http://www.grid-support.ac.uk

http://www.ngs.ac.uk

Using the National Grid Service

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

National e-Science Centre
http://www.nesc.ac.uk/

JISC

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

e-Science
dti

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

Policy for re-use

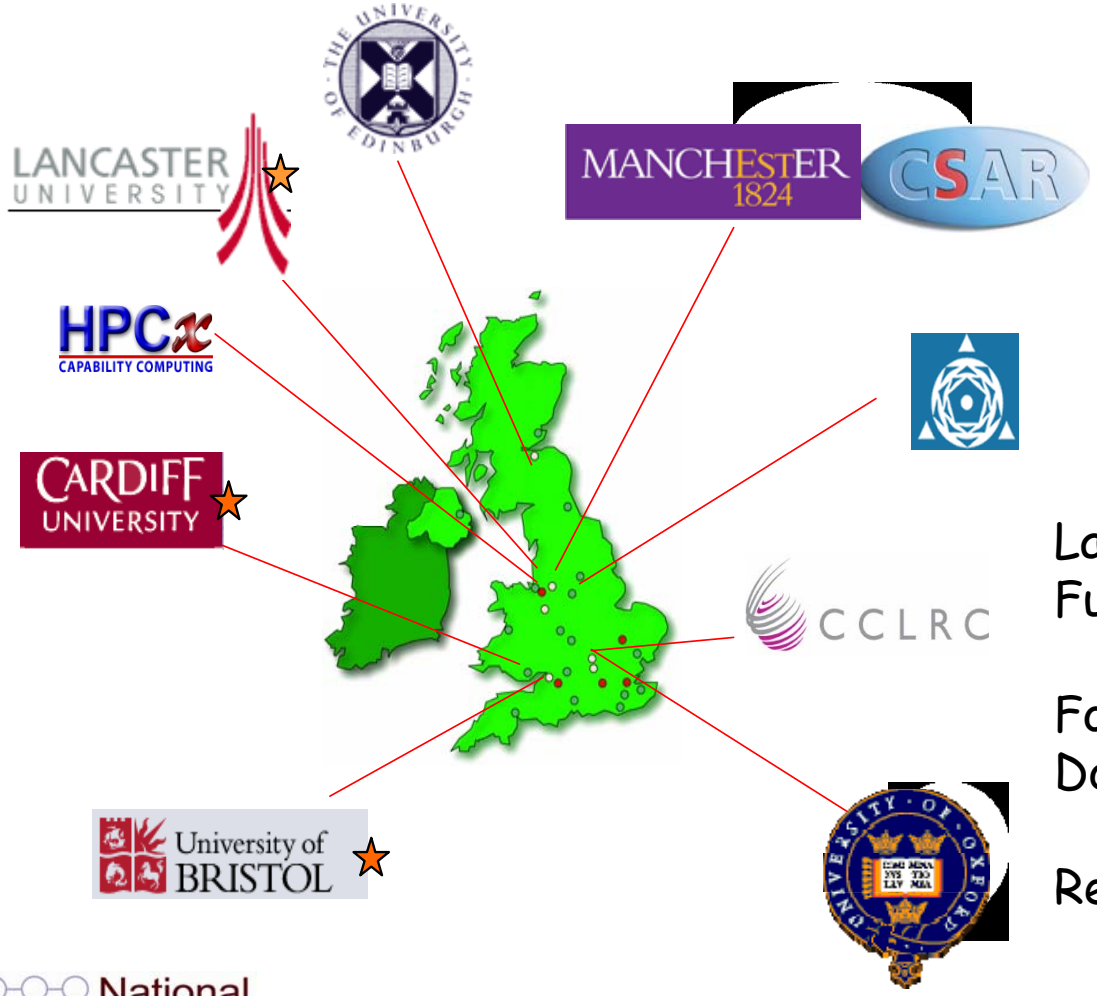
- This presentation can be re-used for academic purposes.

