NGS National Grid Service
http://www.ngs.ac.uk

NW-GRID

Security, Authorisation and Authentication

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

PPARC
http://www.pparc.ac.uk/

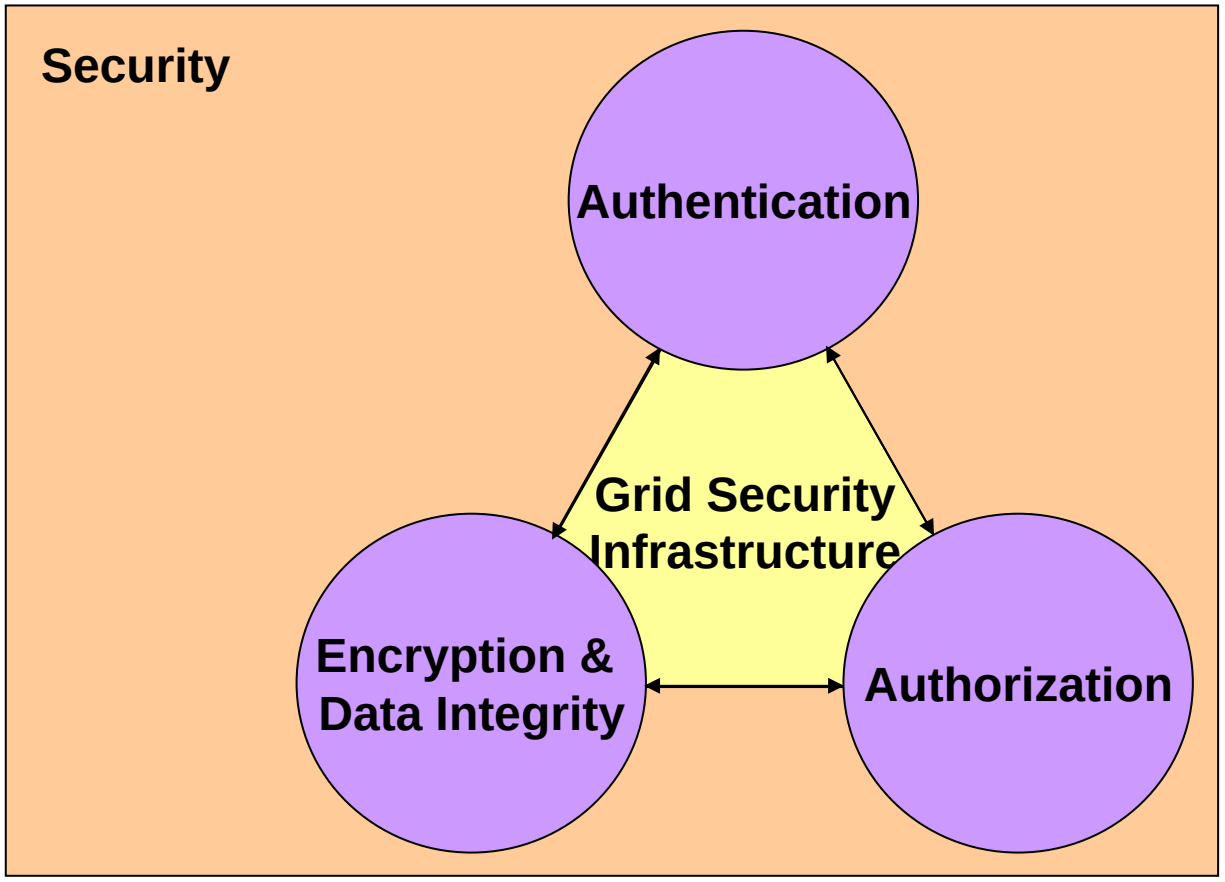
Edinburgh e-Science TOE Training Outreach and Education
http://www.nesc.ac.uk/training

