sicherung
- In Ordner speichern:** backup
- Ordner-Browser:** philipp backup (with 'Ordner anlegen' button)
- Orte:** Suchen, Zuletzt verwendet, philipp, Desktop, Dateisystem
- Buttons:** Hinzufügen, Entfernen, Abbrechen, Speichern
- PKCS12 Dateien:** dropdown menu

Main Window: Zertifikat-Manager

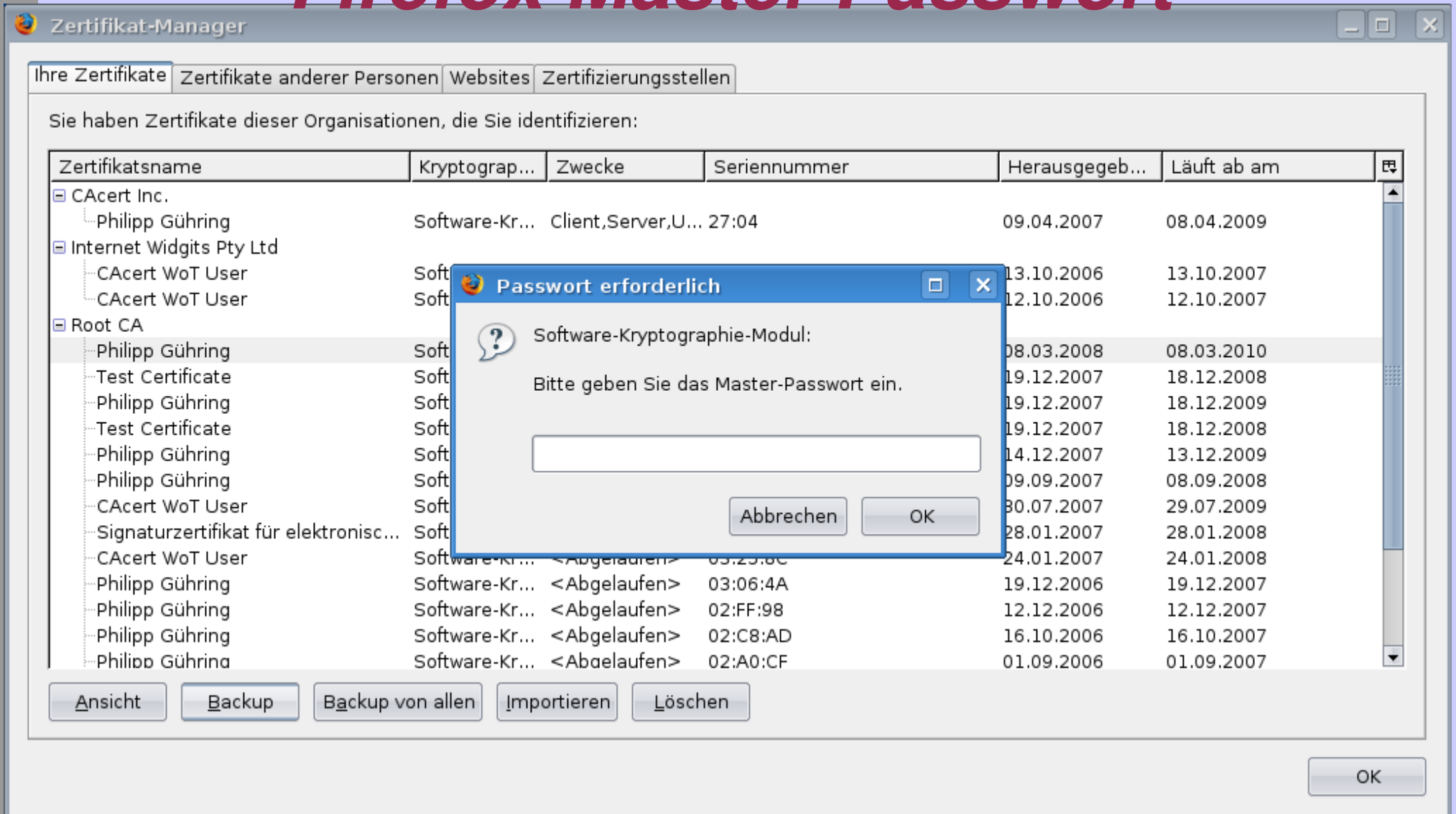
Ihre Zertifikate | Zertifikate

Sie haben Zertifikate d

Zertifikatsname	ft ab am
CAcert Inc.	4.2009
Philipp Gühring	0.2007
Internet Widgits Pty	0.2007
CAcert WoT User	
CAcert WoT User	
Root CA	
Philipp Gühring	3.2010
Test Certificate	2.2008
Philipp Gühring	2.2009
Test Certificate	2.2008
Philipp Gühring	2.2009
Philipp Gühring	9.2008
Philipp Gühring	7.2009
CAcert WoT User	1.2008
Signaturzertifikat	1.2008
CAcert WoT User	2.2007
Philipp Gühring	2.2007
Philipp Gühring	0.2007
Philipp Gühring	9.2007

Ansicht | Back | Hinzufügen | Entfernen | PKCS12 Dateien | Abbrechen | Speichern | OK

Firefox Master Passwort




The screenshot shows the Windows Certificate Manager window. The main window displays a list of certificates under the 'Ihre Zertifikate' tab. A dialog box titled 'Passwort erforderlich' (Password required) is overlaid on the list, asking for the master password for the Software Cryptography Module. The dialog box contains a question mark icon, the text 'Software-Kryptographie-Modul: Bitte geben Sie das Master-Passwort ein.', a text input field, and 'Abbrechen' and 'OK' buttons.

Zertifikatsname	Kryptograp...	Zwecke	Seriennummer	Herausgegeben...	Läuft ab am
CAcert Inc.					
Philipp Gühring	Software-Kr...	Client,Server,U...	27:04	09.04.2007	08.04.2009
Internet Widgits Pty Ltd					
CAcert WoT User	Soft			13.10.2006	13.10.2007
CAcert WoT User	Soft			12.10.2006	12.10.2007
Root CA					
Philipp Gühring	Soft			08.03.2008	08.03.2010
Test Certificate	Soft			19.12.2007	18.12.2008
Philipp Gühring	Soft			19.12.2007	18.12.2009
Test Certificate	Soft			19.12.2007	18.12.2008
Philipp Gühring	Soft			14.12.2007	13.12.2009
Philipp Gühring	Soft			09.09.2007	08.09.2008
CAcert WoT User	Soft			30.07.2007	29.07.2009
Signaturzertifikat für elektronisc...	Soft			28.01.2007	28.01.2008
CAcert WoT User	Software-Kr...	<Abgelaufen>	03:25:8C	24.01.2007	24.01.2008
Philipp Gühring	Software-Kr...	<Abgelaufen>	03:06:4A	19.12.2006	19.12.2007
Philipp Gühring	Software-Kr...	<Abgelaufen>	02:FF:98	12.12.2006	12.12.2007
Philipp Gühring	Software-Kr...	<Abgelaufen>	02:C8:AD	16.10.2006	16.10.2007
Philipp Gühring	Software-Kr...	<Abgelaufen>	02:A0:CF	01.09.2006	01.09.2007

Buttons at the bottom of the Certificate Manager window: Ansicht, Backup, Backup von allen, Importieren, Löschen, OK.

Das Passwort für die Sicherung wählen

 Wählen Sie ein Zertifikats-Backup-Passwort

Das Zertifikats-Backup-Passwort, das Sie hier festlegen, schützt die Backup-Datei, die Sie jetzt erstellen möchten. Sie müssen dieses Passwort festlegen, um mit dem Backup fortzufahren.

Zertifikats-Backup-Passwort:

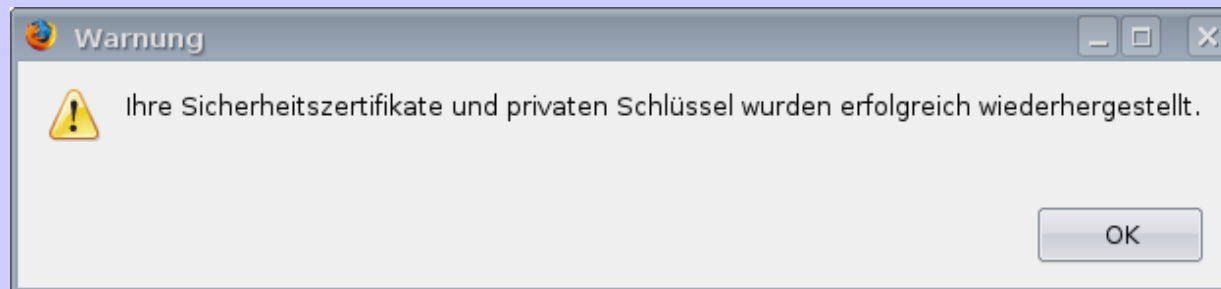
Zertifikats-Backup-Passwort (nochmals):

Wichtig: Wenn Sie Ihr Zertifikats-Backup-Passwort vergessen, können Sie dieses Backup später nicht wiederherstellen. Bitte schreiben Sie es an einem sicheren Platz nieder.

Passwort-Qualitätsmessung

Abbrechen OK

***Der private Schlüssel wurde
in der Datei „Sicherung.p12“
gesichert.***



Web-Login mit Zertifikat



Willkommen bei CAcert.org - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/index.php

CAcert

Einleitung

Es hat lange gedauert, aber das Warten hat sich gelohnt! Endlich bekommt man Sicherheit zum richtigen Preis... Kostenlos!

Jahrelang musste jeder im Internet hohe Gebühren für Sicherheit bezahlen, die in Wirklichkeit gar nicht so teuer sein müsste und schon gar nicht sein sollte.

Die primären Ziele sind:

- Aufnahme des CAcert Zertifikats in die wichtigsten Browser!
- Einen Vertrauens-Mechanismus bereitzustellen, der die Sicherheitsanforderungen von Verschlüsselung erfüllt.

For general documentation and help please see our [Wiki Dokumentation](#) site.

[Aktuelle Nachrichten](#) - [[Weitere Nachrichten](#)]

Bei CAcert.org

- [Mitmachen](#)
- [Community Agreement](#)
- [Root-Zertifikat](#)

Mein Konto

- [Passwort Login](#)
- [Passwort Vergessen](#)
- [Net Cafe Login](#)
- [Zertifikats-LOGIN](#)

