NGS

National Grid Service

Gaining access

Mike Mineter, Guy Warner
Training, Outreach and Education
National e-Science Centre
mjm@nesc.ac.uk, gcw@nesc.ac.uk

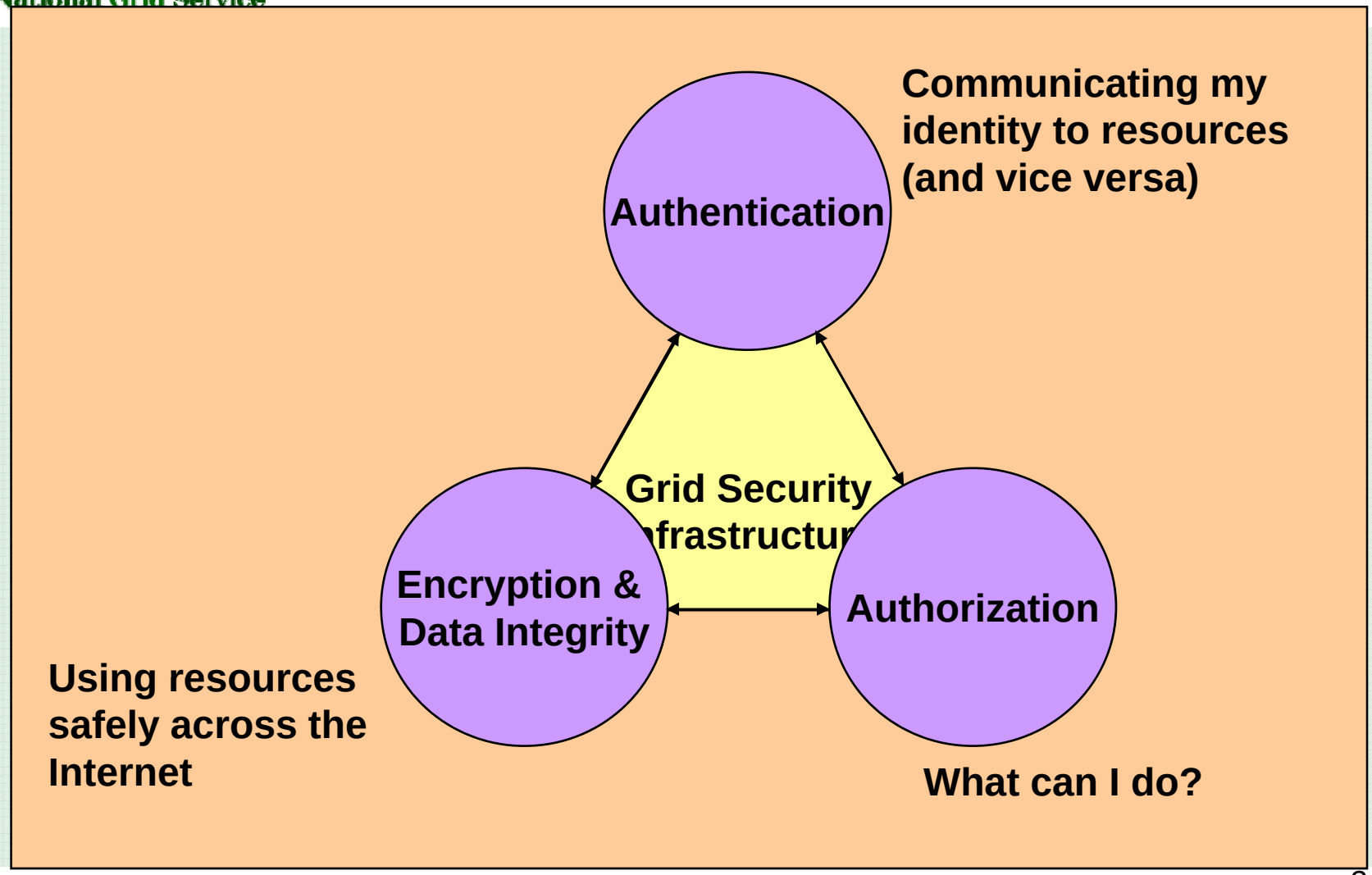
Policy for re-use

- This presentation can be re-used for academic purposes.

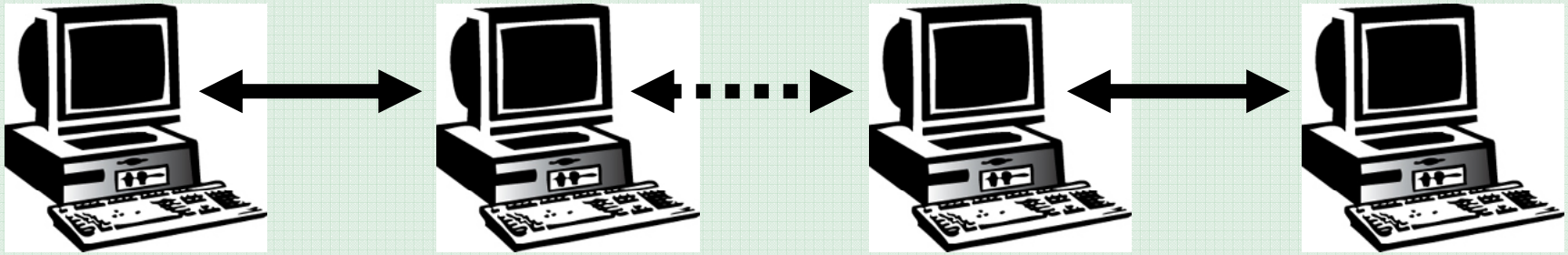
- However if you do so then please let training-support@nesc.ac.uk know. We need to gather statistics of re-use: no. of events, number of people trained. Thank you!!

