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 needs an Open and free to join CAcert?
- The CAcert audit project
- The CAcert hardware and service: the organisation and technology
- The new CAcert (Sub) Root Key: the HowTo for the paranoia
- If time allows the obvious FAQ's:
  - encryption how does this work
  - certificates how to use them: certutil
  - Firefox & Thunderbird and certificate management
  - GPG

http://svn.cacert.org/CAcert/PR/Presentations/CAcertPresentationNLLGG
What is a digital certificate?

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

- X.509 and PGP
certificates are official

- pres. Clinton signed
  S 761 - The Millennium Digital

encryption

Bruce Schneier:

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

- Herbern
- Enigma
  - Germany second world war
  - the mechanism
  - hacked, of course
Enigma technology
RFID chip hacked Dec 2007

- Mifare classic RFID chip of NXP (Philips)
- Karsten Nohl and Henryk Plötz
- Hacked
  - 48 bits but only 16 bits (only 64,000 variations) used
  - not random (dependent on time contact)
- implications:
  - car keys
  - public transportation cards
  - electronic tickets eg FIFA World Cup tickets
encryption key types

symmetric key encryption

sender

encrypted

receiver

encrypt

shared secret

decrypt

© CAcert, 2008. Teus/NLLGG 14th Dec 2008, 90 slides minus 10 to go
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

**Diagram:**

- **A:**
  - **AUTHOR:** Send no money
  - **RECIPIENT:** Send me money
  - **Man in the middle:** Man in the middle

- **B:**
  - **AUTHOR:** Send no money 7012
  - **RECIPIENT:** Send me money 7012
  - **Compare:** Compare 7067 7012

- **C:**
  - **AUTHOR:** Send no money 7012
  - **RECIPIENT:** Send me money 7067
  - **Compare:** Compare 7067 7012

- **D:**
  - **AUTHOR:** Send no money
  - **RECIPIENT:** Send me money 7067
  - **Compare:** Compare 7067 7012

**Notes:**

- private
- public
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?

- **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**
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
CAcert HowTo

- create
  - Private key
  - Cert Sign Req
- have it signed
- import
  - Private Key
  - Public Key: the certificate
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-----
MIICijCCAXICAQAwRTEL4AkGA1UEBhMCTw0ITAfBgkqhkiG9w0BCQEWEWEnRldXNA
hXl5G9tu4um9y2zETMBEGA1UEAxMKVGVLcyBIWd1bJCCASITwDQYJKoZIhvcN

aslwP+uZP9MwdFSwOEL8ldi860FNqLA5SkrlwwefjdPXRugYTXVzCn4pzpY/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
aosp@netup.ru ,p,
CA Cert Signing Auth - Root CA CT,C,C
Teus Hagen's Root CA 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 aosp@netup.ru -d .
-------BEGIN CERTIFICATE-------
MIIE7DCCAtSgAwIBAgIDAv+vMA0GCSqGSIb3DQEBBQUAMhAxGjAcBgNVBAsTFWh0dHA6Ly93d3cuJ0Lm9yZzEiMCAGA1UEAxMzQ0EgQ2VydCBTaWduaW5nIEF1dGhvcml0eTEhqGSIb3DQEJARYSc3VwcG9y
b3QgGQ0ExHjAcBgNVBAsXSC5vYHEyb2N0cy5vYHEyIEhwbGFibGUgQ29ycGluZ3MgQ2VydCBvY3NzIENvdXQgQXV0b3J5IENvbXBvcwIwYXJzZXQgQ2VydCB4MCExOExNMCwwGgYDVR0TAQH
b3QgGQ0ExHjAcBgNVBAsXSC5vYHEyb2N0cy5vYHEyIEhwbGFibGUgQ2VydCBvY3NzIENvdXQgQ2VydCBvY3NzIENvbXBvcwIwYXJzZXQgQ2VydCBvY3NzIENvbXBvcwIwYXJzZXQgQ2VydC
K1aTaRN4xKjsO98Z9rOqrIoKULkkjZYIbV61P6dyHnE7oVxKpQs+wdaOzpML/DwtGfva07uWcM/n2vNg==
-------END CERTIFICATE-------

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

% certutil -L -d . | grep fuare
pg@fuare.at p,P,p
The commerce or the community track?

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

your passport is it really you?

Shahiba Tulaganova UK journalist:

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

- and was able to pass UK border many times with them.
Certificate Authority signature

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

- Certificate Authority
  - the CA Root Key is added into “your” CA-list
    - On which authority?
  - Signs your X.509 public certificate
    - When signed you might be trusted?
Why CAcert?

• mission
  on internet allow everyone to protect their privacy

• no discrimination
• everyone should be able to afford it, and apply it
• high tech, transparent

• volunteers
The implication for CAcert

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

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

- **volunteers** needed
  Short and long term, HR time is costly

- **many discussions**
  OSS Simple Sabotage Manual (US CIA)

- **the sendmail phenomenon**
What is CAcert?

