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

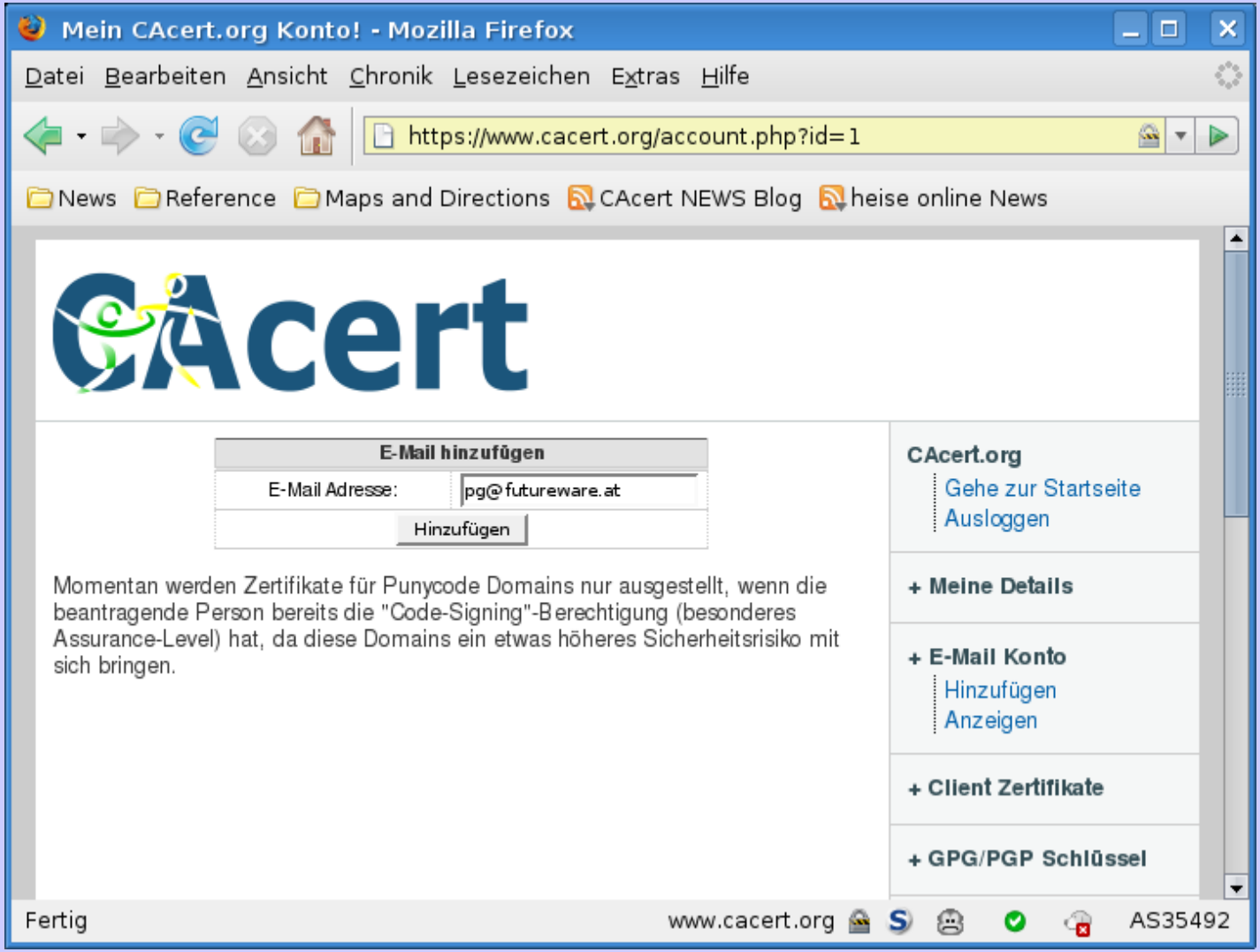
- Serverzertifikate
  - Webserver mit https:// (SSL) absichern
  - Mailserver
  - VPN
- Clientzertifikate
  - S/Mime: Unterschreiben und Verschlüsseln von Emails
  - Anmeldung bei Webseiten
  - Software/Makros/Applets signieren
  - Kostenloser Internetzugang bei Funkfeuer

Client Zertifikate in der Praxis

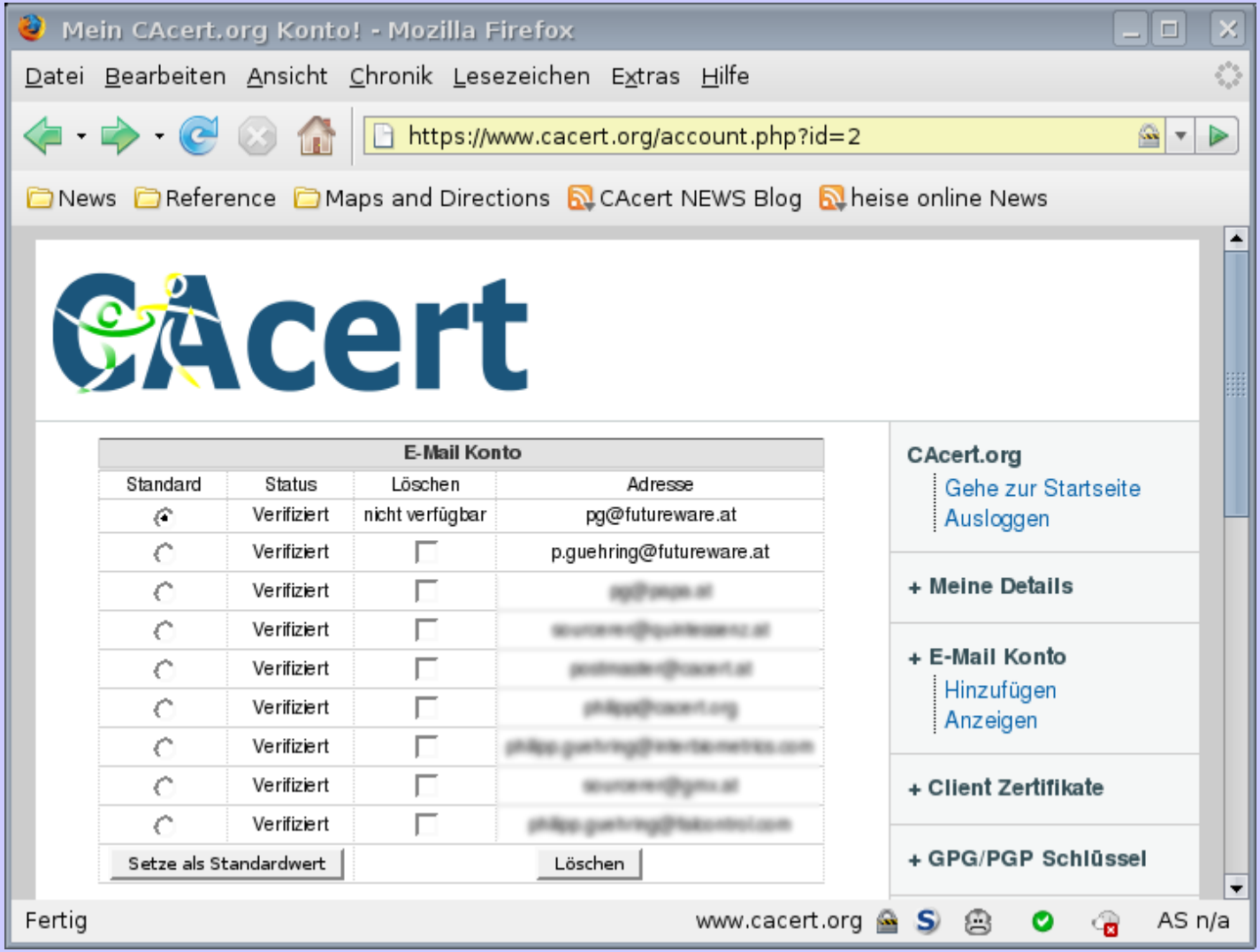
- Firefox
  - Login
  - Email Adressen freischalten
  - Client Zertifikat beantragen
  - Zertifikat installieren
  - Sicherung des Zertifikats
  - auf https://secure.cacert.org/ verwenden

CAcert.org Webseite

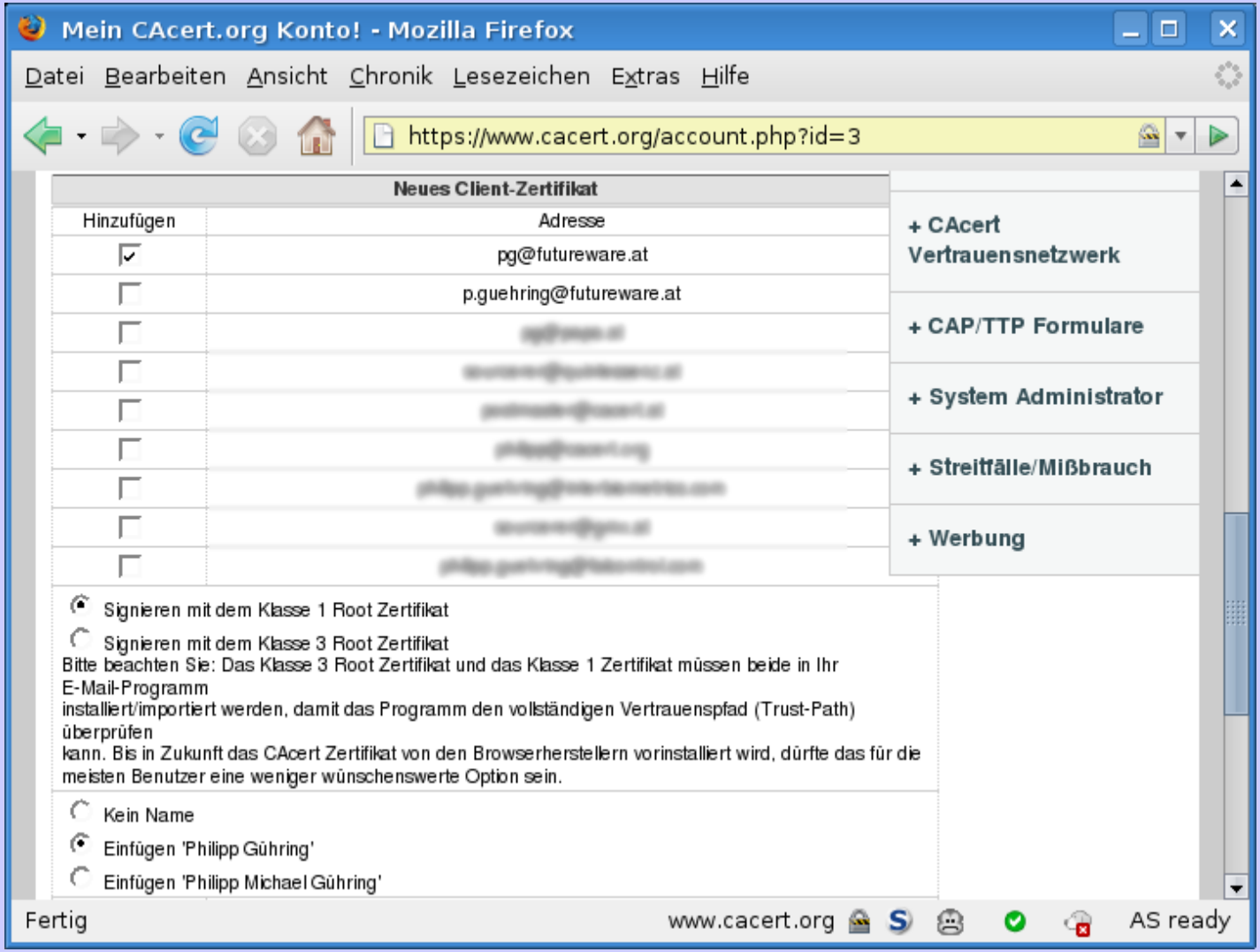
Einloggen, E-Mail Adresse



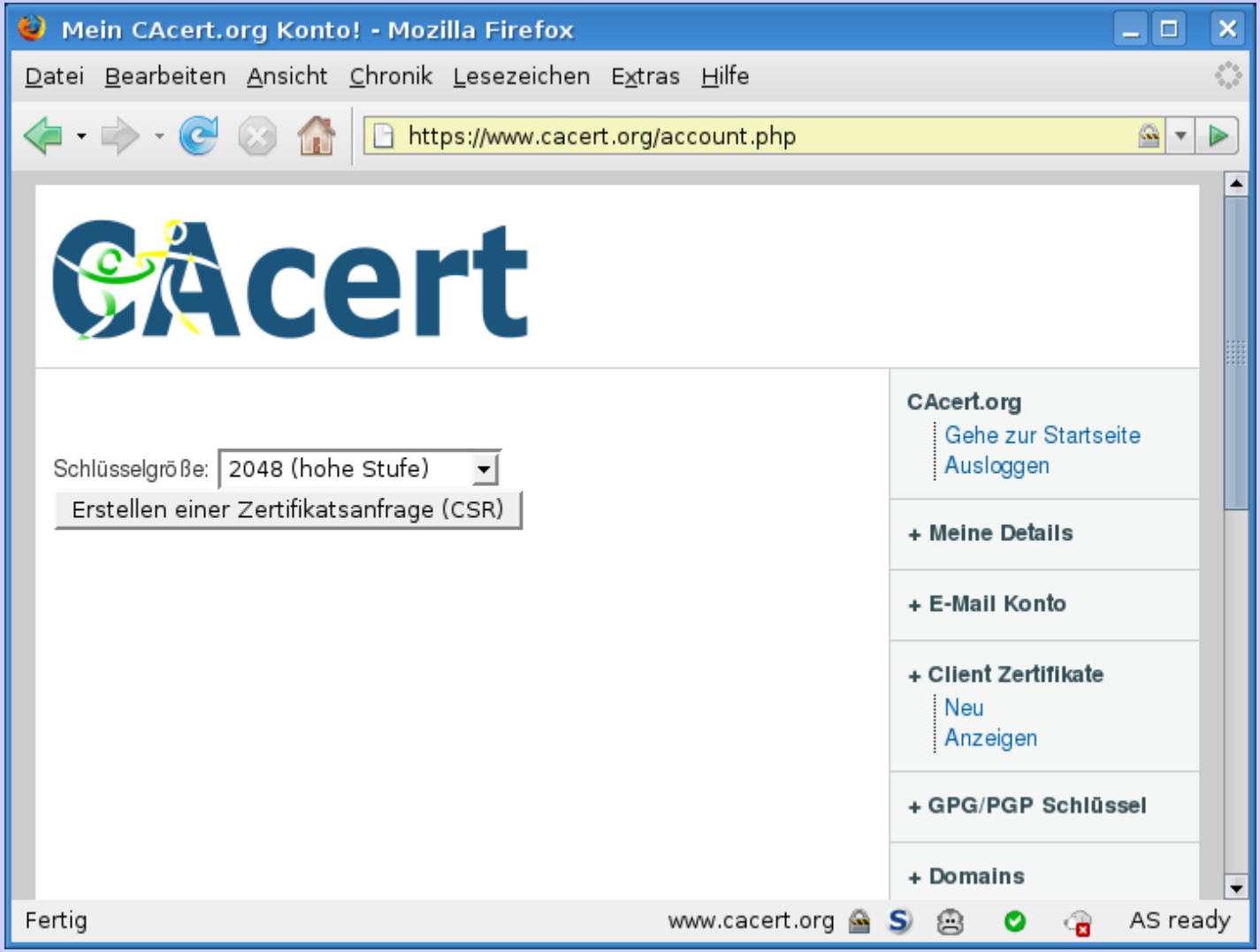
E-Mail Adresse verifiziert



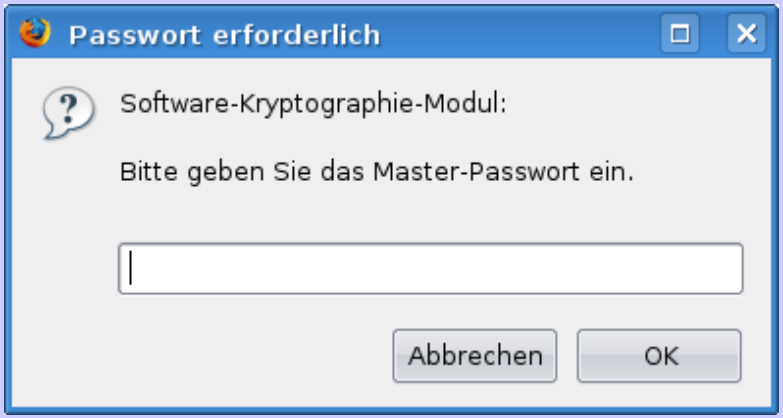
Zertifikat erzeugen ...



