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
  - X.509 digital certificates
  - CAcert community
  - CAcert services
  - the HowTo
  - why should I?
  - me too!

On the internet everybody is a dog

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

trust is not identification!

- who are they?
- trust worthy?

- use digital signatures for identification
- Web of Trust
  - GPG
  - X.509 certificates

Identification (the email from Nigeria)

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

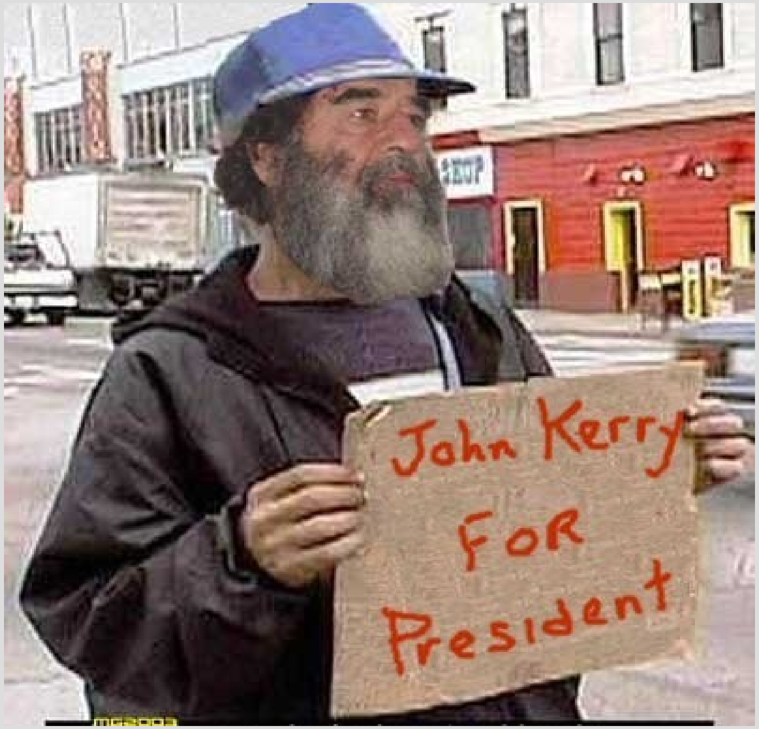
Your passport is it you?

- 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, 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.