- Community of Members, based on WoT
- **CAcert** Inc. association (July 2003, NSW Australia)
- legal entities:
  - Not fully and fully assured Community Members
  - Assurers
  - Arbiters
  - **CAcert** Inc. board (7 members since Nov 2008)
The CAcert supporting techi's

- help desk (80% forgot the password)
- translingo (26 languages)
- support
- non-critical and critical sysadmin teams
- development (php, java, ssh, pearl, http, mysql, openssl)
CAcert Assurance

- help, FAQ, tutorial documents and policies:
  - [http://svn.cacert.org/CAcert/](http://svn.cacert.org/CAcert/)

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

- email lists:
  - help email lists
  - Assurers email list
  - Arbitration email list
  - policy email list
  - association email list
  - Organisation Assurers email list
CAcert agreements

- **CAcert Community Agreement (CCA)**
  - Community Member
  - membership obligations: keys, email contact
  - liability
  - arbitration (max US $ 1000 penalty)

- **Non-Related Persons Agreement (NRP)**
  - license to use CAcert signed certificates
  - disclaimer

- **Contributor License Agreement (CLA)**
Web of Trust and the Relying Parties (RP)

- provisions regarding apportionment of liability
- financial responsibilities:
  - indemnification by relying parties
  - fiduciary relationships

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

- Policy on Policies (PoP) (ready)
- (Individual) Assurance Policy (AP) (ready)
  - Assurer Manual (pending)
- Organisation Ass. Policy (OA policy) (ready)
  - Sub-policies ready for Europe, USA, Australia, ...
  - Organisation Assurer Manual (to do)
- Cert. Policy Statement (CPS) (close to ready)
- Security Manual (close to ready)
CAcert policies (2)

- Remote (Individual) Assurance Policy \((\text{pending})\)
- Dispute Resolution Policy \((\text{ready})\)
- Policy on Foundations \((\text{ready})\)
- Privacy Policy \((\text{ready})\)
- Communication Policy \((\text{ready})\)
HowTo join

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

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

For more information about the CACert Assurance Programme, including detailed guides for Assurer, please visit: http://www.CACert.org

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

For the CACert Organisation Assurance Programme there is a separate specific CAP form.

Date and location of the face-to-face meeting: 2008-12-31, Grubbenvos, the Carabien

### Applicant’s Identity Information

<table>
<thead>
<tr>
<th>points allocated</th>
<th>Exact full name on the ID: (type of ID shown)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>drs. T. Fabrice Ghuege-Denisi</td>
</tr>
<tr>
<td></td>
<td>drs. Teus F. Ghuege-Denisi</td>
</tr>
<tr>
<td></td>
<td>Email address: <a href="mailto:tesu.hagaen@thesu.xs4all.eu">tesu.hagaen@thesu.xs4all.eu</a></td>
</tr>
</tbody>
</table>

Date of Birth 1945-10-06

### Applicant’s Statement

Make sure you have read and agreed with the CACert Community Agreement.

http://www.CACert.org/policy/CACertCommunityAgreement.php

- I hereby confirm that the information stating my Identity Information above is both true and correct, and request the CACert Assurer (see below) to witness my identity in the CACert Assurance Programme.
- I agree to the CACert Community Agreement.

Date 2008-11-04

### Assurer’s Statement

Assurer’s Name: Mr A. B. C. Assurer. Assurer.email@cacert.org

- I, the Assurer, hereby confirm that I have verified the Applicant’s Identity Information, I will witness the Applicant’s identity in the CACert Assurance Programme, and allocate Assurance Points.
- I am a CACert Community Member, have passed the Assurance Challenge, and have been assured with at least 100 Assurance Points.

Date 2008-11-04
CAcert Organisation Assurance

- the organisation entity is in control:
  - (domain) server certificates
  - (email) client certificates
  for individuals within the organisation

- organisation needs to have:
  - CAcert Assured administrator
  > 100 assurance points
Organisation Assurance requirements

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

<table>
<thead>
<tr>
<th>Name of the organisation</th>
<th>Stichting Ophage foundation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address (comma separated)</td>
<td>De Burgerstraat 25, office 268, 1098 SA Amsterdam-Buitenveldert foundation, Netherlands</td>
</tr>
<tr>
<td>Type, jurisdiction (state)</td>
<td>Ophage</td>
</tr>
<tr>
<td>Registered Trade Names</td>
<td>Ophage</td>
</tr>
<tr>
<td>Registration (id. name, region)</td>
<td>NL-238809-A002, Kamer van Koophandel, Amsterdam</td>
</tr>
<tr>
<td>Internet Domain(s)</td>
<td>ophage.eu, ophage.net, ophage.nl, ophage.org</td>
</tr>
<tr>
<td>technical contact info</td>
<td>Görgie H. M. Sampo</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:teus.hagena@thesu.xsf.nl">teus.hagena@thesu.xsf.nl</a></td>
</tr>
</tbody>
</table>

**Organisation's Statement**

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

Director
Gerard K. M. Schrype

☑ 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**

☑ 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

© 2008 CAcert Inc., V3, generated 2008-8-25
What does one get?