Schlüssel Parameter



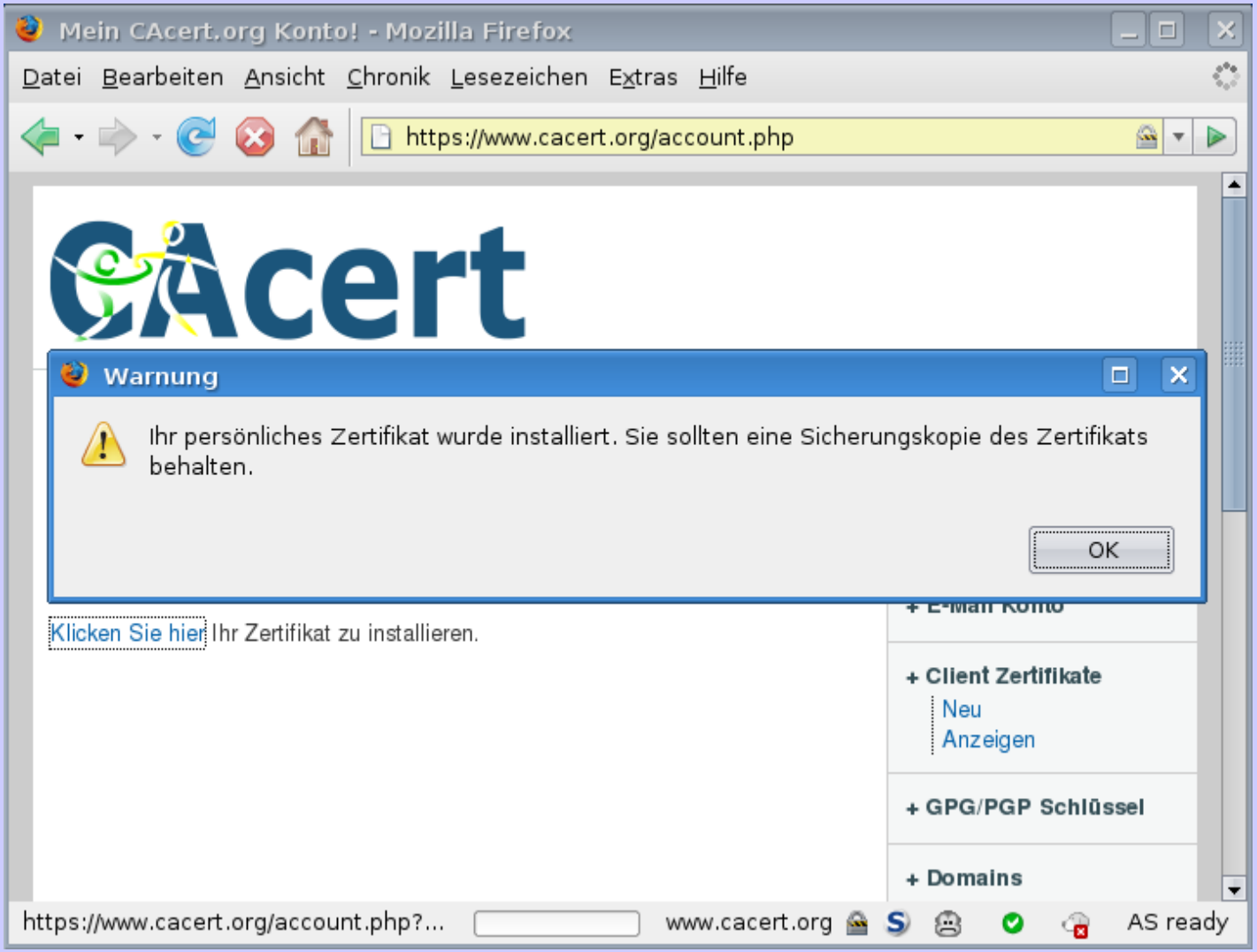
Firefox Master-Passwort zur Aufbewahrung der Schlüssel



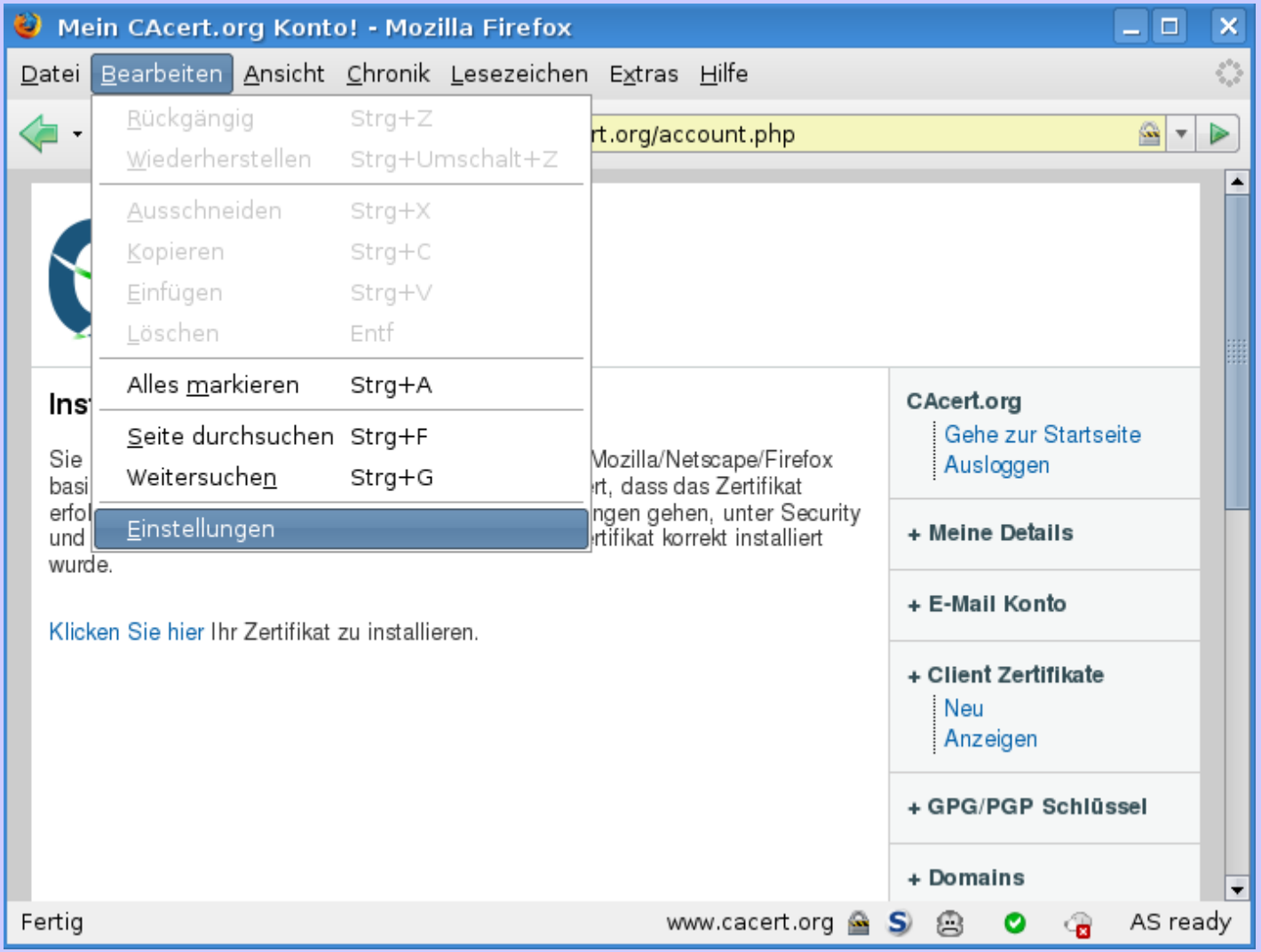
Schlüssel wird erzeugt
Zertifikat wird erzeugt

Zertifikat wurde erzeugt

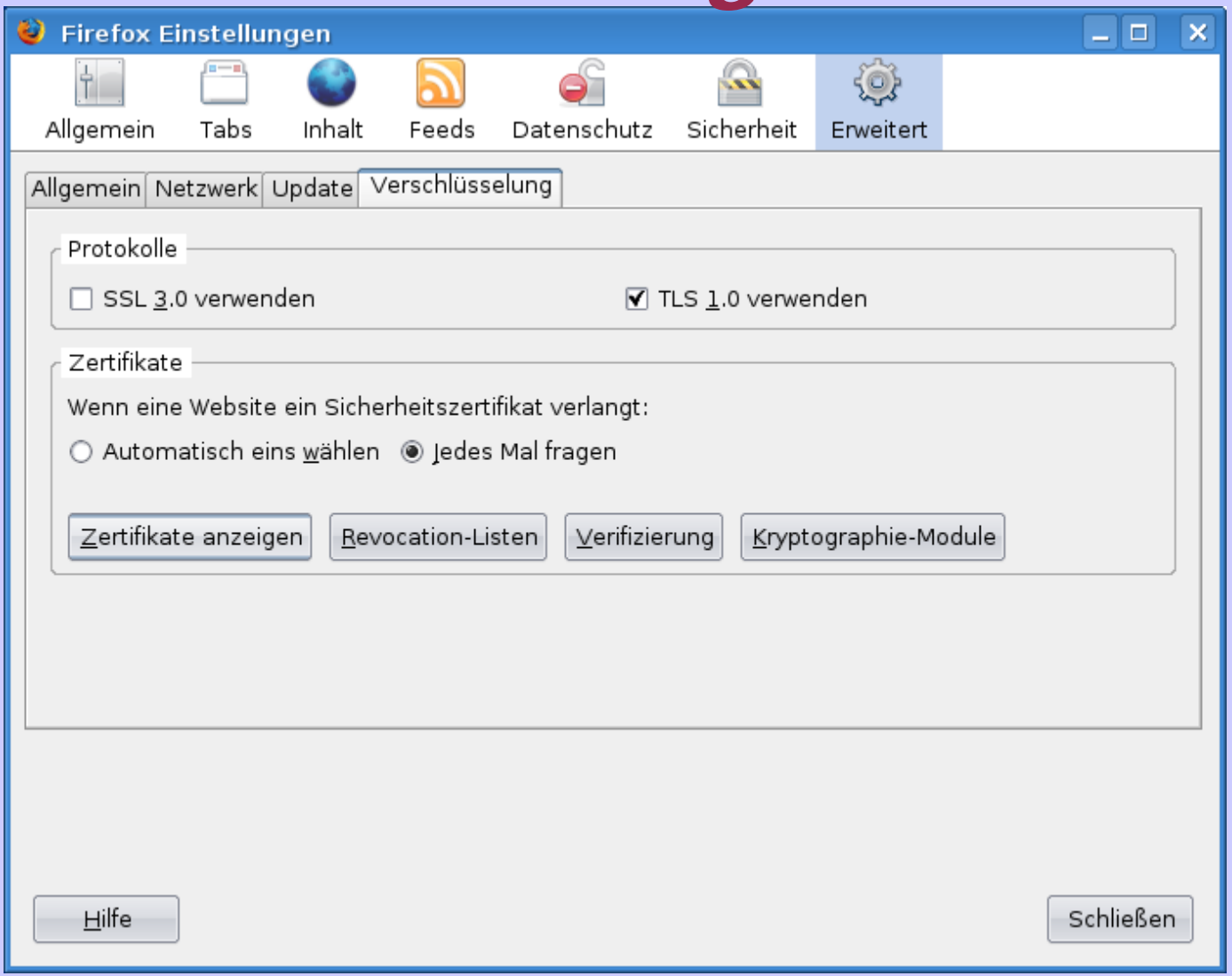
Zertifikat installiert



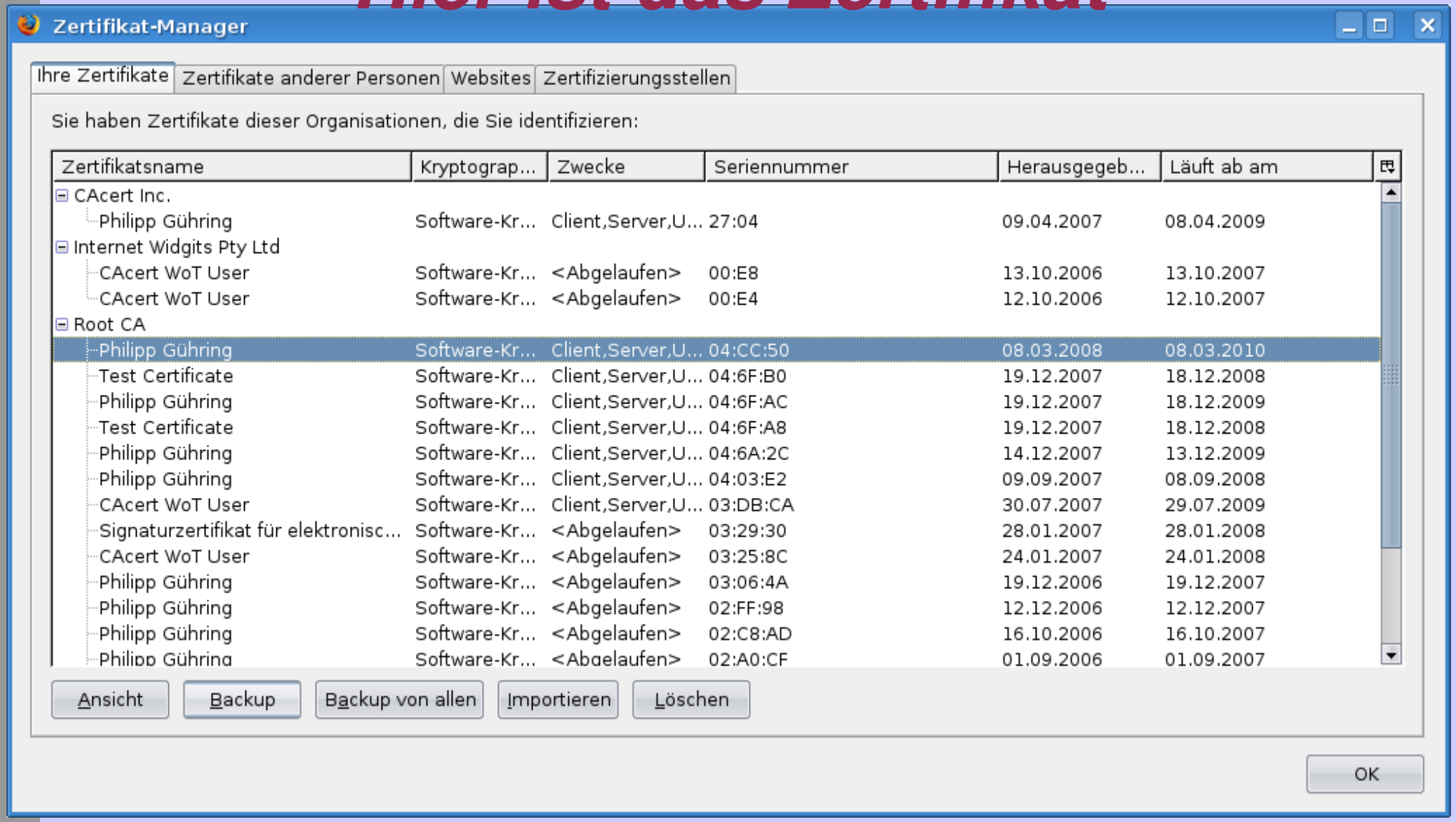
Wo ist das Zertifikat nun?



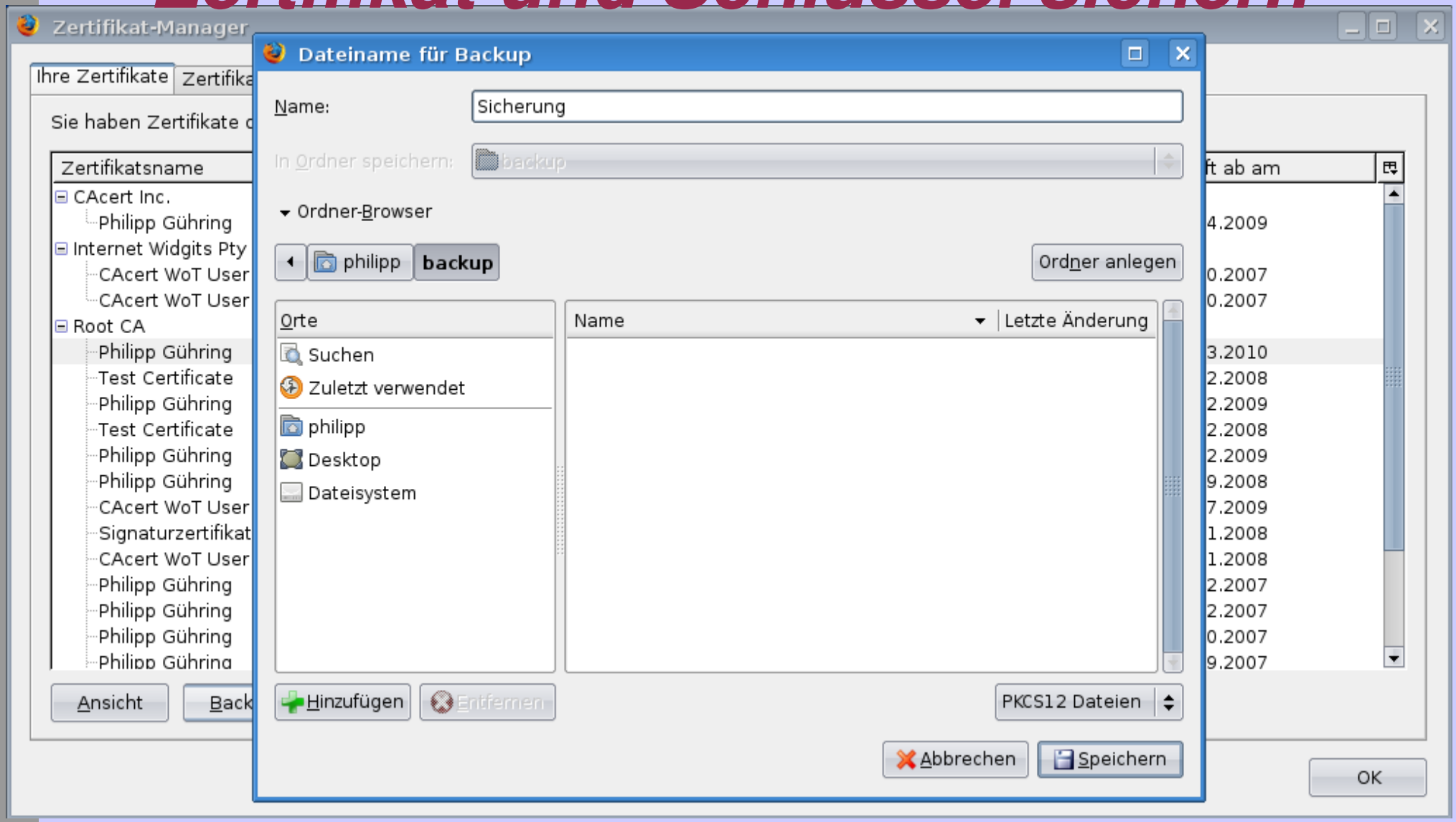
Einstellungen ...



