

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



© Tumo, Yola 1999 Feb.

your passport is it really you?

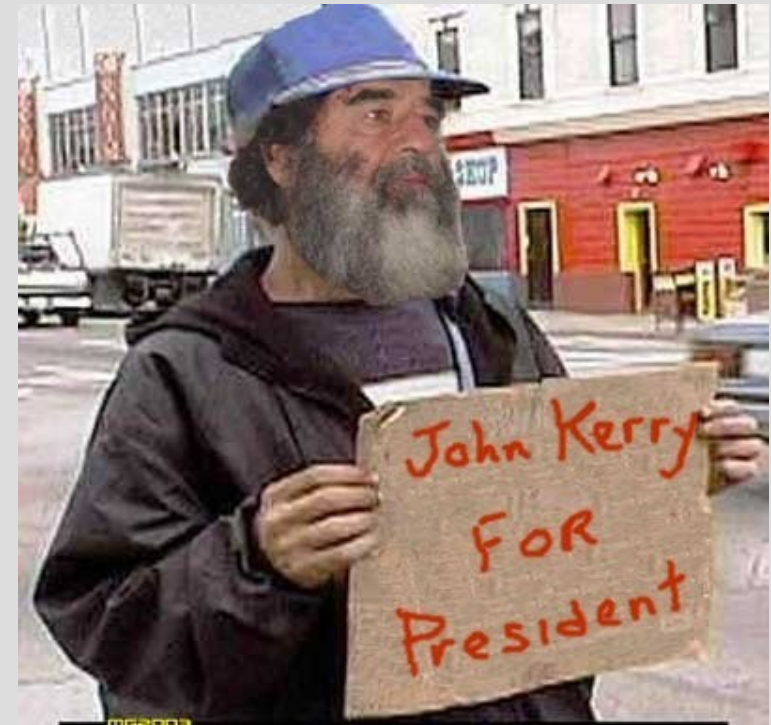
- BBC 1 Panorama 1st of December 2006
- Shahiba Tulaganova UK journalist:
 - within 5 months on east European markets
 - bought 20 EU passports, 5 other
(UK, DId, F, S, NL, B, Es, PO, G, Cs, Pl, Au,)
 - 300-3000 euro each
 - and was able to pass UK border many times with them.



secure digital content

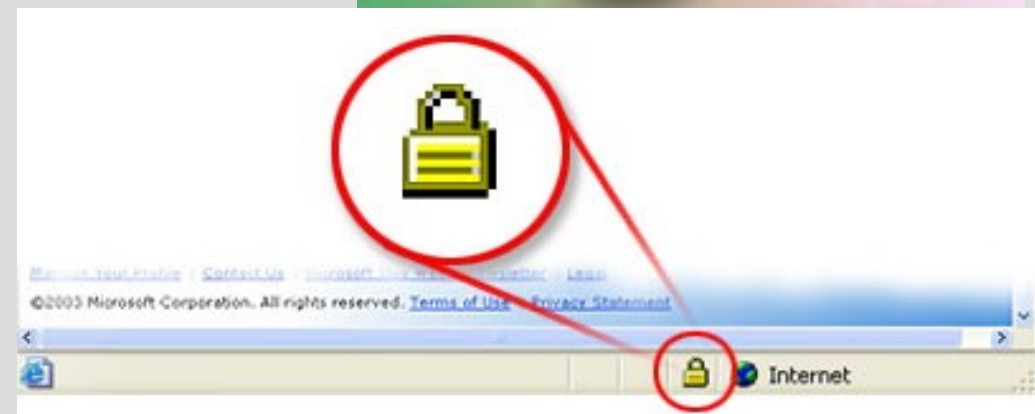
- documents
- images
- software code

- 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:

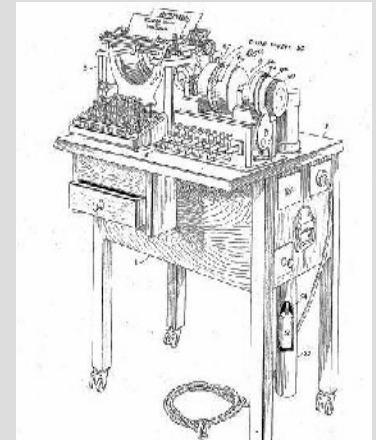
“Any person can invent a security system

so clever

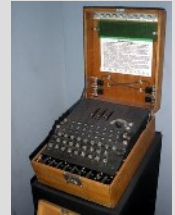
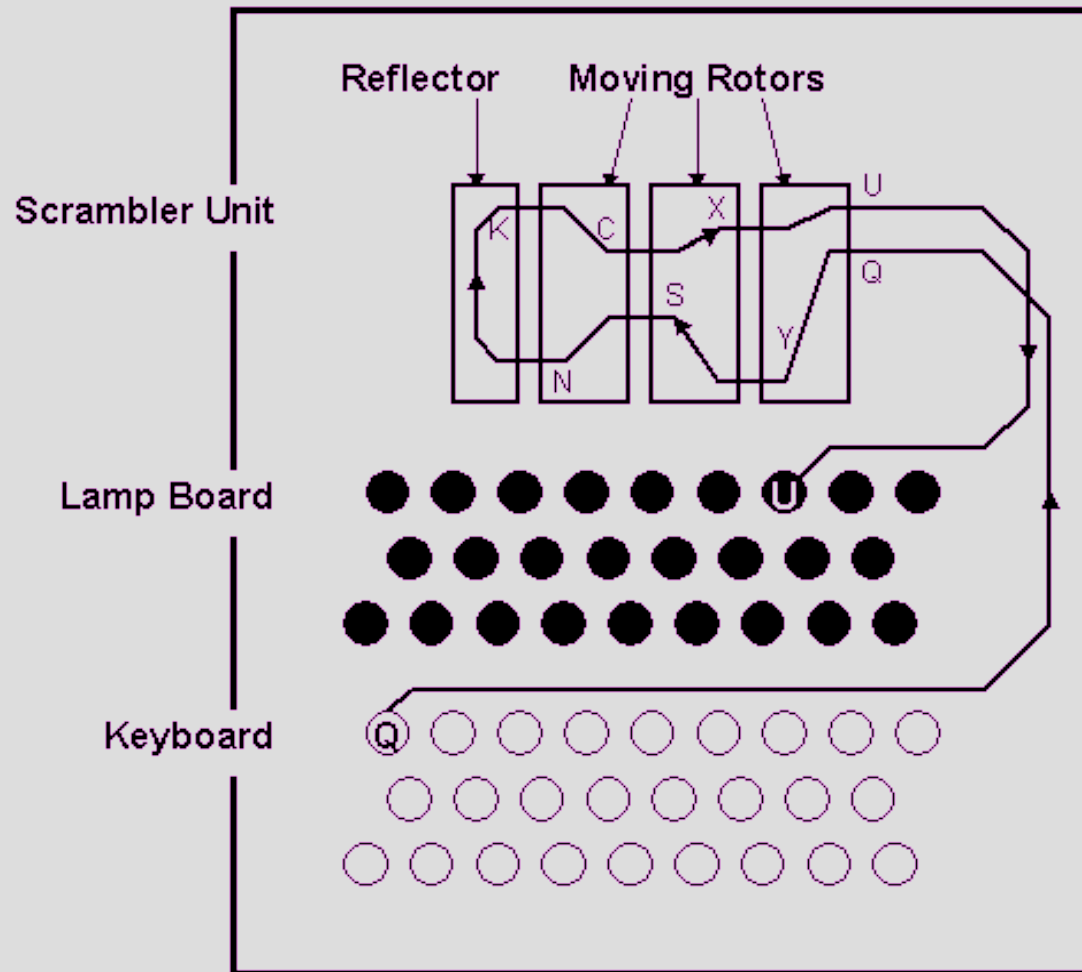
that she or he can't think of how to break it”

