

IT-Security Bootcamp

Michael Lück

FOSSLC e.V.

21.11.2013

Ich doch hab' nichts zu verbergen

- Dann muss mich auch niemand überwachen!
- Regierungen definieren was richtig und falsch ist!
- Was heute richtig ist, kann morgen falsch sein!
- Ich kann nicht kontrollieren, was mit meinen Daten passiert!

Quis custodiet custodes ipsos?

Wer überwacht die Überwacher?

Lesenswert: [3]

Ziel

- Niemand soll meine Emails verändern können
→ **Integrität**
- Niemand außer mir kann in meinem Namen Emails versenden
→ **Authentizität**
- Niemand außer mir soll meine Emails lesen können
→ **Vertraulichkeit**

Diese Anforderungen werden auch als Sicherheitsziele bezeichnet

Was also tun?

Kryptographie

Informationssicherheit [5]

symmetrisch

- einzelner Schlüssel für beide Partner
- nur Vertraulichkeit & Integrität umsetzbar
- effizient

asymmetrisch

- Schlüsselpaar für jeden Partner
- alle Sicherheitsziele umsetzbar
- aufwendig

asymmetrische Kryptographie

Zwei Schlüssel

Was der eine verschlüsselt kann nur der andere entschlüsseln
→ Asymmetrie

- ein Schlüssel wird veröffentlicht
- der andere Schlüssel wird geheim gehalten

asymmetrische Kryptographie

- Absender verschlüsselt mit öffentlichem Schlüssel des Empfängers
→ Nur Empfänger kann öffnen
→ **Vertraulichkeit**
- Absender verschlüsselt mit seinem privatem Schlüssel
→ jeder kann Entschlüsseln
→ nur der Absender kann es verschlüsselt haben
→ **Authentizität**
- Nachricht wird unterwegs verändert
→ beim Entschlüsseln entsteht nur Müll
→ **Integrität**

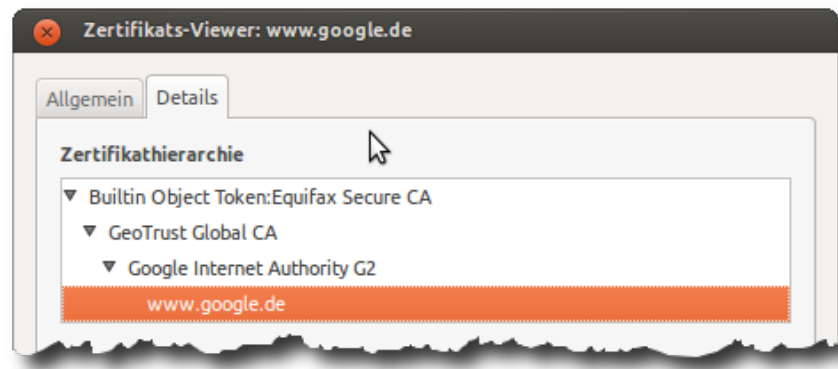
Vertrauen

- ein Schlüsselpaar ist immer einer Identität zugeordnet
- öffentliche Schlüssel müssen verteilt werden
 - mit E-Mail mitschicken
 - von Servern abrufen
 - bei Kommunikation austauschen
 - ...
- Zugehörigkeit muss überprüfbar sein
→ Vertrauensmodelle
 - hierarchisch (X.509)
 - netzförmig (PGP)

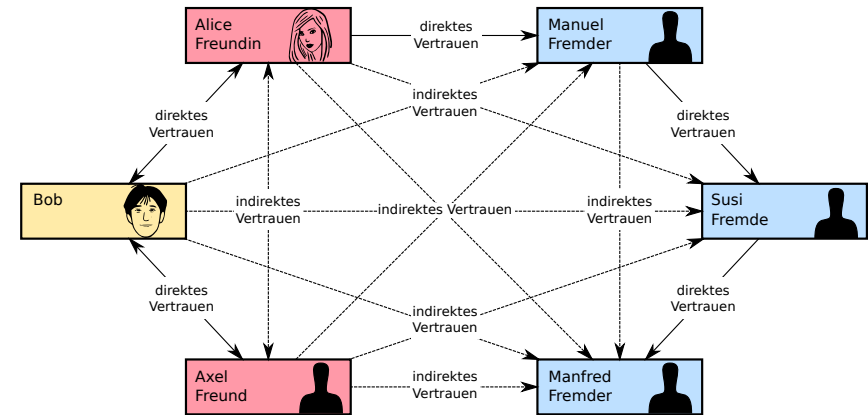
Vertrauensmodelle

- hierarchisch
 - ähnlich Notar
 - Notar bestätigt Zugehörigkeit von Schlüssel zu Person, Server, etc.
→ Zertifikat von Zertifizierungsstelle (CA)
 - Zertifikat wird bei Kommunikation immer mitgeschickt
 - Empfänger kennt Unterschrift des Notars
→ kann Zugehörigkeit prüfen
 - verbreitetes Verfahren
- netzförmig
 - ähnlich einem Social-Graph
 - jeder kann jeden öffentlichen Schlüssel unterschreiben
→ Web-Of-Trust

Trust Chain



Web-Of-Trust



based on [2]

CACert

- <https://www.cacert.org>
- Mischung aus Web-Of-Trust und hierarchischem Modell
- Community Mitglieder vergeben untereinander Punkte
- Community betreibt Zertifizierungsstelle
- wenn Mitglied genug Punkte hat bekommt sie ein Zertifikat
- Zertifikate für EMail oder eigene Server möglich

Genug gelabert

- Schlüsselpaar erzeugen
- Public Key signieren lassen
- verschlüsselte, signierte Emails schreiben und empfangen
- CACert Root Zertifikat importieren

Schlüsselpaar erzeugen

Schlüssel erzeugen:

```
openssl genrsa -des3 -out fosslc.key 4096
```

Zertifikatsrequest erzeugen:

```
openssl req -new -key fosslc.key -out fosslc.csr
```