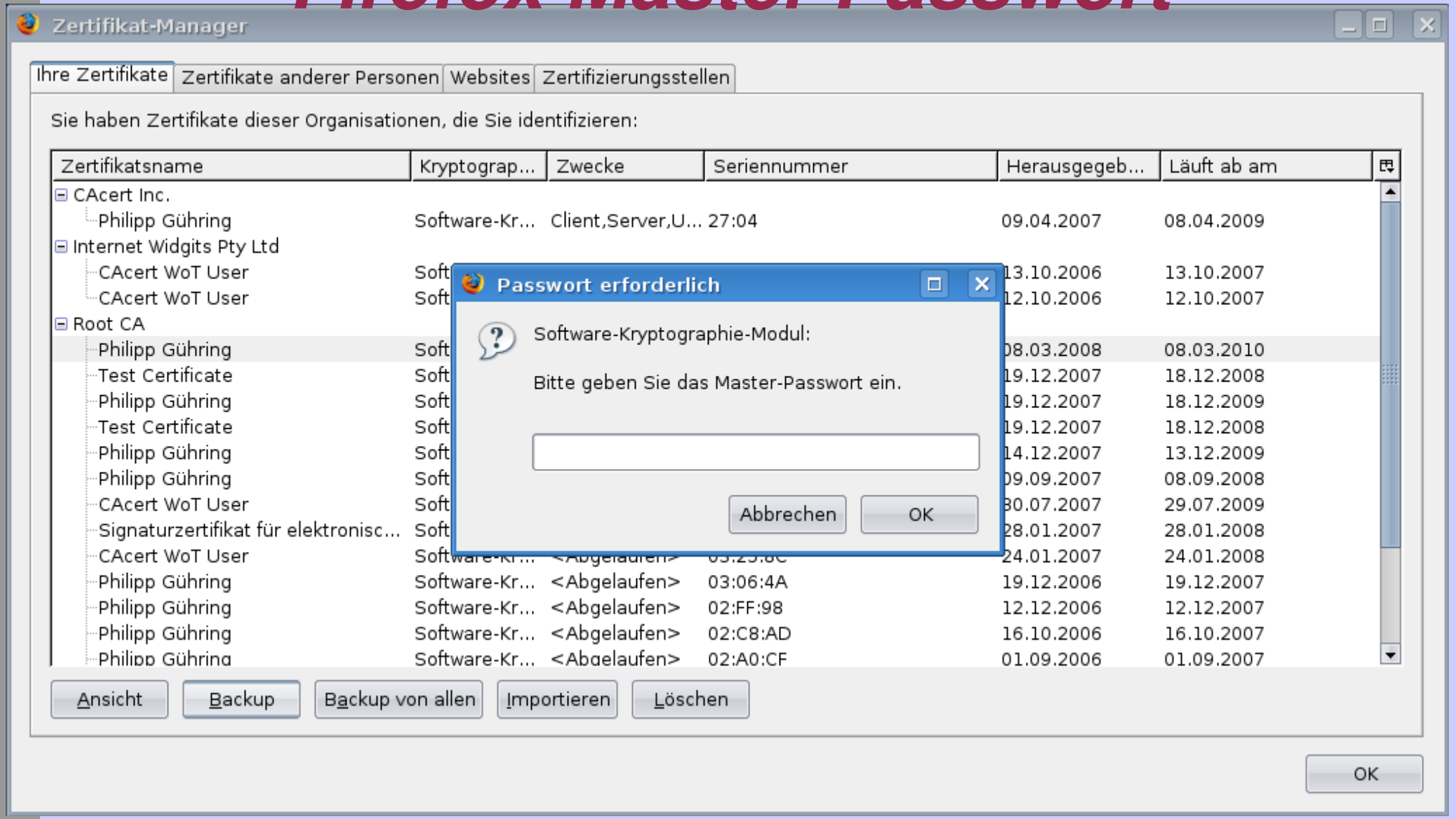
Hier ist das Zertifikat



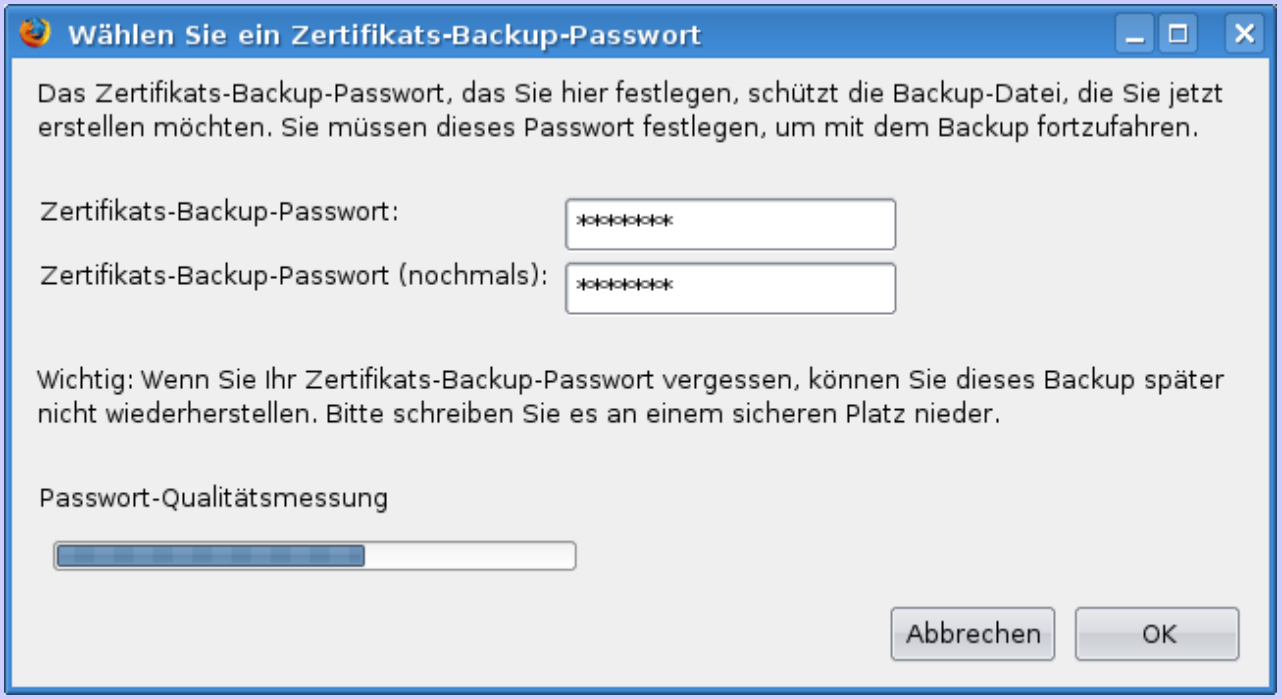
Zertifikat und Schlüssel sichern



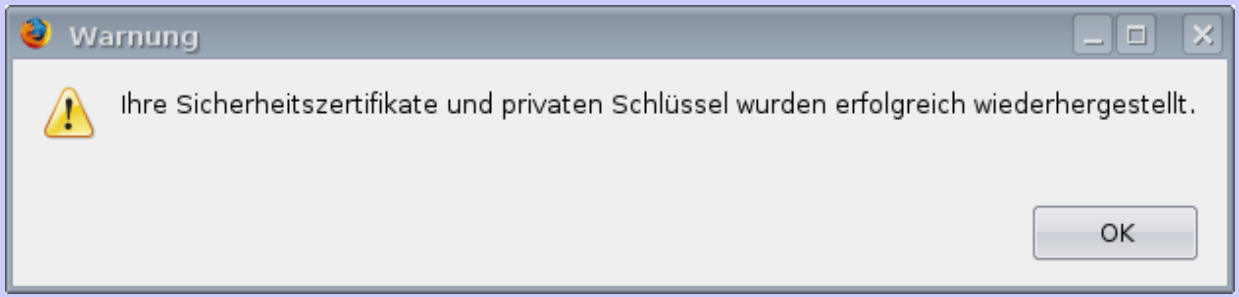
Firefox Master Passwort



Das Passwort für die Sicherung wählen

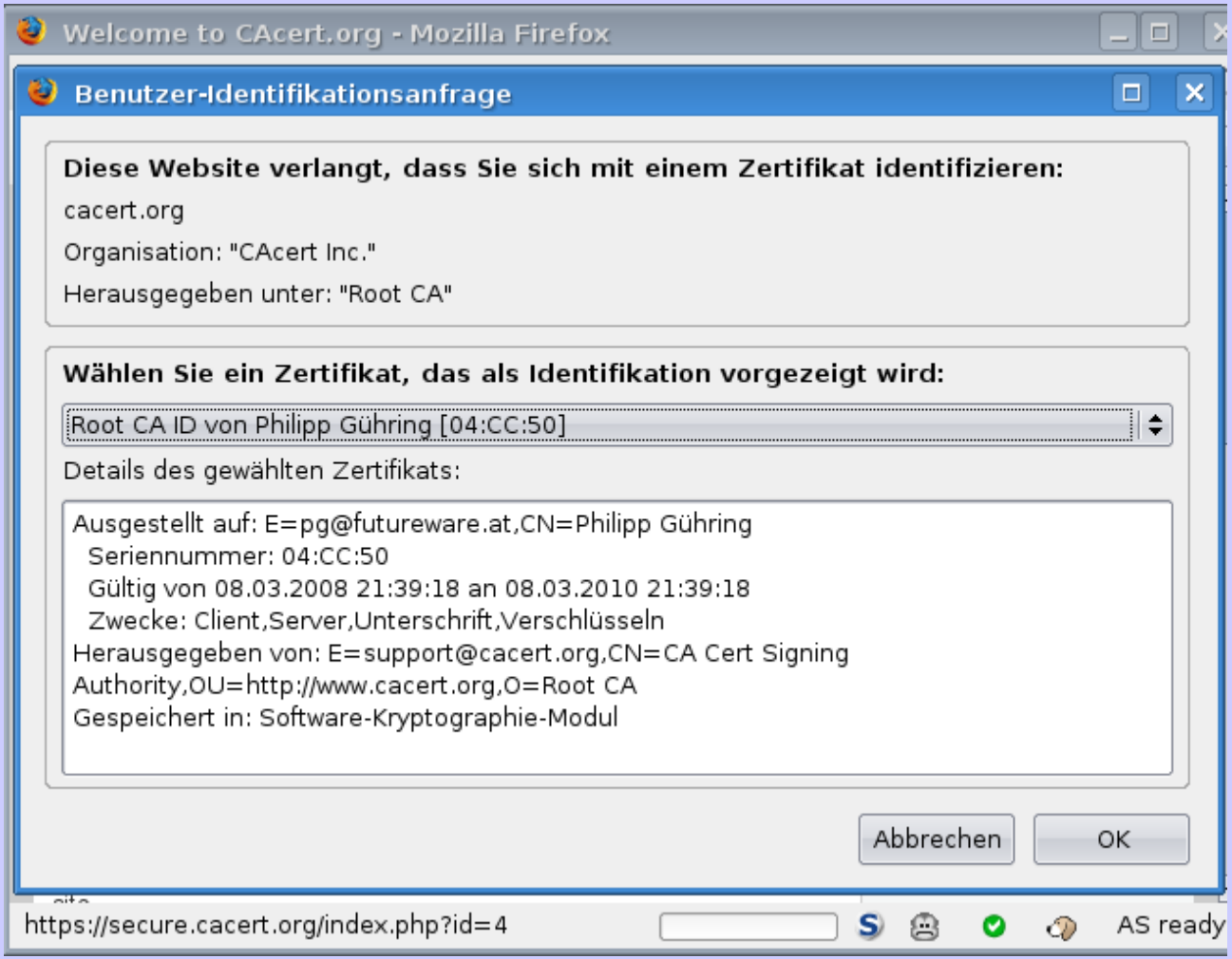


Der private Schlüssel wurde in der Datei „Sicherung.p12“ gesichert.

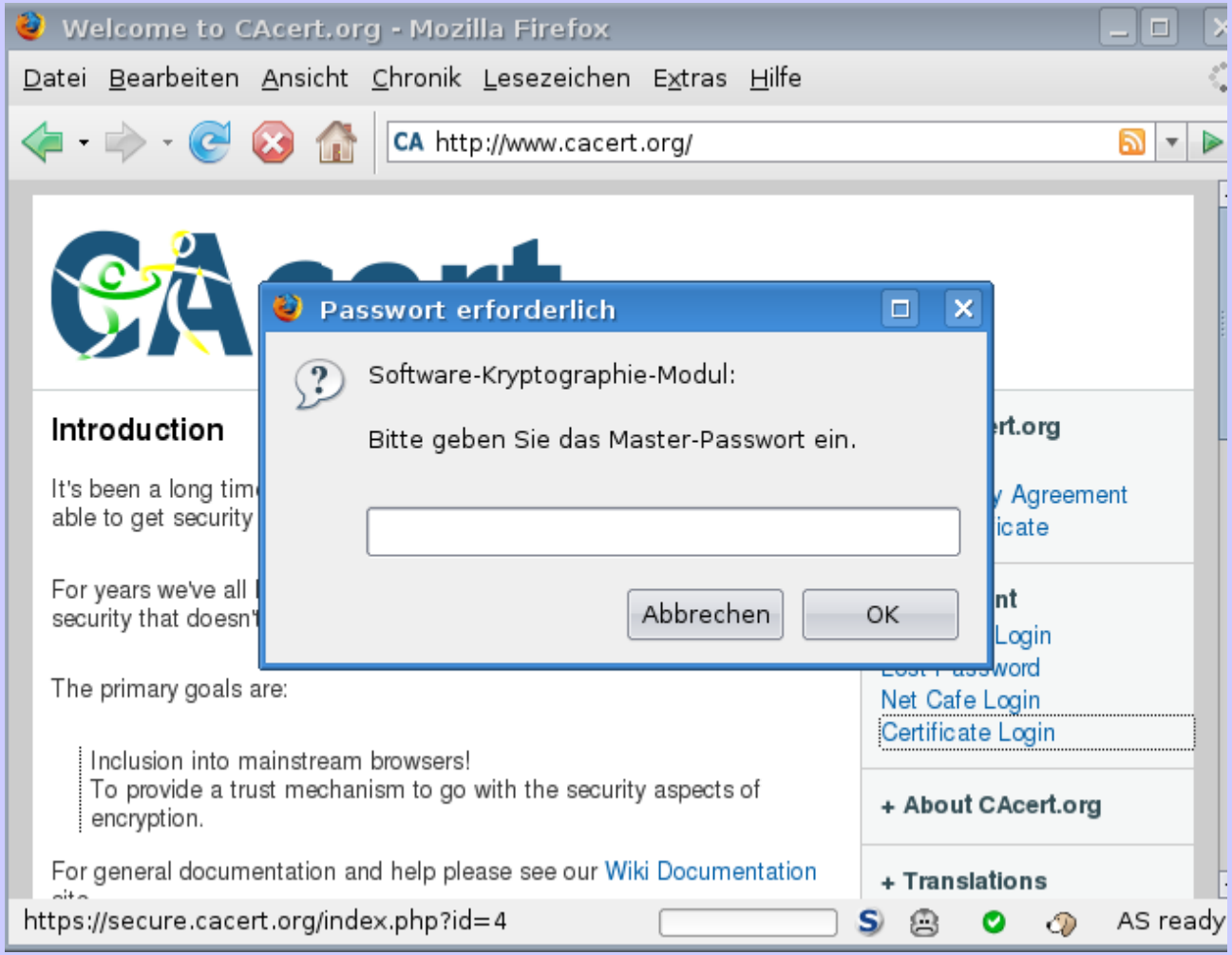


Web-Login mit Zertifikat

Auswahl des Zertifikats



Firefox Master-Passwort



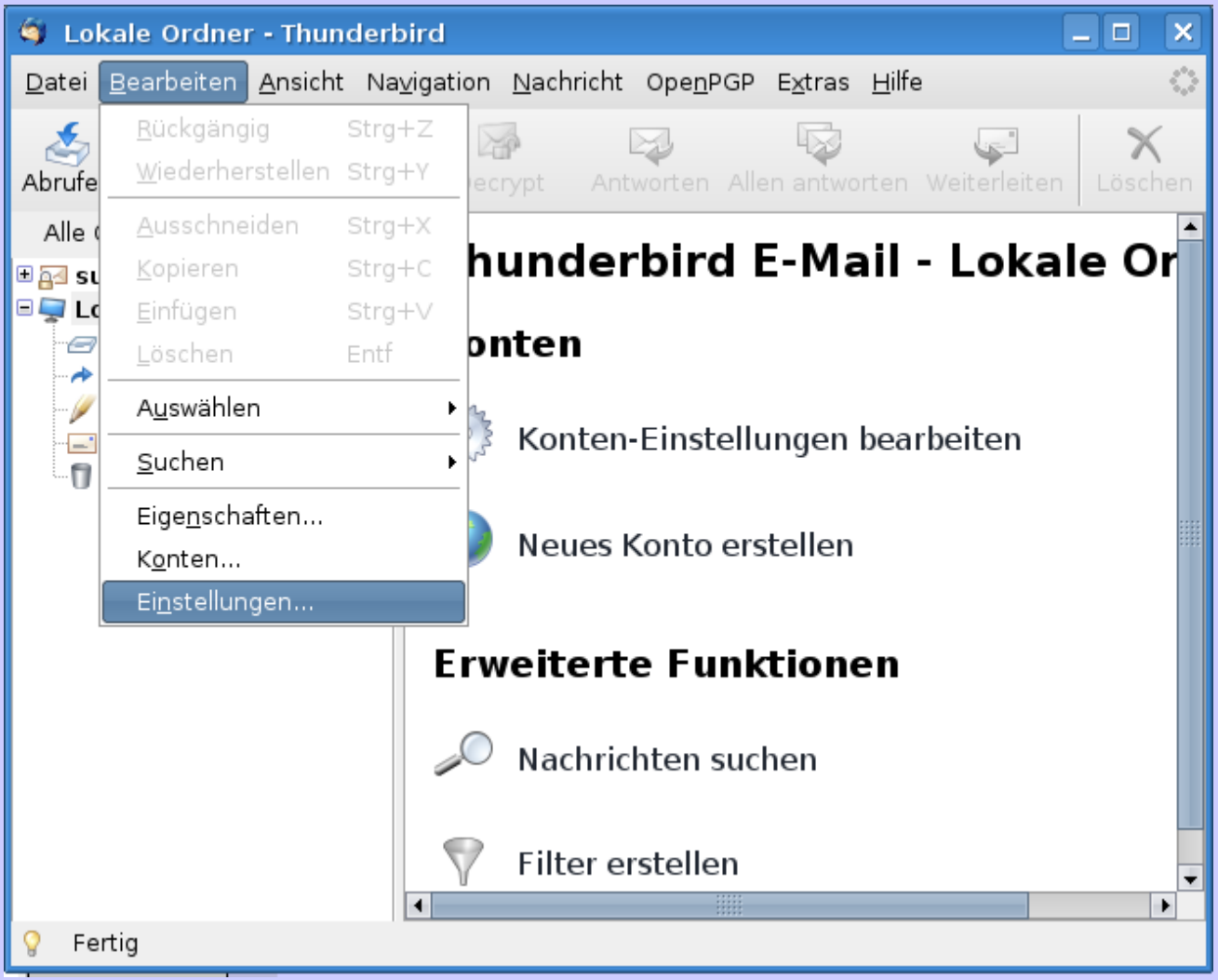
Bin drin!


