

TIP

Remember, your sense of conviction and your involvement with the content of the presentation are critical to its success.

on the internet nobody knows you are a dog



"On the Internet, nobody knows you're a dog."

CAcert: how to get a trust mark without paying the 250K Euro consultancy fee.

teus hagen

content

- What is a digital certificate, encryption technology, identification
- What is a CA about? Why one need an Open and free to join **CAcert**?
- The **CAcert** audit project
- The **CAcert** hardware and service: the organisation and technology
- The new **CAcert** (Sub) Root Key: the HowTo for the paranoia
- If time allows the obvious FAQ's:
 - ➔ encryption how does this work
 - ➔ certificates how to use them: certutil
 - ➔ Firefox & Thunderbird and certificate management
 - ➔ GPG



➔ <http://svn.cacert.org/CAcert/PR/Presentations/CAcertPresentationNLLGG>

What is a digital certificate?

- X.509 standard
- two parts:
 - ➔ private key part
 - ➔ public key part: “X.509 certificate”
maybe accepted as “this is from you”: signed by ?
- X.509 and PGP

certificates are official

- pres. Clinton signed
S 761 - The Millenium Digital
Commerce Act June 30,2000.



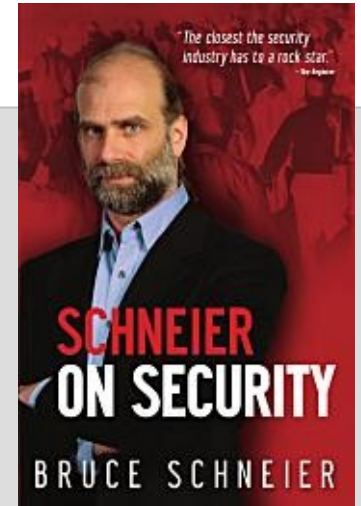
- <http://www.techlawjournal.com/cong106/digsig/Default.htm>

encryption

Bruce Schneier:

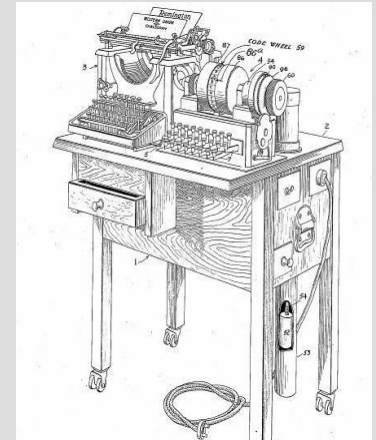
*“Any person can invent a security system
so clever*

that she or he can't think of how to break it”

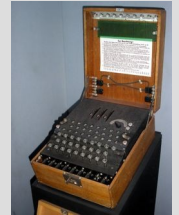
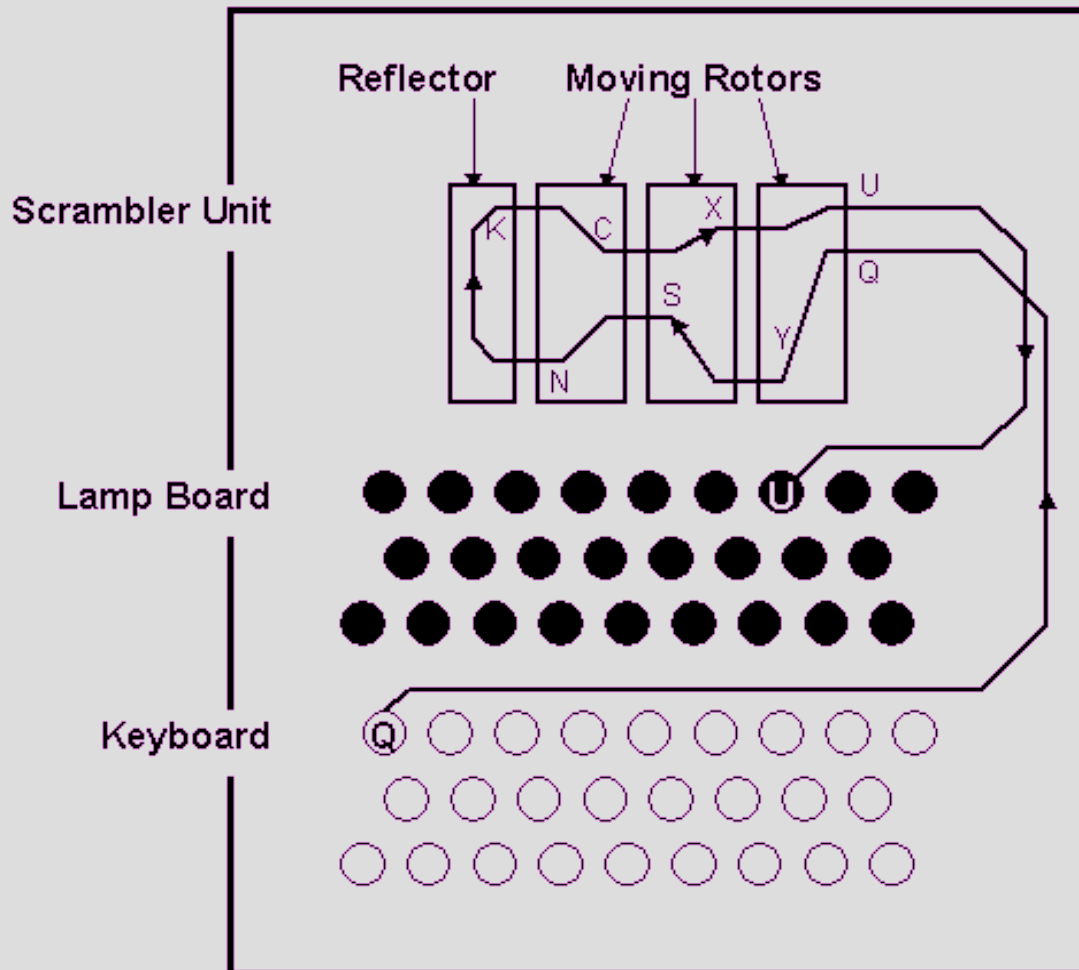


encryption

- Herbern
- Enigma
 - ➔ Germany second world war
 - ➔ the mechanism
 - ➔ hacked, of course



Enigma technology



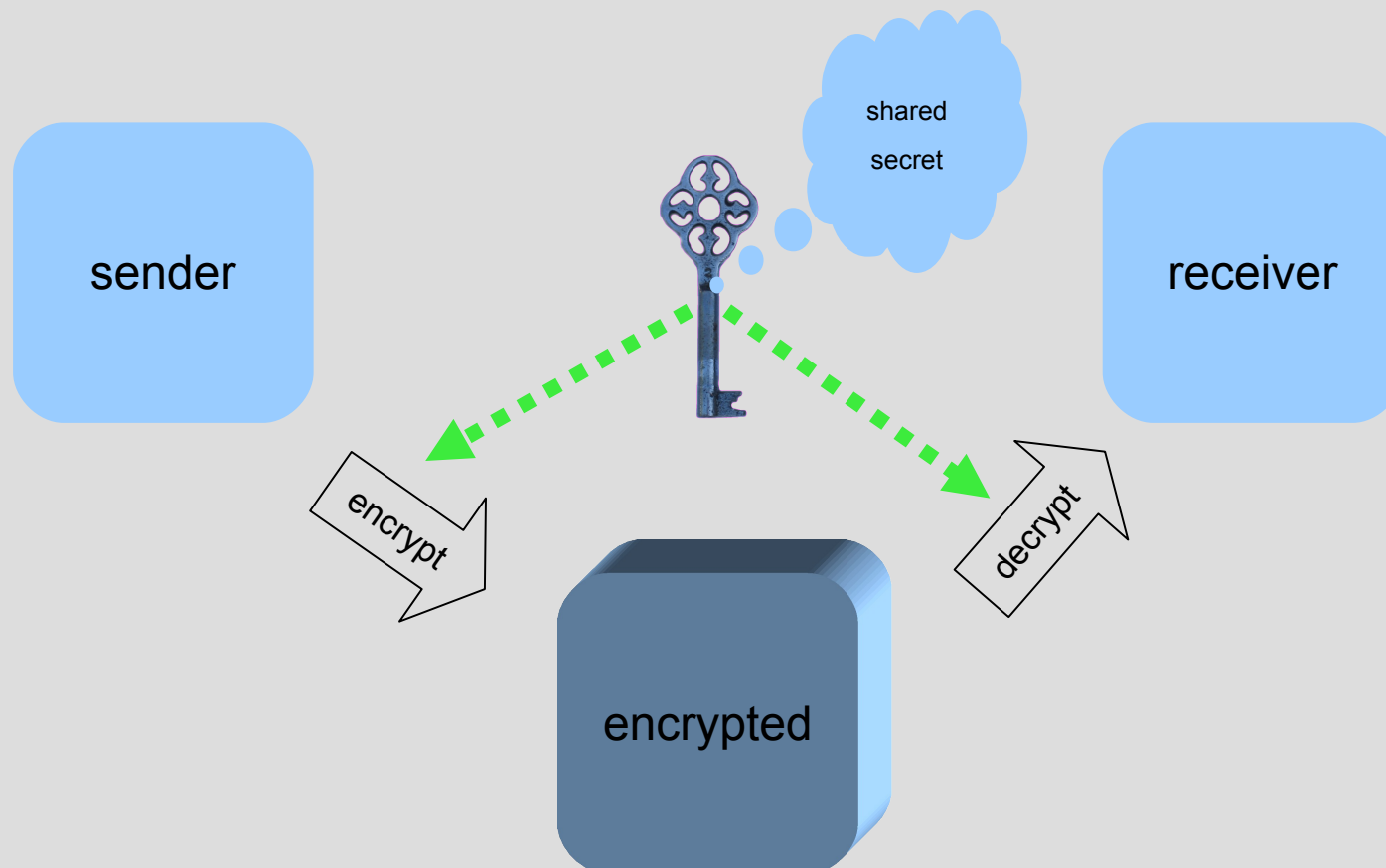
RFID chip hacked Dec 2007

- Mifare classic RFID chip of NXP (Philips)
- Karsten Nohl and Henryk Plötz
- Hacked
 - 48 bits but only 16 bits (only 64.000 variations) used
 - not random (dependent on time contact)
- implications:
 - car keys
 - public transportation cards
 - electronic tickets eg FIFA World Cup tickets