Zertifikat an CA schicken:

```
scp fosslc.csr fosslc@<Server IP>:/tmp
```

Signiertes Zertifikat in PKCS12 Format umwandeln

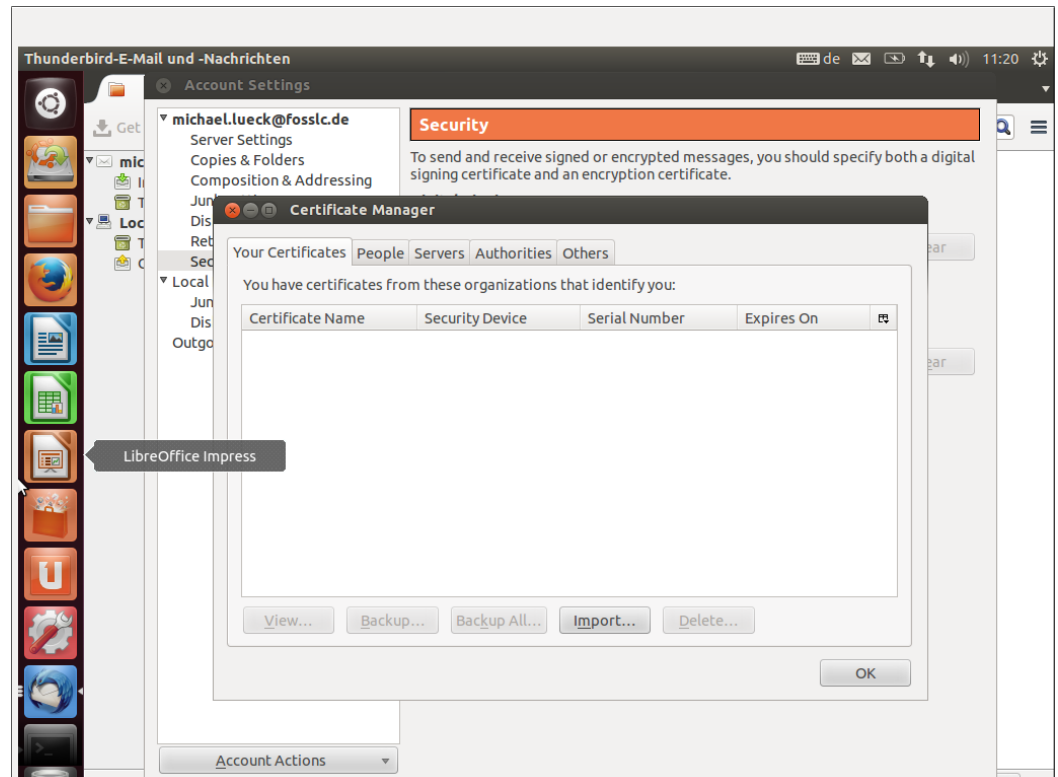
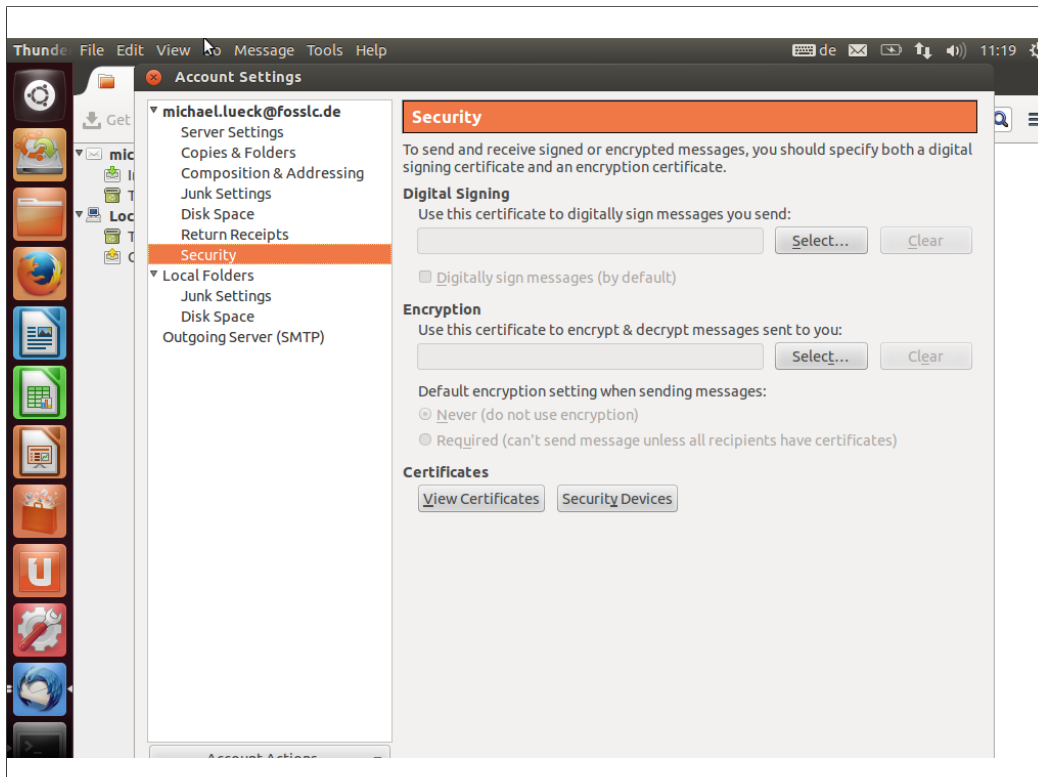
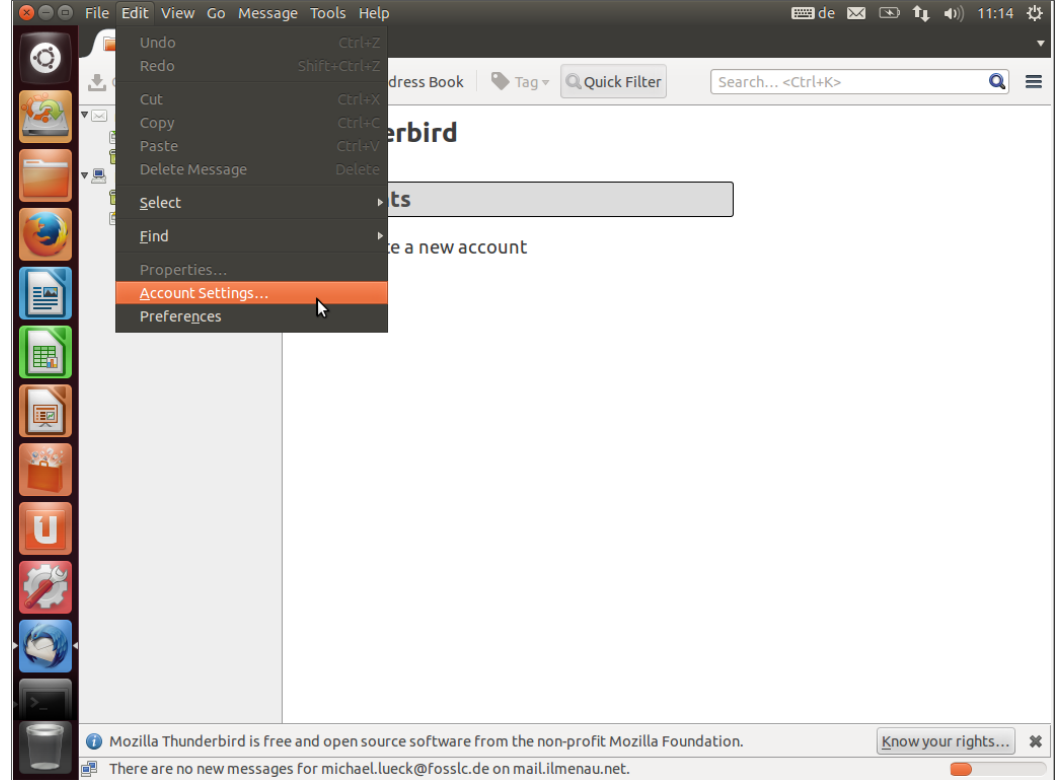
```
openssl pkcs12 -export -in fosslc.crt -inkey  
fosslc.key -out fosslc.p12
```