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

It is free
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” assureds,
  >1100 qualified assureds
- translations into 30 languages
- > 150.000 certificates in use
- >100 on the help desk:
  7 days * 24 hours email support
- world wide
- and CACert certificates are free: at no charge
The unexpected message

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

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

- so I said:

  "CAcert visit this URL how to spend € 250K. If not, I do not trust you."
The audit

- Mozilla CA policy as till November 2008
  mid 2005, David Ross Criteria (DRC)
  the unpublished list:
<table>
<thead>
<tr>
<th>DRC reference(s)</th>
<th>Title / Area</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1</td>
<td>Configuration-Controlled Specification (CCS)</td>
<td>This is effectively the list of controlled documents that the audit insists is in place.</td>
</tr>
<tr>
<td>A.2-3</td>
<td>Certification Practice Statement and Certificate Policy</td>
<td>The core technical rules of the CA.</td>
</tr>
<tr>
<td>A.4</td>
<td>Privacy</td>
<td></td>
</tr>
<tr>
<td>A.5</td>
<td>Security Manual</td>
<td>DRC expects security details to be extracted from CPS/CP.</td>
</tr>
<tr>
<td>A.6</td>
<td>Risks, Liabilities</td>
<td>short list of disclosures.</td>
</tr>
<tr>
<td>B</td>
<td>Access for Subscribers, and &quot;the General Public&quot;</td>
<td>short list of disclosures.</td>
</tr>
<tr>
<td>C.1</td>
<td>Documentation Conformance</td>
<td>&quot;The CA has been repeatedly observed to operate in general conformance with its CPS.&quot;</td>
</tr>
<tr>
<td>C.2-4</td>
<td>Security, Maintaining Root Certificates</td>
<td>&quot;The root certificate private key is stored secure from electronic and physical compromise.&quot;</td>
</tr>
<tr>
<td>C.5-8</td>
<td>Generating / Signing / Renewing / Revoking</td>
<td>&quot;Certificates are signed in a timely manner&quot;</td>
</tr>
<tr>
<td>C.9</td>
<td>Use of External Registration Authority</td>
<td>&quot;RAs provide the CA with complete documentation on each verified applicant for a certificate (see &amp;A.2,w)&quot;</td>
</tr>
</tbody>
</table>
Mozilla web side December 2008

  - Root CA inclusion request (send bug report)
  - information gathering and verification
  - public discussion (2 phases)
  - Inclusion

  ca 11 chapters in total 35 requirements
What do the requirements do?

impose:

- control
- risks
- liabilities
- obligations

for the end user.
CAcert is currently

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

- why?
  
  the "four eyes principle" is unclear,
  the old two Root Key(s): will stall audit
  newer technology and newer use
  no secrecy: openness
  better suited for current organisation
  history was built up
CAcert technical setup

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

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

- internet
- firewall
- test
- sig
- □bit

NAS
web+DB
wiki
blog
bugs
svn
email
OCSP
KVM

signing

Open Architecture Network

CAcert

Oophaga Foundation

NLUUG

hcc
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

- installed Ubuntu 8.10
- install script:
  - upgrade to latest 8.10
  - install tools
    - openssl, java encr lib
    - randomsound
    - statistical packages
  - upload scripts
  - MD5 checks on versions
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
- sign public keys, hash: sha1
What did we do on 28th November 2008?

1. generated Root Key, self signed
2. generated 4 Sub Root Keys, signed by Root Key:
   - not Assured Members Sub Root Key (Class 1)
   - Assured Members Sub Root Key (Class 3)
   - 2 spare Sub Root keys
3. (Sub) Root Keys and passwd sticks for escrow
4. Sub Root Keys and passwd sticks for admin
Keys & passwords for escrow
Admin sub root keys and passwords
CAcert USB stick destruction tool
and ... dismantle used PC

- disk cleaner “shred” took 1.5 day
- deleted audio card
- deleted CDrom

- paranoia said:
  parts (random number, private key) good be on disk, regeneration due to hardware combi

- social engineering seems to be easier ...
What now for the Sub Root Keys?

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

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

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

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

Packages for **Debian GNU/Linux** are available at the [Debian site](http://www.debian.org). **RPM** packages of this software should be available from the [rpmfind](http://rpmfind.net) network.

Packages for other **POSIX-like** operating systems might be available at [Unix Security](http://www.unixsecurity.org). Packages for **Mac OS X** should be available at [Mac GPG](http://macgpg.sourceforge.net).

Sources and precompiled binaries for **RISC OS** are available at [Stefan Bellon’s home page](http://www.sbellon.com). There is also a version compiled for **MS-Windows**. Note that this is a command line version and comes with a graphical installer tool.

- GnuPG 1.4.7 compiled for Microsoft Windows.
- Signature and SHA-1 checksum for previous file.

```
b806e8789c93dc6d08b1291706beb9e5a6e68f
gnupg-w32cli-1.4.7.exe
```

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 assureurs 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?
- What does a certificate look like?
some references and handy URL's

- http://www.cacert.org
- http://svn.cacert.org/CAcert/
- http://www.cacert.nl
- http://sig.cacert.at
- Bruce Schneier:
  - http://schneier.com/blog Hacking the new Boeing 787 Dreamliner airplane
- http://tlsreport.layer8.net/reports/My_URL?protocol=https
TIP

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

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