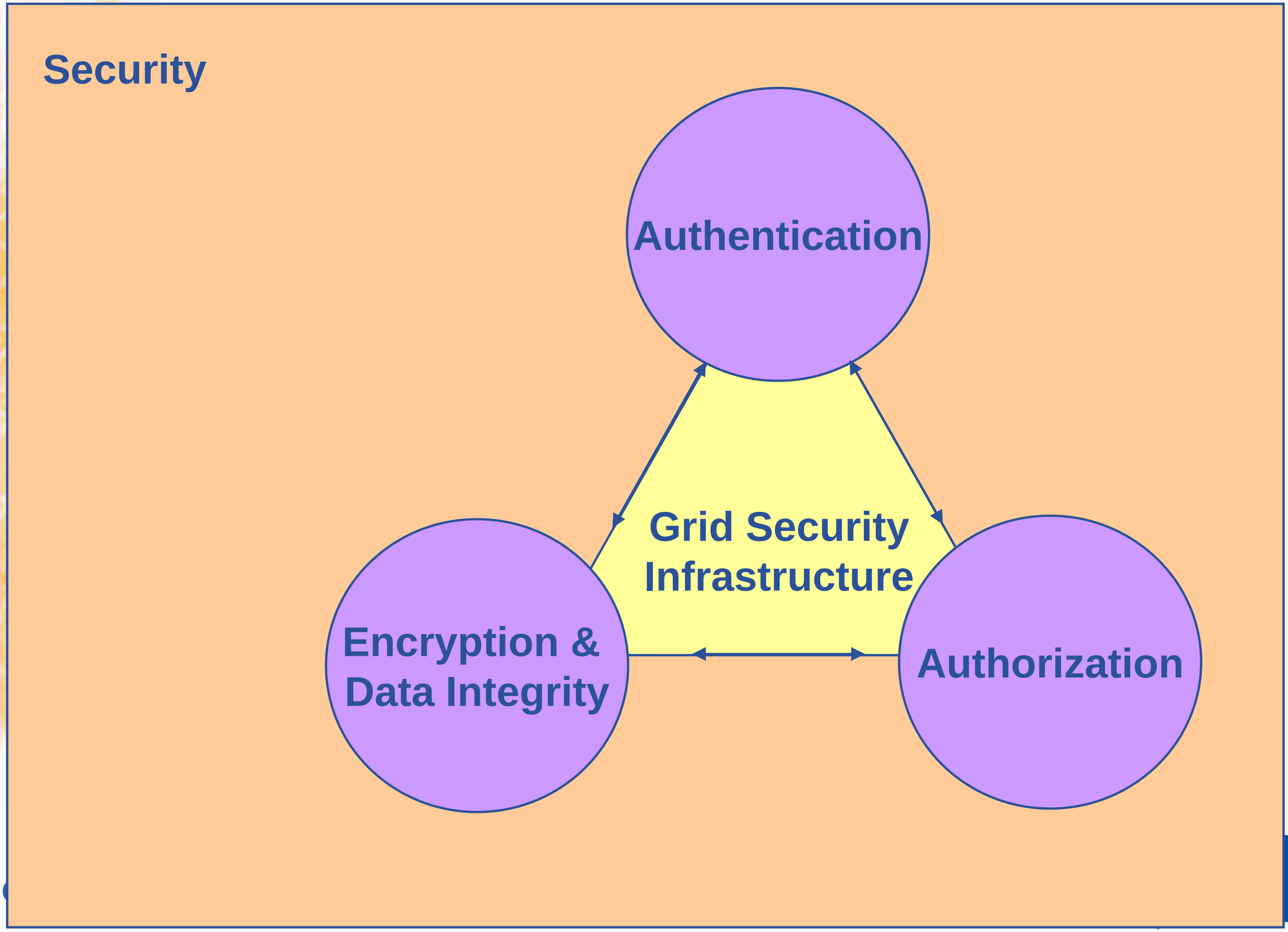
Grid Security

Jinny Chien

Academia Sinica Grid Computing

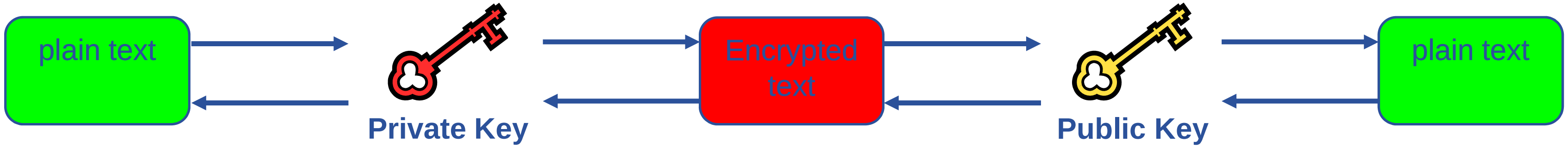
www.eu-egee.org

Security in gLite



Basis of security & authentication

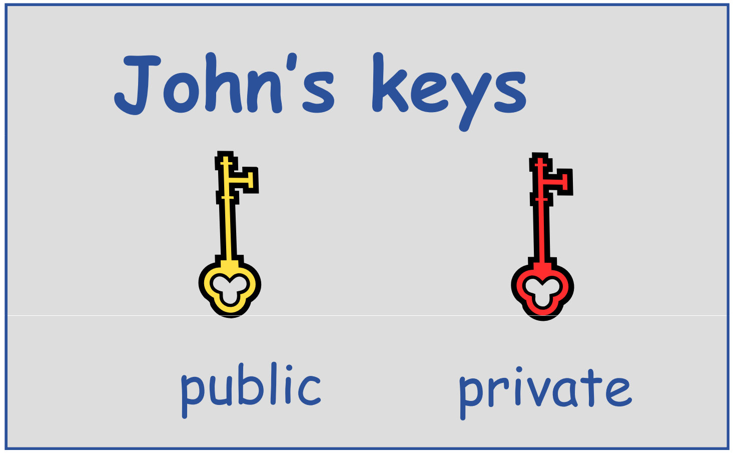
- **Symmetric encryption**
- **Asymmetric encryption…(Public Key Infrastructure)**

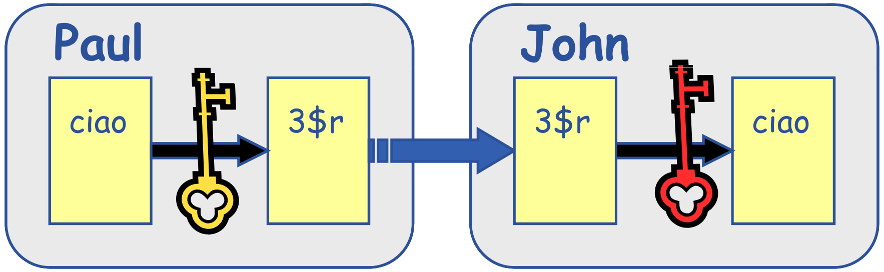


- Private key and public key are in pair.
  - it is *impossible* to derive one key from another key.
- a message encrypted by one key can be decrypted **only** by another one.

An Example of Asymmetric Encryption

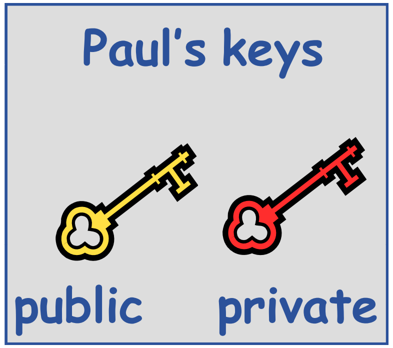
- **Public keys are exchanged**
  - Paul gets John’s public key..
- **Paul encrypts using the *public* key of John**
- **John decrypts using his *private* key;**
- **Public key algorithm: Make sure of data confidentiality**