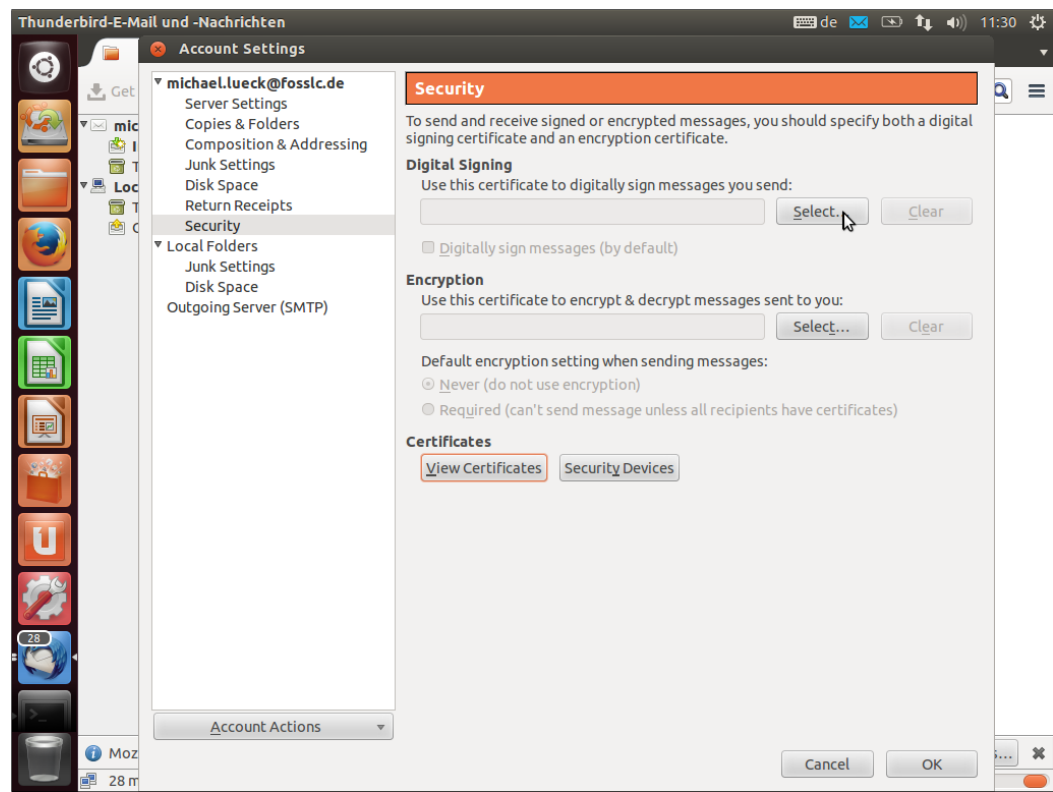
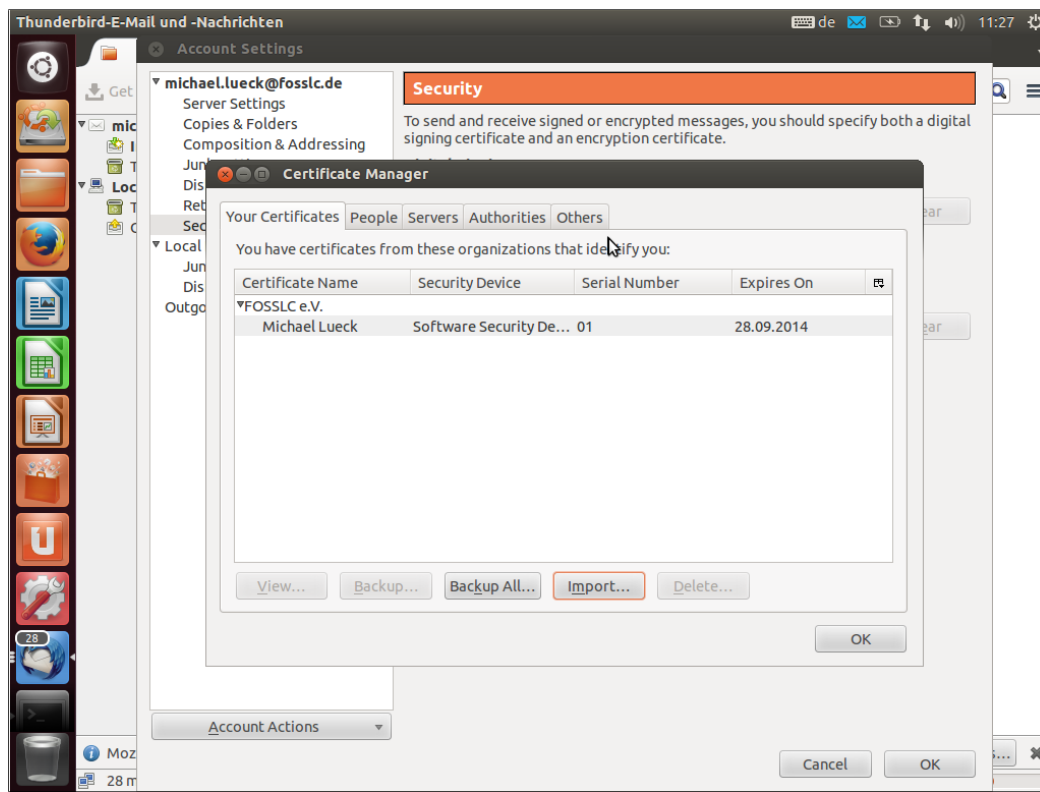
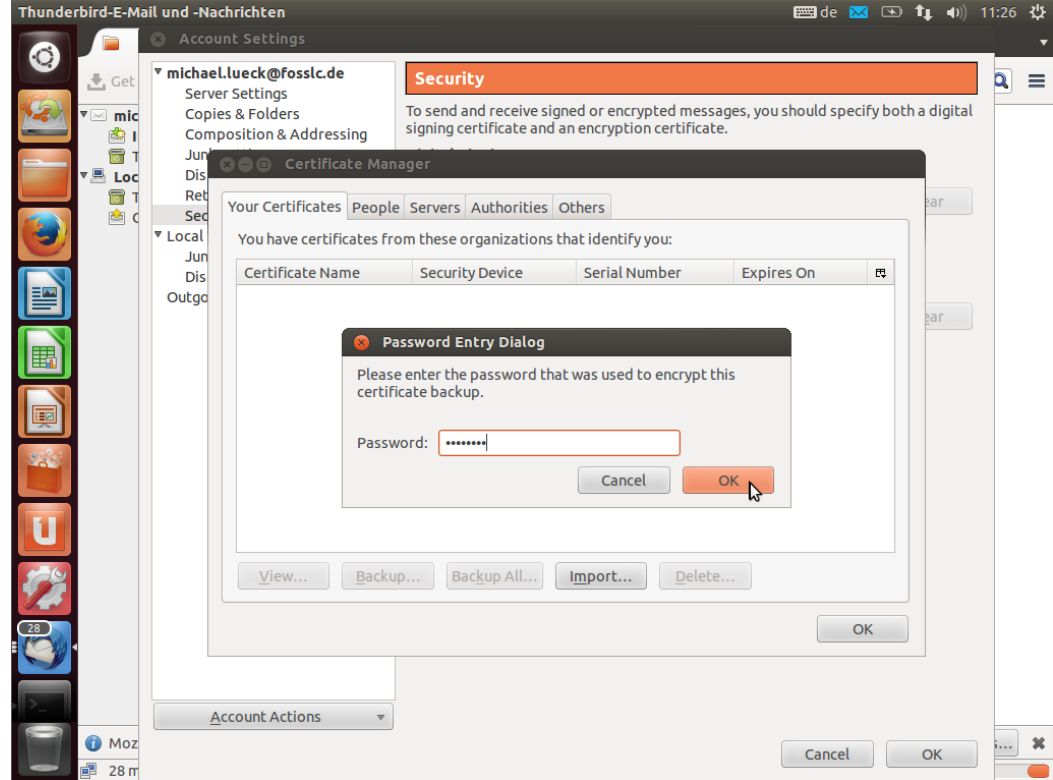
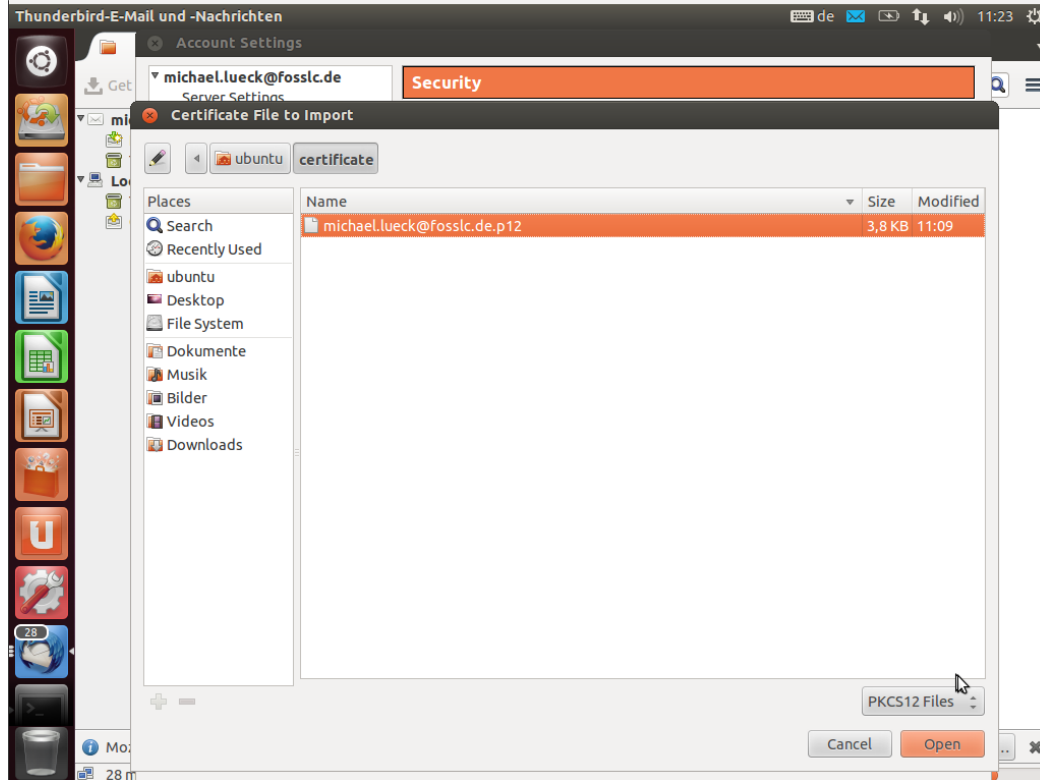
based on [4]