eGee
http://www.eu-egee.org/

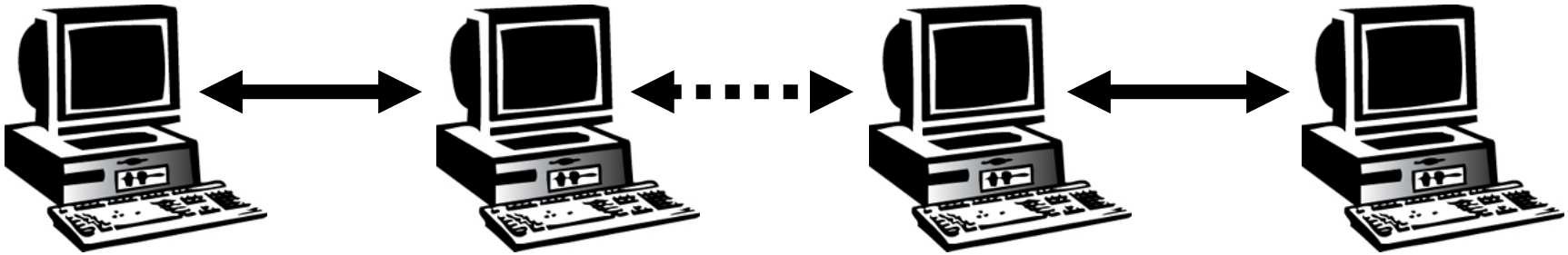
Policy for re-use

- 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!!

Security Overview



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?

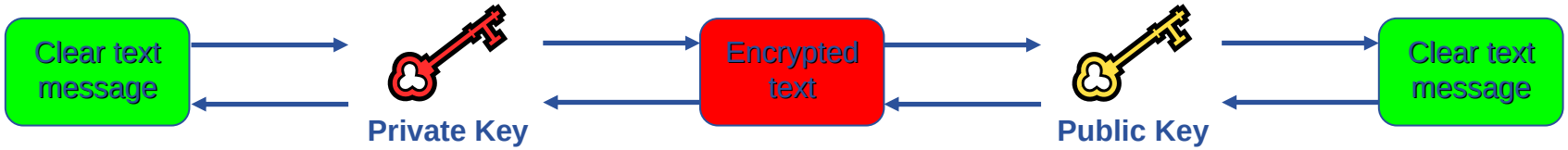
- How does the Resource know who a user is?
- How are rights and that they are allowed access?

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…**

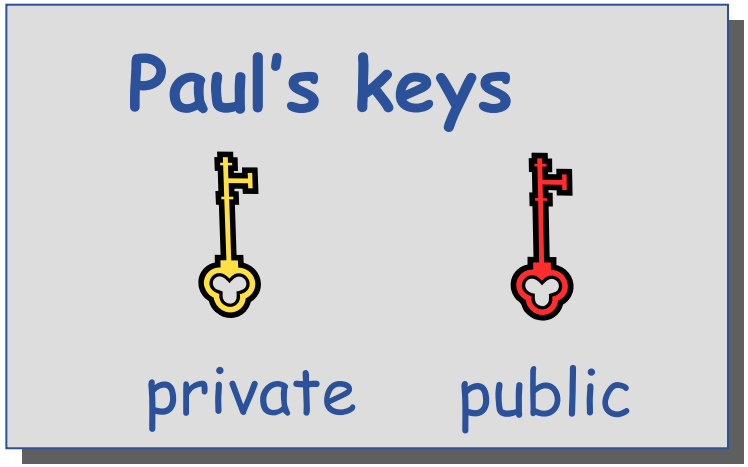


- **…. and Digital signatures …**
  - A hash derived from the message and encrypted with the signer's private key
  - Signature is checked by decrypting with the signer's public key

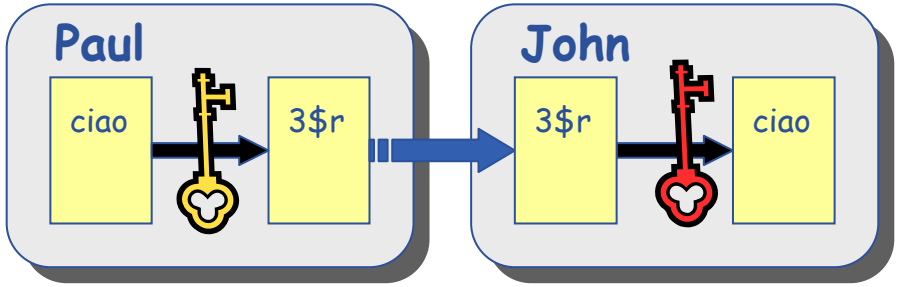
- **Are used to build trust**
  - That a user / site is who they say they are
  - And can be trusted to act in accord with agreed policies

Public Key Algorithms

- **Every user has two keys: one *private* and one *public*:**
  - it is *impossible* to derive the private key from the public one;
  - a message encrypted by one key can be decrypted **only** by the other one.

