

# TIP

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

## what is CAcert about?

### content

- trust and identity
- X.509 digital certificates
- encryption technology
- **CAcert** what it is, how to join and get certificate, services, and why there is a CAcert community
- the HowTo for Linux Firefox/Thunderbird and command line
  - certificate installation
  - certificate usage
- why should I?
- PGP/ GnuPG



## on the internet nobody knows you are a dog



## trust is not identification!

who are they?

trust worthy?

- use digital signatures for identification
- via Web of Trust identification
  - GPG/PGP
  - **CAcert** X.509 certificates



## identification (your email from Nigeria)

- verify email / web
  - sender
  - receiver
  - MTA client
  - MTA server
- forging



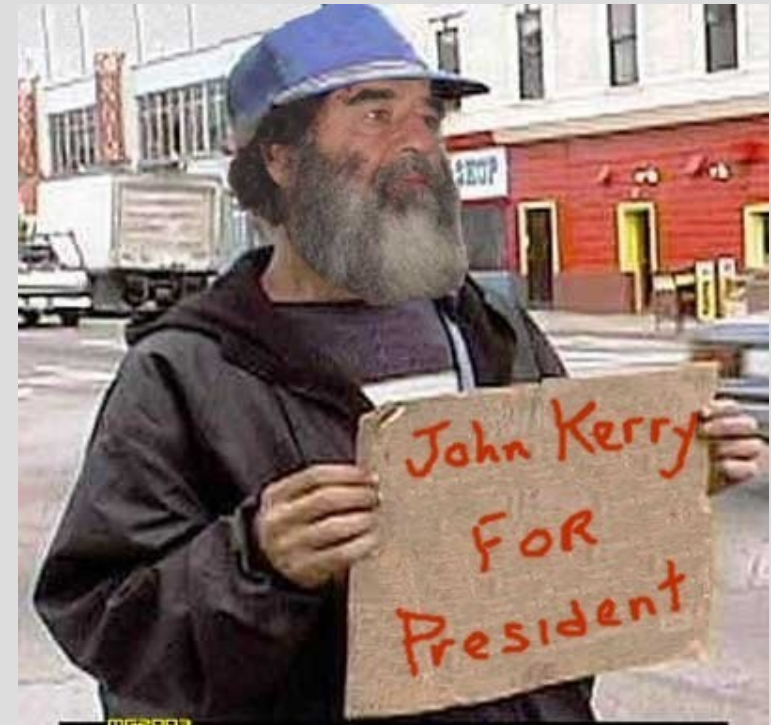
## your passport is it really you?

- BBC 1 Panorama 1<sup>st</sup> of December 2006
- Shahiba Tulaganova UK journalist:
  - within 5 months on east European markets
  - bought 20 EU passports, 5 other  
(UK, Dld, 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.



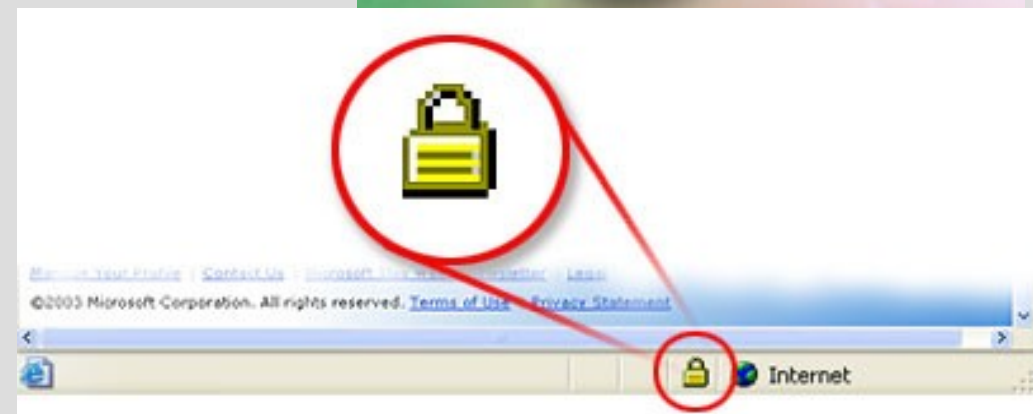
## secure digital content

- documents
- images
- software code
  
- use stamping



## secure data transfer

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





## certificates are official

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



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

## the technology: encryption

- what is encryption
- what is encryption key
  - Symmetric Key or shared key
  - Private and Public key
- applications which use private/public key encryption
  - PGP/GPG
  - X.509 digital certificates

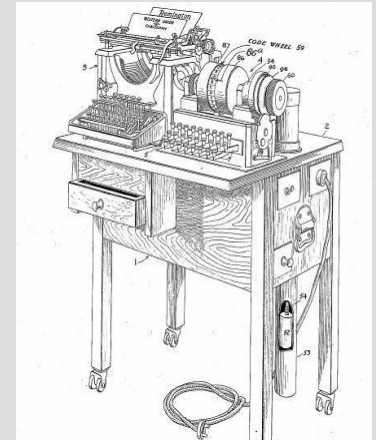
## encryption

Bruce Schneier:

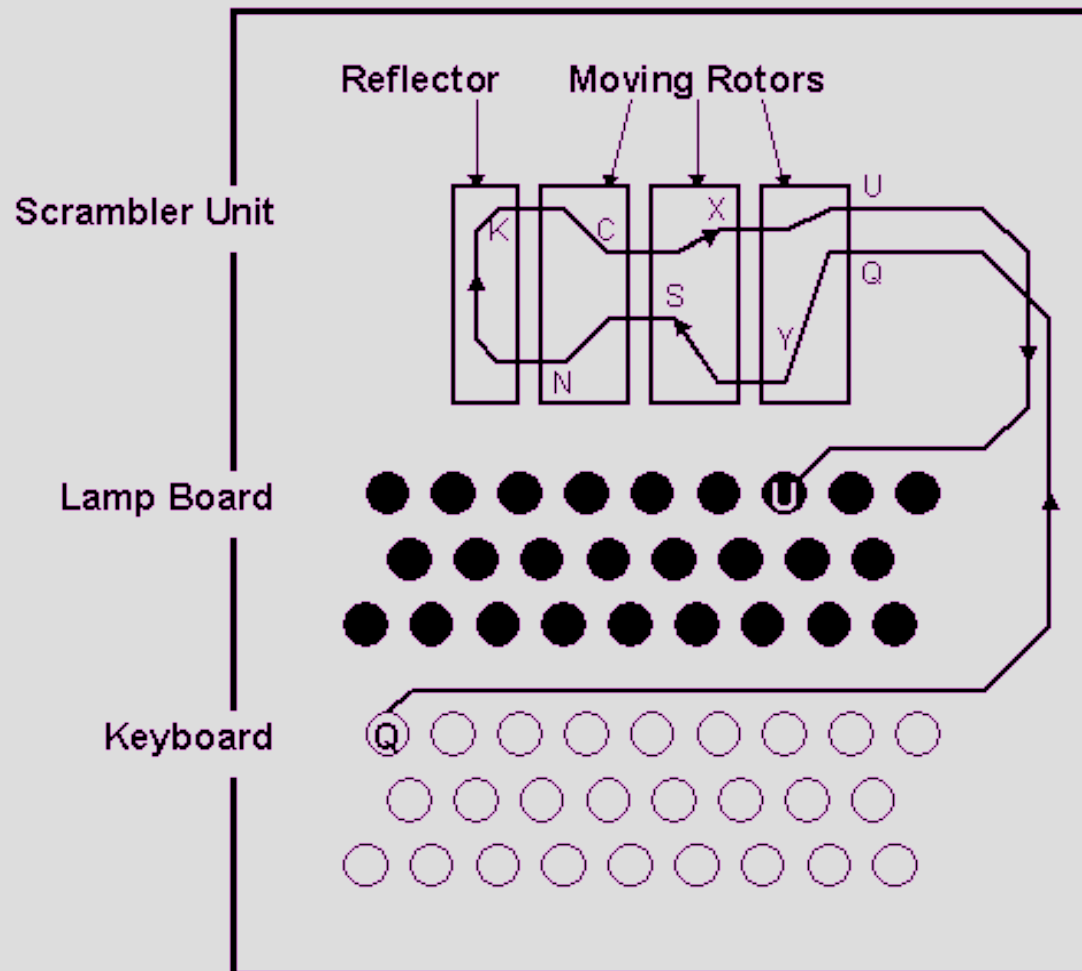
“Any person can invent a security system  
so clever  
that she or he can't think of how to break it”

## encryption

- Herbern
- Enigma
  - Germany second world war
  - The mechanism
  - hacked



# Enigma technology

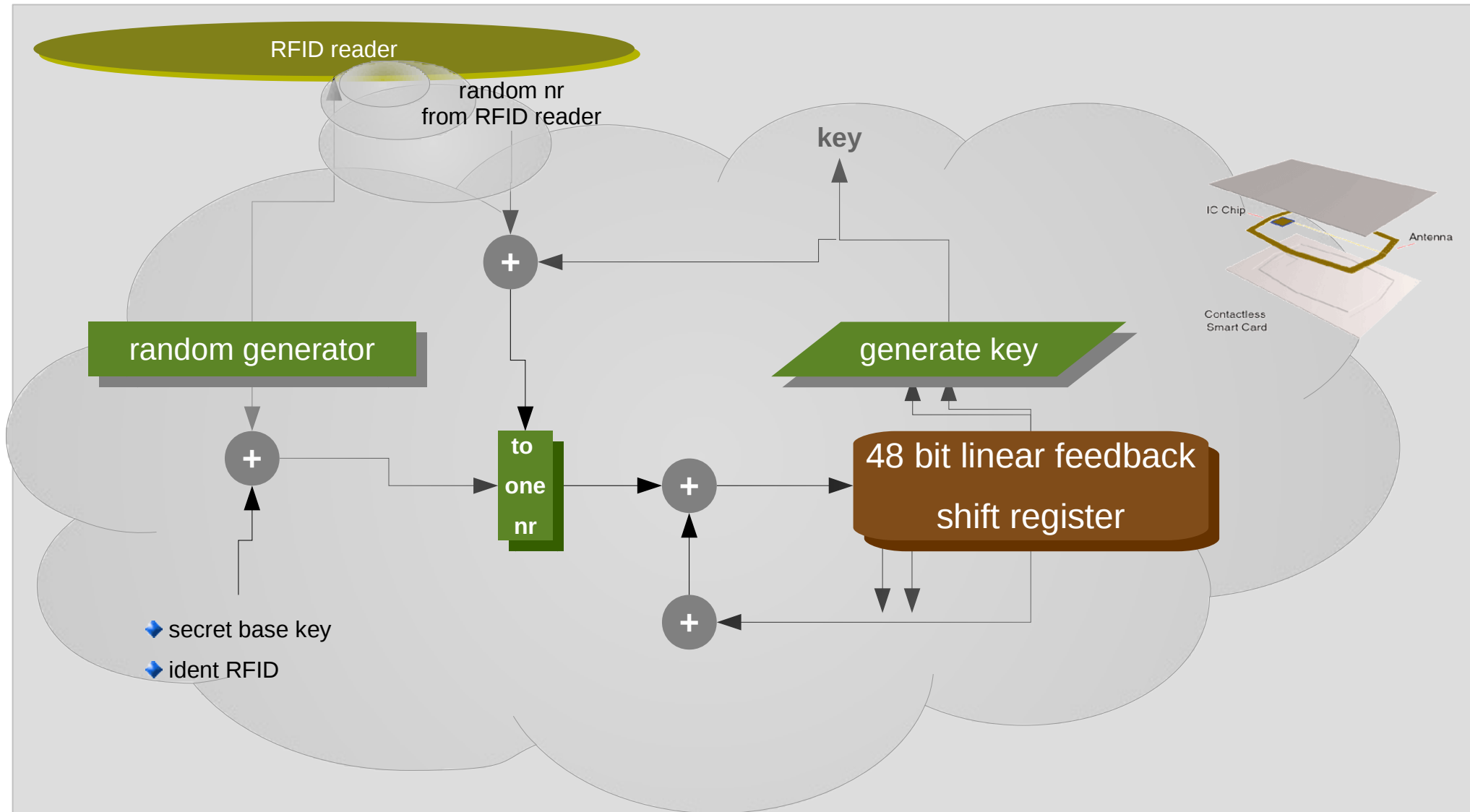


## RFID chip hacked Dec 2007

- 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

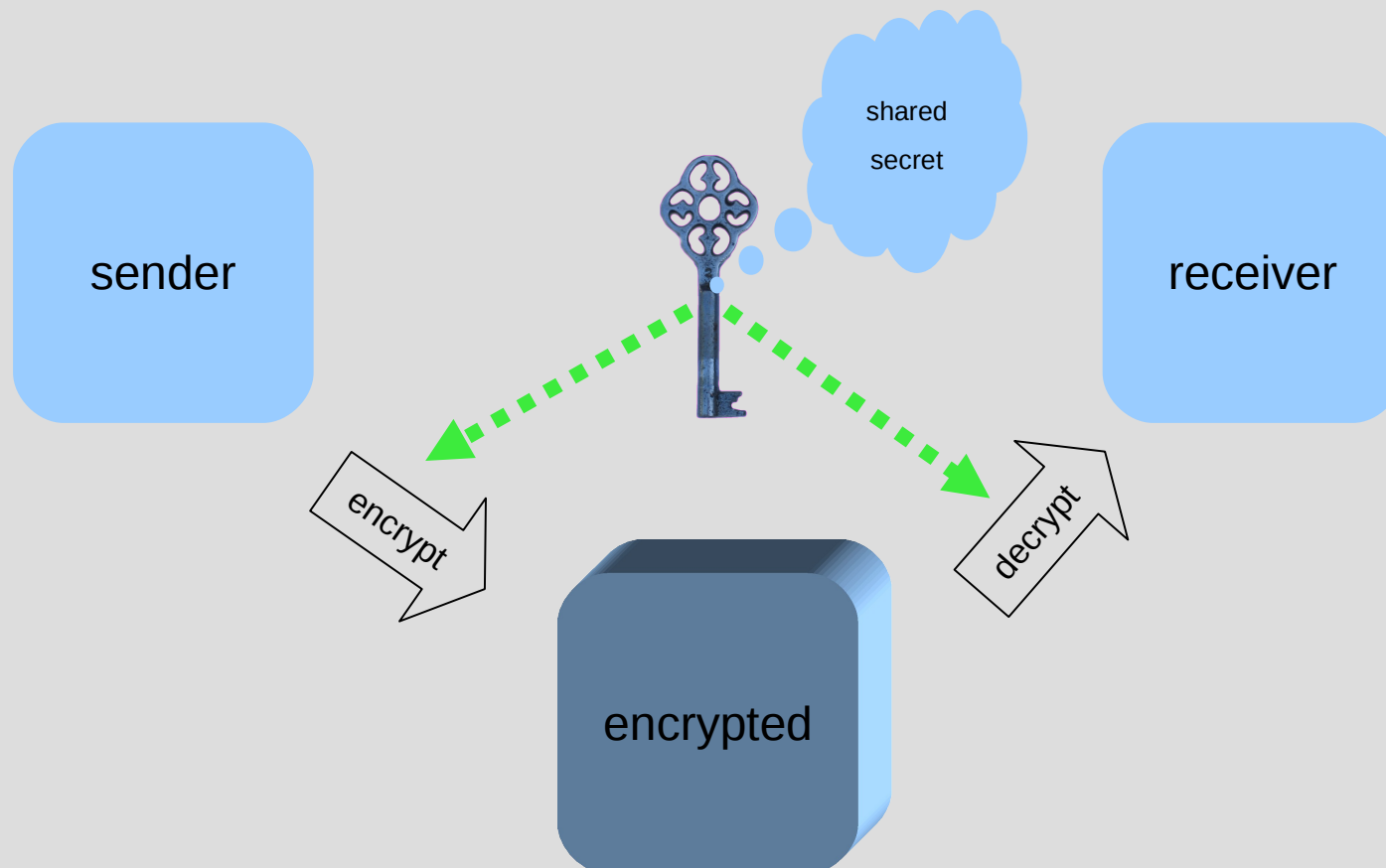


## Mifare Classic workings (Nohl & Plötz)



## encryption key types

### symmetric key encryption





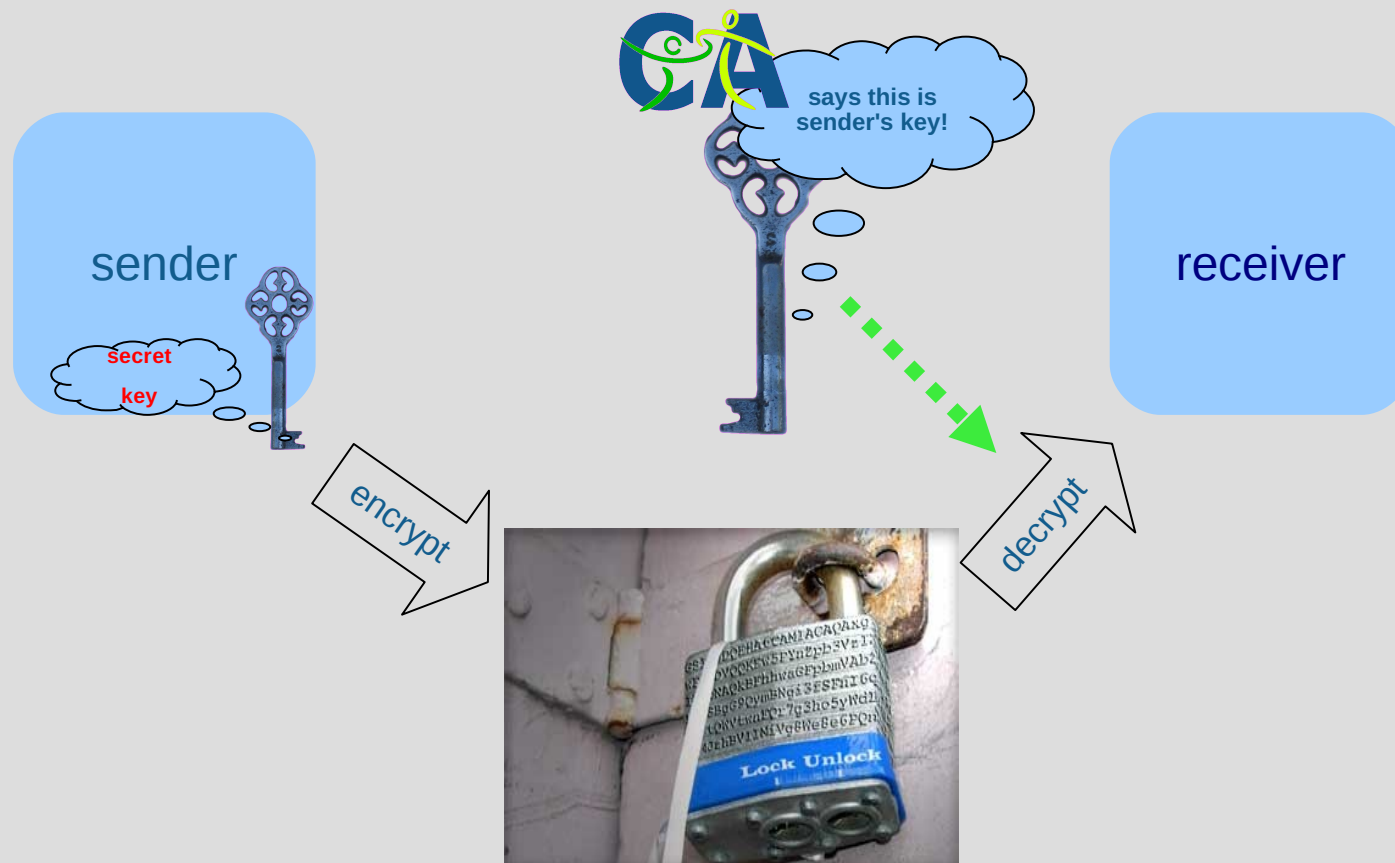
## asymmetric key encryption

that message can only be read by him

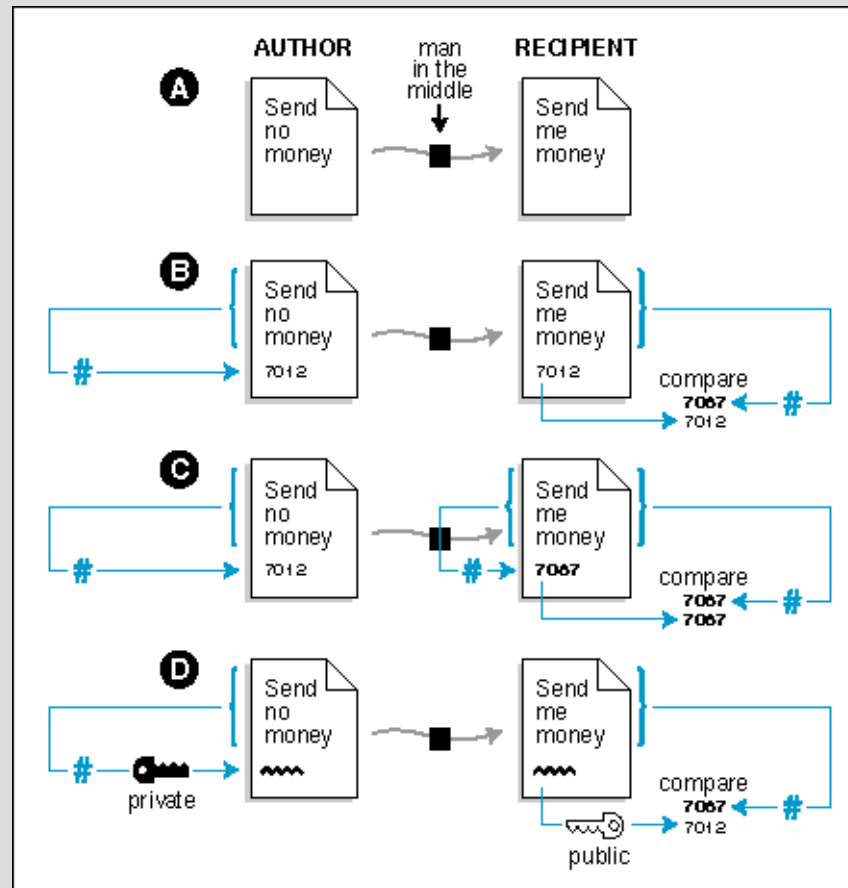


## asymmetric key encryption

that message can only come from him!