encryption

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



Enigma technology



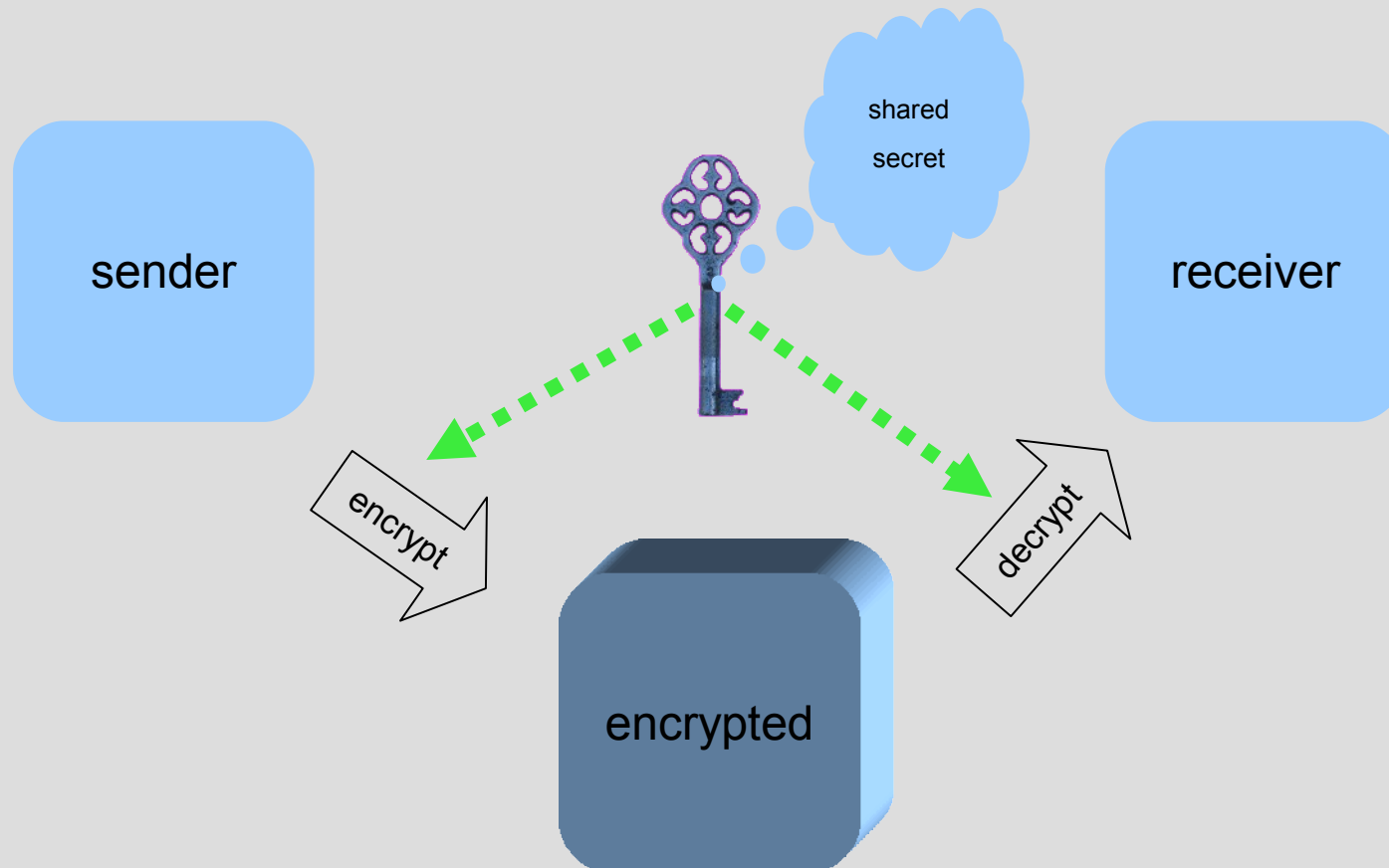
RFID chip hacked Dec 2007

- Mifare RFID chip of NXP (Philips)
- Karsten Nohl and Henryk Plötz
- 48 bits but only 16 bits used
- implications:
 - car keys
 - public transportation cards
 - FIFA World Cup tickets



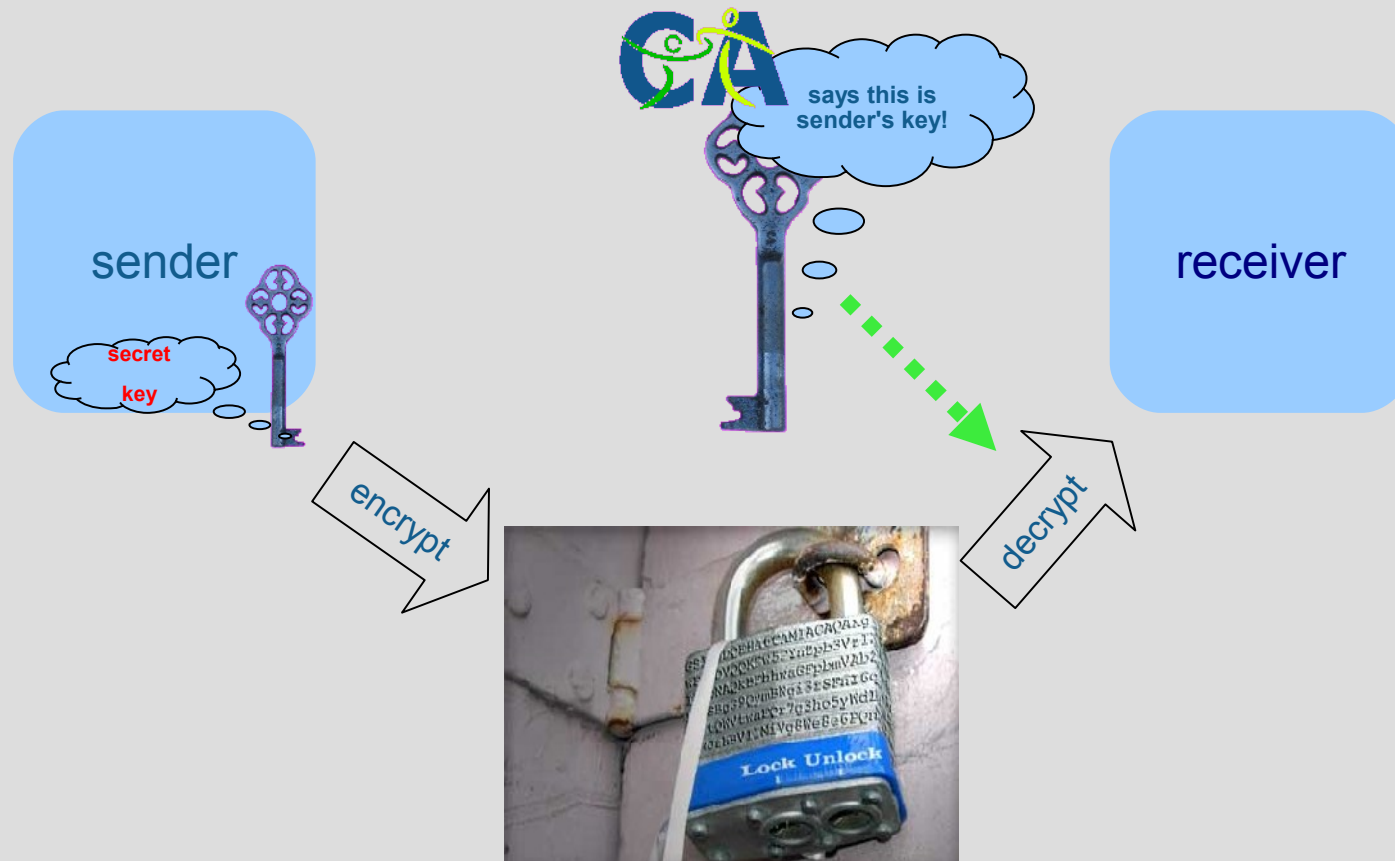
encryption key types

symmetric key encryption

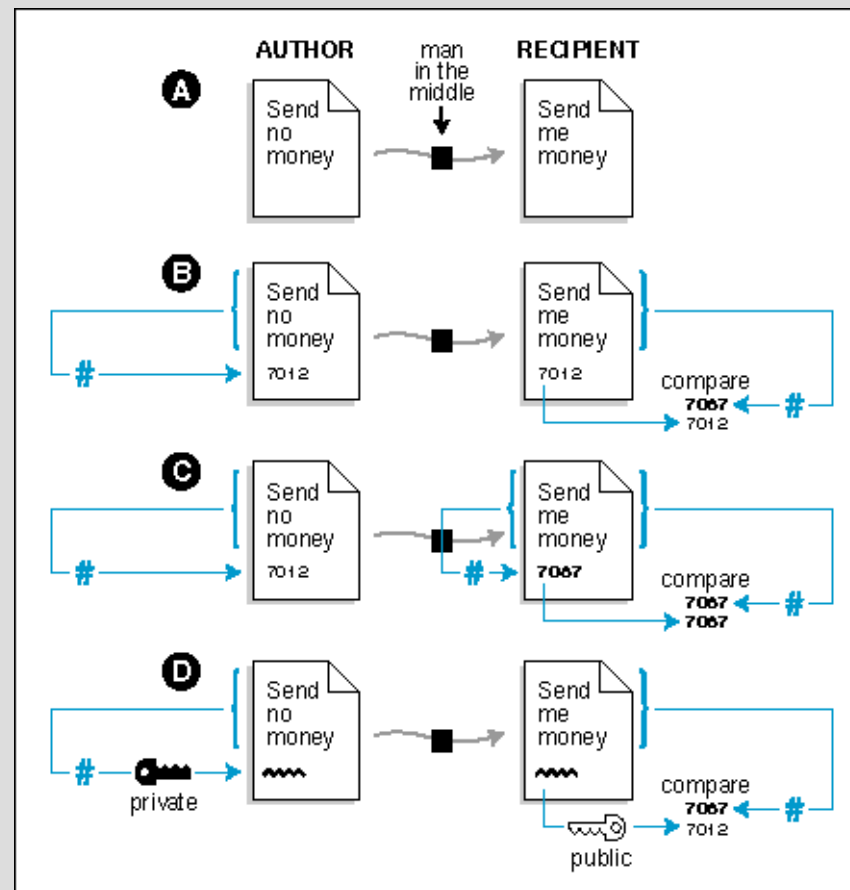


asymmetric key encryption

that message can only come from him!



