TIP

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

on the internet nobody knows you are a dog

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

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

teus hagen

content

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

http://svn.cacert.org/CAcert/PR/Presentations/CAcertPresentationNLLGG

What is a digital certificate?

- X.509 standard

- two parts:

  - private key part

  - public key part: "X.509 certificate"

    maybe accepted as "this is from you": signed by ?

- X.509 and PGP

certificates are official

- pres. Clinton signed

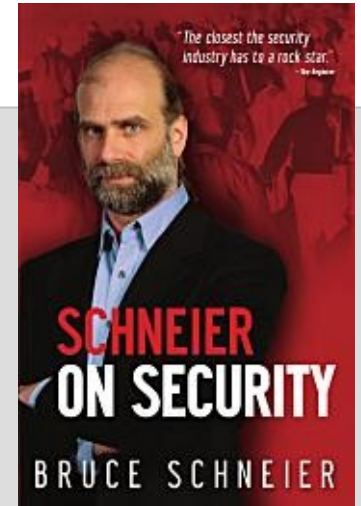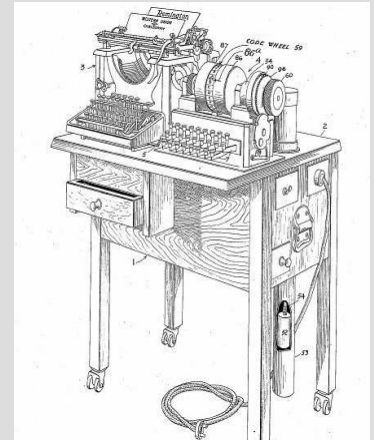 S 761 - The Millenium Digital

  Commerce Act June 30,2000.

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

encryption

Bruce Schneier:

"Any person can invent a security system

so clever

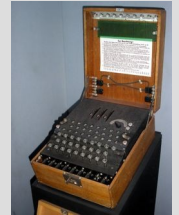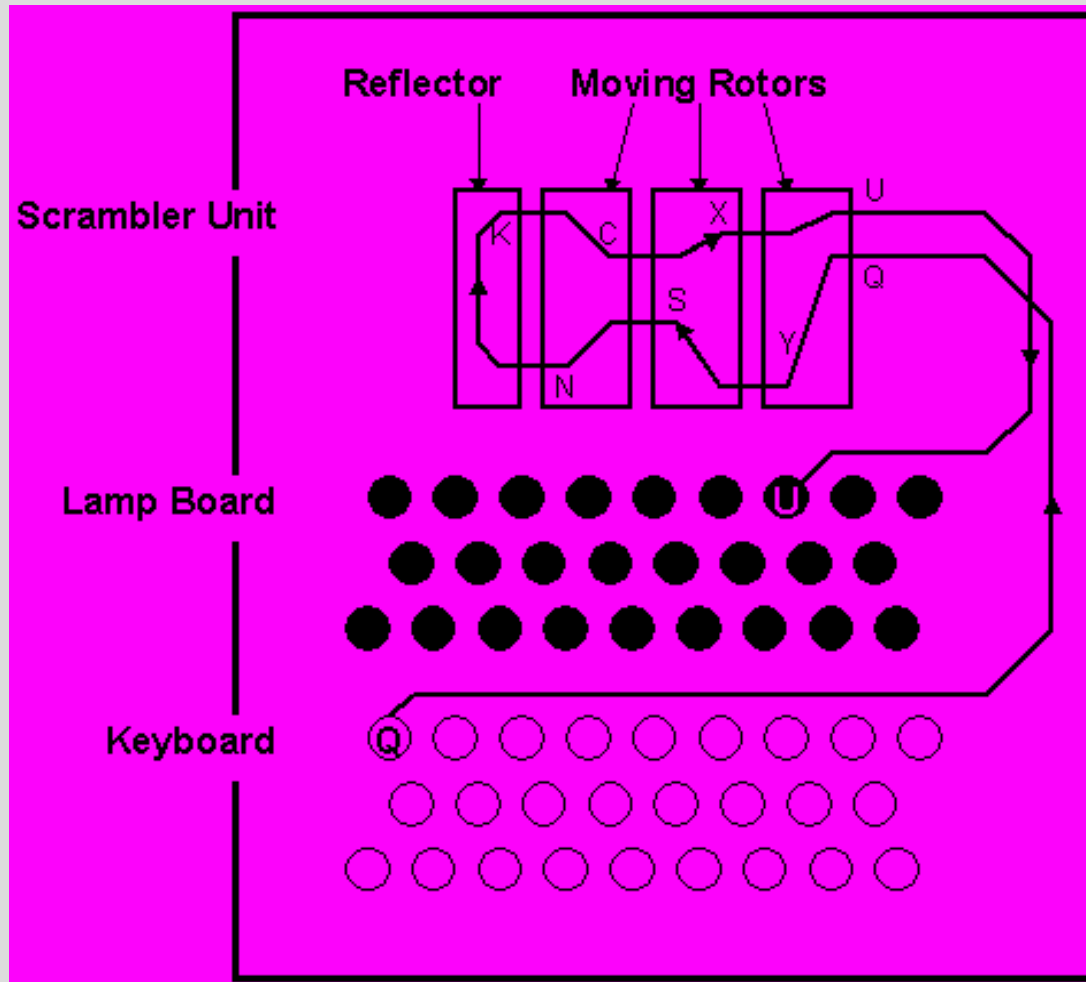*that she or he can't think of how to break it"*

encryption

- Herbern

- Enigma

  - Germany second world war

  - the mechanism
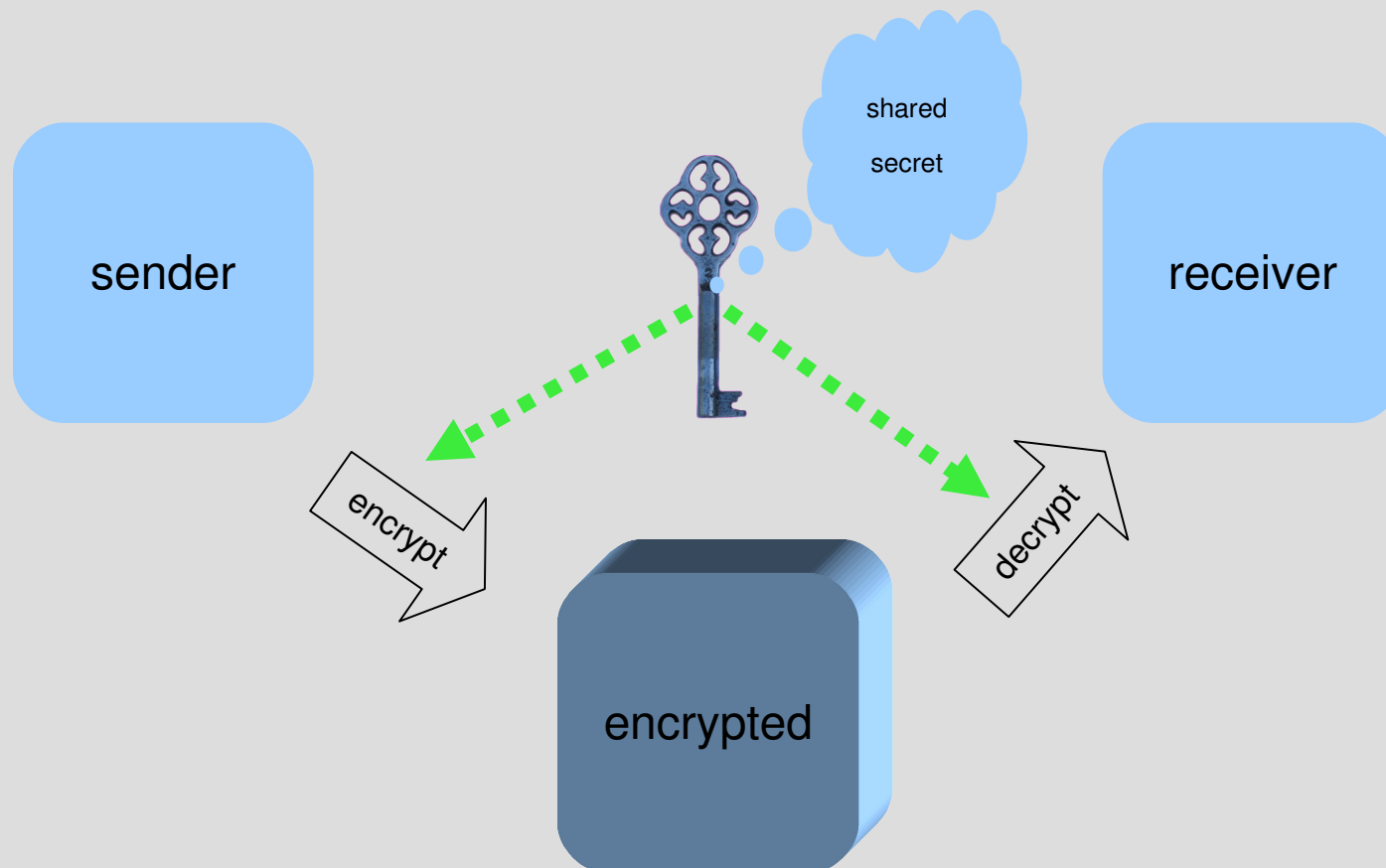
  - hacked, of course

Enigma technology

RFID chip hacked Dec 2007

- Mifare classic RFID chip of NXP (Philips)

- Karsten Nohl and Henryk Plötz

- Hacked

  - 48 bits but only 16 bits (only 64.000 variations) used

  - not random (dependent on time contact)

- implications:

  - car keys

  - public transportation cards

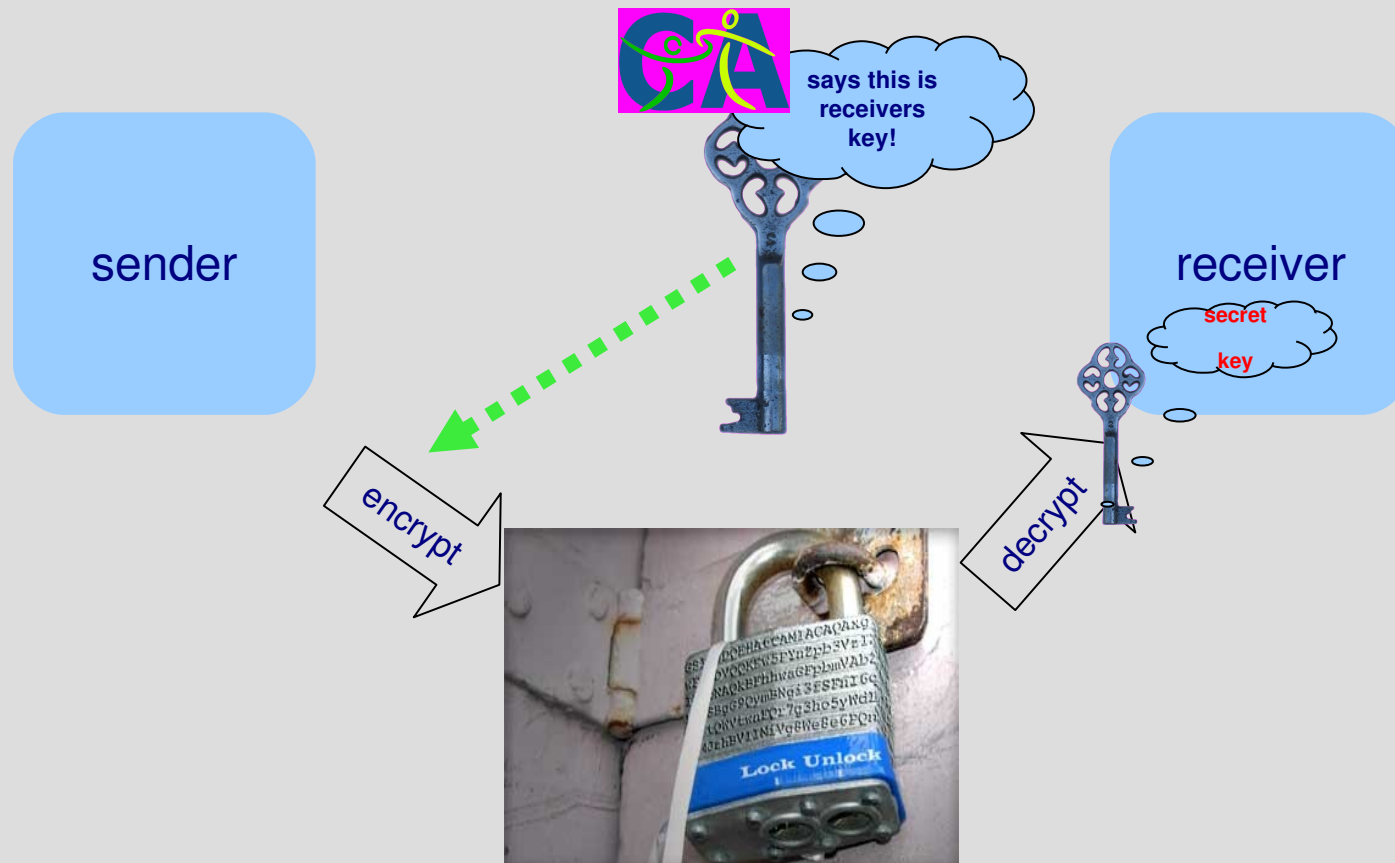 - electronic tickets eg FIFA World Cub tickets

encryption key types
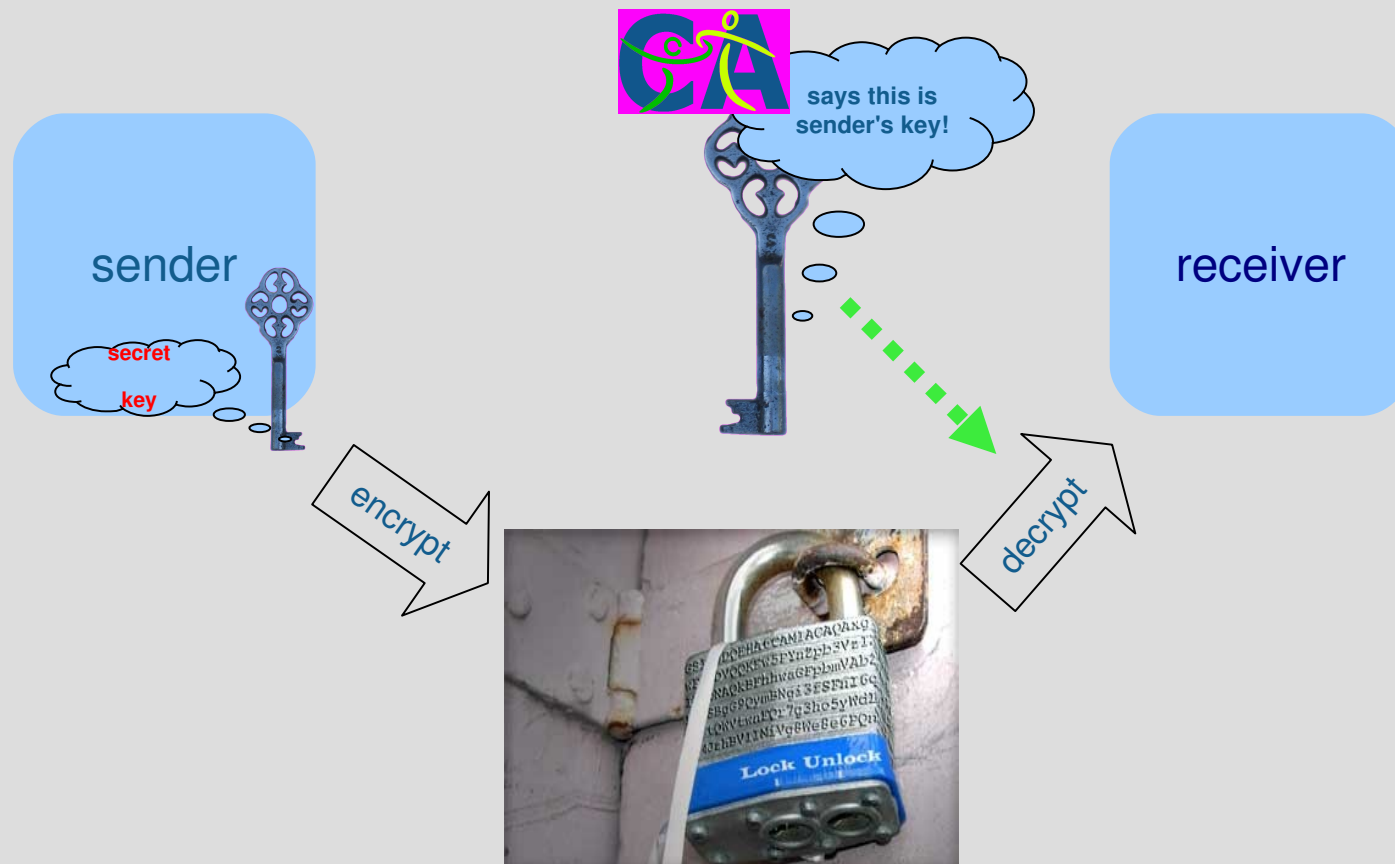
symmetric key encryption

sender

shared
secret

receiver

encrypt

decrypt

encrypted

asymmetric key encryption

that message can only be read by him

says this is receivers key!

sender

receiver

secret key

encrypt

decrypt

Lock Unlock

asymmetric key encryption

that message can only come from him!

says this is sender's key!