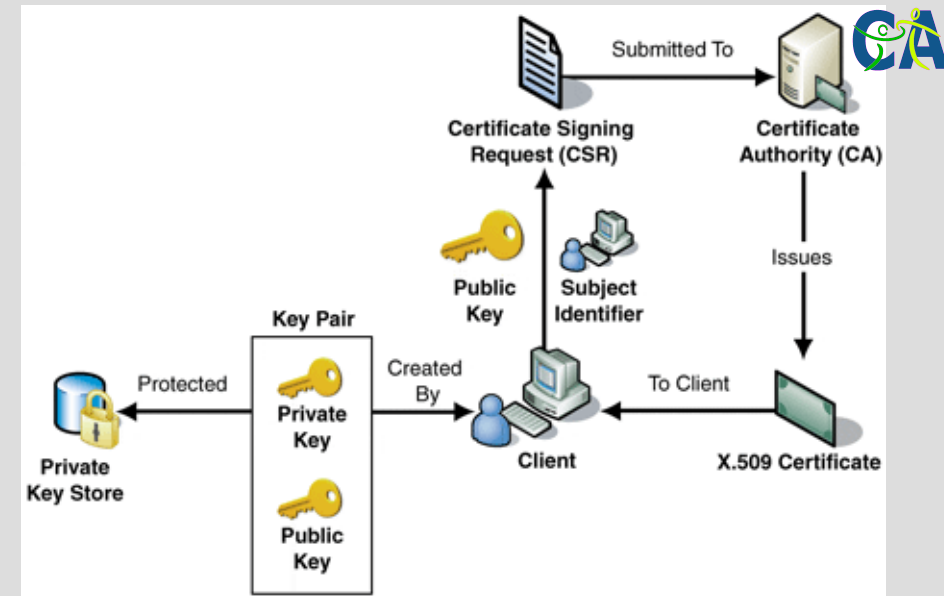
# how do “signatures” work



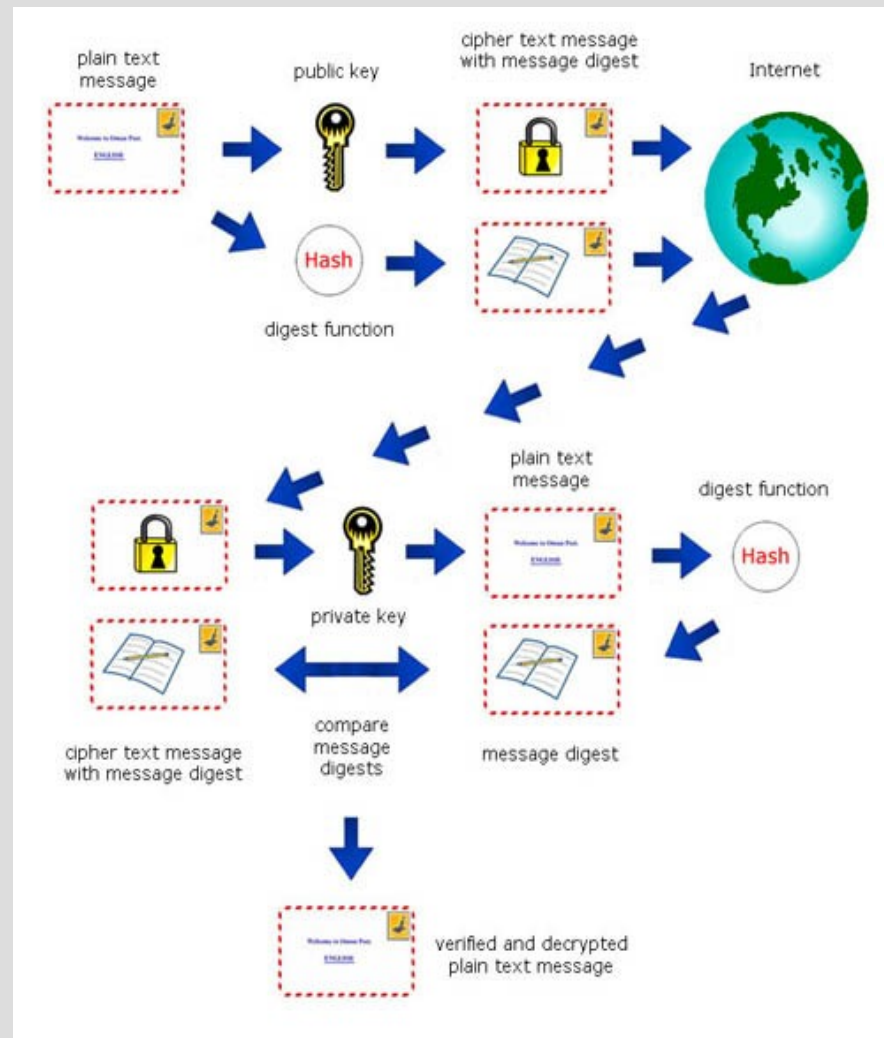
## Certificate Authority signature

- create private key and 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!



# 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 present.
- 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 present.

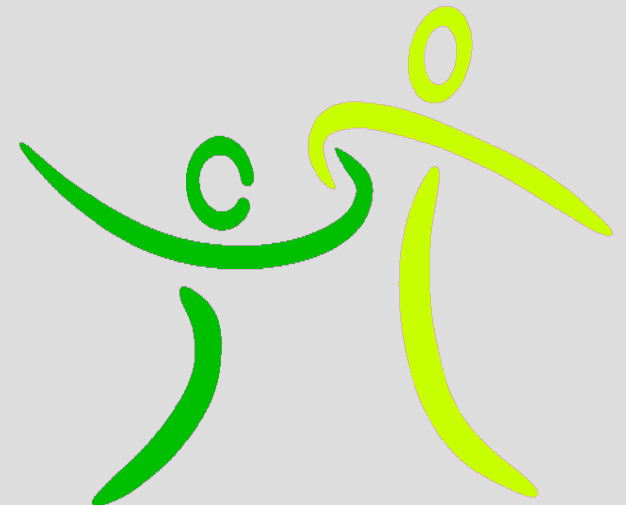
A "Certificate Viewer" window is also open, showing details for the certificate "Philipp Gühring". It displays the following information:

General	
<b>Could not verify this certificate because it has expired.</b>	
<b>Issued To</b>	
Common Name (CN)	
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	02:FF:AF
<b>Issued By</b>	
Common Name (CN)	CA Cert Signing Authority
Organization (O)	Root CA
Organizational Unit (OU)	http://www.cacert.org
<b>Validity</b>	
Issued On	12/12/2006
Expires On	12/12/2007
<b>Fingerprints</b>	
SHA1 Fingerprint	70:1A:93:6F:CA: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

the CAcert CA?

certificates free for everyone

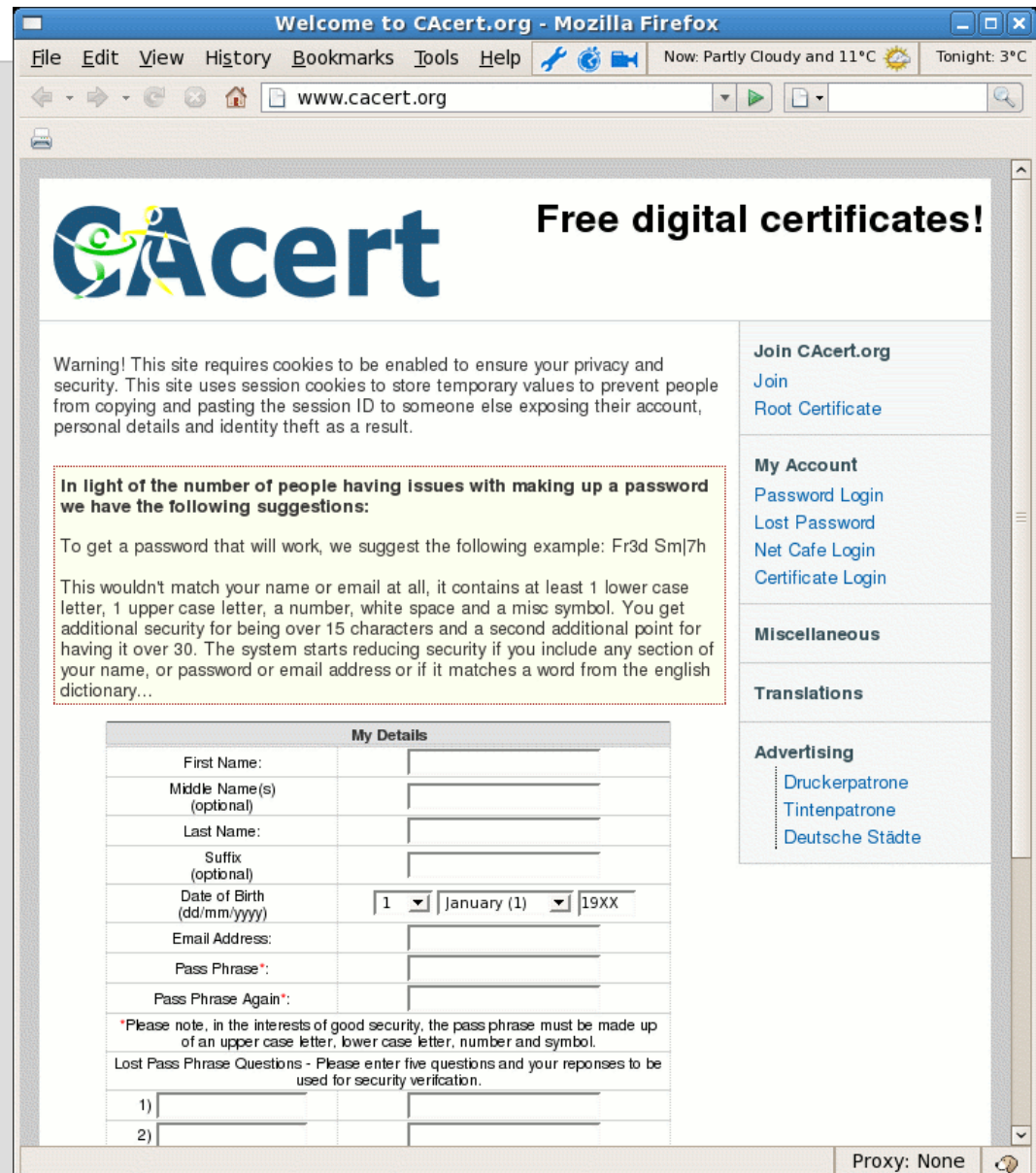
- join CAcert Community
  - agree with privacy rules
  - agree with CAcert Community Agreement
  - get CAcert account: join via <http://www.cacert.org>



# HowTo join Community

register

- 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.

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

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

**Miscellaneous**

**Translations**

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

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

Proxy: None



## Get 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



CAcert Inc. - P.O. Box 4107 - Denistone East NSW 2112 - Australia - <http://www.CAcert.org>

CAcert's Root Certificate fingerprints:

A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B and 135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33

To the Assurer: The CAcert Assurance Programme (CAP) aims to verify the identities of Internet users through face-to-face witnessing of government issued identity documents. The Applicant asks you to verify to CAcert.org that you have met them and verified their identity against one or more original, trusted, government photo identity documents.

If you have ANY doubts or concerns about the Applicant's identity, DO NOT COMPLETE OR SIGN this form.

For more information about the CAcert Assurance Programme, please visit: <http://www.CAcert.org> As the assurer, you are required to keep the signed document on file for 7 years. Should CAcert Inc. have any concerns about a meeting taking place, CAcert Inc. can request proof, in the form of this signed document, to ensure the process is being followed correctly. After 7 years if you wish to dispose of this form it's preferred that you shred and burn it. You do not need to retain copies of ID at all. It's encouraged that you tear the top of this form off and give it to the person you are assuring as a reminder to sign up, and as a side benefit the tear off section also contains a method of offline verification of our fingerprints.

# CAP form

## complete CAP with

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

### Applicant's Statement

Full Names:

Date of Birth: (YYYY-MM-DD)

Email Address:

I hereby confirm that the information stated above is both true and correct, and request the CAcert Assurer (identified below) to witness my identity in the CAcert Assurance Programme.

Applicant's signature:

Date (YYYY-MM-DD): 20\_\_-\_\_-\_\_

### CAcert Assurer

Assurer's Name:

Assurer's signature:

Date (YYYY-MM-DD): 20\_\_-\_\_-\_\_

<input type="checkbox"/> Passport	Photo ID	<input type="checkbox"/> Drivers Licence	Photo ID
<input type="checkbox"/> Identification Card	Photo ID	<input type="checkbox"/> _____	Photo ID

Location of Face-to-face Meeting: \_\_\_\_\_

Points Allocated: \_\_\_\_\_ Notes:

## CAcert Organisation Assurance

- the organisation entity is in control:
  - domain server certificates
  - Email certificates for individuals within the organisation
- Organisation needs to have:
  - CAcert Assured administrator > 100 WoT 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



### CAcert Organisation Assurance Programme COAP

CAcert is an international organisation. The English language is chosen to be the formal language. For your convenience a translation to Dutch is provided here in *italic*. The translation is to be considered a help only. English remains the ruling language.

*CAcert is een internationale organisatie. Engels is de gevoerde taal binnen de organisatie. Als hulp is hier een vertaling in het Nederlands bijgevoegd (cursief). De vertaling dient als hulp. De Engelse tekst is bindend.*

#### Applicant (Aanvrager)

<b>Name of the Organisation</b> ( <u>Naam van de Organisatie</u> )	
<b>Contact email address</b> ( <u>Contact email adres</u> )	
<b>City (Vestigingsplaats)</b>	
<b>State (Provincie)</b>	
<b>Country (Land)</b>	
<b>email(s) of administrator accounts - must match a CAcert account (CAcert Account email adres(sen) van de systeem administrateur)</b>	
<b>Domain(s)</b> ( <u>domein-naam (-namen)</u> )	

As proof for the legality, identity and legality of signatures for the organisation the following official documents, either original or in certified copies and not older as 4 weeks, are attached to this form.

*De volgende bewijstukken voor de officiële naam van de Organisatie, haar rechtsform en de namen van de tekenbevoegden zijn de volgende originelen of gewaarmerkte copien niet ouder dan 4 weken, zijn bijgevoegd:*

--

## What does one get?

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

# 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

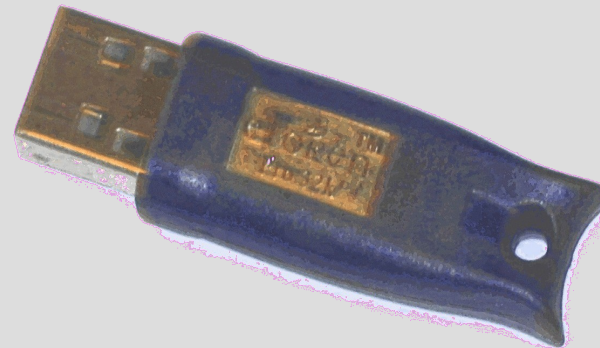
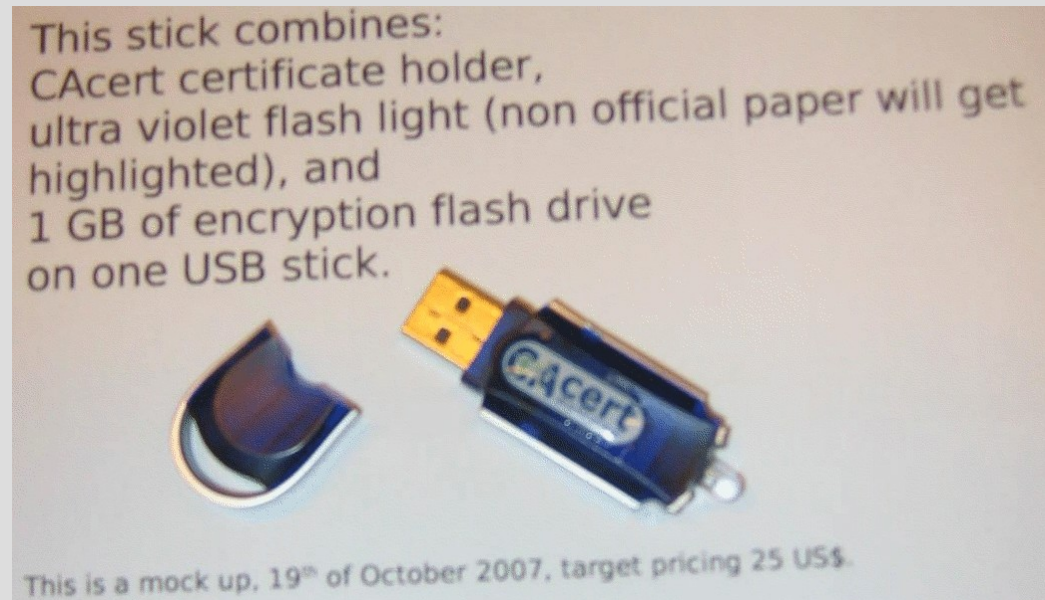
**Fingerprints**

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](#)