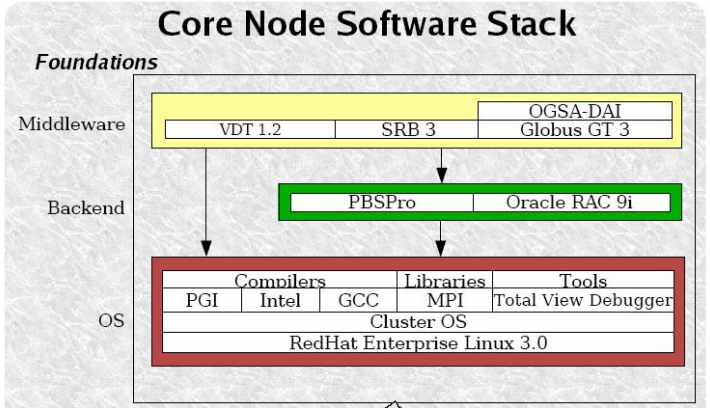
- However if you do so then please let training-support@nesc.ac.uk know. We need to gather statistics of re-use: no. of events, number of people trained. Thank you!!

The National Grid Service

- The core UK grid, resulting from the UK's e-Science programme.
  - Grid: virtual computing across admin domains
- Production use of computational and data grid resources.
- Supported by JISC, and is run by the Grid Operations Support Centre (GOSC).

The National Grid Service





Launched April 2004
Full production - September 2004

Focus on deployment/operations
Do not do development

Responsive to users needs

National e-Science Centre

Today's agenda

Practicals using the National Grid Service

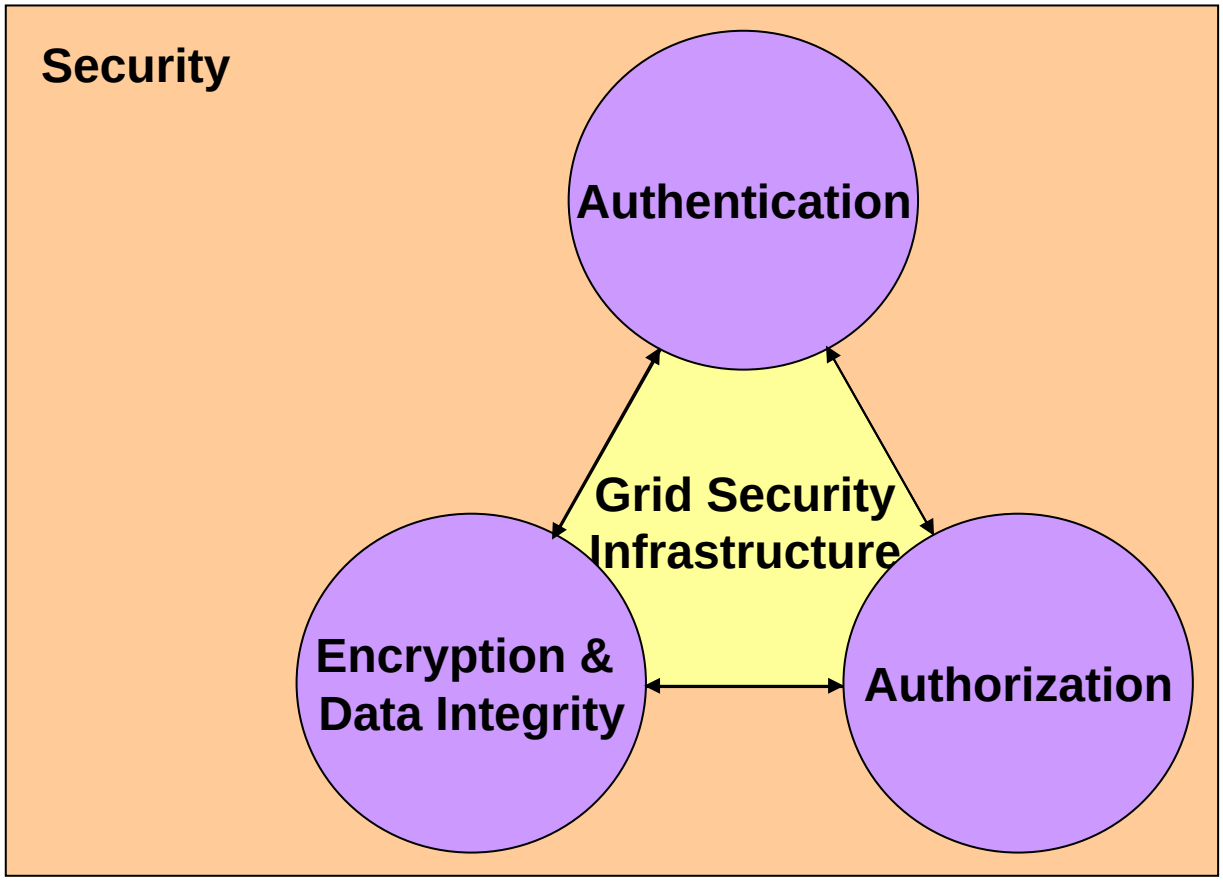
1. Security
2. Job submission
3. Data management