Mein CAcert.org Konto! - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://secure.cacert.org/account.php
CAcert
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

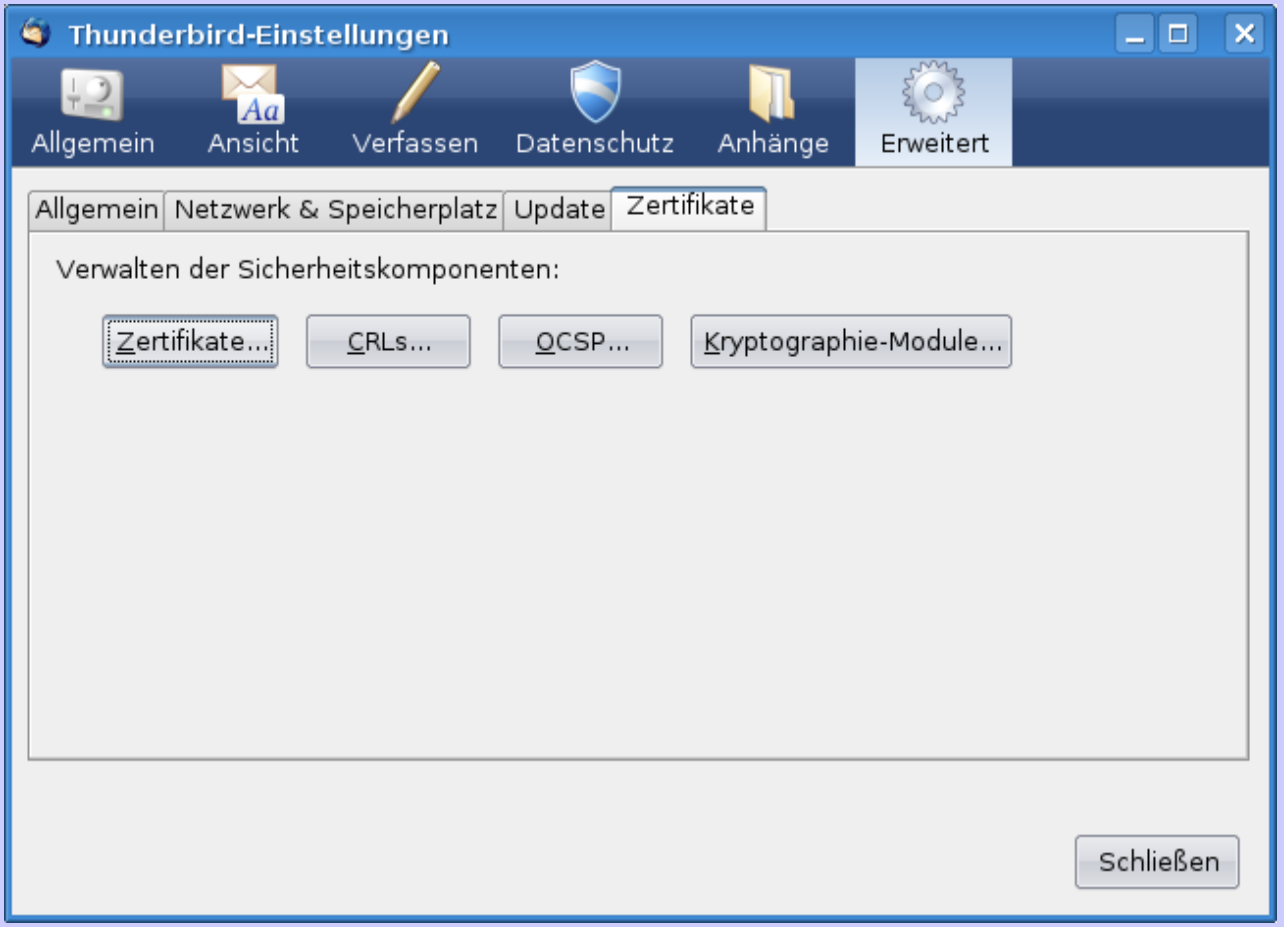
EMail

Thunderbird
Zertifikat importieren
Zertifikat verwenden

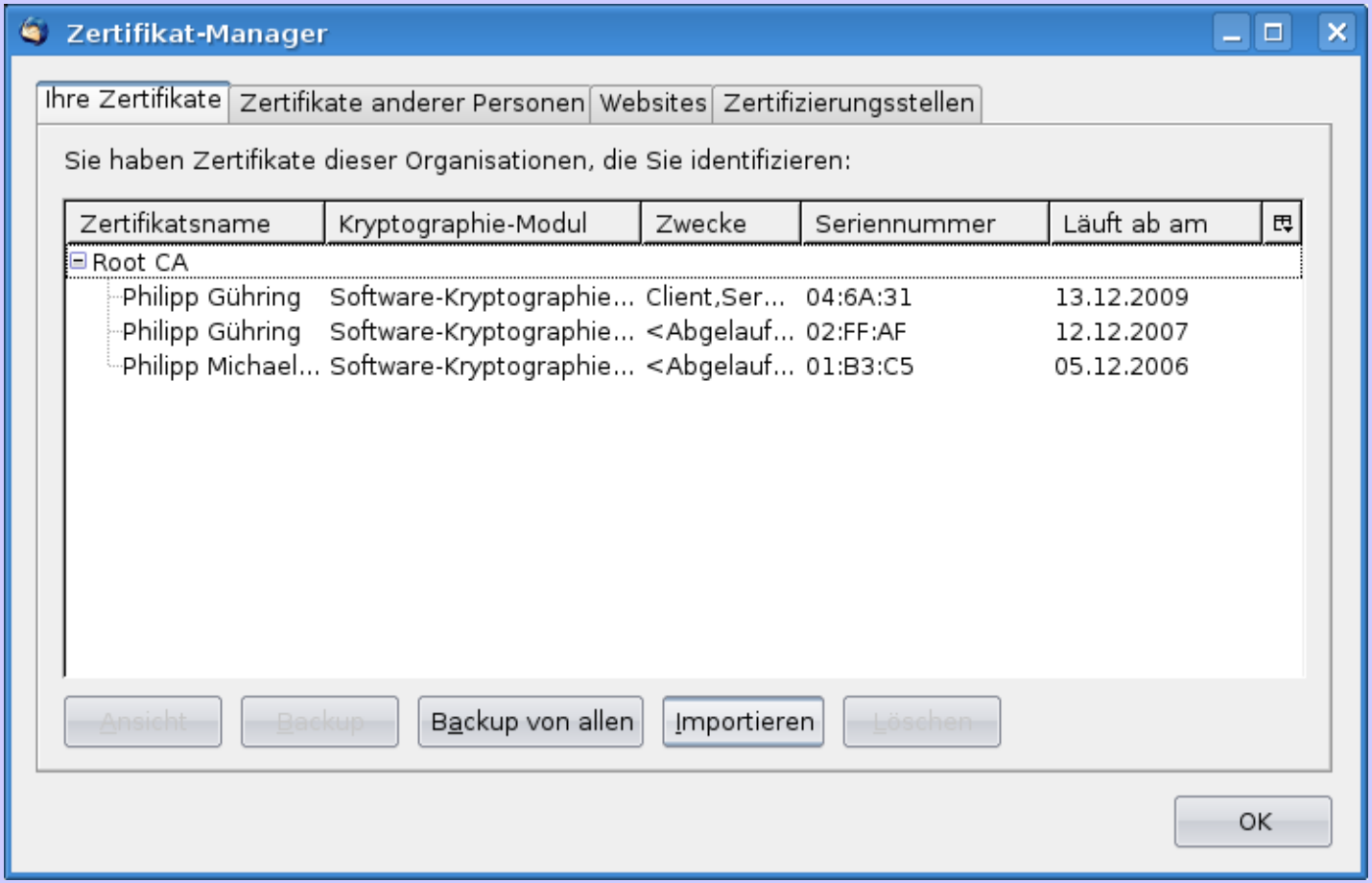
Thunderbird Zertifikat importieren



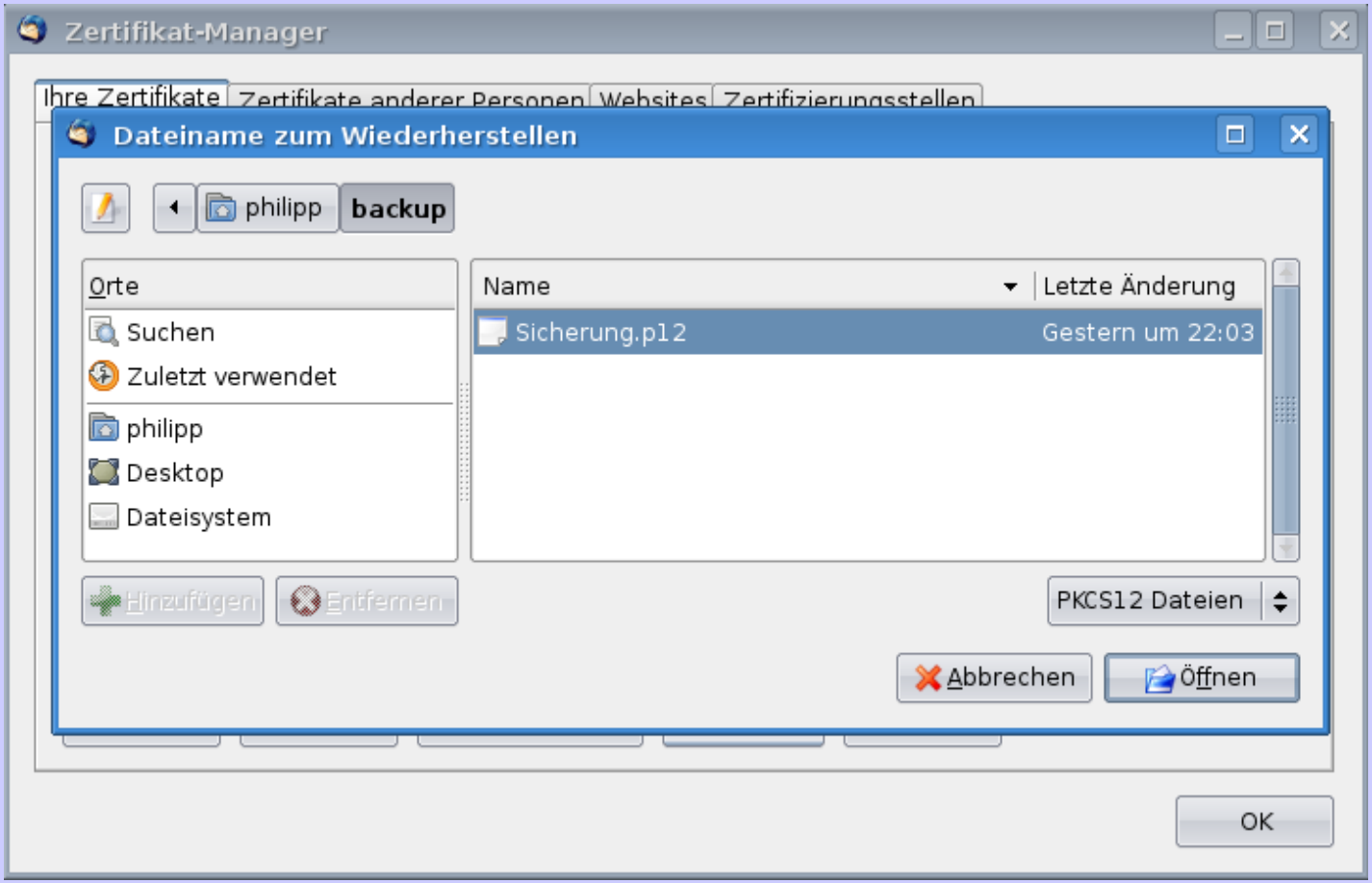
Zertifikate...



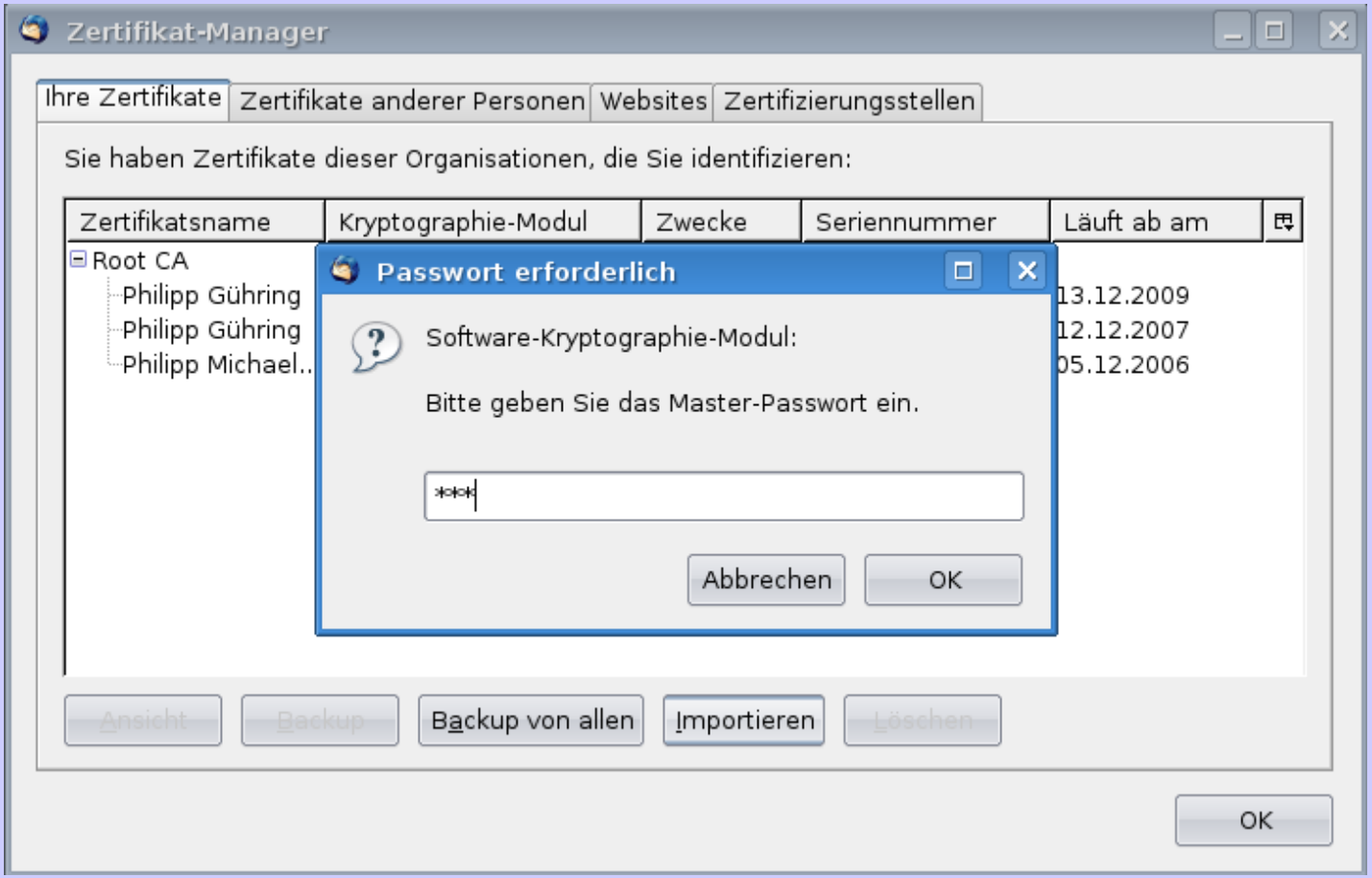
Importieren...