NGS
National Grid Service

Grid security



The Problems - 1



User **Resource**

- How does a user securely access the Resource without having an account on the machines in between or even on the Resource?

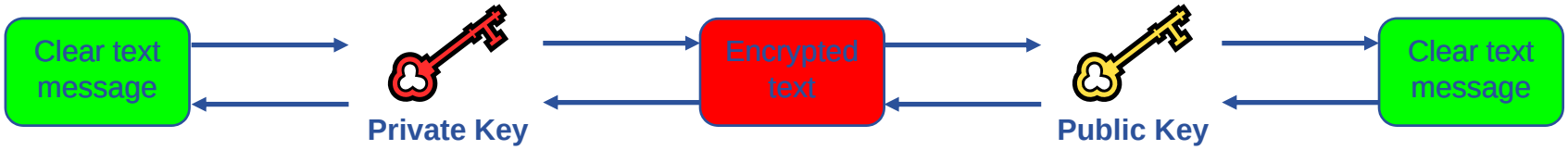
- How does the Resource know who a user is?
- How are rights determined?

The Problems -2: Reducing vulnerability

- Launch attacks to other sites
  - Large distributed farms of machines, perfect for launching a Distributed Denial of Service attack.
- Illegal or inappropriate data distribution and access sensitive information
  - Massive distributed storage capacity ideal for example, for swapping movies.
- Damage caused by viruses, worms etc.
  - Highly connected infrastructure means worms spread faster than on the internet in general.

Basis of security & authentication

- **Asymmetric encryption…**

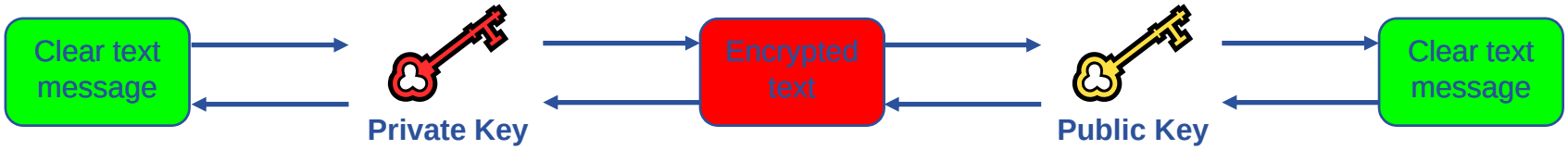


- **…. and Digital signatures …**
  - A hash derived from the message and encrypted with the signer's private key
  - Signature is checked by decrypting with the signer's public key

- **Are used to build trust**
  - That a user / site is who they say they are
  - And can be trusted to act in accord with agreed policies

Basis of security & authentication

- **Asymmetric encryption…**

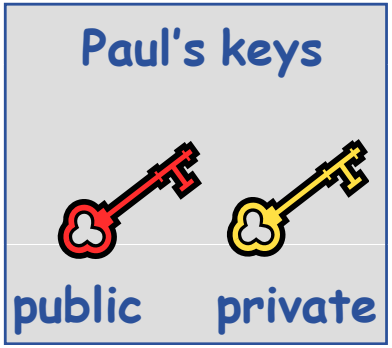


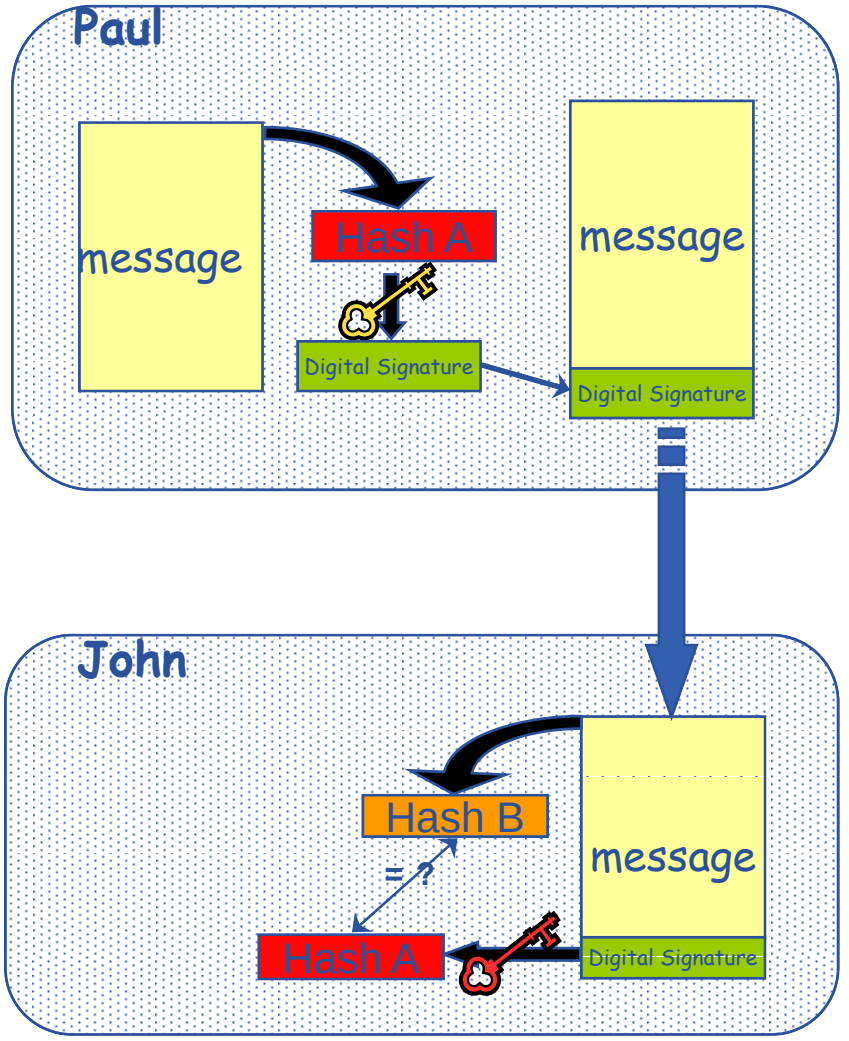
- **…. and Digital signatures …**
  - A hash derived from the message and encrypted with the signer's private key
  - Signature is checked by decrypting with the signer's public key