sender

secret key

receiver

encrypt

decrypt
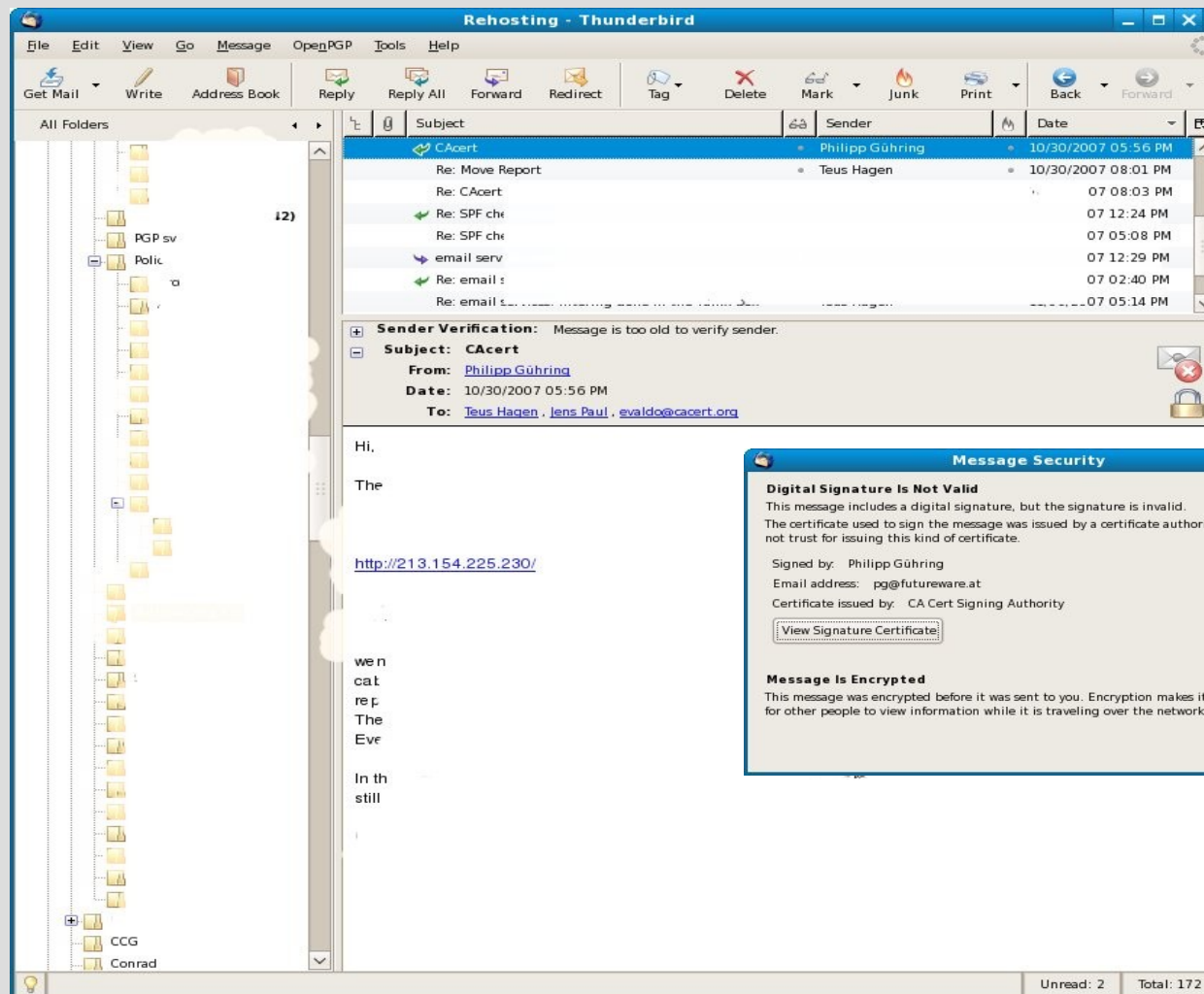
how do "signatures" work
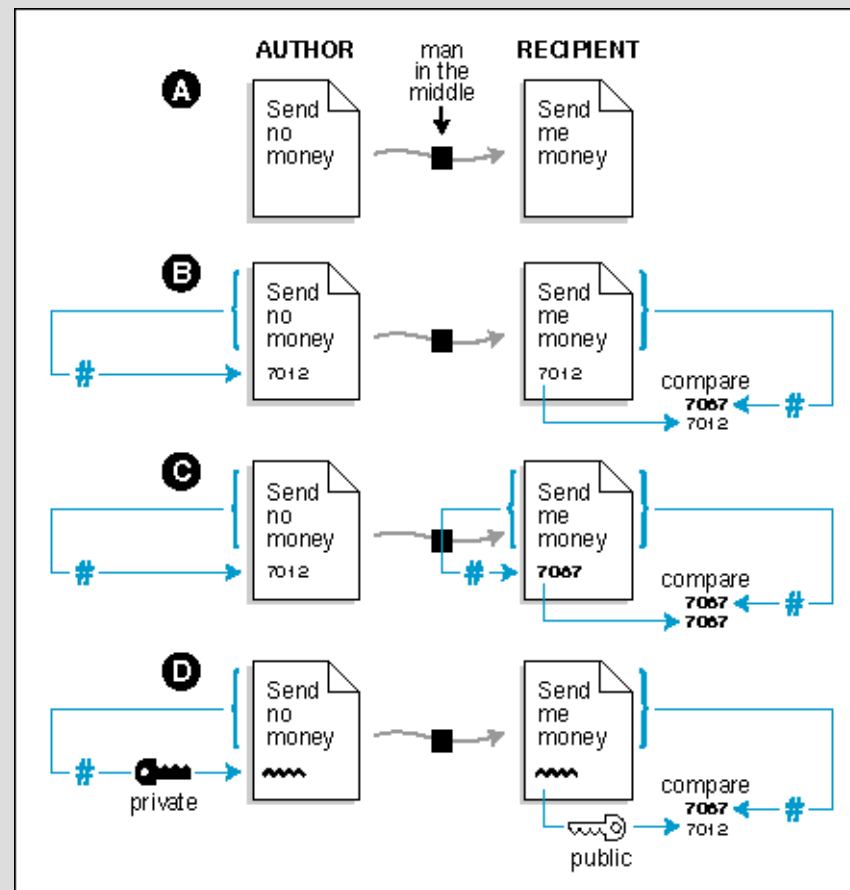
Email and signatures
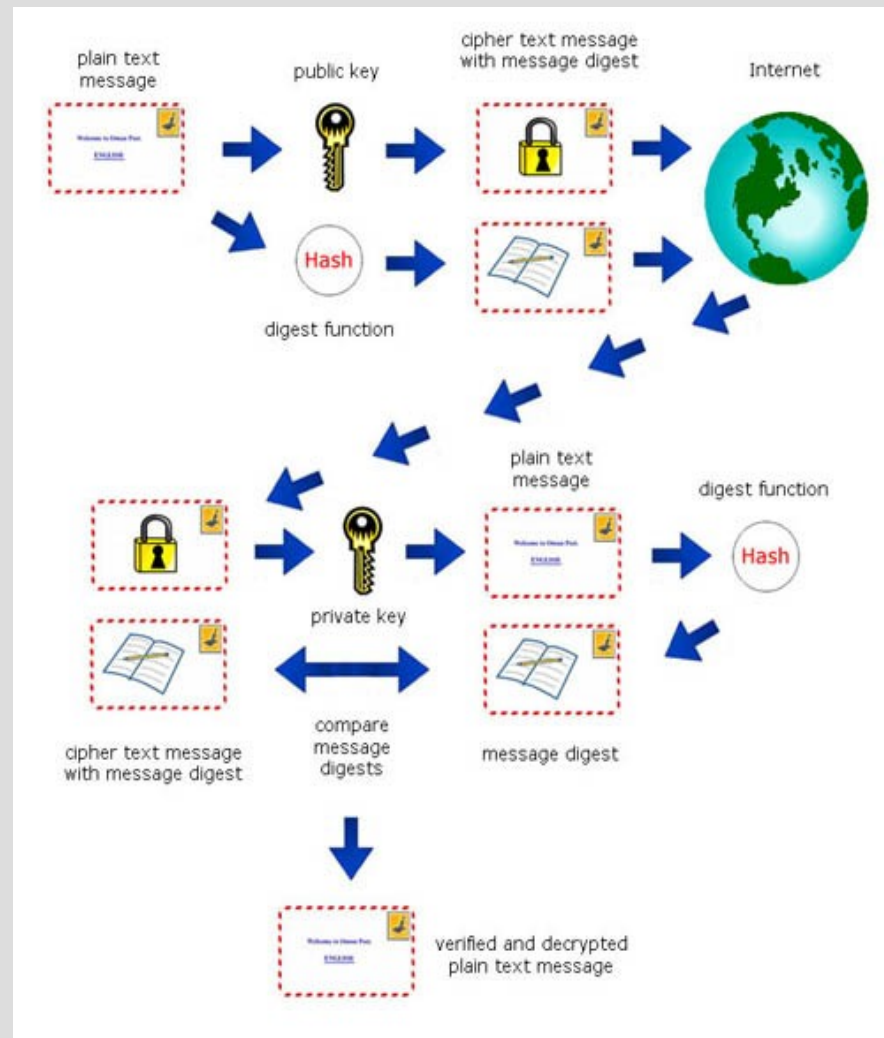
the practice: encrypted and signed email

What can you do with it?

- encrypt & decrypt

- identify data: it is coming from her!

    identity for trade (name, birth date, email address)

- claim

e.g.

  - encrypt data: email, file, internet communication

  - sign documents: eg code signing, signatures

  - time stamping

secure data transfer

- secure Socket Layer

    SSL

- Secure Hypertext Transfer Protocol
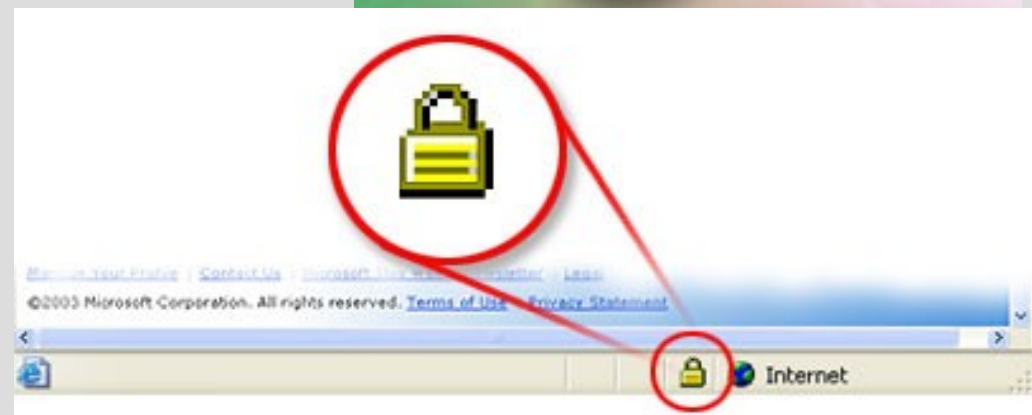
    https

- Virtual Private Network

    VPN

What is a digital certificate?

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

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$.
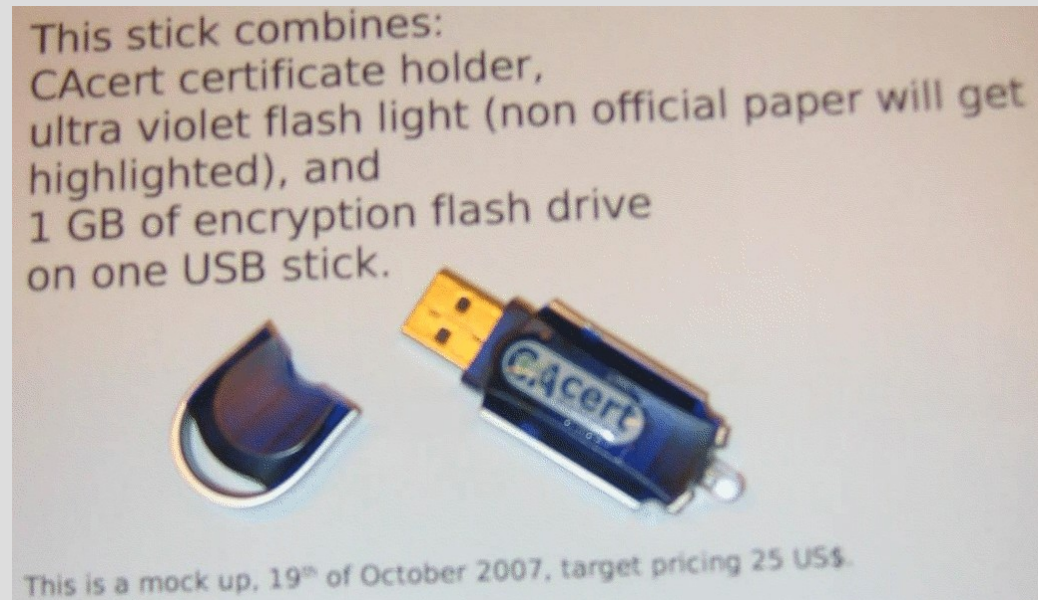
How does a certificate look like?