encryption key types

symmetric key encryption



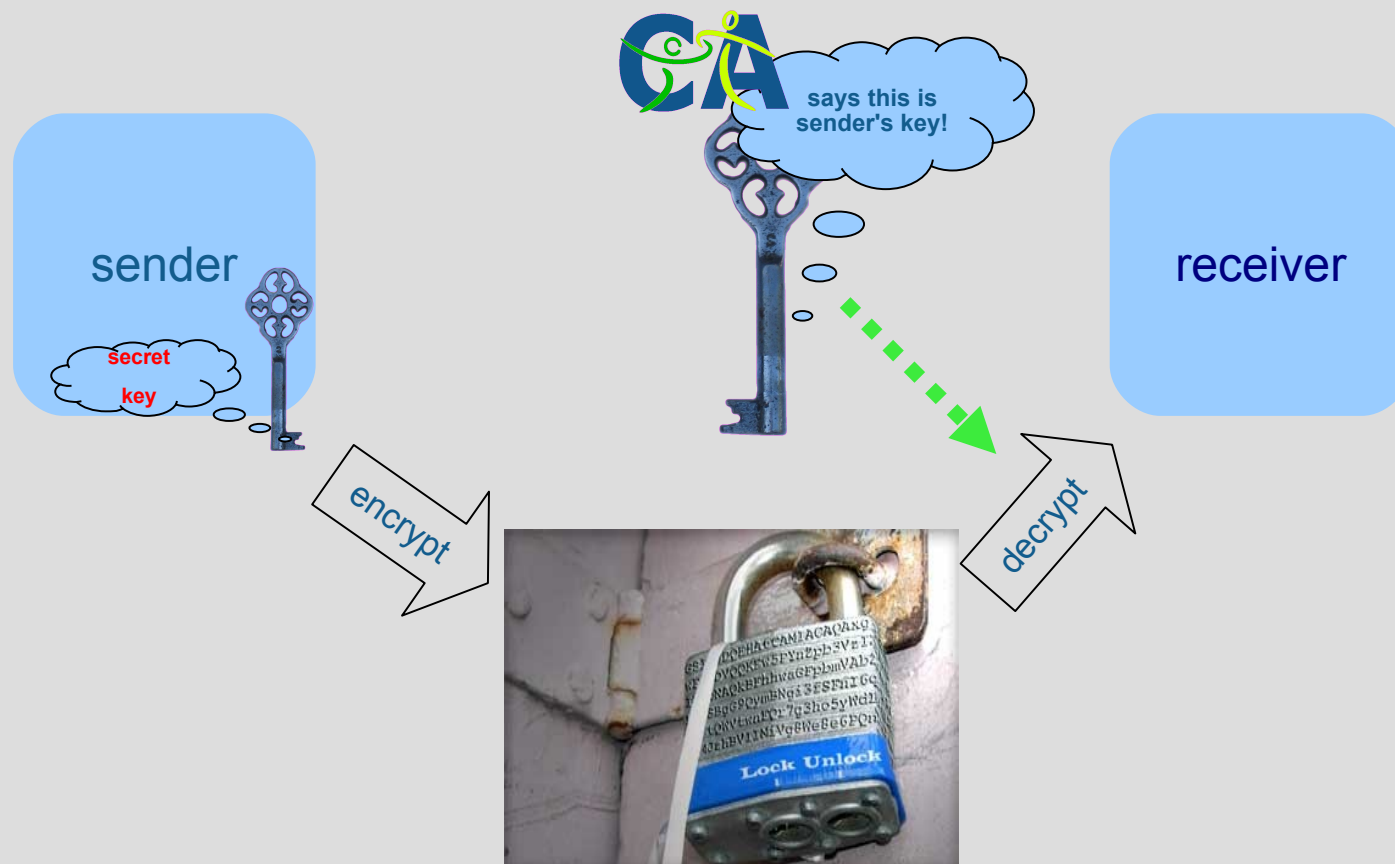
asymmetric key encryption

that message can only be read by him

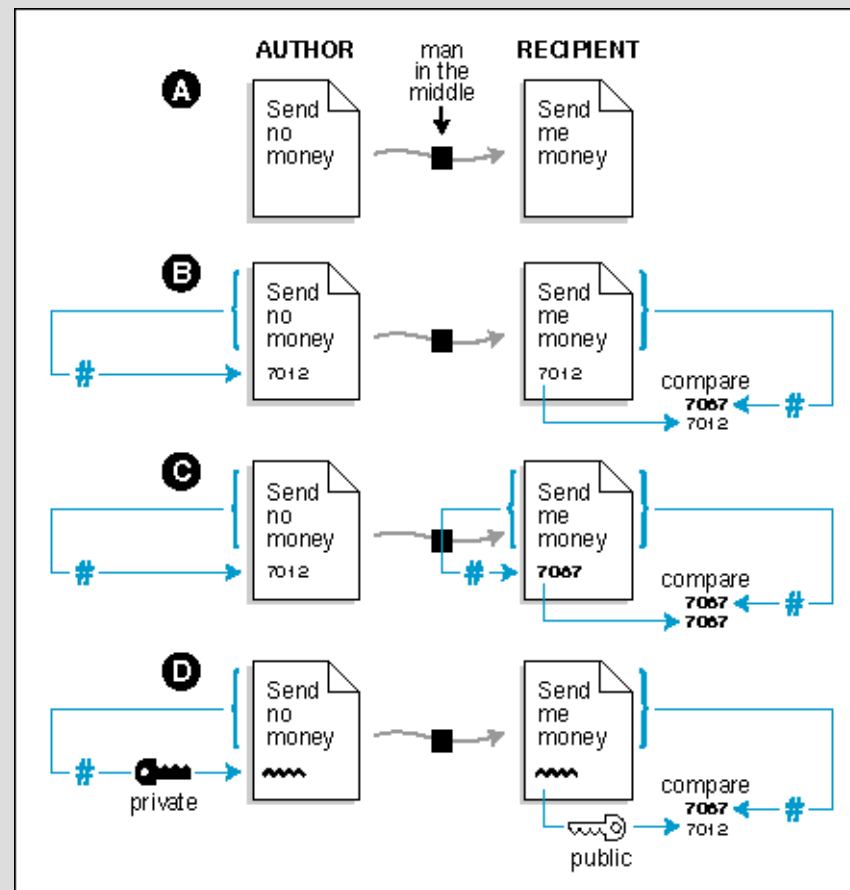


asymmetric key encryption

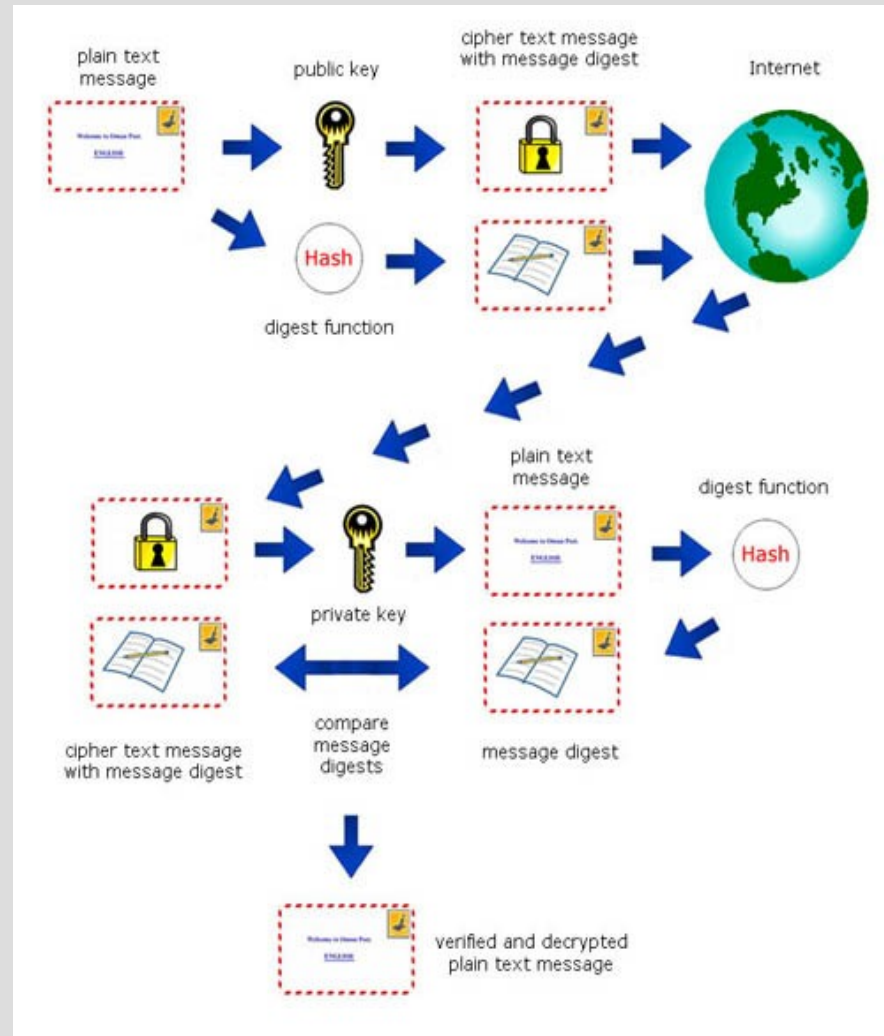
that message can only come from him!



how do “signatures” work



Email and signatures



the practice: encrypted and signed email

The screenshot shows the Thunderbird email client interface. The main window displays an email from Philipp Gühring to Teus Hagen, dated 10/30/2007 05:56 PM. The email subject is "CAcert". The email body contains the text "Hi, The http://213.154.225.230/ wen cat rep. The Eve In th still".

Two error messages are overlaid on the email content:

- Message Security**: Digital Signature Is Not Valid. This message includes a digital signature, but the signature is invalid. The certificate used to sign the message was issued by a certificate authority that you do not trust for issuing this kind of certificate. Signed by: Philipp Gühring, Email address: pg@futureware.at, Certificate issued by: CA Cert Signing Authority. A "View Signature Certificate" button is visible.
- Message Security**: Message is Encrypted. This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network. An "OK" button is visible.

A "Certificate Viewer" window is also open, showing details for the certificate "Philipp Gühring". The window title is "Certificate Viewer: 'Philipp Gühring'". The "General" tab is selected, and the message "Could not verify this certificate because it has expired." is displayed. The certificate details are as follows:

Issued To	
Common Name (CN)	
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	02:FF:AF

Issued By	
Common Name (CN)	CA Cert Signing Authority
Organization (O)	Root CA
Organizational Unit (OU)	http://www.cacert.org

Validity	
Issued On	12/12/2006
Expires On	12/12/2007

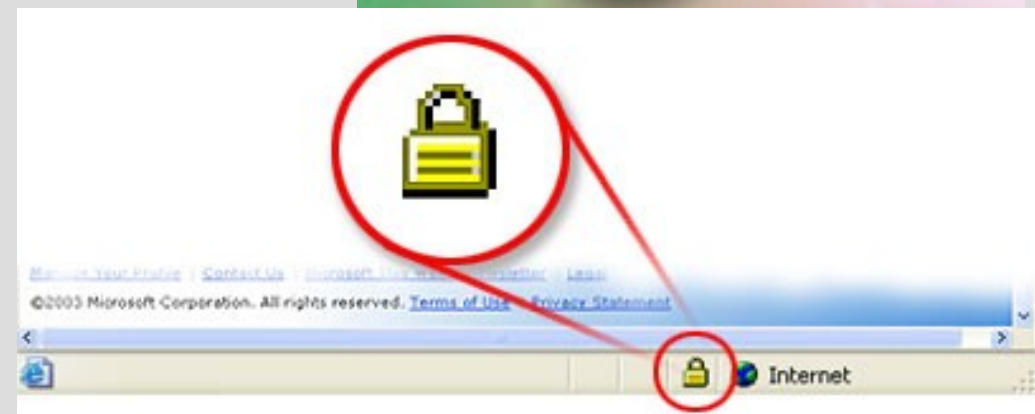
Fingerprints	
SHA1 Fingerprint	70:1A:93:6FCA:06:2A:81:63:DE:75:20:11:7D:7F:ED:0E:91:7D:1C
MD5 Fingerprint	F1:05:B4:26:B0:72:3D:A4:2D:DA:10:53:52:73:BA:C9

What can you do with it?

- encrypt & decrypt
- identify data: it is coming from her!
 identity for trade (name, birth date, email address)
- claim
 e.g.
 - encrypt data: email, file, internet communication
 - sign documents: eg code signing, signatures
 - time stamping

secure data transfer

- secure Socket Layer
SSL
- Secure Hypertext Transfer Protocol
https
- Virtual Private Network
VPN



What is a digital certificate?

A screenshot of a Windows Certificate Viewer window titled "Certificate Viewer: 'Teus Hagen, Oophaga Foundation'". The window has two tabs: "General" (selected) and "Details". Under "General", it states "This certificate has been verified for the following uses:" and lists four categories: "SSL Client Certificate" (highlighted), "SSL Server Certificate", "Email Signer Certificate", and "Email Recipient Certificate". Below this, it shows fields for "Issued To" (Common Name: Teus Hagen, Organization: <Not Part Of Certificate>, Organizational Unit: <Not Part Of Certificate>, Serial Number: 03:5D:AD) and "Issued By" (Common Name: CA Cert Signing Authority, Organization: Root CA, Organizational Unit: http://www.cacert.org). It also shows "Validity" (Issued On: 03/19/2007, Expires On: 03/18/2009) and "Fingerprints" (SHA1: 79:B5:57:6C:EC:02:91:AD:93:2C:B9:11:83:DD:44:72:53:10:22:50, MD5: 7E:B6:2C:69:1D:84:50:57:9C:83:23:20:1D:00:CE:6A). A "Close" button is at the bottom right.

Certificate Viewer: "Teus Hagen, Oophaga Foundation"

General Details

This certificate has been verified for the following uses:

- SSL Client Certificate
- SSL Server Certificate
- Email Signer Certificate
- Email Recipient Certificate

Issued To

Common Name (CN)	Teus Hagen
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	03:5D:AD

Issued By

Common Name (CN)	CA Cert Signing Authority
Organization (O)	Root CA
Organizational Unit (OU)	http://www.cacert.org

Validity

Issued On	03/19/2007
Expires On	03/18/2009

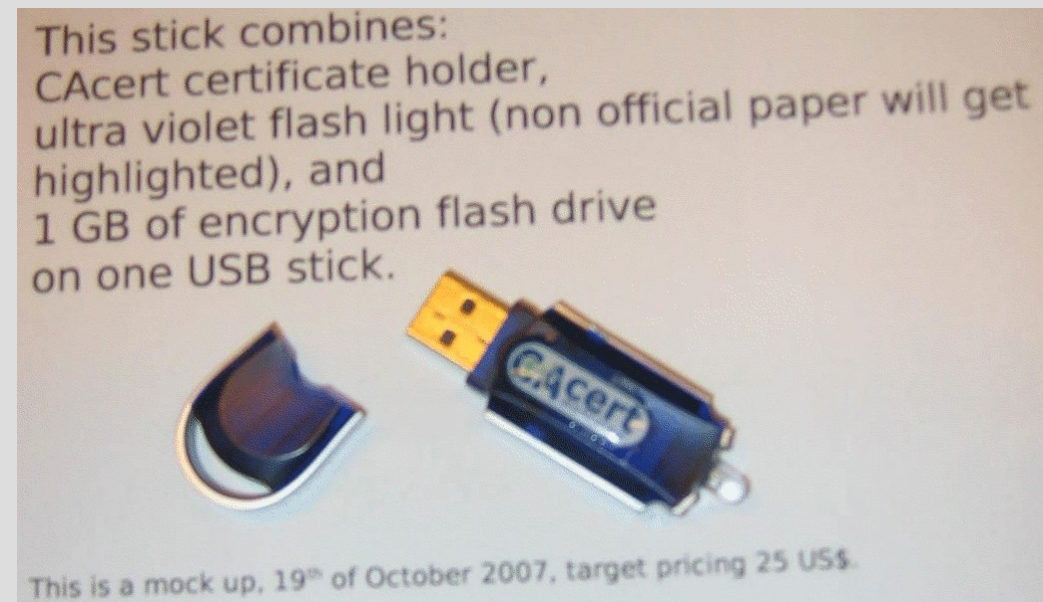
Fingerprints

SHA1 Fingerprint	79:B5:57:6C:EC:02:91:AD:93:2C:B9:11:83:DD:44:72:53:10:22:50
MD5 Fingerprint	7E:B6:2C:69:1D:84:50:57:9C:83:23:20:1D:00:CE:6A

Close

client certificate how to?