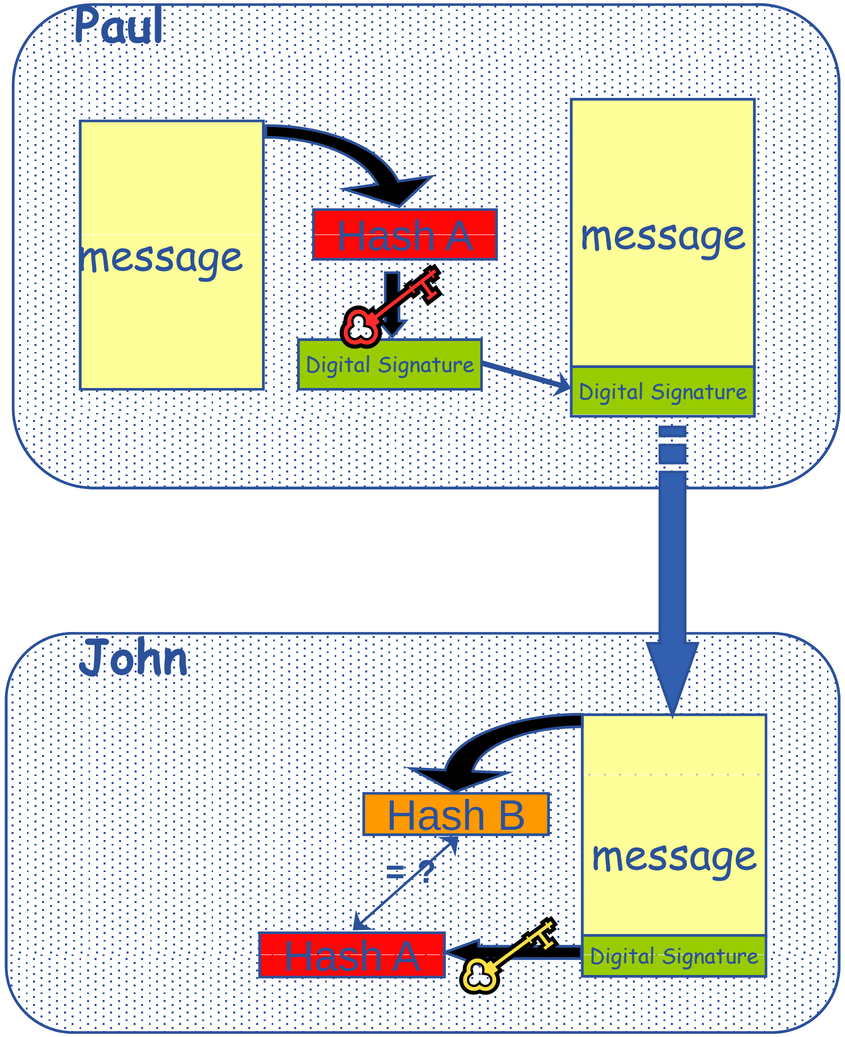




Digital Signature

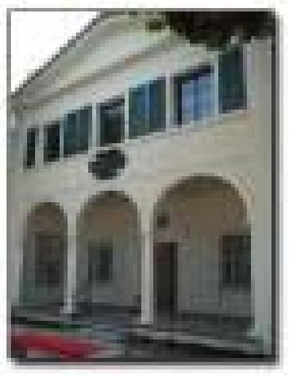
- Paul **calculates the** *hash* **of the message**
- Paul **encrypts the hash using his** *private* **key: the encrypted hash is the** *digital signature*.
- Paul **sends the signed message to** John.
- John **calculates the hash of the message**
- **Decrypts signature, to get Hash A, using Paul's**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