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

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
BAMTFHNpcm9nYXRlLnRoZXVuaXub3JnMR8wHQYJKoZIhvcNAQkBFhB0ZXVzQHRo
X5zNBXH4n5z8ZvNjIDaMXeT7KRMnBOQYgEQIlW/KhO6JDCmLTww0qkJ7MIFvLgql
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
c/01JcpvwDrJrZA5pu9ofrFcB/rc9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
ZanzE6/JL0JVsLYzV1jd/HRhy3TilULn0pEwHpoMxue6x7gZ4mTrWfQoH9oTAR8V
EwYDVQQHEwxHcnViYmVudm9yc3QxEzARBgNVBAoTClRldXMgSGFnZW4xHTAbBgNV
GydDuqwNYDD7es0syXk4f8LVxVyfbvqYBvjyHD0f7yei68cbYe9fi6jL+wG8/xCv
GQFVeboydg2zR8HJaj8ivmju4aCDqOjJzhRSOh++8aB5nuv07HL8jkKuiUtdBT1B
Fw4KlHOO+GNZqRyQXfayNIc4yRJ03bkC9bBIDMI+zdQ=
-----END CERTIFICATE REQUEST-----
```
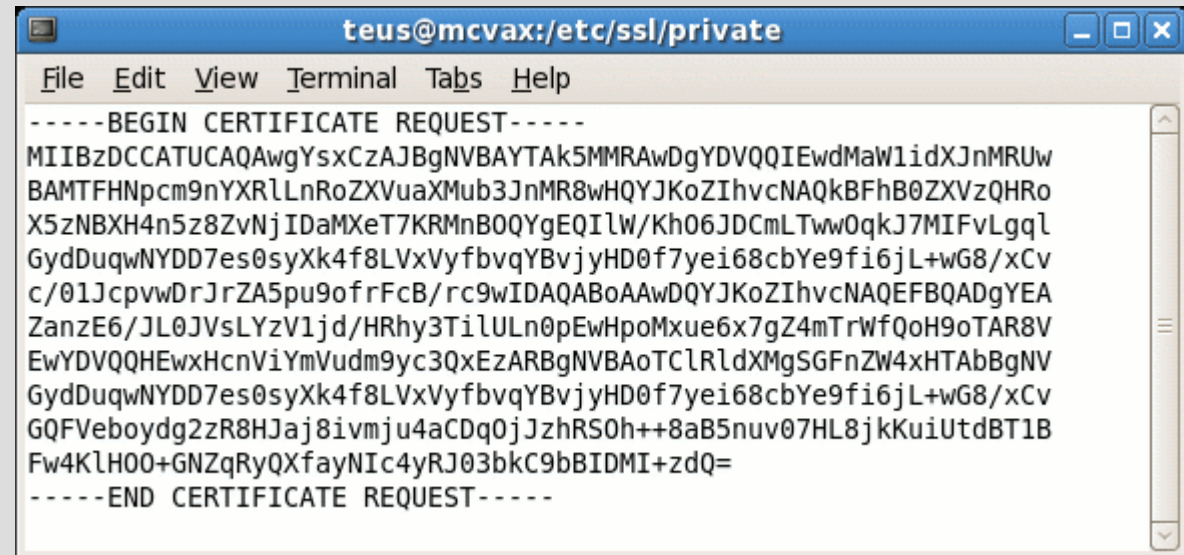
How-To create private and public certificate

get a key manager

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-----
MIICijCCAXICAQAwRTELMAkGA1UEBhMCTkwxITAfBgkqhkiG9w0BCQEWEnRldXNA
bXlfZG9tYWluLm9yZzETMBEGA1UEAxMKVGV1cyBIYWdlbjCCASIwDQYJKoZIhvcN
...
aslwP+uZP9MwdFSwOEL8ldi860FNgLA5Skr1wwewfjtdPXRugYTXVzCn4pzpY/Fz
GS/2xpYuwaQDrz57L+YE4zakeoIuctZW9fWZZOj9
-----END NEW CERTIFICATE REQUEST-----
```

How-To use the command line   certutil

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

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

% certutil -L -a -n aospan@netup.ru -d .
-----BEGIN CERTIFICATE-----
MIIE7DCCAtSgAwIBAgIDAv+vMA0GCSqGSIb3DQEBBQUAMHkxEVBAoTB1Jv
b3QgQ0ExHjAcBgNVBAsTFWh0dHA6Ly93d3cuJ0Lm9yZzEiMCAGA1UEAxMZ
Q0EgQ2VydCBTaWduaW5nIEF1dGhvcml0eTEhqGSIb3DQEJARYSc3VwcG9y
.....
K1aTaRN4xKjsO98Z9rOqrIoKULkkjZYIbV61P6dyHnE7oVxKpQs+wdaOzp
ML/DwtGfvao7uWcM/n2vNg==
-----END CERTIFICATE----

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

  % certutil -L -d . | grep fuare

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


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

The commerce or the community track?

- certificate is linked to identification

    identification is needed for e.g. trade and liability

- identification can be done:

    ➢ via address, transfer of money -> $

    ➢ via Web of Trust and check of ID -> HR

# Identification check is critical

your passport is it really you?

Shahiba Tulaganova UK journalist:

- within 5 months on east European markets

- bought 20 EU passports, 5 other

   (UK, 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.

Certificate Authority signature

- create private key and the public key

- send public key to CA:

    Cert Signing Request (CSR)

- CA signs public key of individual:
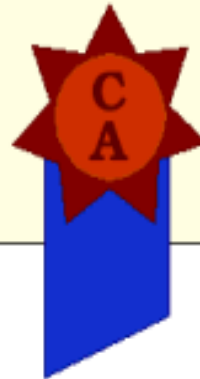
    this public key is from him!
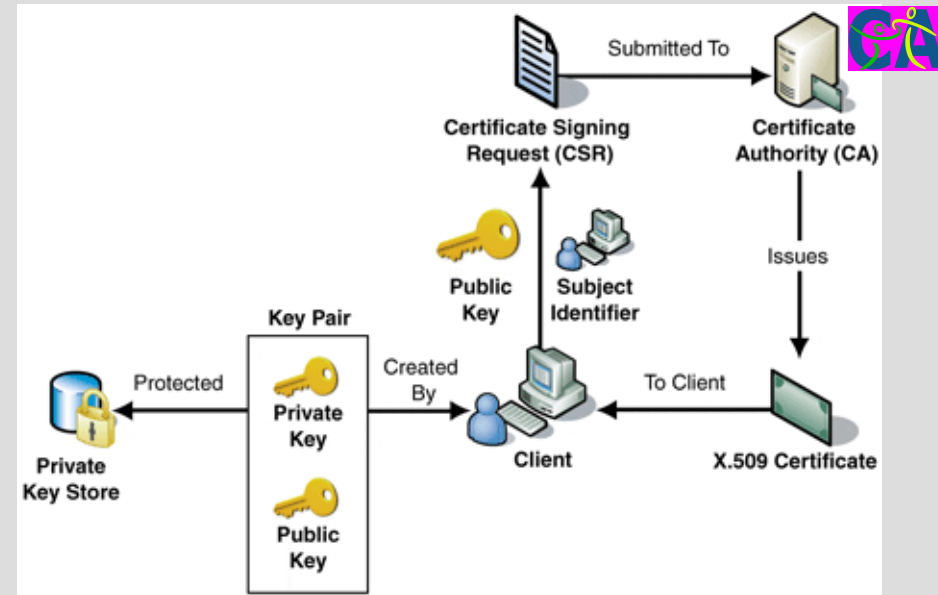
- yes the pub key comes from him!

- yes it is his signature on this email!

this is cool!

What is a CA?

I, _Certificate Authority XYZ_ , do hereby **certify** that
Borja Sotomayor is who he/she claims to be and
that his/her public key is _49E51A3EF1C_.

_Certificate_Authority_XYZ_.
CA's Signature

- Certificate Authority

- the CA Root Key is added into "your" CA-list

  On which authority?

- Signs your X.509 public certificate

Why CAcert?

- mission

    on internet allow everyone to protect their privacy

    - no discrimination

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

    - high tech, transparent

- volunteers

The implication for CAcert

- ## Open CA

  - ### full commitment for openness

  - ### non-profit

  - ### no secrecy:

    - threats

    - updated

    - software tooling used

    - hardware tooling used

    - fully transparent

The disadvantages of openess

- **funding** needed
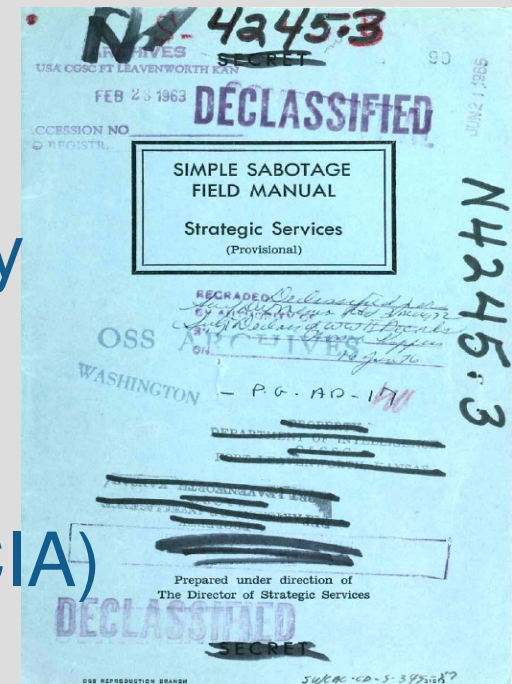
    Hardware, PR, face 2 face meetings, connectivity

- **volunteers** needed

    Short and long term, HR time is costly

- many discussions

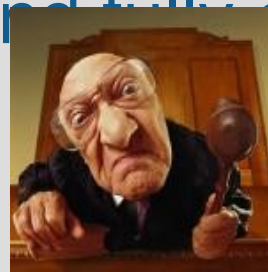   OSS Simple Sabotage Manual (US CIA)

- the sendmail phenomenon

What is CAcert?

- Community of Members, based on WoT

- **CA**cert Inc. association

  (July 2003, NSW Australia)

- legal entities:

  ✳ Not fully and fully assured Community Members

  ✳ Assurers

  ✳ Arbiters

✳ CAcert Inc. board (7 members since Nov 2008)

The CAcert supporting techi's

- help desk (80% forgot the password)

- translingo (26 languages)

- support

- non-critical and critical sysadmin teams

- development (php, java, ssh, pearl, http, mysql, openssl)

- education (Assurer manual, http://cats.cacert.org)

CAcert Assurance

- help, FAQ, tutorial documents and policies:
  - http://svn.cacert.org/CAcert/
  - and FAQ http://wiki.cacert.org/wiki

- **important ones**:
  - **CAcert Community Agreement** (CCA)
  - Non Related Disclaimer and License (NRP)
  - Assurance (Organisation) Policy

CAcert Community communication

- email lists:

  → help email lists

  → Assurers email list

  → Arbitration email list

  → policy email list

  → association email list

  → Organisation Assurers email list

CAcert agreements

- **CAcert Community Agreement (CCA)**
  - Community Member
  - membership obligations: keys, email contac
  - liability
  - arbitration (max US $ 1000 penalty)
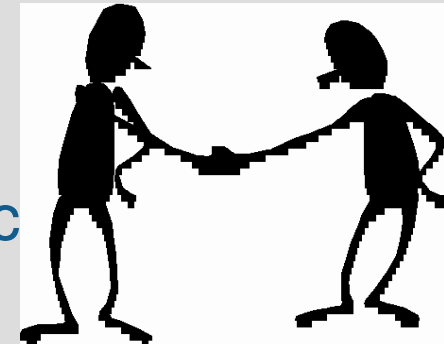
- Non-Related Persons Agreement (NRP)
  - license to use CAcert signed certificates
  - disclaimer

- Contributor License Agreement (CLA)

Web of Trust and the Relying Parties (RP)

- provisions regarding apportionment of liability

- financial responsibilities:

  ➤ indemnification by relying parties

  ➤ fiduciary relationships

- like with Open Source: license and disclaimer, permission to use, no permission to rely on.