- use your browser
- use firefox or
- use thunderbird
 - ➔ edit
 - ➔ preferences
 - ➔ advanced
 - ➔ certificates



How does a certificate look like?

- [mcvax.theunis.org.pem](#)
- [mcvax.theunis.org.key](#)
- [mcvax.theunis.org.csr](#)
- [mcvax.theunis.org.crt](#)
- [mcvax.theunis.org.p12](#)

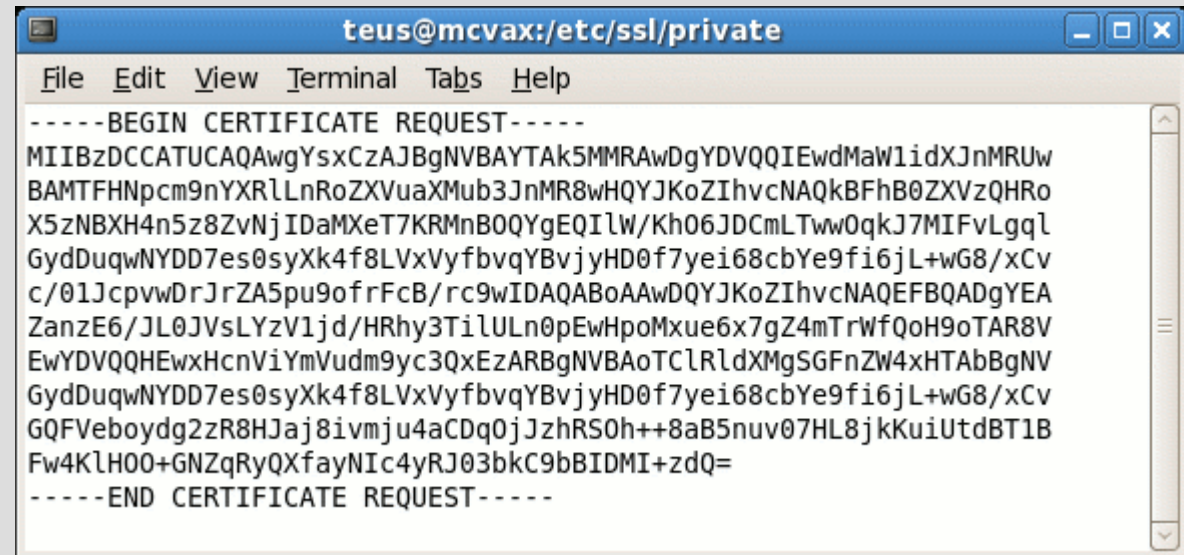
```

teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDcC8ybQIM22owYvH/Wg2iijJA6EhIevHZvnk8sfrgBLikDmivf
c8Q3r758SsRGKvnBYxjPyH1AIcQbTj4Tcm/GCTl8ACK5ofp6/gdhjnpRq2JZhwfM
AoGBAIfcR8ABoNsE0VK5CkFTh12T0wjaPajEed56grU90ipGimFvakp31NKsAG
g2bxdLWoCzH1hhNd...
w3kus/xfowJF...
AGg9i0ielNAj...
GyBjP3KSrLzvU...
w3kus/xfowJBA0KCWIqge/w0s6yX3CsaRc2PwWPhd3N1/3LUttf8hiV9evufEbl5
1yDN059KwJvZ1XyyTaRdx0Y/9CbQsXwkNp4fD0KSTYZX60XyYrhBMYACVmgIwsVb
t9KyfSVtIkVMMIw0GPxAkEAmu1TWqSUvR8jHGtWcebqL8LnhYacKe0NFDA9K3d
FFYkKqcrsygujNujB/P3IE5eBwgEMwDhiwlv0WJ11C8vZA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEFTCCAf2gAwIBAgIDARRSMA0GCSqGSIb3DQEBAUAMHkxEDA0BgNVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWwh0dHA6Ly93d3cuY2FjZjZ0Lm9yZzEiMCAGA1UEAxMZ
Q0EgQ2VydCBTaWduaW5...
MBcGA1UEAxQKi50aGV...
gYkCgYEA3AvMm0CDNt...
fErERir5wWMYz8h9QCh...
8sn4KG7UmgLkg0FAdJ...
hdAMBgNVHRMBAf8EAj...
YIZIAYb4QgQBgorBg...
JKAihiBodHRwOi8vd3...
fgTfs1wJqAPIavUzAk...
kyy1XgBbQQ6Mm7ppq...
NqcXz/f9hmqhGiULeA...
AQQFAA0CAgEAejvbfX...
6vG0e2Ucnd2dsHRLmT...
X/thAu70Fa+0UGmmK3r...
XqJx504AFQMKrpD4xb...
+UFxKrF2e1nBGZF1Ffd/VFT+XamBmicAZAk/c07ghQucJJkRiDyt0c4f0pBMohCA
nZjFR/FxcMwtcjwf9NGmtV0LrL+7zz/suL4Quz0qFN0Q0Pv64u0mpe1DDYCKRlpC
41Kew0vtGLBpvFd4rP00fHrLEoLn09FX9ISQKrwW5+7hn3Q8phT9ik8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwYsxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdMaWlidXJnMRUw
BAMTFHNpcm9nYXRlLnRvZXVuaXMub3JnMR8wHQYJKoZIhvcNAQkBFhB0ZXVzQHRo
X5zNBXh4n5z8ZvNjIdaMxeT7KRMnB0QYgeQILw/Kh06JDCmLTww0qkJ7MIFvLgql
GydDuqwNYDD7es0syXk4f8LVxVYfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
c/01JcpvwDrJrZA5pu9ofrFcB/rc9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
ZanzE6/JL0JVsLYzV1jd/HRhy3TilULn0pEwHpoMxue6x7gZ4mTrWfQoH9oTAR8V
EwYDVQQHEWxHcnViYmVudm9yc3QxEzARBgNVBAoTClRldXMgSGFnZW4xHTABgNV
GydDuqwNYDD7es0syXk4f8LVxVYfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
GQFVeboydg2zR8HJaj8ivmj4aCDQ0jJzhRS0h++8aB5nuv07L8ljKkuiUtdBT1B
Fw4KLH00+GNZqRyQXfayNIc4yRJ03bkC9bBIDMI+zdQ=
-----END CERTIFICATE REQUEST-----

```

CAcert HowTo

- create
 - Private key
 - Cert Sign Req
- have it signed
- import
 - Private Key
 - Public Key: the certificate

A terminal window titled 'teus@mcvax:/etc/ssl/private' showing the output of a 'cat' command on a certificate request file. The output is a PEM-formatted certificate request, starting with '-----BEGIN CERTIFICATE REQUEST-----' and ending with '-----END CERTIFICATE REQUEST-----'. The body of the request is a long string of base64-encoded data.

```
teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwYsxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdMaWlidXJnMRUw
BAMTFHNpcm9nYXRLLnRoZXVuaXMub3JnMR8wHQYJKoZIhvcNAQkBFhB0ZXVzQHRo
X5zNBXH4n5z8ZvNjIDaMXeT7KRMnB0QYgEQILW/Kh06JDCmLTww0qkJ7MIFvLgqL
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
c/01JcpwDrJrZA5pu9ofrFcB/rc9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
ZanzE6/JL0JVvsLYzV1jd/HRhy3TilULn0pEwHpoMxue6x7gZ4mTrWfQoH9oTAR8V
EwYDVQQHEwxHcnViYmVudm9yc3QxEzARBGNVBAoTClRldXMgSGFnZW4xHTAbBgNV
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
GQFVeboydg2zR8HJaj8ivmju4aCDq0jJzhRS0h++8aB5nuv07HL8jkKuiUtdBT1B
Fw4KlH00+GNZqRyQXfayNIc4yRJ03bkC9bBIDMI+zdQ=
-----END CERTIFICATE REQUEST-----
```

How-To create private and public certificate

get a key manager



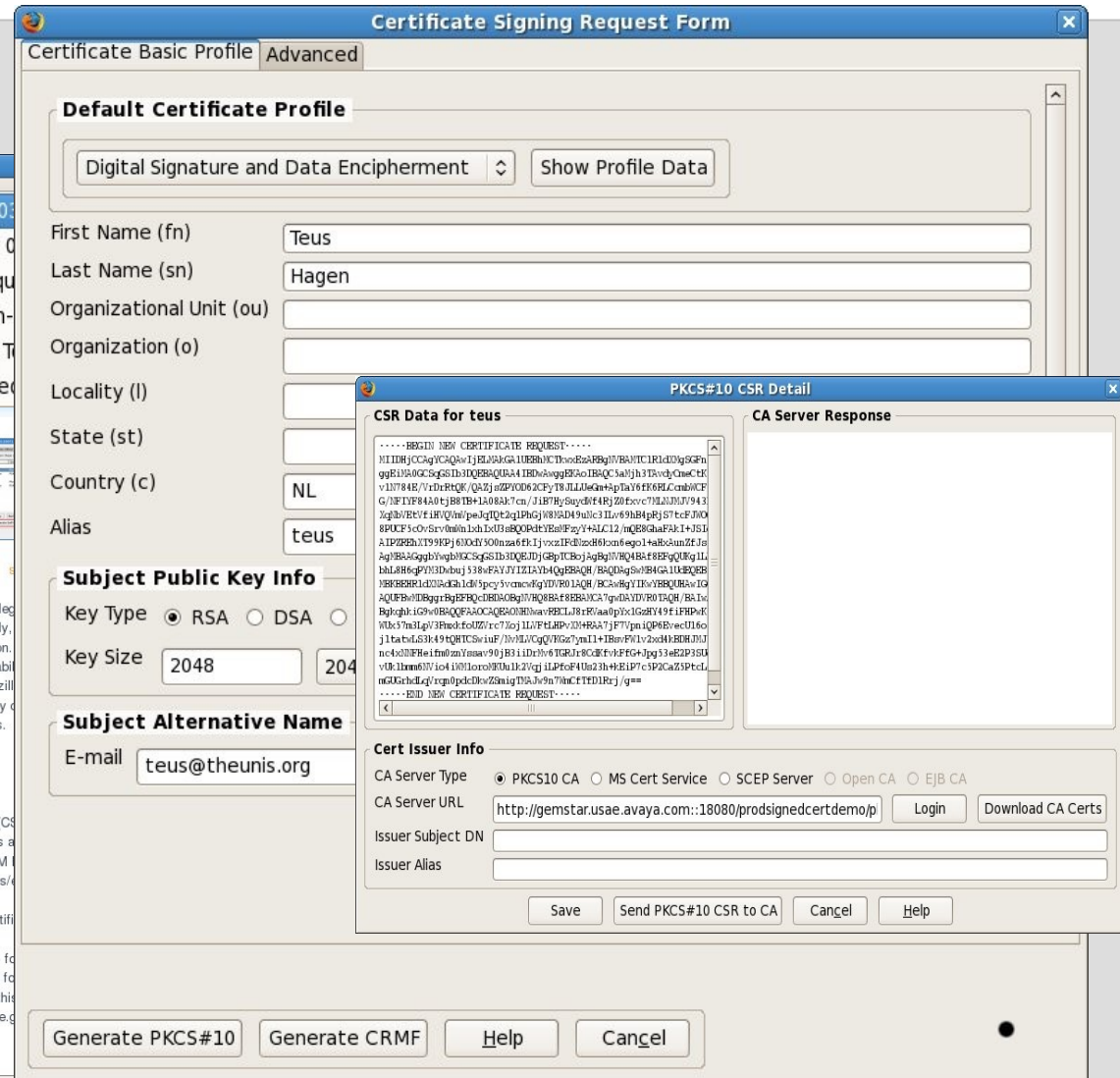
Key Manager (v 0.1.0.20071203)
by [Subrata Mazumdar](#)

KeyManager Tool: Firefox Extension for Key Generation, Certificate Enrollment, and Identity and Authority Delegation

KeyManager is a client side PKI tool for key generation, certificate enrollment, and identity and authority delegation. Currently, export of keys but does not provide GUI for local key generation. Certificate Manager wizard in Mozilla PSM and added the capability of SCEP based certificate enrollment. Our extension enables Mozilla management tool. In addition, the tool supports signing of proxy certificate delegation and provides XUL based GUI for signing of XPI files.

The KeyManager tool has following features :

- Generation of keys and X.509 based self-signed certificate
- Generation of PKCS#10 based Certificate Signing Requests (CSR)
- SCEP based Certificate enrollment - it enables Firefox to act as a SCEP client can be invoked from other extensions and XPCOM
- signing of archive files, including XPI files, for Mozilla add-ons/XUL based GUI for command-line signtool in Mozilla NSS
- Signing of Proxy Certificates (RFC 3820) and other users' certificates
- Signing and verification of Attribute certificates (RFC3281)
- Exporting of private keys (in PKCS#8 and PKCS#12 formats) for use with public key certificate and generation of configuration file for applications, such as cURL, Globus toolkit, etc. (You will find this useful if you are trying to use PKCS#11 compliant engines for Smart Card, etc. based apps.)