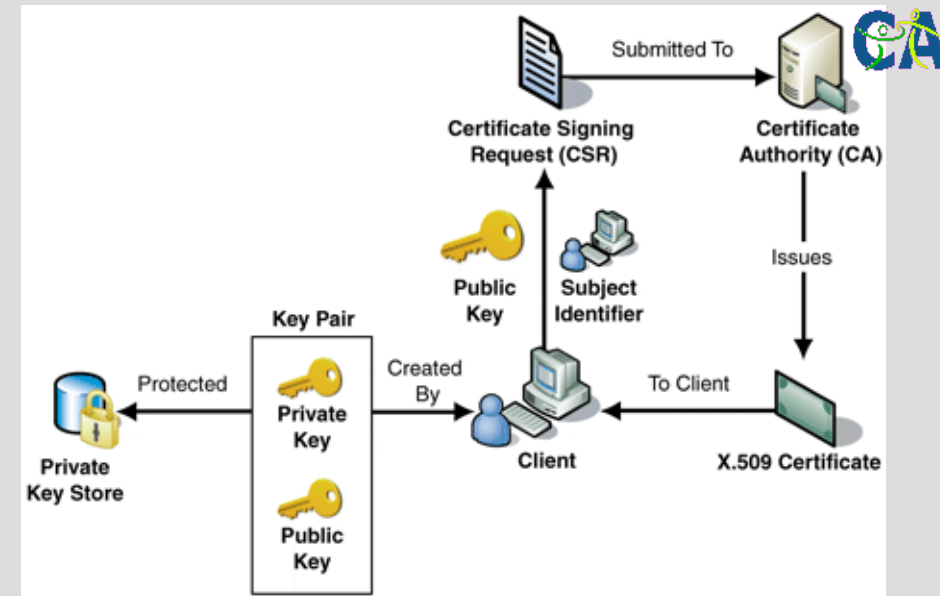
how do “signatures” work



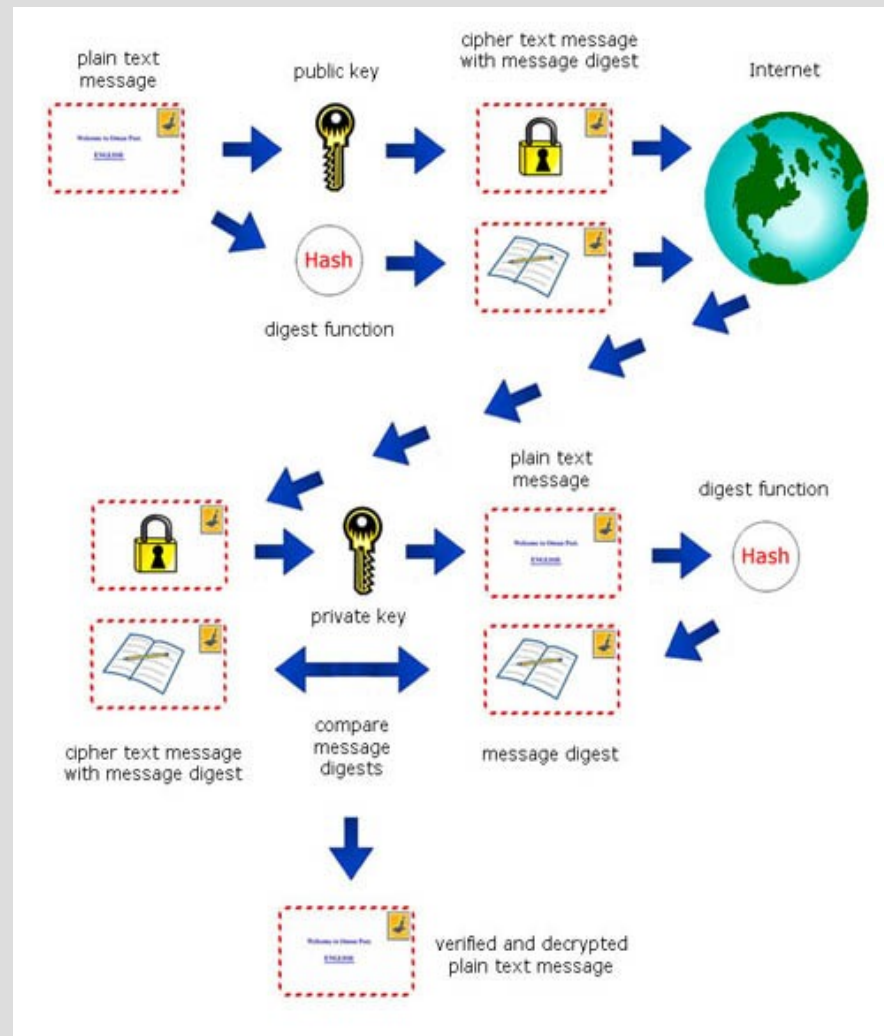
Certificate Authority signature

- 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 content is partially visible, showing "Hi," "The", and a URL "http://213.154.225.230/". Below the email content, there are two error messages:

Sender Verification: Message is too old to verify sender.

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: pgg@futurenet.at
Certificate issued by: CA Cert Signing Authority
[View Signature Certificate](#)

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.

On the right side, a **Certificate Viewer** window is open, showing details for the certificate used to sign the message. The certificate is issued to Philipp Gühring and is no longer valid because it has expired.

Certificate Viewer: "Philipp Gühring"

General Details

Could not verify this certificate because it has expired.

Issued To:
Common Name (CN): Philipp Gühring
Organization (O): <Not part of Cert file>
Organizational Unit (OU): <Not part of Cert file>
Serial Number: 02111111

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

Validity:
Issued On: 12/02/2006
Expires On: 12/02/2007

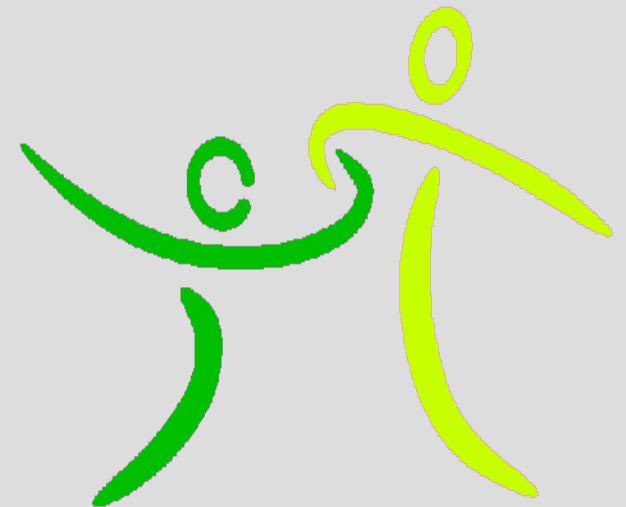
Fingerprints:
SHA1 Fingerprint: 70:CA:93:6F:CA:05:2A:B1:63:DE:75:2C:11:7D:7F:ED:0E:01:7D:1C
MD5 Fingerprint: F3:55:64:25:BC:72:CD:A4:2D:DA:30:53:52:73:3A:C9

Buttons: [Close]

the CAcert CA?