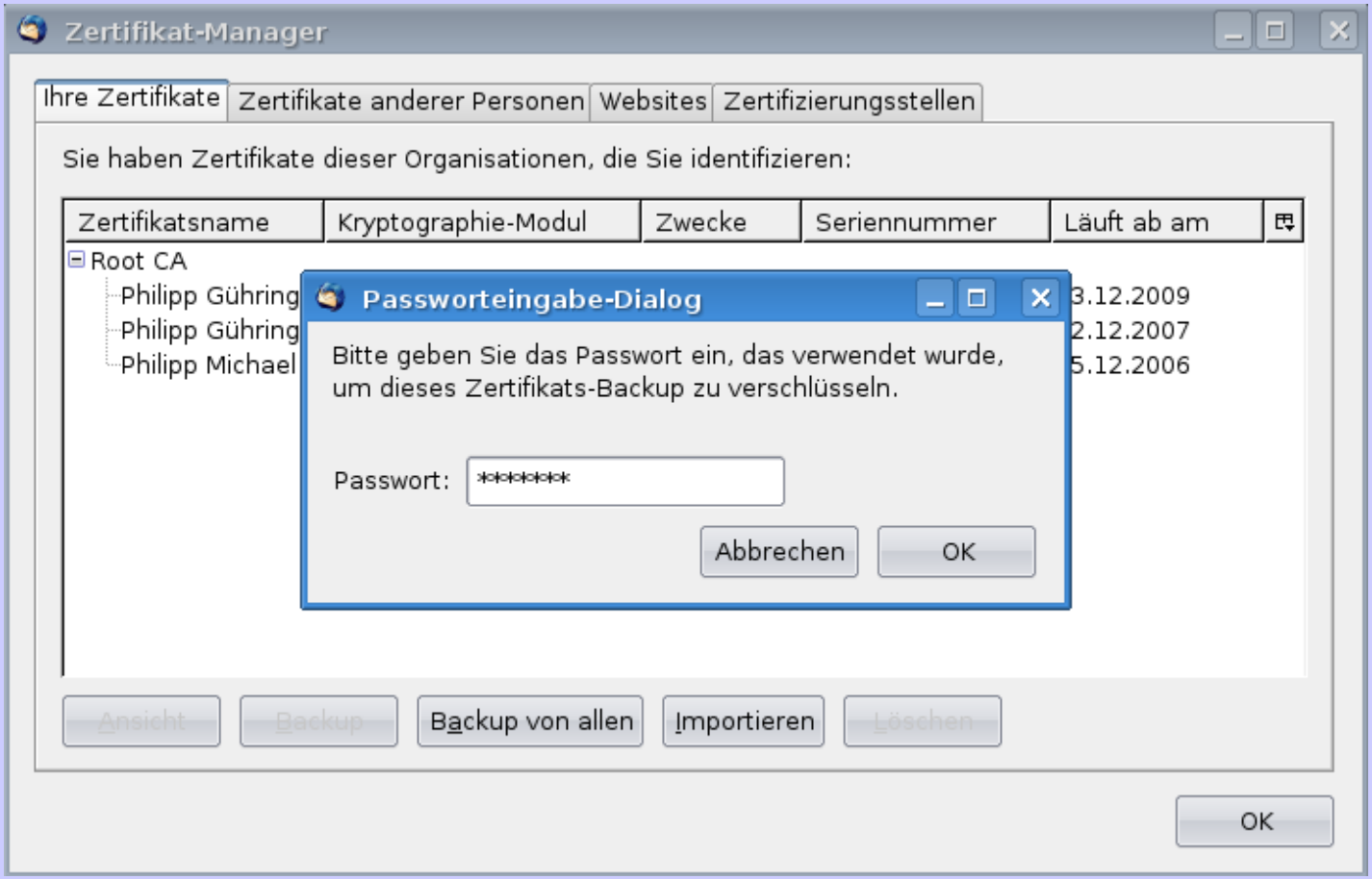
Datei auswählen



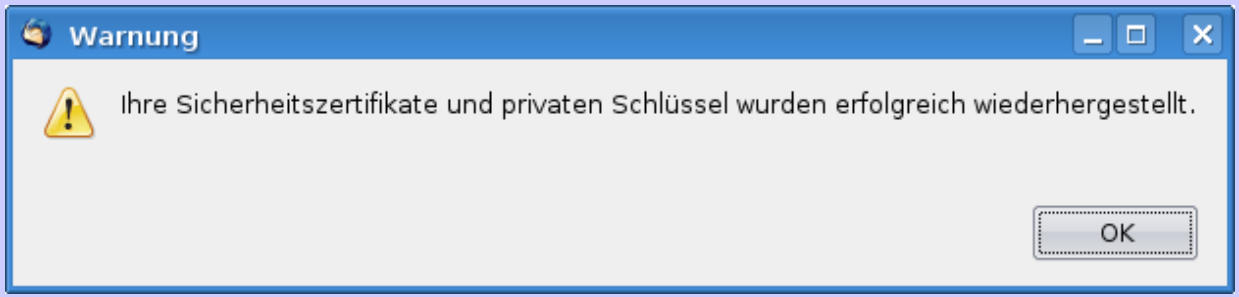
Thunderbird Master Passwort



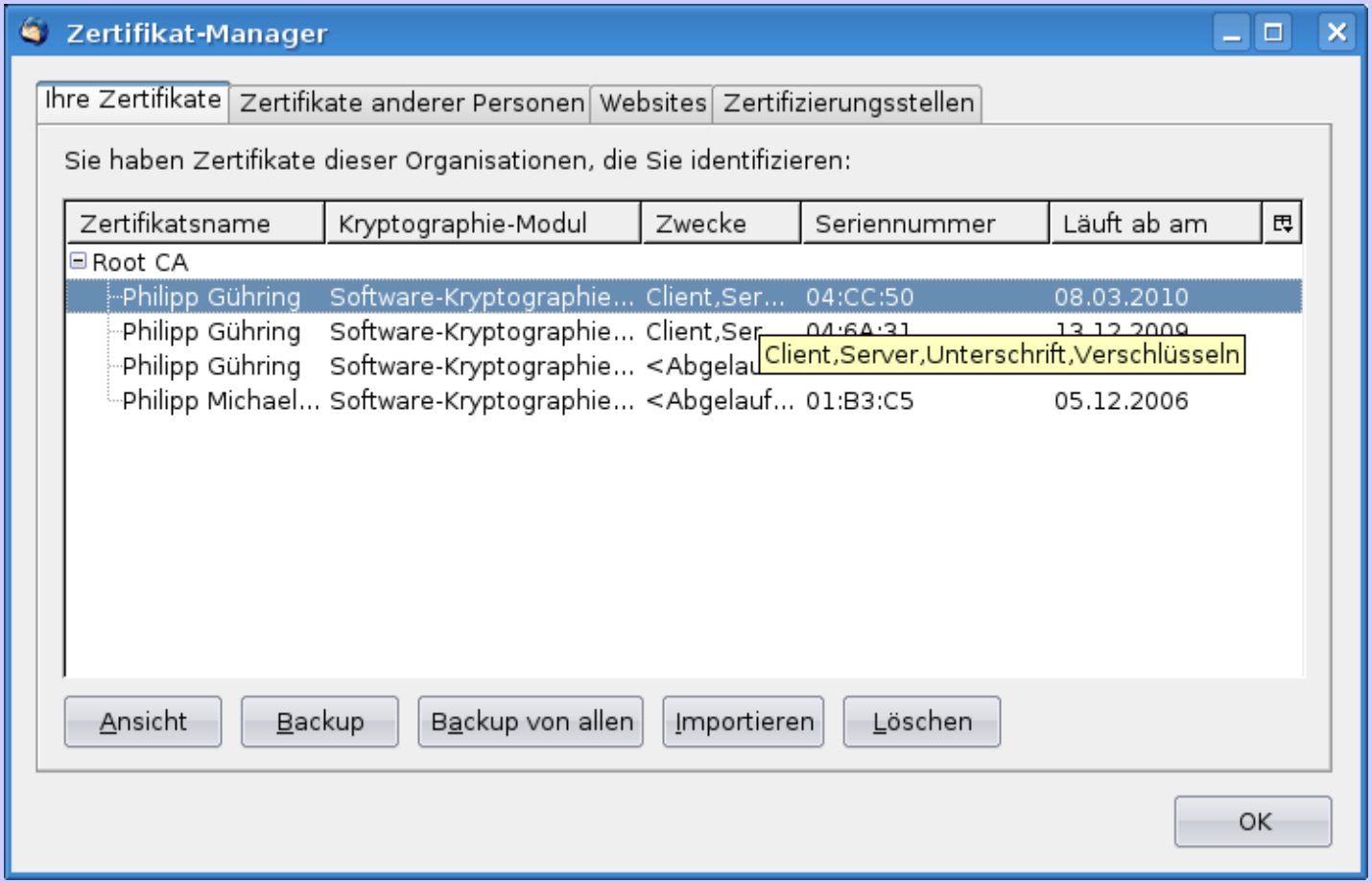
Passwort für das Zertifikat



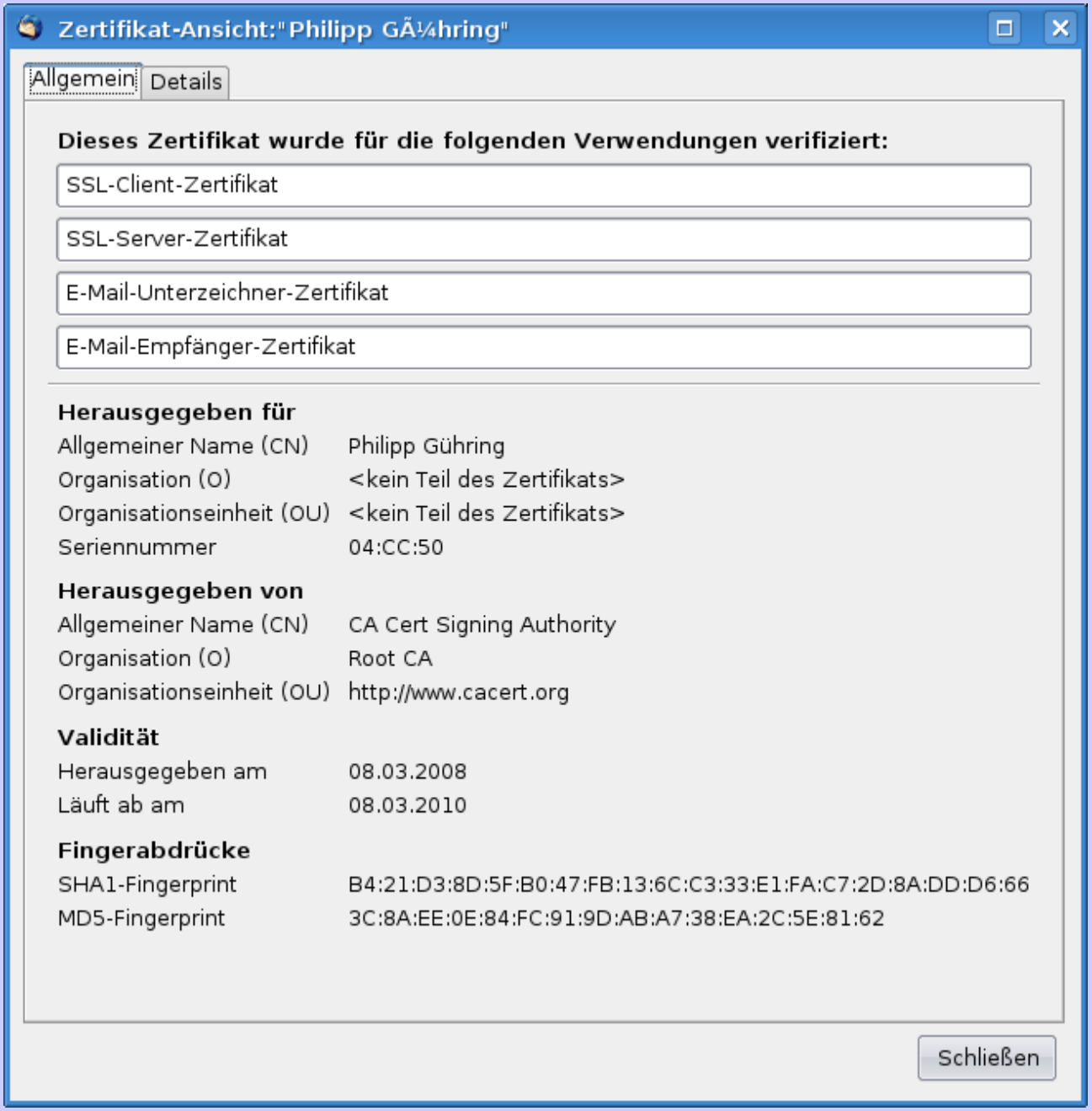
Import erfolgreich



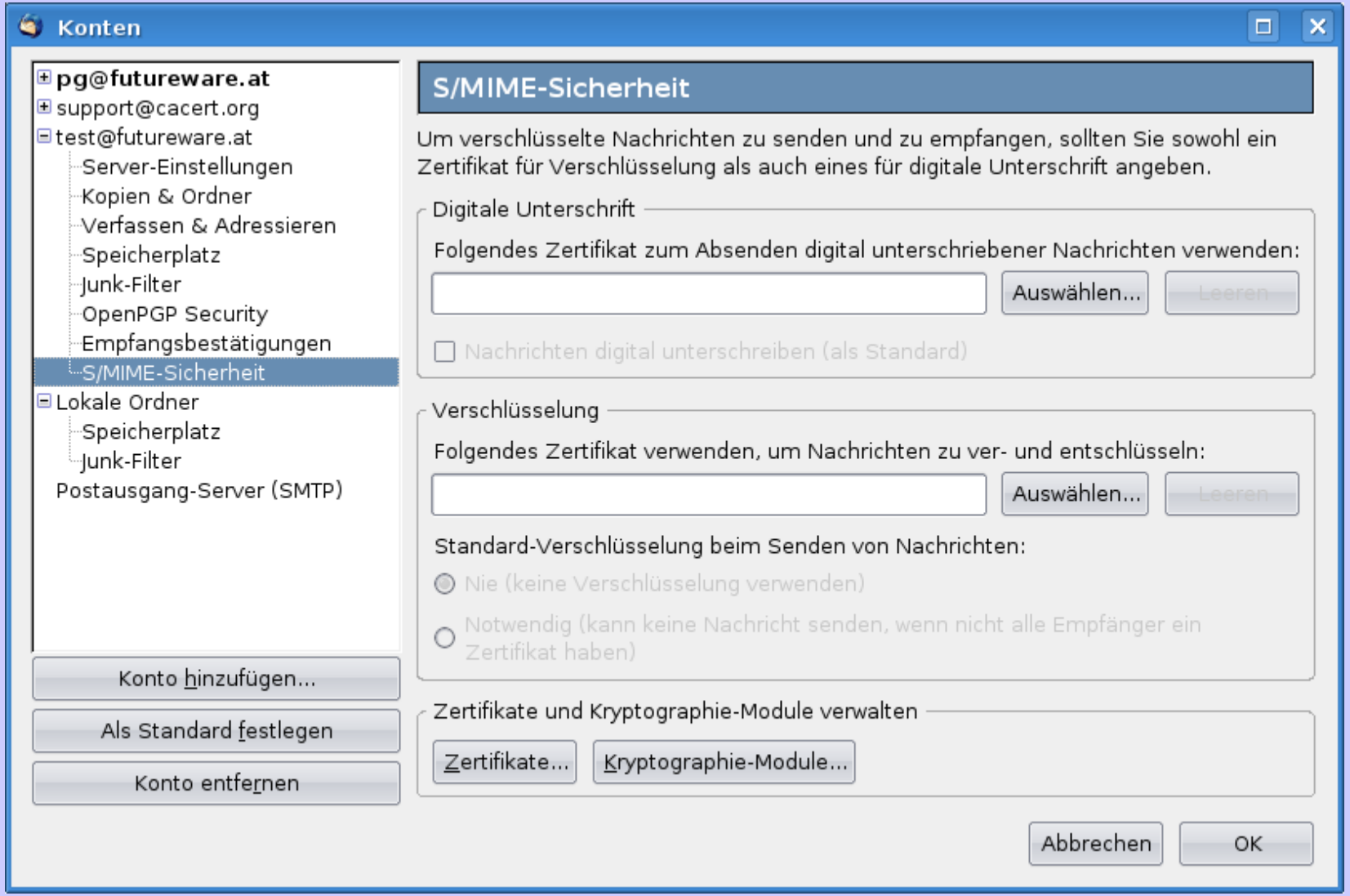
Da ist es


Zertifikat-Manager
Ihre Zertifikate
Zertifikate anderer Personen
Websites
Zertifizierungsstellen
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:
Zertifikatsname
Kryptographie-Modul
Zwecke
Seriennummer
Läuft ab am
Root CA
Philipp Gühring Software-Kryptographie... Client,Ser... 04:CC:50 08.03.2010
Philipp Gühring Software-Kryptographie... Client,Ser... 04:6A:31 13.12.2009
Philipp Gühring Software-Kryptographie... <Abgelau
Philipp Michael... Software-Kryptographie... <Abgelauf... 01:B3:C5 05.12.2006
Client,Server,Unterschrift,Verschlüsseln
Ansicht
Backup
Backup von allen
Importieren
Löschen
OK