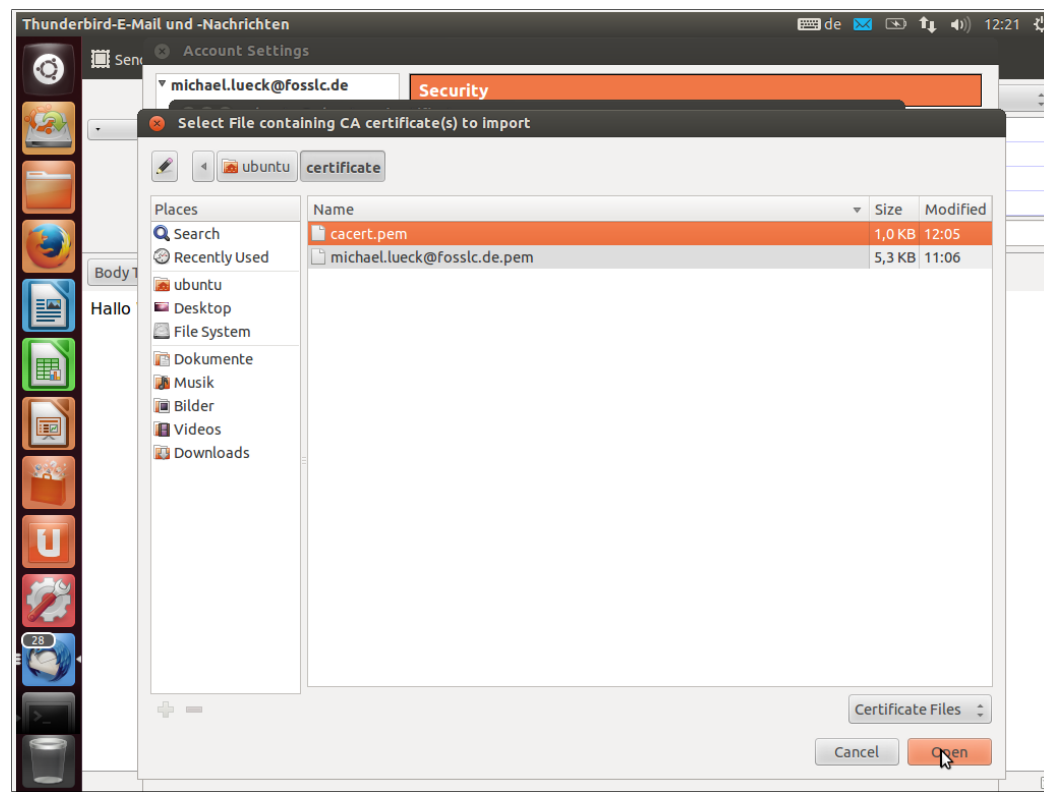
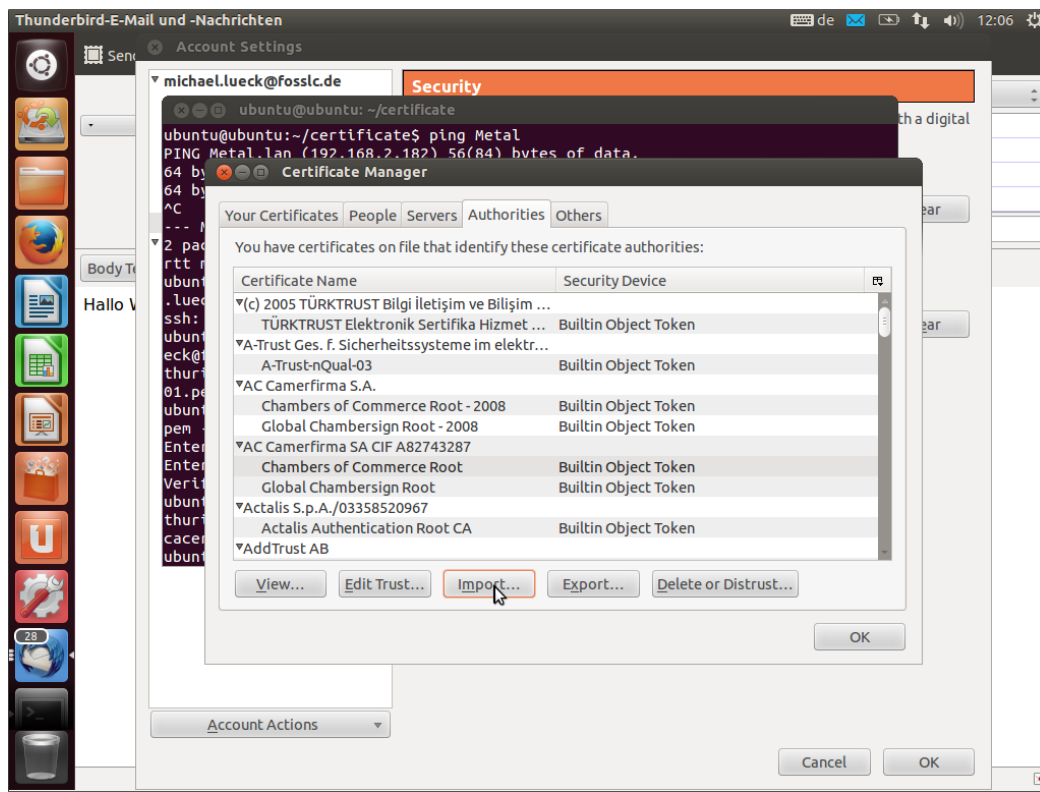
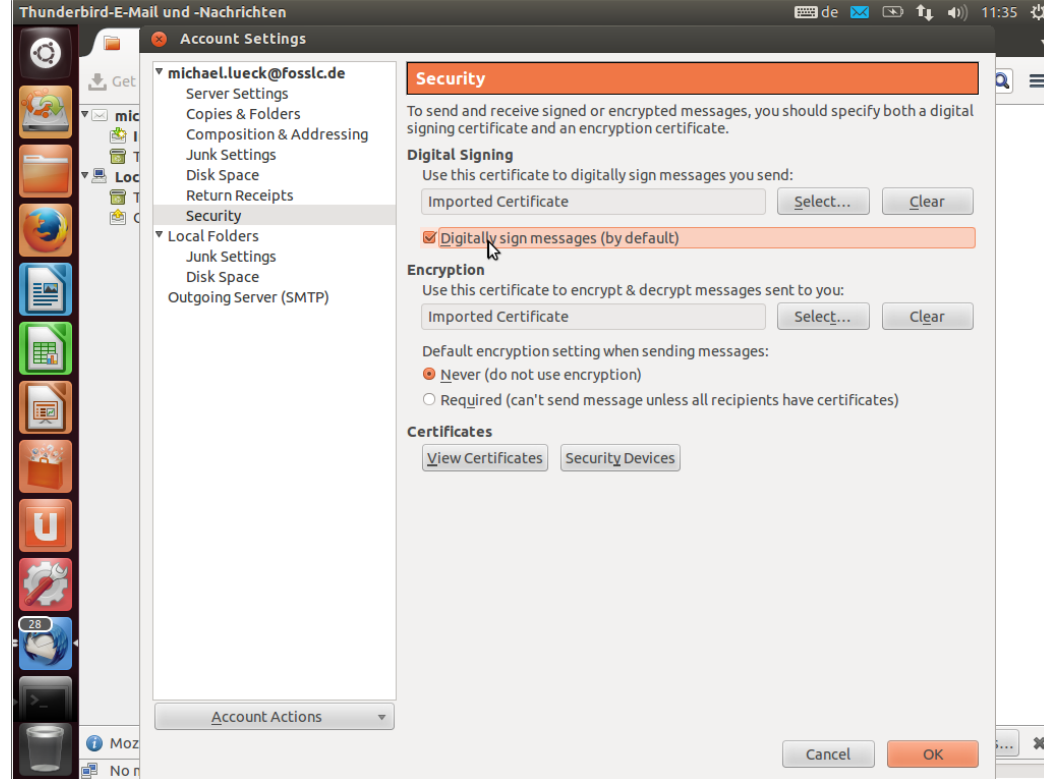
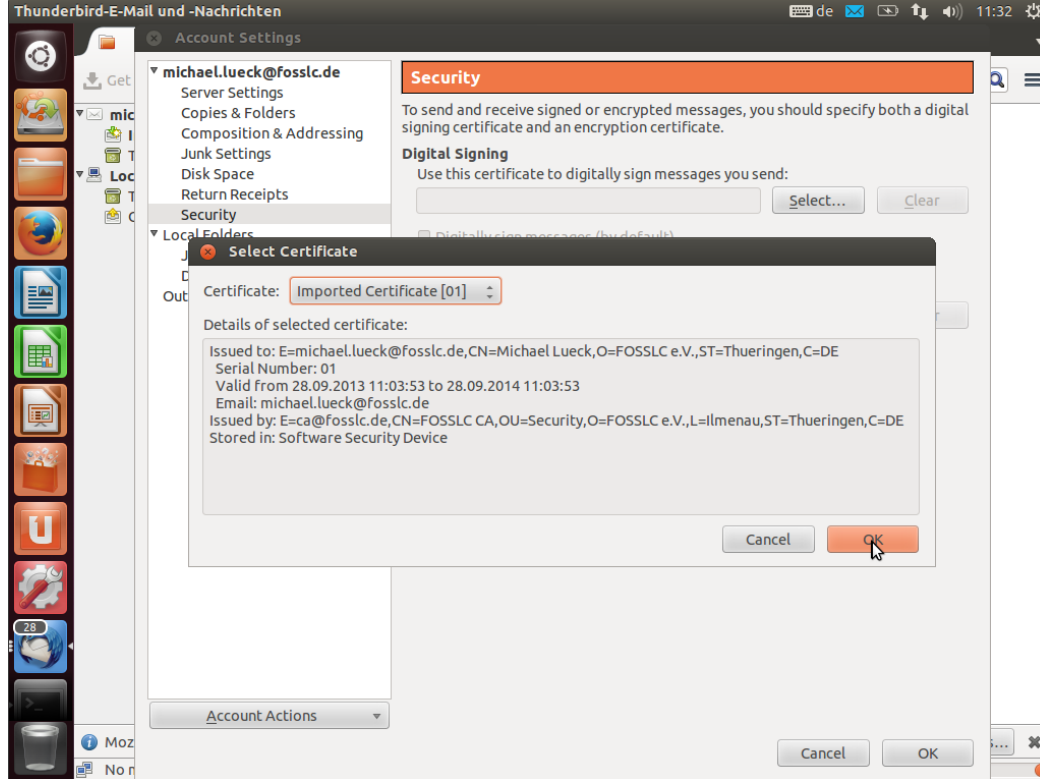
Michael Lück