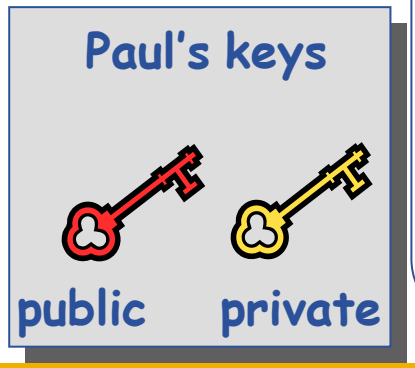


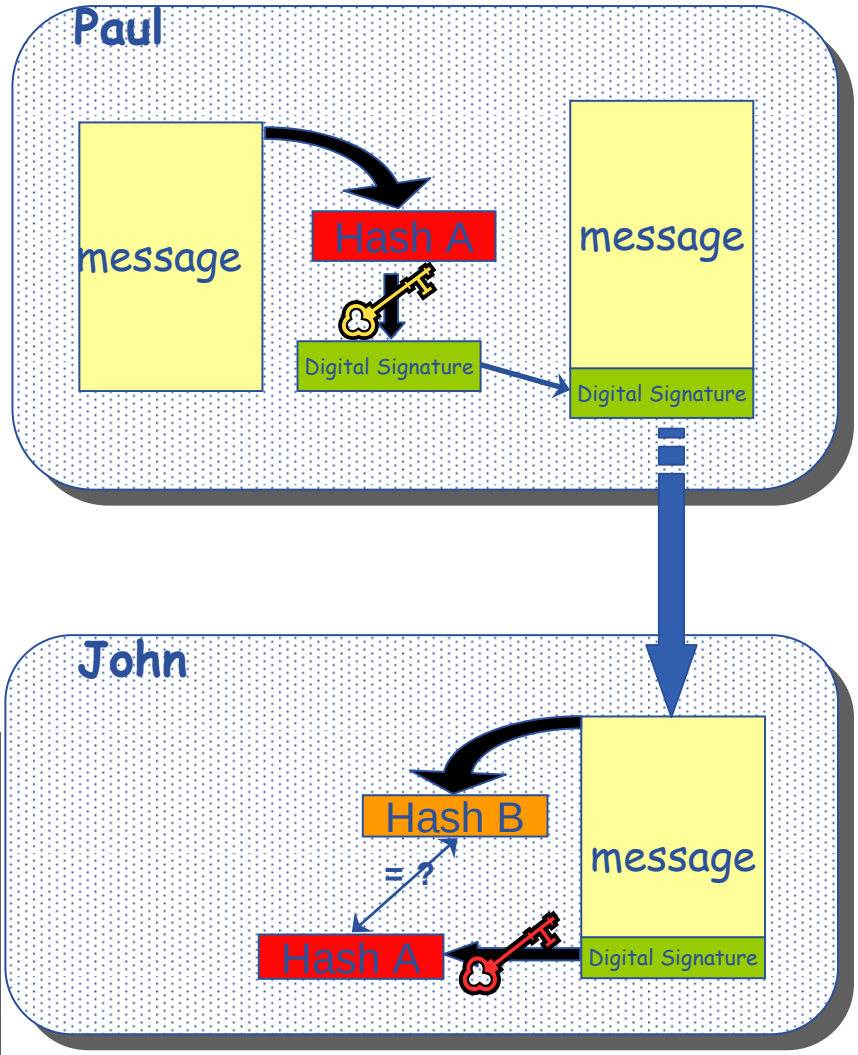
- **Public keys are exchanged**
- **The sender encrypts using his private key**
- **The receiver decrypts using senders public key;**
- **The number of keys is O(n)**