Case studies

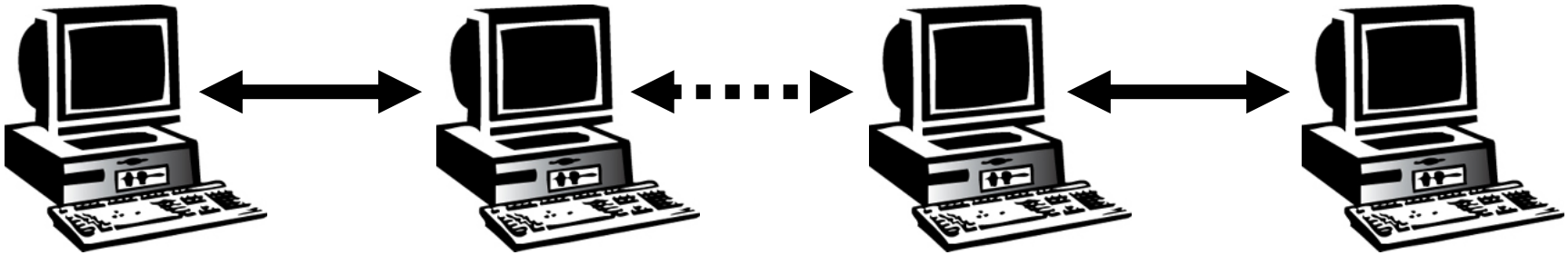
- myGrid
- RealityGrid

Security on the NGS

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?

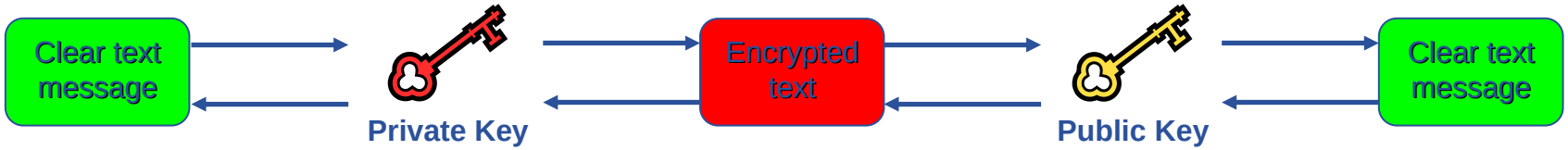
- How does the Resource know who a user is?
- How are rights and that they are allowed access?

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…**

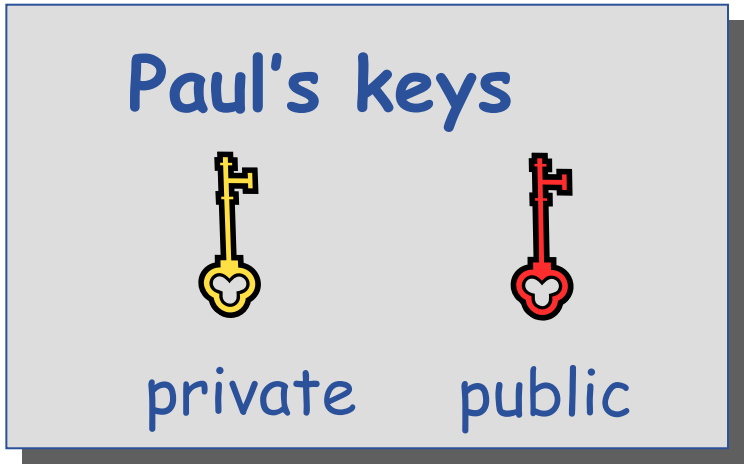


- **…. and Digital signatures …**
  - A hash derived from the message and encrypted with the signer's private key
  - Signature is checked by decrypting with the signer's public key

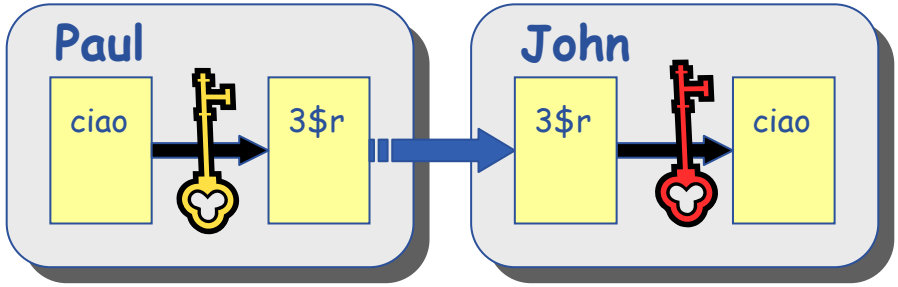
- **Are used to build trust**
  - That a user / site is who they say they are
  - And can be trusted to act in accord with agreed policies

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.