certificates free for everyone

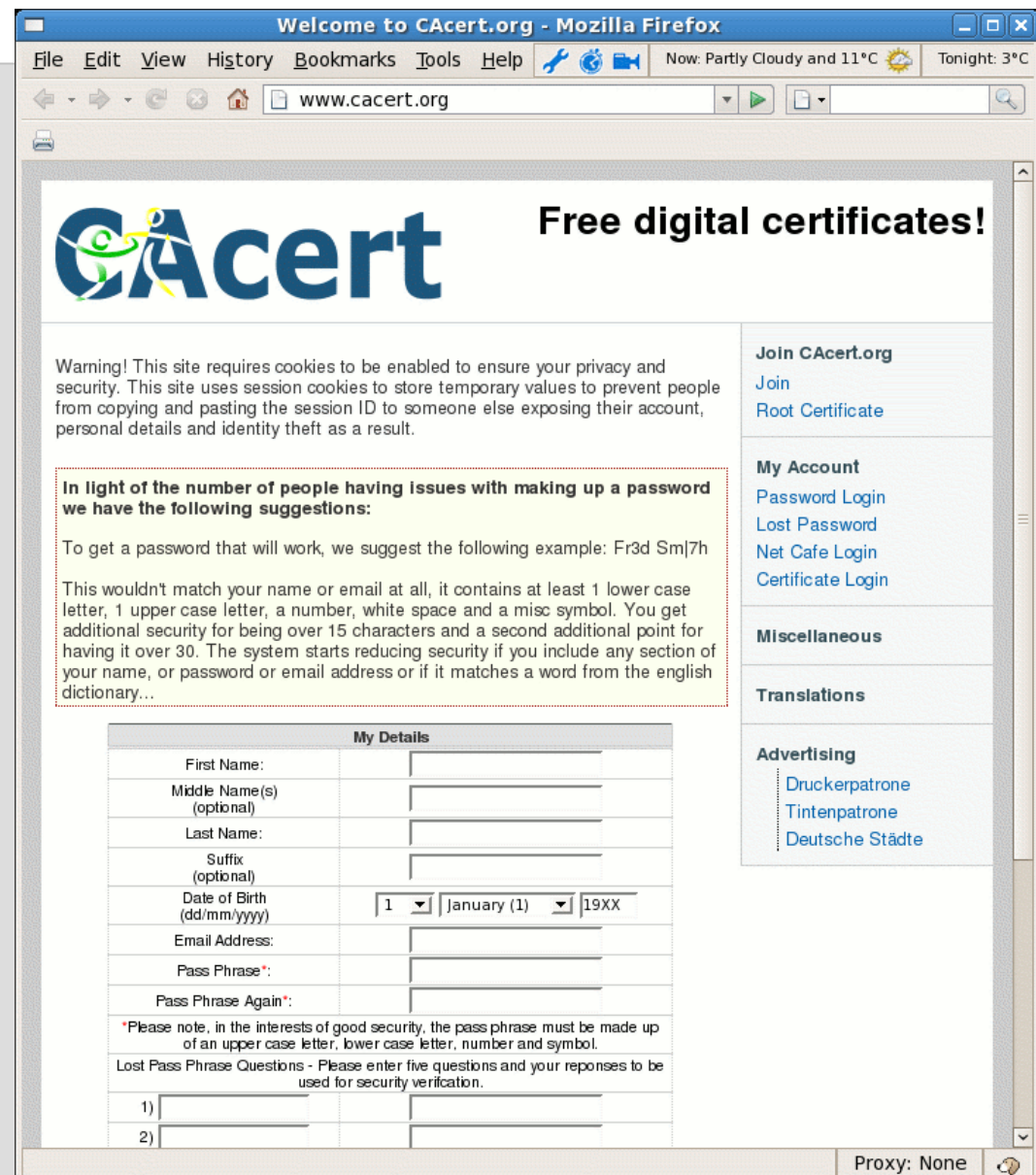
- join CAcert Community
 - agree with privacy rules
 - agree with CAcert Community Agreement
 - get CAcert account: join via <http://www.cacert.org>



HowTo join Community

register

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



The screenshot shows the CAcert.org website in a Mozilla Firefox browser window. The page title is "Welcome to CAcert.org - Mozilla Firefox". The address bar shows "www.cacert.org". The main content area features the CAcert logo and the text "Free digital certificates!". Below this, there is a warning about cookies and a section titled "In light of the number of people having issues with making up a password we have the following suggestions:". This section provides a password example "Fr3d Sm|7h" and explains its complexity requirements. At the bottom, there is a "My Details" form with fields for First Name, Middle Name(s) (optional), Last Name, Suffix (optional), Date of Birth (dd/mm/yyyy), Email Address, Pass Phrase*, Pass Phrase Again*, and Lost Pass Phrase Questions. The right sidebar contains links for "Join CAcert.org", "My Account", "Miscellaneous", "Translations", and "Advertising".

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="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"/>

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)

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

--

It is free

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 in blue), "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

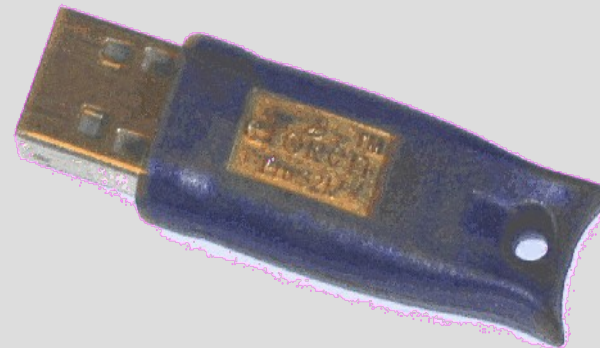
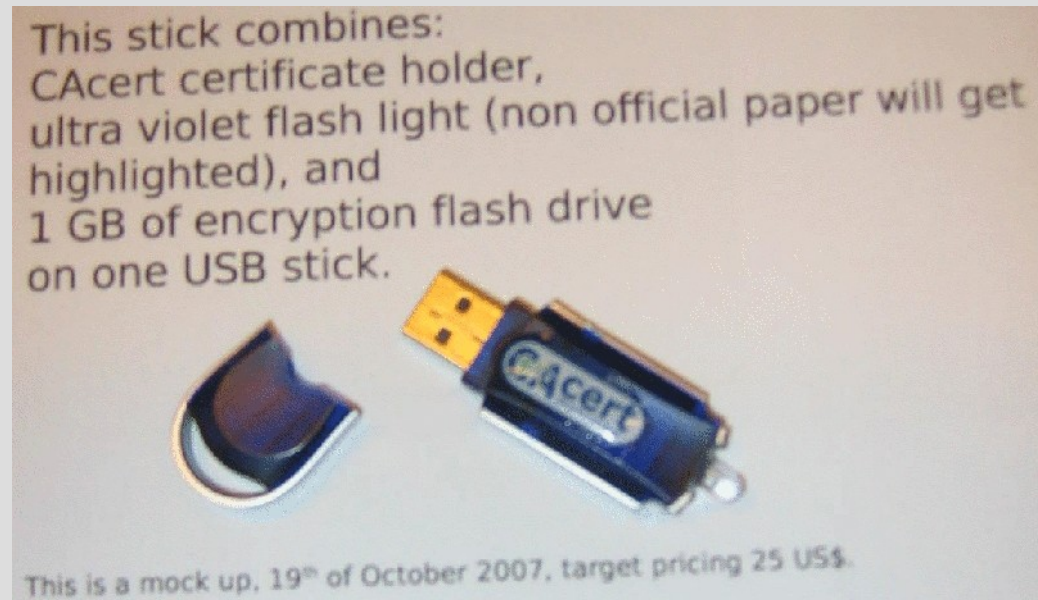
Fingerprints

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

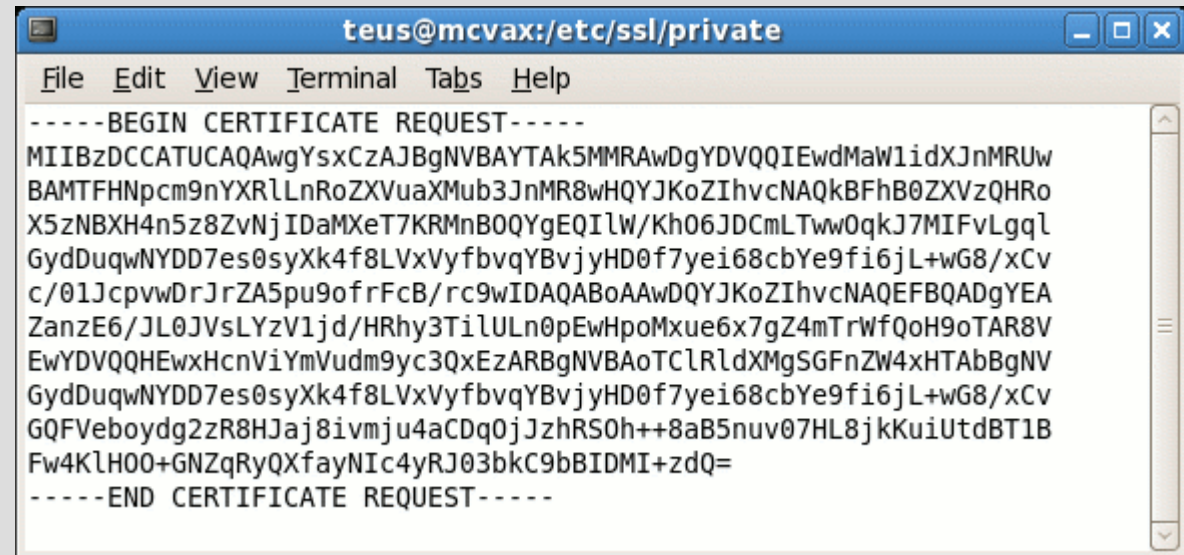
client certificate how to?