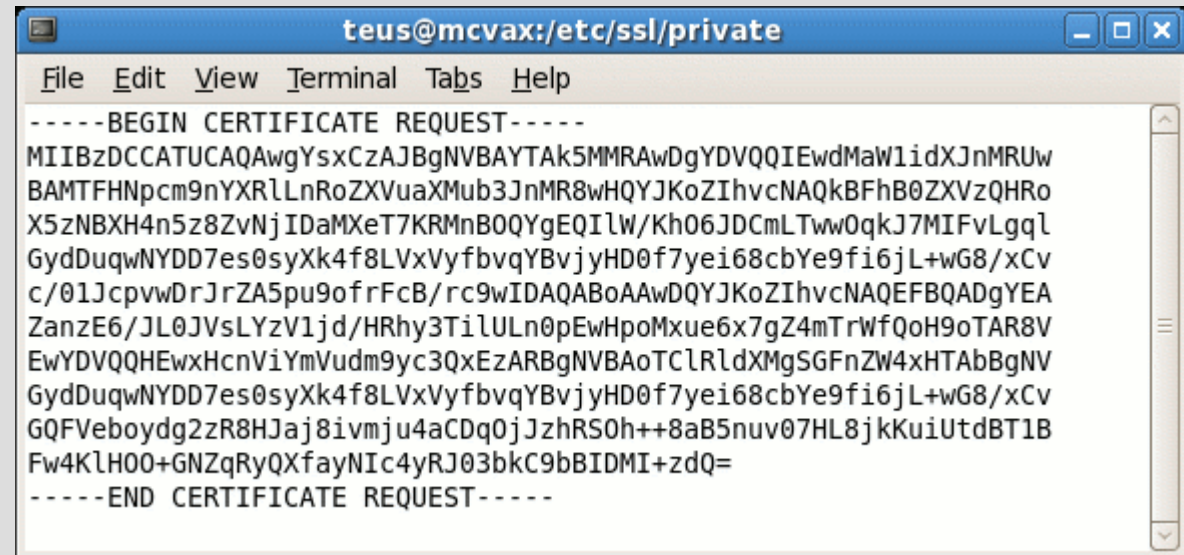
```

teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDcC8ybQIM22owYvH/Wg2iijJA6EhIevHZvnk8sfrgBLikDmivf
c8Q3r758SsRGKvnBYxjPyH1AIcQbTj4Tcm/GCTL8ACK5ofp6/gdhjnpRq2JZhwfM
AoGBAIfcR8ABoNsE0VK5CkFTh12TQwjaPajEed56grU90ipGimFvakap31NKsAG
g2bxdLWoCzH1hhNd...
w3kus/xfowJF...
AGg9i0ielNAj...
GyBjP3KSrLzvU...
w3kus/xfowJBAOKCWlqge/w0s6yX3CsaRcZPwPndN1/3LUttf8hiV9evufEbl5
1yDN059KwJvZ1XyyTaRdx0Y/9CbQsXwkNp4fD0KSTYZX60XyYrhBMYACVmgIwsVb
t9KyfSVtIkVMMIw0GPxAkEAmu1TWqSUvR8jHGtWcebqL8LnhYacKe0NFDA9K3d
FFYkKqcrsygujNujB/P3IE5eBwgEMwDhiwlv0WJ11C8vZA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEFTCCAf2gAwIBAgIDARRSMA0GCSqGSIb3DQEBBAUAMHkxEDA0BgNVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHA6Ly93d3cuY2FjZjZlLm9yZzEiMCAGAUExAMZ
Q0EgQ2VydCBTaWduaW50aGVhZGVzL2F5dC51dC51dC51dC51dC51dC51dC51dC51
MBcGA1UEAxQKi50aGVhZGVzL2F5dC51dC51dC51dC51dC51dC51dC51dC51dC51
gYkCgYEA3AvMm0CDNtc...
fErERir5wWMYz8h9QCh...
8sn4KG7UmgLkg0FAdJ...
hdAMBgNVHRMBAf8EAj...
YIZIAYb4QgQBgorBg...
JKAihiBodHRwOi8vd3...
fgTfs1wJqAPIavUzAk...
kyyk1XgBbQQ6Mm7ppq...
NqcXz/f9hmqhGiULeA...
AQQFAA0CAgEAejvbfX...
6vG0e2Ucnd2dsHRLmT...
X/thAu70Fa+0UGmmK3r...
XqJx504AFQMKrpd4xb...
+UFxKrF2e1nBGZF1Ffd/VFT+XamBmicAZAk/c07ghQucJJkRiDyt0c4f0pBMohCA
nZjFR/FxcMwtcjwf9NGmtV0LrL+7zz/suL4Quz0qFN0Q0Pv64u0mpeIDDYCKRlpC
41Kew0vtGLBpvFd4rP00fHrLEoLn09FX9ISQKrwW5+7hn3Q8phT9ik8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwYsxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdMaWlidXJnMRUw
BAMTFHnNpcm9nYXRLLnR0ZXVuaXMuMub3JnMR8wHQYJKoZIhvcNAQkBFhB0ZXVzQHRo
X5zNBXh4n5z8ZvNjIdaMxeT7KRmNB0QYgeQILw/Kh06JDCmLTww0qkJ7MIFvLgql
GydDuqwNYDD7es0syXk4f8LVxVybqvYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
c/01JcpvwDrJrZA5pu9ofrFcB/rc9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
ZanzE6/JL0JVSLyZV1jd/HRhy3TilULn0pEwHpoMxue6x7gZ4mTrWfQoH9oTAR8V
EwYDVQQHEWxHcnViYmVudm9yY3QxEzARBGNVBAoTCLRldXMgSGFnZW4xHTAbBgNV
GydDuqwNYDD7es0syXk4f8LVxVybqvYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
GQFVeboydg2zR8HJaj8ivmju4aCDq0jJzhRS0h++8aB5nuv07HL8jKkuiUtdBT1B
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 command. The output is a PEM-formatted certificate request, starting with '-----BEGIN CERTIFICATE REQUEST-----' and ending with '-----END CERTIFICATE REQUEST-----'. The request contains a base64-encoded string representing the certificate 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

The screenshot shows the Mozilla Firefox Add-ons page for the 'Key Manager' extension. The page title is 'Key Manager (v 0.1.0.20071203)'. The description reads: 'KeyManager Tool: Firefox Extension for Key Generation, Certificate Enrollment, and Identity and Authority Delegation'. It states that KeyManager is a client-side PKI tool for key generation, certificate enrollment, and identity and authority delegation, packaged as a 'chrome'-based Firefox extension. It mentions that currently, it does not provide a GUI for local key generation, but it has added the capability for SCEP-based certificate enrollment. The extension also supports signing of proxy certificates and provides an XUL-based GUI for signing of XPI files. A list of features is provided: generation of keys and X.509 based self-signed certificates; generation of PKCS#10 based Certificate Signing Requests (CSRs); SCEP-based Certificate enrollment; ability to act as a SCEP client 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); and exporting of private keys in PKCS#8 and PKCS#12 formats for use with public key certificates and generation of configuration files for applications like cURL, Globus toolkit, etc. The page also includes a 'Find Similar Add-Ons' section with 'Privacy & Security' as a recommendation.

The screenshot shows two overlapping windows from the Key Manager application. The background window is the 'Certificate Signing Request Form', which has two tabs: 'Default Certificate Profile' and 'Advanced'. The 'Default Certificate Profile' tab is active, showing a dropdown menu set to 'Digital Signature and Data Encipherment' and a 'Show Profile Data' button. Below this, there are input fields for personal and organizational information: First Name (fn) 'Teus', Last Name (sn) 'Hagen', Organizational Unit (ou), Organization (o), Locality (l), State (st), Country (c) 'NL', and Alias 'teus'. The 'Subject Public Key Info' section shows 'Key Type' set to 'RSA' and 'Key Size' set to '2048'. The 'Subject Alternative Name' section has an 'E-mail' field containing 'teus@theunis.org'. At the bottom of this window are buttons for 'Generate PKCS#10', 'Generate CRMF', 'Help', and 'Cancel'. The foreground window is the 'PKCS#10 CSR Detail' window, which displays the 'CSR Data for teus' as a long block of Base64-encoded text. To the right of this text is a 'CA Server Response' area. Below the CSR data, there is a 'Cert Issuer Info' section with radio buttons for 'CA Server Type' (PKCS10 CA is selected), 'MS Cert Service', 'SCEP Server', 'Open CA', and 'EJB CA'. The 'CA Server URL' is 'http://gemstar.usae.avaya.com:18080/prodsignedcertdemo/jp', with 'Login' and 'Download CA Certs' buttons. The 'Issuer Subject DN' and 'Issuer Alias' fields are empty. At the bottom of this window are buttons for 'Save', 'Send PKCS#10 CSR to CA', 'Cancel', and 'Help'.

## 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-----
MIICijCCAIXICAQAwRTELMAkGA1UEBhMCTkwxITAfBgkqhkiG9w0BCQEWEnRldXNA
bXlfZG9tYWluLm9yZzZETMBEGA1UEAxMKVG91cyBIYWdlbjCCASIwDQYJKoZIhvcN
...
aslwP+uZP9MwdfSwOEL8ldi860FNGLA5Skr1wwewfjtdPXRugYTXVzCn4pzy/Fz
GS/2xpYuwaQDrz57L+YE4zakeoIuctZW9fWZZ0j9
-----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
Q0EgQ2VydCBTaWduaW5nIEF1dGhvcml0eTEhGSIb3DQEJARYSc3VwcG9y
.....
K1aTaRN4xKjs098Z9r0qrIoKULkkjZYIbV61P6dyHnE7oVxKpQs+wda0zp
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
```

## CAcert assurance

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



## 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 is community work

- >10.000 assurers
- translations into 30 languages
- > 100.000 certs in use
- >100 on the help desk:
  - 7 days \* 24 hours email support
- World Wide
- and **CAcert** certificates are **free!**
- at no charge



## CAcert is currently

- being audited, to get into
  - get in software distributions and browser: mozilla, ...
- committed agreements
  - for end user and for usage (license)
- 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



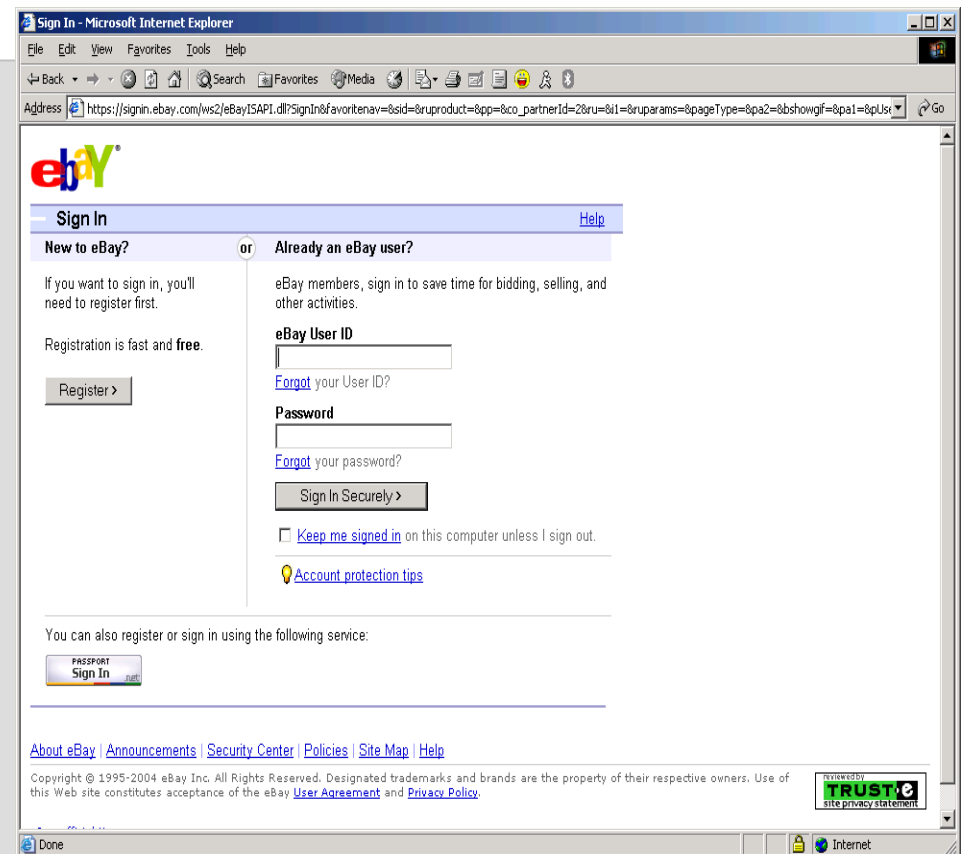
## CAcert is supported

- CAcert services run on Oophaga Foundation highly secured servers in Holland
- sponsored by
  - HCC, NLUUG, NLnet
  - SUN/AMD, Tunix, Cisco, Net Apps
  - and hopefully by you too!

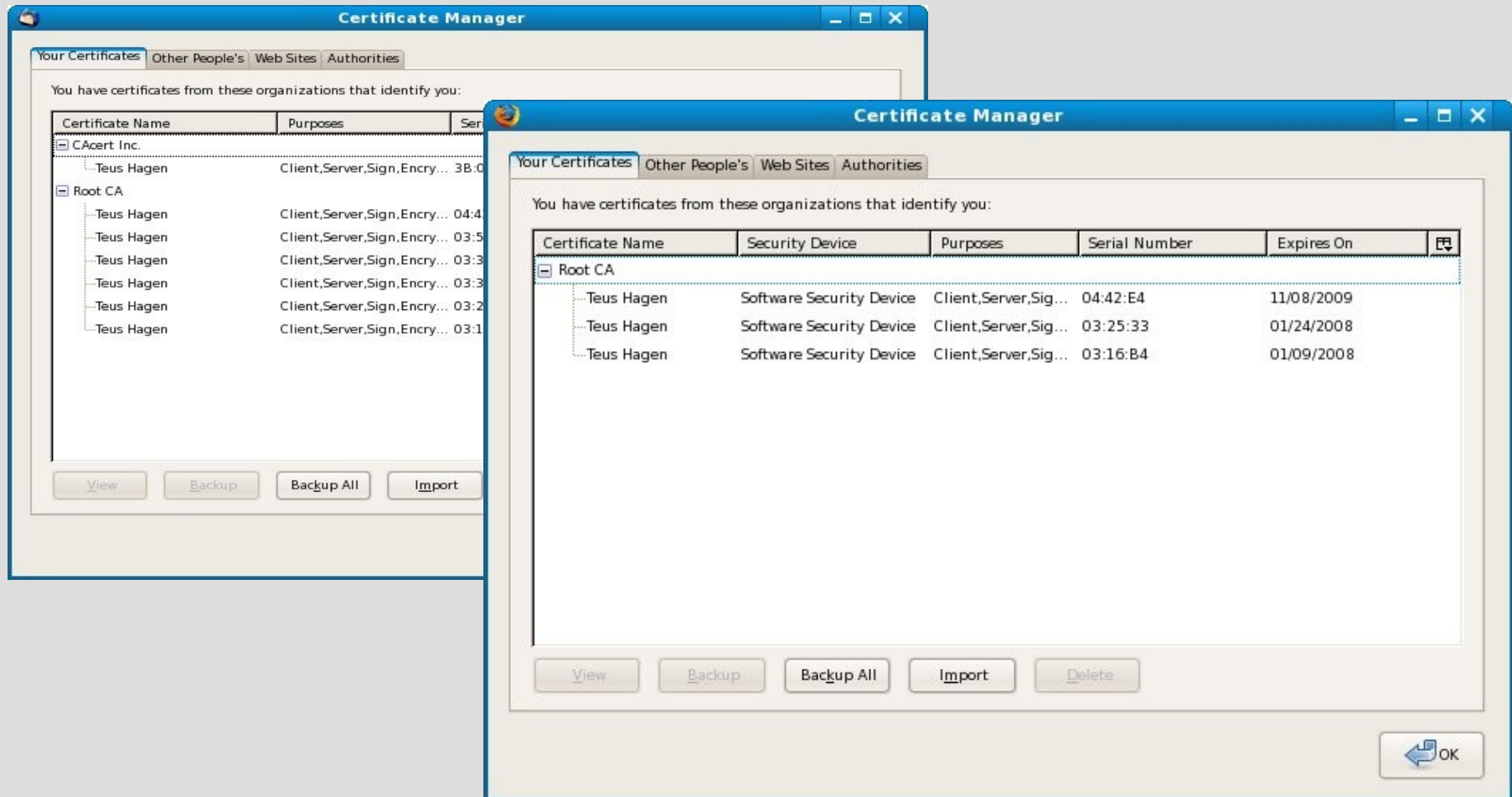


## Use it for:

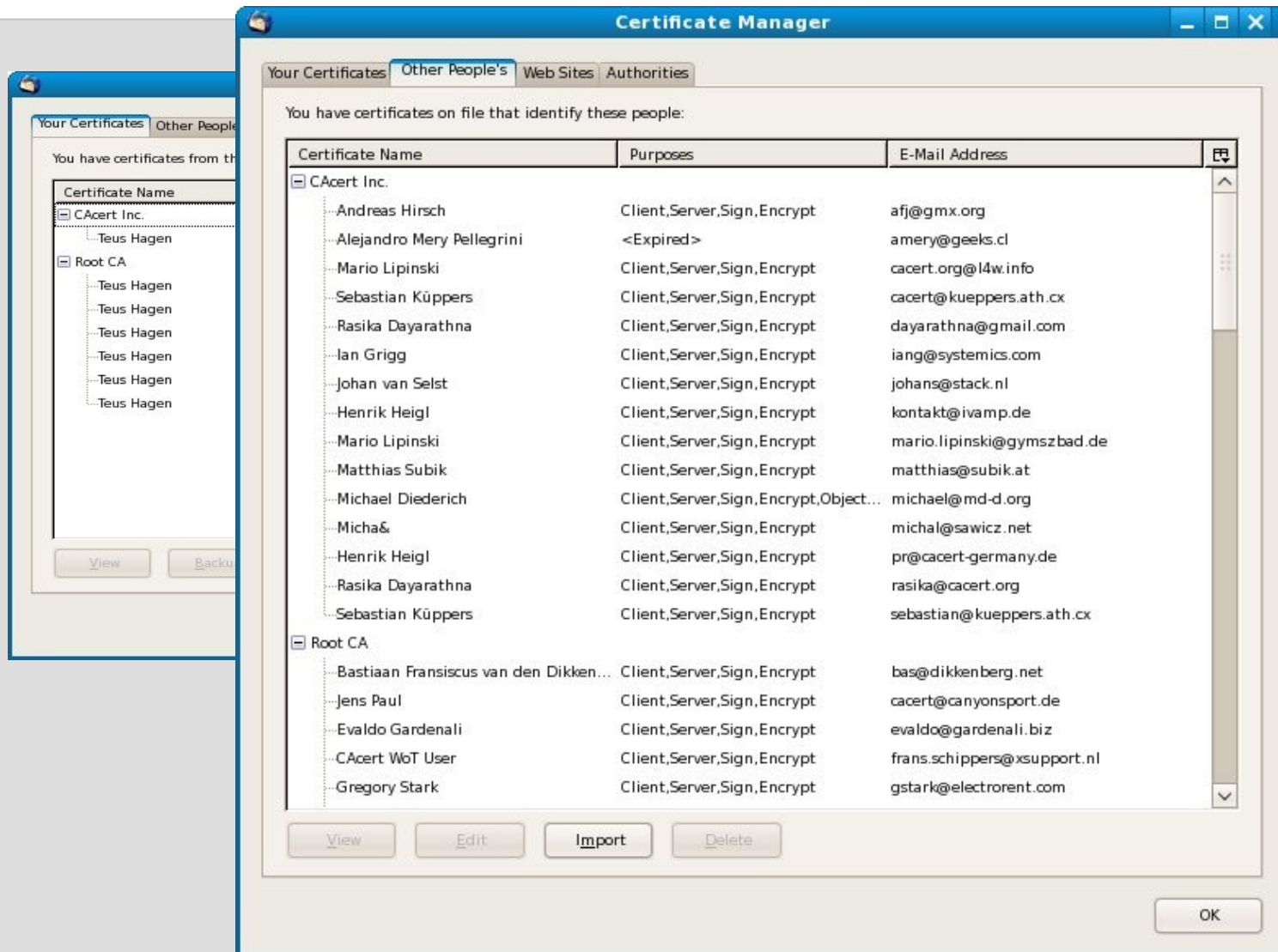
- to login
  - how broken is email address/password pair?
  - Better (single sign on) use CACert cert login!
- to sign documents, really?
- to identify yourself?
- to secure data transports