+ Über CAcert.org

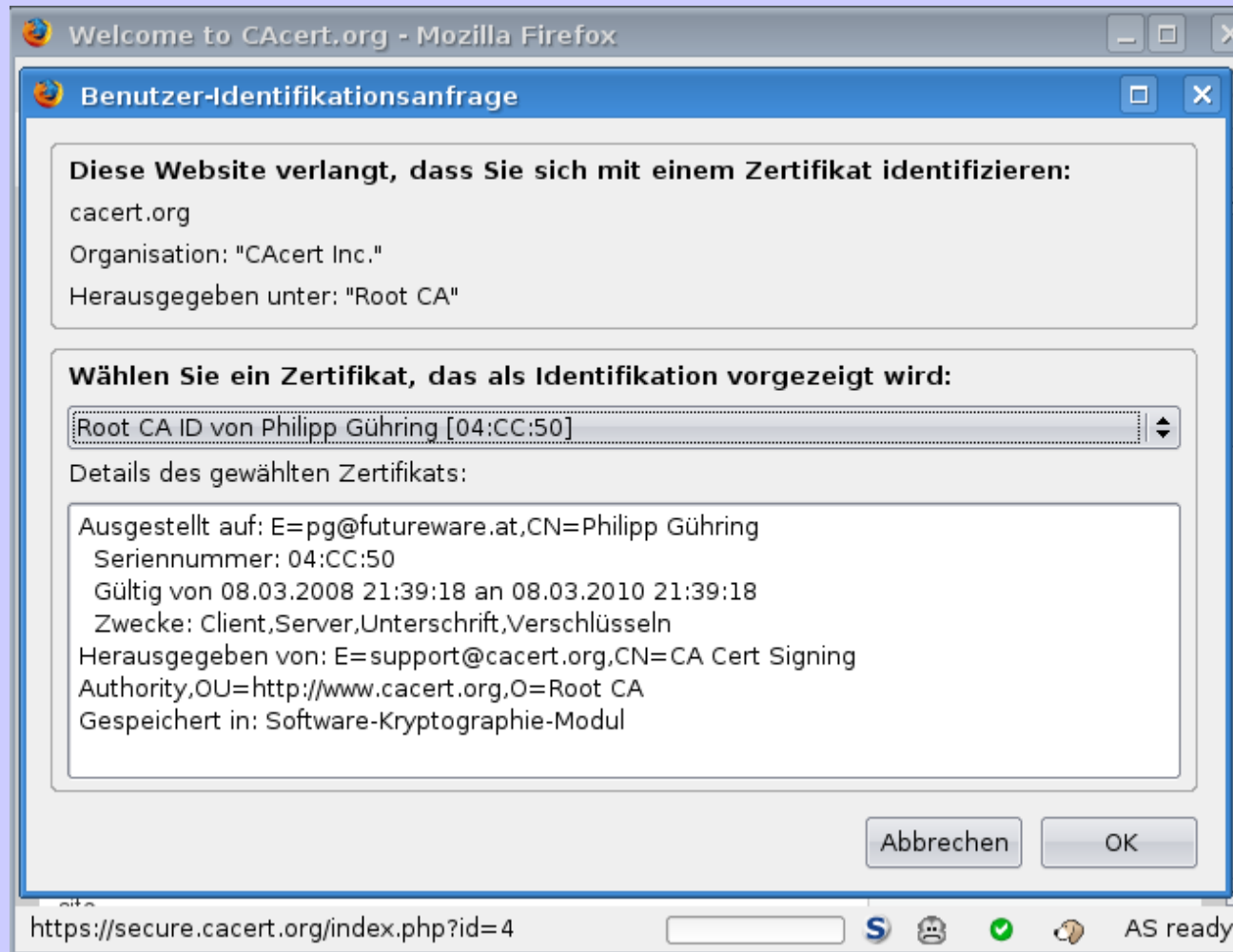
+ Übersetzungen

Werbung

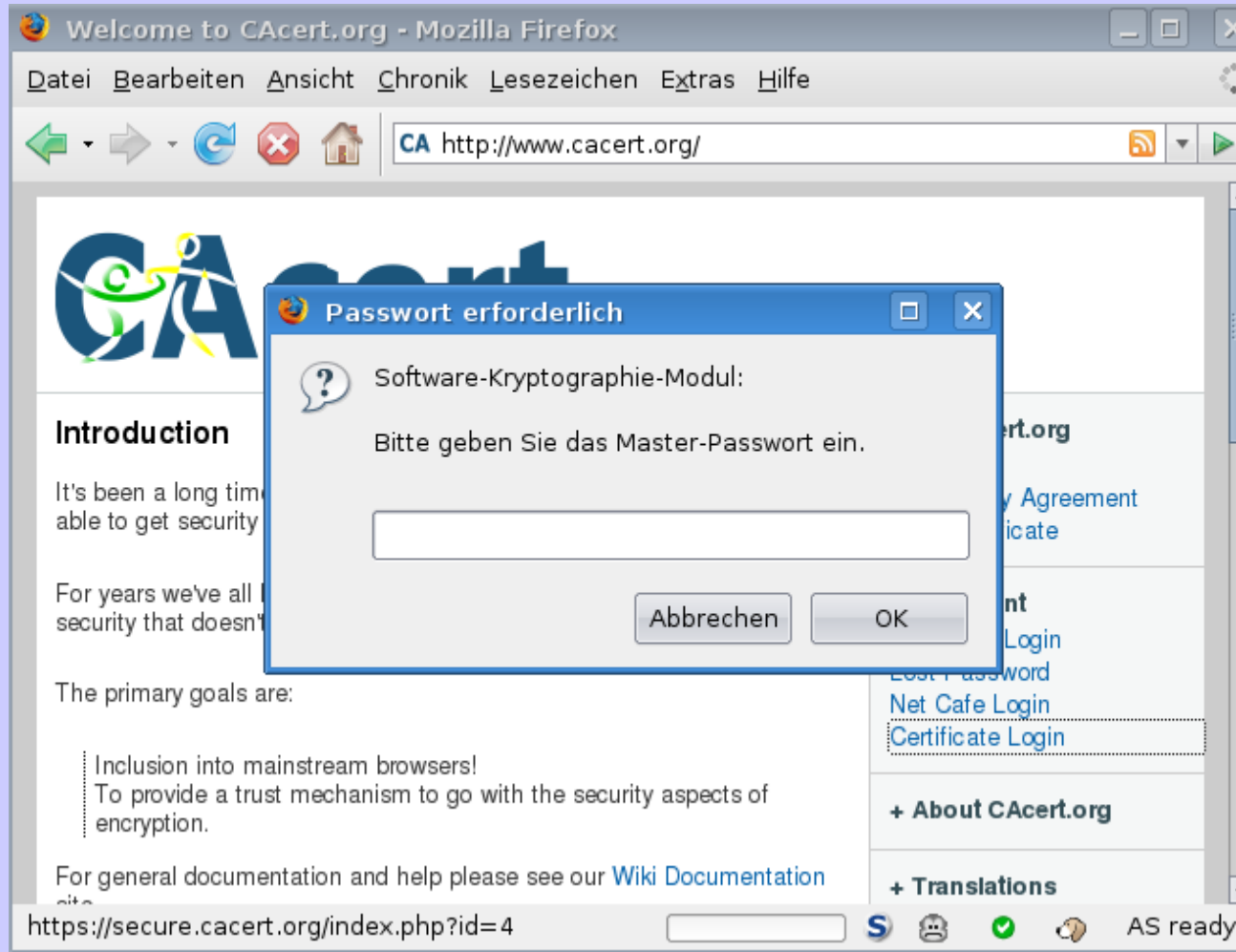
https://secure.cacert.org/index.php?id=4

www.cacert.org AS ready

Auswahl des Zertifikats



Firefox Master-Passwort





Bin drin!

The screenshot shows a Mozilla Firefox browser window titled "Mein CAcert.org Konto! - Mozilla Firefox". The address bar displays "https://secure.cacert.org/account.php". The main content area features the CAcert logo and a "Mein Konto" section with a welcome message and navigation links. A sidebar on the right contains links for "Gehe zur Startseite" and "Ausloggen", along with expandable sections for "Meine Details", "E-Mail Konto", "Client Zertifikate", "GPG/PGP Schlüssel", and "Domains". The status bar at the bottom shows "Fertig" and "AS ready".

Mein Konto

Willkommen im Benutzerbereich der Webseite. Weiter unten finden Sie eine Beschreibung der einzelnen Bereiche der Seite und was Sie dort machen können.

CAcert.org

Wenn Sie Neuigkeiten sehen oder die Sprache ändern wollen, können Sie auf 'Abmelden' oder 'Startseite' klicken. 'Startseite' meldet Sie nicht vom System ab, es bringt Sie nur auf die Startseite. 'Abmelden' beendet Ihre Sitzung und Sie müssen sich erneut einloggen, wenn Sie auf CAcert.org weiterarbeiten wollen.

Meine Details

CAcert.org

- [Gehe zur Startseite](#)
- [Ausloggen](#)