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



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 body consists of a long string of base64-encoded characters.

```
teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwYsxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdMaW1idXJnMRUw
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



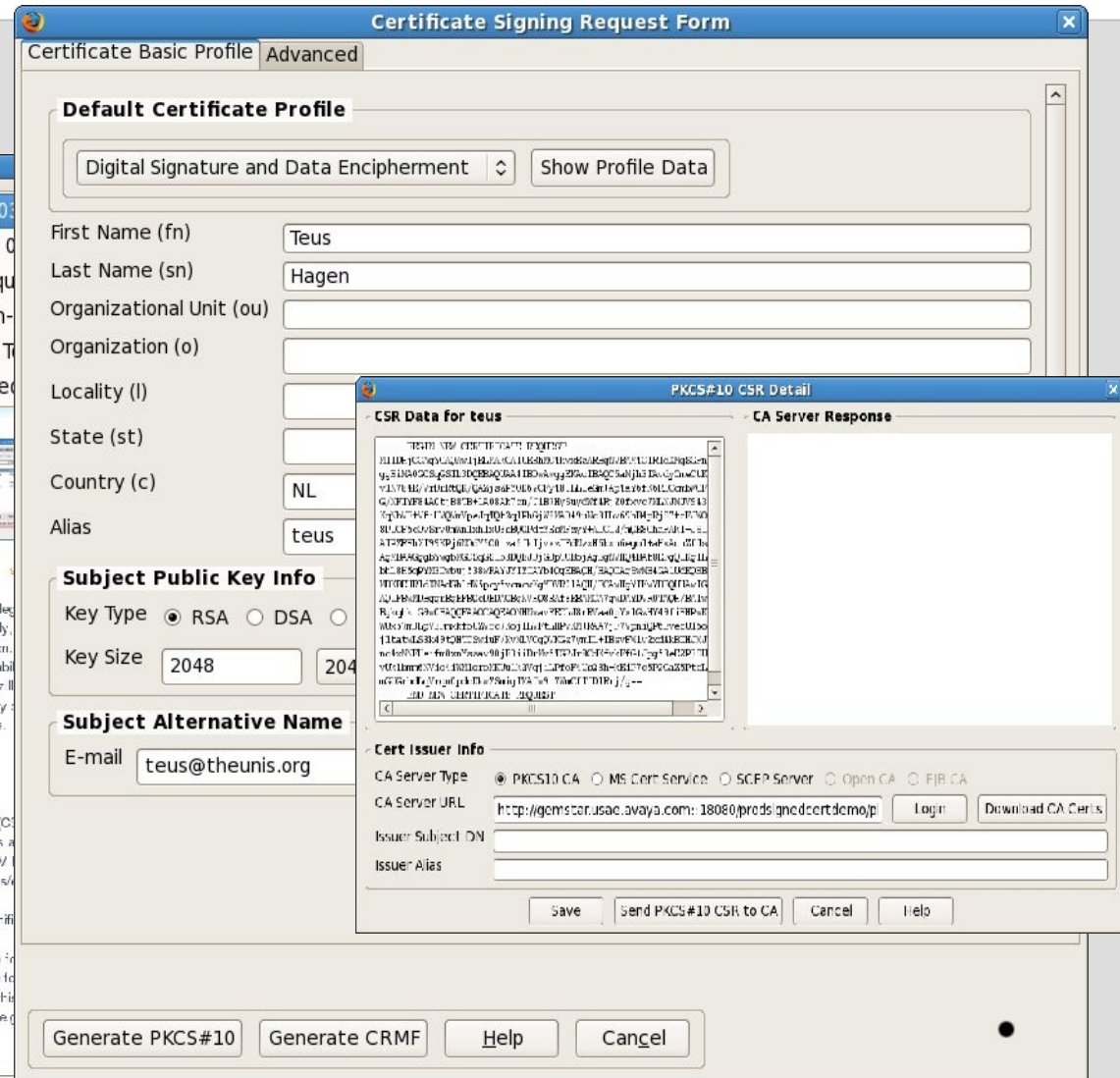
Key Manager (v 0.1.0.20071203)
by [Subrata Misra](#)

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. It is packaged as a "chrome" based Firefox extension. Currently, it does not provide GUI for local key generation, Certificate Manager wizard in Mozilla PSM and added the capability to enroll certificates. Our extension enables Mozilla based certificate enrollment. In addition, the tool supports signing of proxy certificates and provides XUL based GUI for signing of XP 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 it can be invoked from other extensions and XPCOM
- signing of archive files (including XPI files), to Mozilla add-ons
- XUL based GUI for command-line signature in Mozilla NSS
- Signing of Proxy Certificates (RFC3820) and other users certificates
- Signing and verification of Attribute certificates (RFC3281)
- Exporting of private keys in PKCS#8 and PKCS#2 formats
- based public key certificate and generation of configuration file for applications, such as GURU, GnuTLS toolkit, etc. (You will find this in the documentation)



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

CA Server Info
CA Server Type: PKCS10 CA MS Cert Service SCEP Server Open CA FJR CA
CA Server URL: http://gcmstest.usac.avaya.com:18080/predsignedcertdemo/jsp/ Login Download CA Certs

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
```