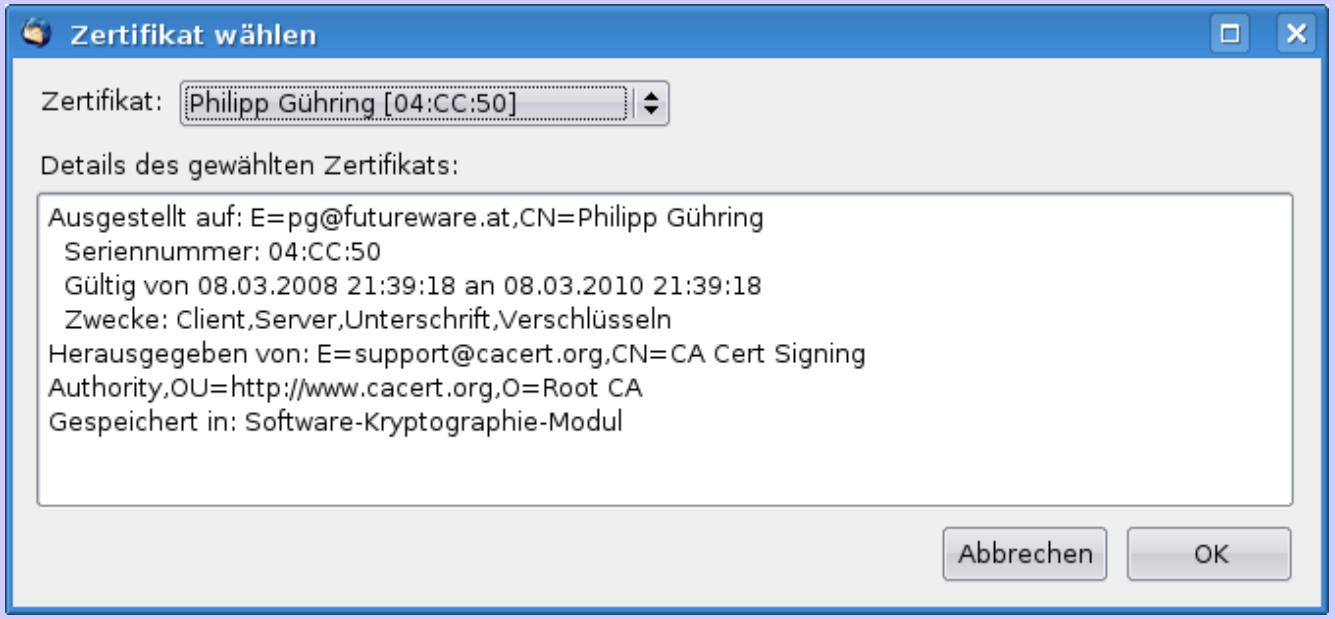
Zertifikat Detailansicht



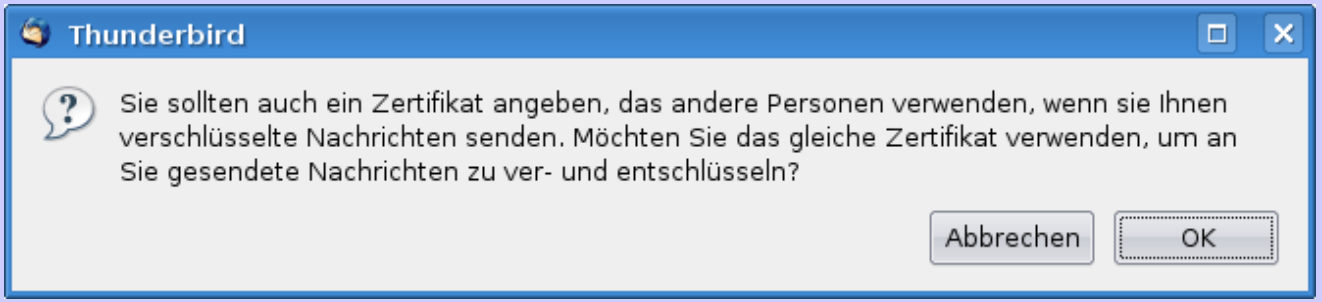
Email-Konten Einstellung



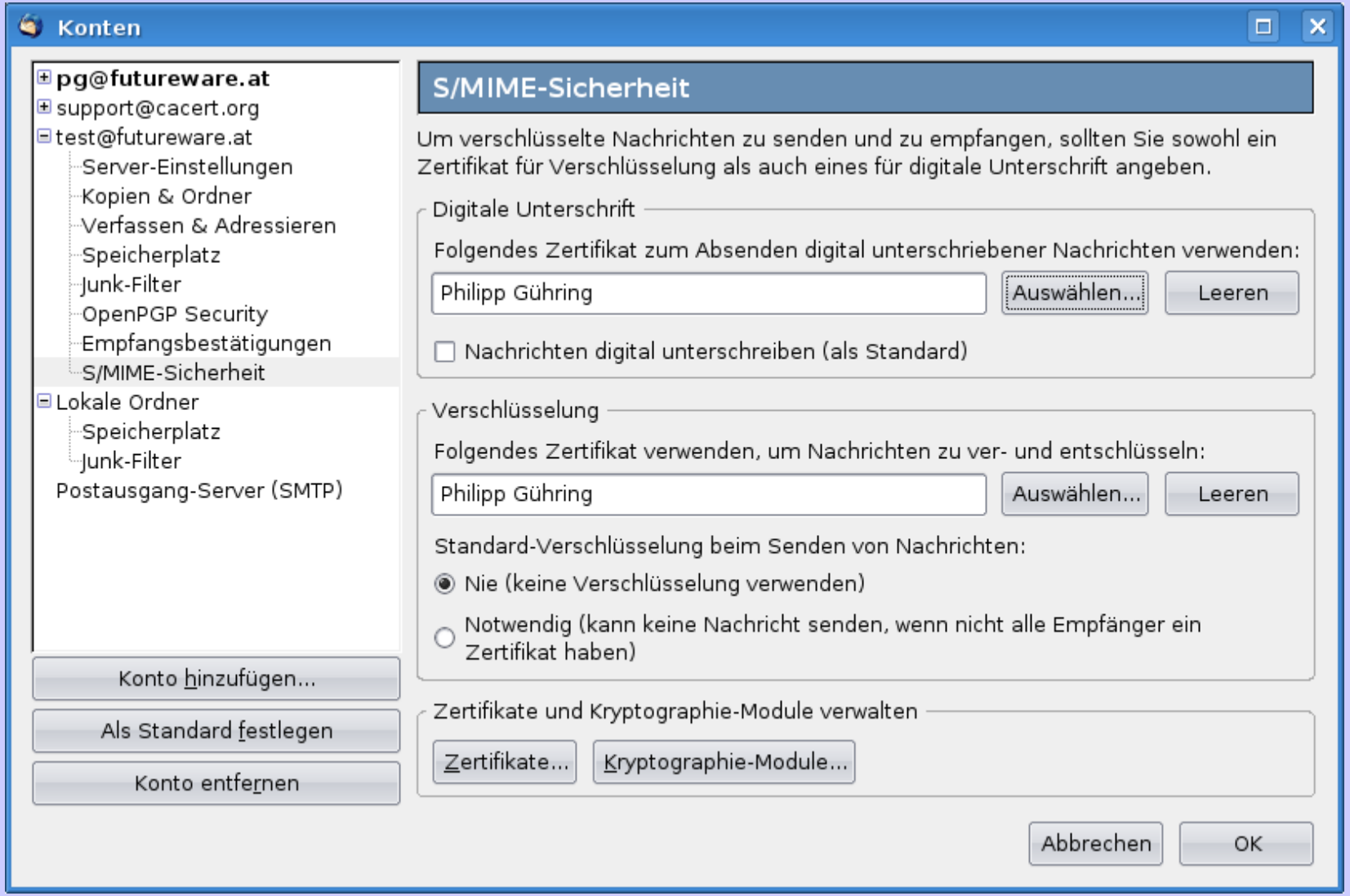
Auswahl des Zertifikats



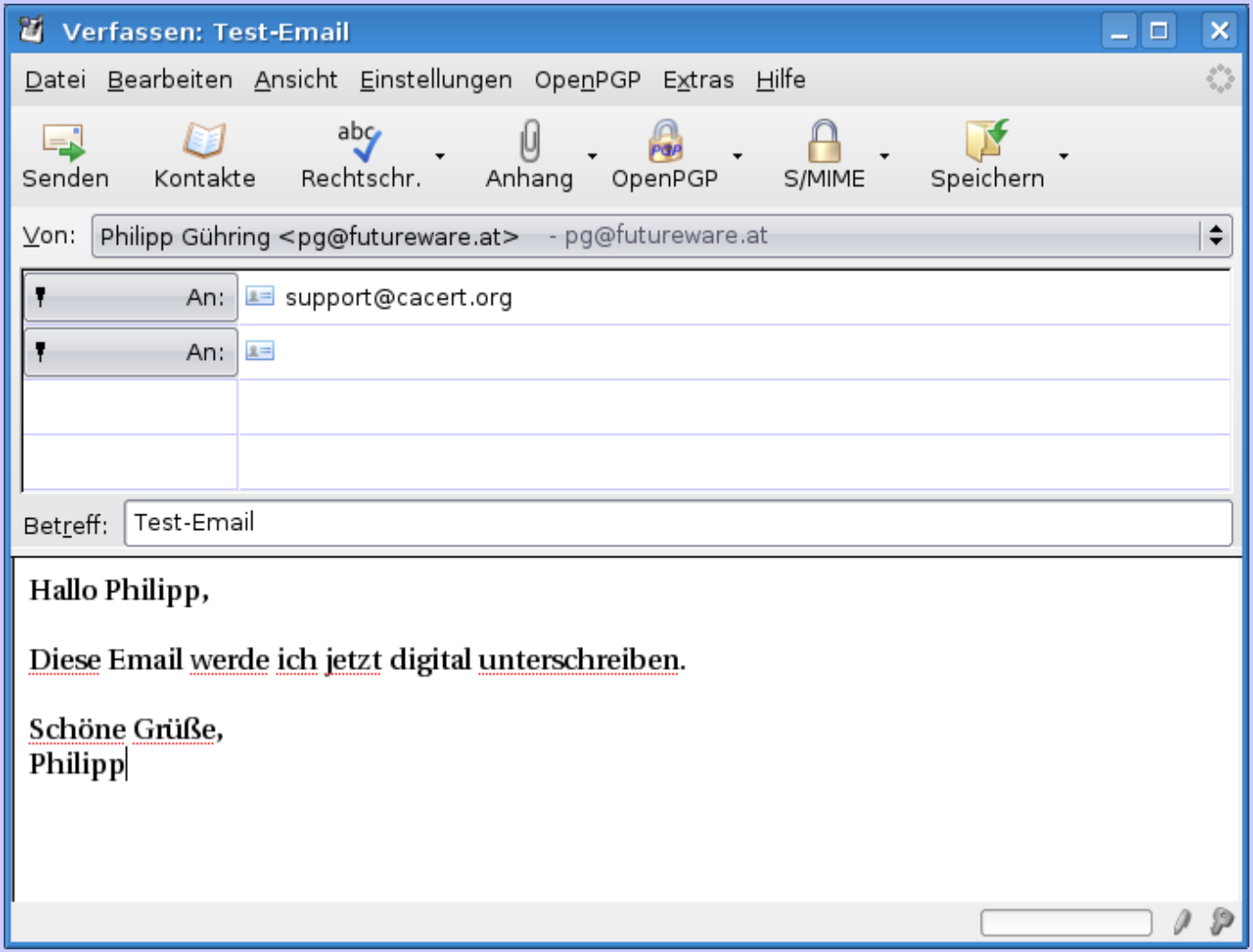
Übernahme


Thunderbird
Sie sollten auch ein Zertifikat angeben, das andere Personen verwenden, wenn sie Ihnen verschlüsselte Nachrichten senden. Möchten Sie das gleiche Zertifikat verwenden, um an Sie gesendete Nachrichten zu ver- und entschlüsseln?
Abbrechen
OK

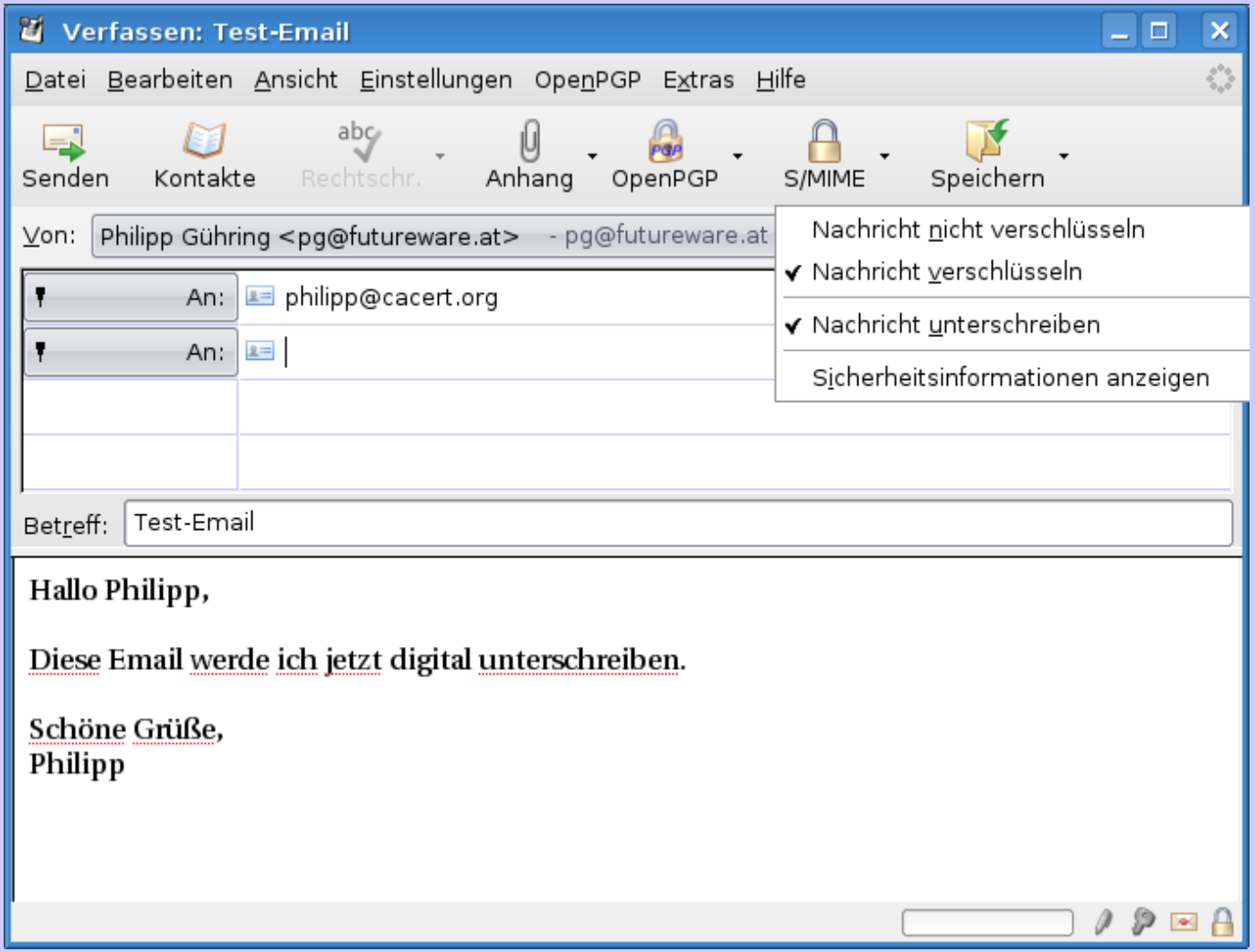
Zertifikat ist zugewiesen



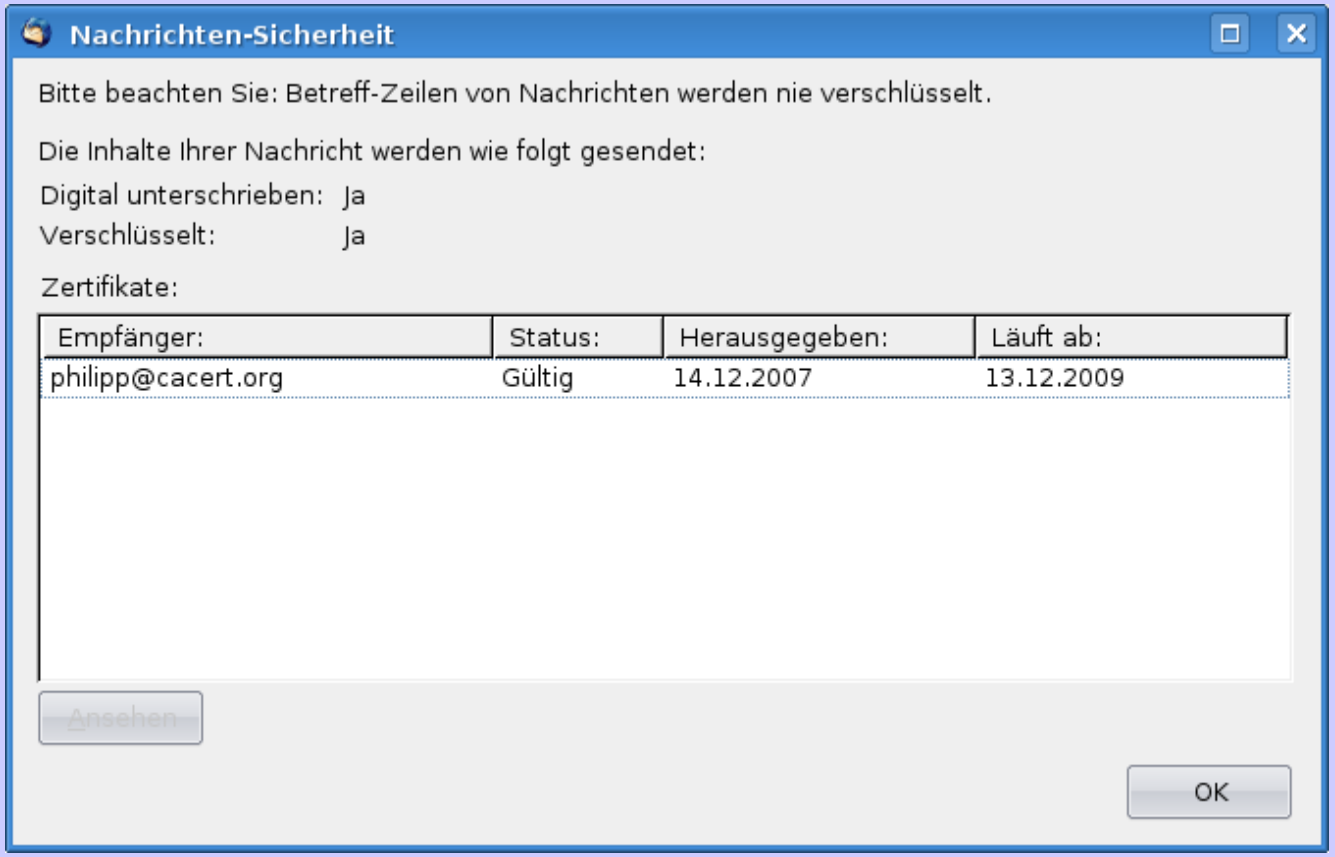
Email schreiben



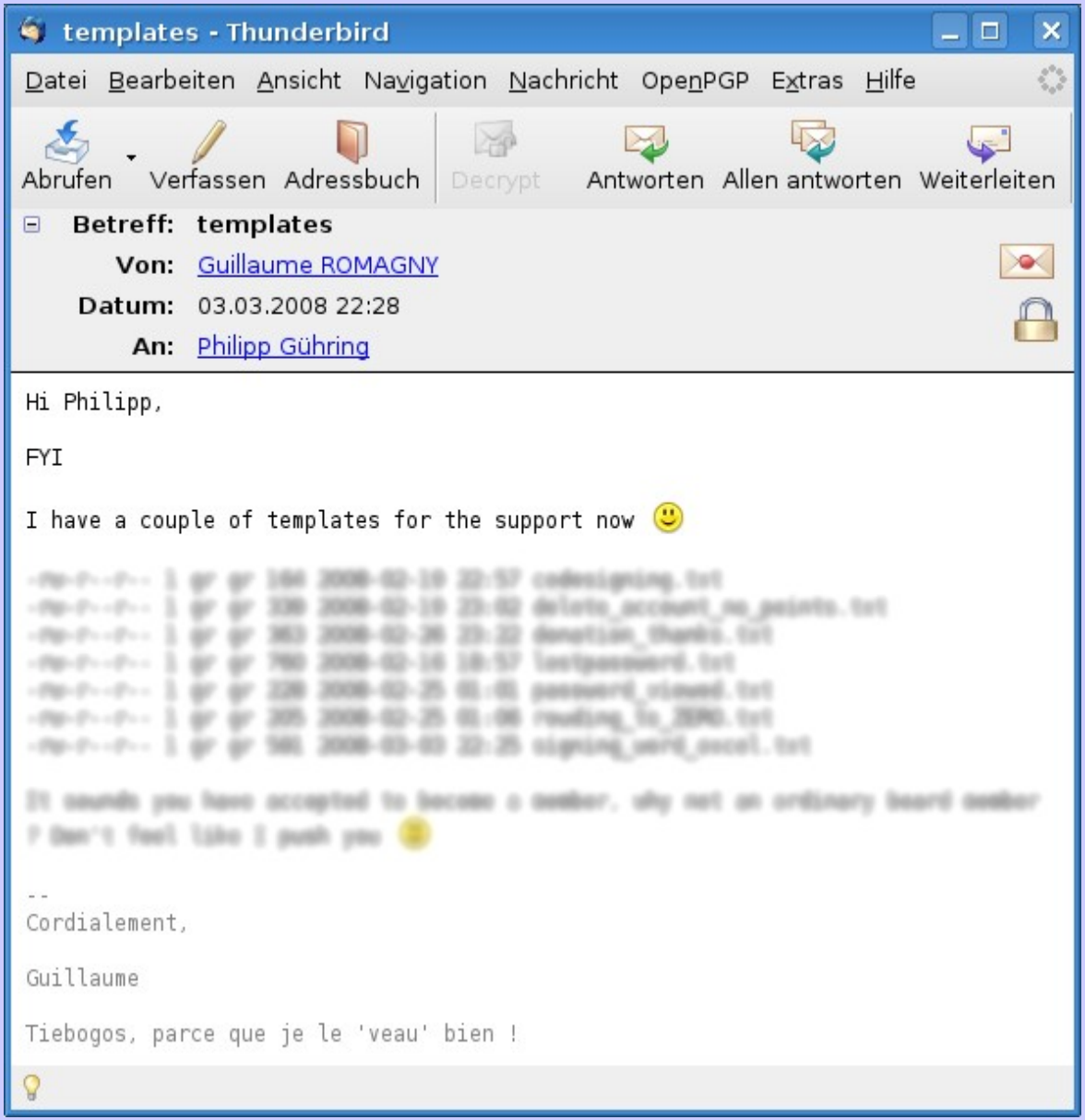
Email unterschreiben und verschl.