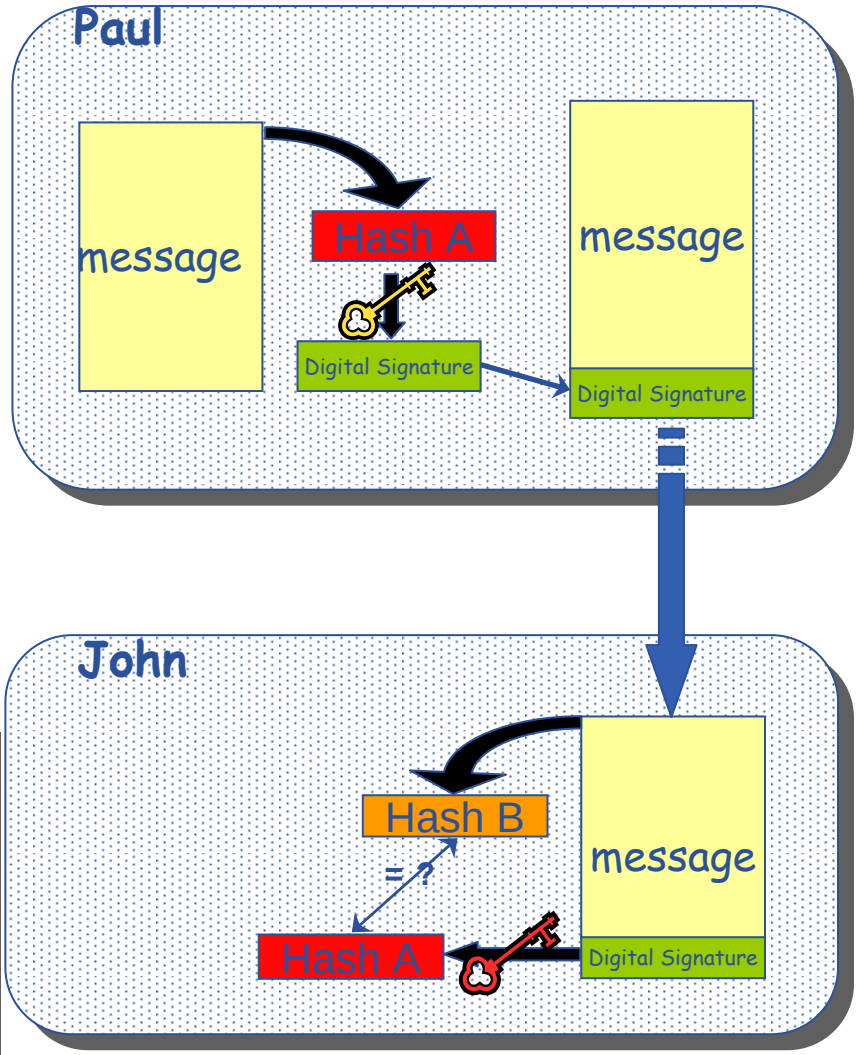


- **Public keys are exchanged**
- **The sender encrypts using his private key**
- **The receiver decrypts using senders public key;**
- **The number of keys is O(n)**