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-----
MIIE7DCCAtSgAwIBAgIDAyVvMA0GCSqGSIb3DQEBAQUAMHkxEVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHA6Ly93d3cuJ0Lm9yZzEiMCAGAlUEAxMZ
Q0EgQ2VydCBTaWduaW5nIEF1dGhvcml0eTEhqsGSIb3DQEJARYSc3VwcG9y
.....
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
```

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



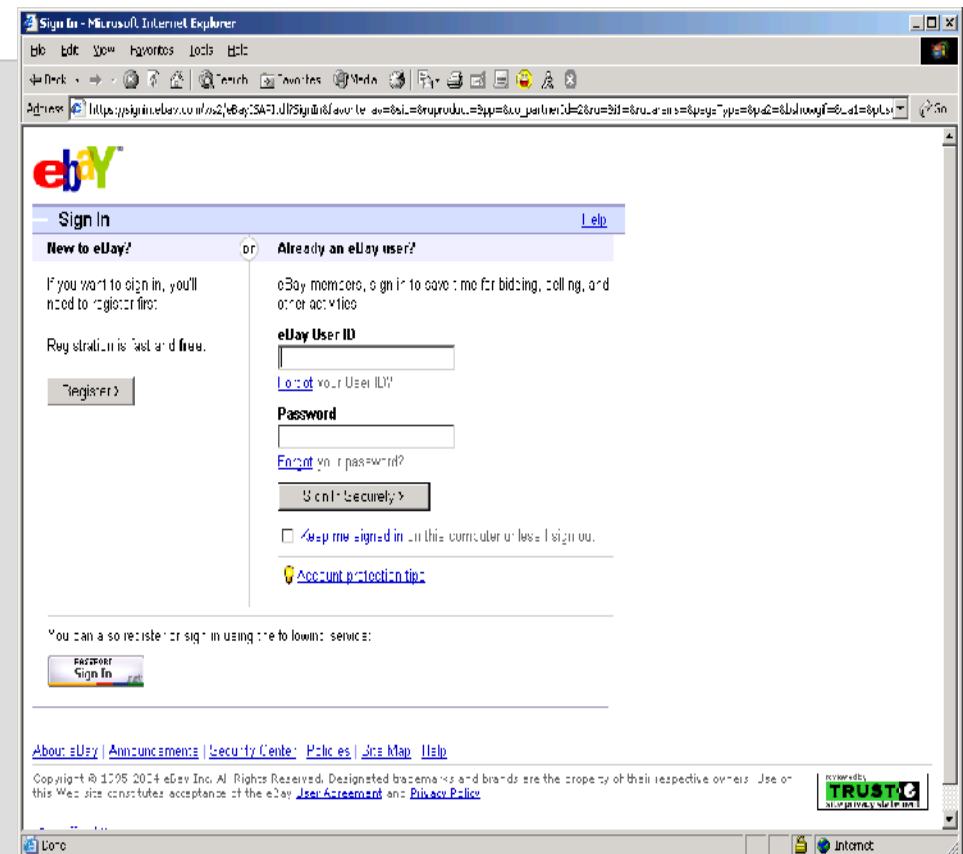
CAcert is supported

- 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!

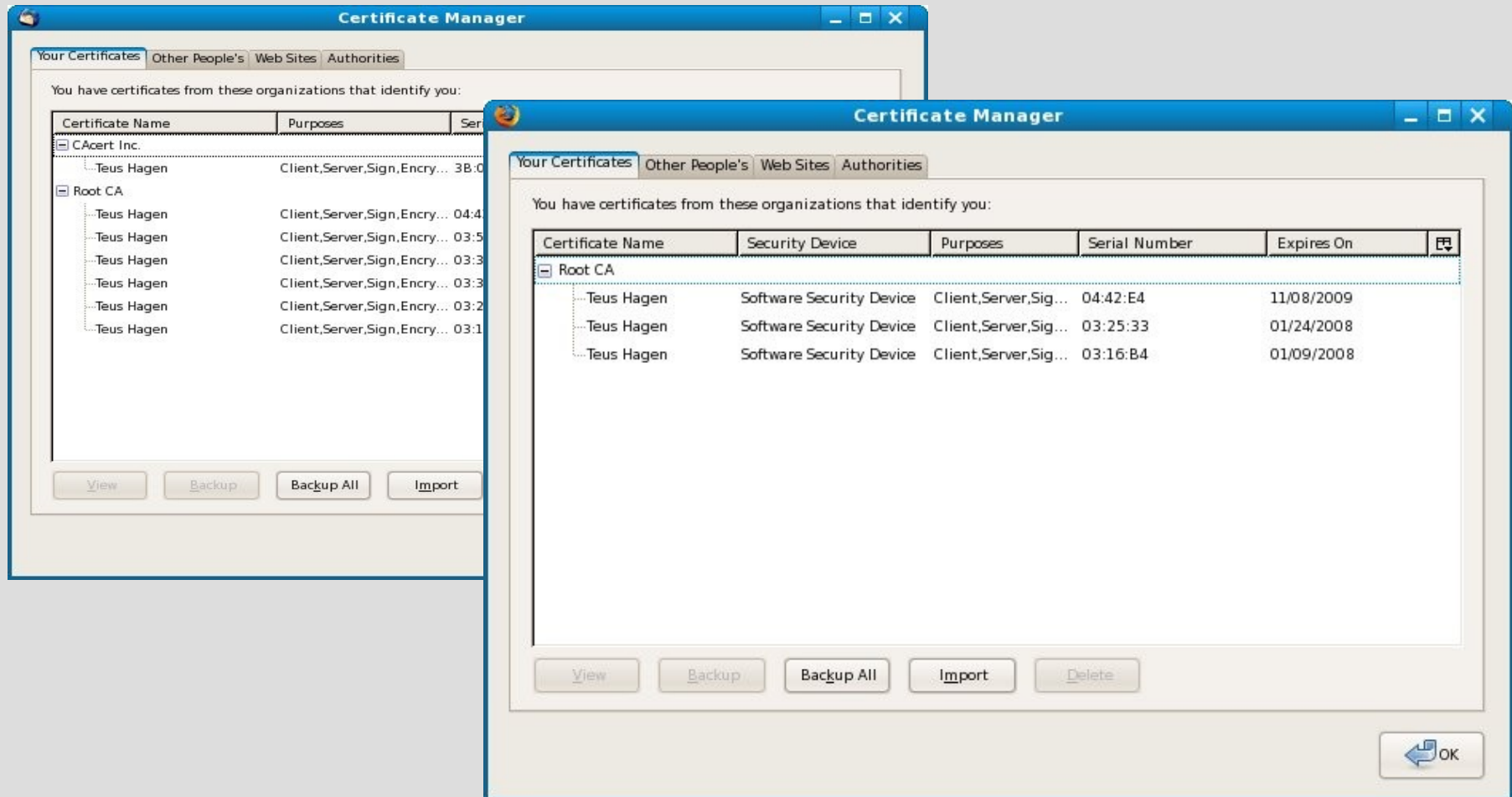


Use it for:

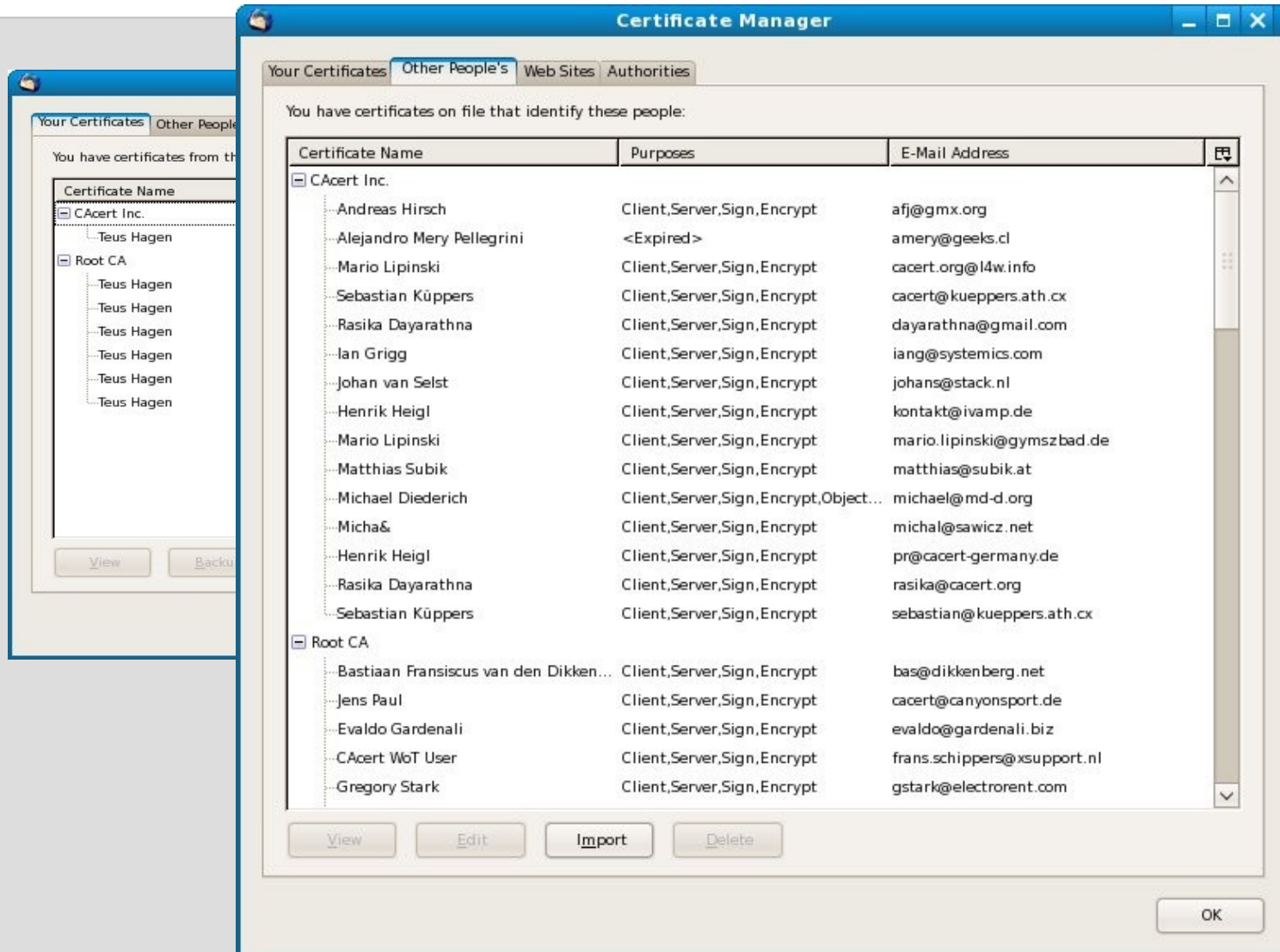
- to login
 - how broken is email address/password pair?
 - Better (single sign on) use CAcert cert login!