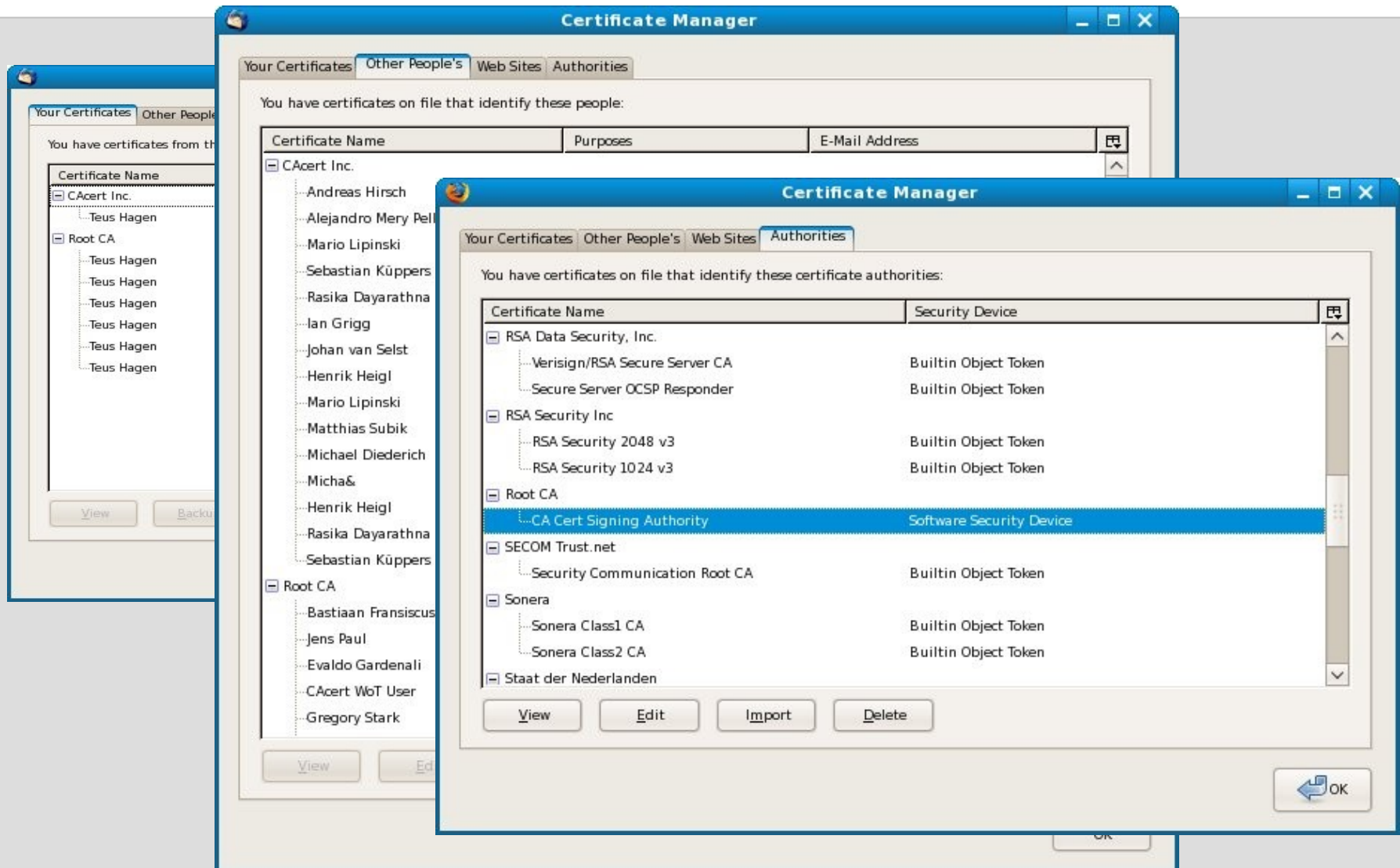
# Thunderbird certificate usage



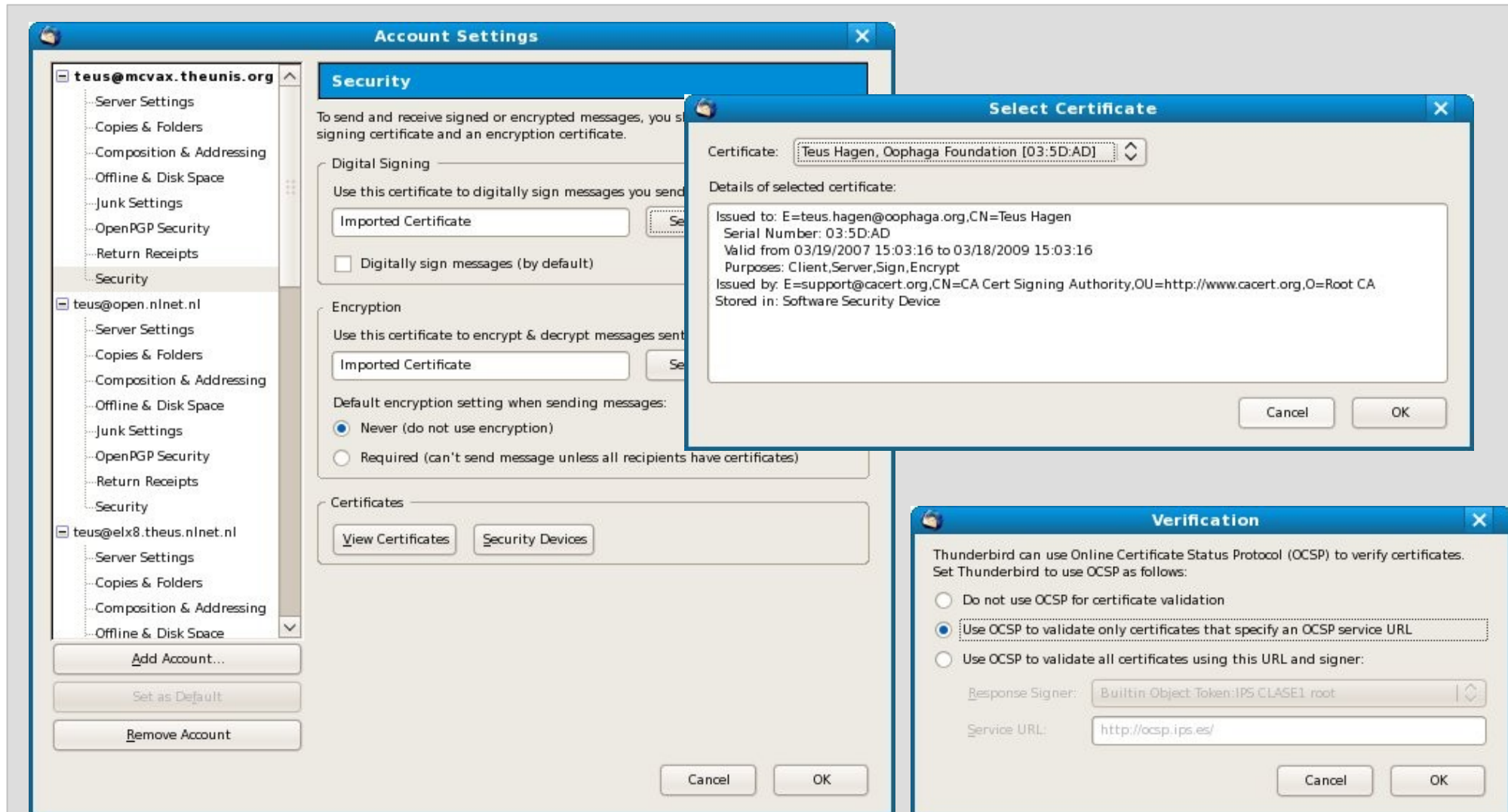
# Thunderbird certificate usage



# 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. Three dialog boxes are overlaid on the settings:

- Select Certificate:** Shows a dropdown menu with 'Teus Hagen, Oophaga Foundation [03:5D:AD]'. The details of the selected certificate are:
  - 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 the Online Certificate Status Protocol (OCSP) and provides three options for validation:
  - 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' is set to 'Builtin Object Token:IPS.CLASE1.root' and the 'Service URL' is 'http://ocsp.ips.es/'.
- Security (partial):** Shows the 'Digital Signing' section with 'Use this certificate to digitally sign messages you send' checked and 'Imported Certificate' selected.

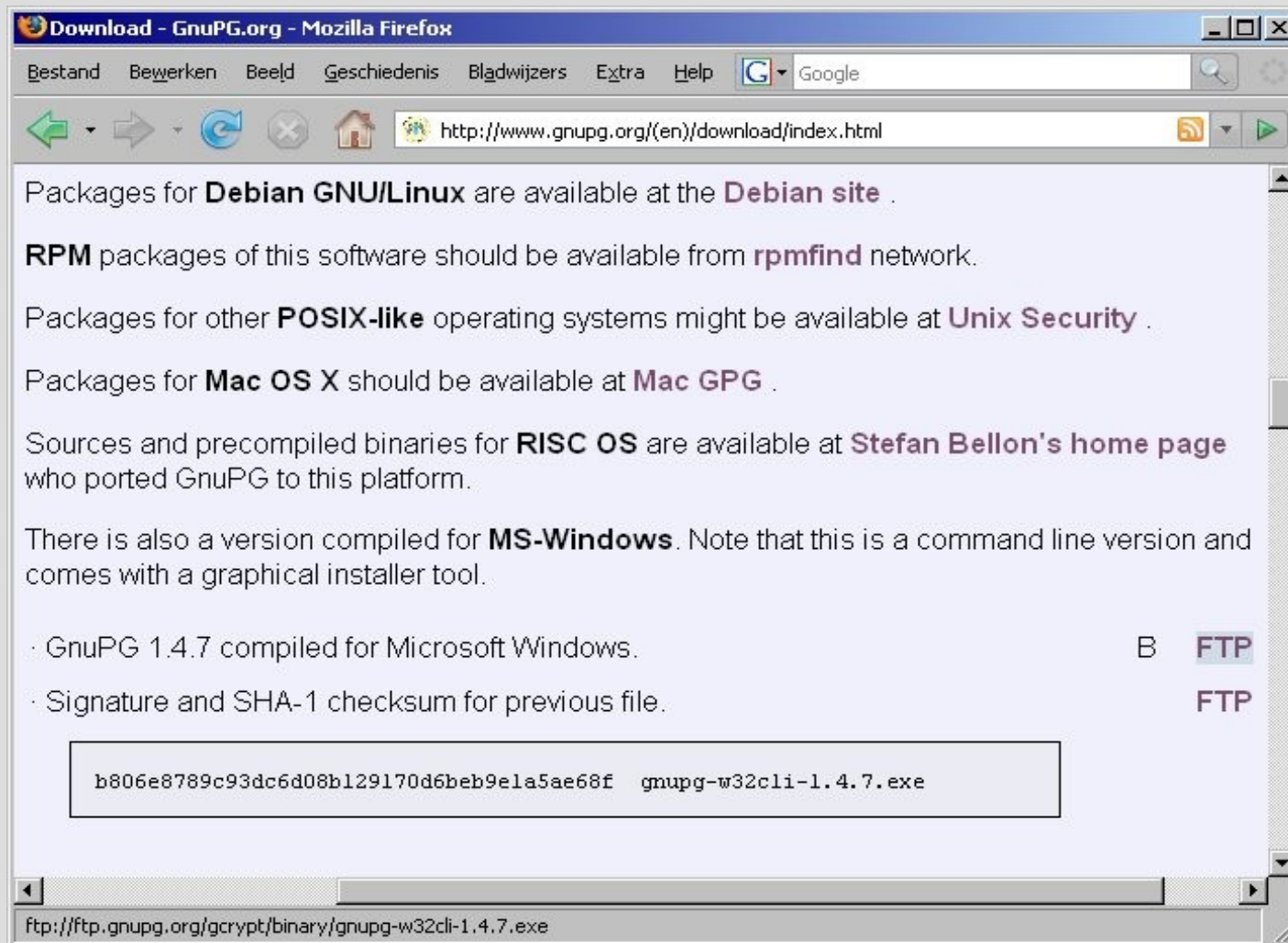


## PGP, GPG or GnuPG

- 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

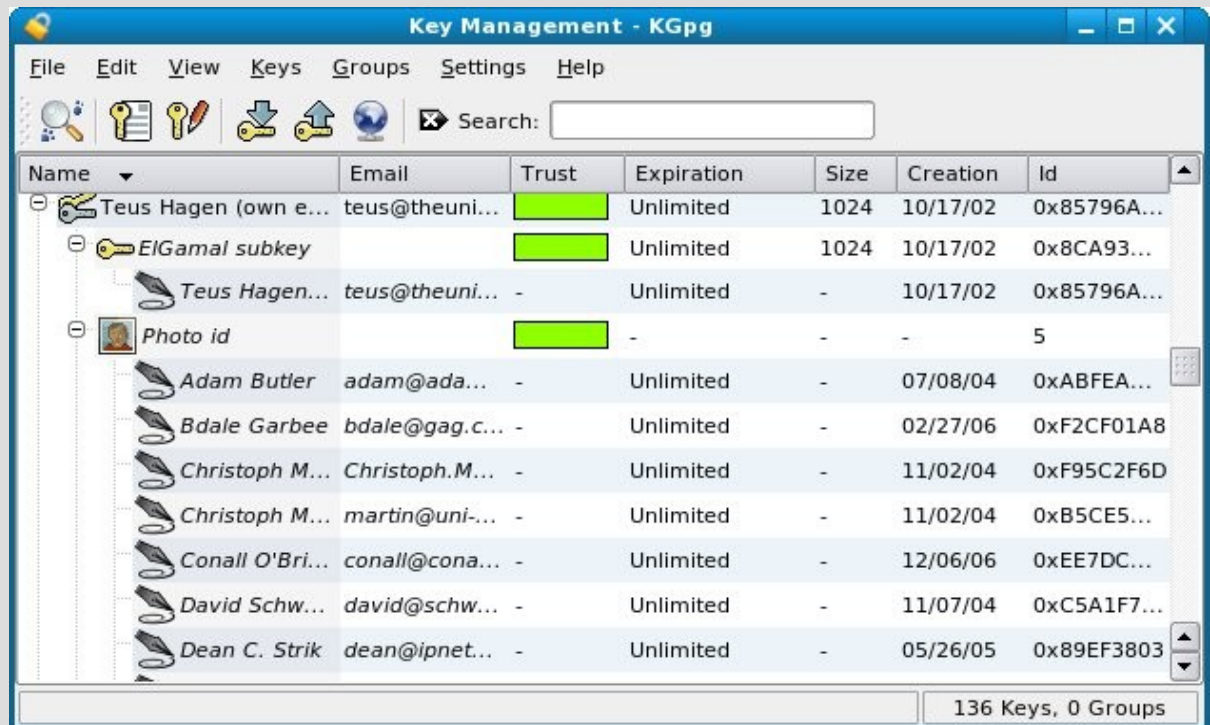


# PGP/GPG install



## GNUPG use

- Thunderbird plugin: OpenPGP/Enigmail
- KGPG



- Gnome Keyring Manager

# KGPG keyring manager



## PGP particularities

- PGP keyservers for public keys
  - [pgp.mit.edu](http://pgp.mit.edu)
  - [keyserver.ubuntu.com](http://keyserver.ubuntu.com)
  - [keys.pgpi.net](http://keys.pgpi.net)
- PGP statistics
  - [pgp.cs.uu.nl](http://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

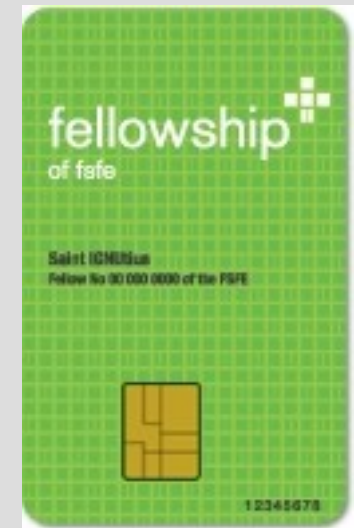
## PGP & X.509 Certificate comments

- 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 keyservers/statistics and spam?
- No X.509 certificate distribution infrastructure

## FSFE and GNUpg

Free Software Foundation Europe

- FSFE Fellowship crypto card





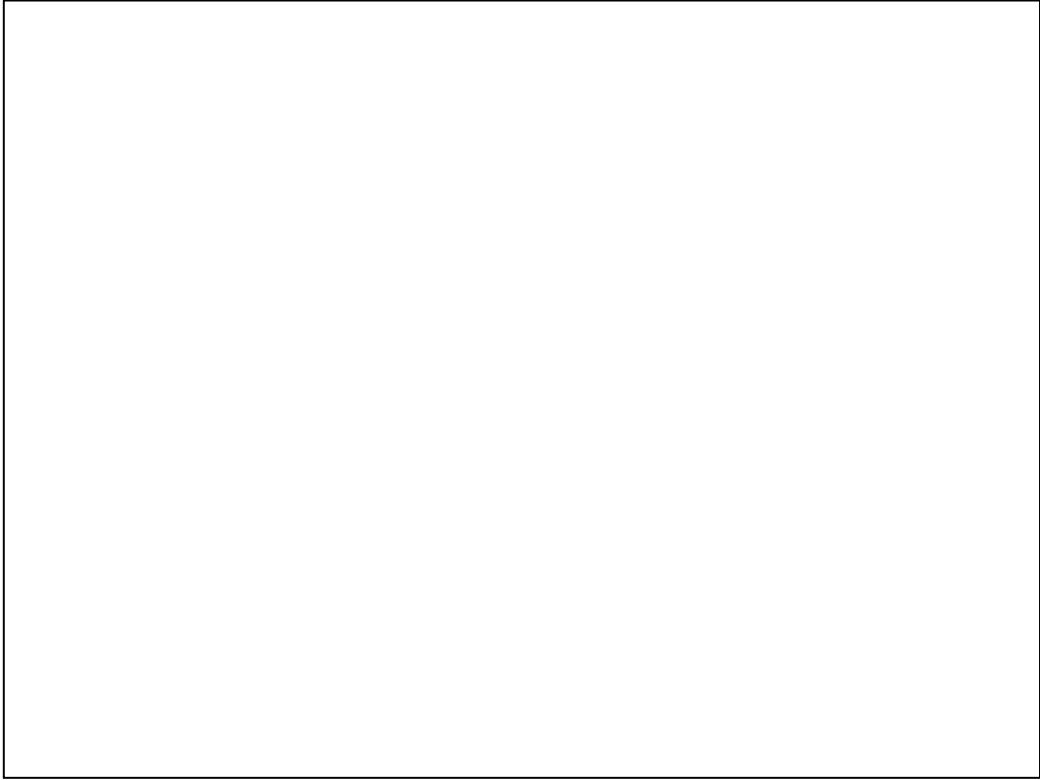
## some references and handy URL's

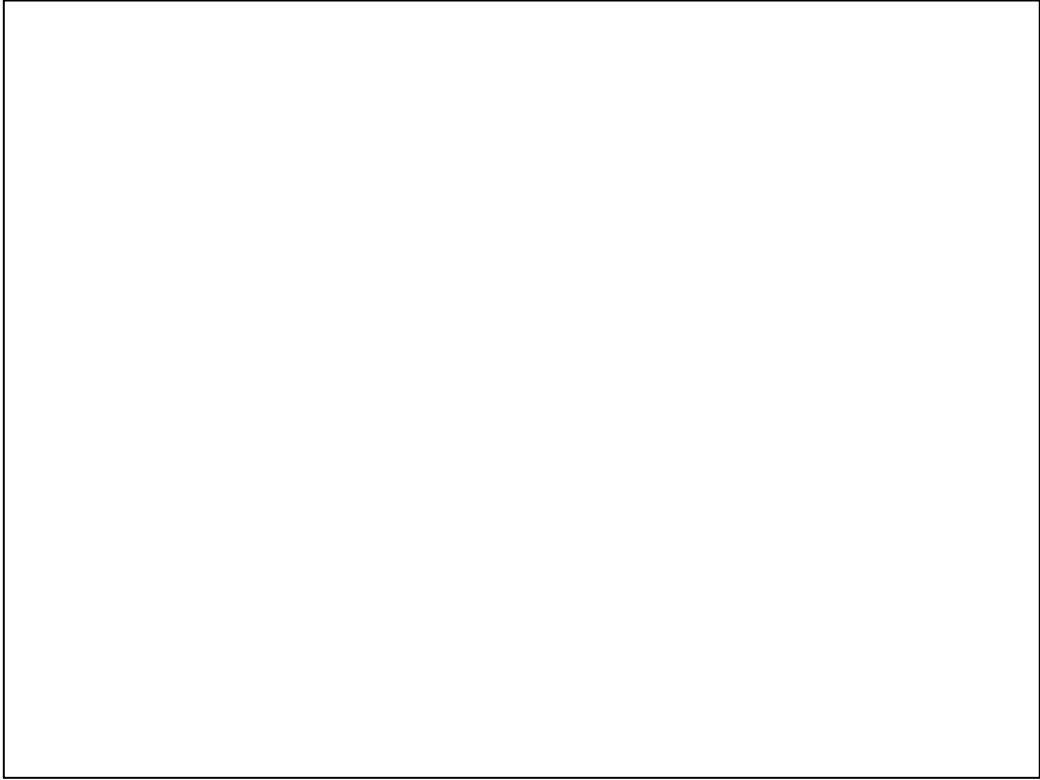
- <http://www.cacert.org>
- <http://wiki.cacert.org/wiki/>
- <http://svn.cacert.org/CACert/>
- <http://www.pgpi.org/doc/pgpintro/>
- <http://www.cacert.nl>
- Google search
- Applied Cryptography, Bruce Schneier, publ. John Wiley, 1996.
- Secrets and Lies: Digital Security in a Networked World, Bruce Scheier, publ. John Wiley, 2000.
- <http://schneier.com/blog> Hacking the new Boeing 787 Dreamliner airplane