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



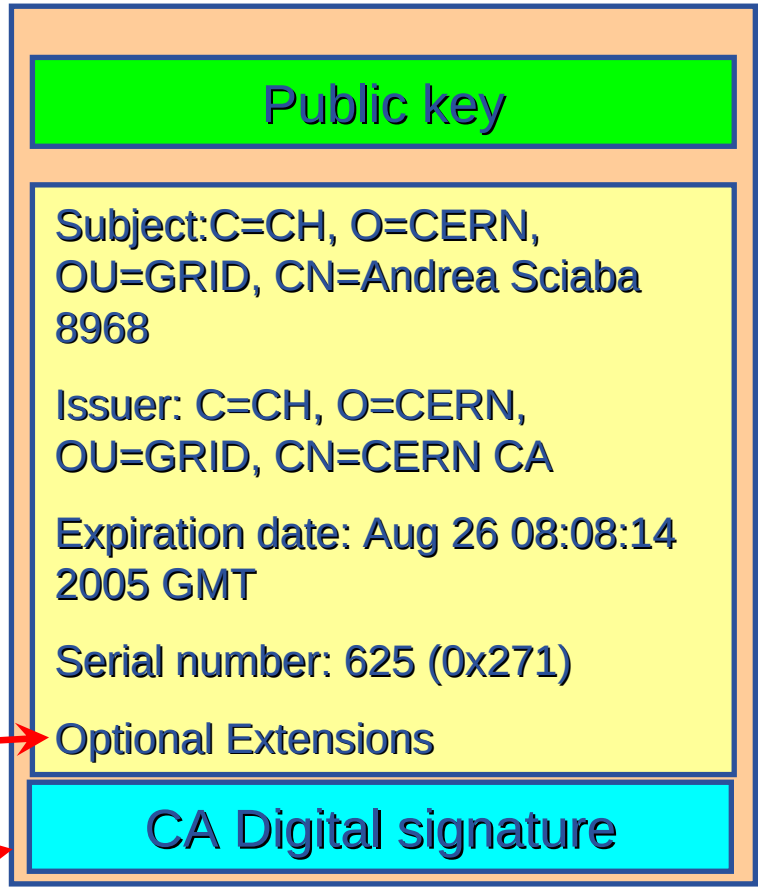
Digital Certificates

- **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

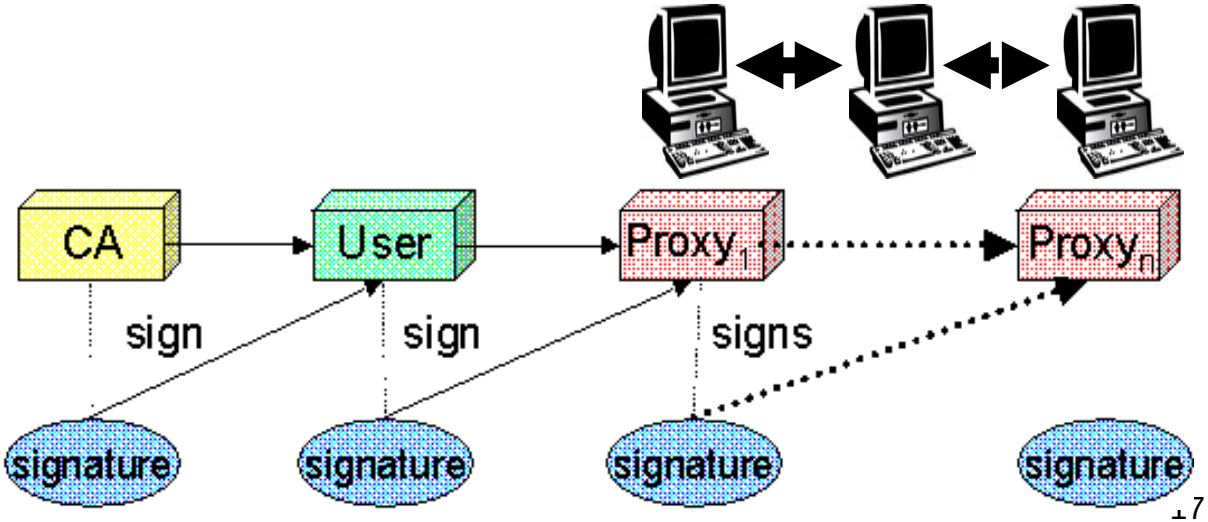
- User's identity has to be certified by one of the national *Certification Authorities* (CAs)
- Resources are also certified by CAs
- CAs are mutually recognized http://www.gridpma.org/,
- CAs each establish a number of people "registration authorities" RAs
- To find RAs in UK go to http://www.grid-support.ac.uk/ca/ralist.htm