+ **Meine Details**

+ **E-Mail Konto**

+ **Client Zertifikate**

+ **GPG/PGP Schlüssel**

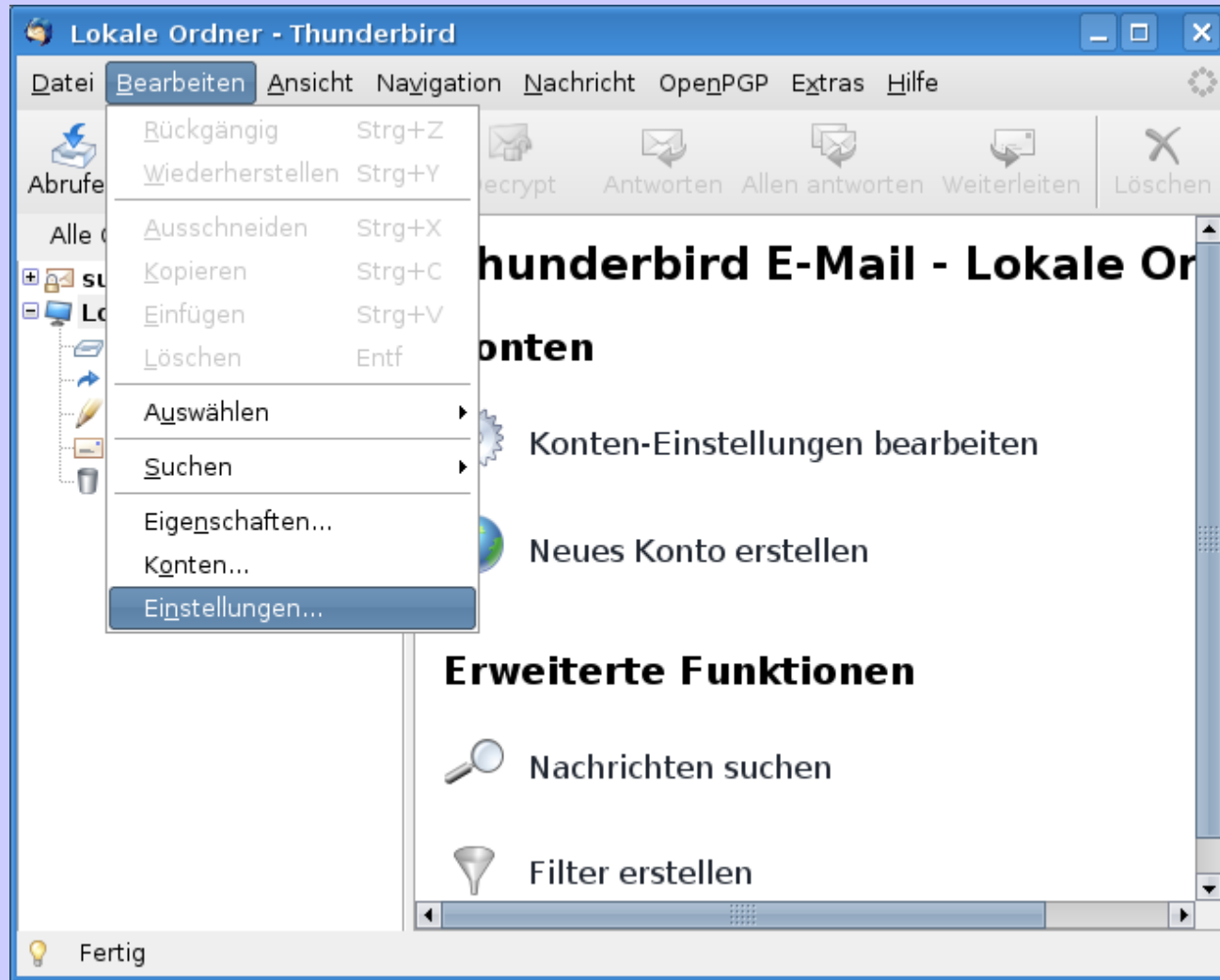
+ **Domains**

Fertig secure.cacert.org AS ready

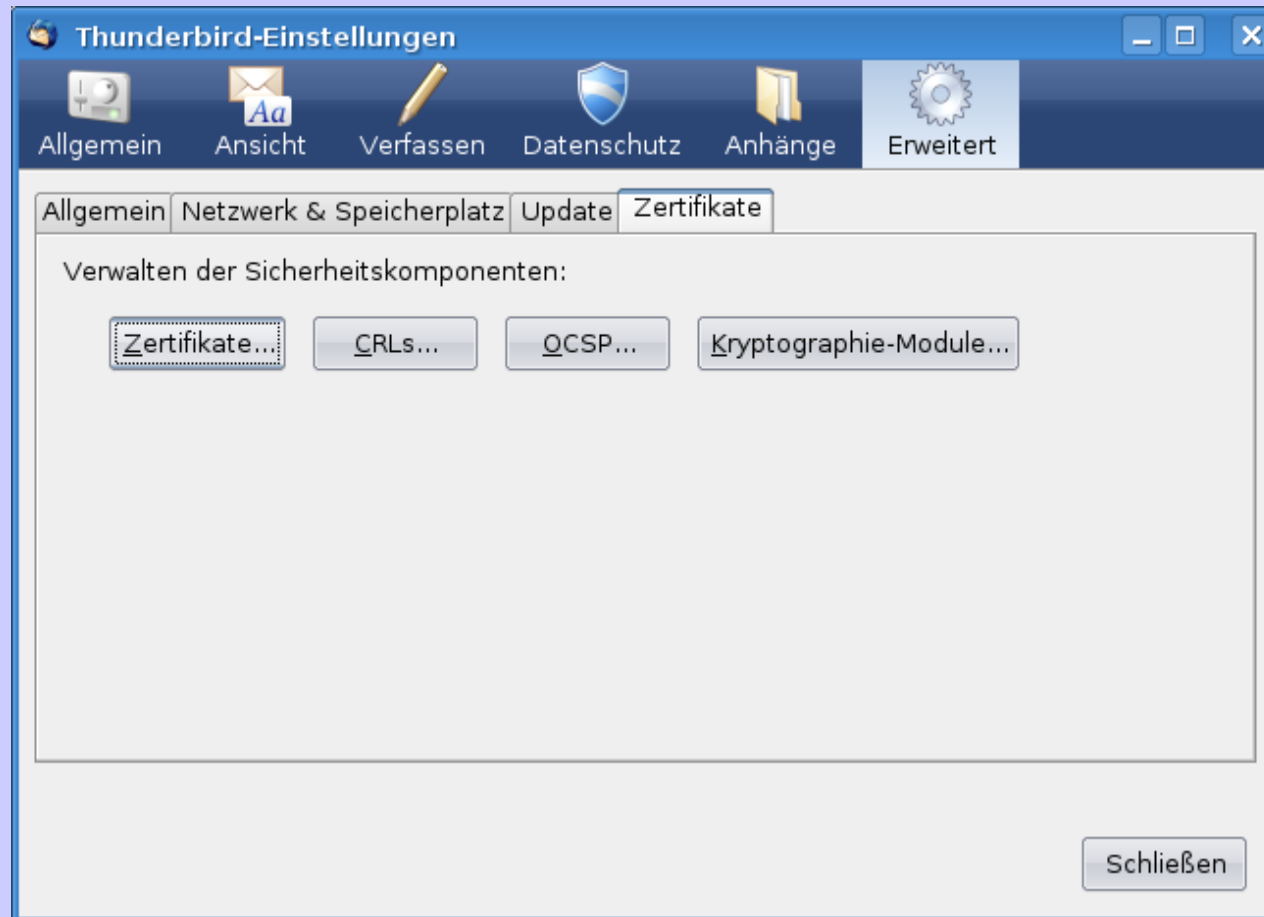
EMail

Thunderbird
Zertifikat importieren
Zertifikat verwenden

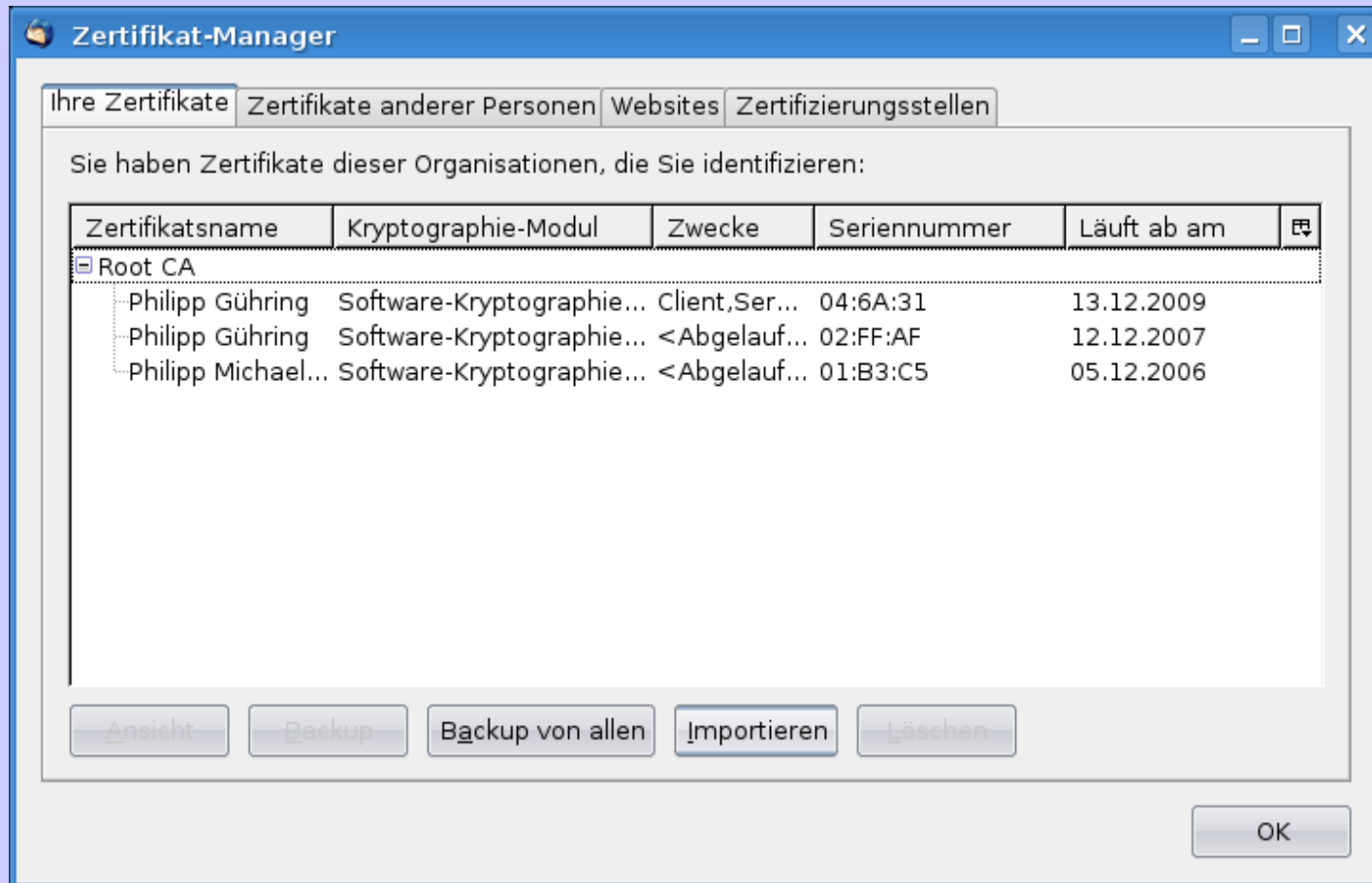
Thunderbird Zertifikat importieren



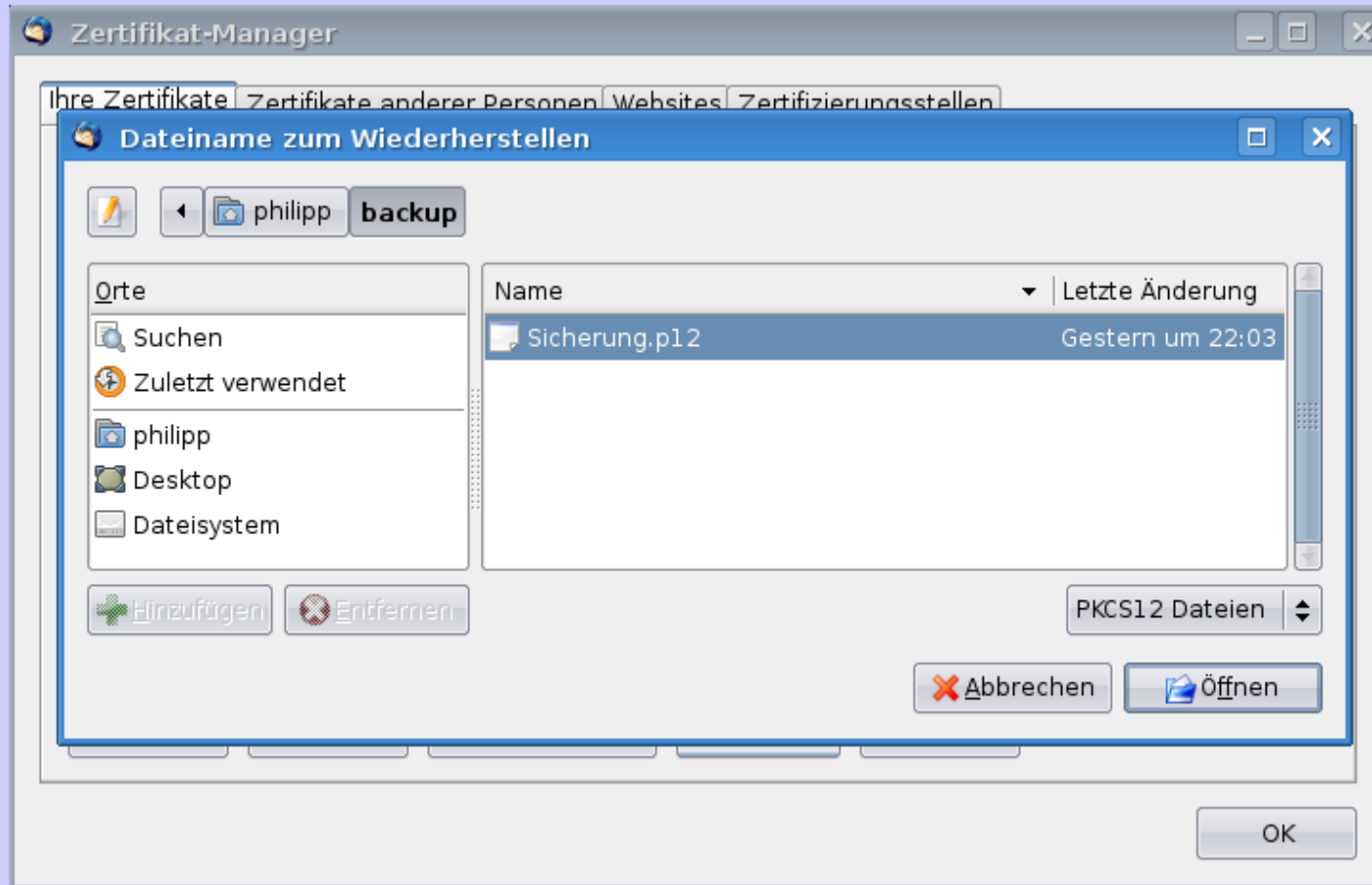
Zertifikate...



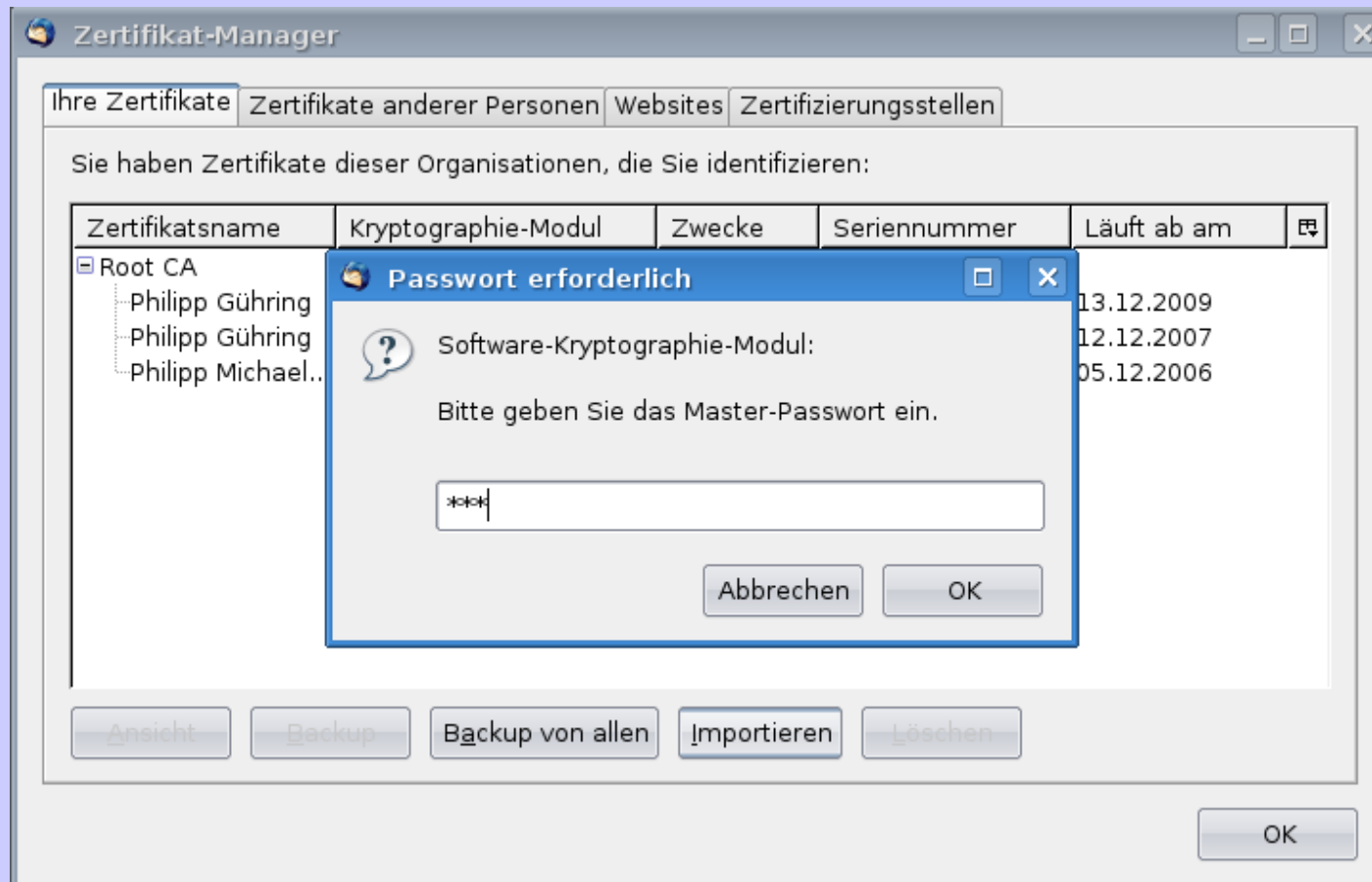
Importieren...