Certificate Signing Request Form

Default Certificate Profile: Digital Signature and Data Encipherment

First Name (fn): Teus
Last Name (sn): Hagen
Organizational Unit (ou):
Organization (o):
Locality (l):
State (st):
Country (c): NL
Alias: teus

Subject Public Key Info
Key Type: RSA DSA ECDSA
Key Size: 2048

Subject Alternative Name
E-mail: teus@theunis.org

PKCS#10 CSR Detail

CSR Data for teus
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDHjCCAgYCAQswJjElaGAgGAUeBhUCThooZaBkgIIBAAITC1RlZDQyOgZn
ggR1VSA0GCSgSIB3DQEBQ0A4IRDo6wggERaoIRaQCSa3h3T3vdyOmsCF
v1N784E/1rtdPkg/QaEJjgPQ062CP2T8JLL04a+9Ba36E0ELCubWCF
G/7E1F8A00rjBB1B+100837cm/1JH7g/Sgqdt4RjZ0rcc713L0J1943
YgQb/ENY4IRQ/0a/paJgU2q1PbGjN8V5D4nuc31L049B4pRjST+cEJMO
8PUCE3c0vSrv0n0LshLxU8hQ0R4cYelPzy4ALC12nqB8ChaF4I4J5I
AIP2REhX19RFPj6X0XV500za64k1jvzxIR40z06com6egp14aB0sunZ1Ja
AgYBA2Ggpb1vqBKCgSgSIB3DQEBQ0A4IRDo6wggERaoIRaQCSa3h3T3vdy
bbL8h6gP7DDeuJ338vFNYJZLAV4QgEBAQH/BAQ0AgSv0BGA1UeBQEg
NBRBHR1d03a-dch1d15pcy5vencd4gYD/001AQH/BCa0Bg1T0vYBQURIsIG
AQUR0vD8ggrBgEFPQCIRB0Gg1vRQ8BA4EBBAUCA7gn0A3YD/001AQH/BA1c
Bj0gh1IG0v9BAQF0CAQ0G0R08v9EBELJ0vF5aap1xIG2B149E1FBP4E
N0v37a2g1/3700d/roZm77cc73oJ1L1F4JAPv204827J7F7m4QPB8ecD06o
j1ba1dL5349HQHCSv1aF/0h1d/CgUQvGaTym11+1B0vF01v2048HBRJDU
nc4vD0F8e1Fm0zmYasav90J8311d1v061GGRJ0C8Cf+rEFG+pg33eZP35U
vUR10m60V1o410010ro0/0h1L2Vcj1L4P0F4Ua23h4E1P7c5P2CaZ5P3cl
n0GzChclq/1cnp0pdcD0vZ8aigT0A3v9n7mCFTED1Rrj/g==
-----END NEW CERTIFICATE REQUEST-----

CA Server Response

Cert Issuer Info
CA Server Type: PKCS10 CA MS Cert Service SCEP Server Open CA EJB CA
CA Server URL: http://gemstar.usae.avaya.com:18080/prodsigndcertdemo/jp Login Download CA Certs
Issuer Subject DN:
Issuer Alias:

Buttons: Generate PKCS#10, Generate CRMF, Help, Cancel



HowTo the command line use openssl

```
$ openssl
OpenSSL> req -new -key my_private.key -out my_request.csr
Enter pass phrase for my_private.key:
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:NL
State or Province Name (full name) [Berkshire]:Limburg
Locality Name (eg, city) [Newbury]:Venlo
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Teus Hagen
Email Address []:teus@theunis.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> quit

$ ls
my_private.key  my_request.csr
$ vi my_request.csr

Get it signed with CAcert,
cut/paste signed cert into my_cert.crt
```

```
$ cat my_cert.crt my_private.key >my_cert.pem
$ rm my_cert.crt my_request.csr my_private.key
$ chmod go-w my_cert.pem
$ vi my_cert.pem

make it ready for import into thunderbird

$ openssl pkcs12 -export -in my_cert.pem -inkey
my_cert.pem -out my_cert.p12
```


HowTo on the command line certutil

```
% certutil -R -a -n teus@my_domain.org -x -t "u,u,u" -s "CN=Teus Hagen, E=teus@my_domain.org, C=NL" -d . -g 2048
>request.csr
Enter Password or Pin for "NSS Certificate DB": my_password_is_a_secret

A random seed must be generated that will be used in the
creation of your key.  One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.

To begin, type keys on the keyboard until this progress meter
is full.  DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:

|*****|

Finished.  Press enter to continue:

Generating key.  This may take a few moments...
% cat request.csr

Certificate request generated by Netscape certutil
Phone: (not specified)

Common Name: Teus Hagen
Email: teus@my_domain.org
Organization: (not specified)
State: (not specified)
Country: NL

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICijCCAXICAQAwRTElMAkGA1UEBhMCTkwITAFBgkqhkiG9w0BCQEWEnRldXNA
bXlfZG9tYWluLm9yZzETMBEGA1UEAxMKVG91cyBIYWdlbjCCASIwDQYJKoZIhvcN
...
aslwP+uZP9MwdFSwOEL81di860FNGLA5SkrlwwewfjtdPXRugYTXVZCn4pzyY/Fz
GS/2xpYuwaQDrz57L+YE4zakeoIuctZW9FWZZOj9
-----END NEW CERTIFICATE REQUEST-----
```


How-To use the command line certutil

```
% cd ~/.thunderbird/*.default ; certutil -H

% certutil -L -d .
sirogate.nl                P,p,p
aospan@netup.ru            ,p,
CA Cert Signing Auth - Root CA    CT,C,C
Teus Hagen's Root CA ID        u,u,u
gstark@rubyservices.com      p,P,p
StartCom Class 2 CA - StartCom Ltd. ,c,
Teus Hagen, Oophaga Foundation  u,u,u
Thawte Freemail Issuing CA - Thawte Consulting ,c,
Staat der Nederlanden Root CA    CT,C,C

% certutil -L -a -n aospan@netup.ru -d .
-----BEGIN CERTIFICATE-----
MIIE7DCCAtSgAwIBAgIDAv+vMA0GCSqGSIB3DQEBBQUAMHkxEVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHA6Ly93d3cuJ0Lm9yZzEiMCAGA1UEAxMZ
Q0EgQ2VydCBTaWduaW5nIEF1dGhvcml0eTEhGqGSIB3DQEJARYSc3VwcG9y
.....
K1aTaRN4xKjsO98Z9rOqrIoKULkkjZYIbV61P6dyHnE7oVxKpQs+wdaOzp
ML/DwtGfvao7uWcM/n2vNg==
-----END CERTIFICATE-----

% certutil -a -n pg@fuare.at -D -d .

% certutil -L -d . | grep fuare

% certutil -A -a -n pg@fuare.at -t "p,P,p" -i pg@fuare.at.crt -d .

% certutil -L -d . | grep fuare
pg@fuare.at                p,P,p
```

The commerce or the community track?

- certificate is linked to identification
 - identification is needed for e.g. trade and liability
- identification can be done:
 - via address, transfer of money -> \$
 - via Web of Trust and check of ID -> HR

Identification check is critical

your passport is it really you?

Shahiba Tulaganova UK journalist:

- ▶ within 5 months on east European markets
- ▶ bought 20 EU passports, 5 other
(UK, DId, F, S, NL, B, Es, PO, G, Cs, Pl, Au,)
- ▶ 300-3000 euro each

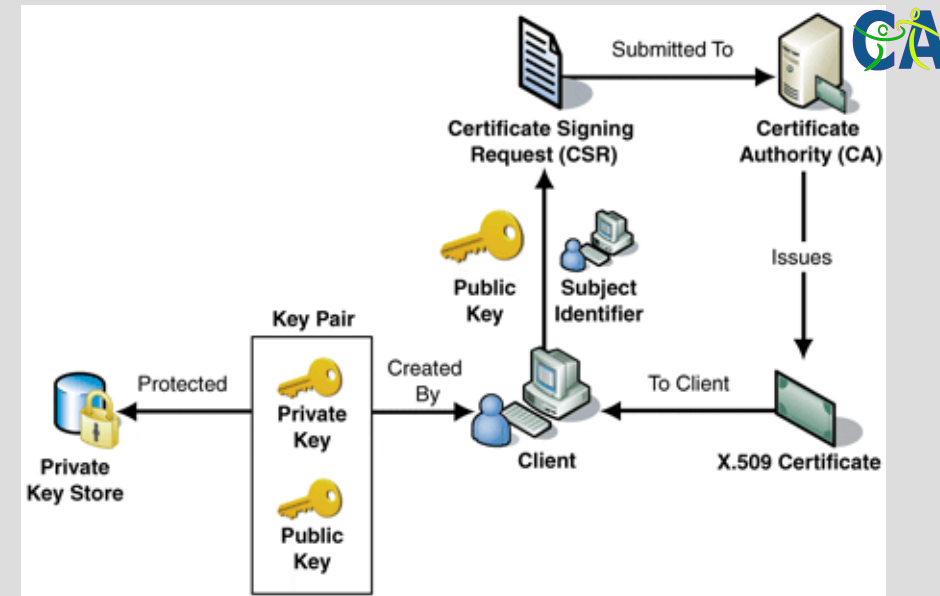
- ▶ and was able to pass UK border many times with them.



Certificate Authority signature

- create private key and the public key
- send public key to CA:
Cert Signing Request (CSR)
- CA signs public key of individual:
this public key is from him!
- yes the pub key comes from him!
- yes it is his signature on this email!

this is cool!



What is a CA?

- Certificate Authority

I, Certificate Authority XYZ, do hereby **certify** that Borja Sotomayor is who he/she claims to be and that his/her public key is 49E51A3EF1C.



Certificate Authority XYZ
CA's Signature

- the CA Root Key is added into “your” CA-list

On which authority?

- Signs your X.509 public certificate

When signed you might be trusted?

Why CAcert?



- mission

on internet allow everyone to protect their privacy

- no discrimination

- everyone should be able to afford it, and apply it

- high tech, transparent

- volunteers

The implication for CAcert

- Open CA
 - full commitment for openness
 - non-profit
 - no secrecy:
 - ▶ threats
 - ▶ updated
 - ▶ software tooling used
 - ▶ hardware tooling used
 - fully transparent

The disadvantages of openness

- **funding** needed

Hardware, PR, face 2 face meetings, connectivity

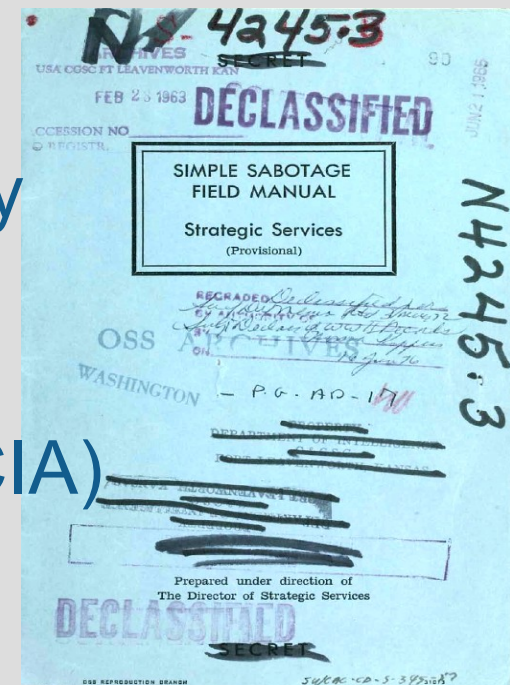
- **volunteers** needed

Short and long term, HR time is costly

- **many discussions**

OSS Simple Sabotage Manual (US CIA)

- **the sendmail phenomenon**



What is CACert?

- Community of Members, based on WoT

- CACert Inc. association
(July 2003, NSW Australia)

- legal entities:

- ★ Not fully and fully assured Community Members



Assurers



Arbiters



- ★ CACert Inc. board (7 members since Nov 2008)



The CACert supporting techi's

- help desk (80% forgot the password)
- translingo (26 languages)
- support
- non-critical and critical sysadmin teams
- development (php, java, ssh, pearl, http, mysql, openssl)
- education (Assurer manual, <http://cats.cacert.org>)

CAcert Assurance

- help, FAQ, tutorial documents and policies:
 - <http://svn.cacert.org/CAcert/>
 - and FAQ <http://wiki.cacert.org/wiki>
- **important ones:**
 - **CAcert Community Agreement (CCA)**
 - **Non Related Disclaimer and License (NRP)**
 - **Assurance (Organisation) Policy**

CAcert Community communication

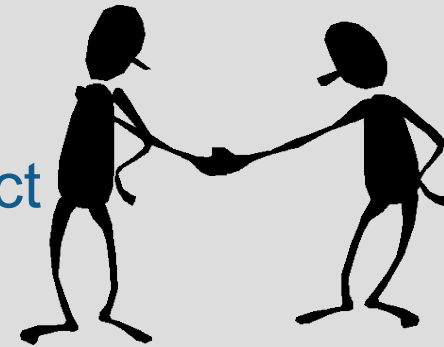
- email lists:
 - ➔ help email lists
 - ➔ Assurers email list
 - ➔ Arbitration email list
 - ➔ policy email list
 - ➔ association email list
 - ➔ Organisation Assurers email list



CAcert agreements

• CAcert Community Agreement (CCA)

- Community Member
- membership obligations: keys, email contact
- liability
- arbitration (max US \$ 1000 penalty)



➤ Non-Related Persons Agreement (NRP)

- license to use CAcert signed certificates
- disclaimer

➤ Contributor License Agreement (CLA)

Web of Trust and the Relying Parties (RP)

- provisions regarding apportionment of liability
- financial responsibilities:
 - ➔ indemnification by relying parties
 - ➔ fiduciary relationships
- like with Open Source: license and disclaimer, permission to use, no permission to rely on.