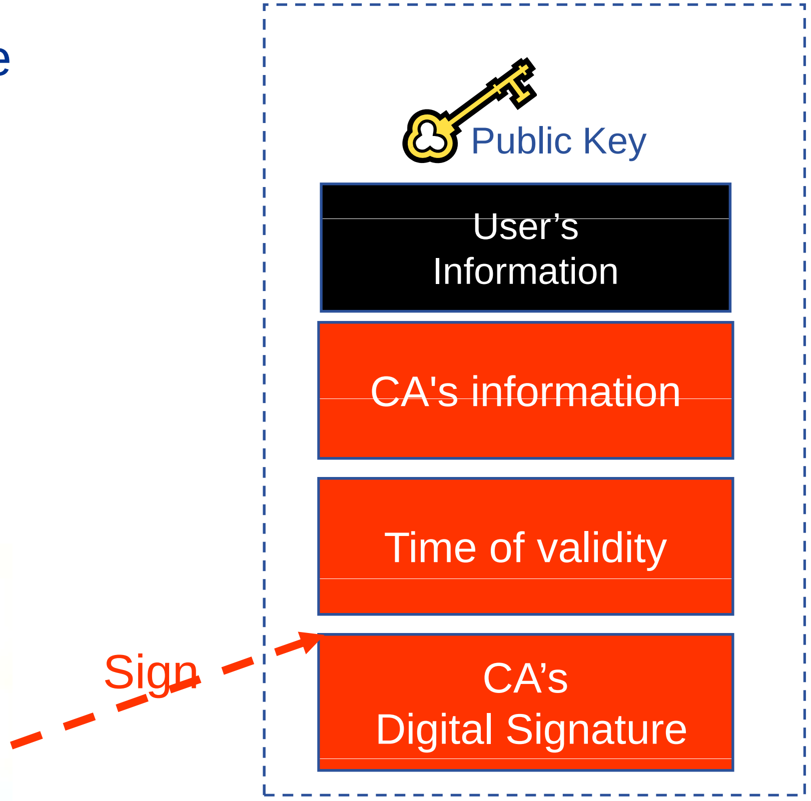


Certificate

- **Certificate**
  - It is based on Digital Signature mechanism.
  - Grid authenticates users or resources by verifying their certificate.
  - Certificate is issued by one of the national *Certification Authorities*.