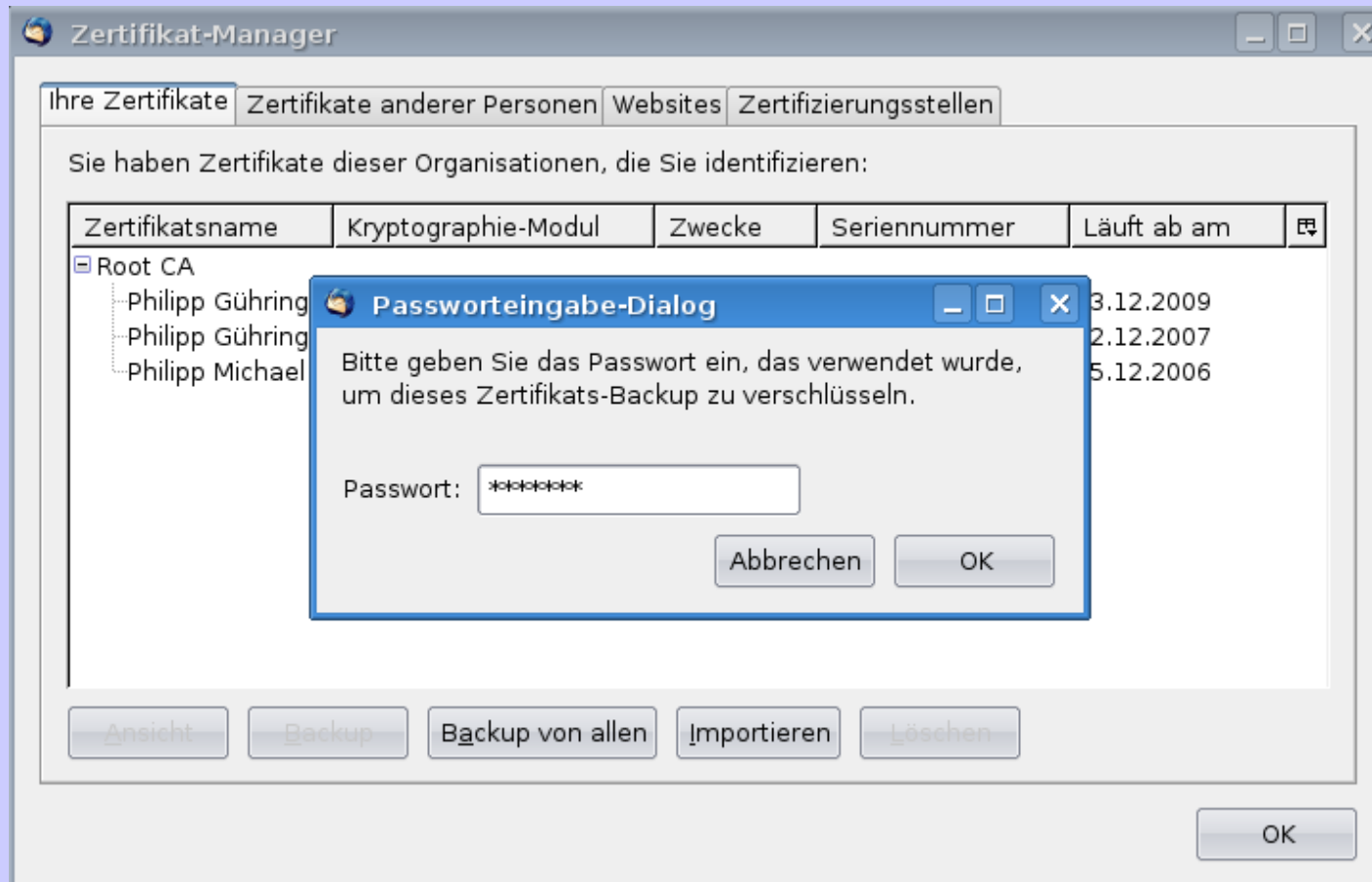
Datei auswählen



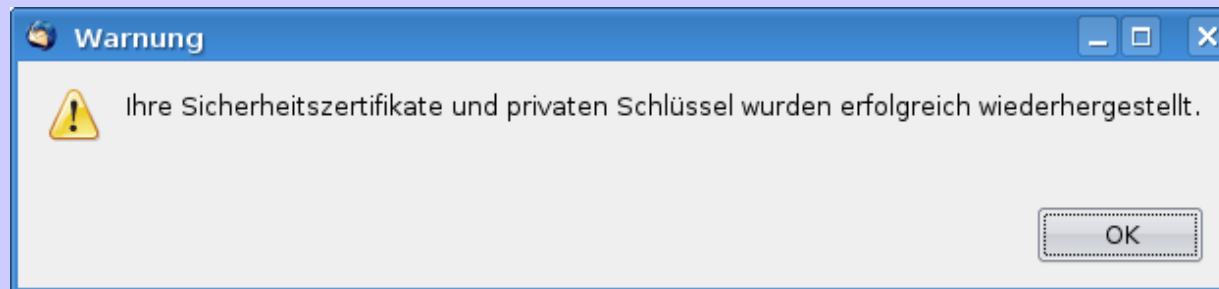
Thunderbird Master Passwort



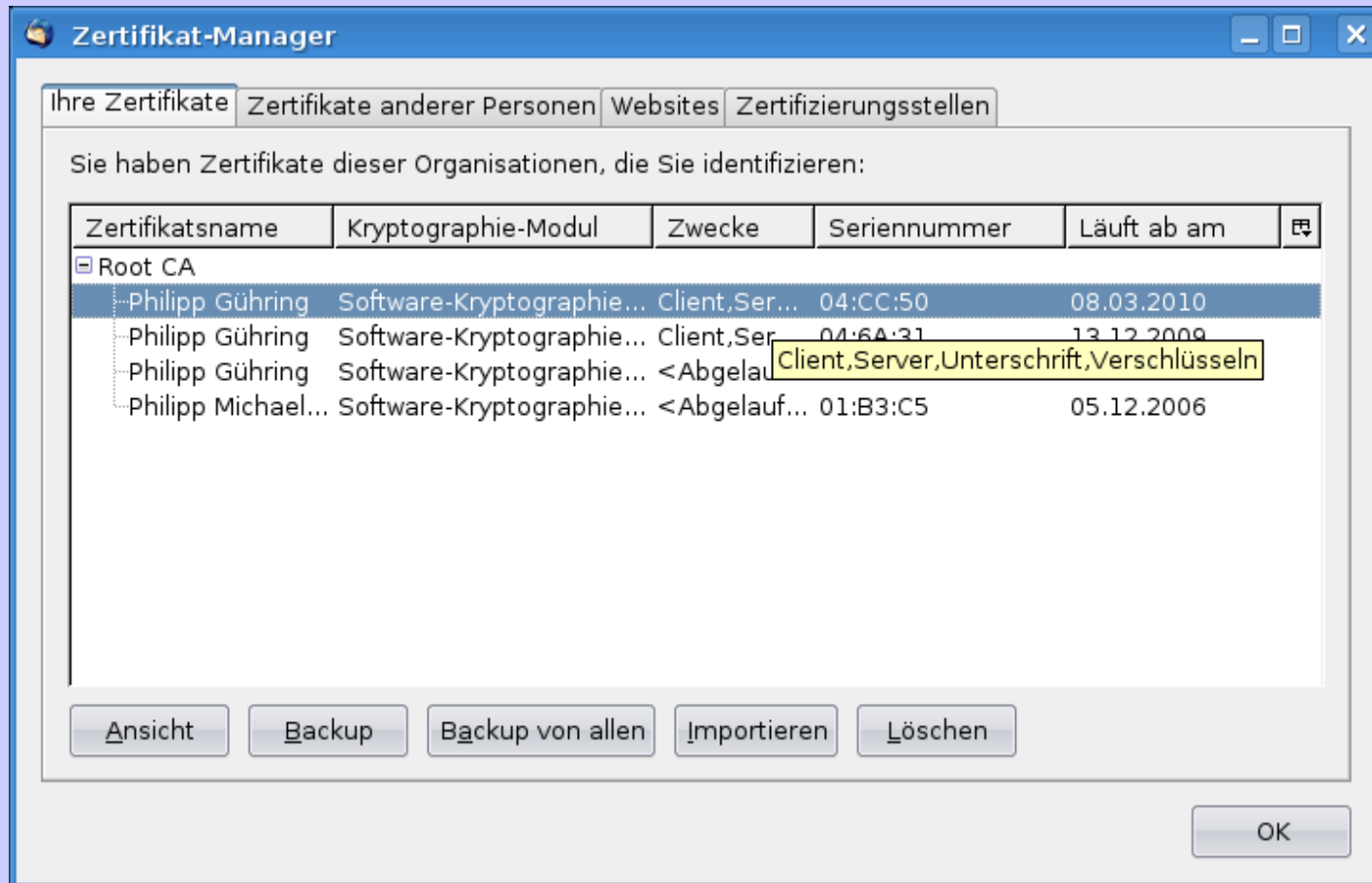
Passwort für das Zertifikat



Import erfolgreich



Da ist es



Zertifikat Detailansicht

Zertifikat-Ansicht: "Philipp GÄ¼hring"

Allgemein Details

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- SSL-Client-Zertifikat
- SSL-Server-Zertifikat
- E-Mail-Unterzeichner-Zertifikat
- E-Mail-Empfänger-Zertifikat

Herausgegeben für

Allgemeiner Name (CN)	Philipp Gühring
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	04:CC:50

Herausgegeben von

Allgemeiner Name (CN)	CA Cert Signing Authority
Organisation (O)	Root CA
Organisationseinheit (OU)	http://www.cacert.org

Validität

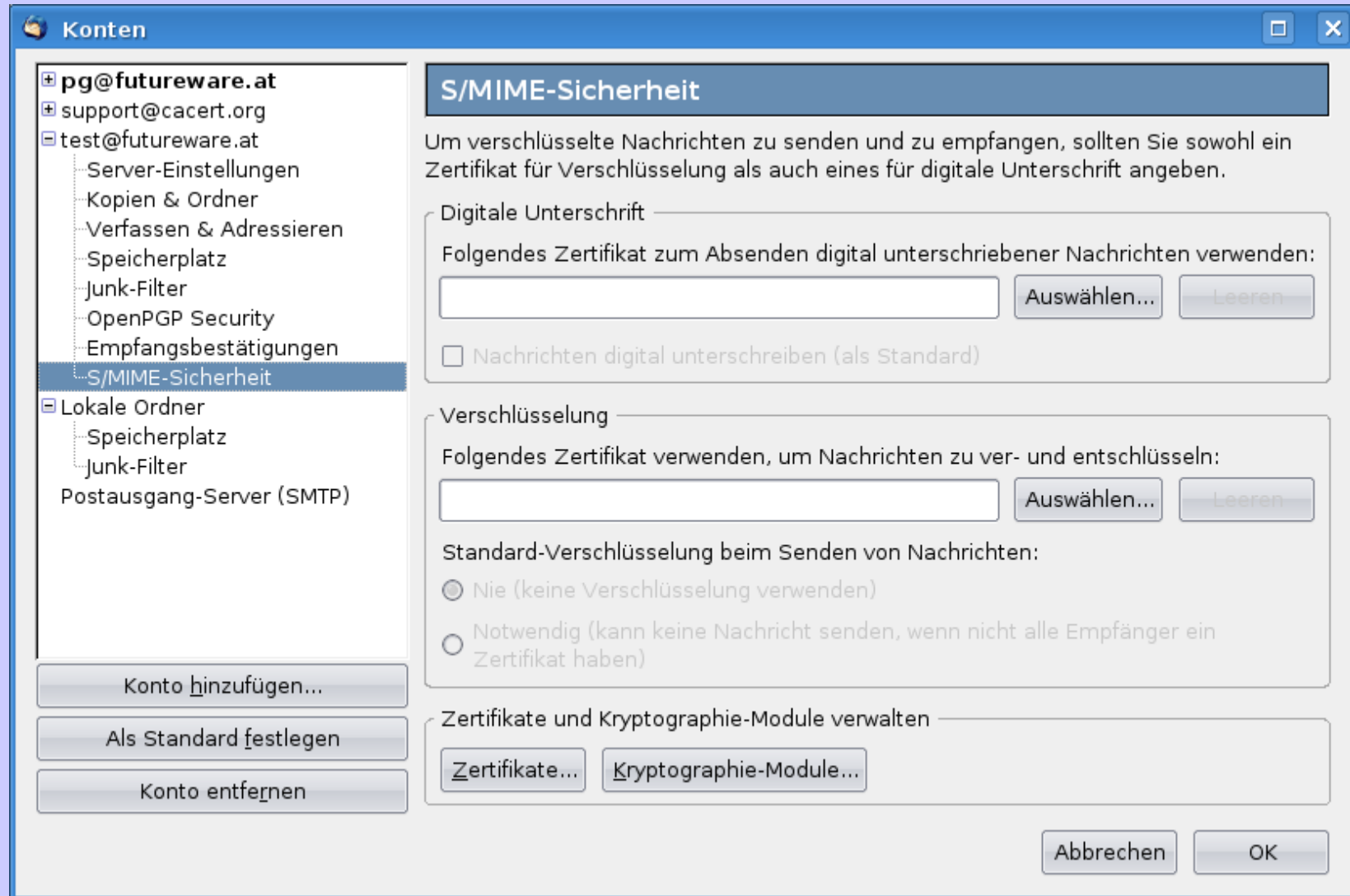
Herausgegeben am	08.03.2008
Läuft ab am	08.03.2010

Fingerabdrücke

SHA1-Fingerprint	B4:21:D3:8D:5F:B0:47:FB:13:6C:C3:33:E1:FA:C7:2D:8A:DD:D6:66
MD5-Fingerprint	3C:8A:EE:0E:84:FC:91:9D:AB:A7:38:EA:2C:5E:81:62

Schließen

Email-Konten Einstellung



Konten

- pg@futureware.at
 - support@cacert.org
 - test@futureware.at
 - Server-Einstellungen
 - Kopien & Ordner
 - Verfassen & Adressieren
 - Speicherplatz
 - Junk-Filter
 - OpenPGP Security
 - Empfangsbestätigungen
 - S/MIME-Sicherheit**
 - Lokale Ordner
 - Speicherplatz
 - Junk-Filter
 - Postausgang-Server (SMTP)

Konto hinzufügen...

Als Standard festlegen

Konto entfernen

S/MIME-Sicherheit

Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.

Digitale Unterschrift

Folgendes Zertifikat zum Absenden digital unterschriebener Nachrichten verwenden:

Nachrichten digital unterschreiben (als Standard)

Verschlüsselung

Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:

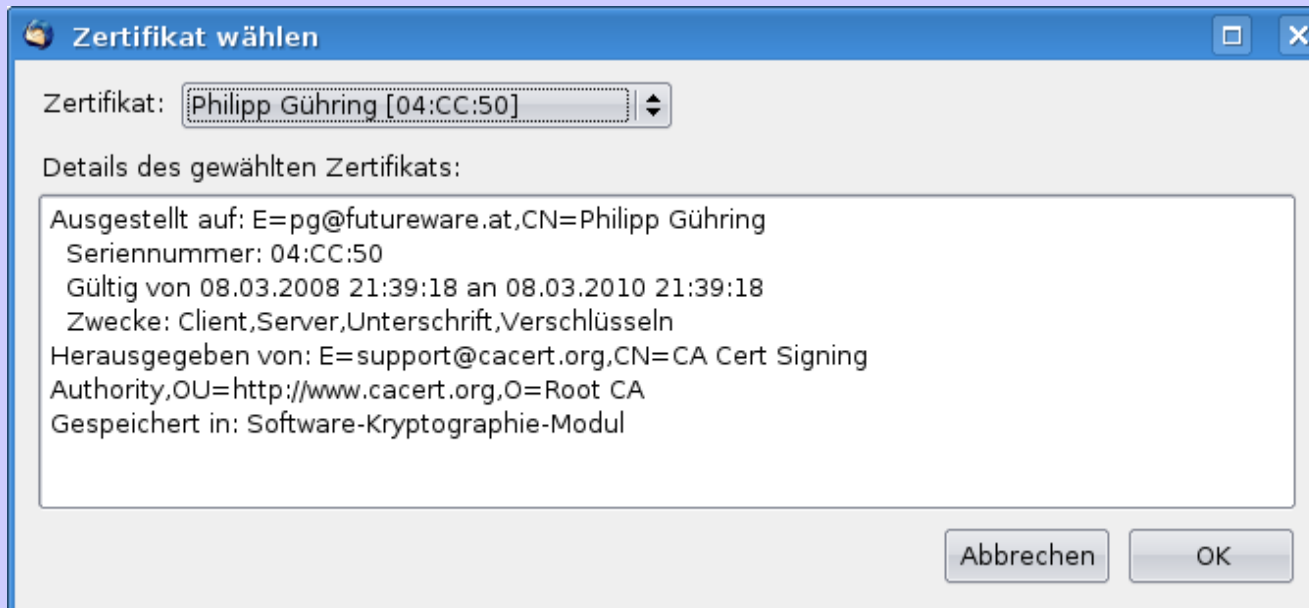
Standard-Verschlüsselung beim Senden von Nachrichten:

Nie (keine Verschlüsselung verwenden)