CAcert Policies

- Policy on Policies (PoP) (**ready**)
- (Individual) Assurance Policy (AP) (**ready**)
 - ➔ Assurer Manual (**pending**)
- Organisation Ass. Policy (OA policy) (**ready**)
 - ➔ Sub-policies ready for Europe, USA, Australia, ...
 - ➔ Organisation Assurer Manual (**to do**)
- Cert. Policy Statement (CPS) (**close to ready**)
- Security Manual (**close to ready**)

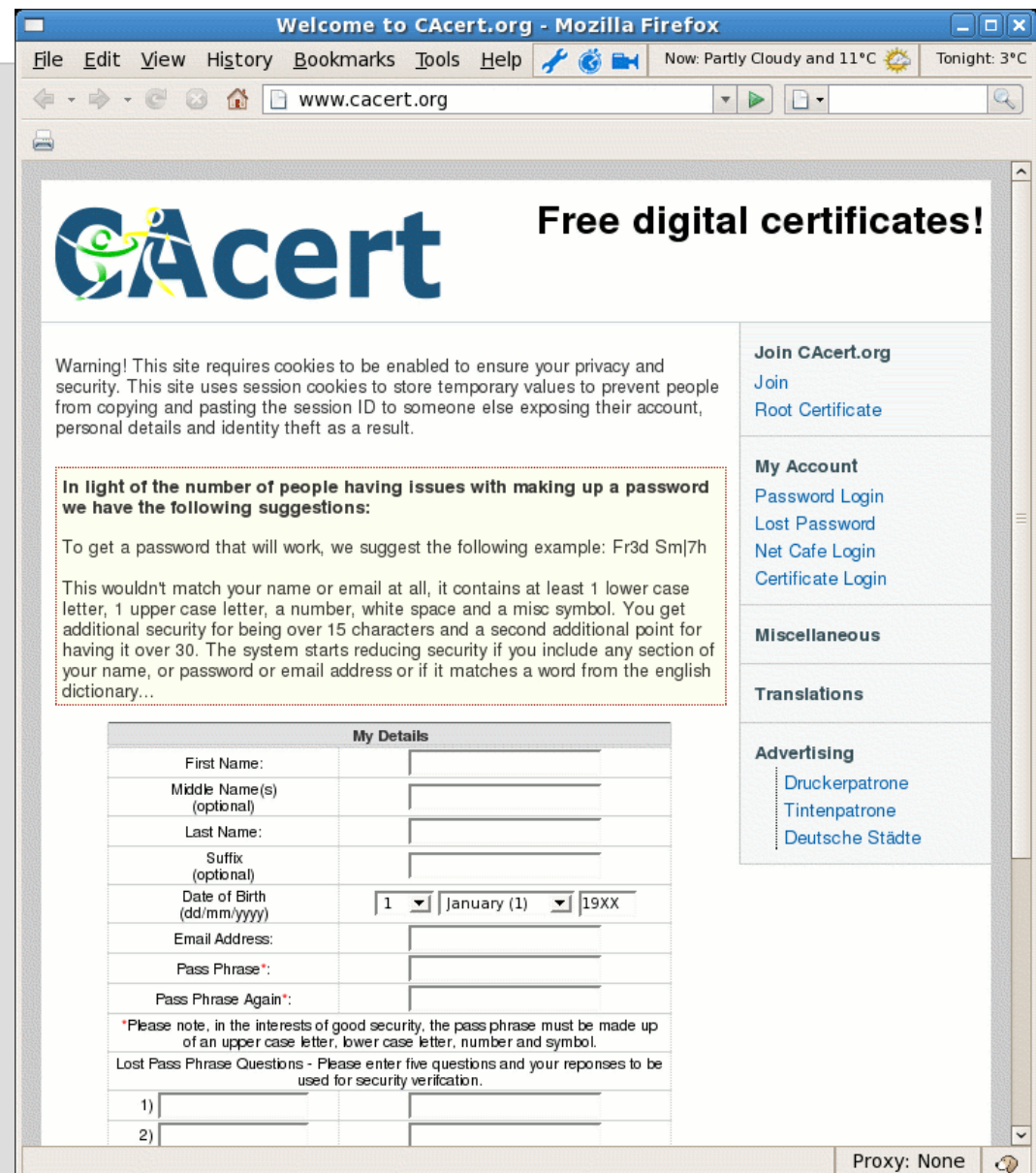
CAcert policies (2)

- Remote (Individual) Assurance Policy (pending)
- Dispute Resolution Policy (ready)
- Policy on Foundations (ready)
- Privacy Policy (ready)
- Communication Policy (ready)

HowTo join Community

HowTo join

- create
 - a CAcert account
 - password/phrase
 - five Q/A's
- remember them!



Welcome to CAcert.org - Mozilla Firefox

File Edit View History Bookmarks Tools Help Now: Partly Cloudy and 11°C Tonight: 3°C

www.cacert.org

CAcert

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.

In light of the number of people having issues with making up a password we have the following suggestions:

To get a password that will work, we suggest the following example: Fr3d Sm|7h

This wouldn't match your name or email at all, it contains at least 1 lower case letter, 1 upper case letter, a number, white space and a misc symbol. You get additional security for being over 15 characters and a second additional point for having it over 30. The system starts reducing security if you include any section of your name, or password or email address or if it matches a word from the english dictionary...

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="password"/>
Pass Phrase Again*:	<input type="password"/>
<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"/>
2)	<input type="text"/>

Join CAcert.org
[Join](#)
[Root Certificate](#)

My Account
[Password Login](#)
[Lost Password](#)
[Net Cafe Login](#)
[Certificate Login](#)

Miscellaneous

Translations

Advertising
[Druckerpatrone](#)
[Tintenpatrone](#)
[Deutsche Städte](#)

Proxy: None

Get your identity checked!

the Assurance

- complete **CAcert Assurance Form** (paper ware)
- show your Identity Cards to **CAcert Assurer**
sign CAP and
show passport, driver license, the more the better
- await Assurer to complete the assurance
you get points **10-35** per assurance (you need >50!)
- and you get an email, view your details
- create email/domain certificate entry
- at home: create, cut/paste your Certificate Sign Request
to **CAcert** web site and import the new certificate



CAP form

complete CAP with

- ➔ full name
- ➔ date of birth
- ➔ primary email address
- ➔ date of Assurance
- ➔ signature while there

The CAcert Assurance Programme (CAP) aims to verify the identities of Internet users through face to face witnessing of government-issued photo identity documents. The Applicant asks the Assurer to verify to the CAcert Community that the Assurer has met and verified the Applicant's identity against original documents. Assurer may leave a copy of the details with the Applicant, and may complete and sign her final form after the meeting. If there are any doubts or concerns about the Applicant's identity, do not allocate points. You are encouraged to perform a mutual Assurance.

For more information about the CAcert Assurance Programme, including detailed guides for CAcert Assurers, please visit: <http://www.CAcert.org>

A CAcert Arbitrator can require the Assurer to deliver the completed form in the event of a dispute. After 7 years this form should be securely disposed of to prevent identity misuse. E.g. shred or burn the form. The Assurer does not retain copies of ID at all.

For the CAcert Organisation Assurance Programme there is a separate special SOAP form.

Date and location of the face-to-face meeting: 2008-12-31, Grubbenvorst, the Carabiën

Applicant's Identity Information		points allocated
Exact full name on the ID: drs. T. Fabrice Ghuege-Denis drs. Teus F. Ghuege-Denis Email address: tesu.hagaen@thesu.xs4all.eu	(type of ID shown) (führerschein/paspoort)	max 20
	Date of Birth 1945-10-06	
Applicant's Statement		
Make sure you have read and agreed with the CAcert Community Agreement http://www.CAcert.org/policy/CAcertCommunityAgreement.php		
<input checked="" type="checkbox"/> I hereby confirm that the information stating my Identity Information above is both true and correct, and request the CAcert Assurer (see below) to witness my identity in the CAcert Assurance Programme.		
<input checked="" type="checkbox"/> I agree to the CAcert Community Agreement.		
Date 2008-11-04	Applicant's signature	
Assurer's Statement		
Assurer's Name: mr A. B. C. Assurer assurer.email@cacert.org	Date of Birth 2010-12-32	
<input checked="" type="checkbox"/> I, the Assurer, hereby confirm that I have verified the Applicant's Identity Information, I will witness the Applicant's identity in the CAcert Assurance Programme, and allocate Assurance Points.		
<input checked="" type="checkbox"/> I am a CAcert Community Member, have passed the Assurance Challenge, and have been assured with at least 100 Assurance Points.		
Date 2008-11-04	Assurer's signature	

CAcert Organisation Assurance

- the organisation entity is in control:
 - ➔ (domain) server certificates
 - ➔ (email) client certificates

for individuals within the organisation
- organisation needs to have:
 - ➔ **CAcert Assured administrator**

> 100 assurance points

Organisation Assurance requirements

- legality of organisation:
 - eg registration proof at trade office
- proof (CEO) signatures/stamps are legal
- proof system administrator can acquire and manage certificates (formal letter of designation)
- completed **CAcert** Organisation Assurance form
- assured by **CAcert** Organisation Assurer

COAP form

CAcert

Organisational

Assurance

Programme

details / policy is
country
dependent

The CAcert Organisation Programme (COAP) aims to verify the identity of the organisation. The Applicant asks the Organisation Assurer to verify to CAcert Community that the information provided by the Applicant is correct, and according to the official trade office registration bodies. For more information about the CAcert Organisation Assurance Programme, including detailed guides to CAcert Organisation Assurers, please visit: <http://www.CAcert.org> A CAcert Arbitor can require the Organisation Assurer to deliver the completed forms and accompanying documents in the event of a dispute.

Organisation Identity Information

Name of the organisation	Stichting Oophaga foundation
Address (comma separated)	De Burgerstraat 25, office 268, 1098 SJ, Amsterdam-Buitenveldert
Type, jurisdiction (state)	foundation, Netherlands
Registered Trade Names	Oophaga
Registration (id, name, region)	NL-238603-AA02, Kamer van Koophandel, Amsterdam
Internet Domain(s)	oophaga.eu, oophaga.net, oophaga.nl, oophaga.org
Technical contact info	Görge H. M. Sämple ☎ +31 77 327996 tesu.hagaen@thesu.xs4.nl.eu

Organisation's Statement

Make sure you have read and agreed with the CAcert Community Agreement
<http://www.CAcert.org/policy/CAcertCommunityAgreement.php>

Director **Gerard H. M. Sämple** ☎ +31 773270066

- I agree to the CAcert Community Agreement.
- I hereby confirm that all information is complete and accurate and will notify CAcert of any updates or changes thereof.
- I am duly authorised to act on behalf of the organisation, I grant certificate administration privileges to the specified organisation administrator and, I request the Organisation Assurer to verify the organisation information according to the Assurance Policies.

Date
2008-08-18

Signature and organisation stamp

Organisation Assurer's Statement

Organisation Assurer **My O. Assurer-Name** ☎ +31737201060
Assurer@cacert.org

- I, the Assurer, hereby confirm that I have verified the official Information for the organisation, I will witness the organisation's identity in the CAcert Organisation Assurance Programme, and complete the Assurance.
- I am a CAcert Community Member, have passed the Organisation Assurance Challenge, and have been appointed for Organisation Assurances within the country where the organisation is registered.

Date
2008-08-25

Organisation Assurer's signature

It is free

What does one get?

- client certificates:
 - ➔ as many as you have email addresses
 - ➔ > 50 assurance points your full name on it!
- server certificates:
 - ➔ as many as you have domains
 - ➔ > 50 assurance points
- code signing:
 - ➔ > 100 assurance points
- stamping service
- HowTo's and on line support

CAcert assurance

- print your CAP form
- take your ID's
- get assured by an Assurer:
 - individual CAP
 - or
 - as organisation COAP
- documents/policies:
 - <http://svn.cacert.org/CAcert/>
 - and FAQ <http://wiki.cacert.org/wiki>



CAcert is community work

- >10.000 “to be” assurers,
>1100 qualified assurers
- translations into 30 languages
- > 150.000 certificates in use
- >100 on the help desk:
 - 7 days * 24 hours email support
- world wide
- and **CAcert** certificates are **free**: at no charge



The unexpected message

- my OS or browser shows the threatening message, something as this:

*“do not know the CA signing this certificate,
do you trust it? YES/NO”*

- so I said:

*“CAcert visit this URL how to spend € 250K.
If not, I do not trust you.”*

The audit

- Mozilla CA policy as till November 2008
mid 2005, David Ross Criteria (DRC)
the unpublished list:

David Ross Criteria (DRC) (thanks to Ian Grigg)

DRC reference(s)	Title / Area	Comments
A.1	Configuration-Controlled Specification (CCS)	This is effectively the list of controlled documents that the audit insists is in place.
A.2-3	Certification Practice Statement and Certificate Policy	The core technical rules of the CA.
A.4	Privacy	
A.5	Security Manual	DRC expects security details to be extracted from CPS/CP.
A.6	Risks, Liabilities	short list of disclosures.
B	Access for Subscribers, and "the General Public"	short list of disclosures.
C.1	Documentation Conformance	<i>"The CA has been repeatedly observed to operate in general conformance with its CPS."</i>
C.2-4	Security, Maintaining Root Certificates	<i>"The root certificate private key is stored secure from electronic and physical compromise."</i>
C.5-8	Generating / Signing / Renewing / Revoking	"Certificates are signed in a timely manner"
C.9	Use of External Registration Authority	<i>"RAs provide the CA with complete documentation on each verified applicant for a certificate (see &A.2,w)"</i>

Mozilla web side December 2008

- https://wiki.mozilla.org/CA:How_to_apply
 - Root CA inclusion request (send bug report)
 - information gathering and verification
 - public discussion (2 phases)
 - Inclusion
- https://wiki.mozilla.org/CA:Information_checklist
 - ca 11 chapters in total 35 requirements

What do the requirements do?

impose:

- ➔ control
- ➔ risks
- ➔ liabilities
- ➔ obligations

for the end user.