- **Are used to build trust**
  - That a user / site is who they say they are
  - And can be trusted to act in accord with agreed policies

Digital Signature

- Paul **calculates the *hash* of the message**
- Paul **encrypts the hash using his *private* key: the encrypted hash is the *digital signature*.**
- Paul **sends the signed message to** John.
- John **calculates the hash of the message**
- **Decrypts signature, to get A, using Paul's *public* key.**
- **If hashes equal:**
  1. message wasn't modified;
  2. hash A is from Paul's private key

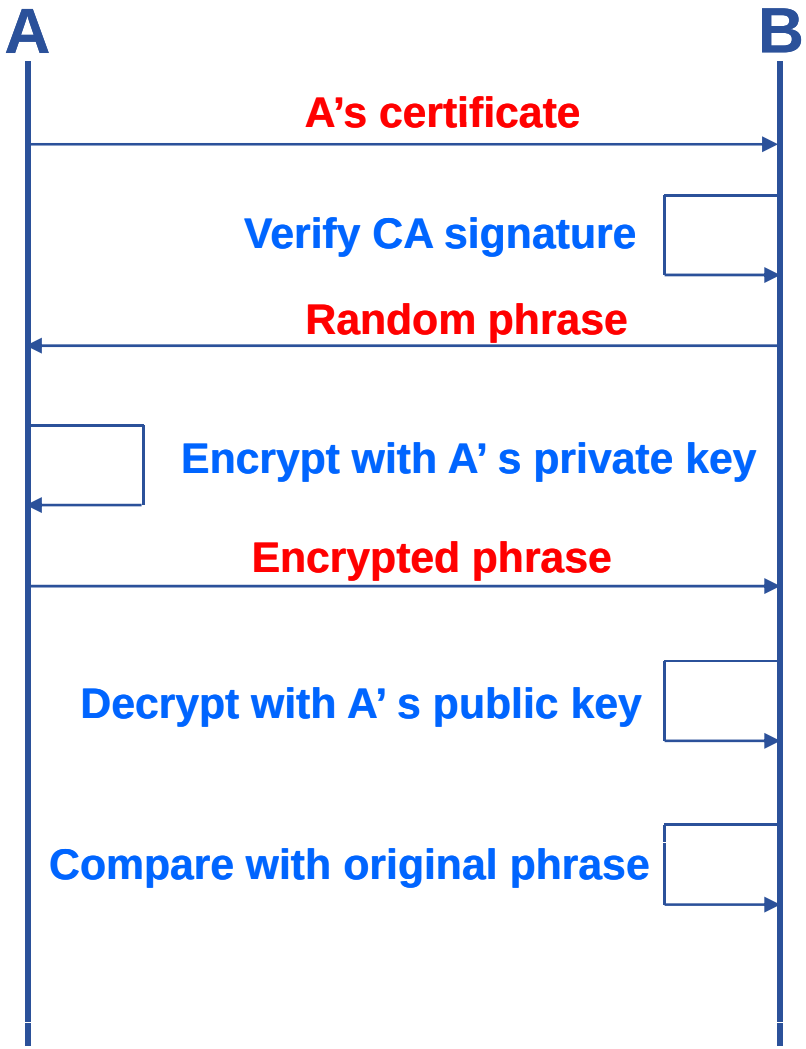




The Grid Security Infrastructure (GSI)

Based on X.509 PKI:

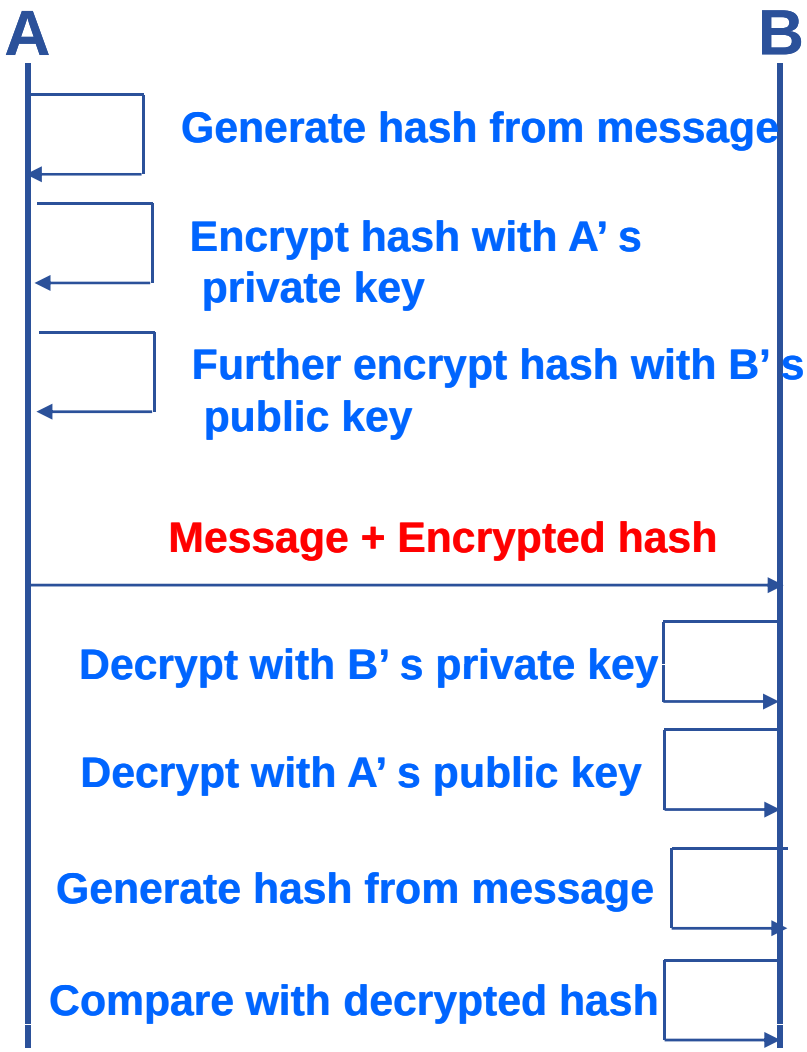
- **every Grid transaction is mutually authenticated:**
  1. A sends his certificate;
  2. B verifies signature in A's certificate using CA public certificate;
  3. B sends to A a challenge string;
  4. A encrypts the challenge string with his private key;
  5. A sends encrypted challenge to B
  6. B uses A's public key to decrypt the challenge.
  7. B compares the decrypted string with the original challenge
  8. If they match, B verified A's identity and A can not repudiate it.
  9. Repeat for A to verify B's identity



The Grid Security Infrastructure (GSI) - continued

After A and B authenticated each other,
for A to send a message to B:

- **Default: message integrity checking**
  - Not private – a test for tampering



.

- **For private communication:**
  - Encrypt all the message (not just hash) - Slower

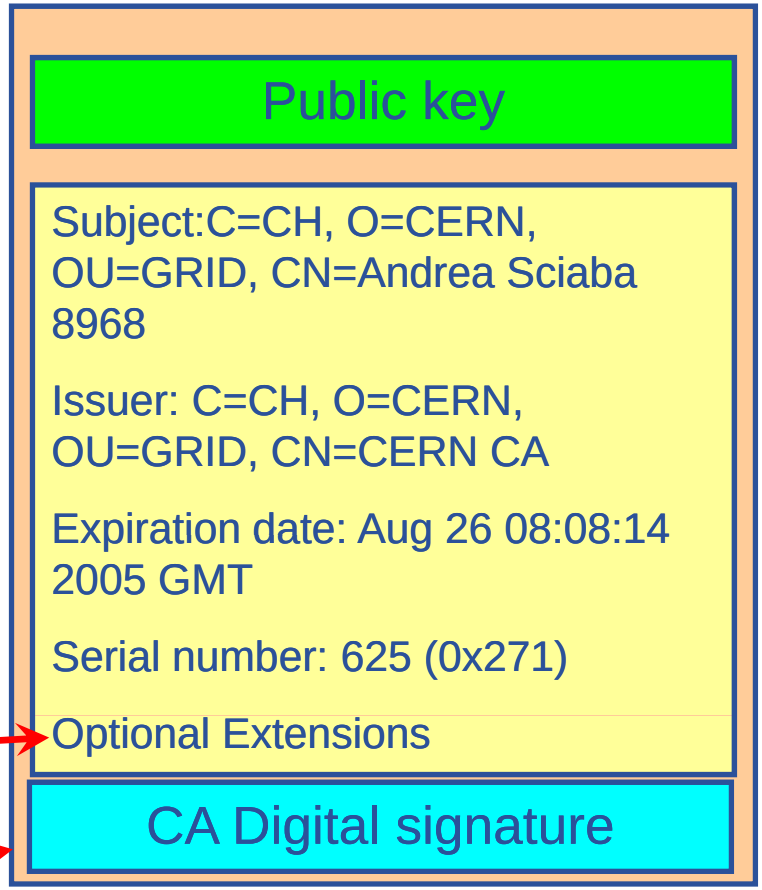
Digital Certificates

- **How can John be sure that Paul's public key is really Paul's public key and not someone else's?**
  - A *third party* certifies correspondence between the public key and Paul's identity.
  - Both John and Paul trust this third party

The "third party" is called a *Certification Authority* (CA).