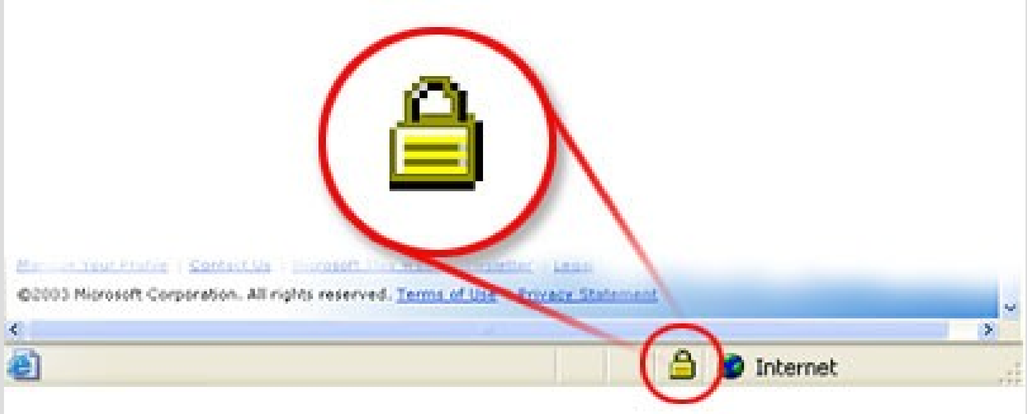
Secure digital content

- documents
- images
- software code
- stamping



Secure data transfer

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



Manage Your Profile | Contact Us | Microsoft [illegible] Newsletter | Legal

©2003 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement

Certificates are official

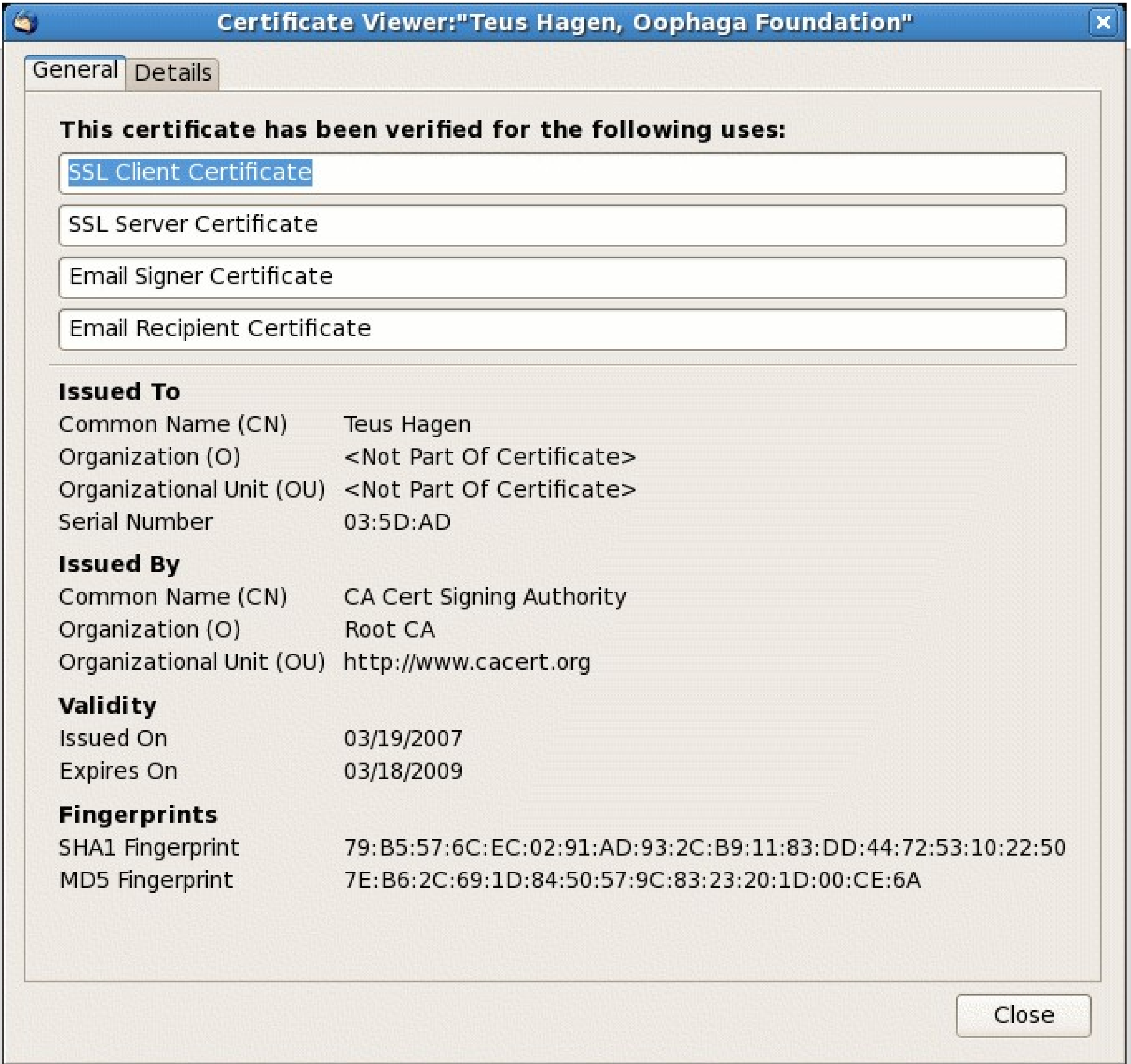
- Pres. Clinton signed

  S 761 - The Millenium Digital

  Commerce Act June 30,2000.