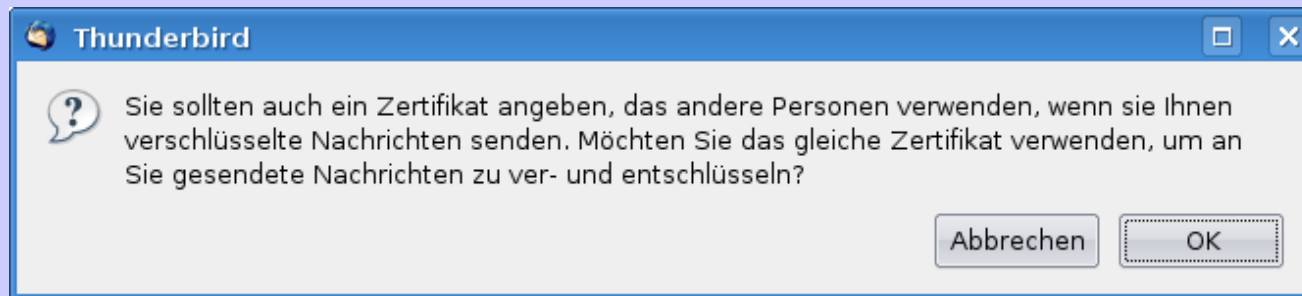
Notwendig (kann keine Nachricht senden, wenn nicht alle Empfänger ein Zertifikat haben)

Zertifikate und Kryptographie-Module verwalten

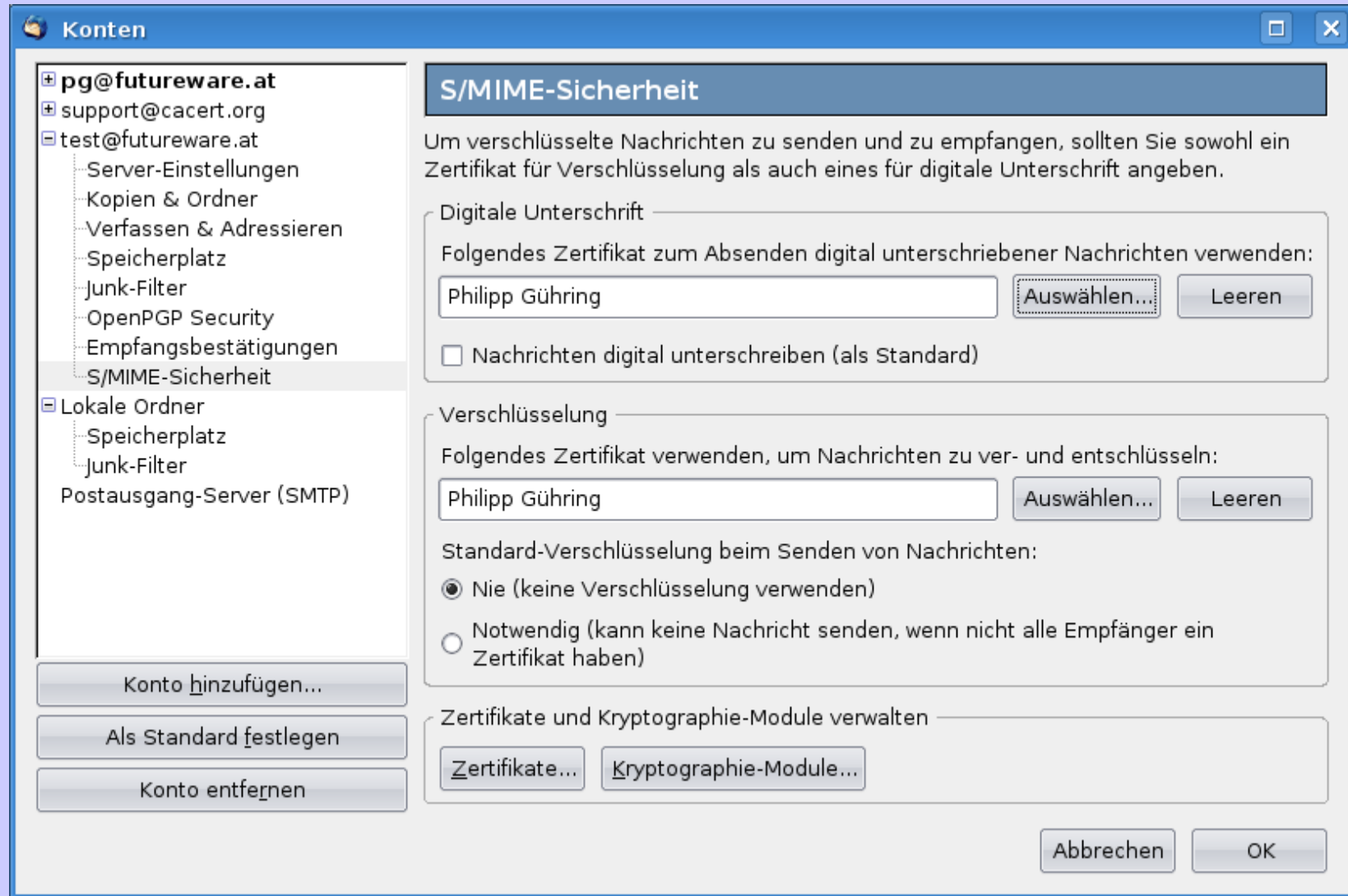
Auswahl des Zertifikats



Übernahme



Zertifikat ist zugewiesen



Konten

- pg@futureware.at
 - support@cacert.org
 - test@futureware.at
 - Server-Einstellungen
 - Kopien & Ordner
 - Verfassen & Adressieren
 - Speicherplatz
 - Junk-Filter
 - OpenPGP Security
 - Empfangsbestätigungen
 - S/MIME-Sicherheit
 - Lokale Ordner
 - Speicherplatz
 - Junk-Filter
 - Postausgang-Server (SMTP)

Konto hinzufügen...

Als Standard festlegen

Konto entfernen

S/MIME-Sicherheit

Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.

Digitale Unterschrift

Folgendes Zertifikat zum Absenden digital unterschriebener Nachrichten verwenden:

Philipp Gühring

Nachrichten digital unterschreiben (als Standard)

Verschlüsselung

Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:

Philipp Gühring

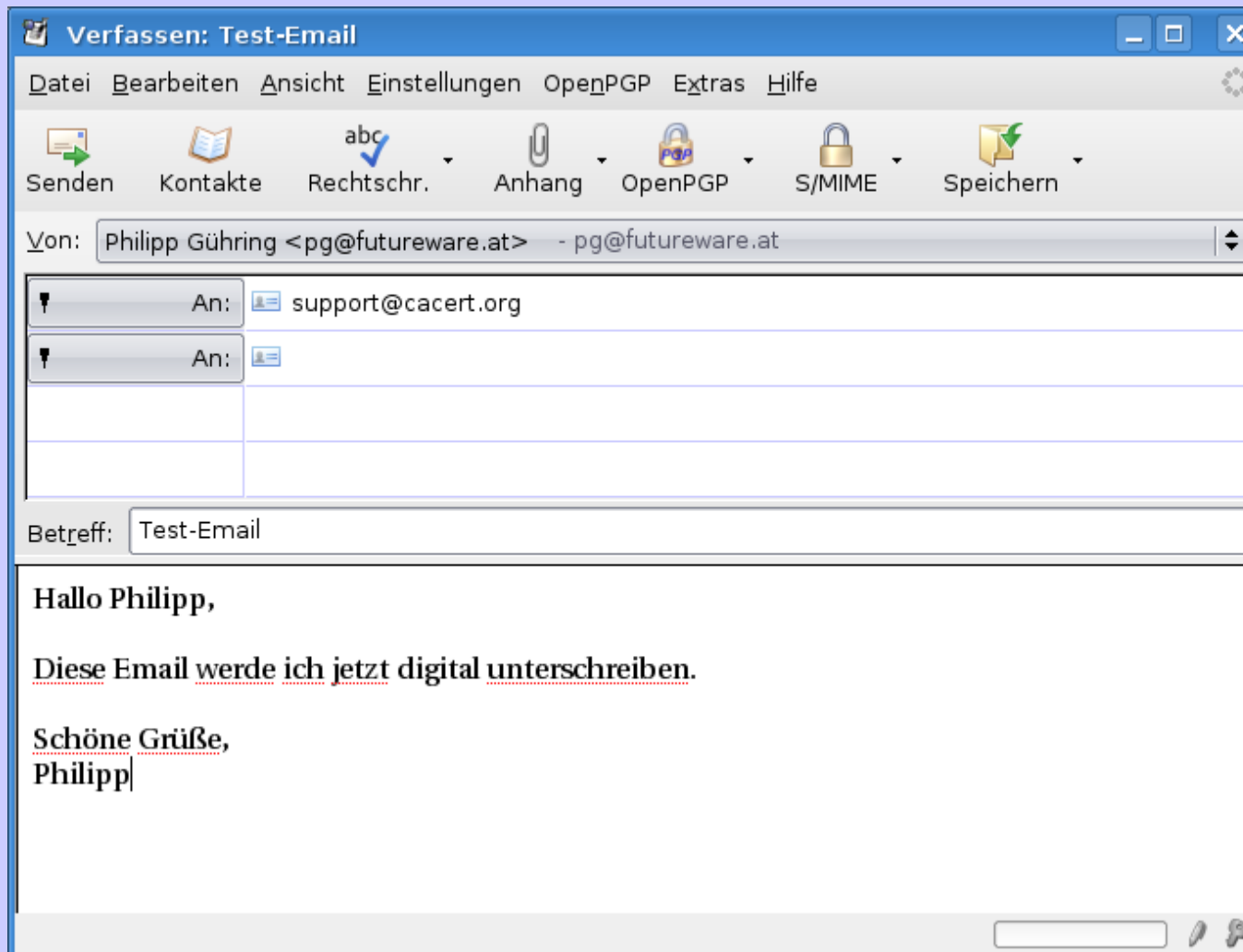
Standard-Verschlüsselung beim Senden von Nachrichten:

Nie (keine Verschlüsselung verwenden)

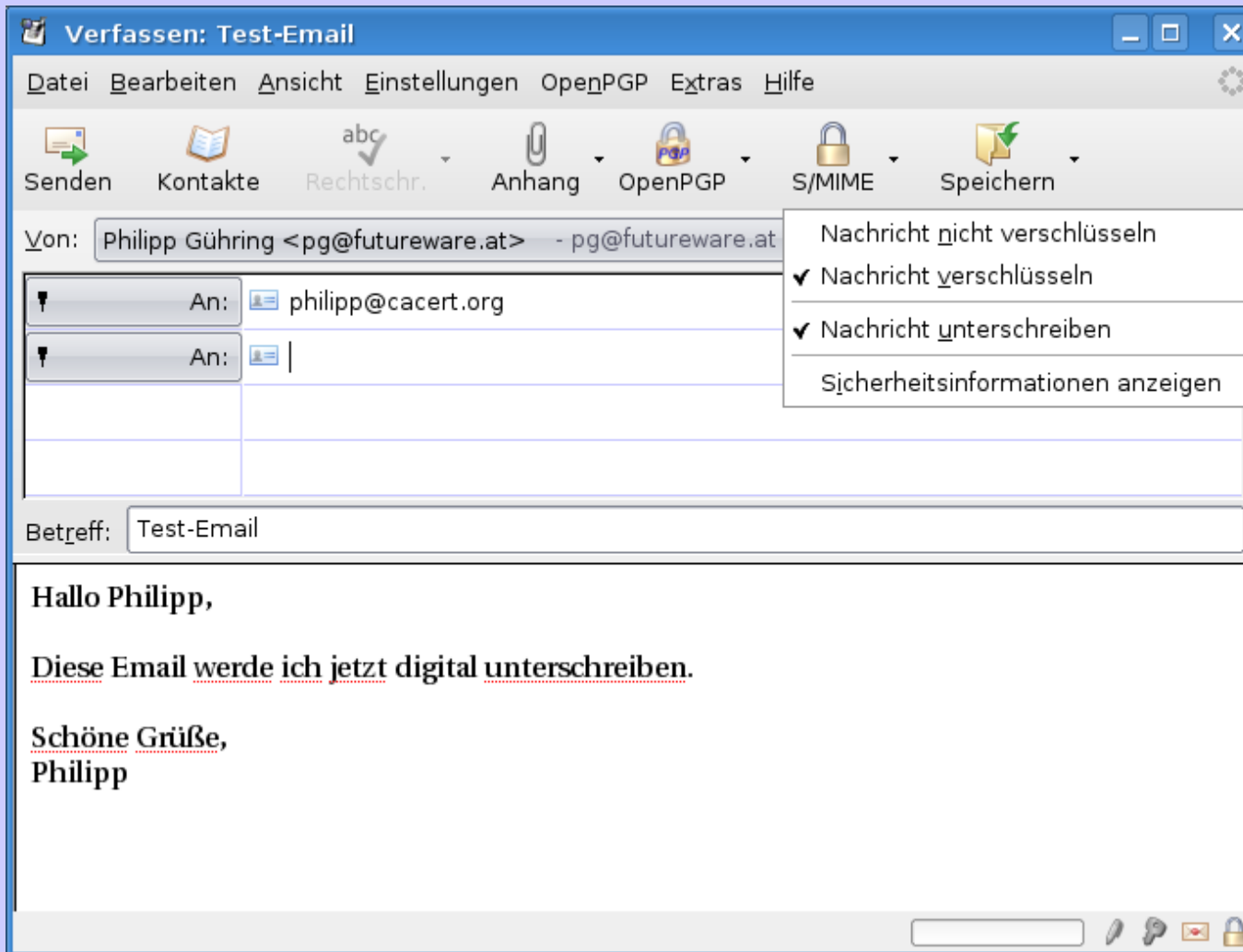
Notwendig (kann keine Nachricht senden, wenn nicht alle Empfänger ein Zertifikat haben)

Zertifikate und Kryptographie-Module verwalten

Email schreiben



Email unterschreiben und verschl.



Sind die Zertifikate aller Empfänger vorhanden?

Nachrichten-Sicherheit

Bitte beachten Sie: Betreff-Zeilen von Nachrichten werden nie verschlüsselt.