CAcert Policies

- Policy on Policies (PoP) (ready)

- (Individual) Assurance Policy (AP) (ready)

  - Assurer Manual (pending)

- Organisation Ass. Policy (OA policy) (ready)

  - Sub-policies ready for Europe, USA, Australia, ...

  - Organisation Assurer Manual (to do)

- Cert. Policy Statement (CPS) (close to ready)

- Security Manual (close to ready)

CAcert policies (2)
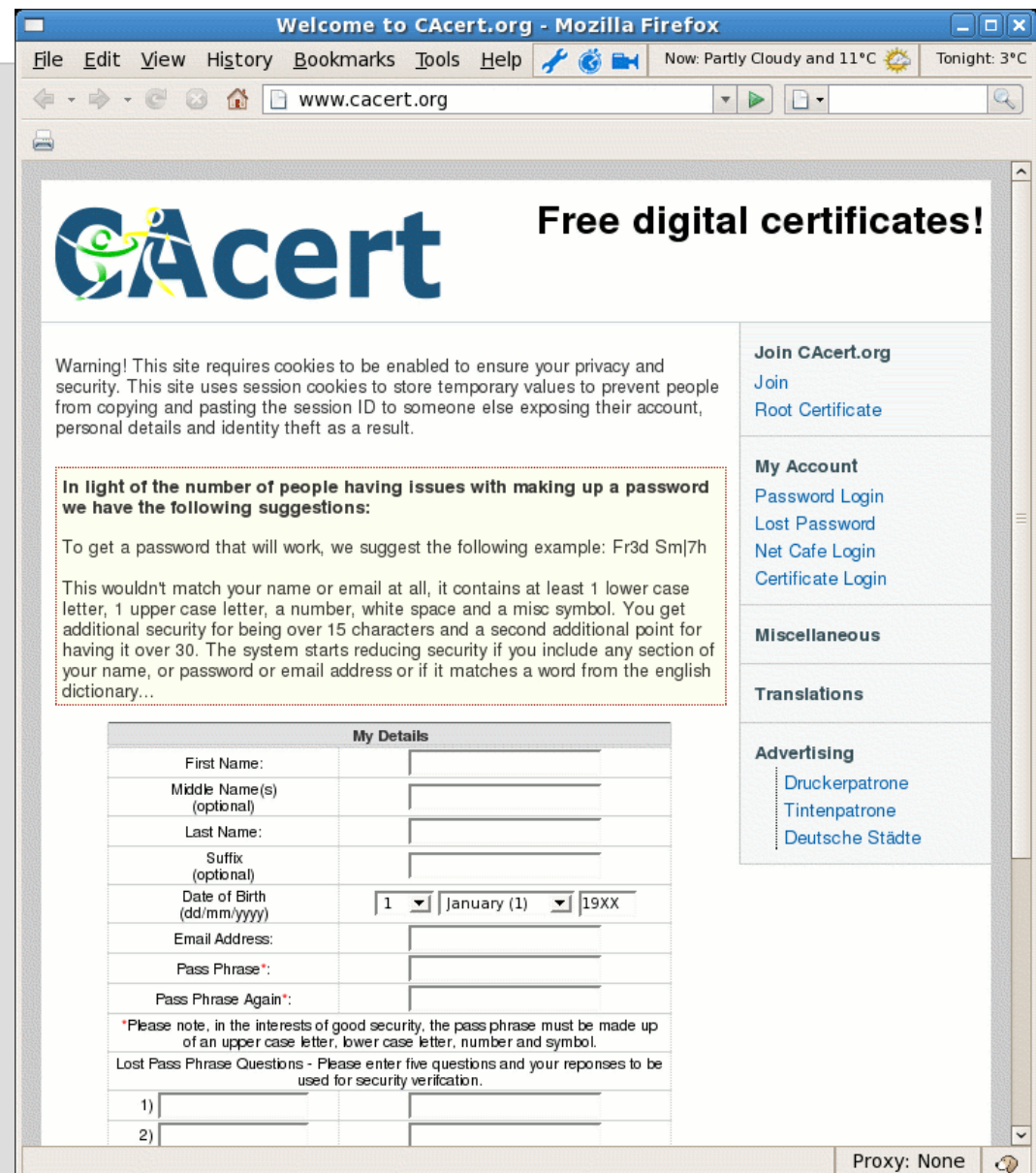
- Remote (Individual) Assurance Policy (pending)

- Dispute Resolution Policy (ready)

- Policy on Foundations (ready)

- Privacy Policy (ready)

- Communication Policy (ready)

HowTo join Community

HowTo join

- create
  - a **CA**cert account
  - password/phrase
  - five Q/A's

- remember them!

Get your identity checked!   the Assurance

- complete **CA**cert Assurance Form (paper ware)

- show your Identity Cards to **CA**cert 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 **CA**cert web site and import the new certificate

CAP form

complete **CAP** with

- full name

- date of birth

- primary email address

- date of Assurance

- signature while there

CAcert Organisation Assurance

- the organisation entity is in control:

  - (domain) server certificates

  - (email) client certificates

    for individuals within the organisation

- organisation needs to have:

  - **CA**cert Assured administrator

    > 100 assurance points

Organisation Assurance requirements

- legality of organisation:

    eg registration proof at trade office

- proof (CEO) signatures/stamps are legal

- proof system administrator can acquire and

    manage certificates (formal letter of designation)

- completed **CA**cert Organisation Assurance form

- assured by **CA**cert Organisation Assurer

COAP form

CAcert

Organisational

Assurance

Programme

details / policy is
country
dependent

CAcert Organisation Assurance Programme
Organisation Information (COAP) form
CAcert Inc. - P.O. Box 4107 - Denistone East NSW 2112 - Australia - http://www.CAcert.org
CAcert's Root Certificate sha1 fingerprints, class 1 : 135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33, class 3: DB4C 4269 073F E9C2 A37D 890A 5C1B 18C4 184E 2A2D

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

Organisation Identity Information

Name of the organisation	**Stichting Oophaga foundation**	
Address (comma separated)	**De Burgerstraat 25, office 268, 1098 SJ, Amsterdam-Buitenveldert**	
Type, jurisdiction (state)	**foundation, Netherlands**	
Registered Trade Names	**Oophaga**	
Registration (id, name, region)	**NL-238603-AA02, Kamer van Koophandel, Amsterdam**	
Internet Domain(s)	**oophaga.eu, oophaga.net, oophaga.nl, oophaga.org**	
Technical contact info	**Görge H. M. Sämple** tesu.hagaen@thesu.xs4all.eu	✆ +31 77 327996

Organisation's Statement

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

| Director | **Gerard H. M. Sühmple** | ✆ +31 773270066 |

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

Date
2008-08-18   Signature and organisation stamp

Organisation Assurer's Statement

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

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

Date
2008-08-25   Organisation Assurer's signature

© 2008 CAcert Inc., V3, generated 2008-8-25

What does one get? It is free

- client certificates:

  - as many as you have email addresses

  - > 50 assurance points your full name on it!

- server certificates:

  - as many as you have domains

  - > 50 assurance points

- code signing:

  - > 100 assurance points

- stamping service

- HowTo's and on line support

CAcert assurance

- print your CAP form
- take your ID's
- get assured by an Assurer:

    individual CAP

    or

    as organisation COAP

- documents/policies:

    http://svn.cacert.org/CAcert/

    and FAQ http://wiki.cacert.org/wiki

CAcert is community work

- >10.000 "to be" assurers,
  >1100 qualified assurers

- translations into 30 languages

- > 150.000 certificates in use

- >100 on the help desk:

  7 days * 24 hours email support

- world wide

- and **CA**cert certificates are **free:** at no charge

The unexpected message

- my OS or browser shows the threatening message,

  something as this:

  "*do not know the CA signing this certificate,*

  do you trust it? YES/NO"

- so I said:

  "**CA***cert visit this URL how to spend € 250K.*

  If not, I do not trust you."

The audit

- Mozilla CA policy as till November 2008

    mid 2005, David Ross Criteria (DRC)

    the unpublished list:

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

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

Mozilla web side December 2008

- https://wiki.mozilla.org/CA:How_to_apply

  - Root CA inclusion request (send bug report)

  - information gathering and verification

  - public discussion (2 phases)

  - Inclusion

- https://wiki.mozilla.org/CA:Information_checklist

  ca 11 chapters in total 35 requirements

What do the requirements do?

impose:

- control

- risks

- liabilities

- obligations

for the end user.