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

What is a digital certificate?



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

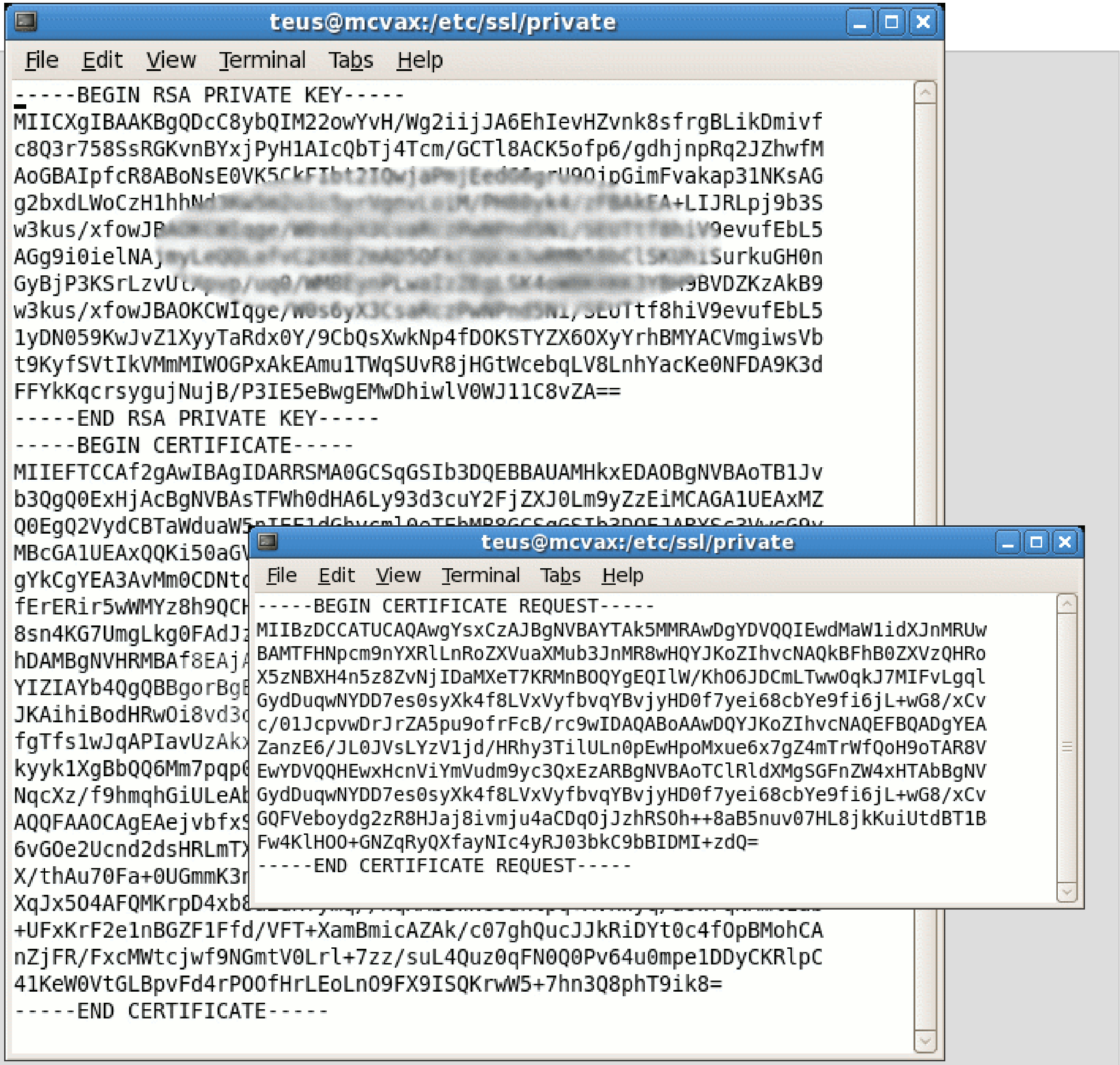
Issued On	03/19/2007
Expires On	03/18/2009

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

How does a cert look like?