CAcert is currently

- being **audited** (Ian Grigg), the goal: to get into software distributions and browser: Mozilla, ...
- put in place committed **agreements** for end user and for usage (license)
- accept and rule community accepted **policies**
- **quality assurance**: education and control
- dispute resolution by **arbitration**
- committed to the EU privacy directive (**EU DPA**)
- **CAcert** services moved into a high **secure location** in Nld
- system admin teams under NDA and background check
- tons of ISO9000 type of buroCrazyness
- endless discussions ...
- the new Root (Sub) Key ...



The CAcert new Root Key

- why?

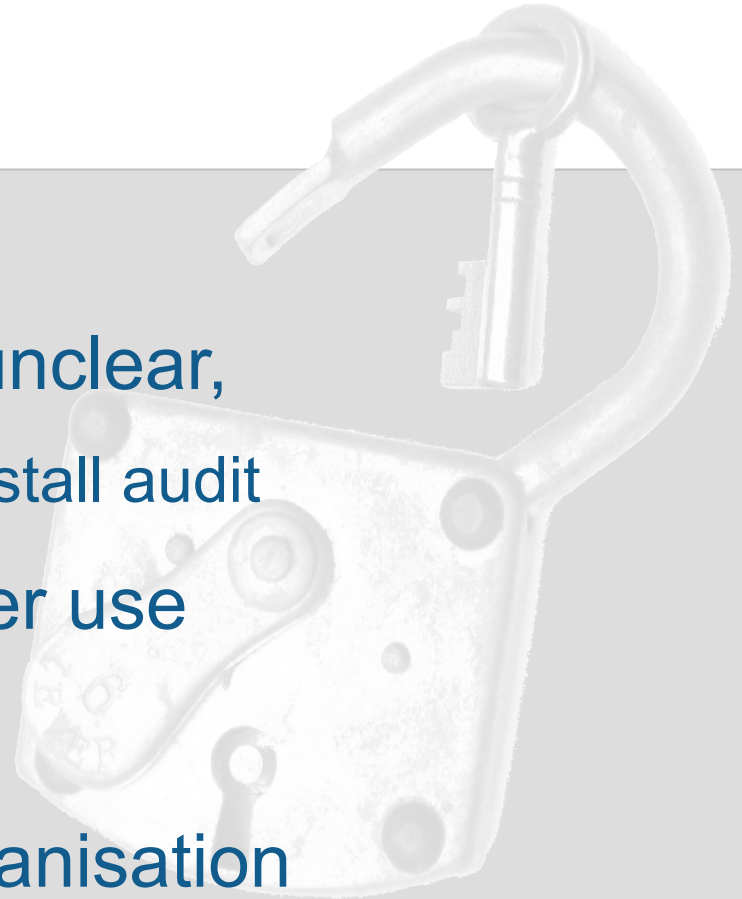
the “*four eyes principle*” is unclear,

the old two Root Key(s): will stall audit
newer technology and newer use

no secrecy: openness

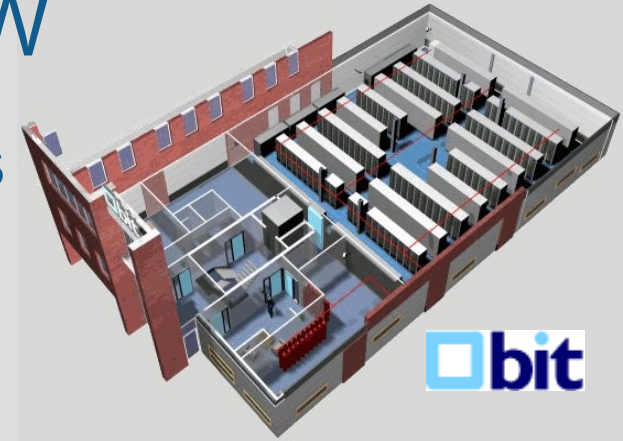
better suited for current organisation

history was built up



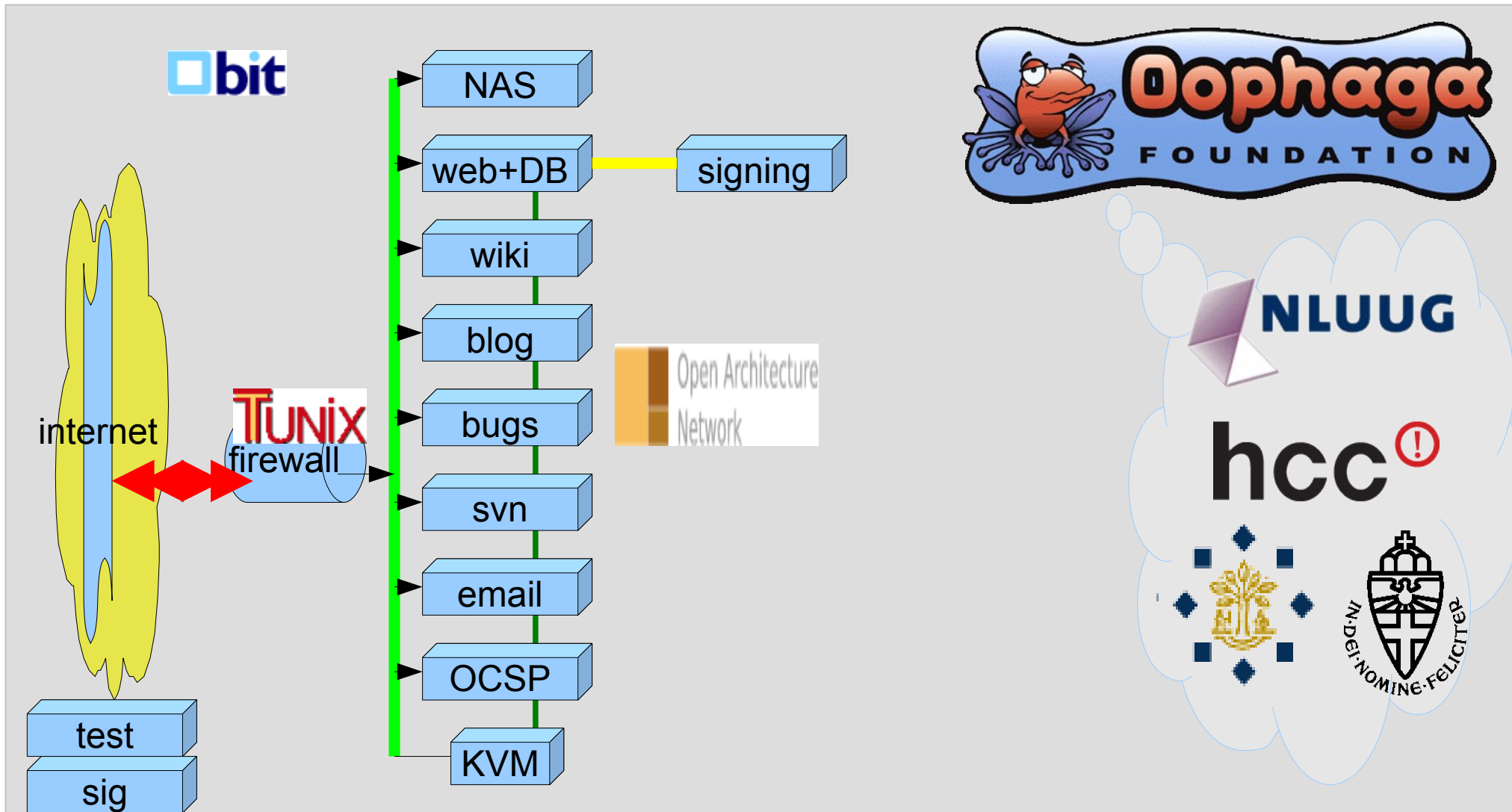
CAcert technical setup

- build on standard of the shelf HW
rack mount PC's, KVM & switches
(a rack full)



- build on standard of the shelf Open Software
Ubuntu, wiki, apache, php, GNU email list, svn,
ssh, openssl, gpg, BSD driven firewalls, ssl, Linux
driven internal firewalls, virtual hosts, ...

The CAcert machinery & servers



How to generate a secret X.509 key

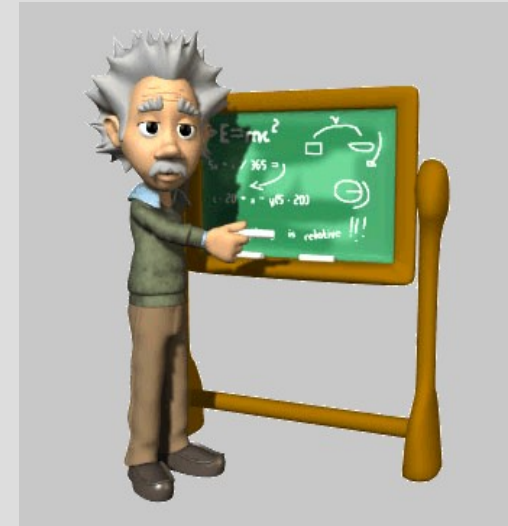
you need:

- ➔ standard of the shelf PC
- ➔ standard audio card
- ➔ standard Open OS: here Ubuntu 8.10
- ➔ standard X.509 tooling: e.g.
 - OpenSSL for key generation
 - Java for certificate information handling
- ➔ standard statistics tooling



Use the right random number

- random number generation
 - you need a lot of them
 - find the right HW combination...
 - find and check the right tooling:
 - ➔ Turbid (www.av8n.com)
 - calibration is complex, time consuming, too slow
 - ➔ **randomsound** (Linux tool, Debian)
 - make sure you have the right HW combination



Check your random numbers

- use <http://sig.cacert.at> to check
- use standard tooling:
 - ➔ statistics:
 - ➔ chi square >0.01
 - ➔ arithmetic mean = 127.5
 - ➔ Monte Carlo = Pi
 - ➔ serial correlation
 - ➔ compression figures, e.g. 7.99999 bits/byte

Statistical tooling

- ent

e.g.: `ent -c`

- israndom

e.g.: `od /dev/random | israndom -n -r`

check, check and check ...

The Key Generation Tooling (GPL)

see: <http://svn.cacert.org/CAcert/Software>

- OS and tools installation: `install.sh`
- key generation tooling: `ceremony.sh`
- copy keys, passwords: `CopyKeys.sh`
- and ... dismantle, destroy unencrypted keys

Install key generation

Internet
updates



Mother
USB
stick

Linux
distro

USB
sticks

- installed Ubuntu 8.10
- install script:
 - upgrade to latest 8.10
 - install tools
 - openssl, java encr lib
 - randomness
 - statistical packages
 - upload scripts
 - MD5 checks on versions

Generate random number

- randomness
 - sample 400K bytes
 - check result

ent:

- 7.999564 bits per byte
- chi square 241.31 50.00 %
- arithm mean value: 275.5056
- Monte Carlo Pi = 3.149971 error 0.27
- serial correlation 0.001544

Generate random number (2)

- ▶ israndom:
 - ▶ length 3145736.0 (ideal 3145728.0)
 - ▶ compression 3163464

Generate keys

- watch out (swap off) for:
 - ◆ random file **only** resides on USB stick and RAM
 - ◆ keys **only** on USB stick and RAM
 - ◆ passwords **only** on USB stick and RAM
- private keys: RSA 4096
- passwords generated size 32 bytes
- public keys publicized
- sign public keys, hash: sha1

What did we do on 28th November 2008 ?

1. generated Root Key, self signed
2. generated 4 Sub Root Keys,
signed by Root Key:
 - ▶ not Assured Members Sub Root Key (Class 1)
 - ▶ Assured Members Sub Root Key (Class 3)
 - ▶ 2 spare Sub Root keys
3. (Sub) Root Keys and passwd sticks for escrow
4. Sub Root Keys and passwd sticks for admin

Keys & passwords for escrow



Admin sub root keys and passwords



CAcert USB stick destruction tool



and ... dismantle used PC

- disk cleaner “shred” took 1.5 day
- deleted audio card
- deleted CDrom
- paranoia said:
 - parts (random number, private key) good be on disk, regeneration due to hardware combi
- social engineering seems to be easier ...

What now for the Sub Root Keys?