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

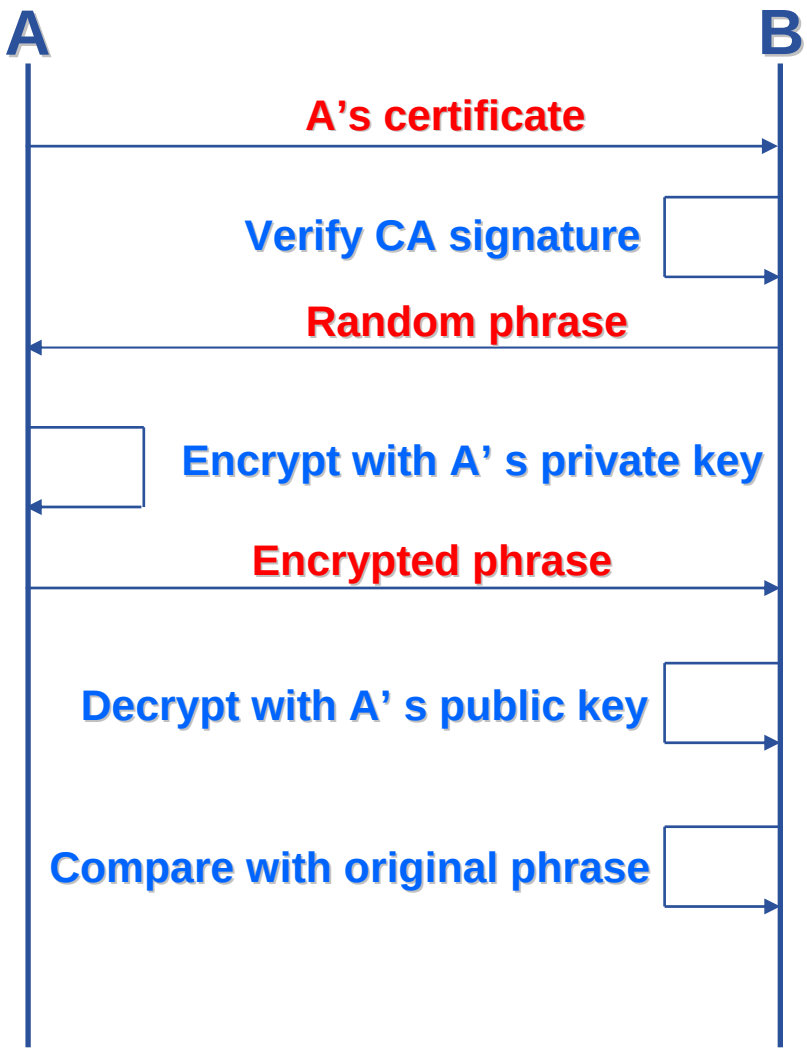




The Grid Security Infrastructure (GSI)

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



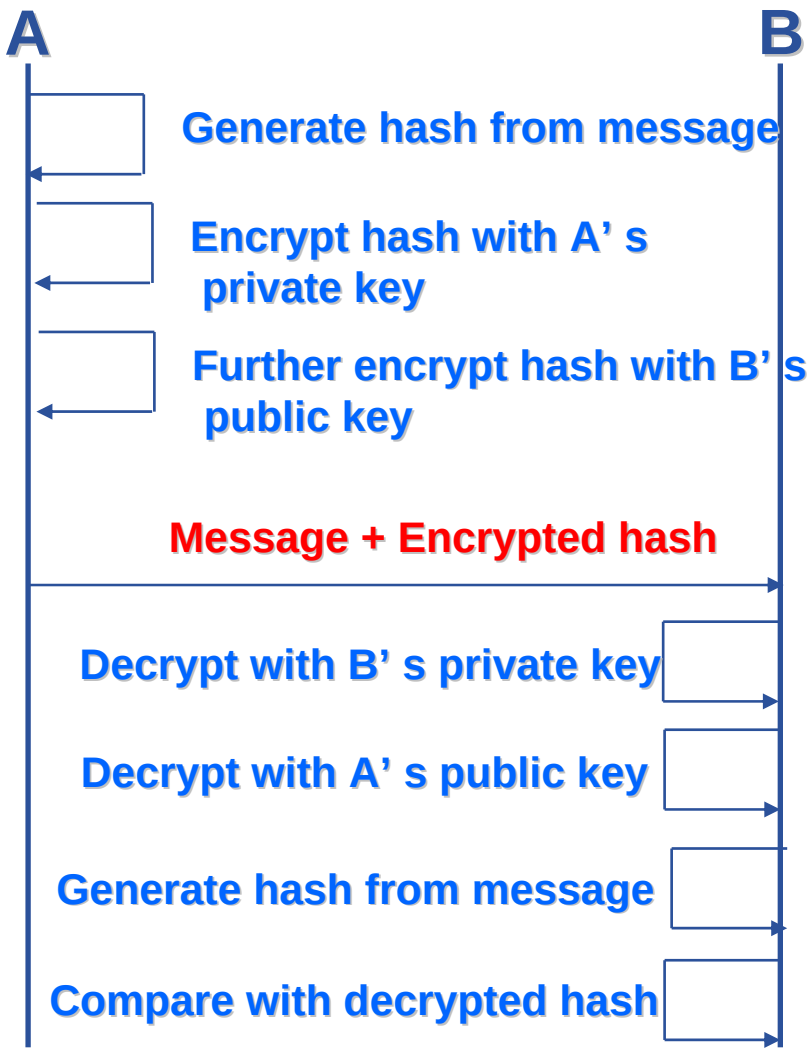
The Grid Security Infrastructure (GSI) - continued