- mcvax.theunis.org.pem
- mcvax.theunis.org.key
- mcvax.theunis.org.csr
- mcvax.theunis.org.crt
- mcvax.theunis.org.p12

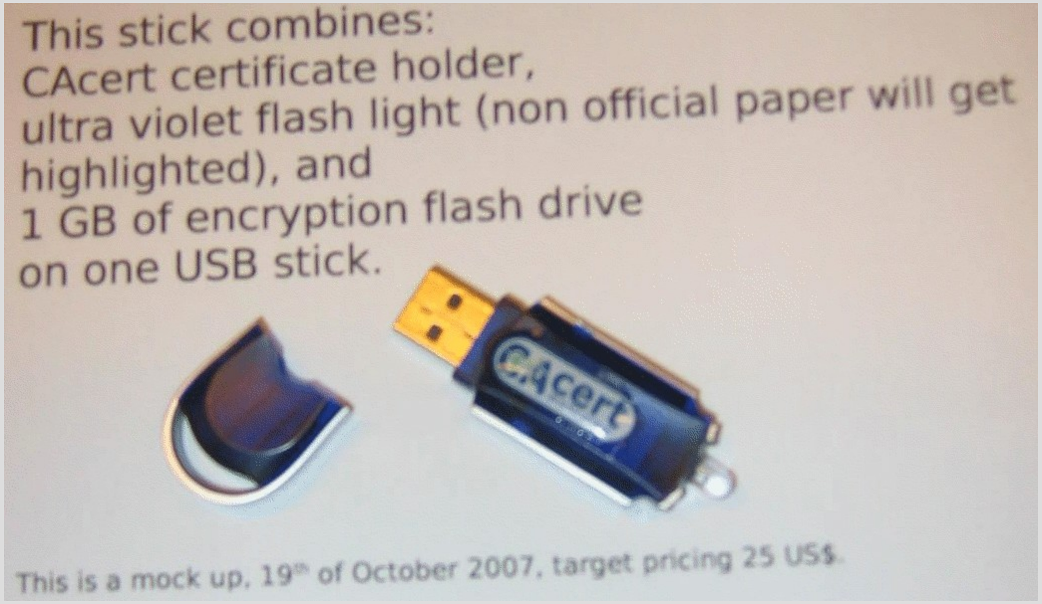

teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help
teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDcC8ybQIM22owYvH/Wg2iijJA6EhIevHZvnk8sfrgBLikDmivf
c8Q3r758SsRGKvnBYxjPyH1AIcQbTj4Tcm/GCTl8ACK5ofp6/gdhjnpRq2JZhwfM
AoGBAIpfcR8ABoNsE0VK5 [redacted] ipGimFvakap31NKsAG
g2bxdLWoCzH1hhN A+LIJRLpj9b3S
w3kus/xfowJB 9evufEbL5
AGg9i0ielNAj SurkuGH0n
GyBjP3KSrLzvUt 9BVDZKzAkB9
w3kus/xfowJBAOKCWIqge/ tf8hiV9evufEbL5
1yDN059KwJvZ1XyyTaRdx0Y/9CbQsXwkNp4fDOKSTYZX6OXyYrhBMYACVmgiwsVb
t9KyfSVtIkVMmMIWOGPxAkEAmu1TWqSUvR8jHGtWcebqLV8LnhYacKe0NFDA9K3d
FFYkKqcrsygujNujB/P3IE5eBwgEMwDhiwlV0WJ11C8vZA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEFTCCAf2gAwIBAgIDARRSMA0GCSqGSIb3DQEBBAUAMHkxEDAOBgNVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHA6Ly93d3cuY2FjZXJ0Lm9yZzEiMCAGA1UEAxMZ
Q0EgQ2VydCBTaWduaW5
MBcGA1UEAxQQKi50aGV
gYkCgYEA3AvMm0CDNtc
fErERir5wWMYz8h9QCH
8sn4KG7UmgLkg0FAdJz