- to sign documents, really?
- to identify yourself?
- to secure data transports



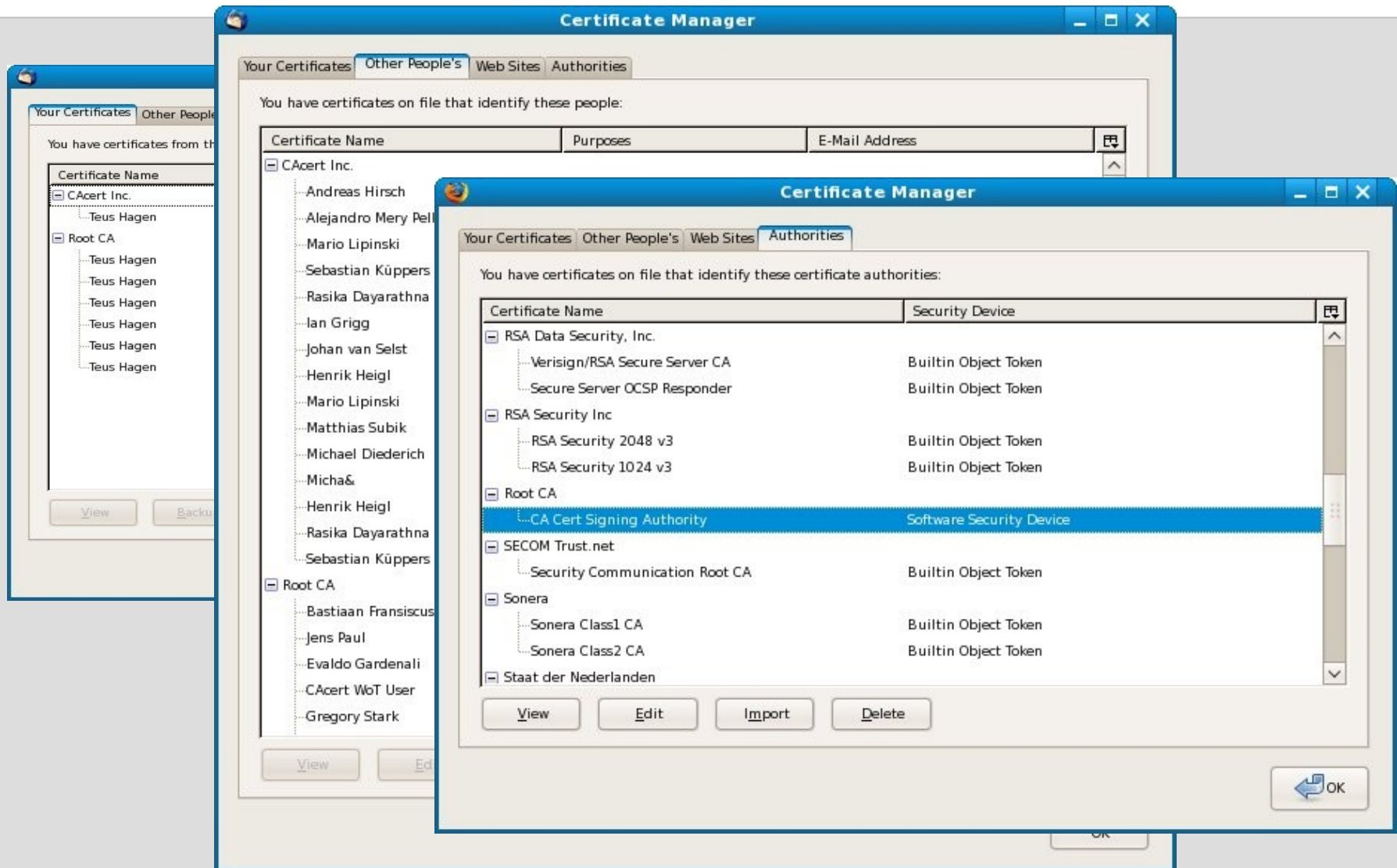
Thunderbird certificate usage



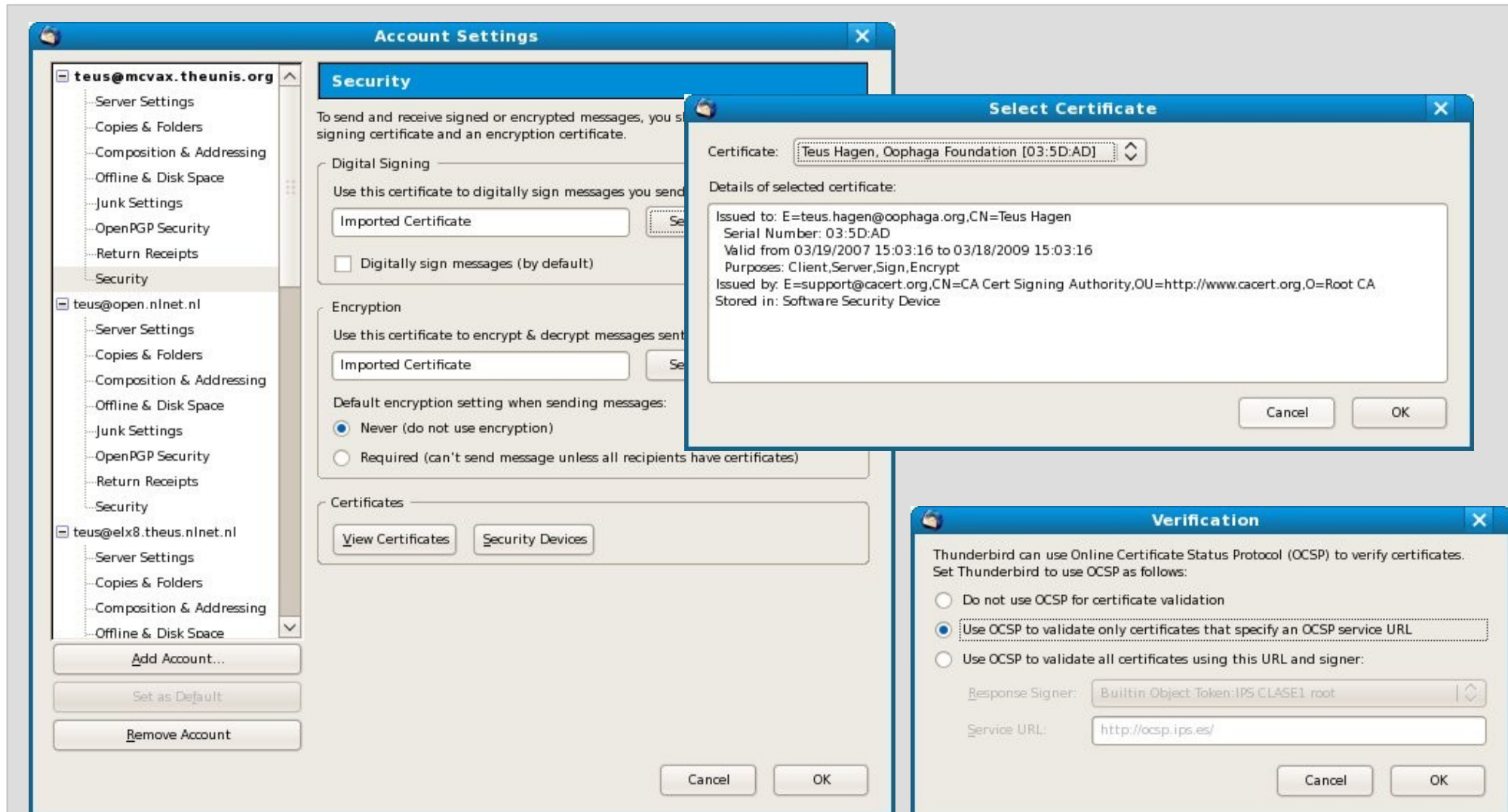
Thunderbird certificate usage



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. The **Digital Signing** section includes a dropdown menu set to `Imported Certificate` and a checkbox for `Digitally sign messages (by default)`. The **Encryption** section includes a dropdown menu set to `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:

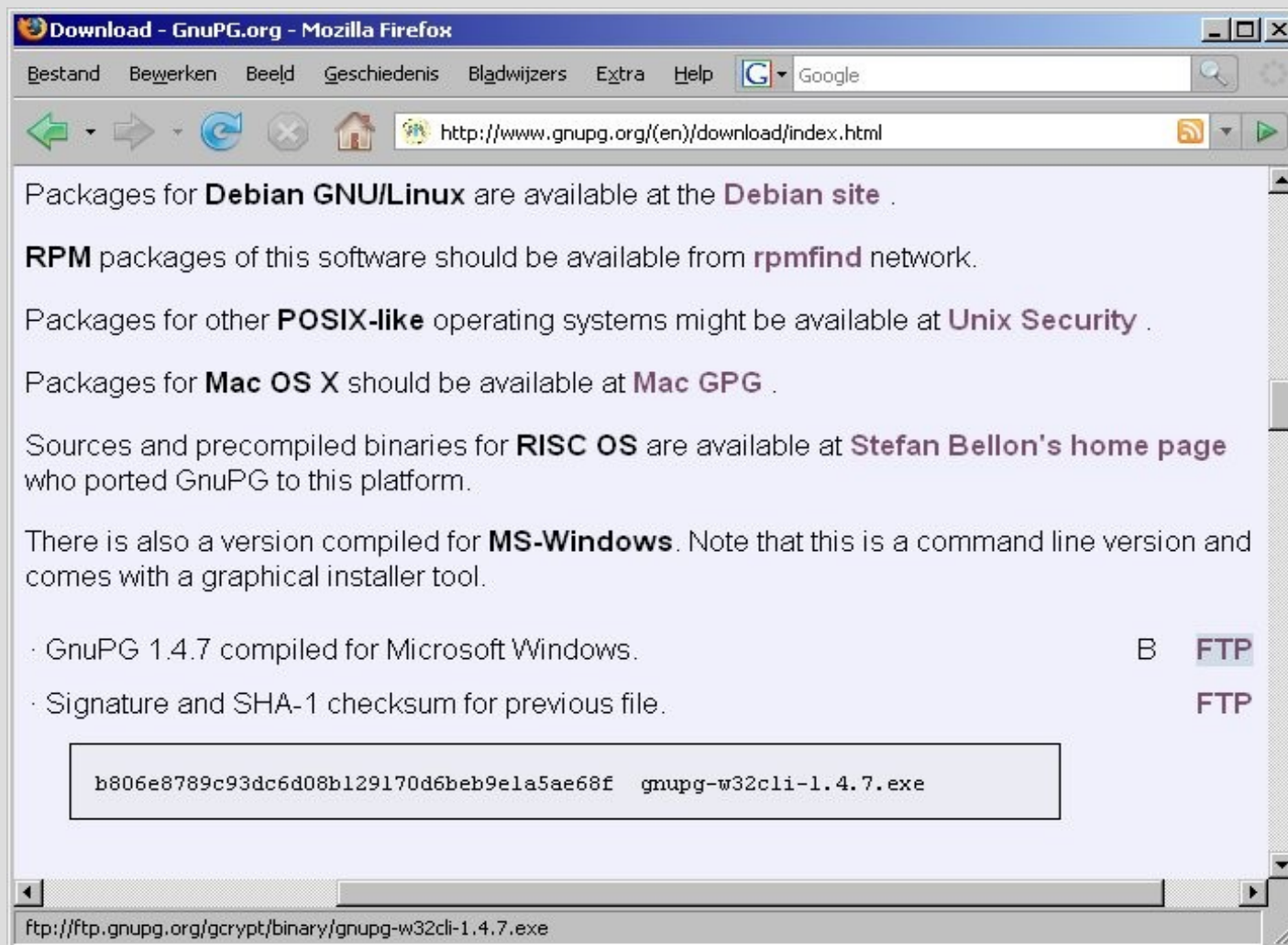
```
Issued to: E=teus.hagen@oophaga.org,CN=Teus Hagen
Serial Number: 03:5D:AD