Die Inhalte Ihrer Nachricht werden wie folgt gesendet:

Digital unterschrieben: ja
Verschlüsselt: ja

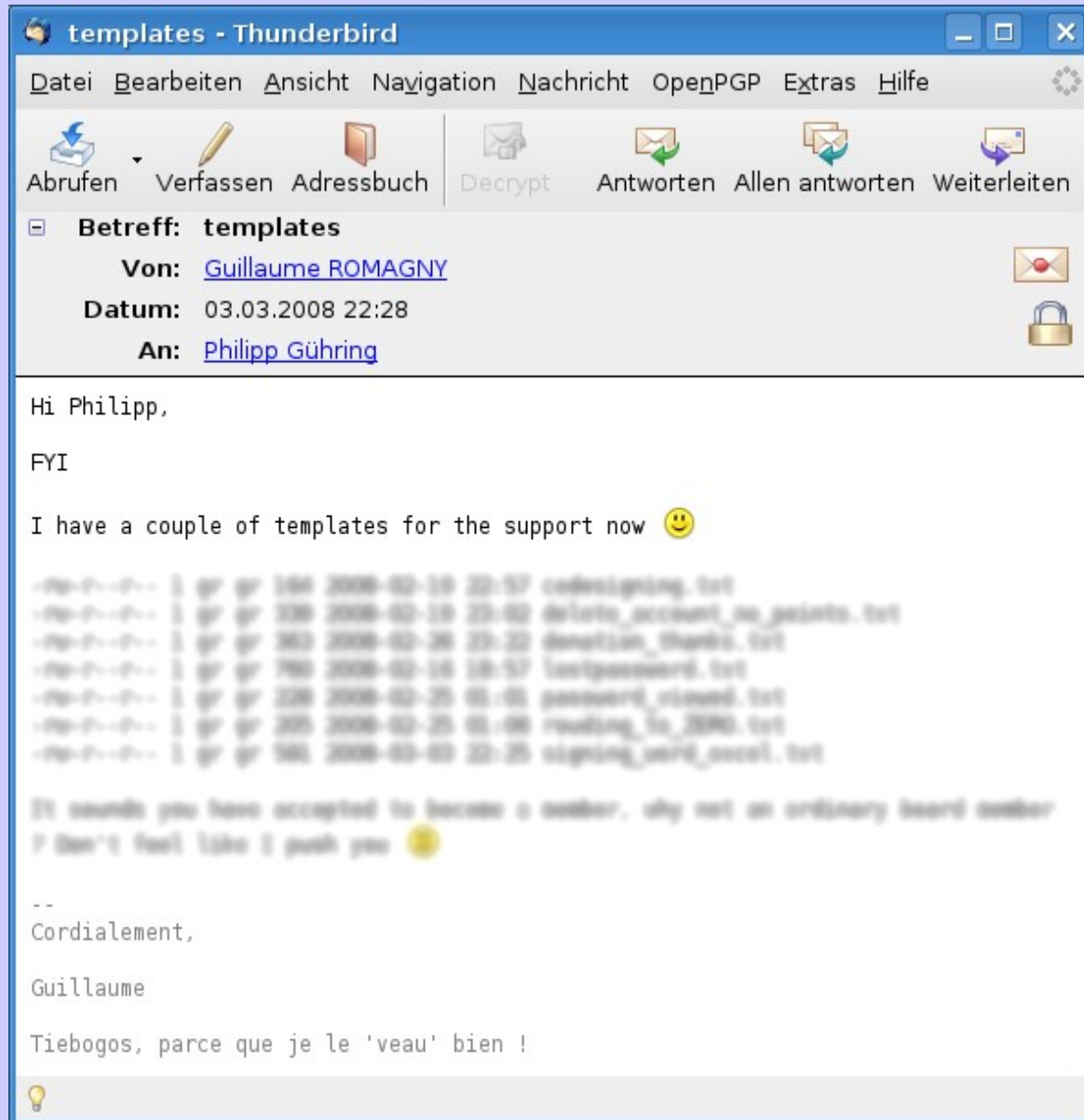
Zertifikate:

Empfänger:	Status:	Herausgegeben:	Läuft ab:
philipp@cacert.org	Gültig	14.12.2007	13.12.2009

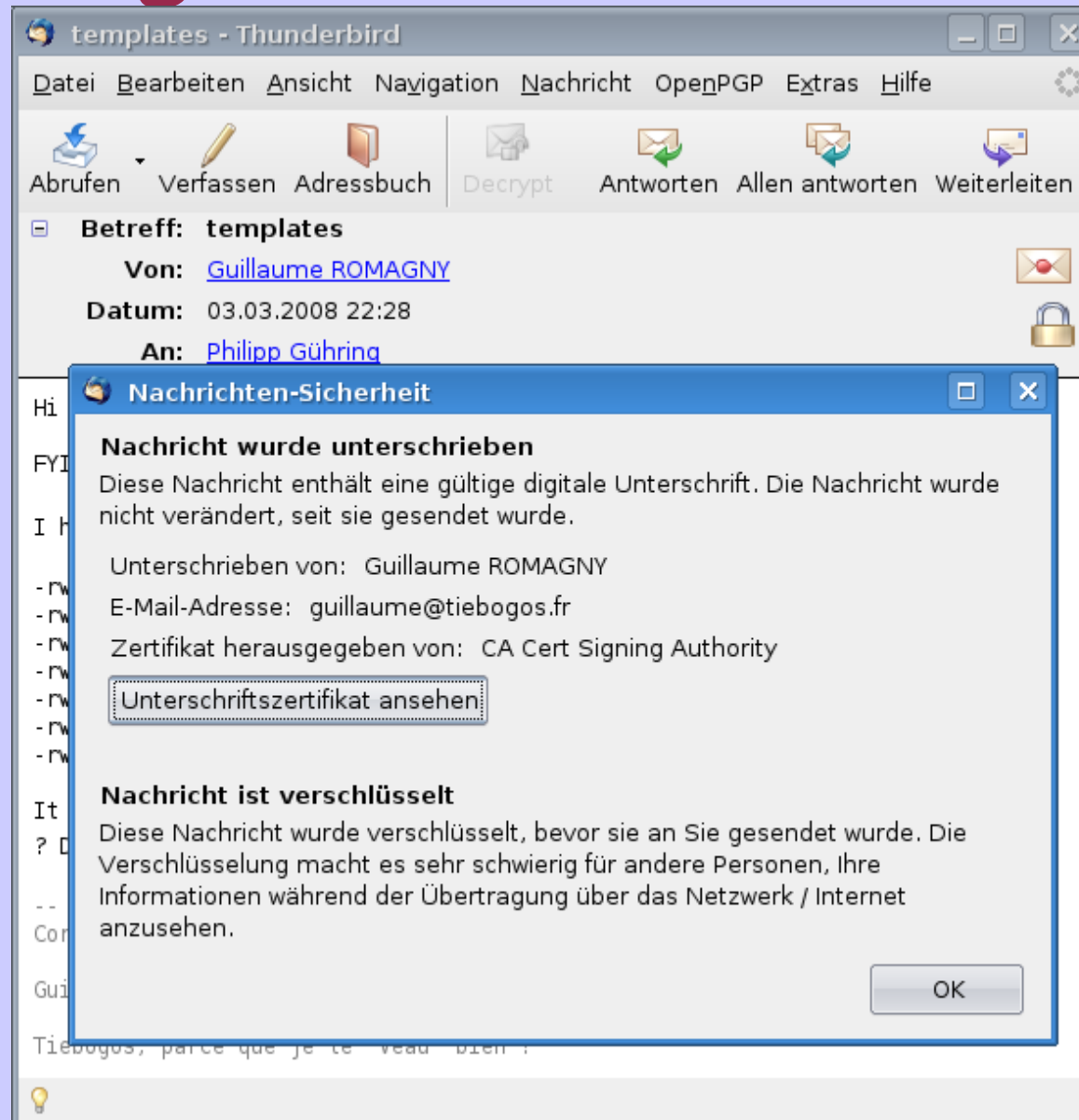
Ansehen

OK

Empfangen einer verschlüsselten Email:



Signator kontrollieren



The screenshot shows the Thunderbird email client interface. The main window displays an email with the following details:

- Betreff:** templates
- Von:** [Guillaume ROMAGNY](#)
- Datum:** 03.03.2008 22:28
- An:** [Philipp Gühring](#)

A security warning dialog box titled "Nachrichten-Sicherheit" 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: Guillaume ROMAGNY
- E-Mail-Adresse: guillaume@tiebogus.fr
- Zertifikat herausgegeben von: CA Cert Signing Authority
- [Unterschriftszertifikat ansehen](#)
- Nachricht ist verschlüsselt**
Diese Nachricht wurde verschlüsselt, bevor sie an Sie gesendet wurde. Die Verschlüsselung macht es sehr schwierig für andere Personen, Ihre Informationen während der Übertragung über das Netzwerk / Internet anzusehen.

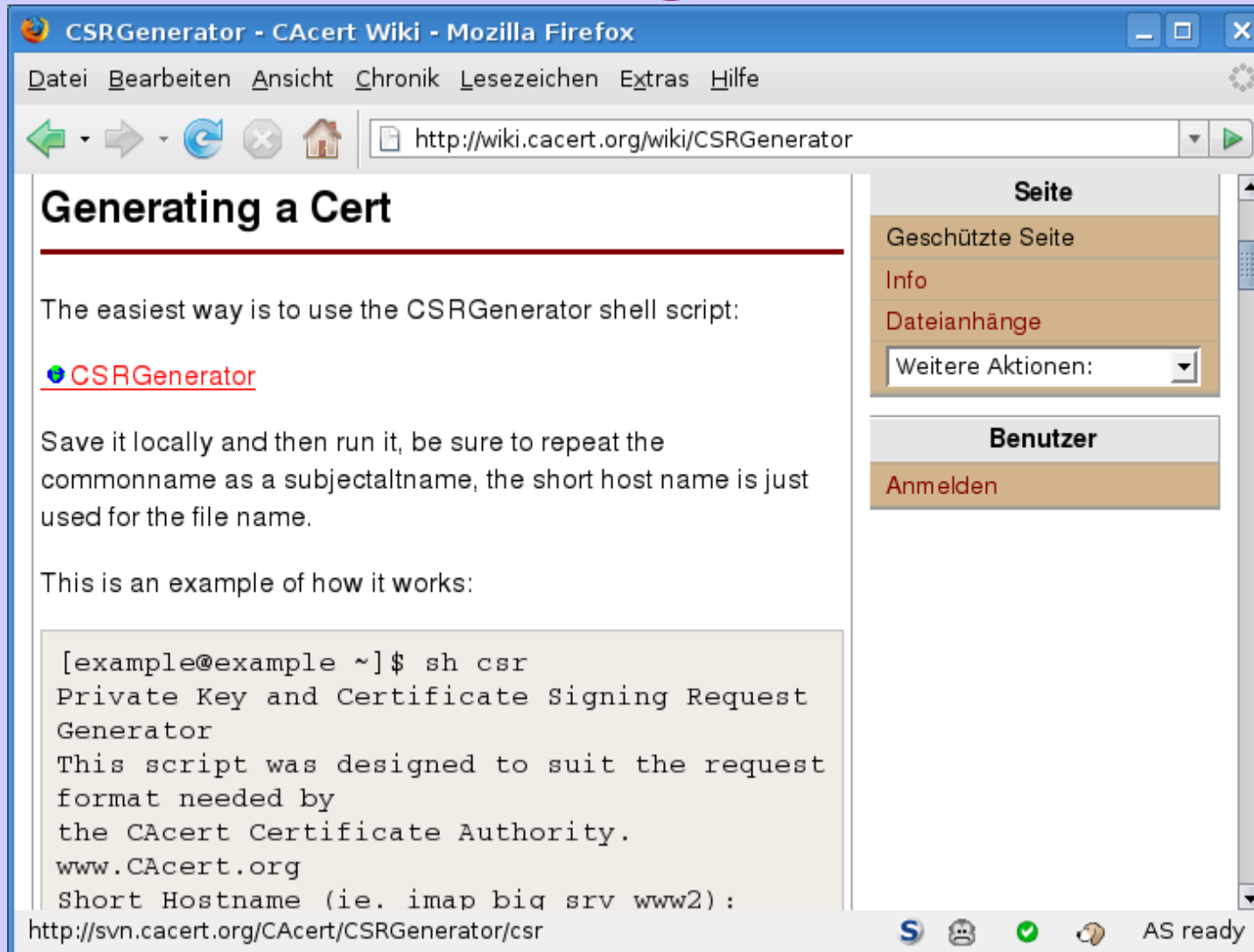
An "OK" button is located at the bottom right of the dialog box.



Server Zertifikat in der Praxis

- ◆ Apache
 - ◆ CSR generieren
 - ◆ Login
 - ◆ Domain freischalten
 - ◆ Server Zertifikat beantragen
- ◆ Vhosts:
<http://wiki.cacert.org/wiki/VhostTaskForce>

Zertifikatsgenerator



CSRGenerator - CAcert Wiki - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://wiki.cacert.org/wiki/CSRGenerator

Generating a Cert

The easiest way is to use the CSRGenerator shell script:

[CSRGenerator](#)

Save it locally and then run it, be sure to repeat the commonname as a subjectaltname, the short host name is just used for the file name.