hDAMBgNVHRMBAf8EAjA
YIZIAYb4QgQBBgorBgE
JKAihiBodHRwOi8vd3c
fgTfs1wJqAPIavUzAkx
kyyk1XgBbQQ6Mm7pqp0
NqcXz/f9hmqhGiULeAb
AQQFAAOCAgEAejvbfx9
6vGOe2Ucnd2dsHRLmTX
X/thAu70Fa+0UGmmK3r
XqJx5O4AFQMKrpD4xb8
+UFxKrF2e1nBGZF1Ffd/VFT+XamBmicAZAk/c07ghQucJJkRiDYt0c4fOpBMohCA
nZjFR/FxcMWtcjwf9NGmtV0Lrl+7zz/suL4Quz0qFN0Q0Pv64u0mpe1DDyCKRlpC
41KeW0VtGLBpvFd4rPOOfHrLEoLnO9FX9ISQKrwW5+7hn3Q8phT9ik8=
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwgYsxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdMaW1idXJnMRUw
BAMTFHNpcm9nYXRlLnRoZXVuaXMub3JnMR8wHQYJKoZIhvcNAQkBFhB0ZXVzQHRo
X5zNBXH4n5z8ZvNjIDaMXeT7KRMnBOQYgEQIlW/KhO6JDCmLTwwOqkJ7MIFvLgql
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
c/01JcpvwDrJrZA5pu9ofrFcB/rc9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
ZanzE6/JL0JVsLYzV1jd/HRhy3TilULn0pEwHpoMxue6x7gZ4mTrWfQoH9oTAR8V
EwYDVQQHEwxHcnViYmVudm9yc3QxEzARBgNVBAoTClRldXMgSGFnZW4xHTAbBgNV
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
GQFVeboydg2zR8HJaj8ivmju4aCDqOjJzhRSOh++8aB5nuv07HL8jkKuiUtdBT1B
Fw4KlHOO+GNZqRyQXfayNIc4yRJ03bkC9bBIDMI+zdQ=