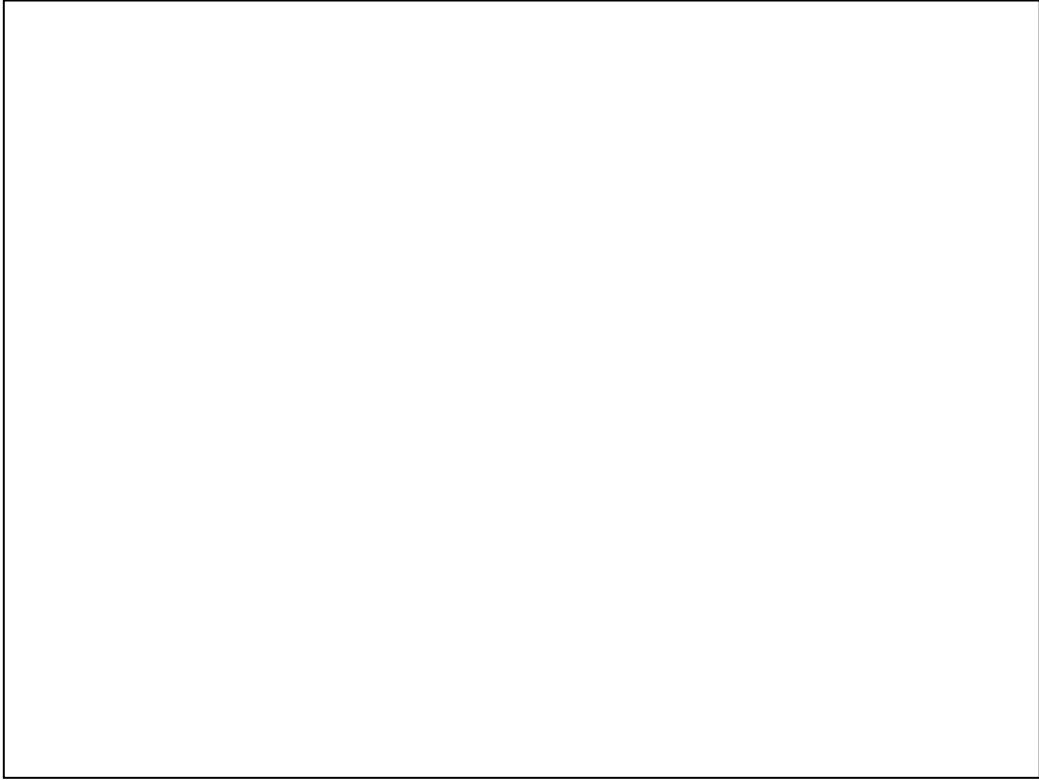
CAcert is for and by you!



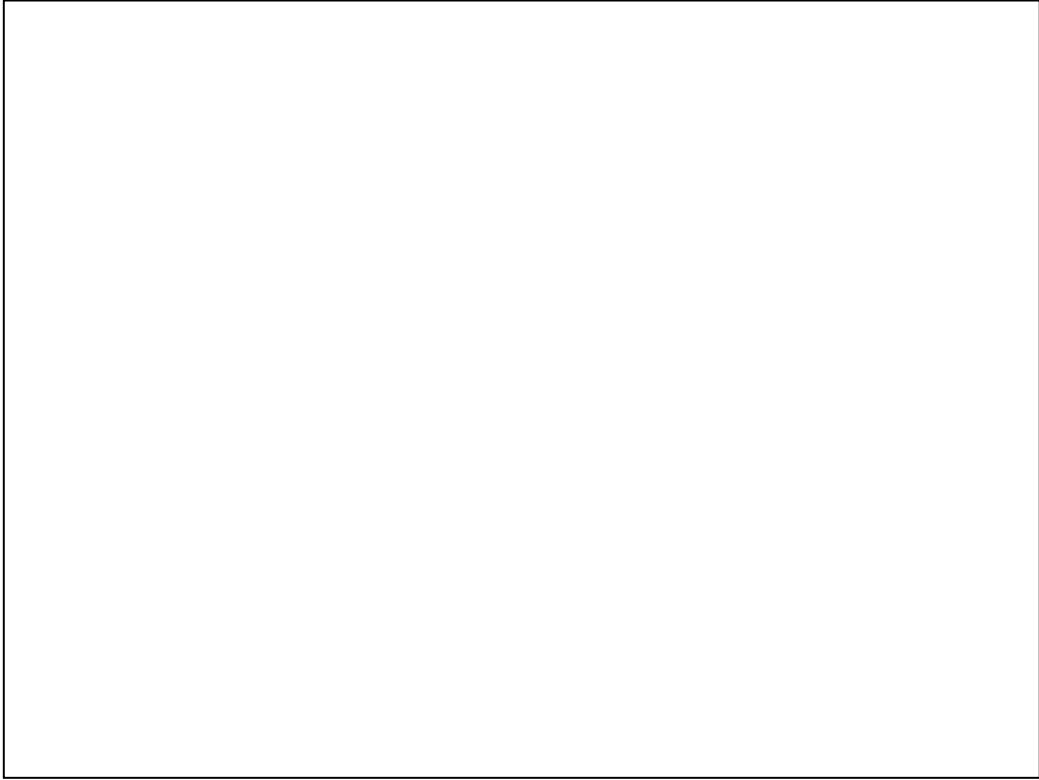
Thanks, some materials are used from: Wren Hunt, Ian Grigg and others



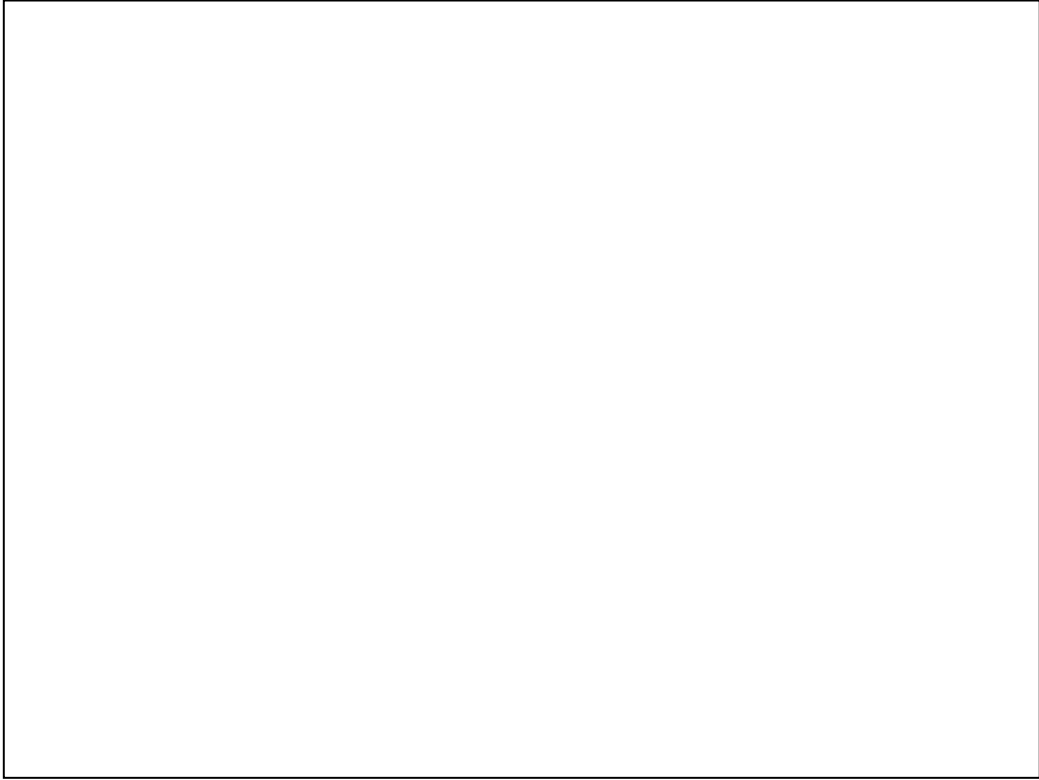




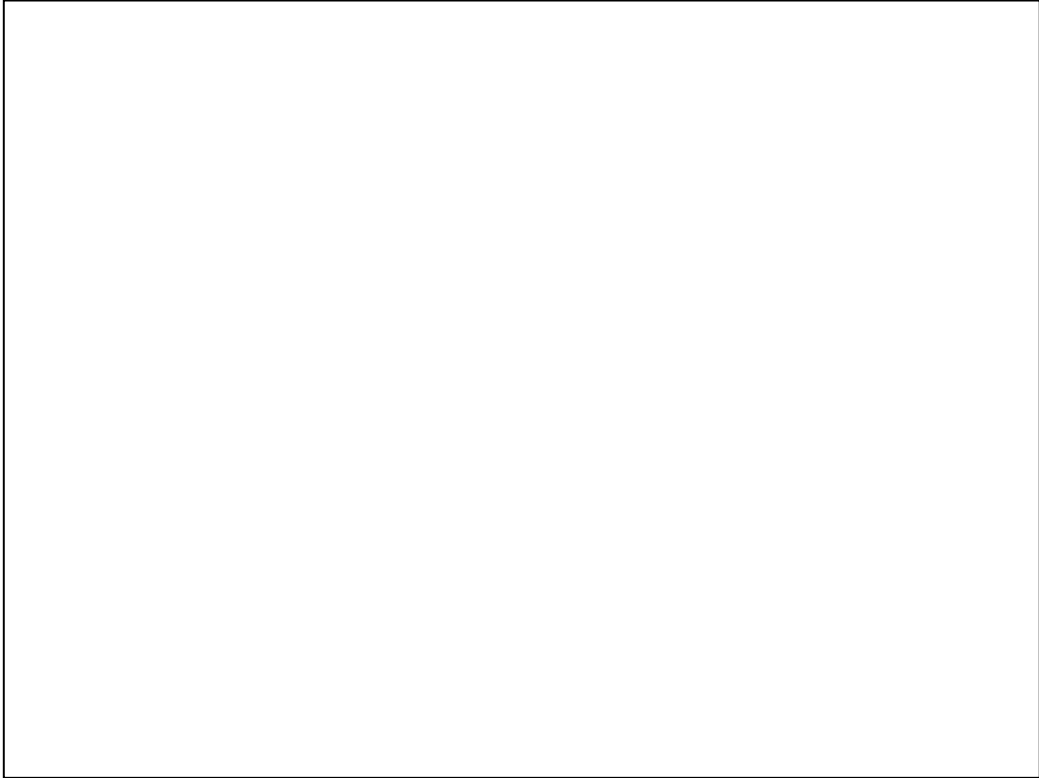
What can you do if you are not willing to be a dog



Trust is something else as you know who you are talking to  
Do you know who you are talking to? Trust in identity.



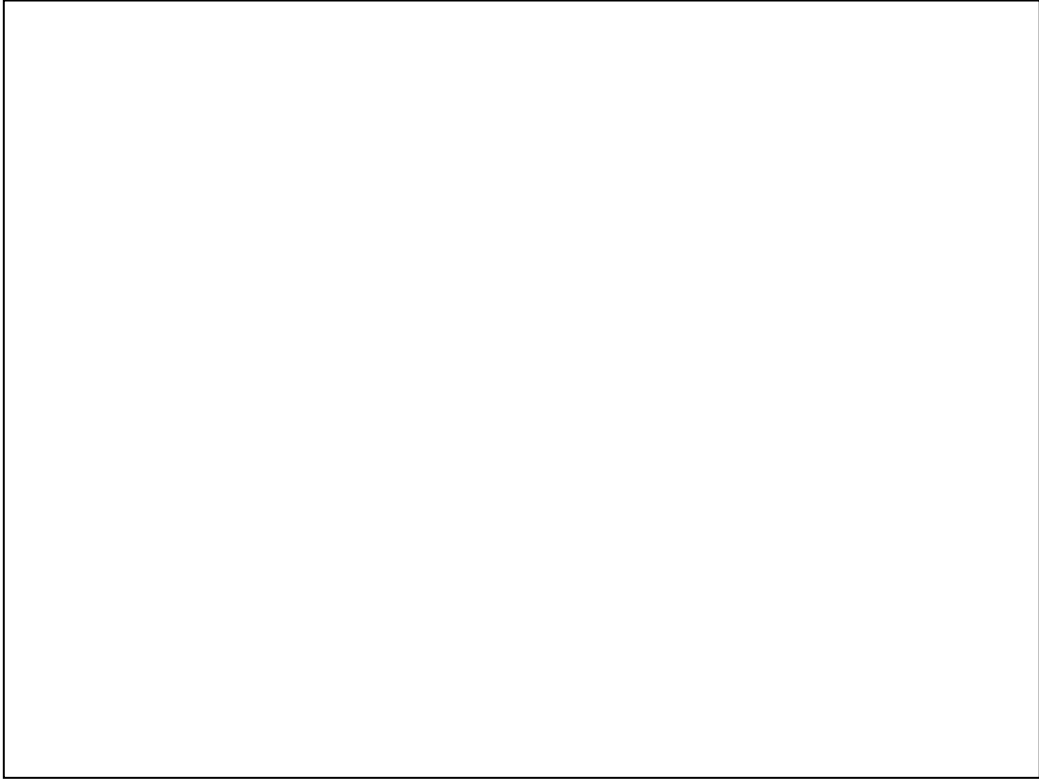
Trust in the email sender



Need a formal identity, well that seems to be easy

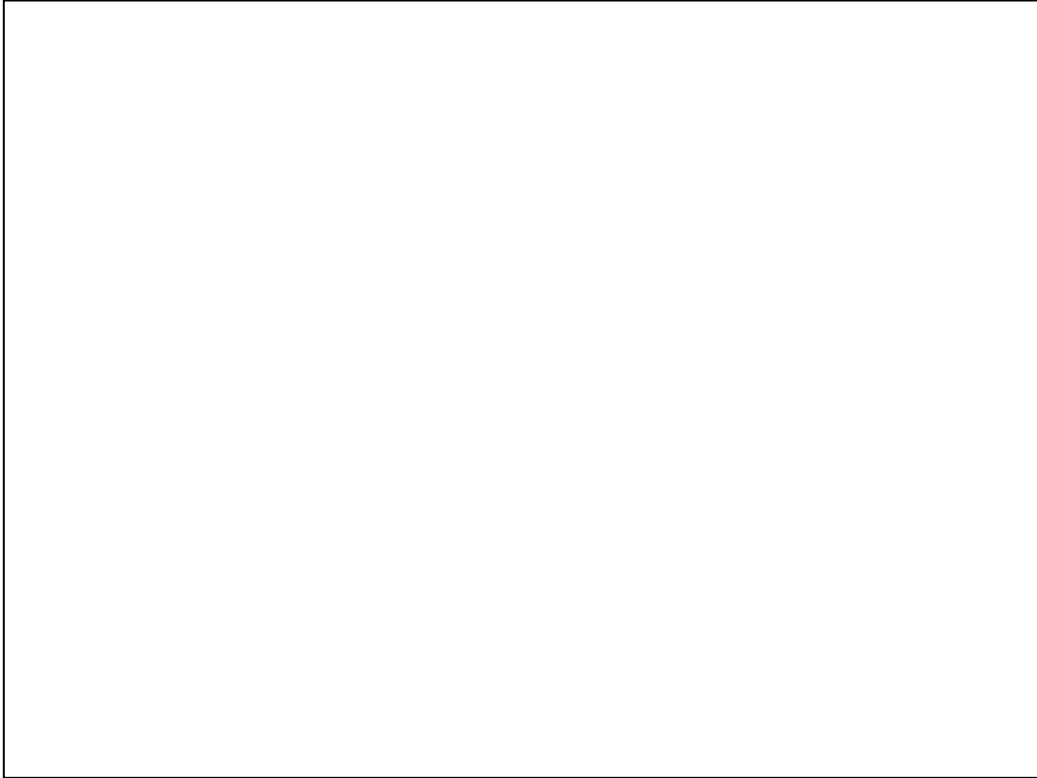
Identities are hard to check, so you need more people to check it: Web of Identity trust





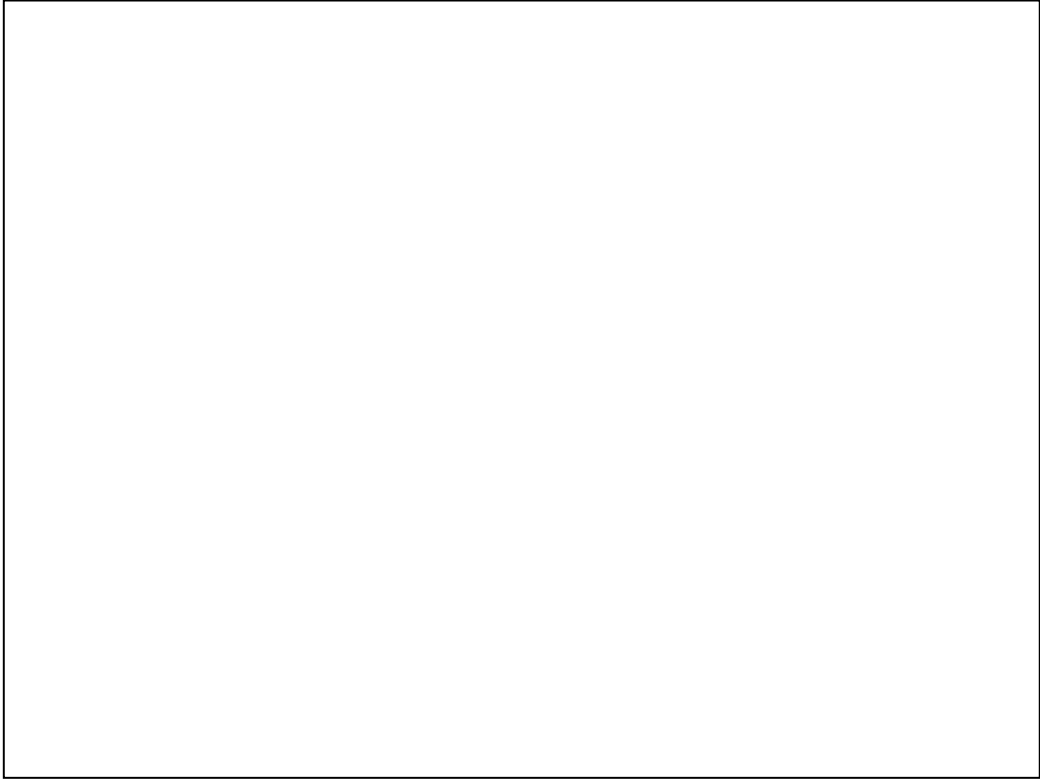
Where certificates are used for.