RA list

	Owen J E Maroney	
Lancaster University (LeSC)	Mike Pacey	Lancaster LeSC
Lancaster University (Physics)	Alexander Finch	Lancaster Physics
Leeds University	Stephen Corbett Barbara Edmondson Jitesh Rathod	Leeds ISS
Leicester University	*No active operators**	Leicester Physics
Liverpool University	Clifford Addison Smith Ian	Liverpool CSD
Liverpool University	*No active operators**	Liverpool Physics
Manchester Metropolitan University	Ian Cook	ManchesterMet ISU
Manchester University (HEP)	Alessandra Forti Colin Morey Andrew Mcnab Sabah Salih	Manchester HEP
Manchester University (MC)	Michael Jones Mark Mc Keown	Manchester MC
NERC (CEH)	Sebastian Adams Nicolas Bertrand Paul Burnett	NERC CEH
NERC (POL)	Dave Cable	NERC POL
NERC (SO)	*No active operators**	NERC SO
NeSC, Edinburgh	Dave Berry David Mcnicol Jeremy Nowell Charaka Palansuriya Steve Thorn	Edinburgh NeSC
Newcastle University	Mark Hewitt	Newcastle NERoSC

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



User Responsibilities

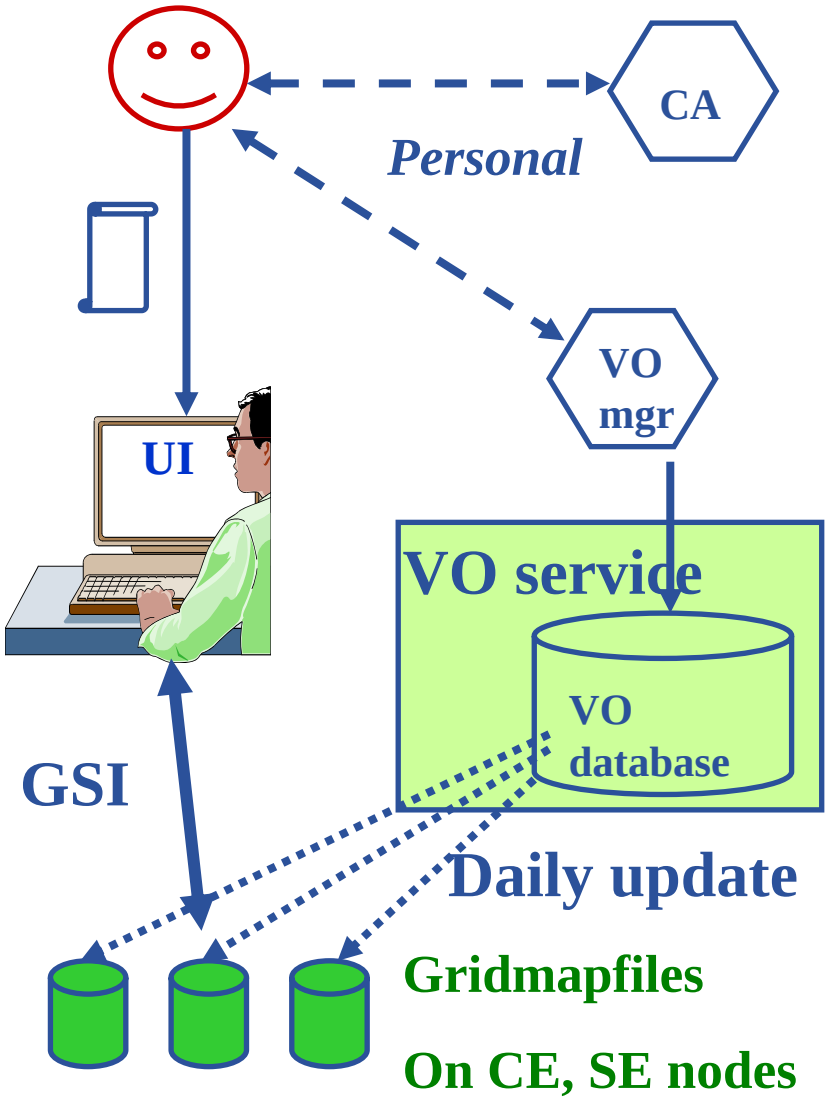
- Keep your private key secure.
- Do not loan your certificate to anyone.
- Report to your local/regional contact if your certificate has been compromised.
- Do not launch a delegation service for longer than your current task needs.