- get them installed (done)
- get them evaluated (pending)
- get policy for use of certificates defined and accepted (to do)

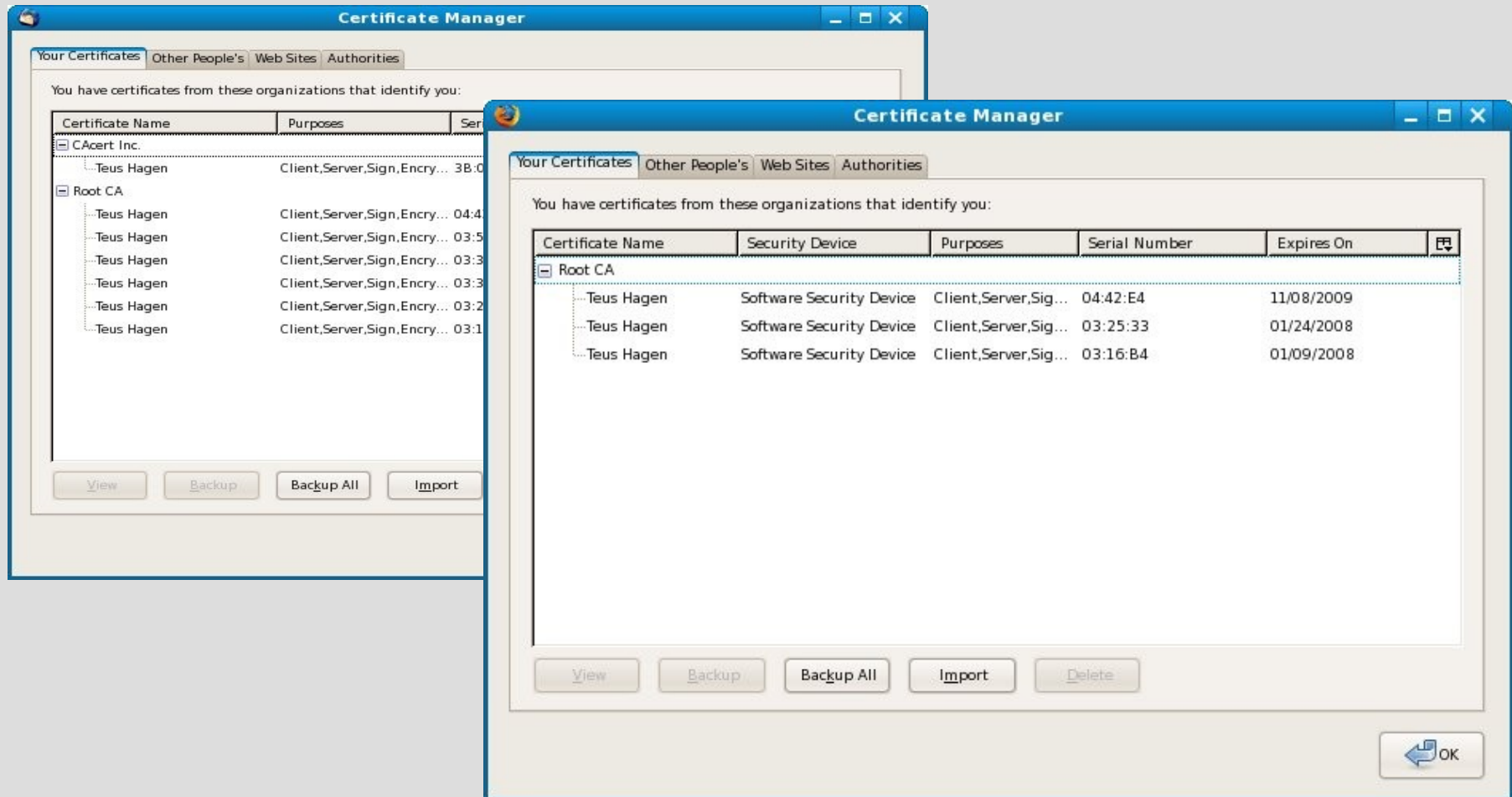
What now for audit

- finish audit project (36K Euro NLnet funding)
 - ➔ finish policies: CPS, sec & OA manuals
 - ➔ have auditor check on rulings
 - ➔ auditor final visits to location, assurance events
- send Mozilla ready signal and wait ...

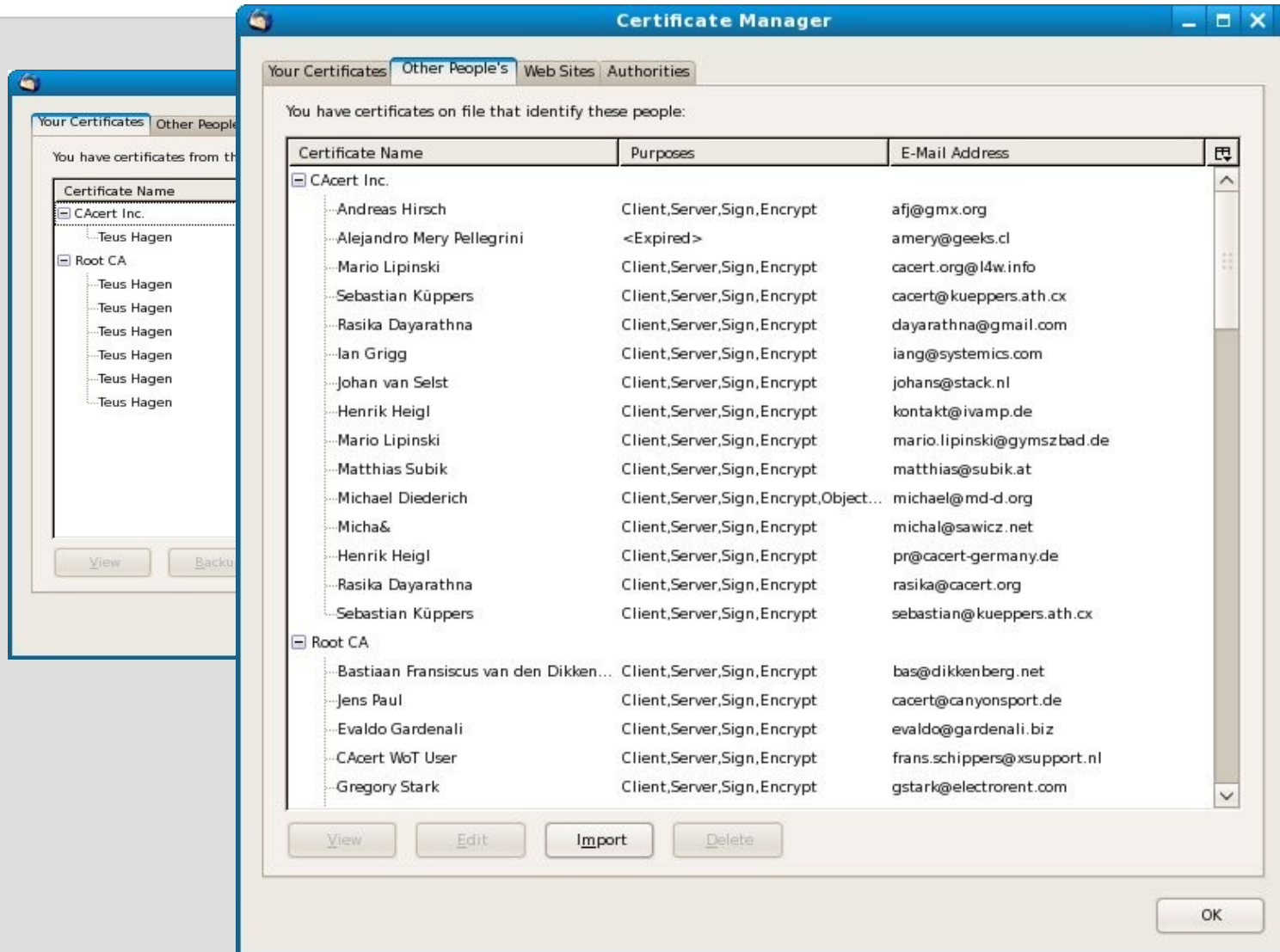
in the mean time, this is for you ...

- get people assured (scale up)
- get active for:
 - ▶ assurances (become a real Assurer and RFM)
 - ▶ developments
 - ▶ support
 - ▶ and: ... have fun as system admin & developer,
and join the teams ... get in touch!