***Certification Authorities*. CA**



Sign

Public Key

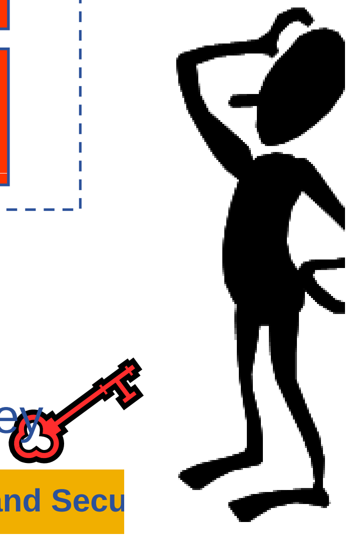
User's Information

CA's information

Time of validity

CA's Digital Signature

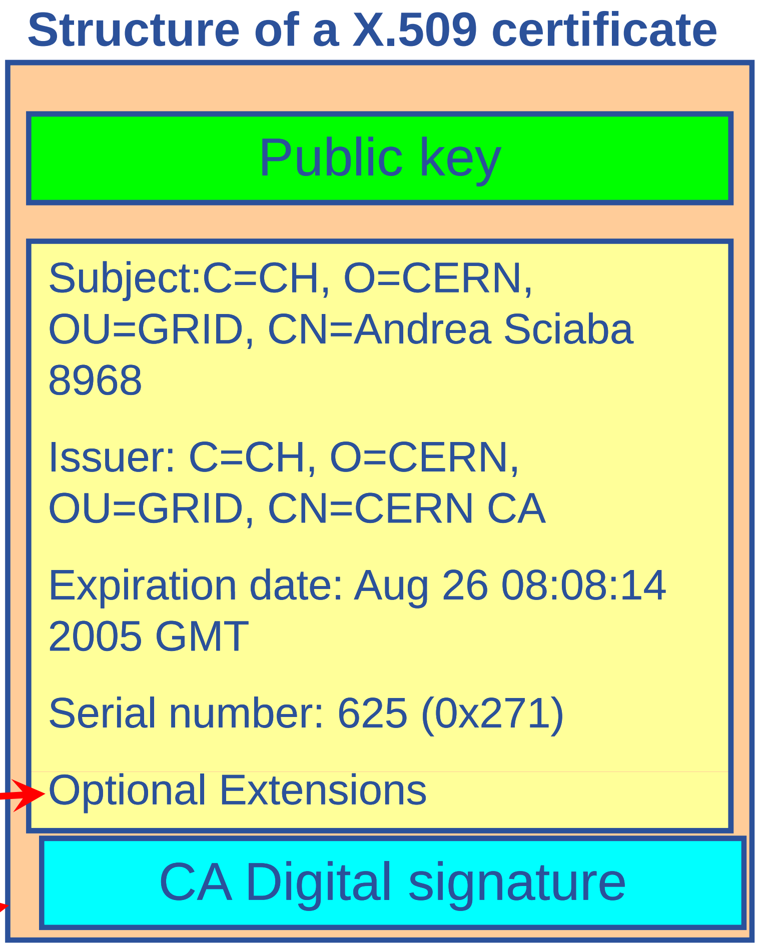
certificate



private key

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



Structure of a X.509 certificate

Public key

Subject:C=CH, O=CERN, OU=GRID, CN=Andrea Sciaba 8968

Issuer: C=CH, O=CERN, OU=GRID, CN=CERN CA

Expiration date: Aug 26 08:08:14 2005 GMT

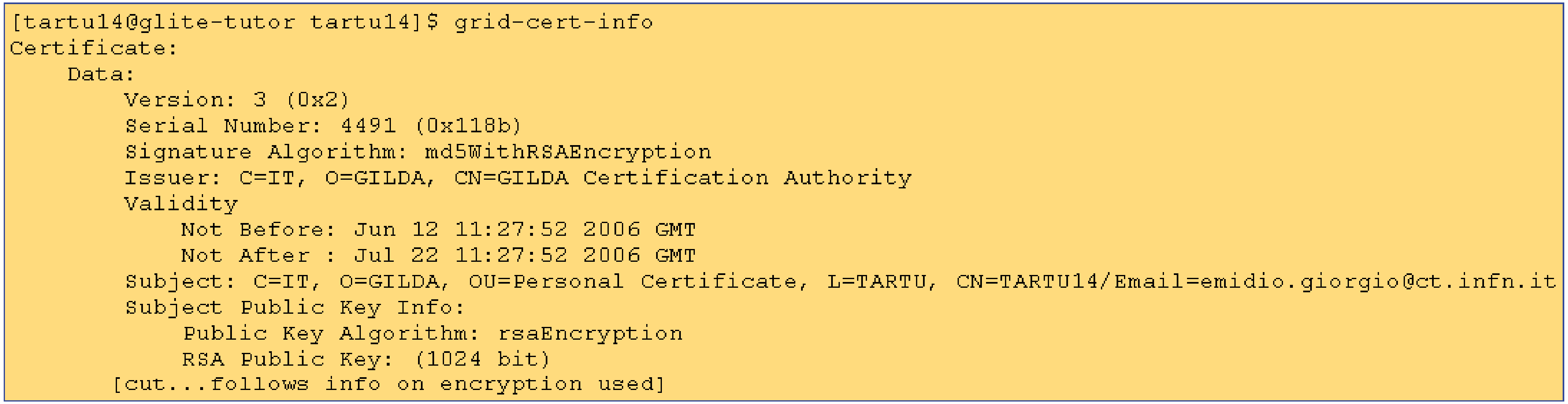
Serial number: 625 (0x271)