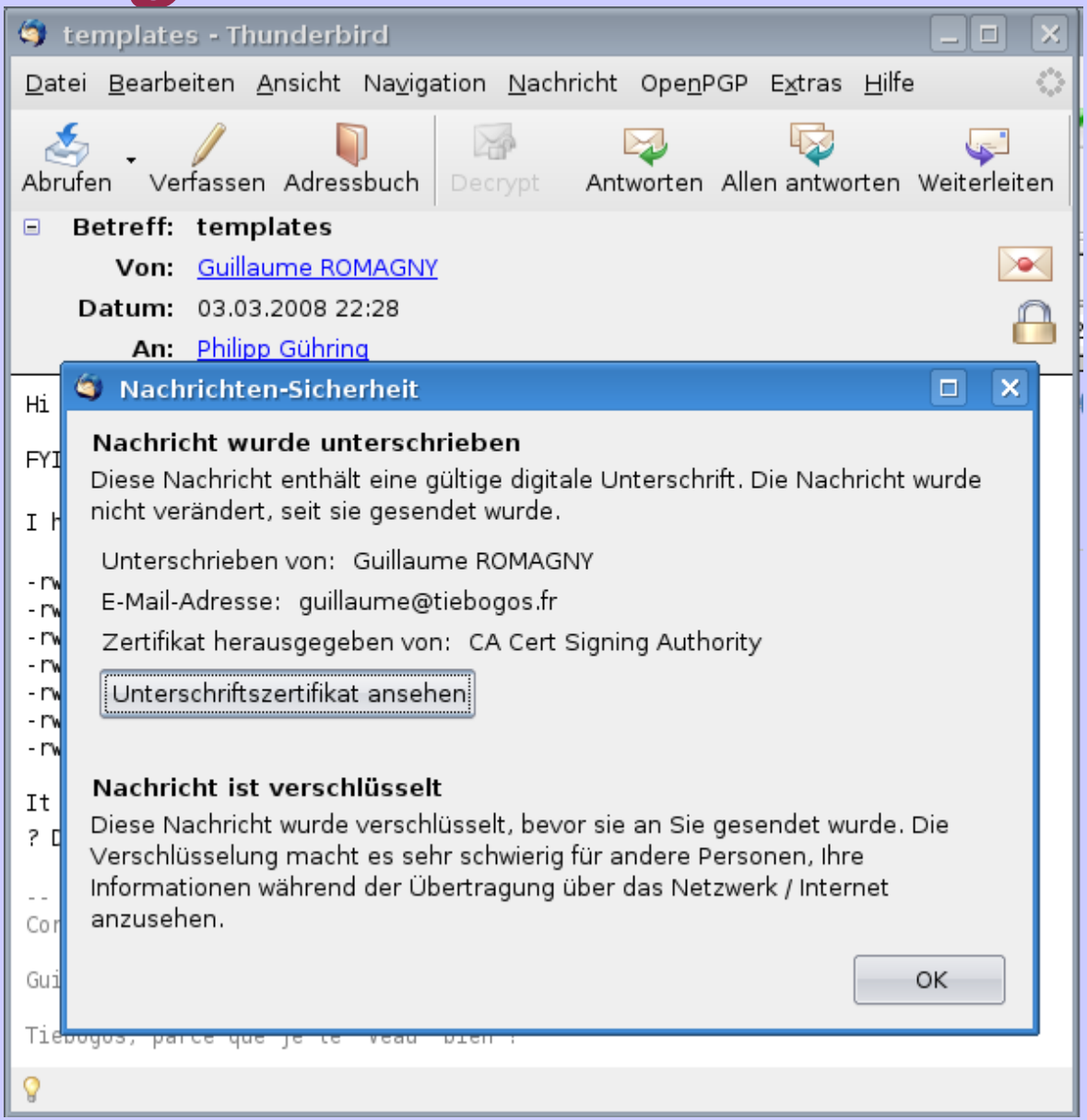
Sind die Zertifikate aller Empfänger vorhanden?



Empfangen einer verschlüsselten Email:



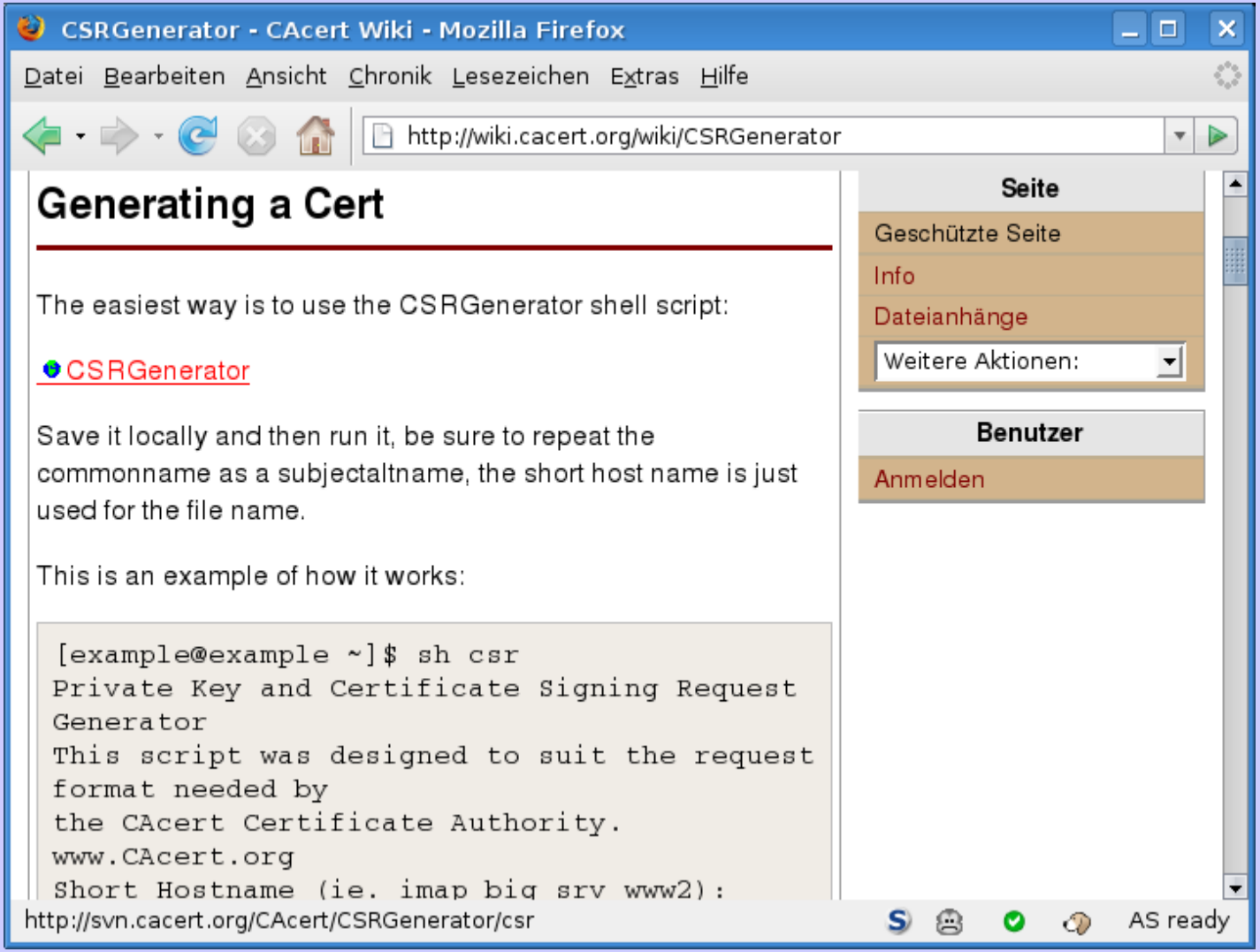
Signator kontrollieren



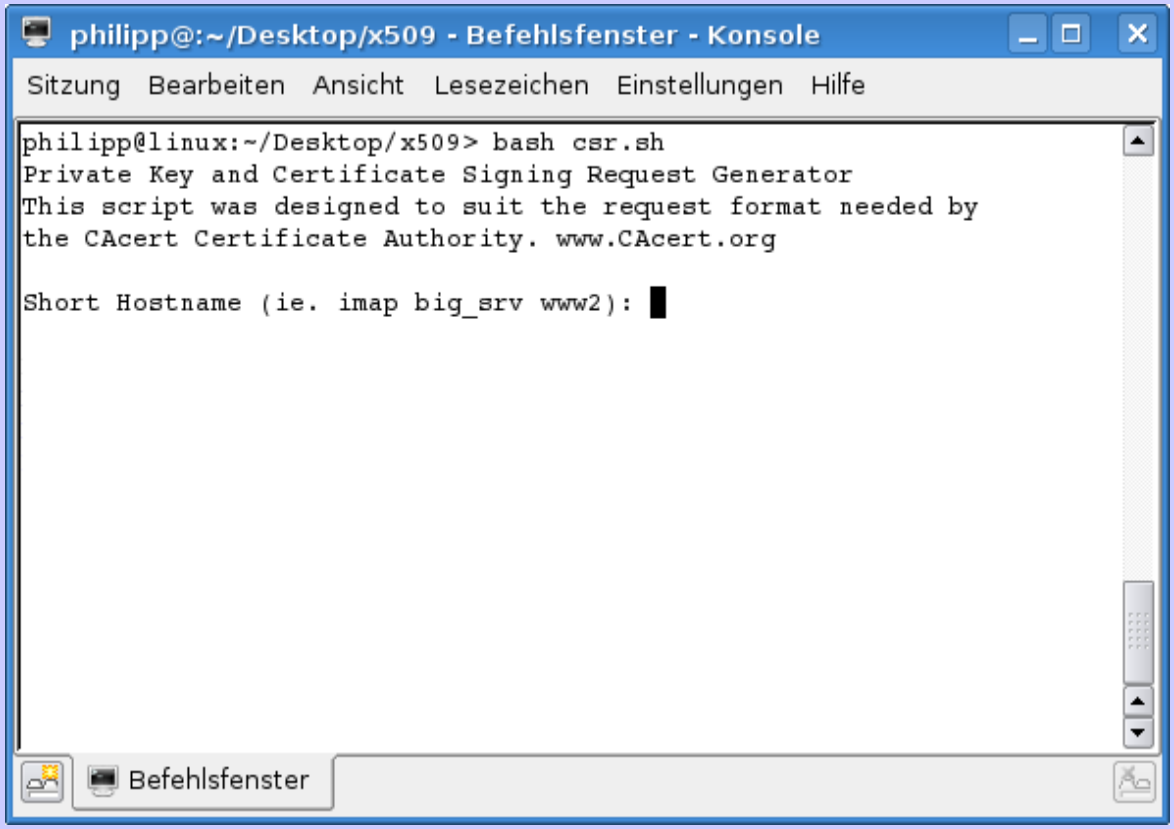
Server Zertifikat in der Praxis

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

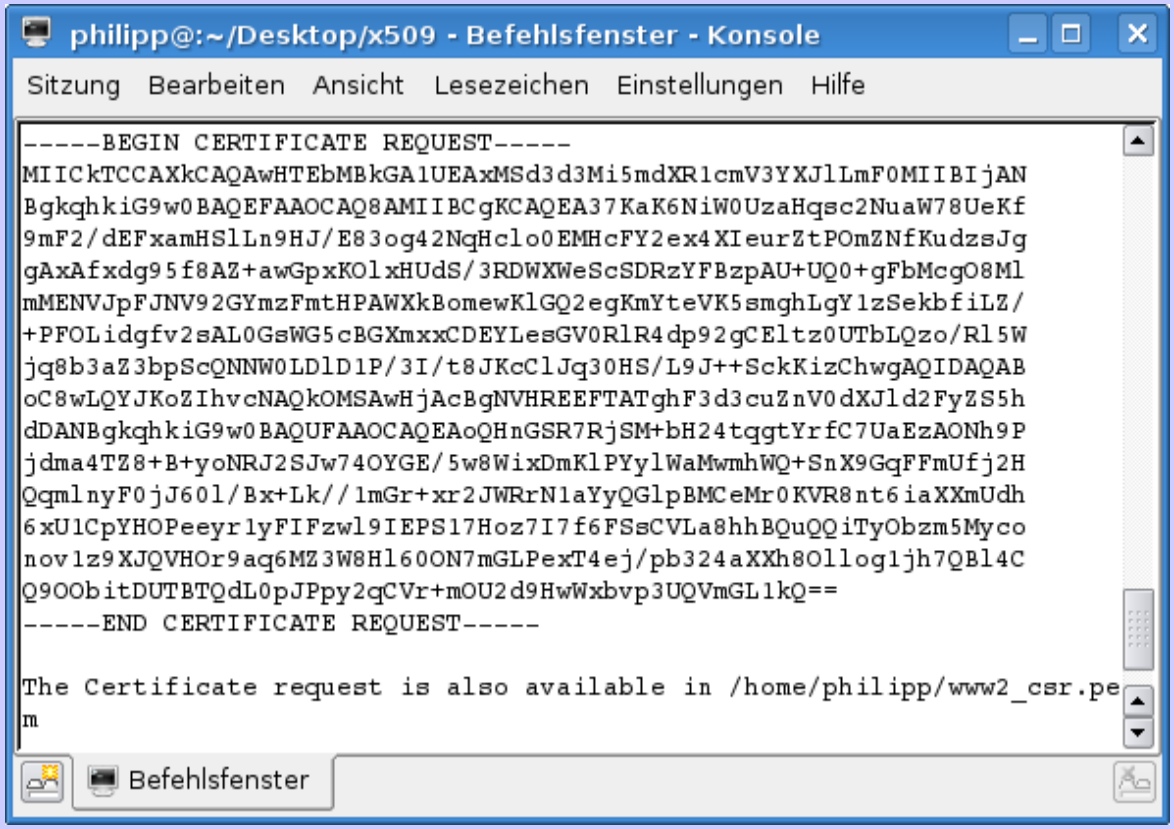
Zertifikatsgenerator



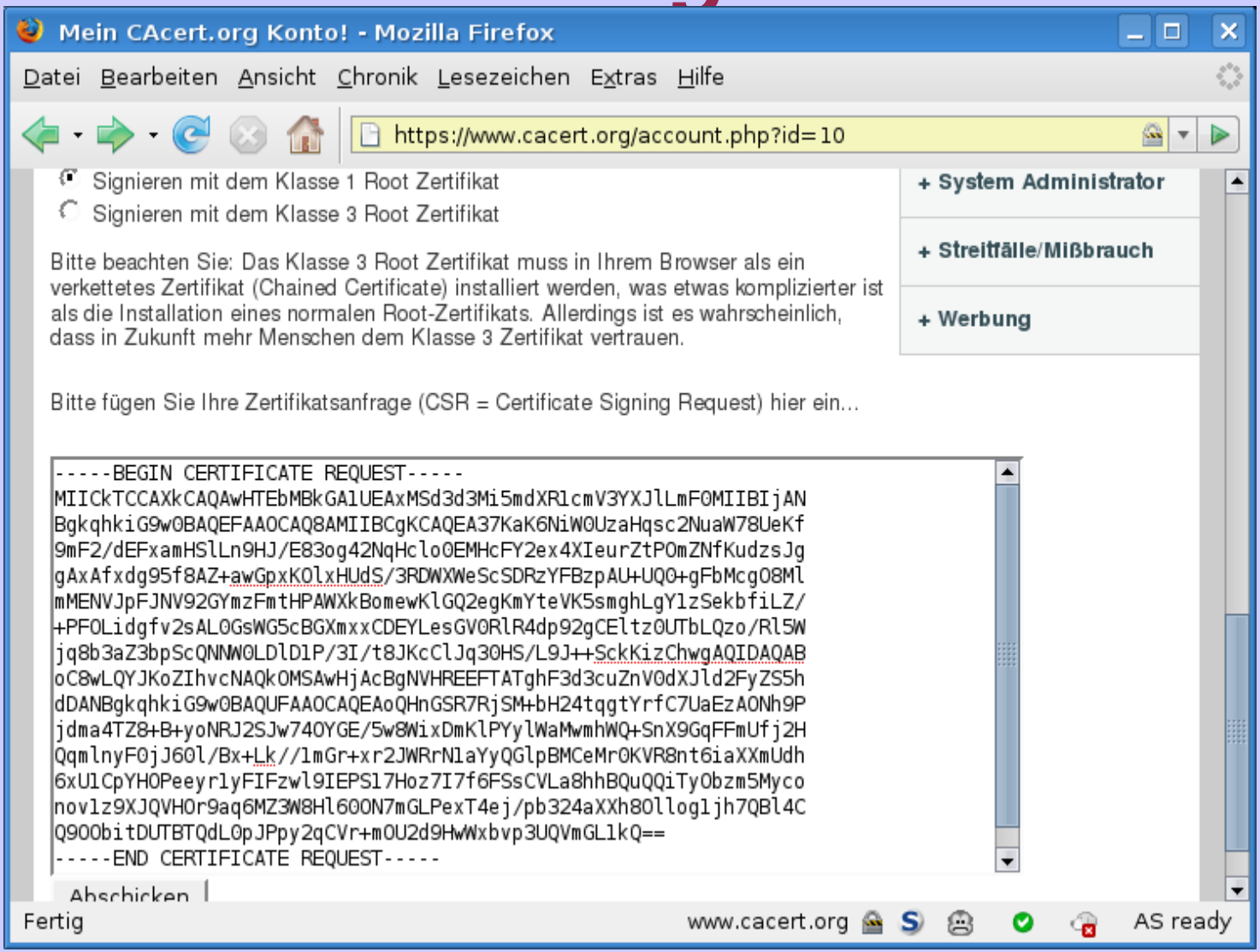
Zertifikatsgenerator



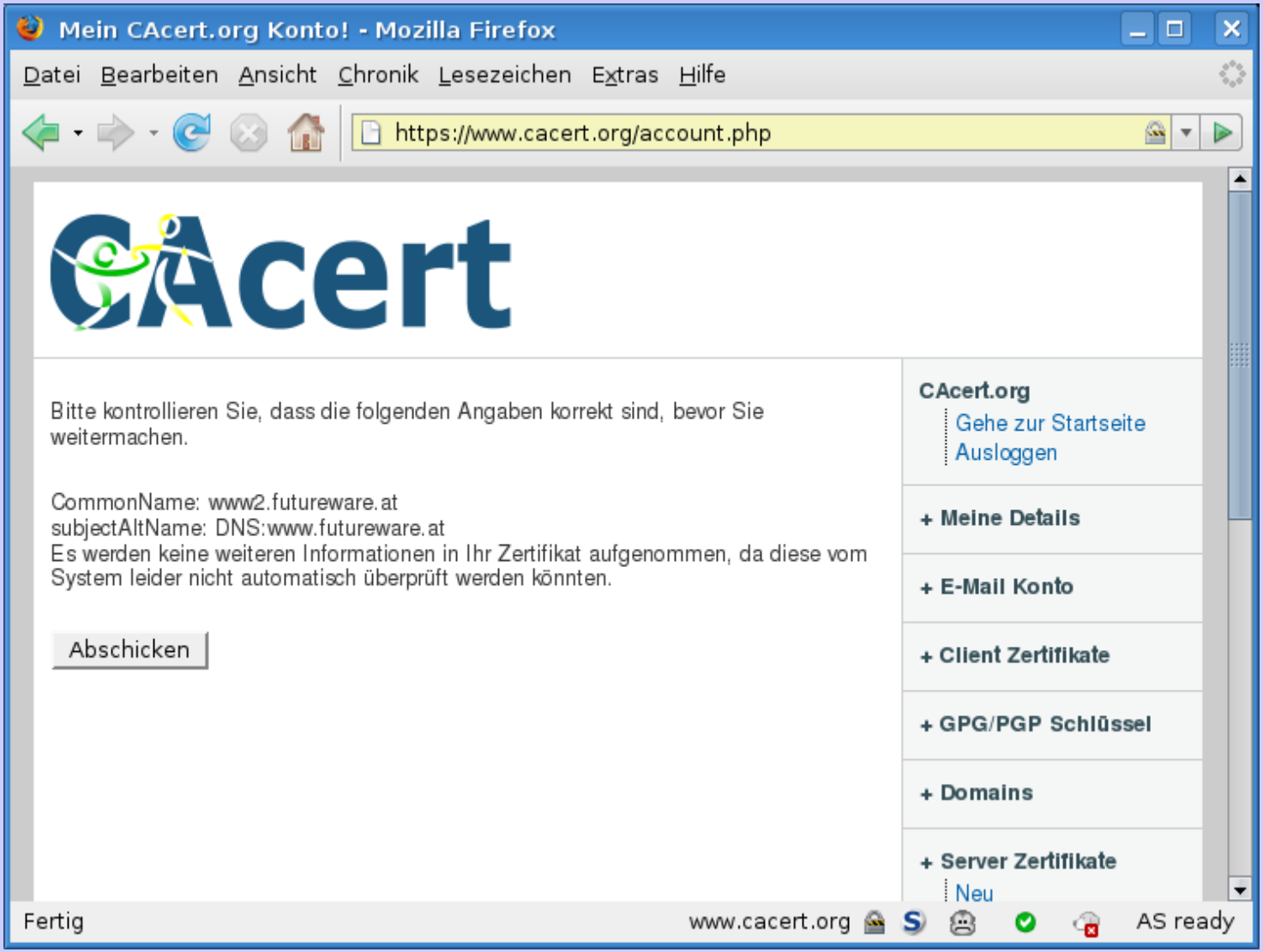
CSR Zertifikatsanfrage



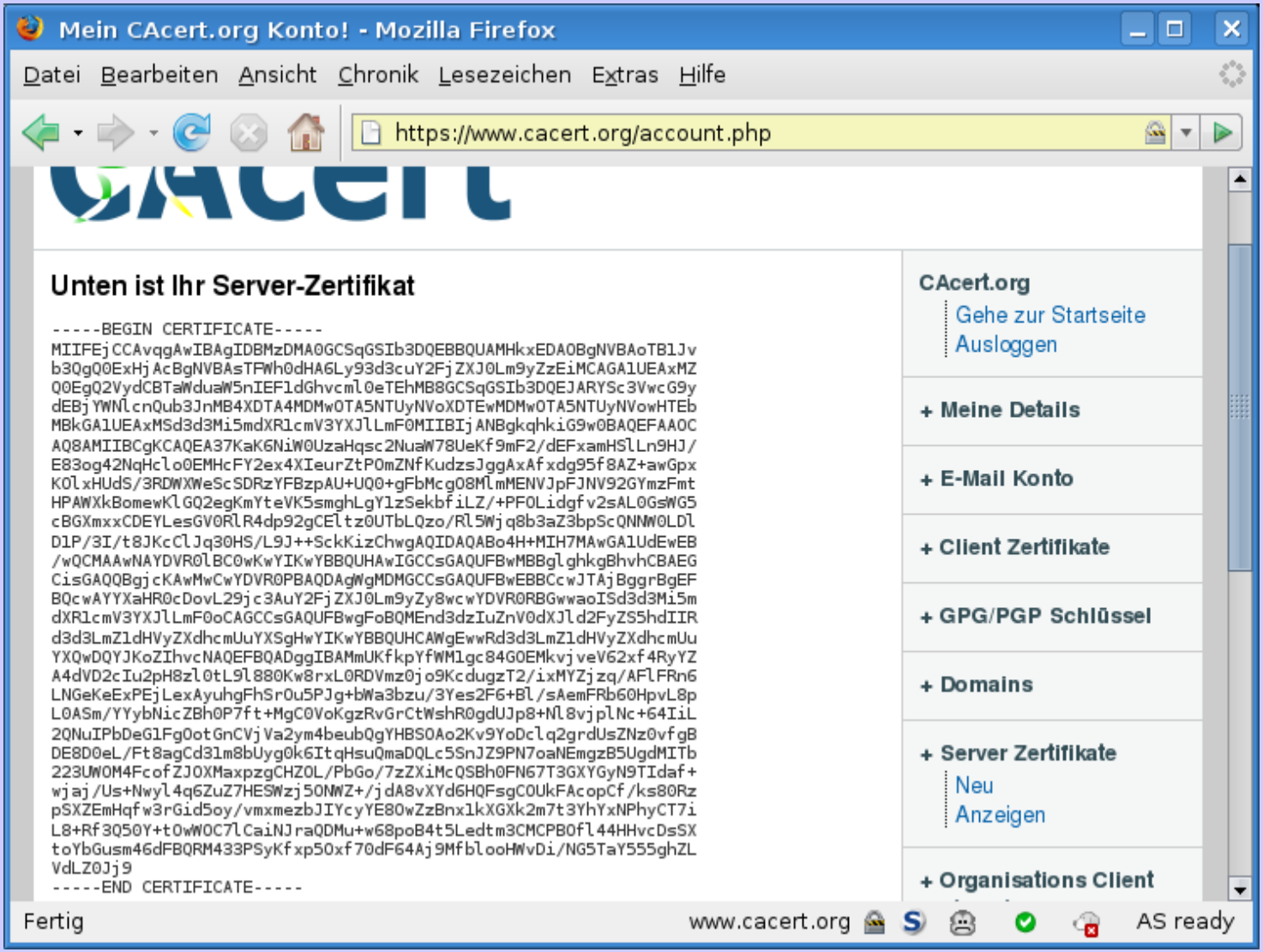
Zertifikatsanfrage zu CAcert



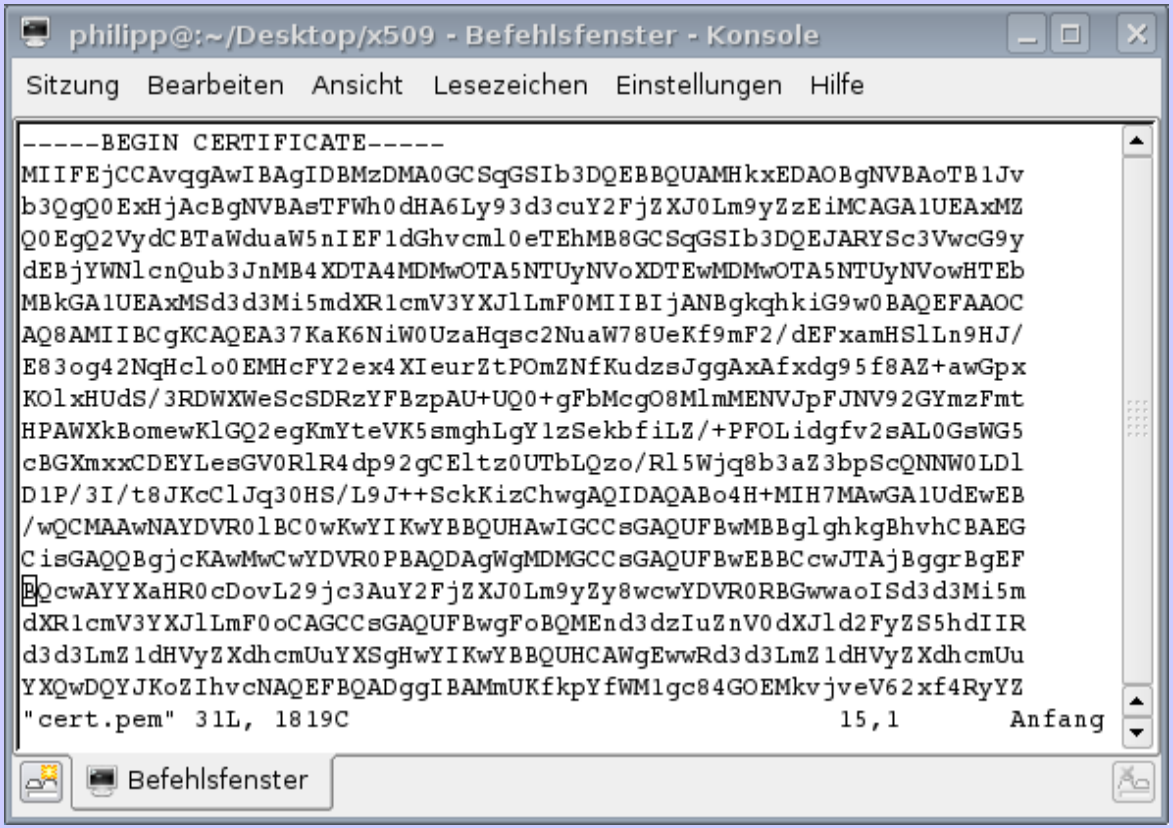
Kontrolle


Mein CAcert.org Konto! - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://www.cacert.org/account.php
CAcert
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.
Abschicken
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

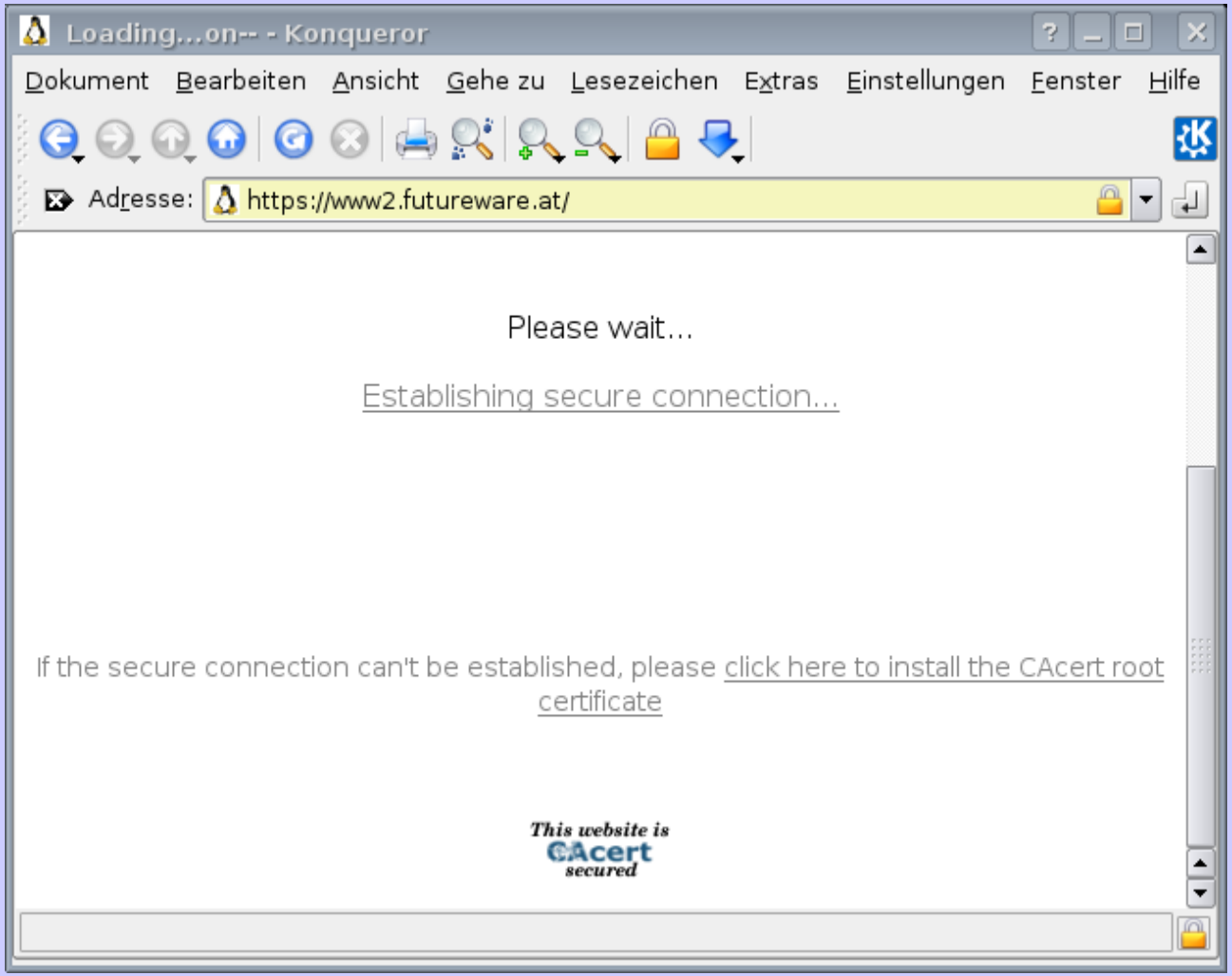
Fertiges Zertifikat



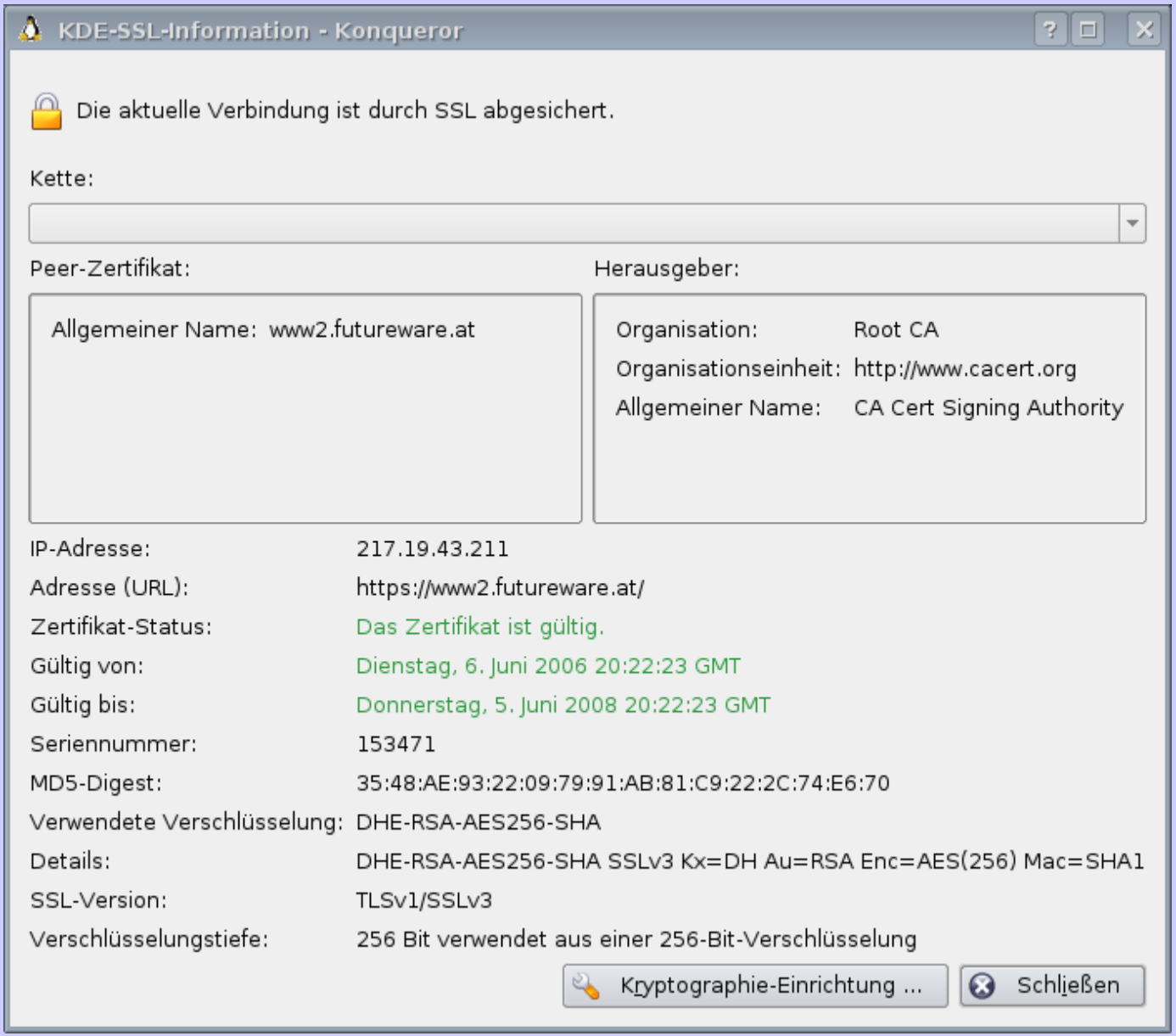
Zertifikat in Datei speichern



Zertifikat im Webserver installiert



Zertifikatsdetails



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?