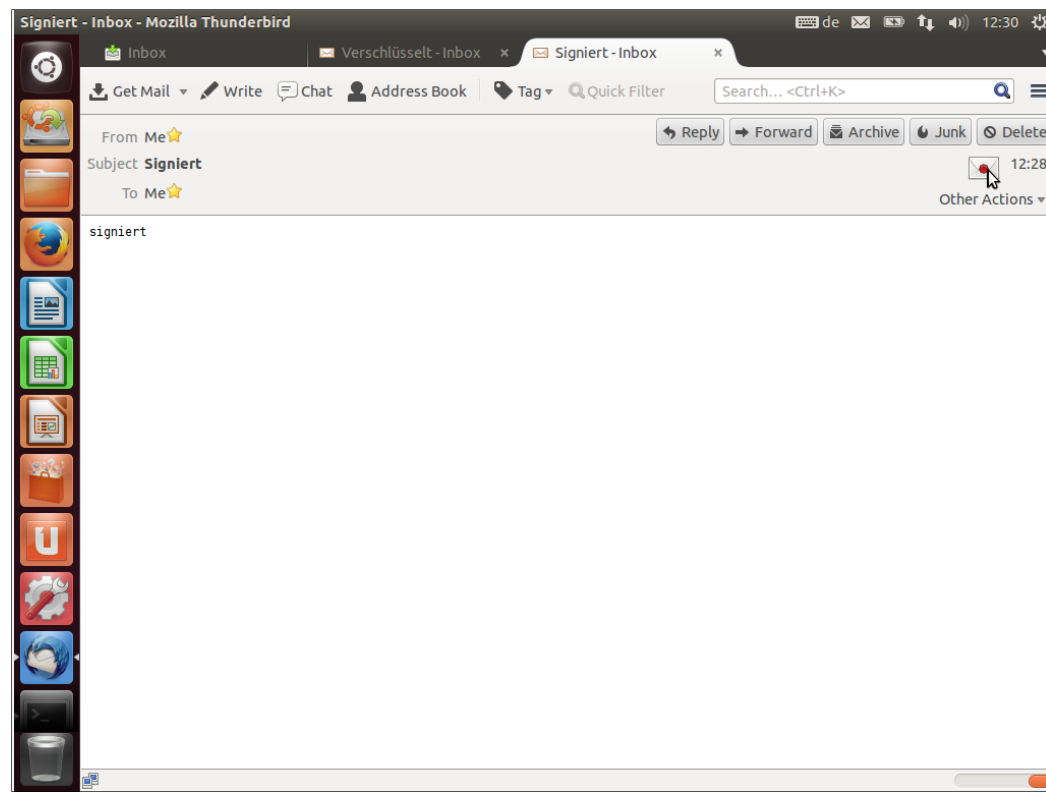
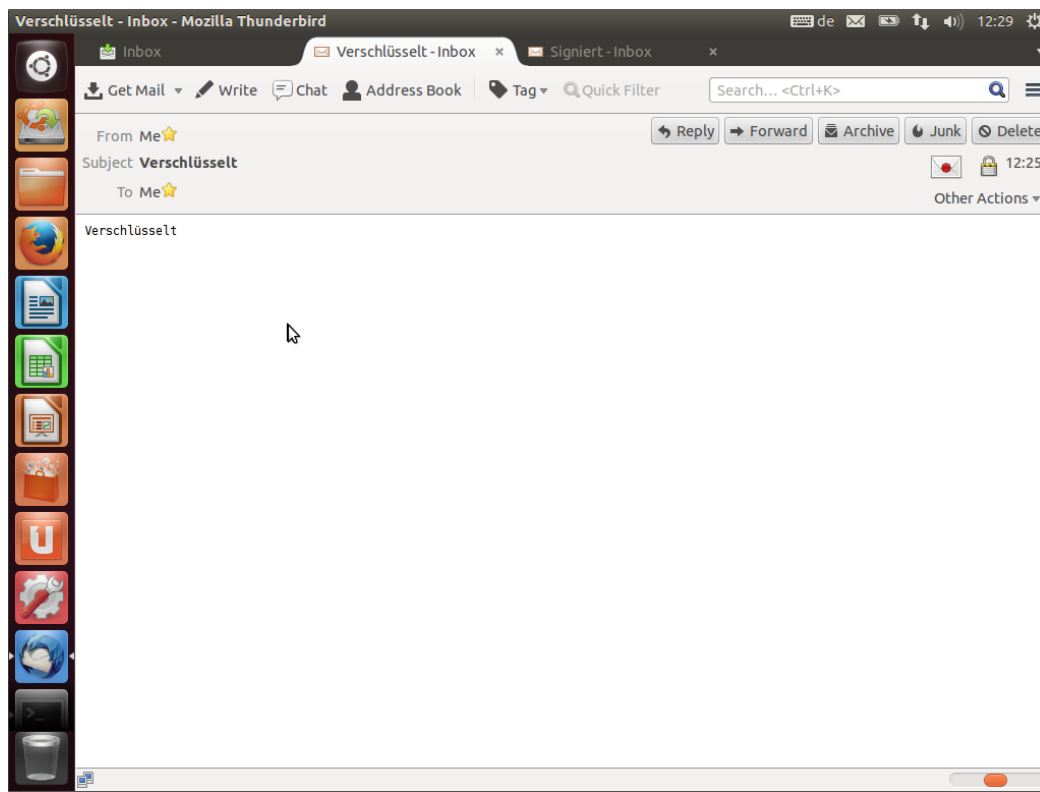
