TIP

Remember, your sense of conviction and your involvement with the content of the presentation are critical to its success.
what is CAcert about?

content

- trust and identity
- X.509 digital certificates
- encryption technology
- CAcert what it is, how to join and get certificate, services, and why there is a CAcert community
- the HowTo for Linux Firefox/Thunderbird and command line
  - certificate installation
  - certificate usage
- why should I?
- PGP/ GnuPG
on the internet nobody knows you are a dog
trust is not identification!

who are they? trust worthy?

- use digital signatures for identification
- via Web of Trust identification
  - GPG/PGP
  - CAcert X.509 certificates
identification (your email from Nigeria)

- verify email / web
  - sender
  - receiver
  - MTA client
  - MTA server
- forging
your passport is it really you?

- BBC 1 Panorama 1\textsuperscript{st} of December 2006
- Shahiba Tulaganova UK journalist:
  - within 5 months on east European markets
  - bought 20 EU passports, 5 other
    (UK, Dld, F, S, NL, B, Es, PO, G, Cs, Pl, Au, ....)
  - 300-3000 euro each

  - and was able to pass UK border many times with them.
secure digital content

- documents
- images
- software code
- use stamping
secure data transfer

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

- Pres. Clinton signed

the technology: encryption

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

Bruce Schneier:

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

- Herbern
- Enigma
  - Germany second world war
  - The mechanism
  - hacked
Enigma technology
RFID chip hacked Dec 2007

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

- RFID reader
- Random number from RFID reader
- Random generator
- Secret base key
- Identify RFID
- To one nr
- 48 bit linear feedback shift register
- Generate key
- Key
encryption key types

symmetric key encryption

sender

encrypted

receiver

shared secret

encrypt

decrypt
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:

- **Author**: Sends no money
- **Recipient**: Sends me money
- **Man in the middle**
  - A: Send no money 7012
  - B: Send me money 7012
  - C: Compare 7057 7012
  - D: Compare 7057 7012

- **Private**
  - D: Compare 7057 7012
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 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
How To join Community

register
• create
  – a CAcert account
  – password/phrase
  – five Q/A's
• remember them!
Get 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
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__-__-__

<table>
<thead>
<tr>
<th>Passport</th>
<th>Photo ID</th>
<th>Drivers Licence</th>
<th>Photo ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification Card</td>
<td>Photo ID</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

Location of Face-to-face Meeting: ____________________________

Points Allocated: ______ Notes: ____________________________

© CAcert, 2008 Teus/HCC-Venlo 8 Jan 2008 50 slides minus 26 to go
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 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)**

<table>
<thead>
<tr>
<th>Name of the Organisation (Naam van de Organisatie)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact email address (Contact email adres)</td>
</tr>
<tr>
<td>City (Vestigingsplaats)</td>
</tr>
<tr>
<td>State (Provincie)</td>
</tr>
<tr>
<td>Country (Land)</td>
</tr>
<tr>
<td>email(s) or administrator accounts - must match a CAcert account (CAcert Account email adres(sen) van de systeem administrator)</td>
</tr>
<tr>
<td>Domain(s) (domein-naam (-namen))</td>
</tr>
</tbody>
</table>

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 originele of gekoppelde copieën niet ouder dan 4 weken, zijn bijgevoegd:**