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



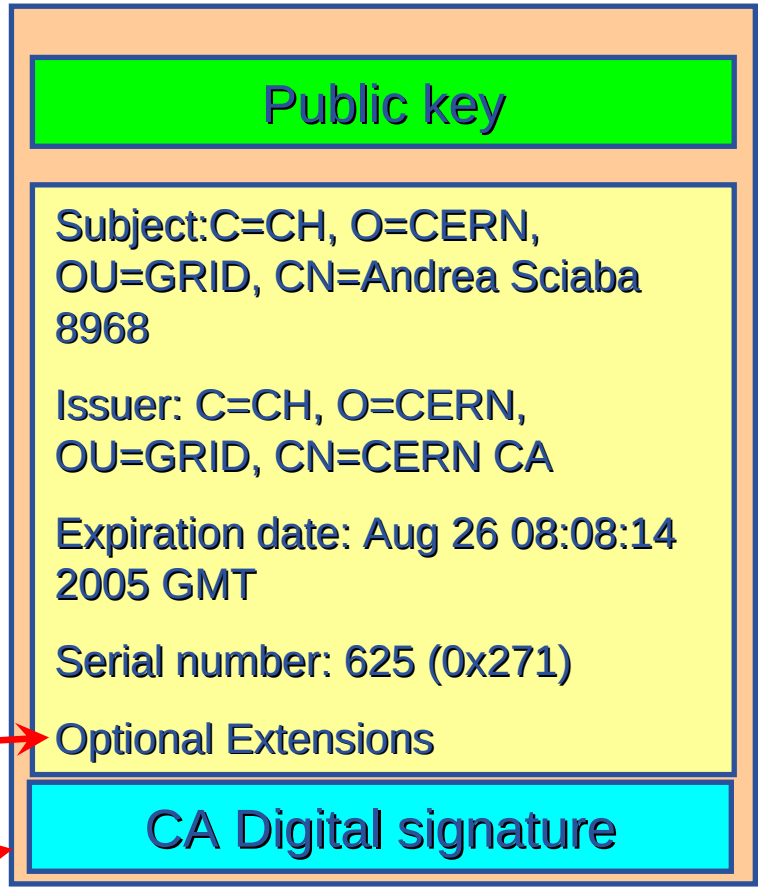
Digital Certificates

- **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

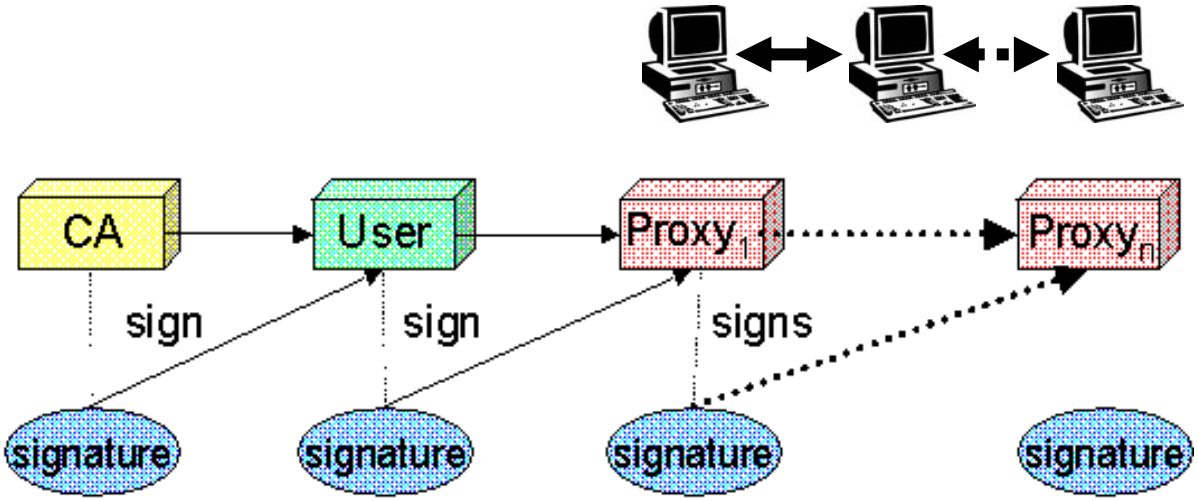


Certification Authorities

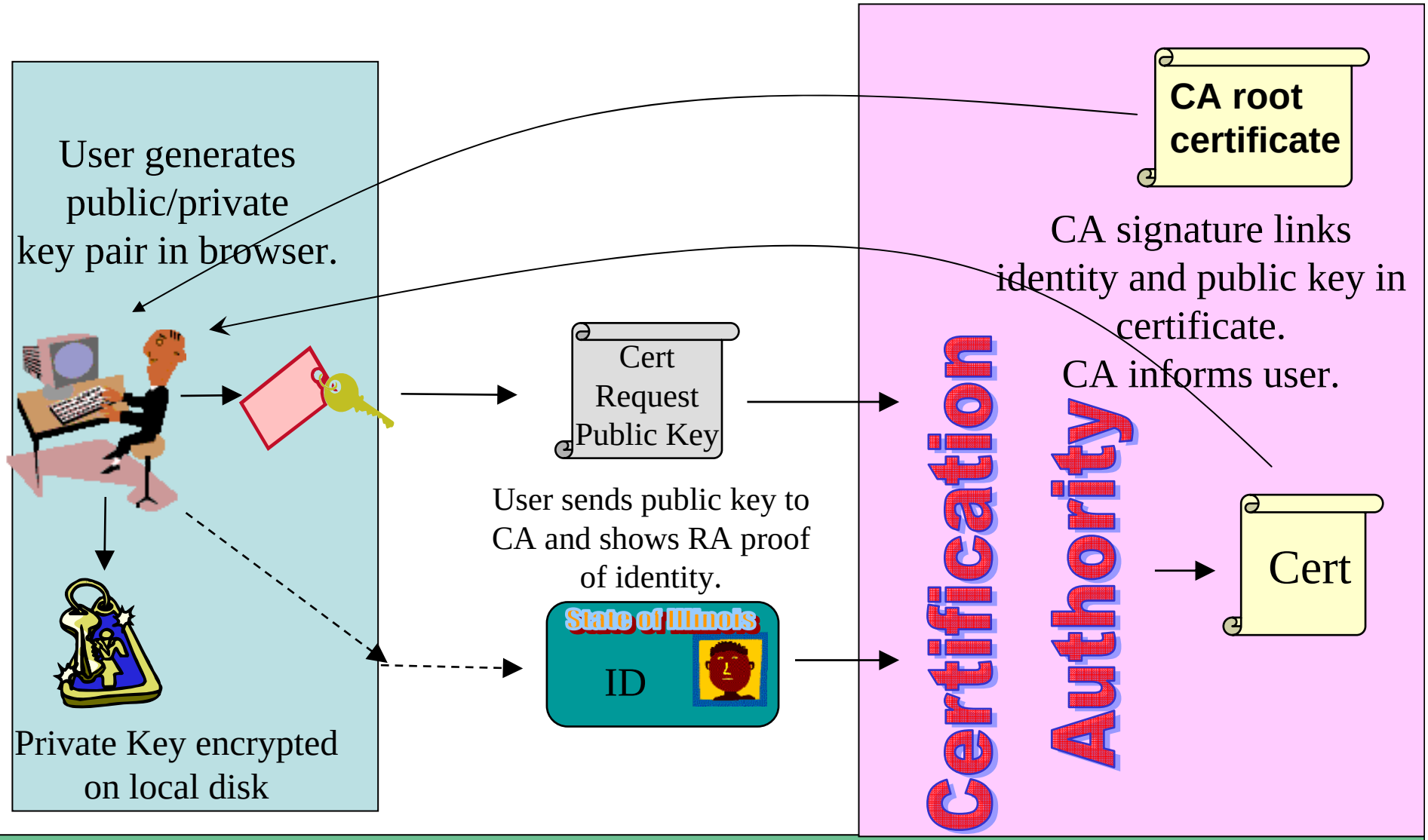
- User's identity has to be certified by one of the national *Certification Authorities* (CAs)
- Resources are also certified by CAs
- CAs are mutually recognized http://www.gridpma.org/,
- CAs each establish a number of people "registration authorities" RAs
- To find RAs in UK go to http://www.grid-support.ac.uk/ca/ralist.htm