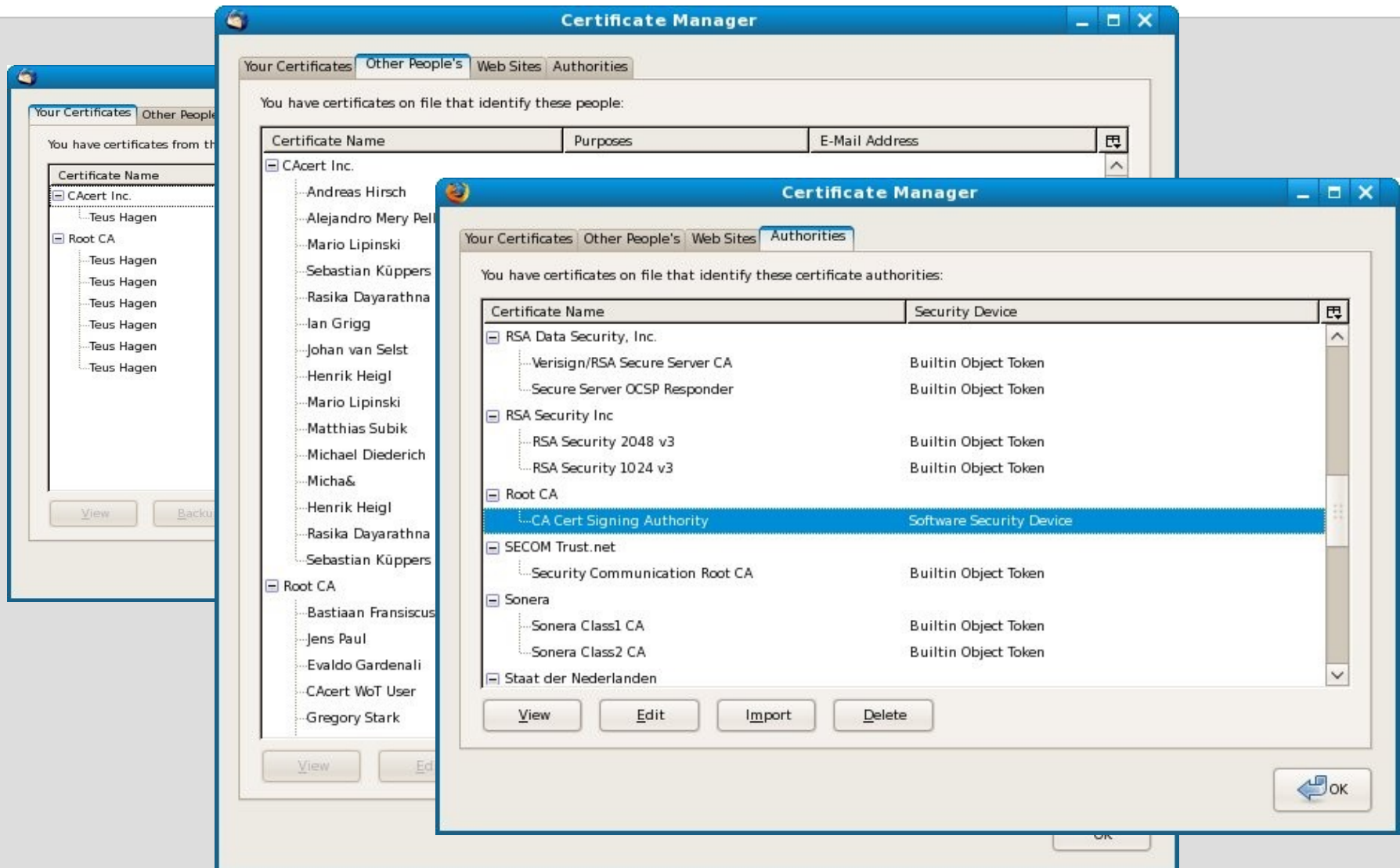
Thunderbird certificate usage



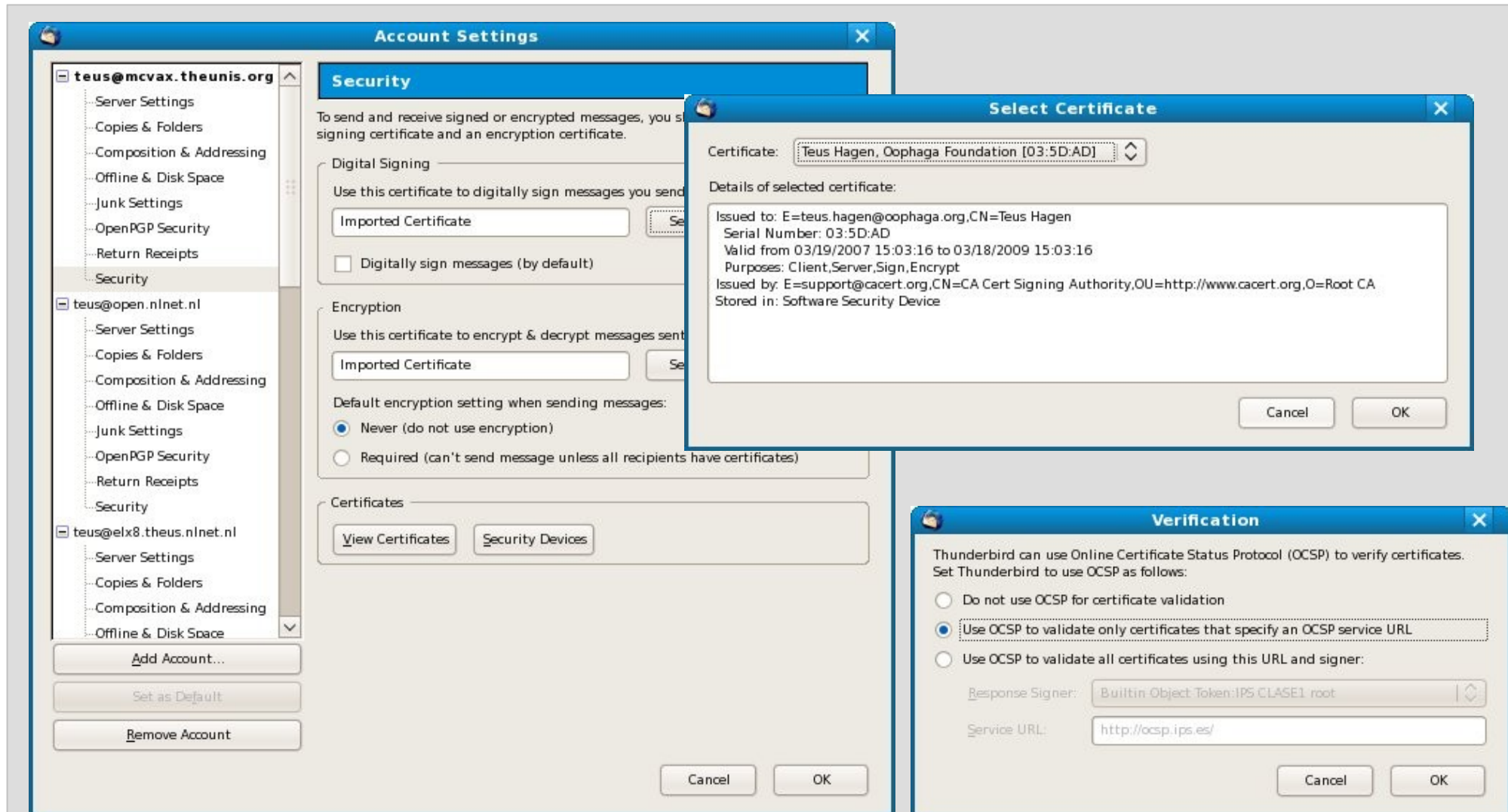
Thunderbird certificate usage



Thunderbird certificate usage



Thunderbird certificate usage



The screenshot displays the Thunderbird Account Settings window for the account `teus@mcvax.theunis.org`. The **Security** tab is active, showing options for digital signing and encryption. The **Digital Signing** section includes a dropdown for "Imported Certificate" and a checkbox for "Digitally sign messages (by default)". The **Encryption** section includes a dropdown for "Imported Certificate" and radio buttons for "Never (do not use encryption)" (selected) and "Required (can't send message unless all recipients have certificates)". The **Certificates** section has buttons for "View Certificates" and "Security Devices".

Three dialog boxes are overlaid on the settings window:

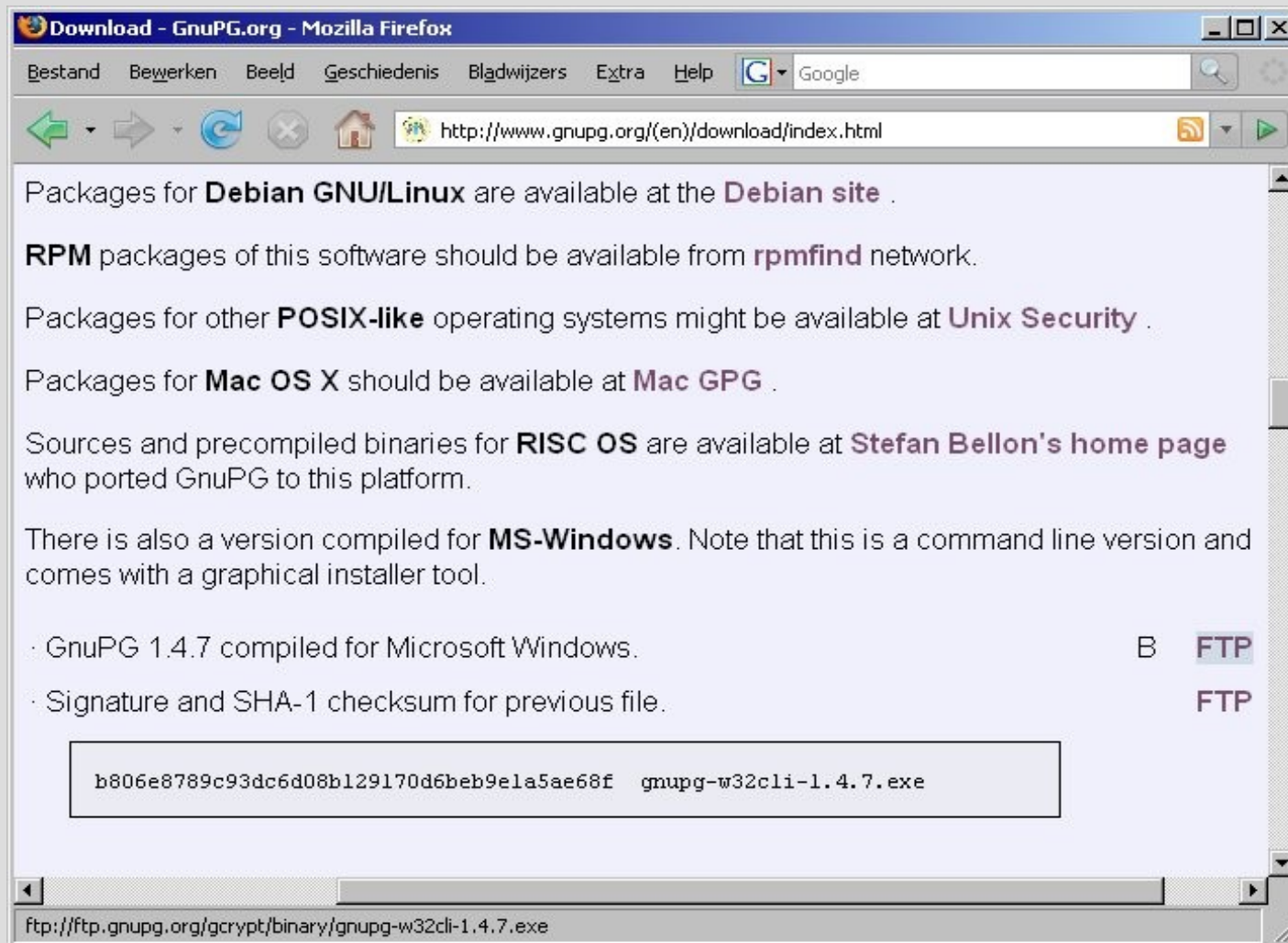
- Select Certificate**: Shows a dropdown menu with "Teus Hagen, Oophaga Foundation [03:5D:AD]" selected. The details of the selected certificate are displayed in a text area:
Issued to: E=teus.hagen@oophaga.org,CN=Teus Hagen
Serial Number: 03:5D:AD
Valid from 03/19/2007 15:03:16 to 03/18/2009 15:03:16
Purposes: Client,Server,Sign,Encrypt
Issued by: E=support@cacert.org,CN=CA Cert Signing Authority,OU=http://www.cacert.org,O=Root CA
Stored in: Software Security Device
- Verification**: Explains that Thunderbird can use Online Certificate Status Protocol (OCSP) to verify certificates. It offers three options:
 - Do not use OCSP for certificate validation
 - Use OCSP to validate only certificates that specify an OCSP service URL
 - Use OCSP to validate all certificates using this URL and signer:The "Response Signer" dropdown is set to "Builtin Object Token:IPS.CLASE1.root" and the "Service URL" text box contains "http://ocsp.ips.es/".
- Security**: A partially visible dialog box in the background, likely related to the certificate selection process.

PGP, GPG or GnuPG

- private/public key encryption
- Web-of-Trust
 - ➔ the game of collecting signatures
 - ➔ have your finger print ready
- sub-keys
- commonly used as check in Open Software distributions and repositories

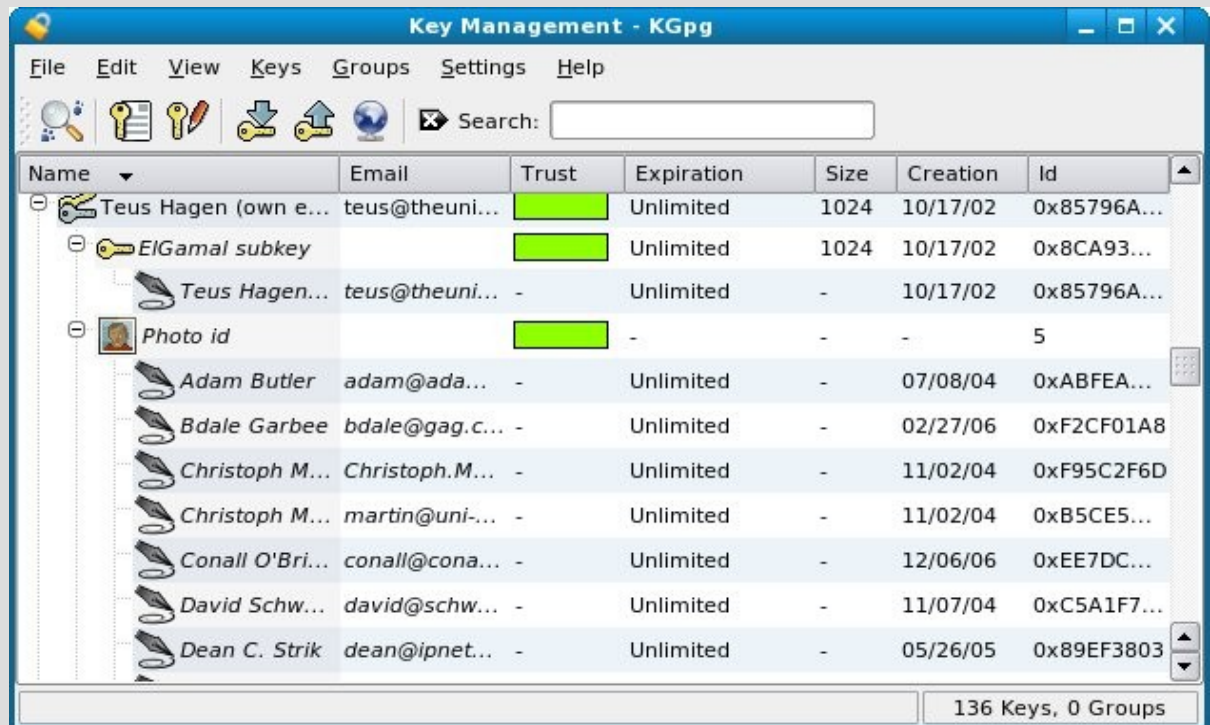


PGP/GPG install



GNUPG use

- Thunderbird plugin: OpenPGP/Enigmail
- KGPG



- Gnome Keyring Manager

KGPG keyring manager



PGP particularities

- PGP keyservers for public keys
 - ➔ pgp.mit.edu
 - ➔ keyserver.ubuntu.com
 - ➔ keys.pgpi.net
- PGP statistics
 - ➔ pgp.cs.uu.nl
 - ➔ the game of ranking

PGP and CAcert key signature

- Once a CAcert certificate you can have your PGP key signed by CAcert
- Usually CAcert assurers are willing to sign your PGP key as well

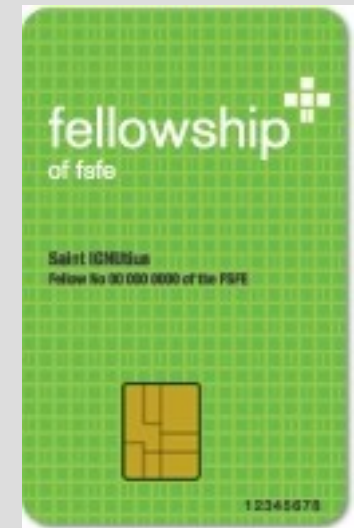
PGP & X.509 Certificate comments

- PGP name check is weak
- PGP ID check is weak (no policy)
- PGP no community agreement
- PGP young standard, pretty mature (> 15 years)
- X.509 are used in internet protocol (browser) communication
- PGP well used within technical Open Source community
- PGP not easy to install in email handlers
- PGP main use: email and software distribution
- PGP key servers/statistics and spam?
- No X.509 certificate distribution infrastructure

FSFE and GNUpg

Free Software Foundation Europe

- FSFE Fellowship crypto card



Questions to ask now:

- How to recover my password, why so complex?
- How do I get involved?
- How to import/distribute certificates?
- How to use OpenSSL?
- Why should we have an Organisation Assurance?
- What is changing for me now?
- The CAcert <http://wiki.cacert.org/wiki/> says this, and you say that? Where do I find the search button?
- <http://svn.cacert.org/CAcert/> Is a place to look for?
- What is the difference between CAcert Community Member and CAcert Association Member?
- What does a certificate look like?

some references and handy URL's

- <http://www.cacert.org>
- <http://wiki.cacert.org/wiki/>
- <http://svn.cacert.org/CACert/>
- <http://www.pgpi.org/doc/pgpintro/>
- <http://www.cacert.nl>
- <http://sig.cacert.at>
- Bruce Schneier:
 - ➔ Applied Cryptography, publ. John Wiley, 1996.
 - ➔ Secrets and Lies: Digital Security in a Networked World, publ. John Wiley, 2000.
 - ➔ <http://schneier.com/blog> Hacking the new Boeing 787 Dreamliner airplane
- http://tlsreport.layer8.net/reports/My_URL?protocol=https

A decorative graphic featuring several thick, curved lines in green and yellow. In the center is an orange diamond shape containing the word 'TIP' in yellow, underlined. Below the diamond is a block of text.

TIP

Remember, your sense of conviction and your involvement with **CAcert** are critical to its success.

Thanks, some materials are used from: Wren Hunt, Ian Grigg and others