---

© CACert, 2008 Teus/HCC-Venlo 8 Jan 2008 50 slides minus 29 to go
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?
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-----
MIICijCCAXICAQAwRTElMAkGA1UEBhMCTkwxITAfBgkqhkiG9w0BCQEWEnRldXNA
bXlfZG9tYWluLm9yZzETMBEGA1UEAxMKVGV1cyBIYWdlbi5vQYJKoZIhvcN
...
aslwP+uZP9MwdFSwOEL8ldi860FMgLAs5Kr1wwewfjtDPXRugYTXVzCn4pzpY/Fz
GS/2xpYuwaQDrz57L+YE4zakeoZunctZW9fWZZOj9
-----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+vMA0GCSqGSIb3DQEBBQUAMHkxEVBAoTB1j
b3QgQ0ExHjAcBgNVBAstTFWhdHA6Ly93d3cuJ0Lm9yZzEiMCAGA1UEAxMZ
Q0EgQ2VydCBTaW5rYWlvdXJldGVuIGFuZ3VhcmRlIENPEkRQMS0w
K1aTaRN4xKjsO98Z9r0qrIoKULkkjZyIbV61P6dyHnE7oVxKpQs+wdaOzp
ML/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
```
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 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

Certificate: Teus Hagen, Oephega Foundation [03:5D:AD]
Details of selected certificate:
- Issued to: E=teus.hagen@oephega.org, C=NL
- Serial Number: 03:5D:AD
- Valid from 02/19/2007 15:03:16 to 03/18/2009 15:03:16
- Purposes: [Client, Server, Sign, Encrypt]
- Issued by: E=suppport@ca.cert, C=NL
- Root CA
- Stored in: Software Security Device

Thunderbird can use Online Certificate Status Protocol (OCSP) to verify certificates. Set Thunderbird to use OCSP as follows:
- 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:
  - Response Signed: Built-in Object Token: IPS OBJECT Token
  - Service URL: http://ocsp.ips.es/
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 reproitories
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 [rpmfind](http://www.rpmfind.net/) network.  

Packages for other **POSIX-like** operating systems might be available at [Unix Security](http://unixsecurity.diehl.de/).  

Packages for **Mac OS X** should be available at [Mac GPG](http://www.maccrypt.info/).  

Sources and precompiled binaries for **RISC OS** are available at [Stefan Bellon’s home page](http://www.stefanbellon.de/).  

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.  