This is an example of how it works:

```
[example@example ~]$ sh csr
Private Key and Certificate Signing Request
Generator
This script was designed to suit the request
format needed by
the CAcert Certificate Authority.
www.CAcert.org
Short Hostname (ie. imap big srv www2):
http://svn.cacert.org/CAcert/CSRGenerator/csr
```

Seite

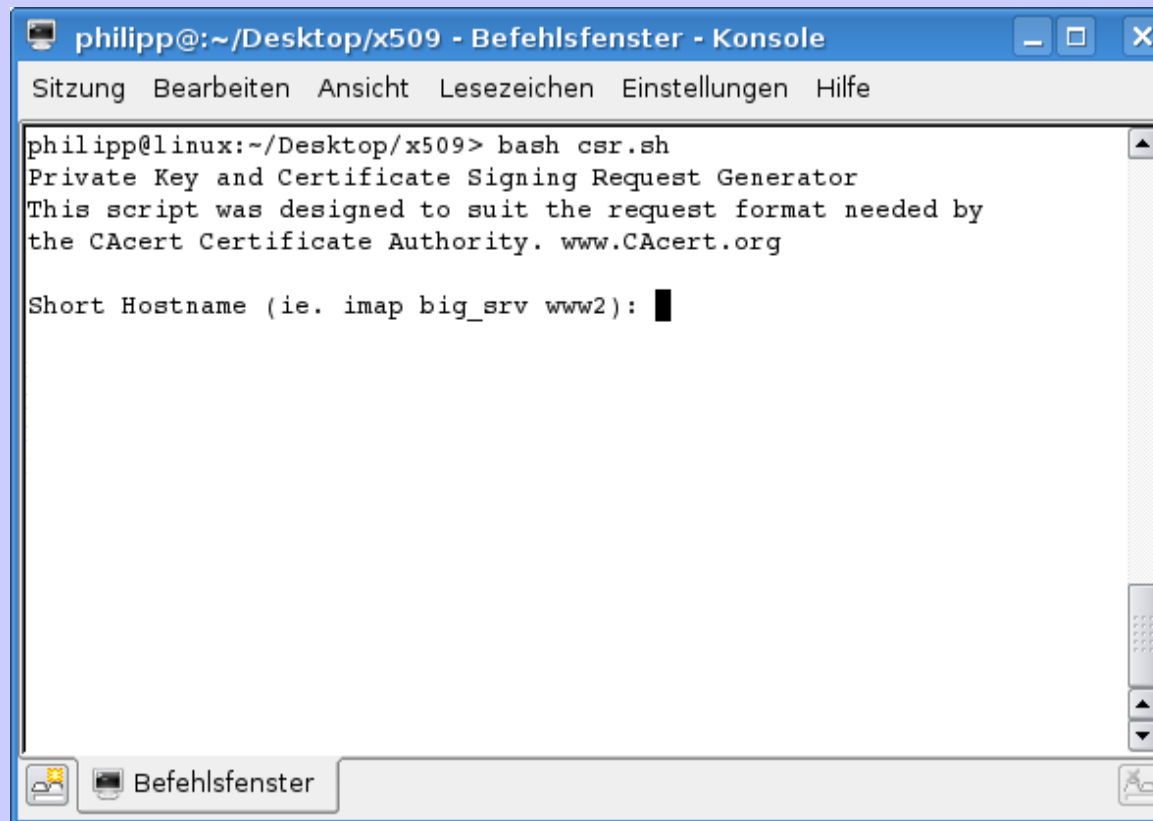
- Geschützte Seite
- Info
- Dateianhänge
- Weitere Aktionen:

Benutzer

- Anmelden

AS ready

Zertifikatsgenerator

A terminal window titled 'philipp@:~/Desktop/x509 - Befehlsfenster - Konsole'. The window contains the following text:

```
philipp@linux:~/Desktop/x509> bash csr.sh
Private Key and Certificate Signing Request Generator
This script was designed to suit the request format needed by
the CAcert Certificate Authority. www.CAcert.org

Short Hostname (ie. imap big_srv www2): █
```

The terminal window has a menu bar with 'Sitzung', 'Bearbeiten', 'Ansicht', 'Lesezeichen', 'Einstellungen', and 'Hilfe'. The window title bar includes standard Linux window controls (minimize, maximize, close) and the window title. The terminal output shows the execution of a script named 'csr.sh' which prompts for a short hostname.

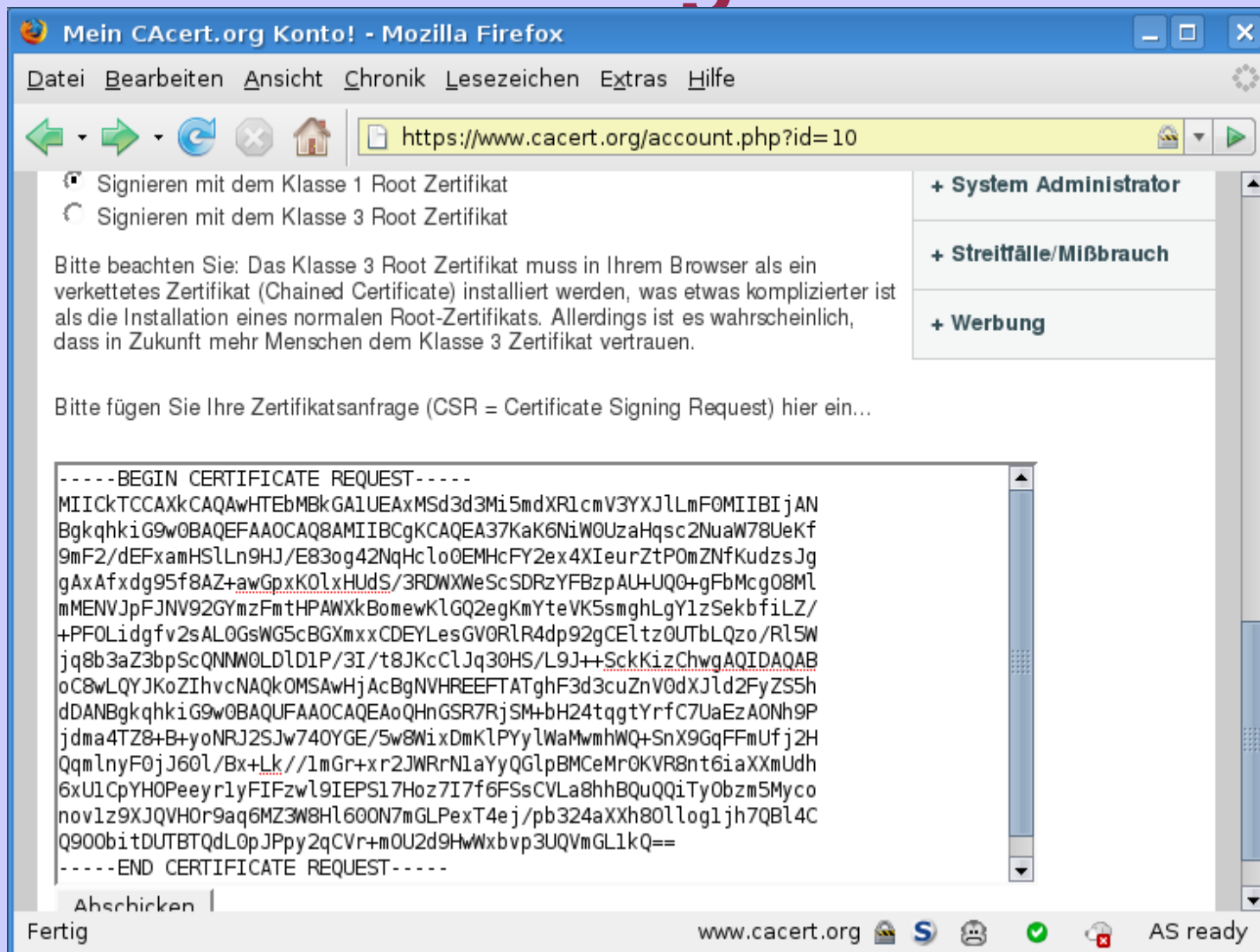
CSR Zertifikatsanfrage

```
philipp@:~/Desktop/x509 - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

-----BEGIN CERTIFICATE REQUEST-----
MIICkTCCAXkCAQAwHTEbMBkGA1UEAxMSd3d3Mi5mdXR1cmV3YXJlLmF0MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA37KaK6NiW0UzaHqsc2NuaW78UeKf
9mF2/dEFxamHSLn9HJ/E83og42NqHcl0EMHcFY2ex4XIeurZtPomZnfKudzsJg
gAxAfxdg95f8AZ+awGpxK0lxHuds/3RDWXWeScSDRzYFBzPAU+UQ0+gFbMcgO8Ml
mMENVJpFJNV92GYmzFmthPAWXkBomewKlGQ2egKmYteVK5smghLgY1zSekbfILZ/
+PFOLidgfv2sAL0GsWG5cBGXmxxCDEYLesGV0RlR4dp92gCEltz0UTbLQzo/Rl5W
jq8b3aZ3bpScQNNW0LD1D1P/3I/t8JKcClJq30HS/L9J++SckKizChwgAQIDAQAB
oC8wLQYJKoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghF3d3cuZnV0dXJld2FyZS5h
dDANBgkqhkiG9w0BAQUFAAOCAQEAoQHnGSR7RjSM+bH24tqgtYrfc7UaEzAONh9P
jdma4TZ8+B+yoNRJ2SJw74OYGE/5w8WixDmKlPYylWaMwmhWQ+SnX9GqFFmUfj2H
QqmlnyF0jJ60l/Bx+Lk//1mGr+xr2JWRrN1aYyQGlpBMCeMr0KVR8nt6iaXXmUdh
6xU1CpYHOpeeyrlyFIFzwl9IEPS17Hoz7I7f6FSsCVLa8hhBQuQQiTyObzm5Myco
nov1z9XJQVHOR9aq6MZ3W8H160ON7mGLPext4ej/pb324aXXh8Olllog1jh7QB14C
Q90ObitDUTBTQdL0pJppy2qCVr+mOU2d9HwWxbvp3UQVmGL1kQ==
-----END CERTIFICATE REQUEST-----

The Certificate request is also available in /home/philipp/www2_csr.pe
m
```

Zertifikatsanfrage zu CAcert



Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php?id=10

Signieren mit dem Klasse 1 Root Zertifikat
 Signieren mit dem Klasse 3 Root Zertifikat

Bitte beachten Sie: Das Klasse 3 Root Zertifikat muss in Ihrem Browser als ein verkettetes Zertifikat (Chained Certificate) installiert werden, was etwas komplizierter ist als die Installation eines normalen Root-Zertifikats. Allerdings ist es wahrscheinlich, dass in Zukunft mehr Menschen dem Klasse 3 Zertifikat vertrauen.

Bitte fügen Sie Ihre Zertifikatsanfrage (CSR = Certificate Signing Request) hier ein...

```

-----BEGIN CERTIFICATE REQUEST-----
MIICKTCCAXkCAQAwHTEbMBkGA1UEAxMSd3d3Mi5mdXR1cmV3YXJlLmF0MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA37KaK6NiW0UzaHqsc2NuaW78UeKf
9mF2/DEFxamHsLn9HJ/E83og42NqHc lo0EMHcFY2ex4XIeurZtP0mZNfKudzSjg
gAxAfxdg95f8AZ+awGpxK0LxHudS/3RDWXWeScSDRzYFBzpAU+UQ0+gFbMcg08Ml
mMENVJpFJNV92GYmzFmthPAWXkBomewKlGQ2egKmYteVK5smghLgY1zSekbfiLZ/
+PFOLidgfv2sALOGsWG5cBGXmxxCDEYLesGV0RLR4dp92gCEltz0UTbLQzo/RL5W
jq8b3aZ3bpScQNNWOLDlD1P/3I/t8JKcClJq30HS/L9J++SckKizChwgAQIDAQAB
oC8wLQYJKoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghF3d3cuZnV0dXJld2FyZS5h
dDANBgkqhkiG9w0BAQUFAAOCAQEAAoQHnGSR7RjSM+bH24tqgtYrfC7UaEzA0Nh9P
jdma4TZ8+B+yoNRJ2SJw740YGE/5w8WixDmKLPyylWaMwmhWQ+SnX9GqFFmUfj2H
QqmInyF0jJ60l/Bx+Lk//lmGr+xr2JWRrNlaYyQGlpBMCEmr0KVR8nt6iaXXmUdh
6xUlCpYH0PeeyrlyFIFzwl9IEPS17Hoz7I7f6FSsCVLa8hhBQUQqITy0bzm5Myco
nov1z9XJQVH0r9aq6MZ3W8Hl600N7mGLPexT4ej/pb324aXXh80llog1jh7QB14C
Q900bitDUTBTQdL0pJPPy2qCvR+mOU2d9HwWxbvp3UQVmqGLlkQ==
-----END CERTIFICATE REQUEST-----
  
```

Abschicken

Fertig

www.cacert.org AS ready

Kontrolle

Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php



Bitte kontrollieren Sie, dass die folgenden Angaben korrekt sind, bevor Sie weitermachen.

CommonName: www2.futureware.at
subjectAltName: DNS:www.futureware.at
Es werden keine weiteren Informationen in Ihr Zertifikat aufgenommen, da diese vom System leider nicht automatisch überprüft werden könnten.