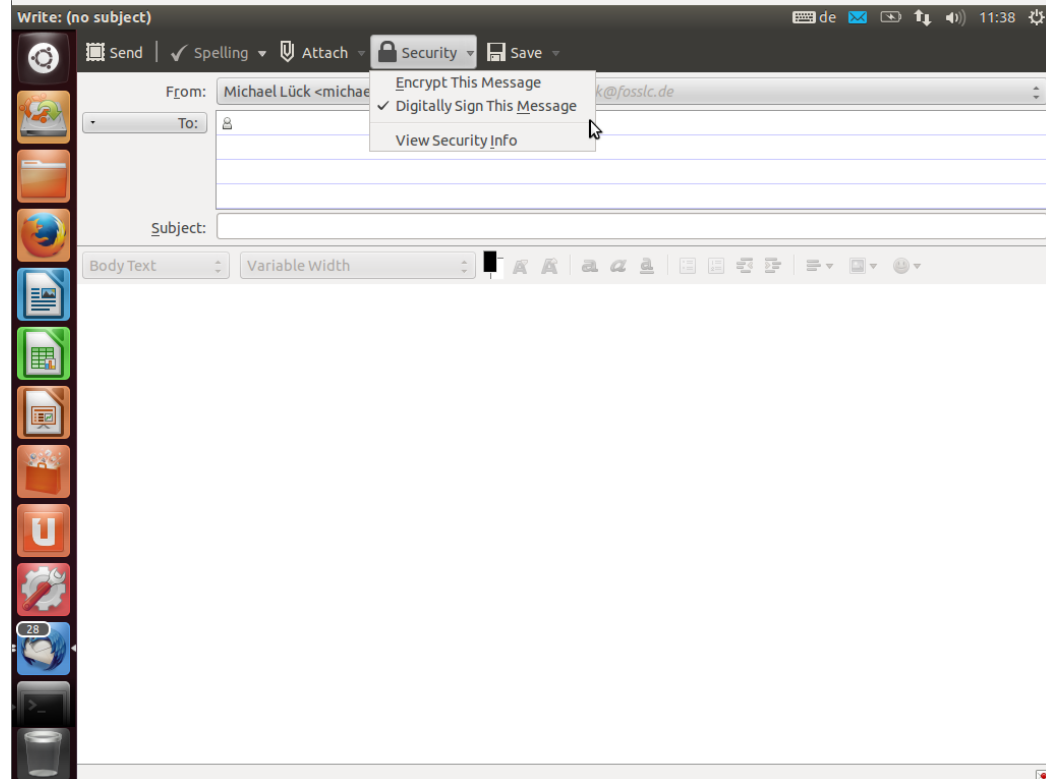
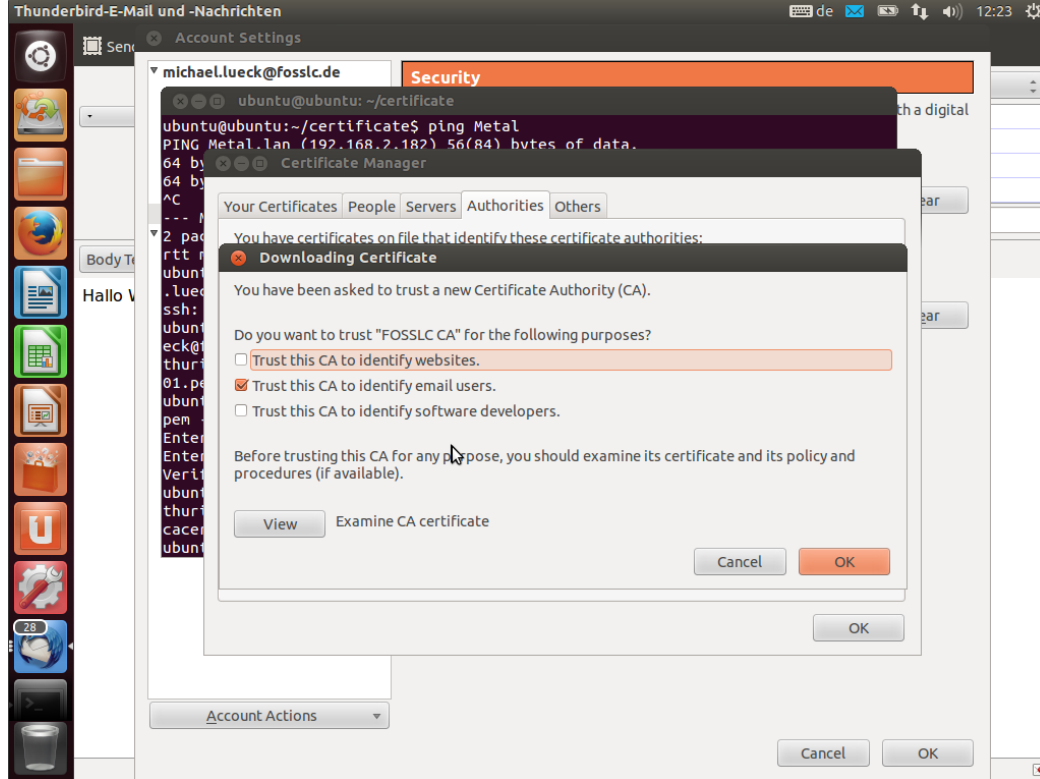
FOSSLC e.V.