```bash
b806e8789c93dc6d08b129170d6beb9ela5ae68f  gnupg-w32cli-1.4.7.exe
```

ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.7.exe
GNUPG use

- Thunderbird plugin: OpenGPG/Enigmail
- KGPG

- Gnome Keyring Manager
KGPG keyring manager

Key Properties - KGpg

Name: Teus Hagen
Email: teus@theunis.org
Comment: own email address
Creation: Thursday 17 October 2002
Expiration: Unlimited
Trust: Ultimate
Owner trust: Ultimately
Key ID: C4B1079885796A23
Algorithm: DSA
Length: 1024
Fingerprint: 4B35 2980 5FC9 F182 C297 6D85 C4B1 0798 8579 6A23

© CAcert, 2008 Teus/HCC-Venlo 8 Jan 2008 50 slides minus 52 to go
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
some references and handy URL's

- http://www.cacert.org
- http://svn.cacert.org/CAcert/
- http://www.cacert.nl
- Google search
- http://schneier.com/blog Hacking the new Boeing 787 Dreamliner airplane
CAcert is for and by 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, Ian Grigg and others
What can you do if you are not willing to be a dog
Trust is something else as you know who you are talking to
Do you know who you are talking to? Trust in identity.
Trust in the email sender
Need a formal identity, well that seems to be easy
Identities are hard to check, so you need more people to check it: Web of Identity trust
Where certificates are used for.
You learn easy to appriciate them. For sure after the accident.
Ever clicked on the little lock?
View the certificate offered by the web server. Note that even banks forgot to renew
the certificate. Still to meet a person who has not experienced that the bank web site
offered an out of date certificate. We all have to learn.
Two examples of encryption technology
the latter we apply with certificates
Note this statement is proven ever and ever again right
The famous one from the second world war. Invented in Germany, used and trusted as THE coding system. However hacked by the Britain.
The secret shared key is the three offset of the wheels. That is the seed of the coding. After every character, one internal wheel is put one place to the right, and the other internal wheel to the left. So the Caesar encryption gets less obvious.

But frequency statistics help you to break this...
A late one, just today. 200 million (says NXP), publications say 2K million sold of this chip. 1K type single price 0.85 US$, >100K 0.45 US$. 4K des variant US$ 2.50.
Credit card size. Contactless 10cm. Antenna is biggest part, chip 1 mm**2
Ultra light paper US$ 0.50-0.16 512 eeprom on it.
Mainly applied in door entrance control, access control.
Karsten from Uni of Virgenia sounds like the science man
Henryk sounds like the hacker
10K building blocks, only 70 different.

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

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

Privacy is a big issue.
Mifare Classic workings (Nohl & Plötz)

- RFID reader
- Random nr from RFID reader
- Random generator
- 48 bit linear feedback shift register
- Generate key
- Key
- Secret base key
- Ident RFID
- One nr
- To one nr
Ever given your password/phrase away? Who not? Well shared secrets are not shared.
Social engineering is an easy hacking tool. Keep secrets to yourself only.
This looks crazy: publicing the encryption or decryption key. But it is not. It gets complicated now. But it is a rich tool.

How do you know the pub key is from him. Once encrypted with one key it can only be decrypted with the other... It is simple, but have a good thought about it.
OK we know the mechanism. How do you apply it.
How to make sure the content is readable and it can be check that the message came from this sender.

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

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

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

How do we know the publick key is his one? We need an authosrity to say yes his name is on that key.
A real live example. First the mechanism.
How does the example work with email
How does encrypted and signed email show up in Thunderbird.

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

Is the signature ok?

Is this an error or a warning.
Sopend money or join the CAcert community.
Be a member
The portal to secure yourself...

But know what you do! Read the agreement. Know it is based on the Open Source mind set. It is free, and it should remain free. And it should be improved. You need to contribute and that contribution should be free as well.
Feedback what you think is not right.
Password
five questions and answers to remember just in case
note you can login CAcert web site with your CAcert certificate. No password to remember. Well when is your certificate expired. Yes two years ago I gave my password, one not that easy to guess....

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

You have more as one name and can proof it? Well you can do so, but need ID proofs. (Not implemented yet).
Well, once there. How to prove it is you. Have your identity checked.

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

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

One assurance give you 10-35 points. You need at least 50 to get your name on the
cert. The best is to collect 100 points so with some knowledge of how this works you
can assure others and help to enlarge the community
Every assurance you need one form. Start to print out at least 4 of them. Yes a lot of paper work.
Note that your name on the form should be identical to your passport and the name you provided on the CAcert account.

Name should be identical to account full name, and ID shown.
More names are possible but you need to proof it.
Married name? No problem but show it to an assurer.
The latter requires some implementation still.
CAcert Organisation Assurance

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

Organisation Assurance is possible now.
But ask for the CAcert subpolicy for this in your country!
Currently only: Germany and Holland.
## Organisation Assurance requirements

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

**CAcert Organisational Assurance Programme**

details / policy is country dependent

<table>
<thead>
<tr>
<th>Name of the Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter Name]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter Name]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact email address</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter Email]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>City (negenhonderd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter City]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State (wettelijke)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter State]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country (land)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter Country]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email of administrator (beste)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter Email]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Account (Accountnummer / Account number)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Enter Account]</td>
</tr>
</tbody>
</table>

As proof for the legality, identity and capacity of signatories for the organisation the following official documents, either original or certified copies and not older than 3 weeks, are attached to this form:

1. 
2. 
3. 

(Ongeveer de officiele namen van de Organisatie. Haar rechtshouding en de genoemde van de te benutten regels zijn de officiële ondertekenen of geautoriseerde (opname niet ouder dan 4 weken).)
P12 is binary format and is password protected. The others are ascii and not password protected. It matters for the private key. Keep it save.

You do not want to lose them. What about all your emails encrypted and you lost your private key?
How to create keys see later.

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

Private (Key) and CSR can be combined in one file the PEM file. Most browsers and email handlers need a binary p12 file. So you need to convert PEM to P12 (can be done by openssl and others.).
For non 64 bit machines Firefox/Thunderbird has an easy add on to create a key and to make the CSR ready.
Note that CAcert only will allow name (CN) and email address. CAcert tries to keep traceability and privacy info as low as possible.
This is in the openssl package. The arguments are rich. To get started you need only to know a little.
Certutil come from the nss-tool package. It operates on the database
firefox/thunderbird use.

Look here: cd ~/.thunderbird/*/default
eg cert8.db

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

Make sure if you try things out you make a backup.
Certutil is a handy tool to extract collected publick key, signed certificates from the database (user certificates from Thunderbird).
Certificate collect is fully dependent on email sent signed to you.