CAcert.org
Gehe zur Startseite
Ausloggen

+ Meine Details

+ E-Mail Konto

+ Client Zertifikate

+ GPG/PGP Schlüssel

+ Domains

+ Server Zertifikate
Neu

Fertig

www.cacert.org AS ready



Fertiges Zertifikat

Mein CAcert.org Konto! - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.cacert.org/account.php

CAcert.org

Unten ist Ihr Server-Zertifikat

```
-----BEGIN CERTIFICATE-----
MIIFEjCCAavqgAwIBAgIDBMzDMA0GCSqGSIb3DQEBAQUAMHkxEDA0BgNVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHAGLy93d3cuY2FjZXJ0Lm9yZzEiMCAgA1UEAxMZ
Q0EgQ2VydCBTaWduaW5nIEF1dGhvcml0eTEhMB8GCSqGSIb3DQEJARYSc3VwcG9y
dEBjYWNLcnQub3JnMB4XDTA4MDMwOTA5NTUyNVowXDTAwMDMwOTA5NTUyNVowHTEb
MBkGA1UEAxMSd3d3Mi5mdXR1cmV3YXJlLmF0MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQA8MIIBCgKCAQEA37KaK6NiW0UzaHqsc2NuaW78UeKf9mF2/dEFxamHSLLn9HJ/
E83og42NgHcl00EMHcFY2ex4XIeurZtP0mZNFkudzsjggAxAfxdg95f8AZ+awGpx
K0LxHudS/3RDWXWeScSDRzYFBzPAU+UQ0+gFbMcg08MlMENVJpFJNV92GYmzFmT
HPAWXkBomewKLgQ2egKmYteVK5smghLgY1zSekbfilZ/+PF0Lidgfv2sAL0GswG5
cBGXmxcDEYLesGV0RLR4dp92gCEltz0UTbLQzo/RL5Wjq8b3aZ3bpScQNNW0LDL
D1P/3I/t8JKcClJq30HS/L9J++SckKizChwgAQIDAQABo4H+MIH7MAwGA1UdEwEB
/wQCMAAwNAYDVR0LBCEwKwYIKwYBBQUHAwIGCCsGAQUFBwMBBgLghkgBhvCBAAEG
CisGAQQBggKCAwMwCwYDVROPAQDAgWgMDMGCCsGAQUFBwEBBCCwJTAjBggrBgEF
BQcwAYYXaHR0cDovL29jczAuY2FjZXJ0Lm9yZy8wYDVR0RBGwwaoISd3d3Mi5m
dXR1cmV3YXJlLmF0CAGCCsGAQUFBwFoBQMEnd3dzIuZnV0dXJld2FyZS5hdIIR
d3d3LmZldHVyZXdhcmUuYXNzGHWYIKwYBBQUHCAWgEwRd3d3LmZldHVyZXdhcmUu
YXQwDQYJKoZIhvcNAQEFBQADggIBAMmUKfYFWM1gc84G0EMkvjveV62xf4RyYZ
A4dVD2cIu2pH8z10tL9L880Kw8rxL0RDVvmz0j09KcdugzT2/ixMYZjzq/AF1FRn6
LNgeKeExPEjLexAyuhgFhSr0u5PJg+bWa3bzu/3Yes2F6+Bl/sAemFRb60HpvL8p
L0ASm/YYybNlcZBh0P7ft+MgC0VoKgzRvGrCtWshR0gdUJp8+Nl8vjplNc+64IiL
2QNuIPbDeG1Fg0otGncVjVa2ym4beubQgYHBS0Ao2Kv9YoDclq2grdUsZnZ0vfGB
DE8D0eL/Ft8agCd3Lm8BUyg0k6ItqHsuQmaDQLc5SnJZ9PN7oaNEmgzB5UgdMITb
223UW0M4FcofZJ0XMaxpzgCHZOL/PbGo/7zZXiMcQSBh0FN67T3GYGyN9TIdaf+
wjaaj/Us+Nwyl4q6ZuZ7HESWzj50NwZ+/jdA8vXYd6H0FsgC0UkFAcopCF/ks80Rz
pSXZEmHqfW3rGid5oy/vmxmezBJIYcyYE80wZzBnx1kXGk2m7t3YhYxNPhyCT7i
L8+Rf3Q50Y+t0wWOC7LcainJraQDMu+w68poB4t5LedtM3CMCPB0fL44HHvcDsSX
toYbGusm46dfBQRM433PSyKfXp50xf70df64Aj9Mfbl0ohWvDi/NG5TaY555ghZL
VdLZ0Jj9
-----END CERTIFICATE-----
```

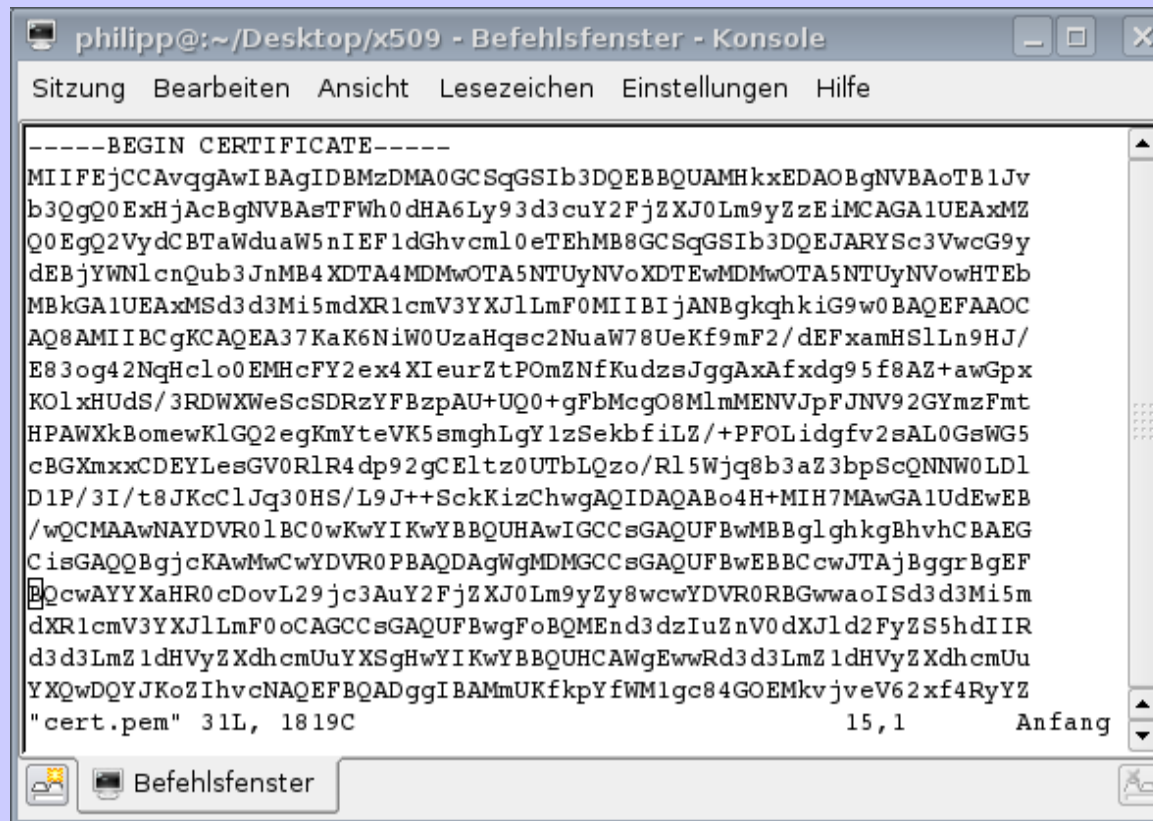
Fertig

www.cacert.org

AS ready

- CAcert.org
 - Gehe zur Startseite
 - Ausloggen
- + Meine Details
- + E-Mail Konto
- + Client Zertifikate
- + GPG/PGP Schlüssel
- + Domains
- + Server Zertifikate
 - Neu
 - Anzeigen
- + Organisations Client

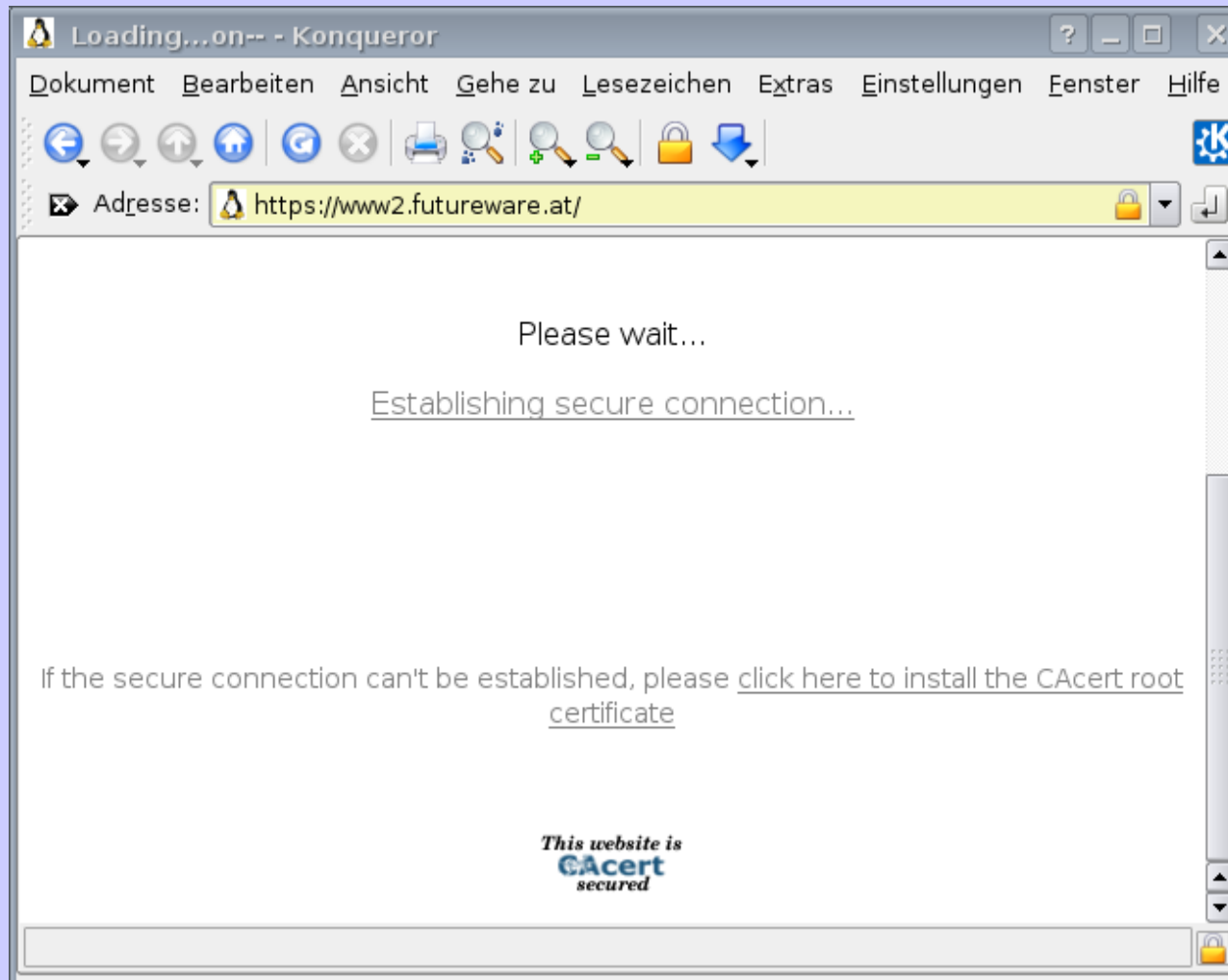
Zertifikat in Datei speichern



```
philipp@:~/Desktop/x509 - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe


-----BEGIN CERTIFICATE-----
MIIFEjCCAvqgAwIBAgIDBMzDMA0GCSqGSIb3DQEJBQUAMHkxEDAObgNVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHA6Ly93d3cuY2FjZS5XJ0Lm9yZzEiMCAGA1UEAxMZ
Q0EgQ2VydCBTaWduYW5nIEF1dGhvcml0eTEhMB8GCSqGSIb3DQEJARYSc3VwcG9y
dEBjYWNlcnQub3JnMB4XDTA4MDMwOTA5NTUyNVoXDTEwMDMwOTA5NTUyNVowHTEb
MBkGA1UEAxMSd3d3Mi5mdXR1cmV3YXJlLmF0MIIBIjANBgkqhkiG9w0BAQEFAAOCC
AQ8AMIIBCgKCAQEA37KaK6NiW0UzaHqsc2NuaW78UeKf9mF2/dEFxamHSlLn9HJ/
E83og42NqHcl0EMHcFY2ex4XIeurZtPomZNfKudzsJggAxAfxdg95f8AZ+awGpx
KOlXHudS/3RDWXWeScSDRzYFBzpaU+UQ0+gFbMcgO8MlMENVJpFJNV92GYmzFmt
HPAWXkBomewKlGQ2egKmYteVK5smghLgY1zSekbfilZ/+PFOLidgfv2sAL0GsWG5
cBGXmxxCDEYLesGV0RlR4dp92gCEltz0UTbLQzo/Rl5Wjq8b3az3bpScQNNW0LD1
D1P/3I/t8JKcClJq30HS/L9J++SckKizChwgAQIDAQABo4H+MIH7MAwGA1UdEwEB
/wQCMAAwNAYDVR0lBC0wKwYIKwYBBQUHAWIGCCsGAQUFBwMBBglghkgBhvhCBAEG
CisGAQQBgjcKAwMwCwYDVR0PBAQDAgWgMDMGCCsGAQUFBwEBBCCwJTAjBggrBgEF
BQcwAYYXaHR0cDovL29jc3AuY2FjZS5XJ0Lm9yZy8wYDVR0RBGwwaoISd3d3Mi5m
dXR1cmV3YXJlLmF0cAGCCsGAQUFBwgFoBQMEnd3dzIuZnV0dXJld2FyZS5hdIIR
d3d3LmZldHVyZXdhemUuYXNqHwYIKwYBBQUHCAWgEwwRd3d3LmZldHVyZXdhemUu
YXQwDQYJKoZIhvcNAQEFBQADggIBAMmUKfkyFwM1gc84GOEMkvjveV62xf4RyYZ
"cert.pem" 31L, 1819C                                     15,1      Anfang
```

Zertifikat im Webserver installiert



Zertifikatsdetails

KDE-SSL-Information - Konqueror

 Die aktuelle Verbindung ist durch SSL abgesichert.

Kette:

Peer-Zertifikat:

Herausgeber:

Allgemeiner Name: www2.futureware.at	Organisation: Root CA
	Organisationseinheit: http://www.cacert.org
	Allgemeiner Name: CA Cert Signing Authority

IP-Adresse: 217.19.43.211

Adresse (URL): https://www2.futureware.at/

Zertifikat-Status: **Das Zertifikat ist gültig.**

Gültig von: **Dienstag, 6. Juni 2006 20:22:23 GMT**

Gültig bis: **Donnerstag, 5. Juni 2008 20:22:23 GMT**

Seriennummer: 153471



MD5-Digest: 35:48:AE:93:22:09:79:91:AB:81:C9:22:2C:74:E6:70

Verwendete Verschlüsselung: DHE-RSA-AES256-SHA

Details: DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1

SSL-Version: TLSv1/SSLv3

Verschlüsselungstiefe: 256 Bit verwendet aus einer 256-Bit-Verschlüsselung

 Kryptographie-Einrichtung ...  Schließen

Wann soll ich ein Zertifikat widerrufen?

- ◆ Wurden mit dem Zertifikat digitale Signaturen gemacht?
- ◆ War das Zertifikat falsch ausgestellt?
- ◆ Besteht akute Mißbrauchsgefahr?

Danke

- ◆ <http://www.cacert.org/>
- ◆ <http://wiki.cacert.org/>
- ◆ support@cacert.org

Noch Fragen?