Sichere Emailkommunikation, November 2013, CC-BY-SA

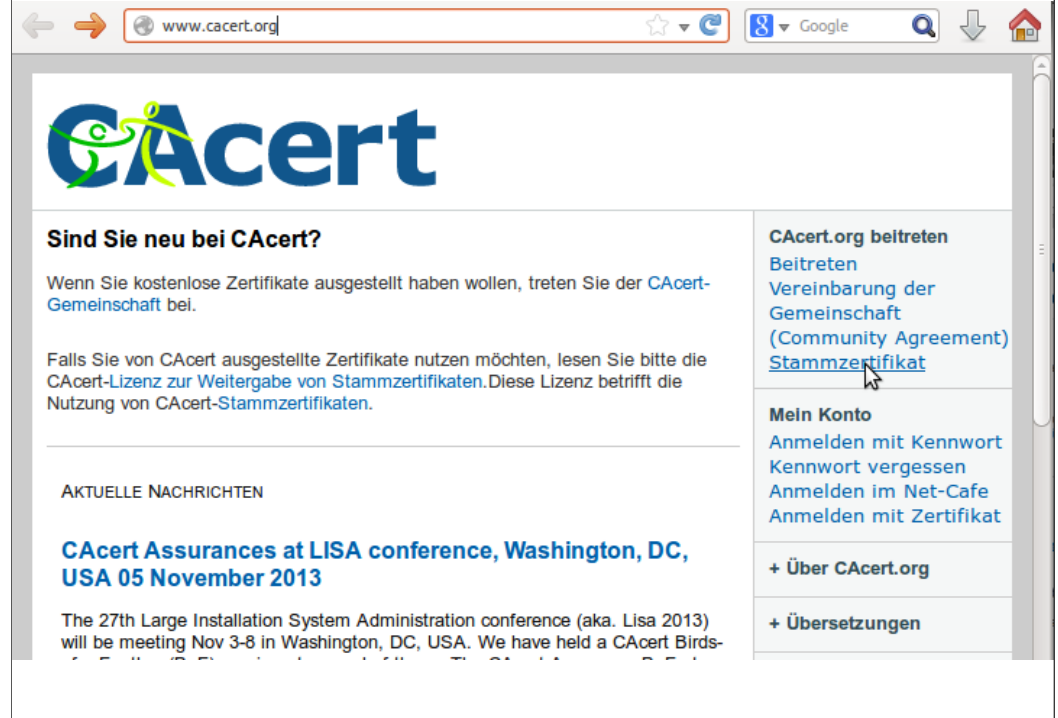




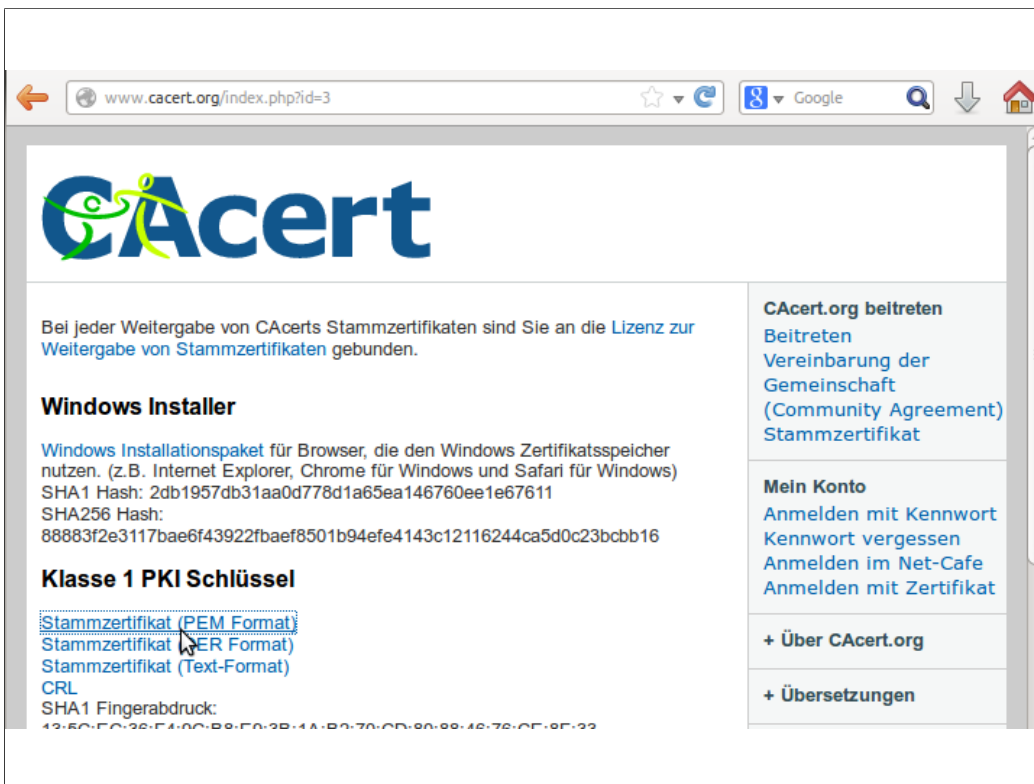




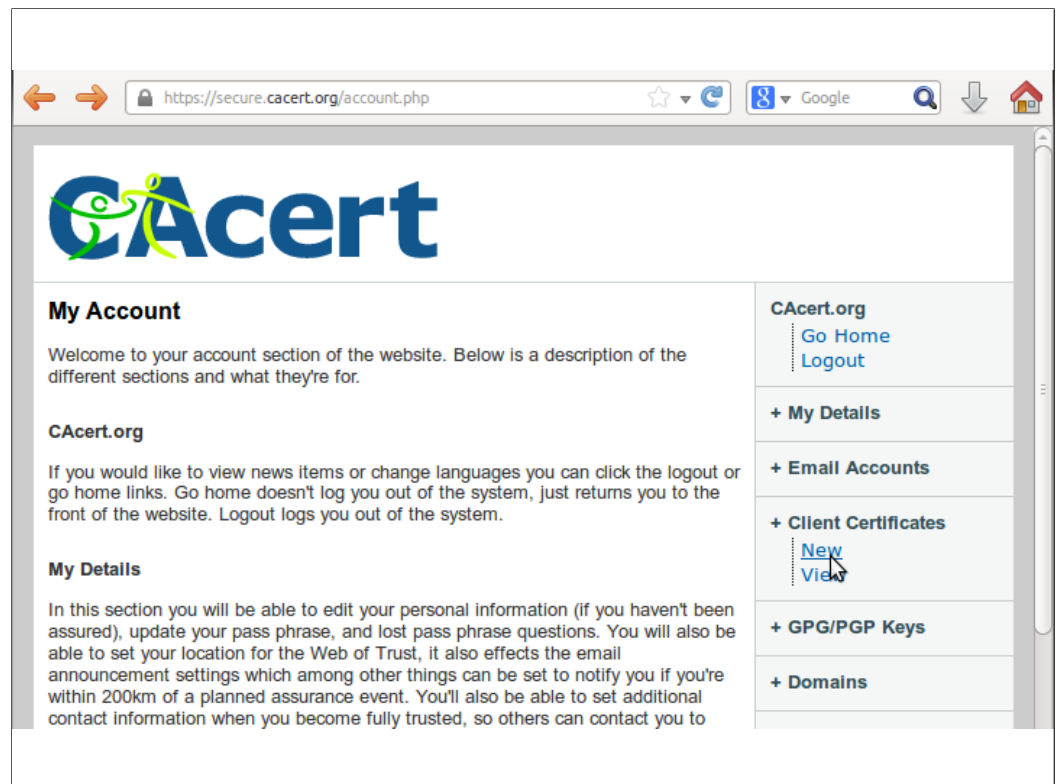
- CA Cert Root Zertifikat importieren
- Zertifikat anlegen (im Browser) [1]



The screenshot shows the CAcert.org homepage. The browser address bar displays 'www.cacert.org'. The page features the CAcert logo at the top. Below the logo, there is a section titled 'Sind Sie neu bei CAcert?' (Are you new to CAcert?). This section contains text about joining the community and using certificates, with links to the 'CAcert-Lizenz zur Weitergabe von Stammzertifikaten' (CAcert license for distribution of root certificates) and 'Stammzertifikat' (Root certificate). To the right, there is a sidebar with links for 'CAcert.org beitreten' (Join CAcert.org), 'Mein Konto' (My account), and '+ Über CAcert.org' (About CAcert.org). The main content area also includes a section for 'AKTUELLE NACHRICHTEN' (Latest news) with a headline about the 'CAcert Assurances at LISA conference, Washington, DC, USA 05 November 2013'.