Grid Security Infrastructure - proxies

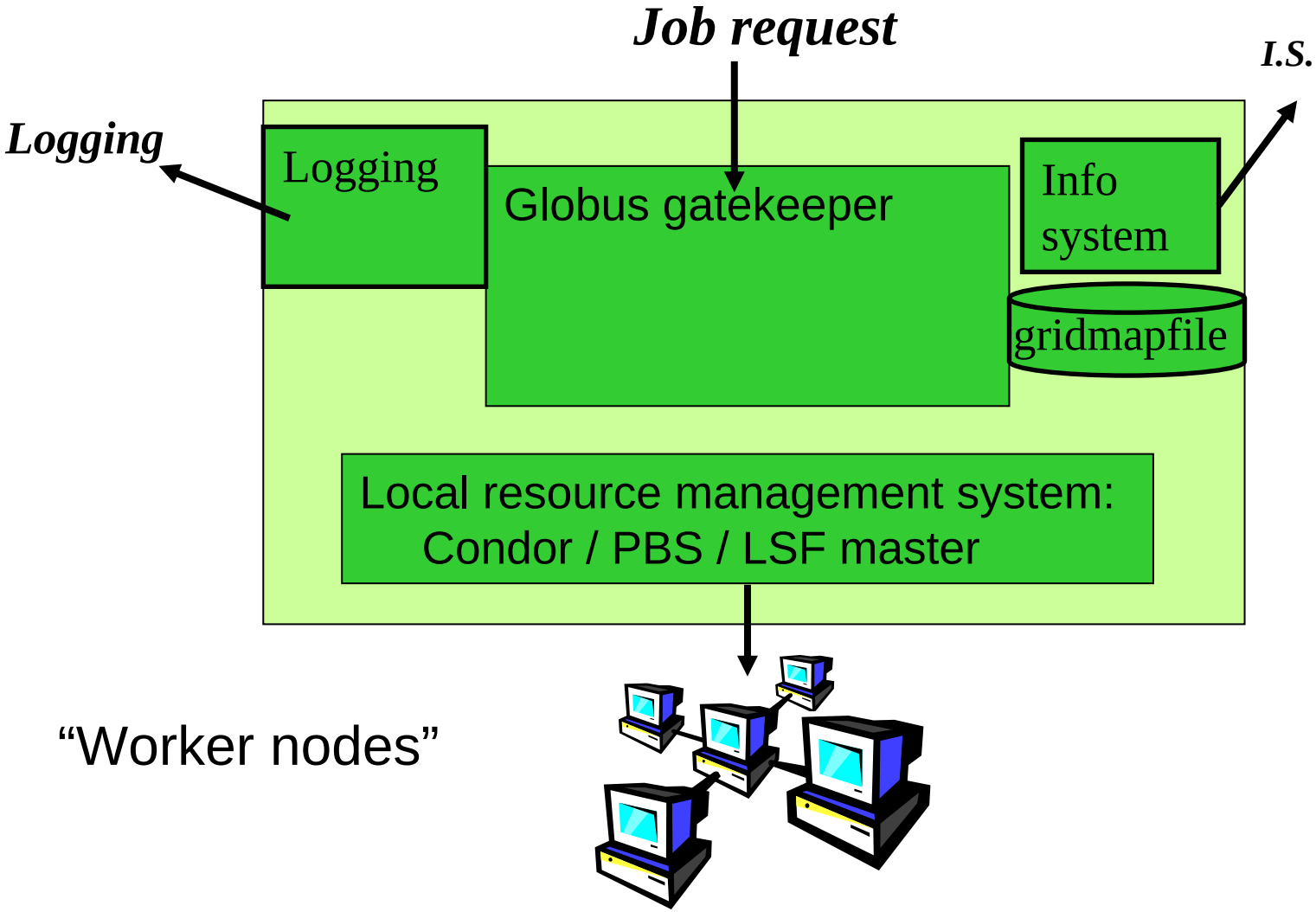
- To support delegation: A delegates to B the right to act on behalf of A
- proxy certificates *extend X.509 certificates*
  - Short-lived certificates signed by the user's certificate or a proxy
  - Reduces security risk, enables delegation



Certificate Request



"Compute element": An LRMS queue



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