X.509 Certificates

- **An X.509 Certificate contains:**
  - owner's public key;
  - identity of the owner;
  - info on the CA;
  - time of validity;
  - Serial number;
  - Optional extensions
  - digital signature of the CA

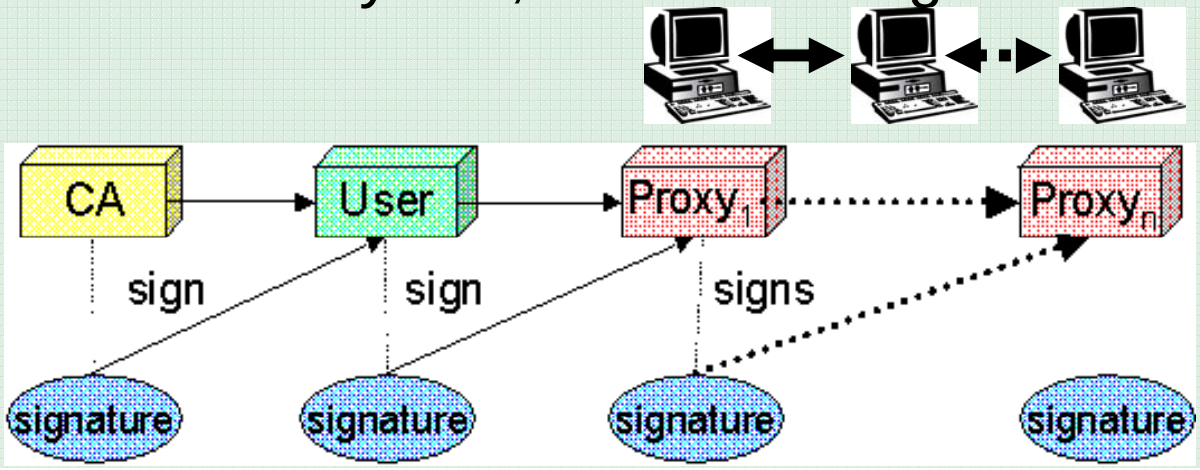


Certification Authorities

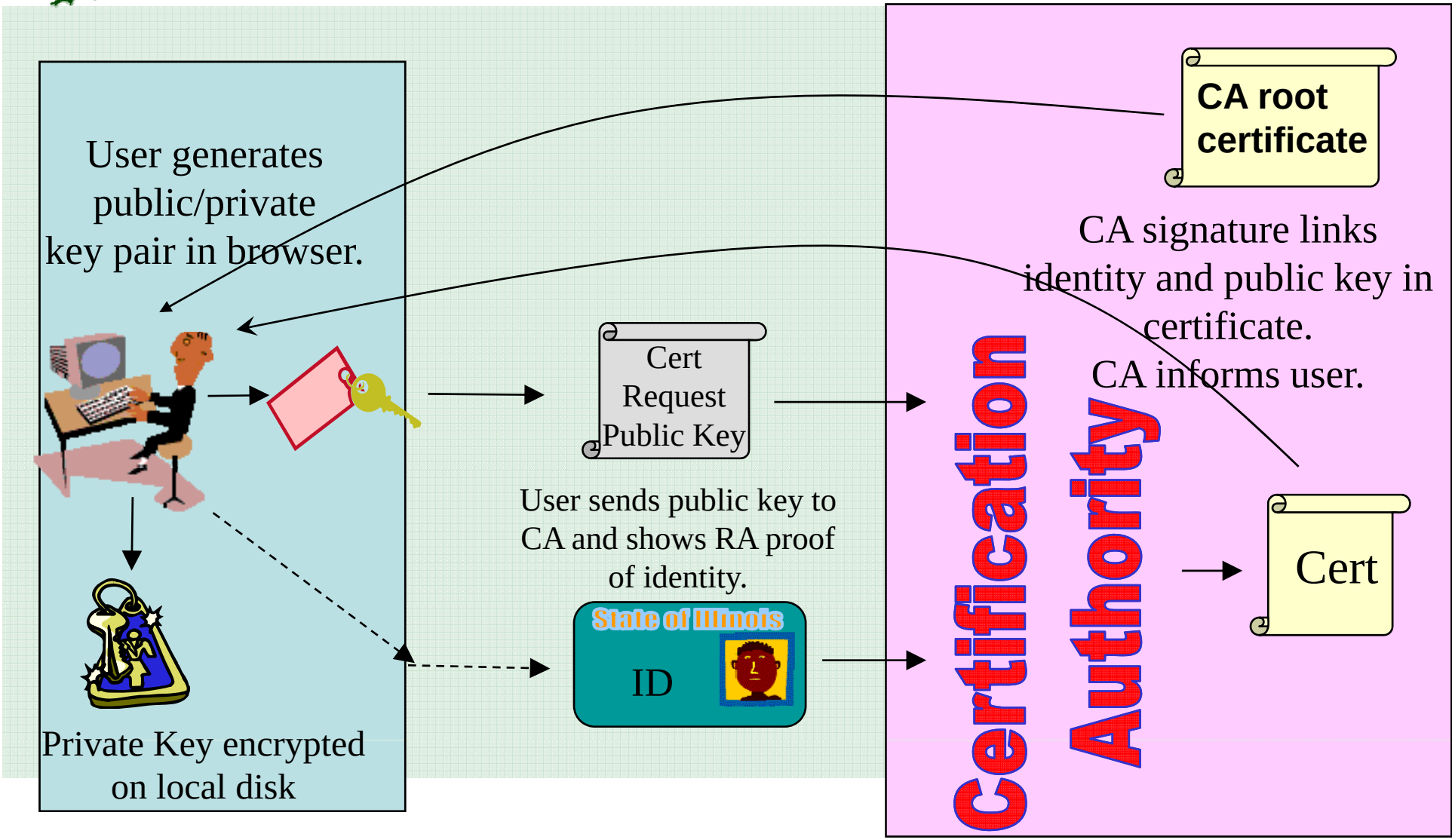
- User's identity has to be certified by one of the national *Certification Authorities* (CAs)
- Resources are also certified by CAs
- CAs are mutually recognized http://www.gridpma.org/,
- CAs each establish a number of people "registration authorities" RAs
- To find RAs in UK go to http://www.grid-support.ac.uk/ca/ralist.htm