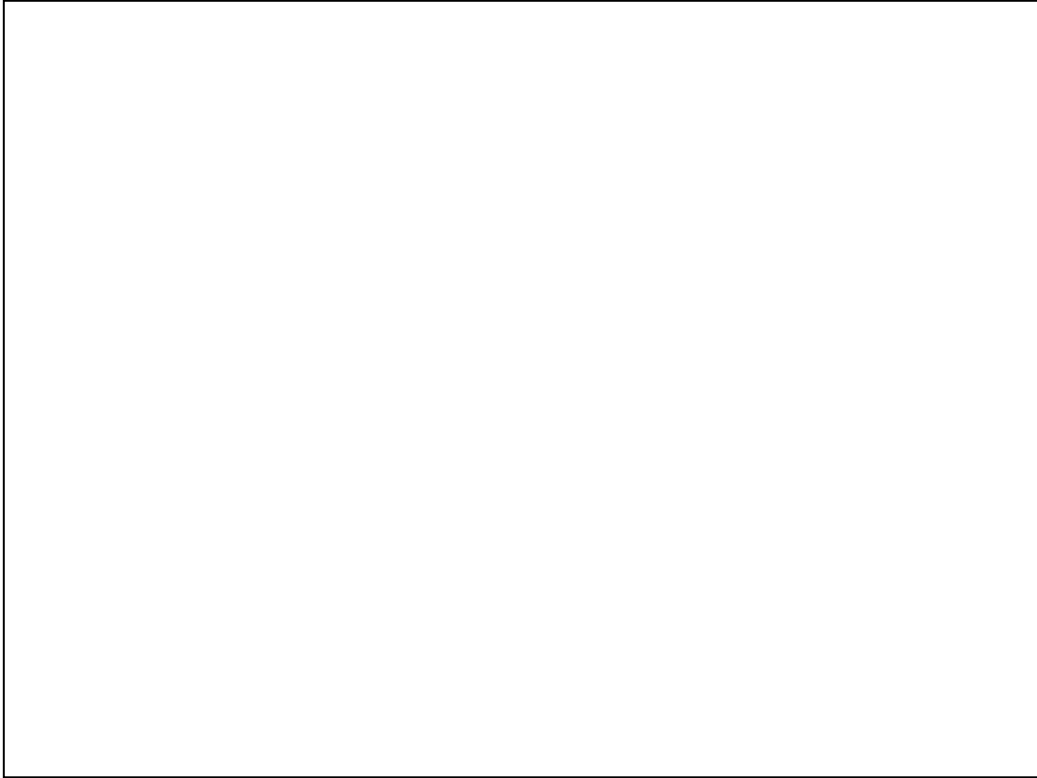
You learn easy to appreciate them. For sure after the accident.



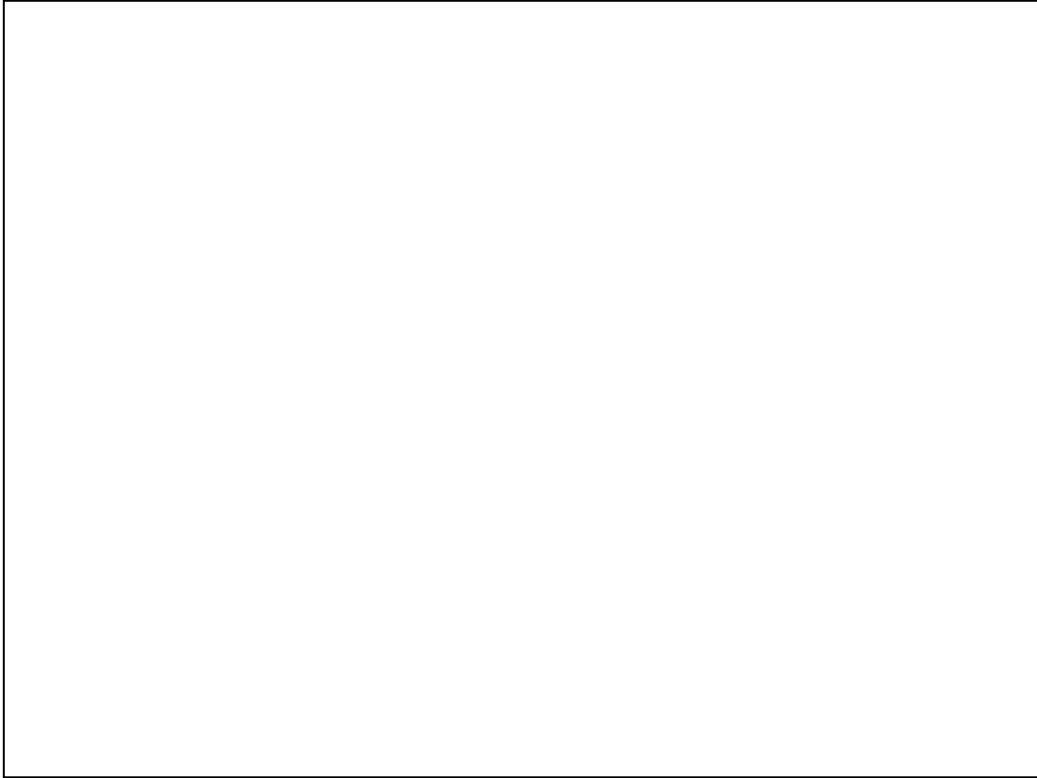
Ever clicked on the little lock?

View the certificate offered by the web server. Note that even banks forgot to renew the certificate. Still to meet a person who has not experienced that the bank web site offered an out of date certificate. We all have to learn.





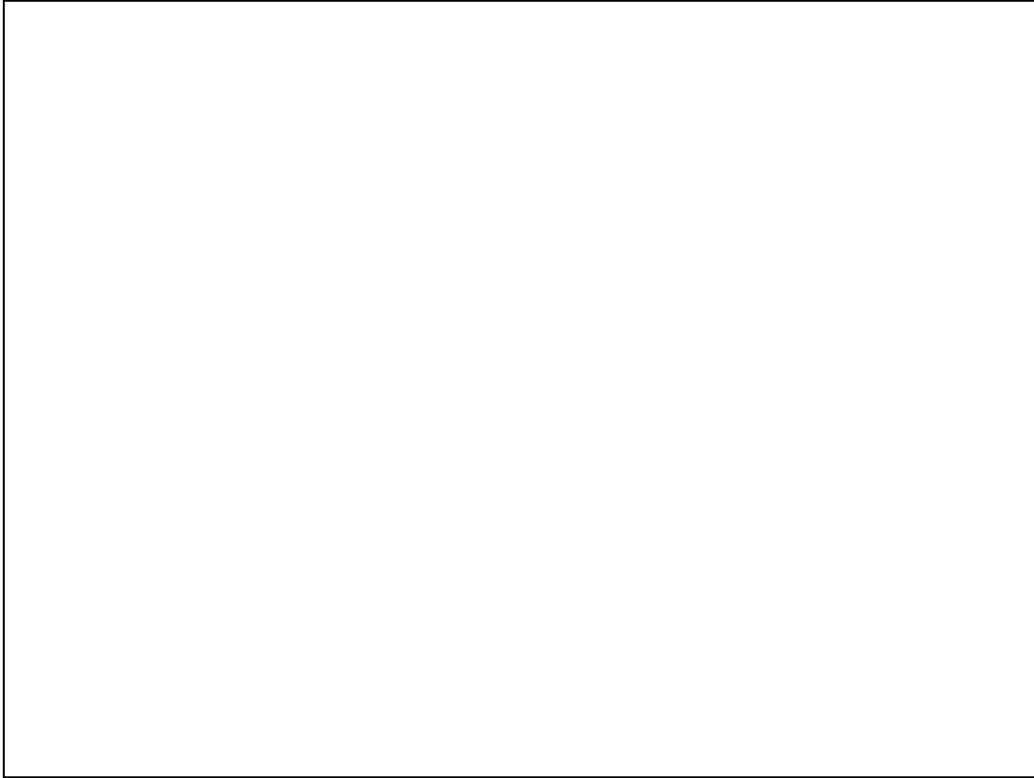
Two examples of encryption technology  
the latter we apply with certificates



Note this statement is proven ever and ever again right



The famous one from the second world war. Invented in Germany, used and trusted as THE coding system. However hacked by the Britain.



The secret shared key is the three offset of the wheels That is the seed of the coding.  
after every character one internal wheel is put one place to the right, and the other  
internal wheel to the left. So the ceasar encryption get less obvious.  
But frequency statistics help you to break this...



A late one, just today. 200 million (says NXP), publications say 2K million sold of this chip. 1K type single price 0.85 US\$, >100K 0.45 US\$. 4K des variant US\$ 2.50. Credit card size. Contactless 10cm. Antenna is biggest part, chip 1 mm\*\*2

Ultra light paper US\$ 0.50-0.16 512 eeprom on it.

Mainly applied in door entrance control, access control.

Karsten from Uni of Virginia sounds like the science man

Henryk sounds like the hacker

10K building blocks, only 70 different.

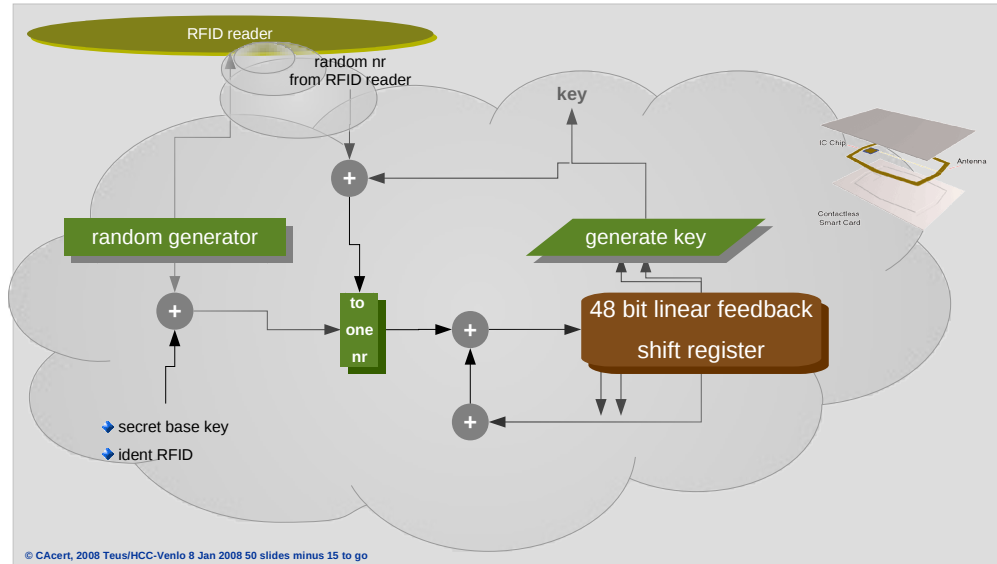
Secret key in chip not yet known. Just a matter of time and promise from two hackers.

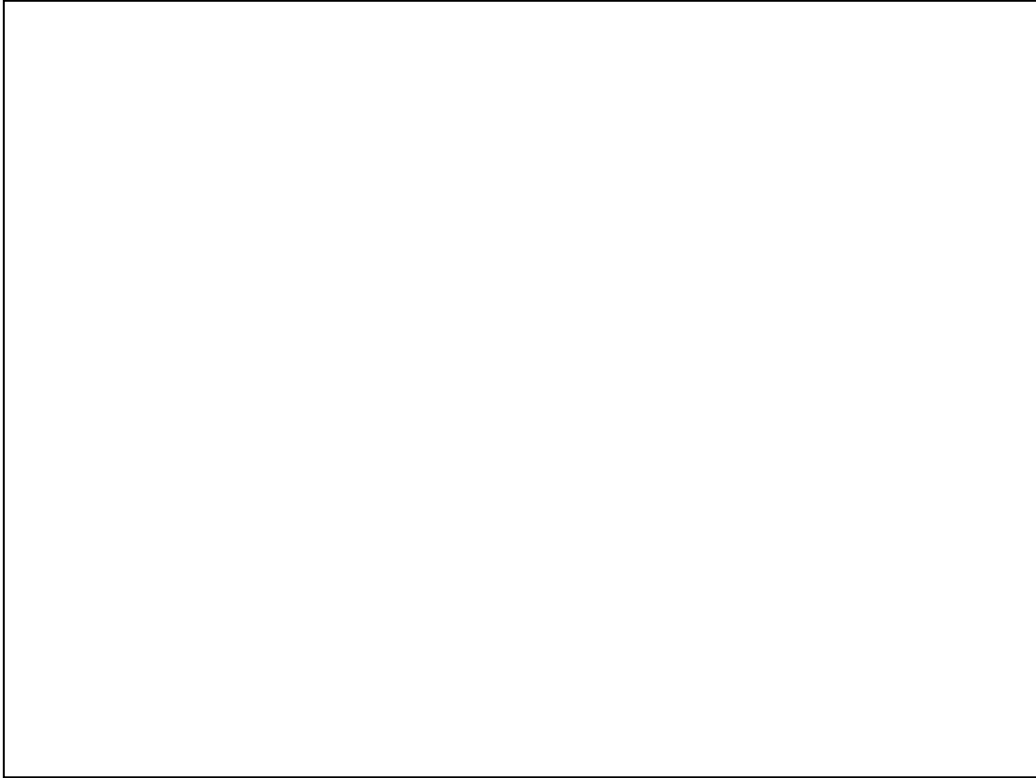
There is a nice movie about what id done to your privacy with RFID.

Privacy is a big issue.



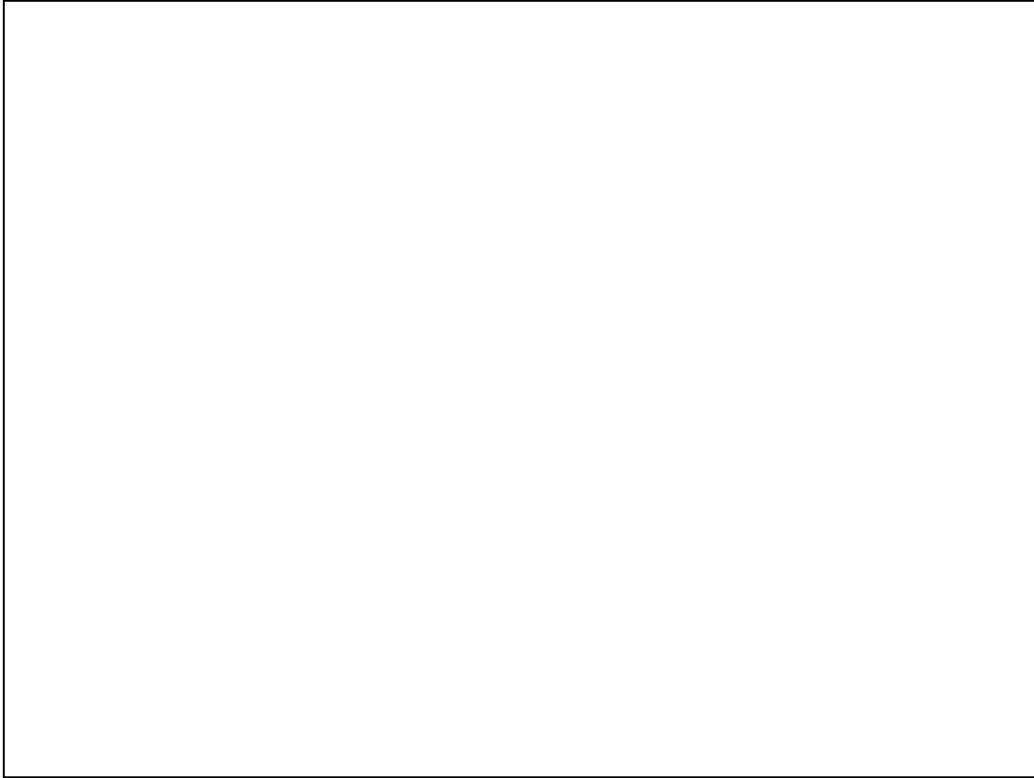
## Mifare Classic workings (Nohl & Plötz)





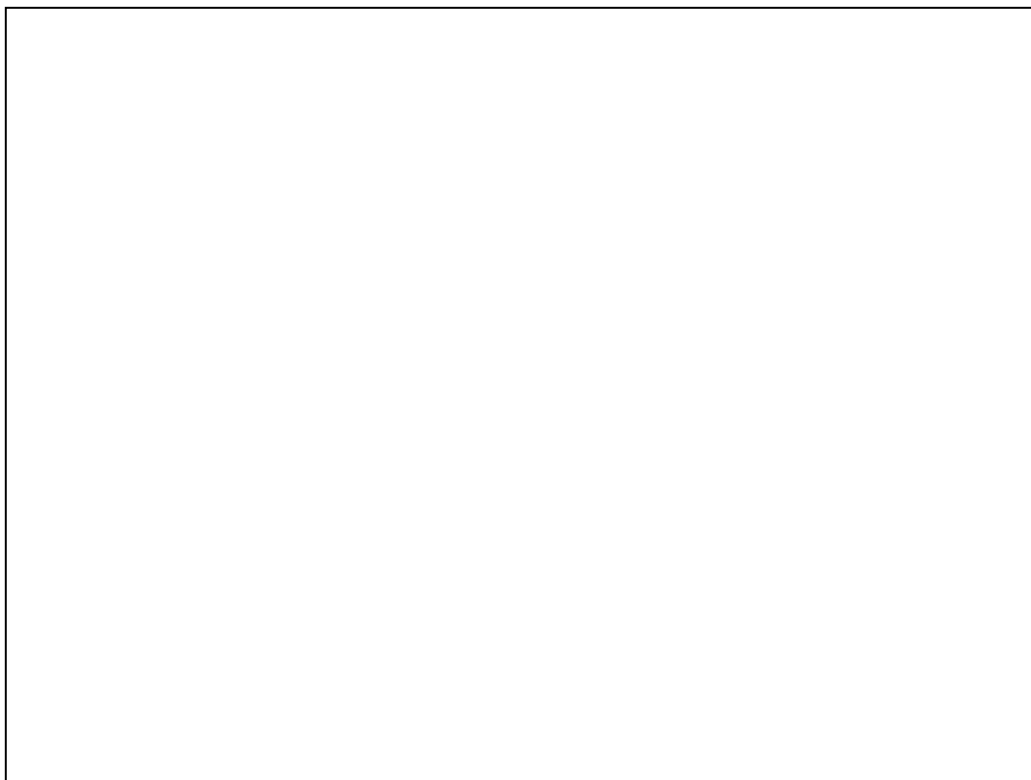
Ever given your password/phrase away? Who not? Well shared secrets are not shared.

Social engineeruig is an easy hacking tool. Keep secrets to yourself only.

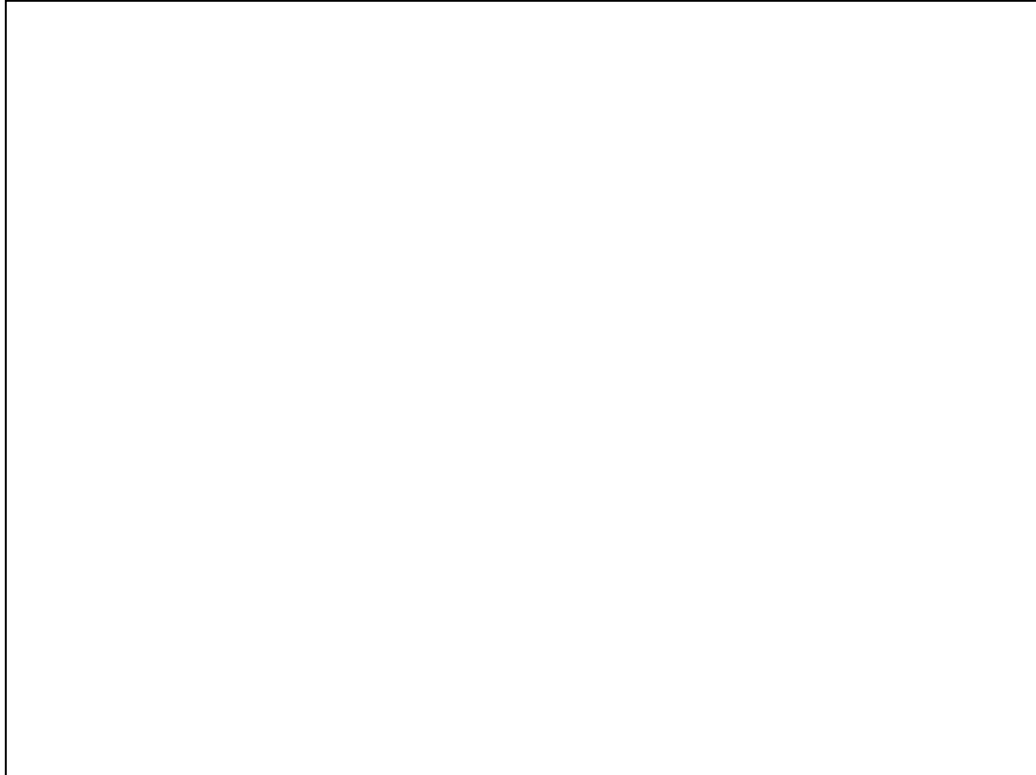


This looks crazy: publicing the encryption or decryption key. But it is not. It get complicated now. But it is a rich tool.