The screenshot shows the CAcert.org 'index.php?id=3' page. The browser address bar displays 'www.cacert.org/index.php?id=3'. The page features the CAcert logo at the top. Below the logo, there is a section titled 'Bei jeder Weitergabe von CAcerts Stammzertifikaten sind Sie an die Lizenz zur Weitergabe von Stammzertifikaten gebunden.' (When you distribute CAcert's root certificates, you are bound by the license for the distribution of root certificates). This section includes a 'Windows Installer' section with a link to the 'Windows Installationspaket' (Windows installation package) and a 'Klasse 1 PKI Schlüssel' (Class 1 PKI key) section with links to 'Stammzertifikat (PEM Format)' (Root certificate (PEM format)), 'Stammzertifikat (DER Format)' (Root certificate (DER format)), 'Stammzertifikat (Text-Format)' (Root certificate (text format)), 'CRL', and 'SHA1 Fingerabdruck' (SHA1 fingerprint). To the right, there is a sidebar with links for 'CAcert.org beitreten' (Join CAcert.org), 'Mein Konto' (My account), and '+ Über CAcert.org' (About CAcert.org).



The screenshot shows the CAcert.org 'secure.cacert.org/account.php' page. The browser address bar displays 'https://secure.cacert.org/account.php'. The page features the CAcert logo at the top. Below the logo, there is a section titled 'My Account'. This section contains text about the account section and a description of the different sections. To the right, there is a sidebar with links for 'CAcert.org', 'Go Home', 'Logout', '+ My Details', '+ Email Accounts', '+ Client Certificates', '+ GPG/PGP Keys', and '+ Domains'. The main content area also includes a section for 'CAcert.org' with a link to 'New View' and a section for 'My Details' with a link to 'New View'.

- + CAcert Web of Trust
- + CAP Forms
- + Disputes/Abuses
- + About CAcert.org

New Client Certificate		+ Disputes/Abuses
Add	Address	+ About CAcert.org
☒	michael@lueckonline.net	
☒	michael.lueck@fossli.de	
☒ 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 'Michael Lück'		
☒ Enable certificate login with this certificate By allowing certificate login, this certificate can be used to login into this account at https://secure.cacert.org/ .		
Optional comment, only used in the certificate overview max. 100 characters 		
☐ Show advanced options		
☒ I accept the CAcert Community Agreement (CCA). Please Note: You need to accept the CCA to proceed.		
Next		

← <https://secure.cacert.org/account.php> ☆ ▾   ▾ Google 🔍 ⬇️ 🏠



CAcert

Keysize:

CAcert.org
[Go Home](#)
[Logout](#)

+ My Details

+ Email Accounts

+ Client Certificates
[New](#)
[View](#)

+ GPG/PGP Keys

+ Domains

[illegible]

Lj+u8RXNkx/H78+eRxEhXGmEvGdHtSLwCpSPtT3Uo5ayd8rZ4PU8b4HmBLzLjAgkscqg4J4b+088A/AM3P9rQpDhr77HNM9P1oLRSRnHmdkgg0GpU9a7R5vYBhSwdVtEo5GmnpPw/KHFkbsE8Ej3d4w0vnm9HBLwQwJvWOC+3x9GdMfPqoV4MwL1tPVMpMBYbXhU4YT4PZ9fsg0kQwEwNvU0/zvchqTwnrLXhUgT2WnLRhU7Vz6jQJdXkziardjbxOU987DtMdiP55ep0ZbnyDptslg8EGlso569E5Uzmop7yxfUlpdPghUnsf+UzadZAgBAA9jlgvGFITIBDAMBgNHRMBFA8EajAAMFYGCGSGAG6+ETB00R7FkldbyBzXG0e9e1bb2V4dY2VdJgmLmWdH9M5YIEZSR5UuqAgVhZC8vdmlyIthRvIgh0dH4hUy93dcuqQ6QZAJ0L9bY5Za08BgN1H386F8E8BAC6AgQvOATDVRlB0kNmXtQYkYBBQUuqW0GQC5XaUfMwPwC8BgRGEEAY13QCBgRgBgEGAYT5C3gMdBgLghkghvBnCBAEWqYkYUyBBQUuqAqEEJ3jAKMCGIC5G6AUFBAzBHhZ0dW0r18vbnZzc53Y7WMLcnq33NMDG6A1UdhWqU3GqJqkcoCKGIGih0dH4SLy5jcmwU7FjZJX0L9bY5Za08Y2vZx2vaUuY33sLzWnGdU1UdeEQ00MfKBFZ1p2ZhZwmAbHvL2vtv2bmkbmUubmV0gRdtYn0WYfL5mL5Wn+QGVZc3nSt5Y5KZtANBgkqhkiG9w0BAQ0FAAOCAGeA5HmGdY2McyYJL3EG4dEbm3mJ9L4UFL7p3joFakbVbCBCE09dWkTzJ1CMLE+CHM75ux+q3GGAqJb0sznJAY7aXrLl2uLmPw93948EETiUwHvB9J85TVTm2VpwLtl+AFFH567dFnsaBf89F983BfP4U0ApvgL/LD6953J5s+ddcCEIEFZT08QBKVB8z4w6Ywx9+rK4vLzUo,UpIqP7uSABLw08EHF+4X53NulrPm0PokRilbyakvewL7dGcmSE57k9SG6A1GhXZ2jWnKStFDnSokp0xbDlA7NujLh4D9Nj3CC4+Lj+HjKqGFQI7P7T3E39J7:cltdNtA05hQ1V4yzc3nSt5c0YE7ML0IhbnbN0Y5AOcYqG5vLzA+wmE0uG0L9S0c6FauN9Lp7FCbAjhpEW6G6/K9z3f1BdR7F86bUuq34gPkG5DXEM9w0yQBpGfme,Txk7WbpbRcPrbNcJ4r845SbVbclgTE0dIBDVLrSmj5wHMYrrcR2SMd67DCkS0Xw0amZkbr/rBf;IToQw71LH2ydcVt/bcAgPR6hqqZp66J5xba0S9t94Mw4Pw5YHxcZu3YLLBkz/rH8Z724LzGvd08VBt6T1y5a0qL7Y3oeynM5L+0gsdU1UwAYDYL3MH7136u54=-

-----END CERTIFICATE-----

Information about the certificate	
Renew/Revoke/Delete	☐
Status	Valid
Email Address	michael@lueckonline.net
SerialNumber	0E00CC
Revoked	Not Revoked
Expires	2015-10-28 19:13:52
Login	☒
Comment	



CACert Community.

Email certificates.

<http://wiki.cacert.org/EmailCertificates>, 2011.
[Online; accessed 28-Oktober-2013].



Ogmios.

Web of trust.svg — wikimedia commons.

http://http://commons.wikimedia.org/wiki/File:Web_of_Trust.svg, 2009.
[Online; accessed 14-September-2013].



Bruce Schneier.

The eternal value of privacy.

<https://www.schneier.com/essay-114.html>, 2006.
[Online; accessed 24-September-2013].



Ubuntu Documentation Team.

Certificates.

<https://help.ubuntu.com/lts/serverguide/certificates-and-security.html>, 2013.
[Online; accessed 06-Oktober-2013].



Wikipedia.

Kryptographie — Wikipedia, the free encyclopedia.

<http://de.wikipedia.org/wiki/Kryptographie>, 2013.
[Online; accessed 24-September-2013].