Grid Security Infrastructure - proxies

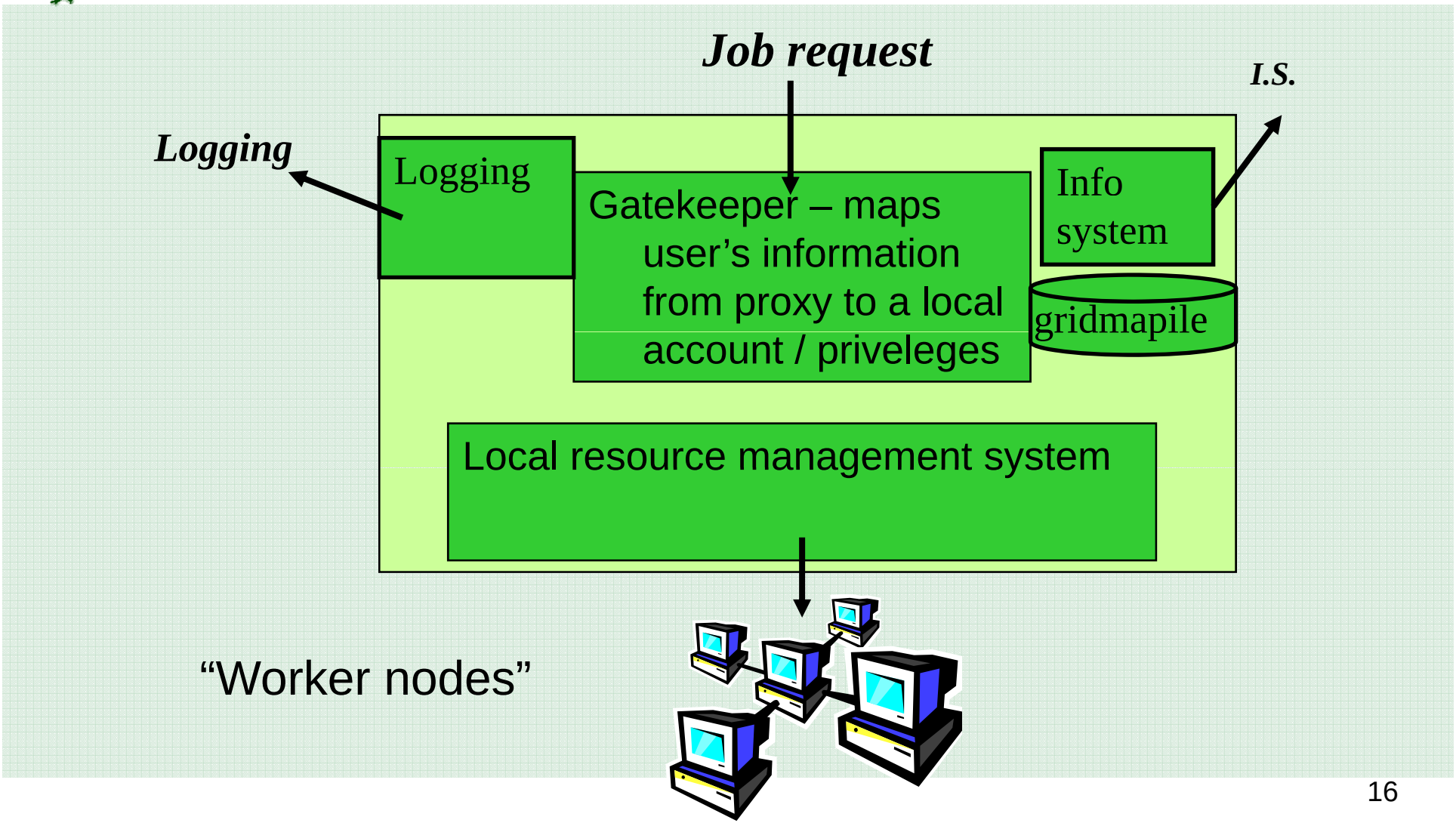
- To support delegation: A delegates to B the right to act on behalf of A
- proxy certificates extend X.509 certificates
  - Short-lived certificates signed by the user's certificate or a proxy
  - Reduces security risk, enables delegation



Certificate Request



Running a job



User Responsibilities

- Keep your private key secure – *on USB drive only*
- Do not loan your certificate to anyone.
- Report to your local/regional contact if your certificate has been compromised.
- Do not launch a delegation service for longer than your current task needs.