How do you know the pub key is from him. Once encryped with one key it can only be decrypted with the other... It is simple, but have a good thought about it.



OK we know the mechanism. How do you apply it.



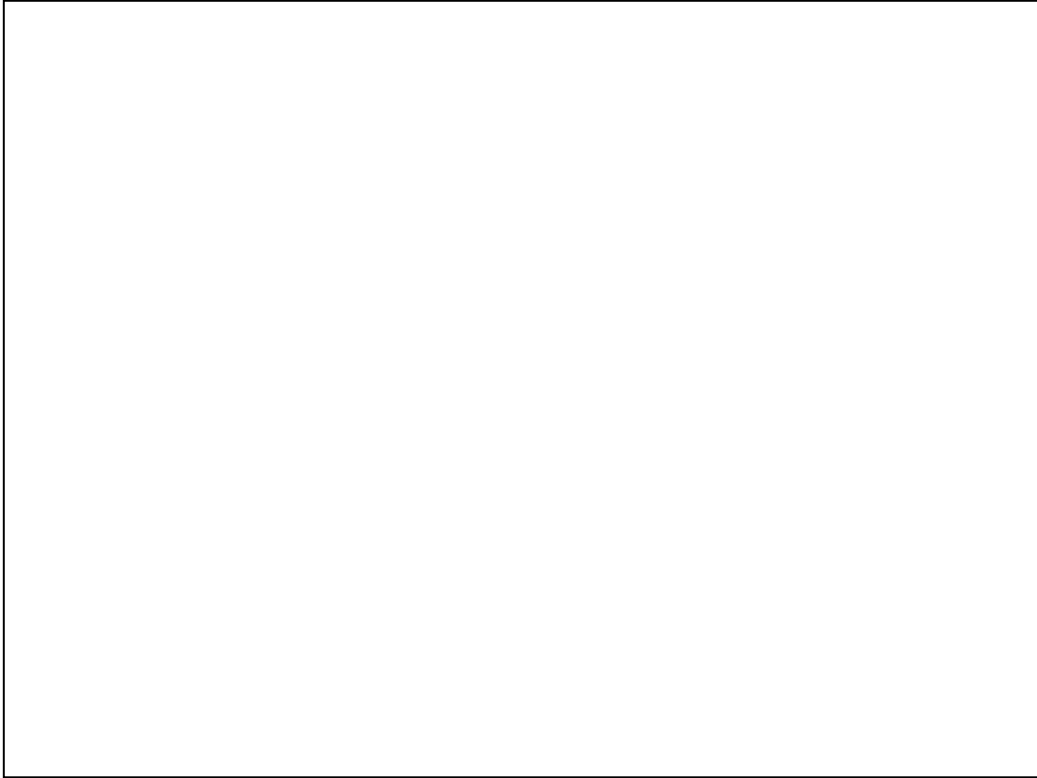
How to make sure the content is readable and it can be checked that the message came from this sender.

We use a type of checksum which is unique for the message.

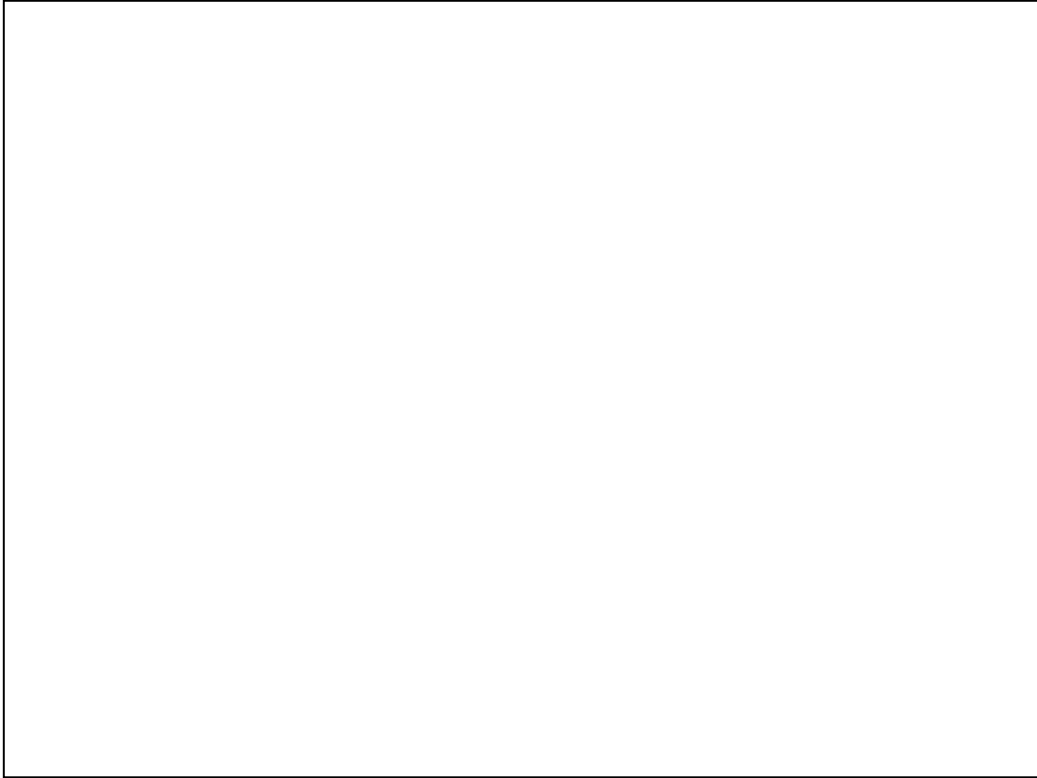
How to secure that the checksum is the right one and still can be checked by everybody?

We encrypt it with the private key of the sender. Everyone (we have published this key) can apply the public deciphering key. So we know the checksum is calculated by the sender.

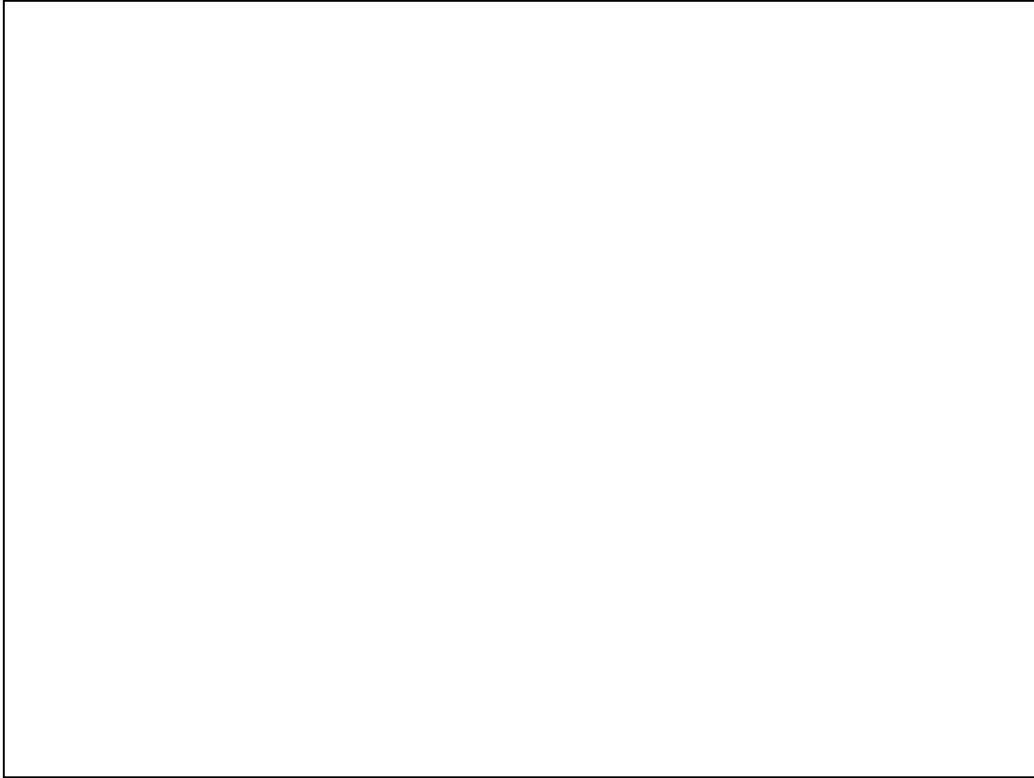
How do we know the public key is his one? We need an authority to say yes his name is on that key.



A real live example. First the mechanism.



How does the example work with email



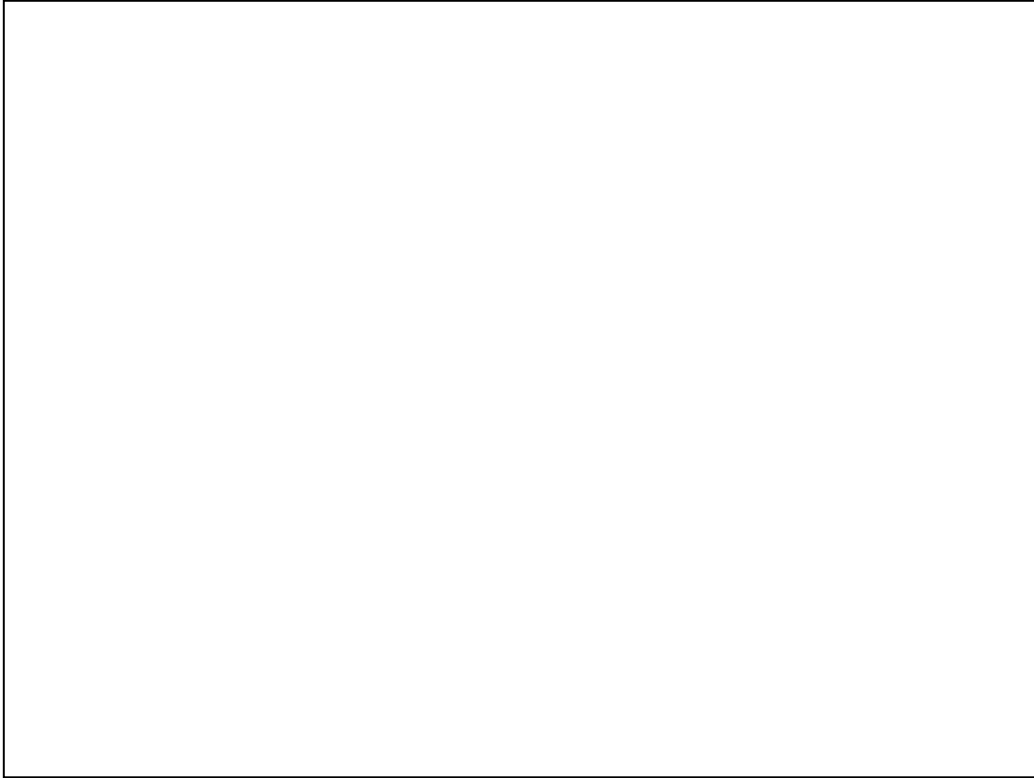
How does encrypted and signed email show up in Thunderbird.

Note the lock (encrypted) and envelope (signed) icon. Note the warning symbol on the envelope. Look at the certificate by clicking on the icons. Have a close look and well the certificate was expired.

Is the signature ok?

Is this an error or a warning.





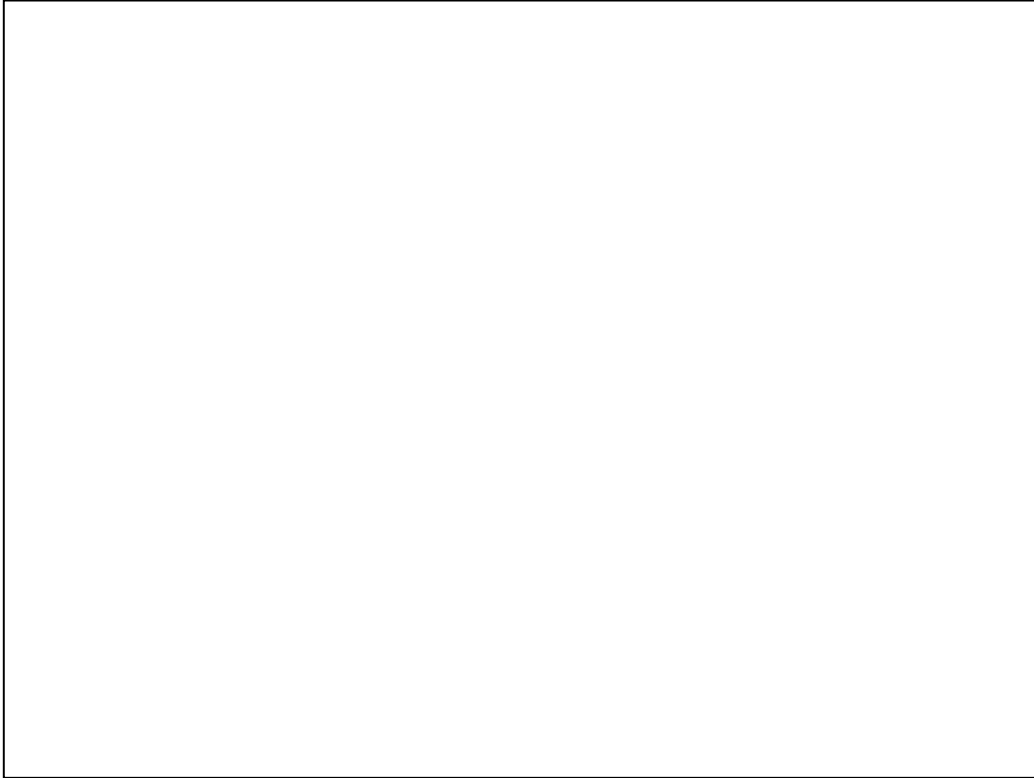
Spend money or join the CAcert community.

Be a member

The portal to secure yourself...

But know what you do! Read the agreement. Know it is based on the Open Source mind set. It is free, and it should remain free. And it should be improved. You need to contribute and that contribution should be free as well.

Feedback what you think is not right.



#### Password

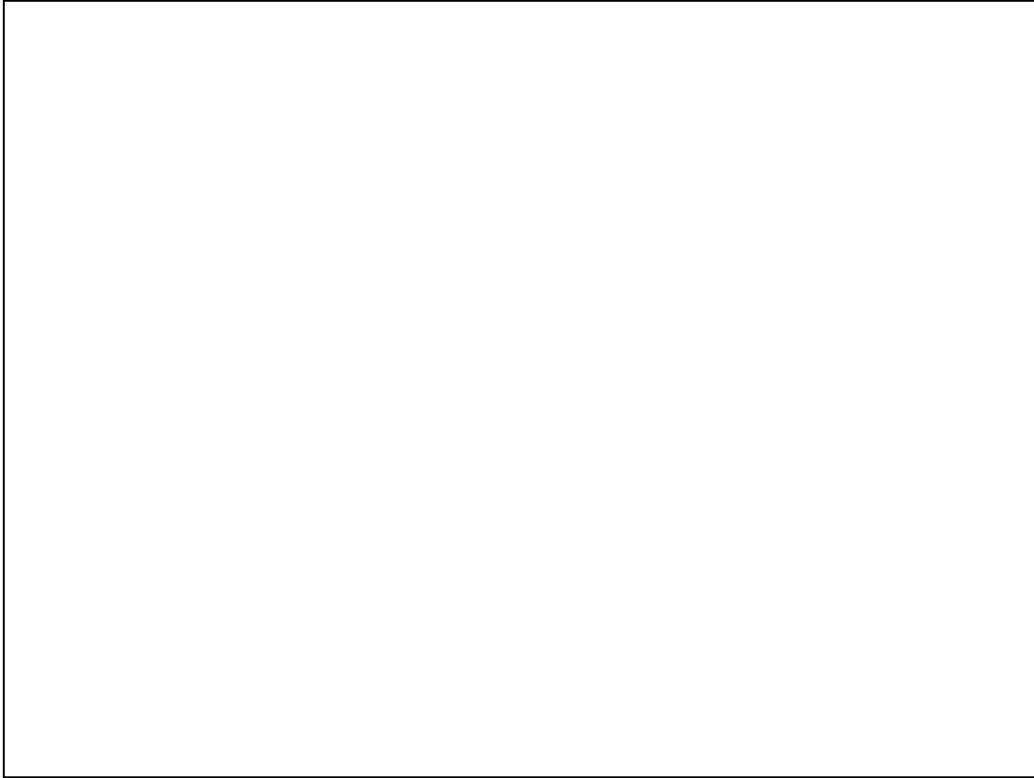
five questions and answers to remember just in case

note you can login CAcert web site with your CAcert certificate. No password to remember. Well when is your certificate expired. Yes two years ago I gave my password, one not that easy to guess....

Make sure the full name you provided is the same as on your passport (birth certificate).

Birth date?

You have more as one name and can proof it? Well you can do so, but need ID proofs. (Not implemented yet).

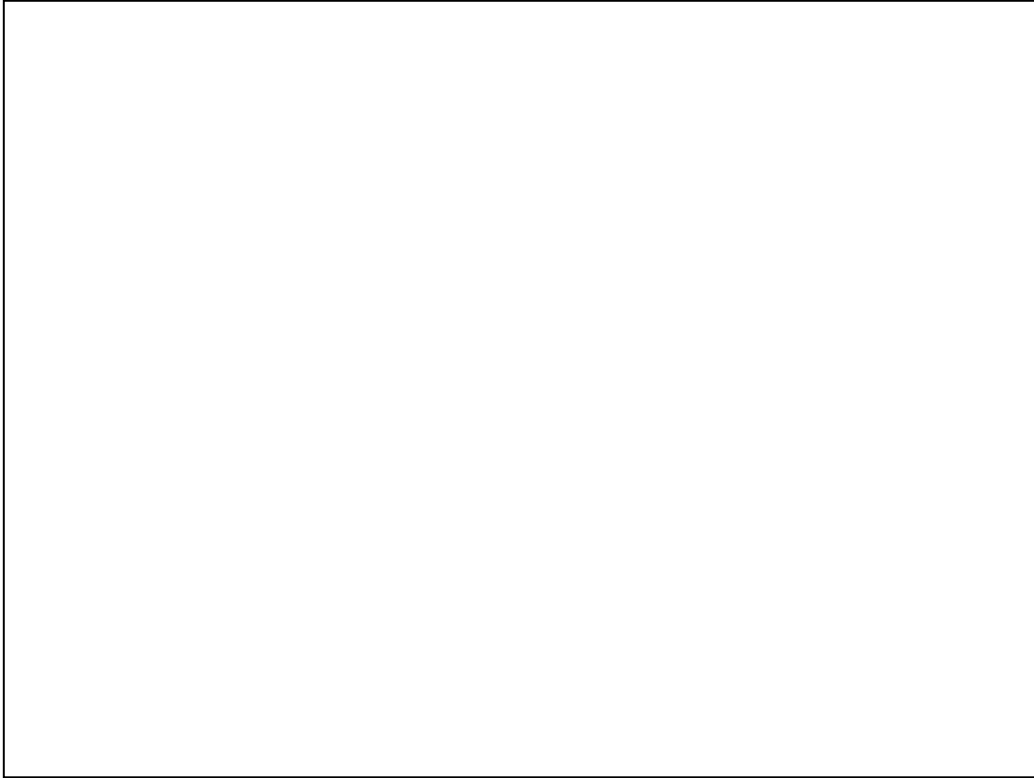


Well, once there. How to prove it is you. Have your identity checked.

Note you need to do that with more as one assurer.

Where to find him? Look at the assurer location finder. Or and that is pretty effective go to an assurer event.

One assurance give you 10-35 points. You need at least 50 to get your name on the cert. The best is to collect 100 points so with some knowledge of how this works you can assure others and help to enlarge the community



Every assurance you need one form. Start to print out at least 4 of them. Yes a lot of paper work.

Note that your name on the form should be identical to your passport and the name you provided on the CAcert account.

Name should be identical to account full name, and ID shown.

More names are possible but you need to proof it.

Married name? No problem but show it to an assurer.

The latter requires some implementation still.



## CAcert Organisation Assurance

- the organisation entity is in control:
  - domain server certificates
  - Email certificates for individuals within the organisation
- Organisation needs to have:
  - CAcert Assured administrator > 100 WoT points

© CAcert, 2008 Teus/HCC-Venlo 8 Jan 2008 50 slides minus 27 to go

Organisation Assurance is possible now.

But ask for the CAcert subpolicy for this in your country!