-----END CERTIFICATE REQUEST-----
```

Client certificate how to?

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

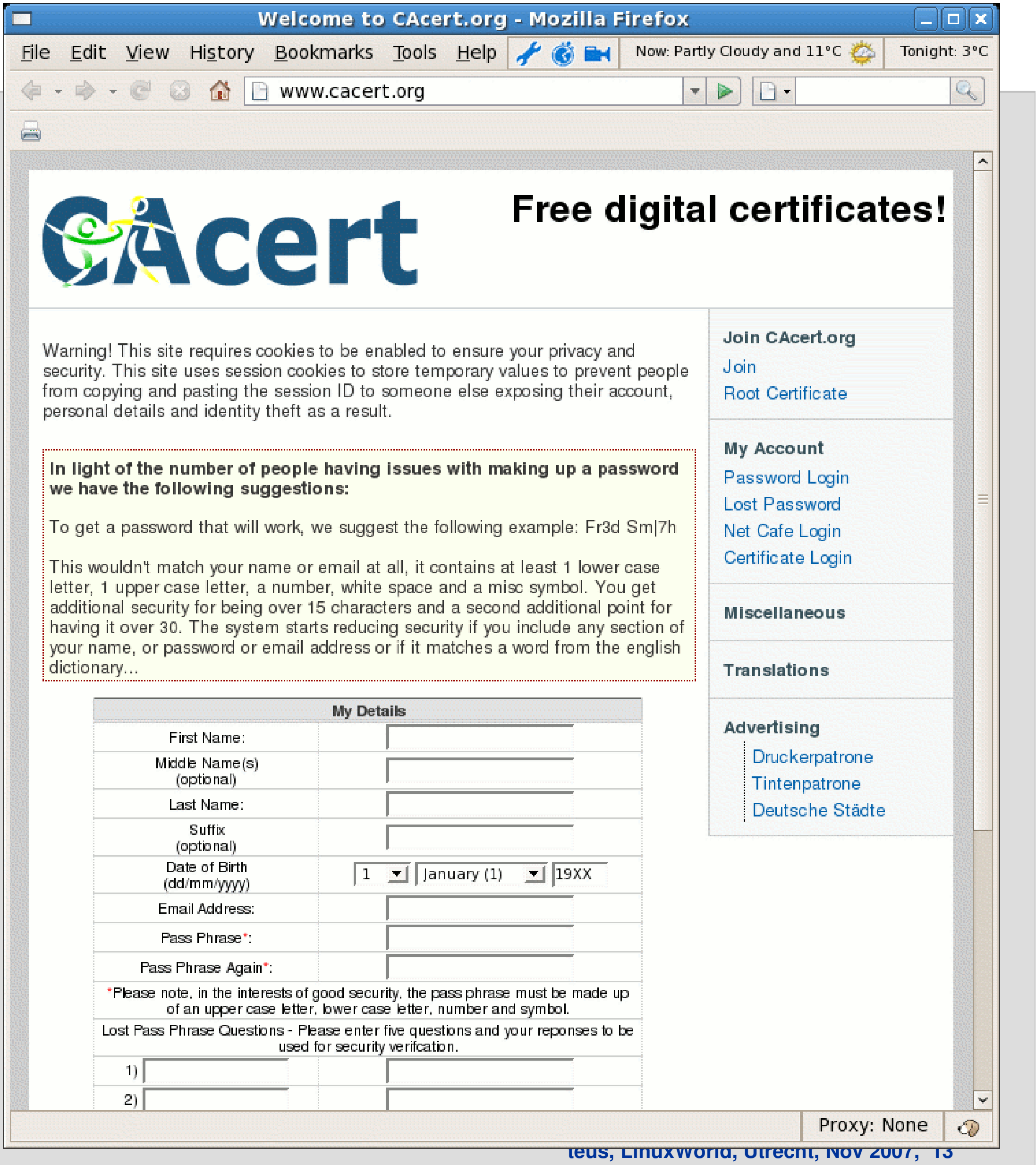


This stick combines:
CAcert certificate holder,
ultra violet flash light (non official paper will get highlighted), and
1 GB of encryption flash drive
on one USB stick.

This is a mock up, 19th of October 2007, target pricing 25 US$.

CAcert HowTo

- join/register
- create
  - a CAcert account



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
Proxy: None

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:	
Middle Name(s) (optional)	
Last Name:	
Suffix (optional)	
Date of Birth (dd/mm/yyyy)	1 ▾ January (1) ▾ 19XX
Email Address:	
Pass Phrase*:	
Pass Phrase Again*:	

*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 reponses to be used for security verifcation.

1)

2)

Join CAcert.org
- Join
- Root Certificate

My Account
- Password Login
- Lost Password
- Net Cafe Login
- Certificate Login

Miscellaneous

Translations

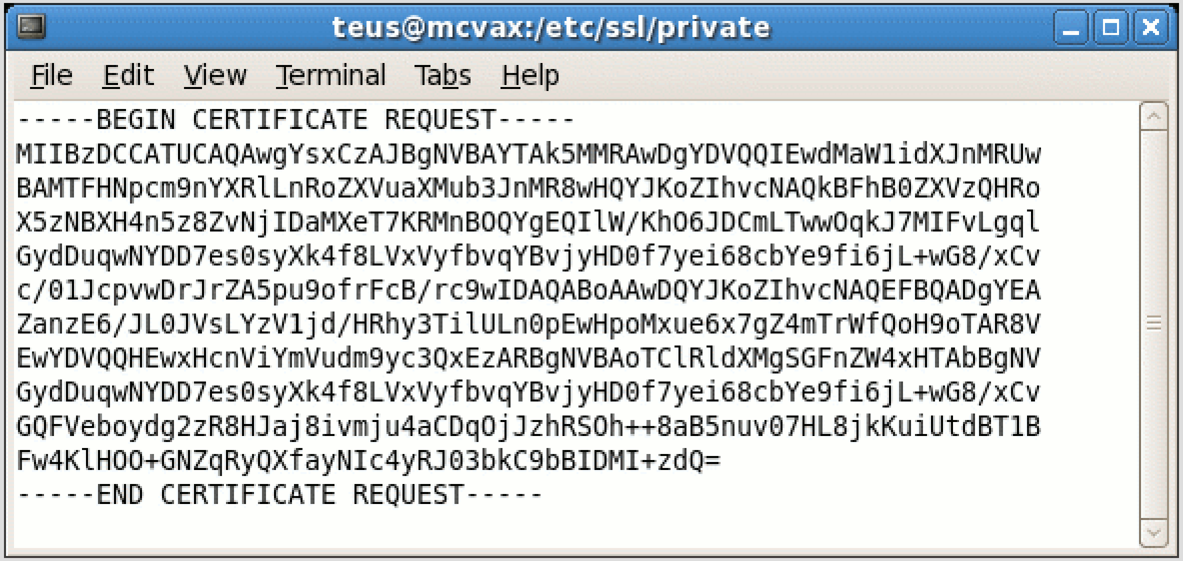