CAcert is currently

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

The CAcert new Root Key

- why?

    the "*four eyes principle*" is unclear,

      the old two Root Key(s): will stall audit

    newer technology and newer use

    no secrecy: openness

    better suited for current organisation

    history was built up
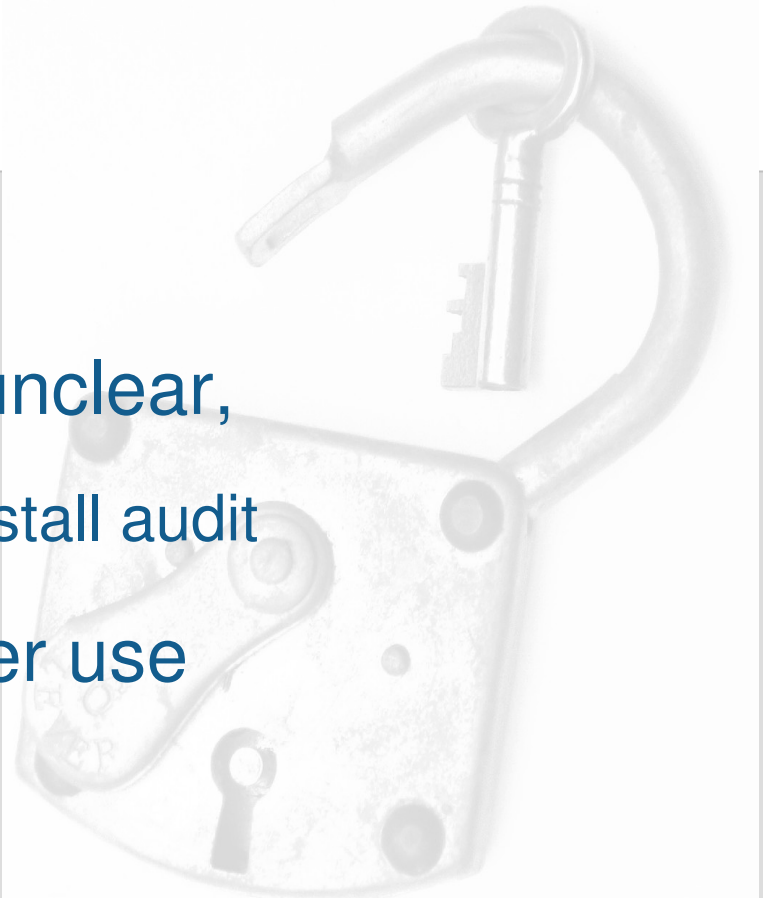
CAcert technical setup

- build on standard of the shelf HW

    rack mount PC's, KVM & switches

    (a rack full)
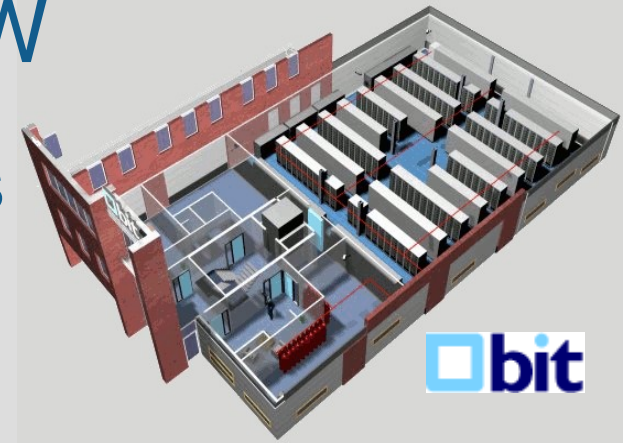
- build on standard of the shelf Open Software

    Ubuntu, wiki, apache, php, GNU email list, svn,

    ssh, openssl, gpg, BSD driven firewalls, ssl, Linux

    driven internal firewalls, virtual hosts, ...

The CAcert machinery & servers
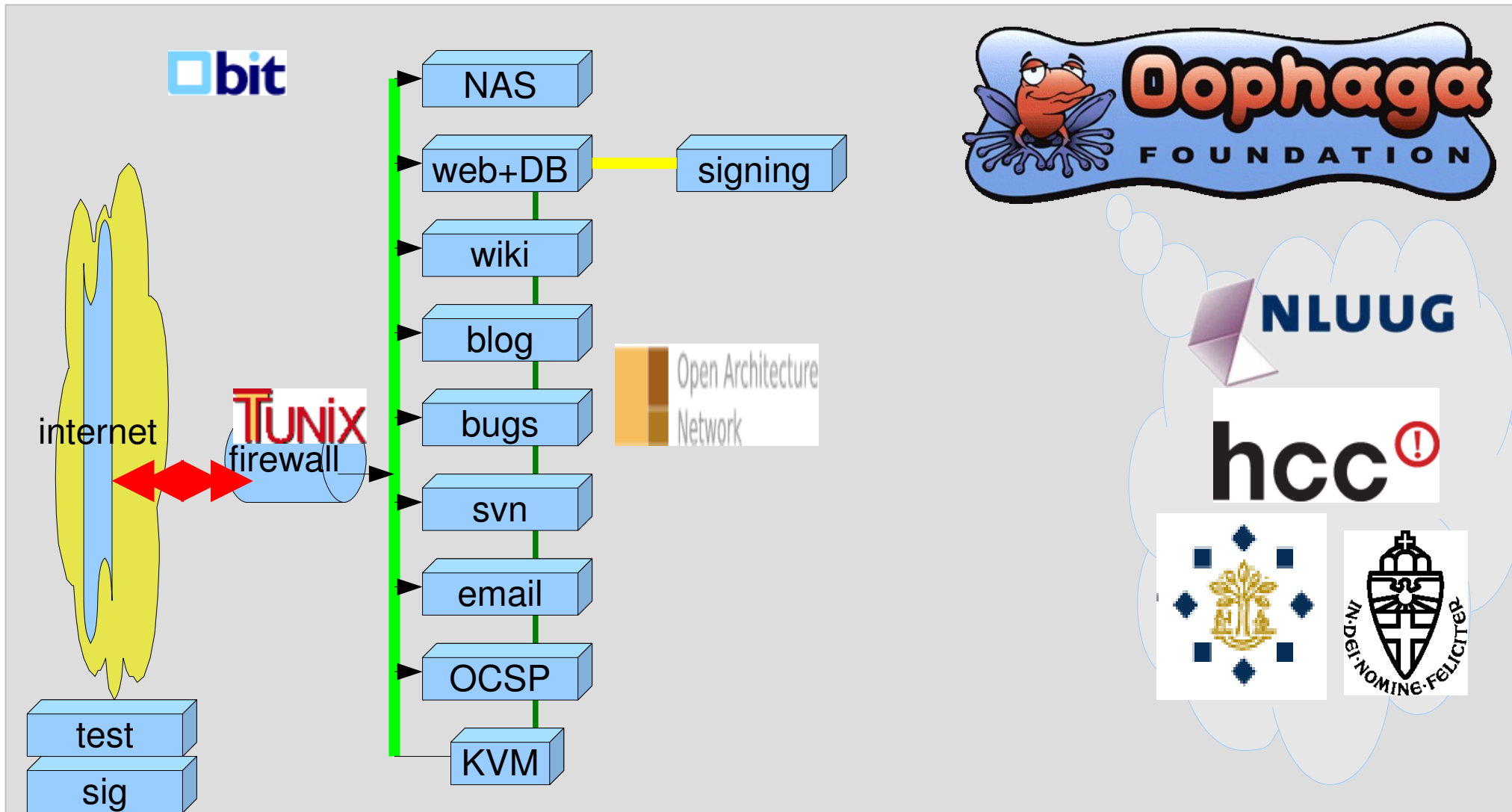
How to generate a secret X.509 key

you need:

- standard of the shelf PC

- standard audio card

- standard Open OS: here Ubuntu 8.10

- standard X.509 tooling: e.g.

    OpenSSL for key generation

    Java for certificate information handling

- standard statistics tooling

Use the right random number

- random number generation

  - you need a lot of them

  - find the right HW combination...

  - find and check the right tooling:

    - Turbid (www.av8n.com)

      calibration is complex, time consuming, too slow

    - randomsound (Linux tool, Debian)

      make sure you have the right HW combination
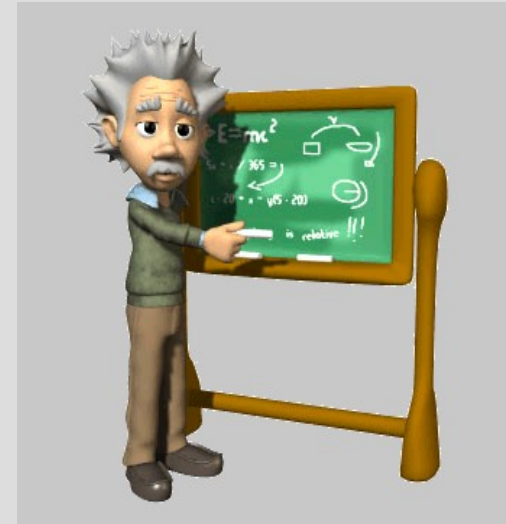
Check your random numbers

- use http://sig.cacert.at to check

- use standard tooling:

  - statistics:

    - chi square >0.01

    - arithmetic mean = 127.5

    - Monte Carlo = Pi

    - serial correlation

  - compression figures, e.g. 7.99999 bits/byte

Statistical tooling

- `ent`

  e.g.: `ent -c`

- `israndom`

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

  check, check and check ...

The Key Generation Tooling (GPL)

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

- OS and tools installation: install.sh

- key generation tooling: ceremony.sh

- copy keys, passwords: CopyKeys.sh

- and ... dismantle, destroy unencrypted keys

Install key generation

Internet

updates

Linux
distro

Mother

USB

stick

USB

sticks
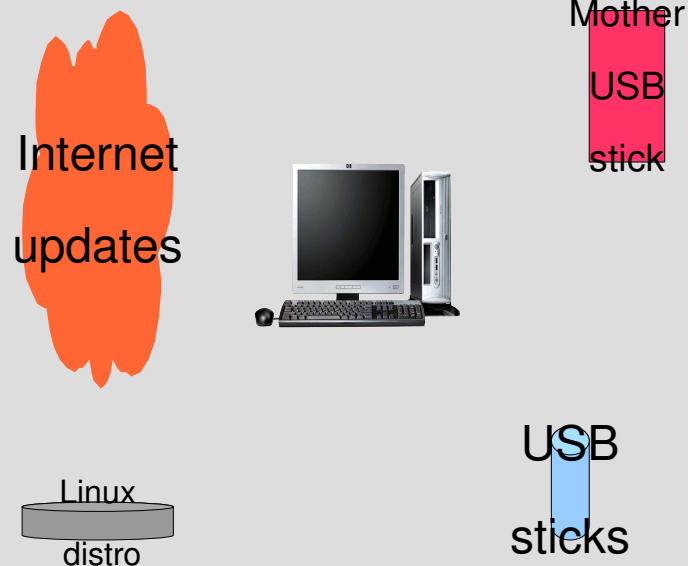
- installed Ubuntu 8.10

- install script:

  - upgrade to latest 8.10

  - install tools

    - openssl, java encr lib

    - randomsound

    - statistical packages

  - upload scripts

Generate random number

- randomsound

  - sample 400K bytes

  - check result

  ent:

    - 7.999564 bits per byte

    - chi square 241.31 50.00 %

    - arithm mean value: 275.5056

    - Monte Carlo Pi = 3.149971 error 0.27

    - serial correlation 0.001544

Generate random number (2)

➤ `israndom:`

  ➤ length 3145736.0 (ideal 3145728.0)

  ➤ compression 3163464

Generate keys

- watch out (swap off) for:

  - random file *only* resides on USB stick and RAM

  - keys *only* on USB stick and RAM

  - passwords *only* on USB stick and RAM

- private keys: RSA 4096

- passwords generated size 32 bytes

- public keys publicized

What did we do on 28th November 2008 ?