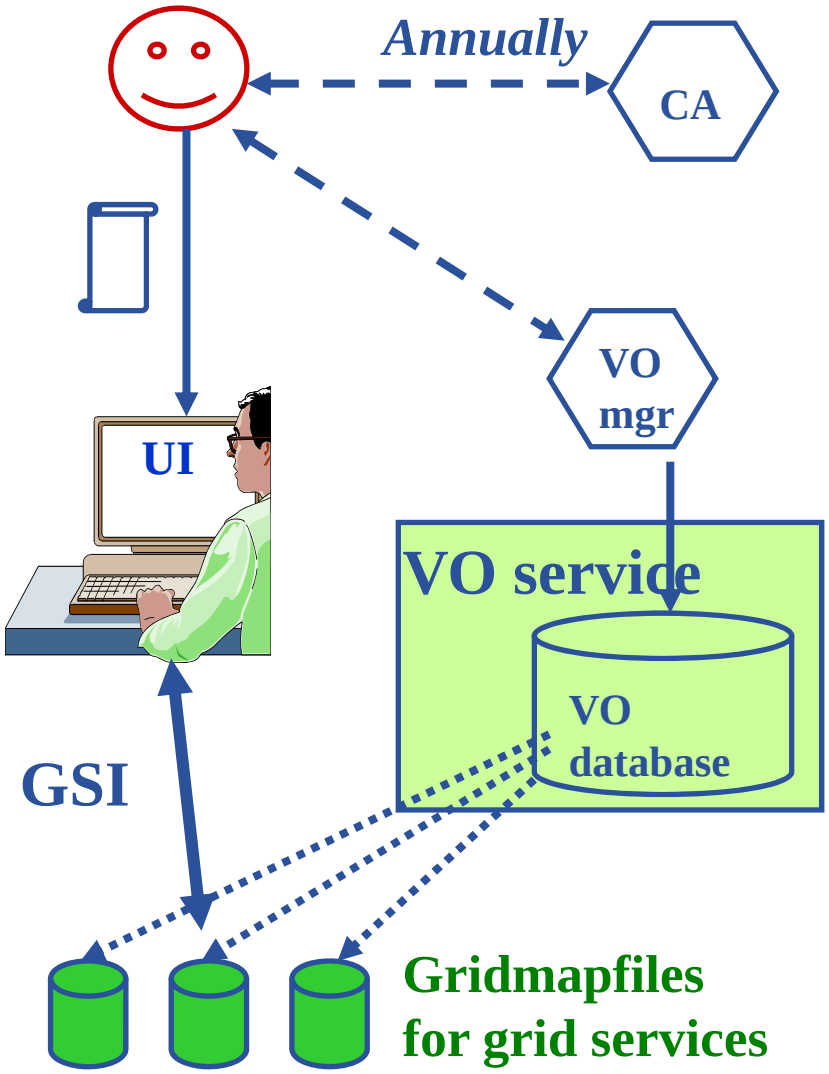
If your certificate or delegated service is used by someone other than you, it cannot be proven that it was not you.

AA Summary

- **Authentication**
  - User obtains certificate from Certificate Authority
  - Connects to UI by gsissh (/ssh) UI is the user's interface to Grid
  - (Uploads certificate to UI)
  - (Single logon – to UI - create proxy)
  - then **Grid Security Infrastructure uses proxies**

- **Authorisation**
  - User joins Virtual Organisation
  - VO negotiates access to Grid nodes and resources
  - Authorisation tested by resource:

Gridmapfile (or similar) maps user to local account



MyProxy Service

- You may need:
  - To interact with a grid from many machines
    - And you realise that you must NOT, EVER leave your certificate where anyone can find and use it….
  - To use diverse grid services and delegating the right for them to act on your behalf
  - To run jobs that might last longer than the lifetime of a short-lived proxy
- MyProxy service holds a long-lived proxy and issues a short-lived proxy when you need one

Connecting to Resources: Tutorial

The Training Certificate Authority

- A fully functional certificate authority for issuing low-assurance certificates
- Low-assurance allows:
  - Certificates issued to local organiser and not the attendee.
  - Attendees do not need to sign UK Terms and conditions of use.
  - Identity checks on attendees are not needed.
- No need for the attendee to do anything pre-event.
- All certificate Distinguished Names (DN's) are known pre-event.
- DN's are of the form "/C=UK//O=Grid/O=Training/CU=NeSC/CN=UserXX" where XX is a two digit number

NGS
National Grid Service

Issued To

Common Name (CN)	User00
Organisation (O)	Grid
Organisational Unit (OU)	NeSC
Serial Number	05:C4