Advertising
- Druckerpatrone
- Tintenpatrone
- Deutsche Städte

CAcert HowTo

- 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 HowTo

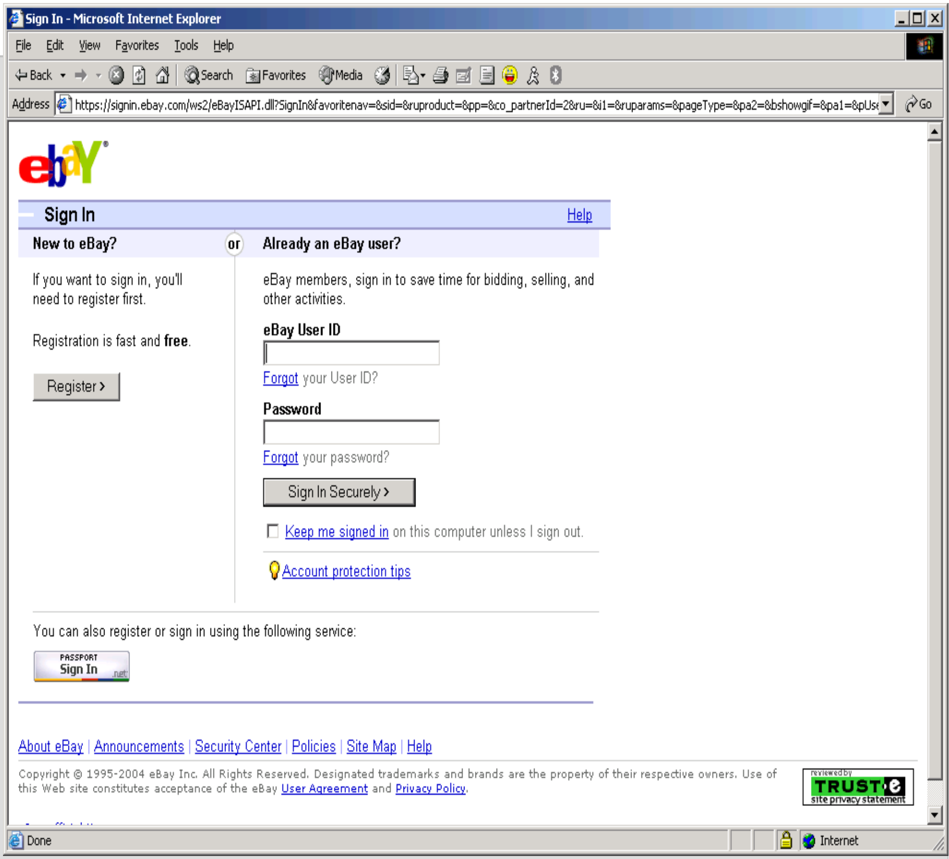
- create
  - Private key
  - Cert Sign Req
- have it signed
- import
  - Private Key
  - Public Key: the certificate


teus@mcvax:/etc/ssl/private
File Edit View Terminal Tabs Help

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwgYsxCzAJBgNVBAYTAk5MMRAwDgYDVQQIEwdMaW1idXJnMRUw
BAMTFHNpcm9nYXRlLnRoZXVuaXMub3JnMR8wHQYJKoZIhvcNAQkBFhB0ZXVzQHRo
X5zNBXH4n5z8ZvNjIDaMXeT7KRMnBOQYgEQIlW/KhO6JDCmLTwwOqkJ7MIFvLgql
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
c/01JcpvwDrJrZA5pu9ofrFcB/rc9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
ZanzE6/JL0JVsLYzV1jd/HRhy3TilULn0pEwHpoMxue6x7gZ4mTrWfQoH9oTAR8V
EwYDVQQHEwxHcnViYmVudm9yc3QxEzARBgNVBAoTClRldXMgSGFnZW4xHTAbBgNV
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
GQFVeboydg2zR8HJaj8ivmju4aCDqOjJzhRSOh++8aB5nuv07HL8jkKuiUtdBT1B
Fw4KlHOO+GNZqRyQXfayNIc4yRJ03bkC9bBIDMI+zdQ=
-----END CERTIFICATE REQUEST-----
```