1. generated Root Key, self signed

2. generated 4 Sub Root Keys,

    signed by Root Key:

   - ▸ not Assured Members Sub Root Key (Class 1)

   - ▸ Assured Members Sub Root Key (Class 3)

   - ▸ 2 spare Sub Root keys

3. (Sub) Root Keys and passwd sticks for escrow

4. Sub Root Keys and passwd sticks for admin

Keys & passwords for escrow

Admin sub root keys and passwords

CAcert USB stick destruction tool

and ... dismantle used PC

- disk cleaner "shred" took 1.5 day

- deleted audio card

- deleted CDrom

- paranoia said:

  parts (random number, private key) good be on

  disk, regeneration due to hardware combi

What now for the Sub Root Keys?

- get them installed (done)

- get them evaluated (pending)

- get policy for use of certificates

  defined and accepted (to do)
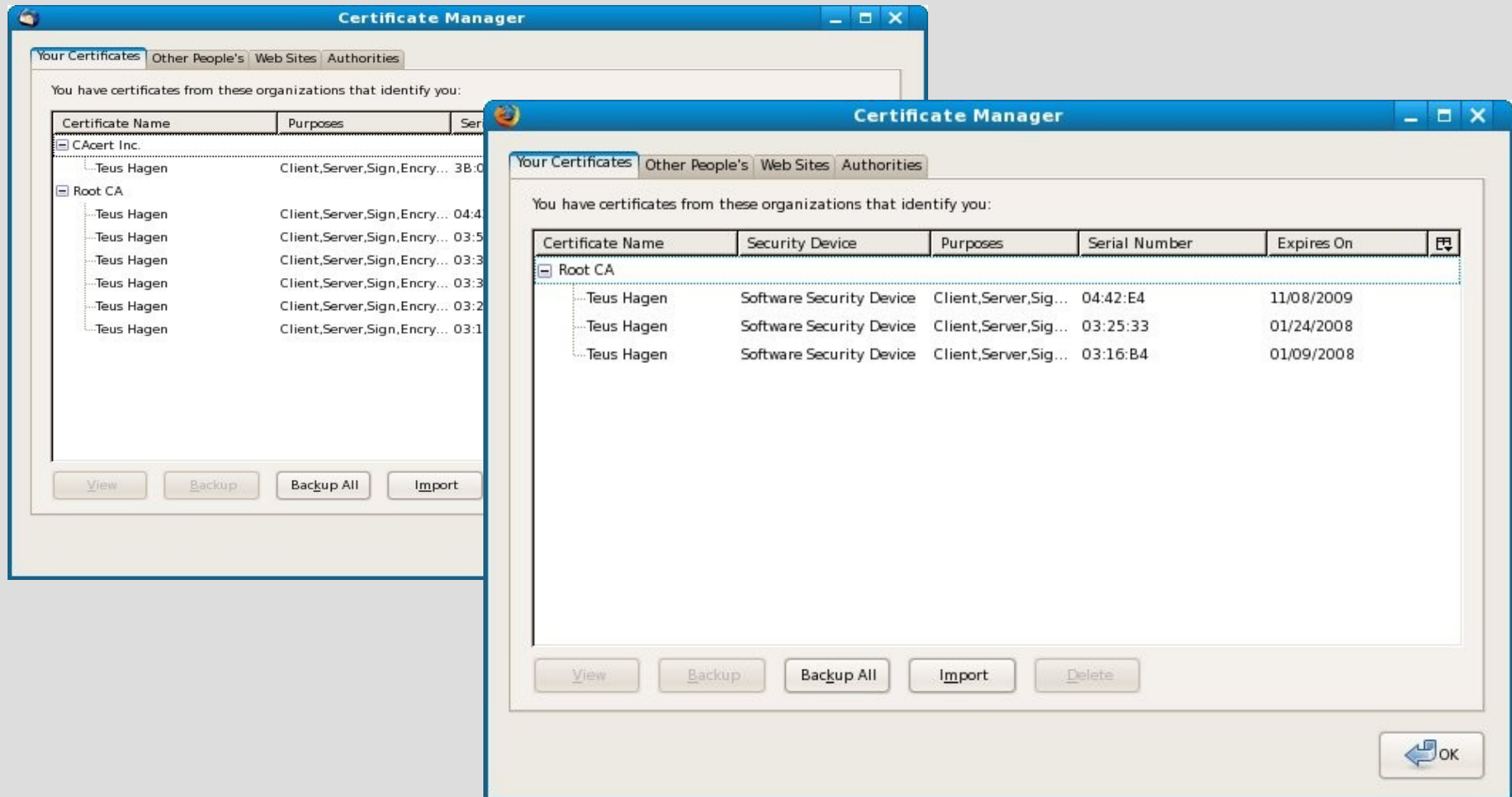
What now for audit

- finish audit project (36K Euro NLnet funding)

  - finish policies: CPS, sec & OA manuals

  - have auditor check on rulings

  - auditor final visits to location, assurance events

- send Mozilla ready signal and wait ...

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

- get people assured (scale up)

- get active for:

  ▶ assurances (become a real Assurer and RFM)

  ▶ developments

  ▶ support

  ▶ and: ... have fun as system admin & developer,

    and join the teams ... get in touch!