Currently only: Germany and Holland.



## 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



### CAcert Organisation Assurance Programme COAP

CAcert is an international organisation. The English language is chosen to be the formal language. For your convenience a translation to Dutch is provided here in *italic*. The translation is to be considered a help only. English remains the ruling language.

*CAcert is een internationale organisatie. Engels is de gevoerde taal binnen de organisatie. Als hulp is hier een vertaling in het Nederlands bijgevoegd (cursief). De vertaling dient als hulp. De Engelse tekst is bindend.*

#### Applicant (*Aanvrager*)

Name of the Organisation <i>(Naam van de Organisatie)</i>	
Contact email address <i>(Contact email adres)</i>	
City ( <i>Vestigingsplaats</i> )	
State ( <i>Provincie</i> )	
Country ( <i>Land</i> )	
email(s) of administrator accounts - must match a CAcert account ( <i>CAcert Account email adres(sen) van de systeem administrateur</i> )	
Domain(s) <i>(domein-naam, (-namen))</i>	

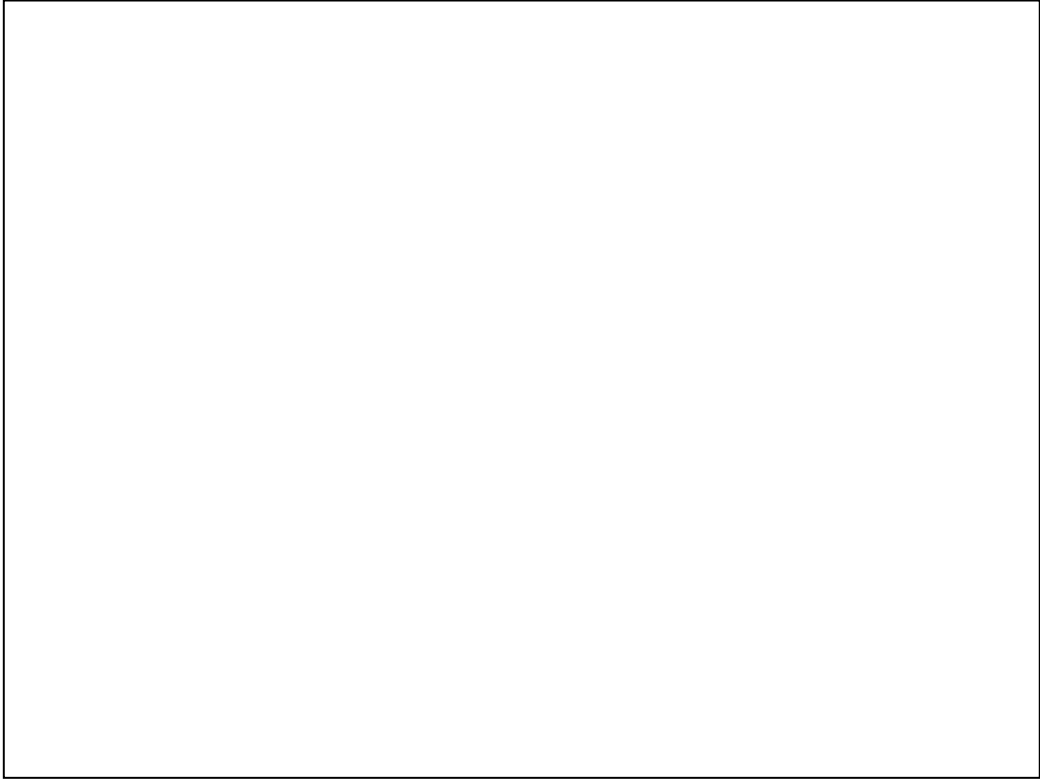
As proof for the legality, identity and legality of signatures for the organisation the following official documents, either original or in certified copies and not older as 4 weeks, are attached to this form.

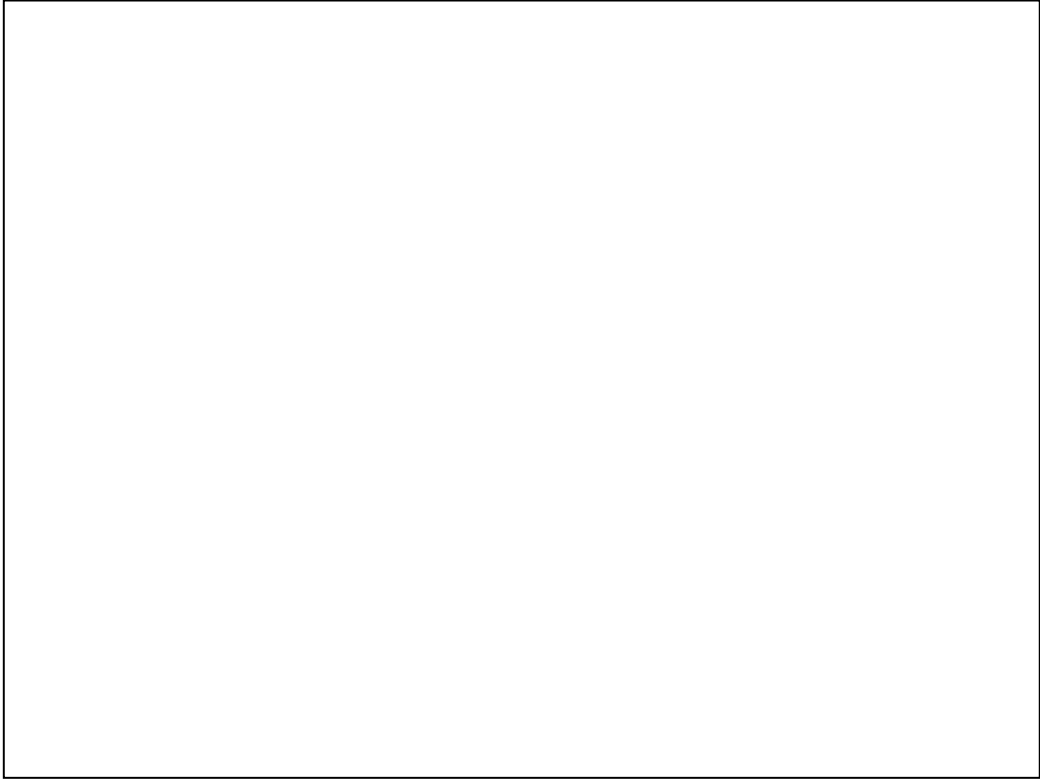
*De volgende bewijstukken voor de officiële naam van de Organisatie, haar rechtsform en de namen van de tekenbevoegden zijn de volgende originelen of gewaarmerkte copien niet ouder dan 4 weken, zijn bijgevoegd.*

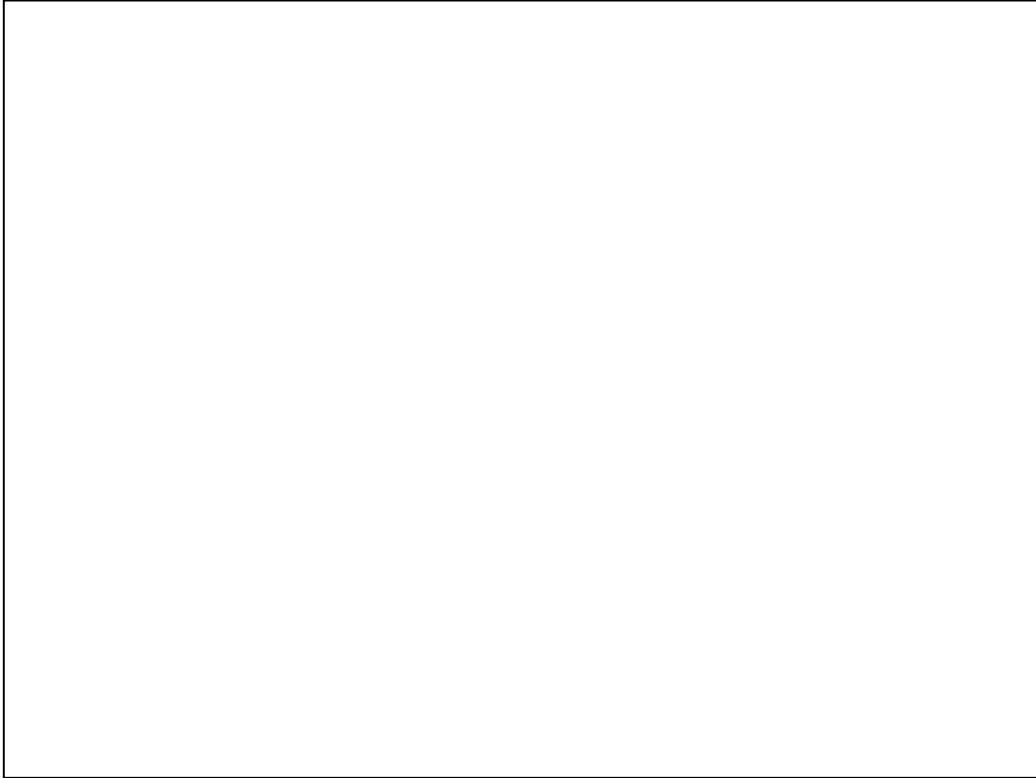
--







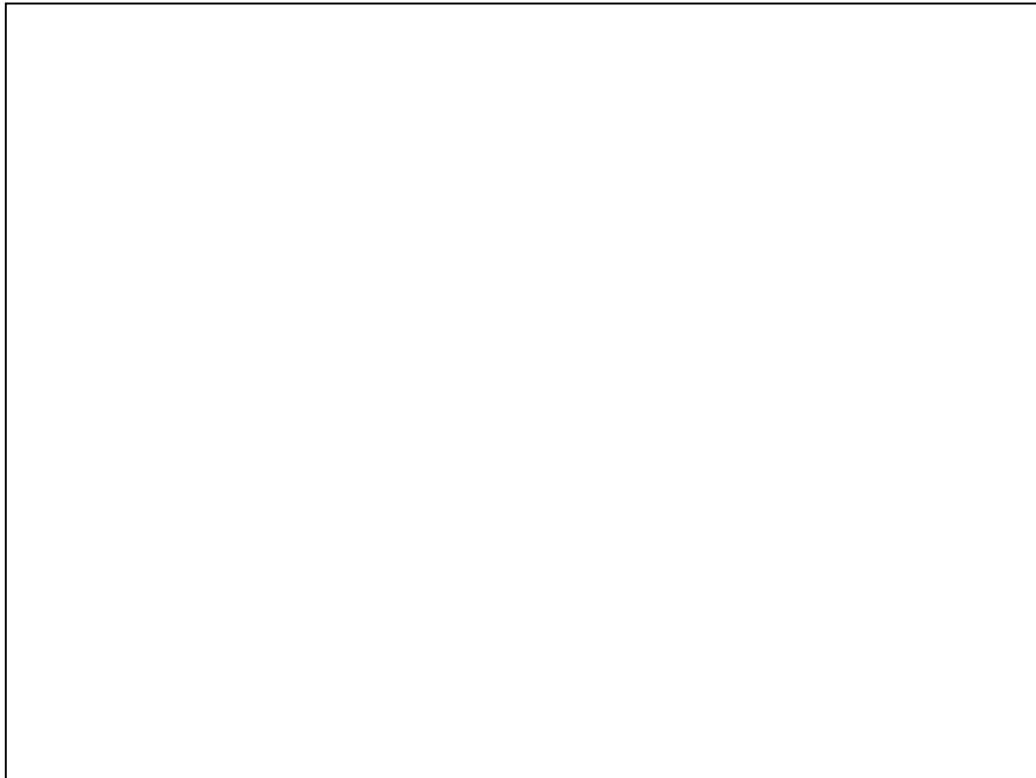




P12 is binary format and is password protected.

The others are ascii and not password protected. It matters for the private key. Keep it save.,

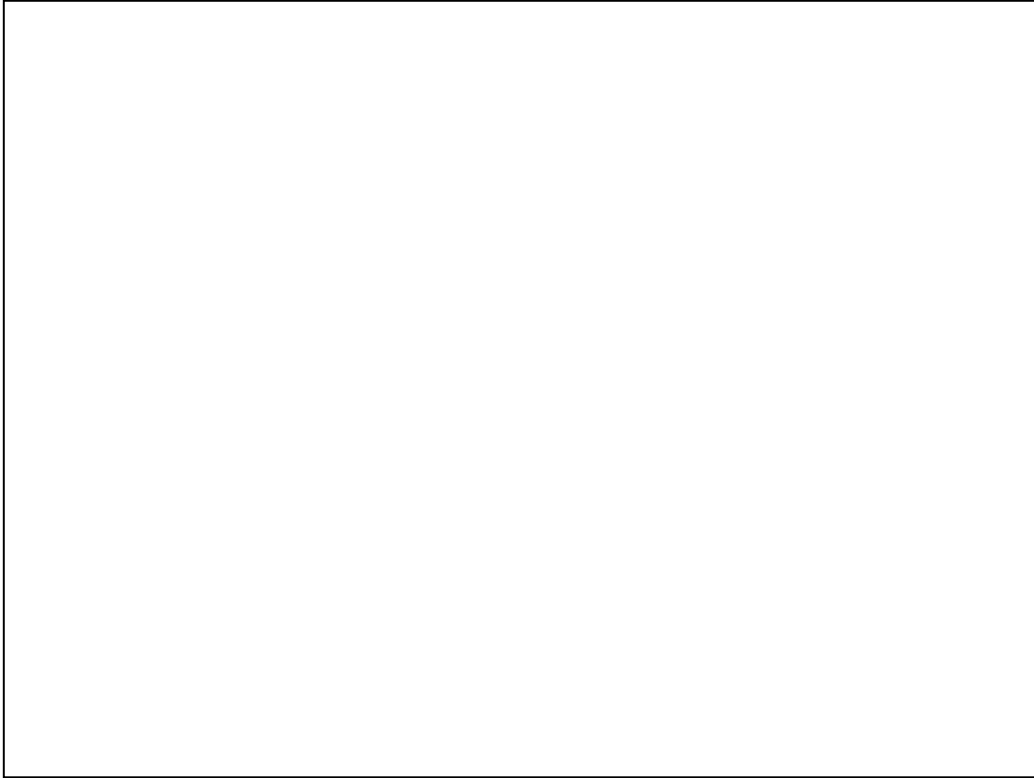
You do not want to loose them. What about all your emails encrypted and you lost your private key?



How to create keys see later.

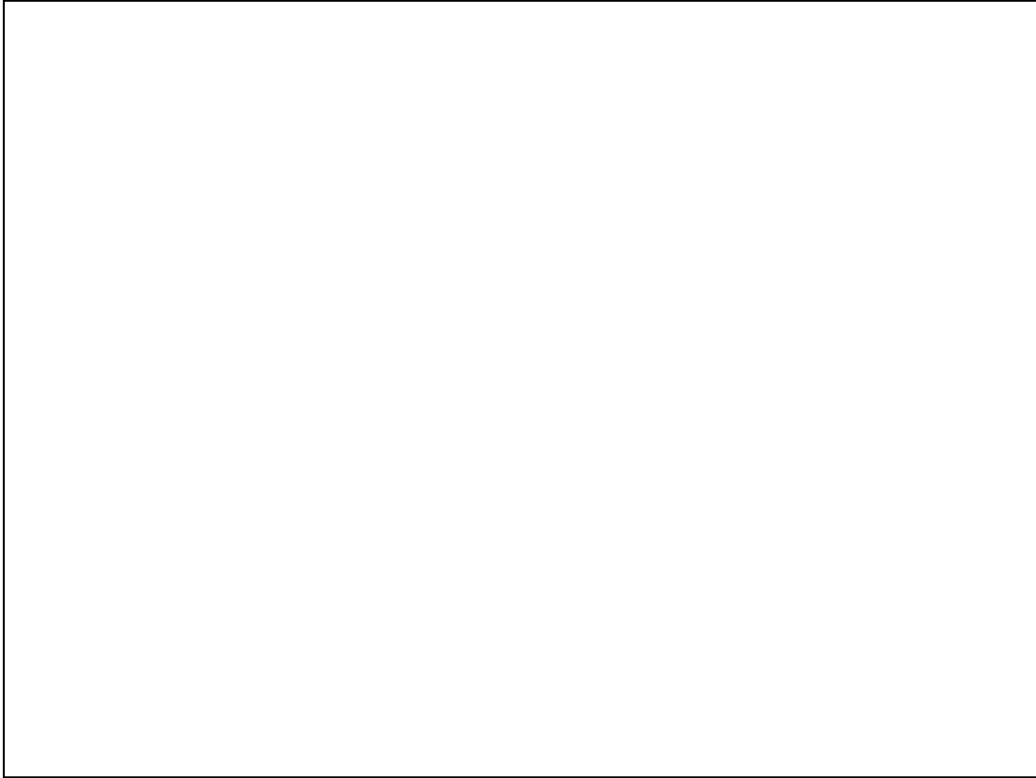
CSR is your pub key with the question for the CA to sign it. It is returned by the CA as certificate (CSR).

Private (Key) and CSR can be combined in one file the PEM file. Most browsers and email handlers need a binary p12 file. So you need to convert PEM to P12 (can be done by openssl and others.).



For non 64 bit machines Firefox/Thunderbird has an easy add on to create a key and to make the CSR ready.

Note that CAcert only will allow name (CN) and email address. CAcert tries to keep traceability and privacy info as low as possible.



This is in the openssl package. The arguments are rich. To get5 started you need only to know a little.



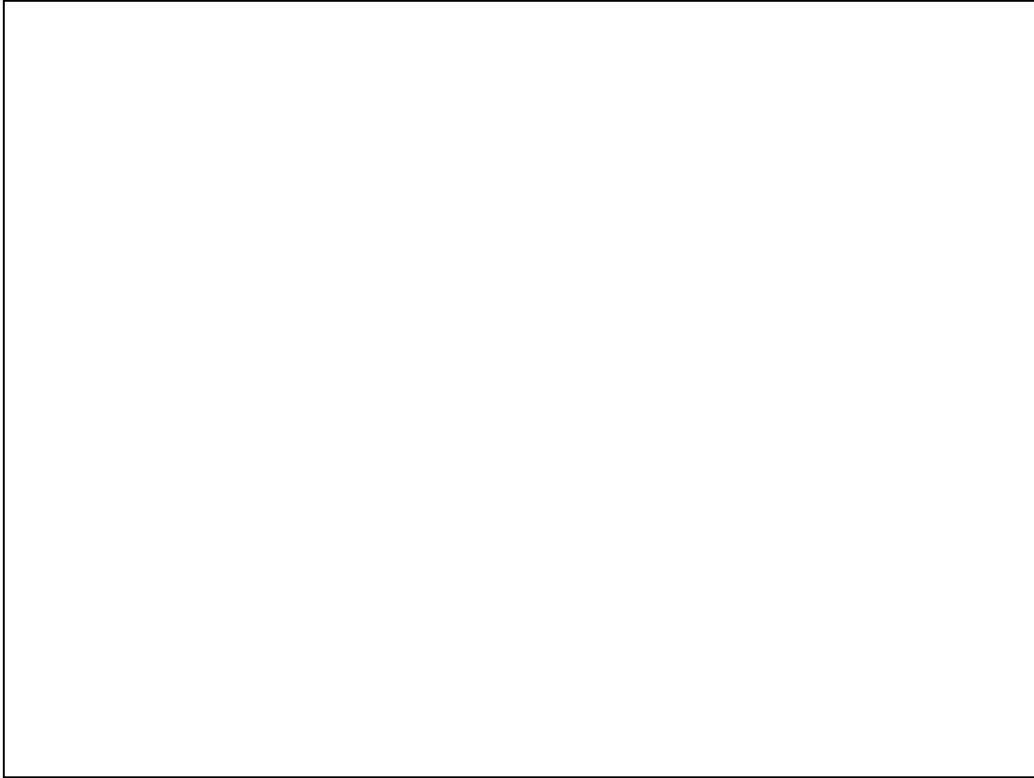
Certutil come from the nss-tool package. It operates on the database  
firefox/thunderbird use.

Look here: `cd ~/.thunderbird/*.default`

eg cert8.db

Make sure you take these files with you when you move from one system to the  
other.

Make sure if you try things out you make a backup.



Certutil is a handy tool to extract collected public key, signed certificates from the database (user certificates from Thunderbird).

Certificate collect is fully dependent on email sent signed to you.