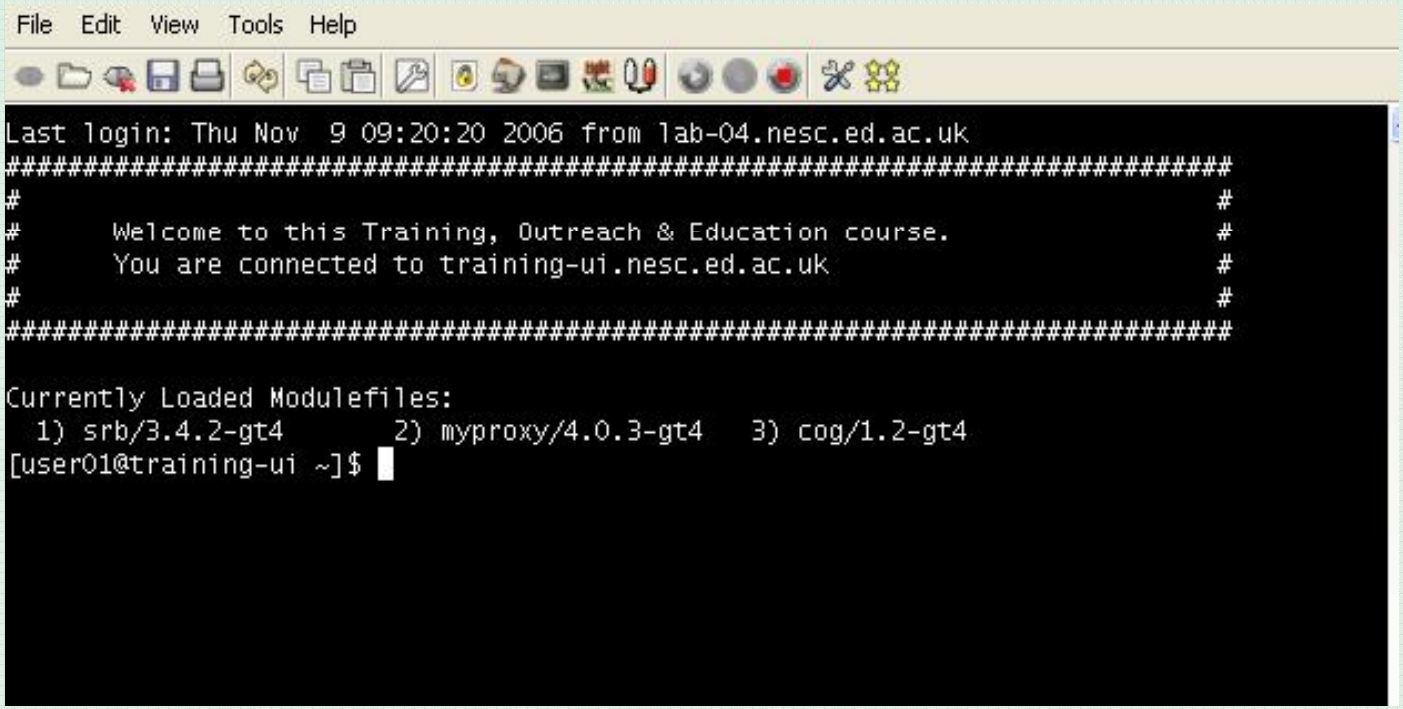
Issued By

Common Name (CN)	Root
Organisation (O)	Grid
Organisational Unit (OU)	Authority

Validity

Issued On	06/01/2008
Expires On	19/01/2008

Java gsissh



- Java ssh tool modified by NGS to include GSI authentication
- Now a sourceforge project
- Run by java web start, as an applet or standalone

What we will be doing

- Trainers have loaded your training certificates into a MyProxy server
- We will be using MyProxy to obtain a proxy for use in any NGS service we access
  - Initially GSISSH from Java

NGS
National Grid Service

First practical

- There is some command-line use on LINUX today – you may prefer to work in pairs
- Lead you through the process of connecting to resources using your certificate

Tutorial Step 2

- Launch gsissh from desktop shortcut.
- File then New Connection
- Connect to “training-ui.nesc.ed.ac.uk”

1. Username: userNN, where NN is a user number I give you
2. Passphrase – on whiteboard
3. Click “Use MyProxy”

Last step

grid-proxy-info - to see information about the proxy in your terminal.

```
[user00@training-ui ~]$ grid-proxy-info
subject  : /C=UK/O=Grid/O=Training/OU=NeSC/CN=User00/CN=1499174244/CN=427269680/
CN=1853652565/CN=772320611
issuer   : /C=UK/O=Grid/O=Training/OU=NeSC/CN=User00/CN=1499174244/CN=427269680/
CN=1853652565
identity : /C=UK/O=Grid/O=Training/OU=NeSC/CN=User00
type     : Proxy draft (pre-RFC) compliant impersonation proxy
strength : 512 bits
path     : /tmp/x509up_p27280.fileeju5Eo.1
timeleft : 11:57:40
```

Note also: Tools->sftp allows you to transfer files to/from local workstation

NGS
National Grid Service

Now…..

- Connect using gsissh to an Oxford node

gsissh -p 2222 ngs.oerc.ox.ac.uk

- Look at the proxy – see its issued by the one on training-ui

grid-proxy-info

Then ^D to log out from Oxford and leave your session on training-ui open.

NGS
National Grid Service

So far….

- Seen proxy certificates in use to create a terminal session on remote machines
- GSI permits
  - identity to be communicated
  - Message source/destination to be known with confidence
  - Message integrity to be checked
- Java GSISSH allows terminal sessions to be established and supports file transfer to/from desktop

Building on Globus

- The Globus toolkit is the basis of (almost all) the compute services on the NGS
- On training-ui run the following: (all on one line)

globus-job-run ngs.oerc.ox.ac.uk/jobmanager-pbs /bin/hostname –f

This shows a simple command being executed on a worker node of the cluster in Oxford, using your proxy certificate to again access.