Thunderbird certificate usage

Thunderbird certficate usage

Thunderbird certificate usage

Thunderbird certificate usage

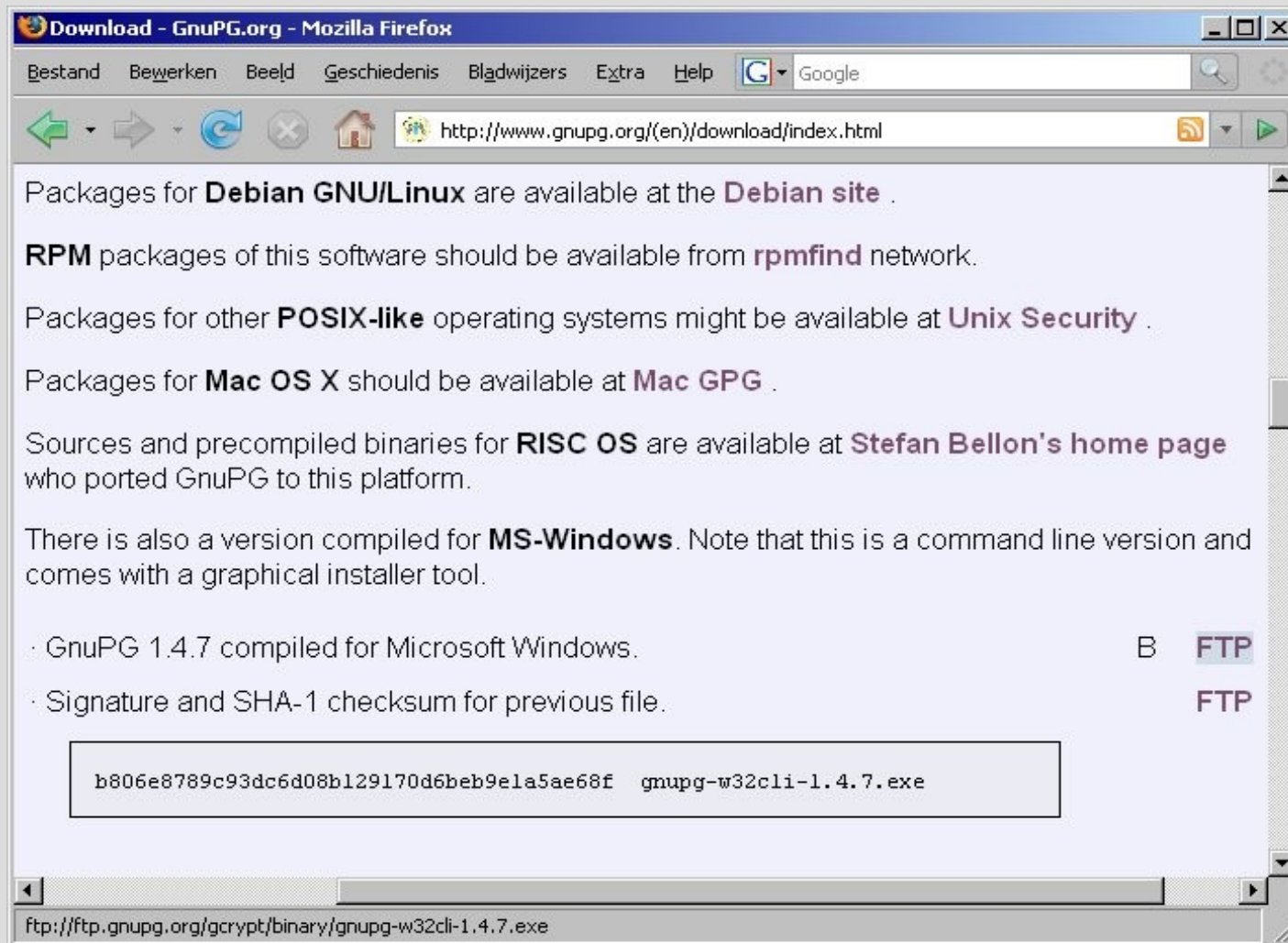# PGP, GPG or GnuPG

- private/public key encryption

- Web-of-Trust

  - the game of collecting signatures

  - have your finger print ready

- sub-keys

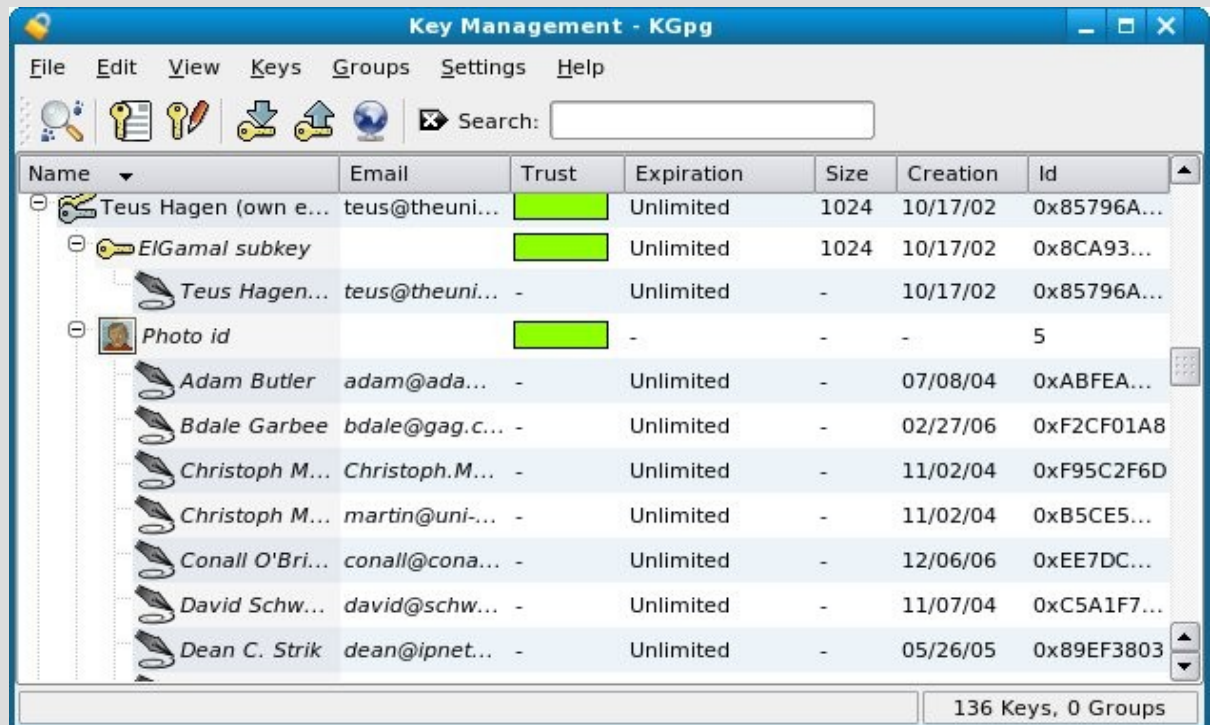- commonly used as check in Open Software distributions and reprocitories
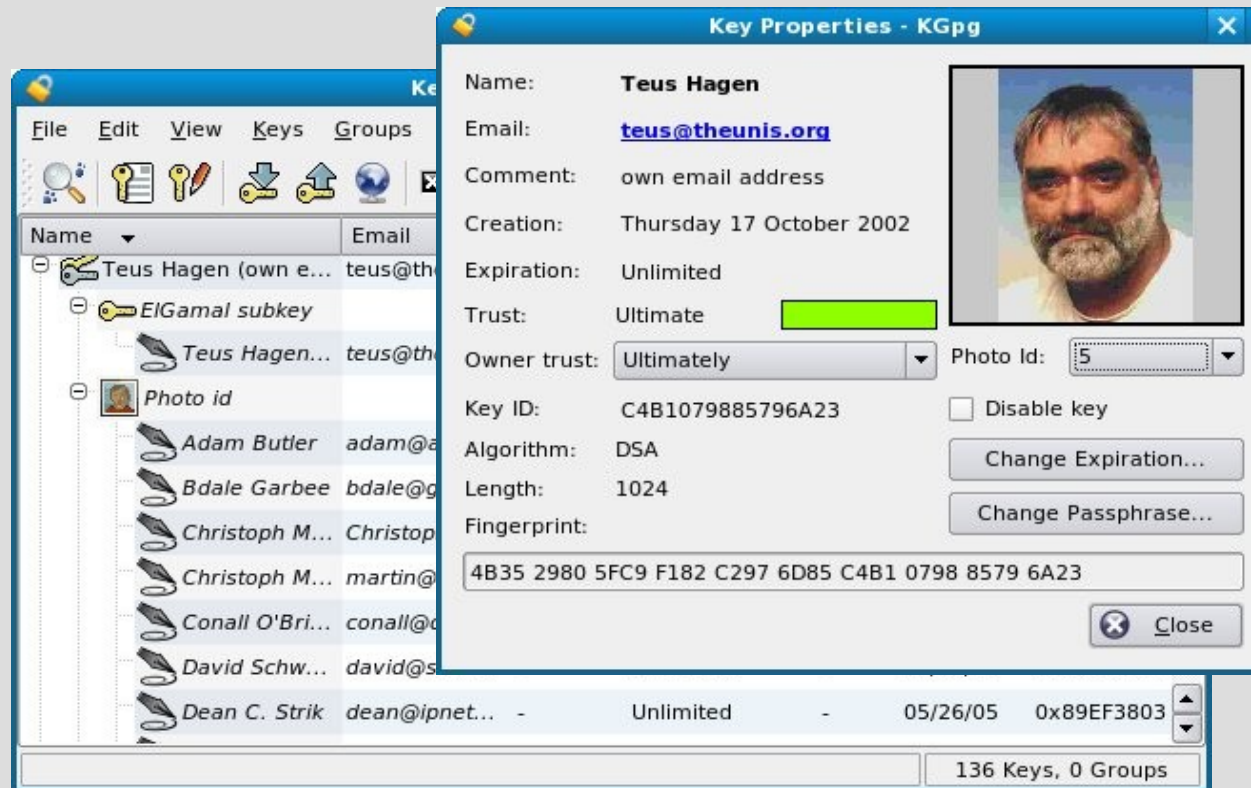
PGP/GPG install

GNUPG use

- Thunderbird plugin: OpenGPG/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 keyservers/statistics and spam?

- No X.509 certificate distribution infrastructure

FSFE and GNUpg

## Free Software Foundation Europe

- FSFE Fellowship crypto card
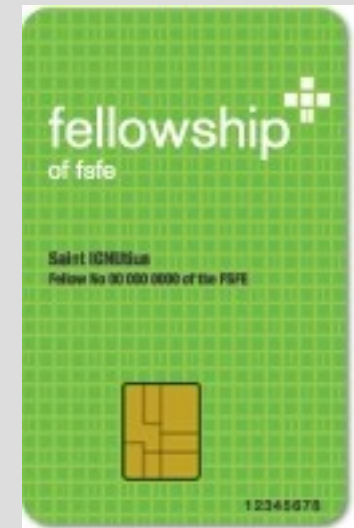
Questions to ask now:

- How to recover my password, why so complex?

- How do I get involved?

- How to import/distribute certificates?

- How to use OpenSSL?

- Why should we have an Organisation Assurance?

- What is changing for me now?

- The CAcert http://wiki.cacert.org/wiki/ says this, and you say that? Where do I find the search button?

- http://svn.cacert.org/CAcert/ Is a place to look for?

- What is the difference between CAcert Community Member and CAcert Association Member?

some references and handy URL's

- http://www.cacert.org

- http://wiki.cacert.org/wiki/

- http://svn.cacert.org/CAcert/

- http://www.pgpi.org/doc/pgpintro/

- http://www.cacert.nl

- http://sig.cacert.at

- Bruce Schneier:

  → Applied Cryptographyr, publ. John Wiley, 1996.

  → Secrets and Lies: Digital Security in a Networked World, publ. John Wiley, 2000.

  → http://schneier.com/blog Hacking the new Boeing 787 Dreamliner airplane

- http://tlsreport.layer8.net/reports/My_URL?protocol=https
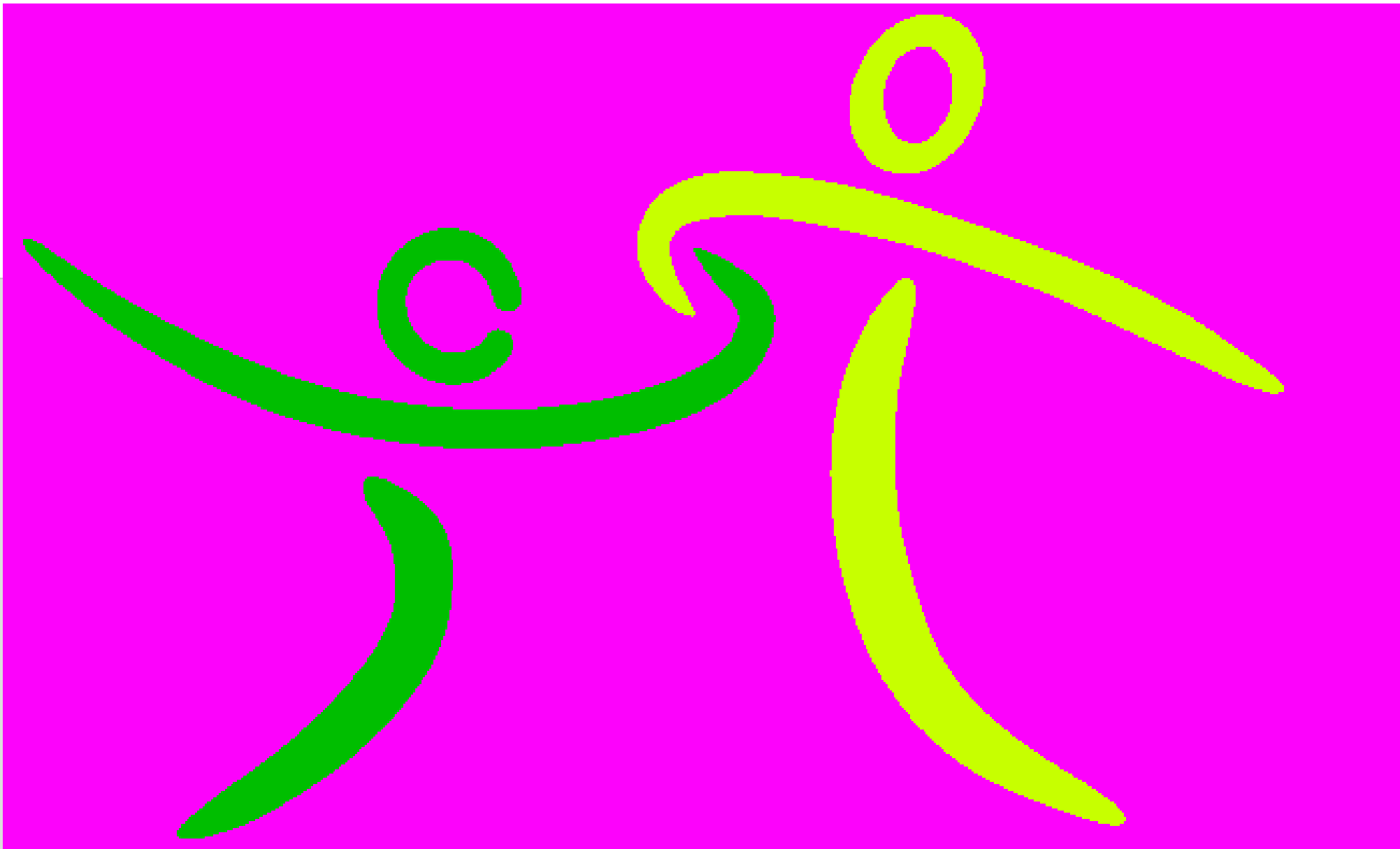
Thanks, some materials are used from: Wren Hunt, Ian Grigg and others