Use it

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



Sign In - Microsoft Internet Explorer

https://signin.ebay.com/ws2/eBayISAPI.dll?SignIn&favoritenav=&sid=&ruproduct=&pp=&co_partnerId=2&ru=&i1=&ruparams=&pageType=&pa2=&bshowgif=&pa1=&pUs

Sign In Help

New to eBay? or Already an eBay user?

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

☐ Keep me signed in on this computer unless I sign out.

Account protection tips

You can also register or sign in using the following service:

About eBay | Announcements | Security Center | Policies | Site Map | Help

Copyright © 1995-2004 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

CAcert is community work

- >10.000 assurers
- translations into 30 languages
- > 100.000 certs in use
- >100 on the help desk: 7 * 24 email support
- World Wide
- and CAcert certs are **free**!

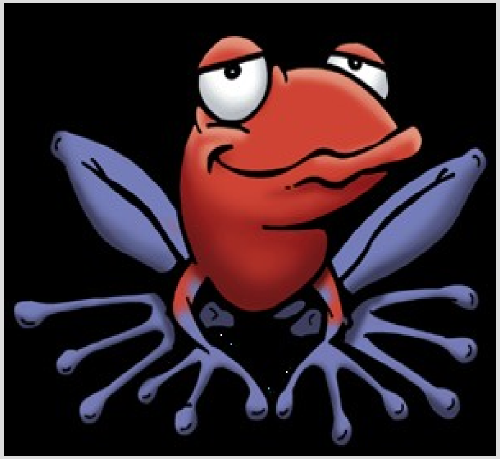
CAcert is currently

- 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

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!



Open Architecture Network bit TUNIX sonance artistic.network

CAcert is you!

TIP

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

Thanks, some materials are used from: Wren Hunt, Jens Paul