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

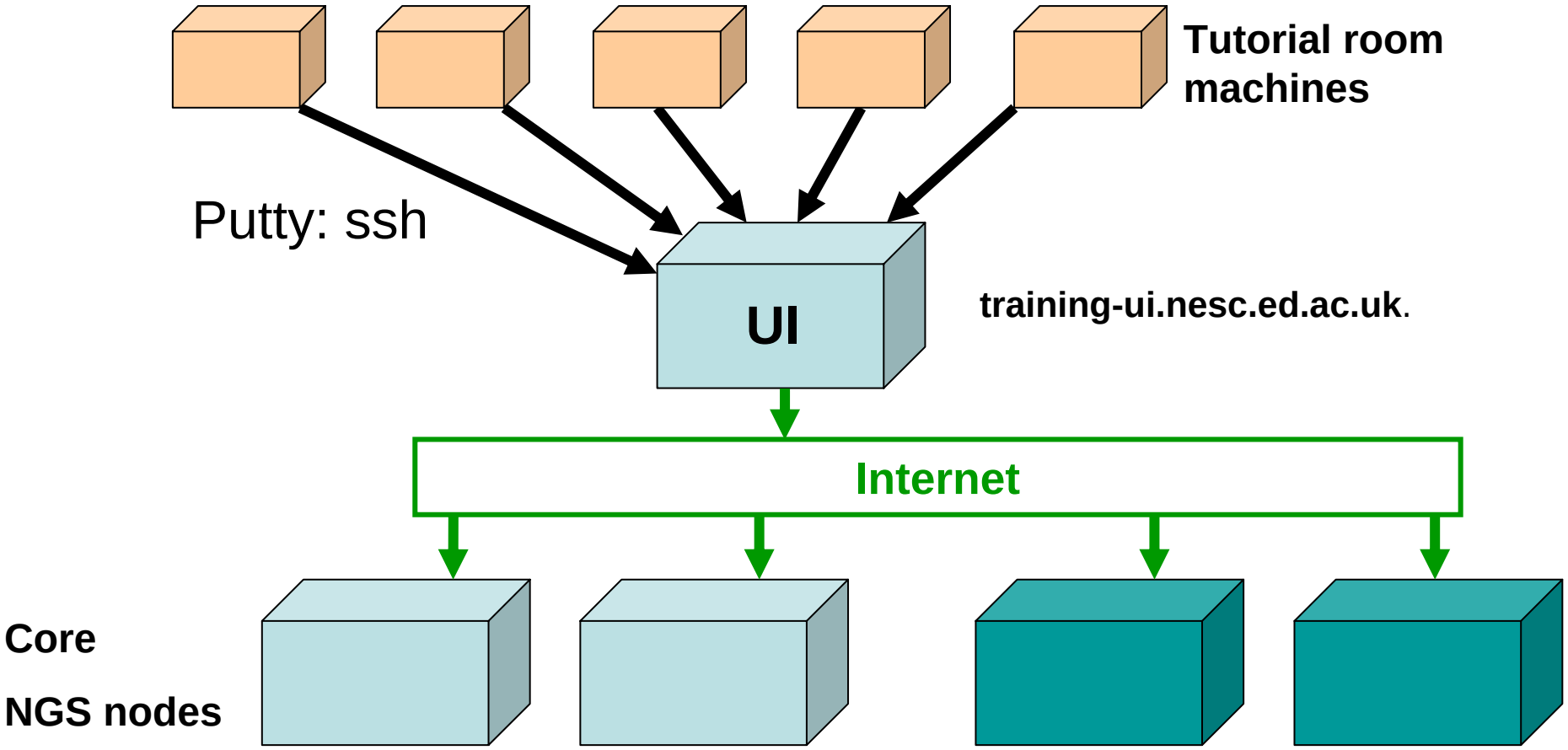
Summary

- **Authentication**
  - User obtains certificate from Certificate Authority
  - Connects to UI by ssh
  - Downloads certificate
  - Single logon – to UI - create proxy
  - then **Grid Security Infrastructure uses proxies to identify users to other machines**
- **Authorisation**
  - User joins Virtual Organisation
  - VO negotiates access to Grid nodes and resources (CE, SE)
  - Authorisation tested by CE, SE:

gridmapfile maps user to local account



Our setup


Tutorial room machines
Putty: ssh
UI
training-ui.nesc.ed.ac.uk.
Internet
Core
NGS nodes

The Practical

- You should have been given an information sheet containing your username and password

1. Login to your workstation
2. Open a browser window and follow the link from http://agenda.cern.ch/fullAgenda.php?ida=a06578
3. Click on the “further information” for *this* practical.
4. Follow instructions to use the putty program to connect to training-ui.nesc.ed.ac.uk
    1. Accept key when prompted by training-ui