Valid from 03/19/2007 15:03:16 to 03/18/2009 15:03:16
Purposes: Client,Server,Sign,Encrypt
Issued by: E=support@cacert.org,CN=CA Cert Signing Authority,OU=http://www.cacert.org,O=Root CA
Stored in: Software Security Device
```
- 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

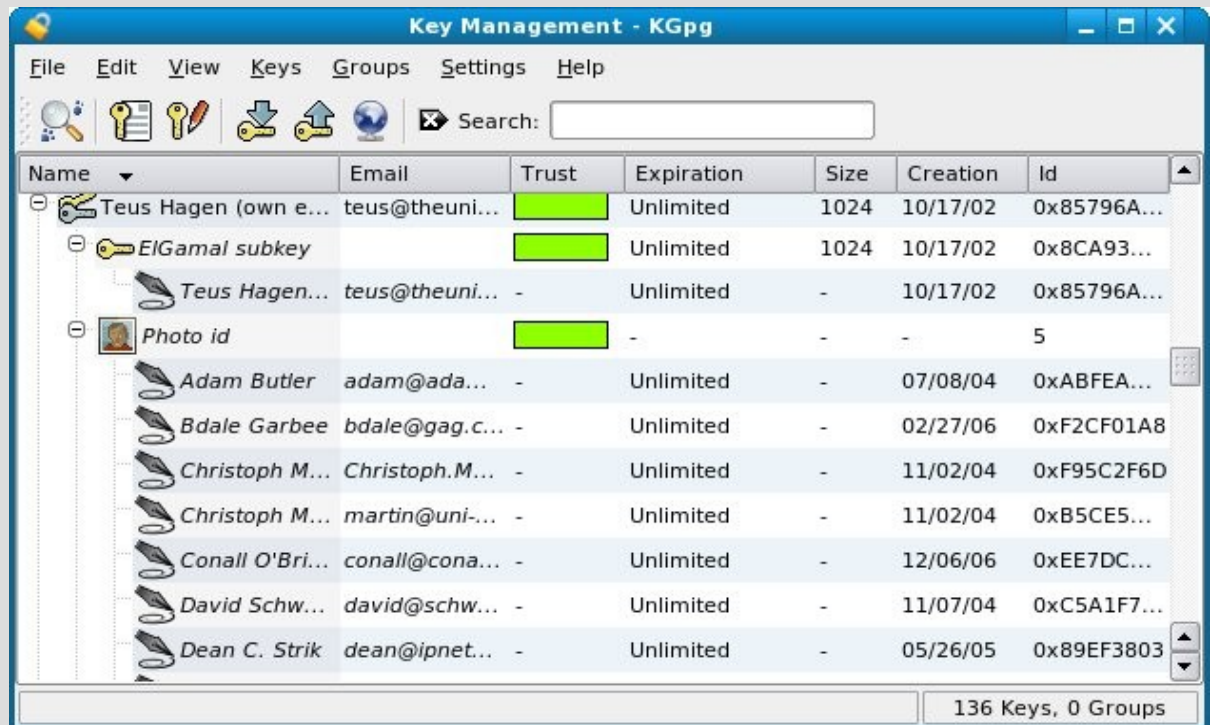


PGP/GPG install



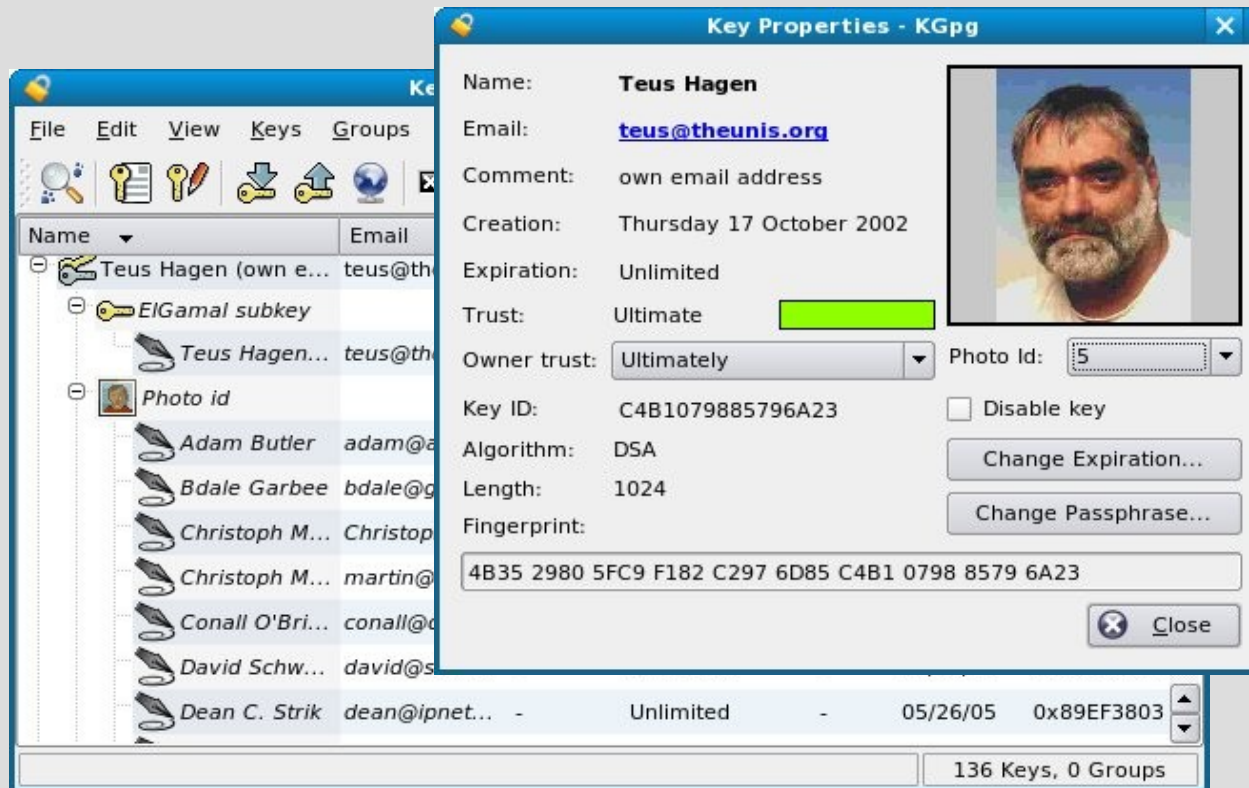
GNUPG use

- 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

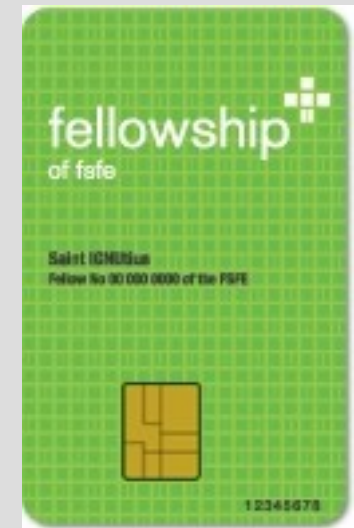
PGP & X.509 Certificate comments

- 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



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!



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