Optional Extensions

CA Digital signature

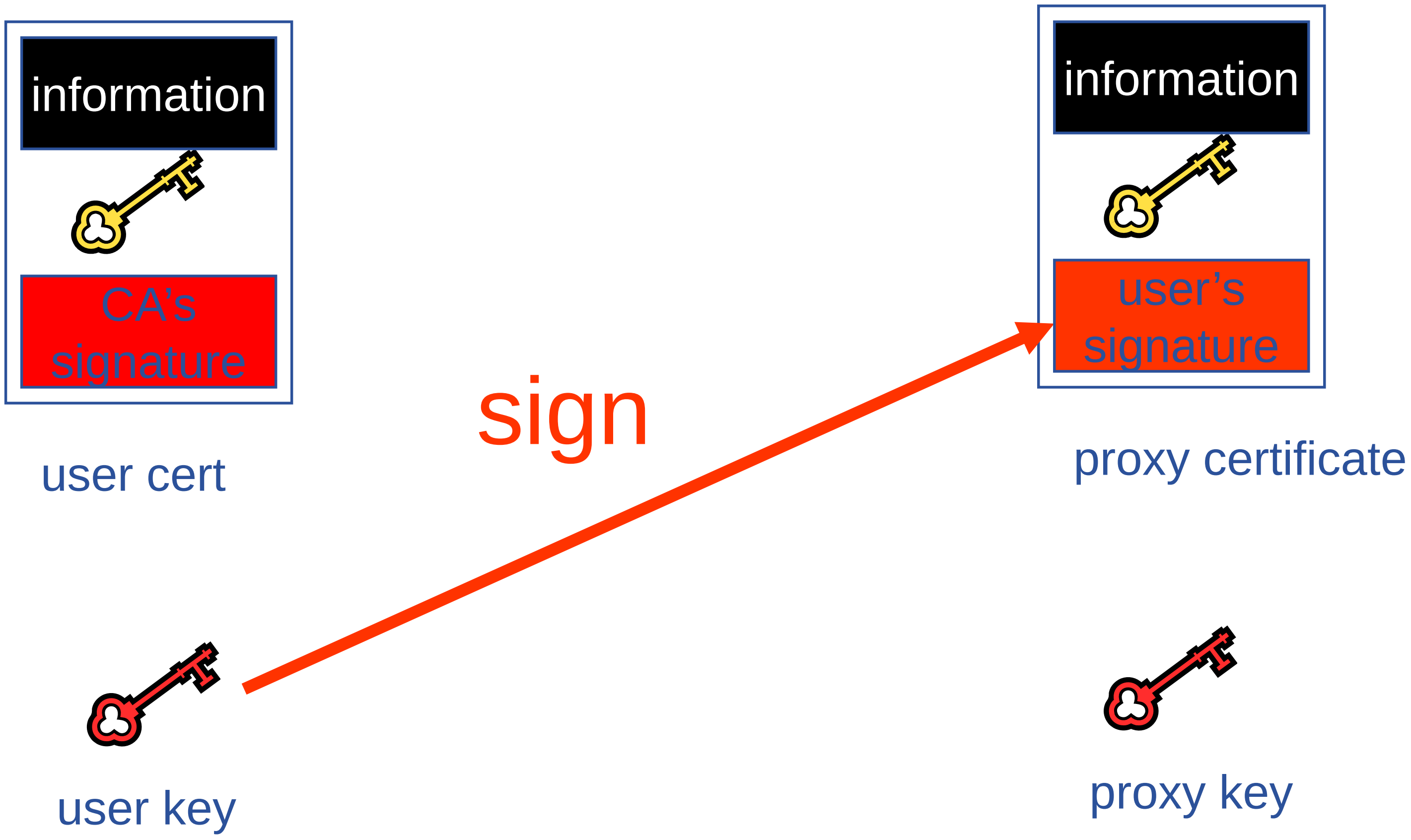
Example: X.509 Certificates

grid-cert-info

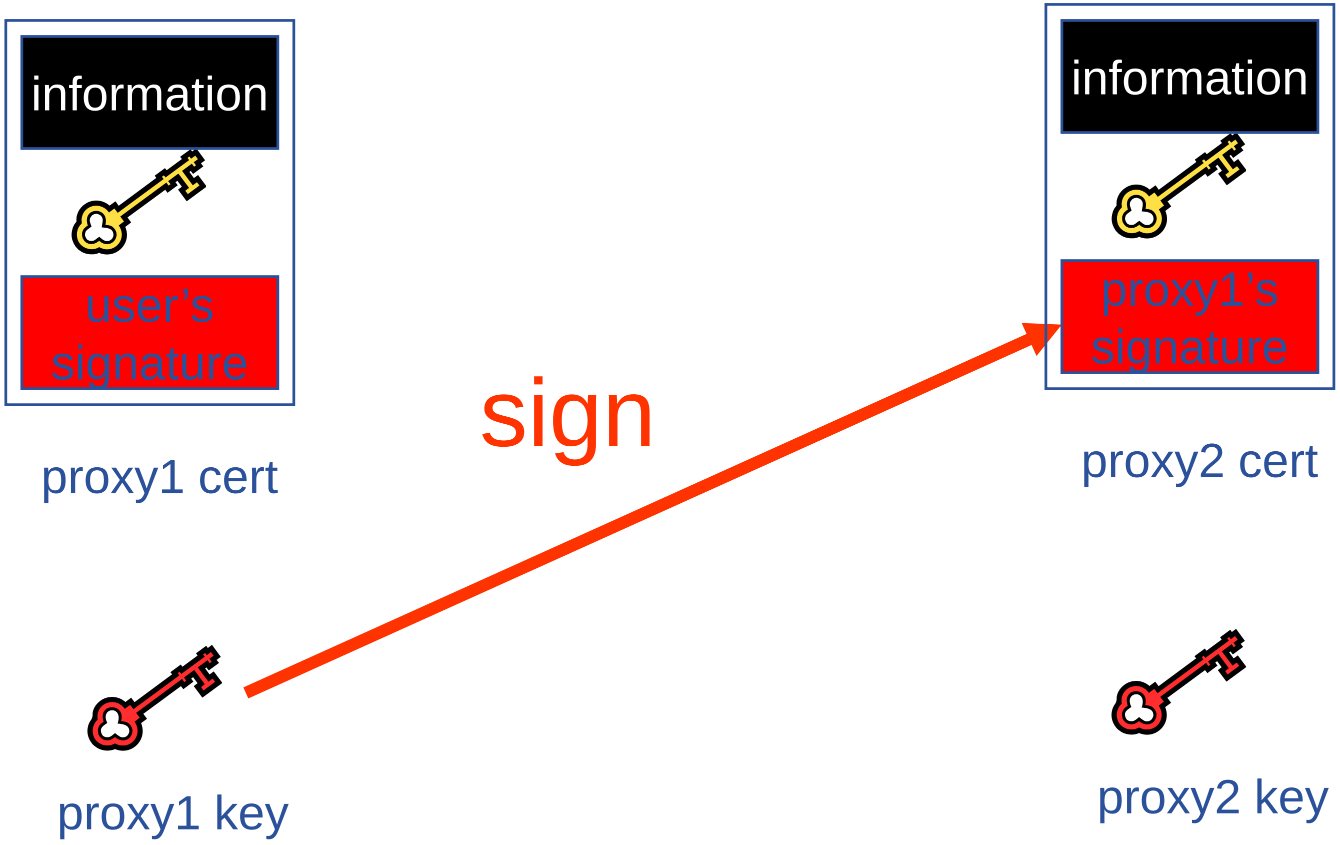


```
[tartu14@glite-tutor tartu14]$ grid-cert-info
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4491 (0x118b)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=IT, O=GILDA, CN=GILDA Certification Authority
        Validity
            Not Before: Jun 12 11:27:52 2006 GMT
            Not After : Jul 22 11:27:52 2006 GMT
        Subject: C=IT, O=GILDA, OU=Personal Certificate, L=TARTU, CN=TARTU14/Email=emidio.giorgio@ct.infn.it
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
       [cut...follows info on encryption used]
```

Proxy certificate



Proxy delegation

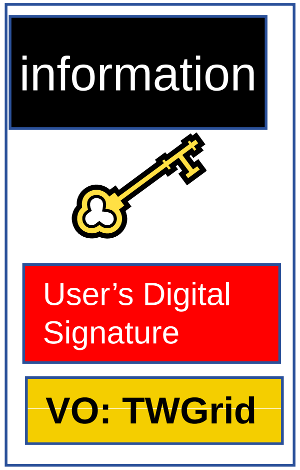


Evolution of VO management

- **VOMS**

(Virtual Organization Membership Service)

  - VO Administration :
    - check which VO the user belongs to
    - Add VO information on user’s proxy certificate.



information

User’s Digital Signature

VO: TWGrid

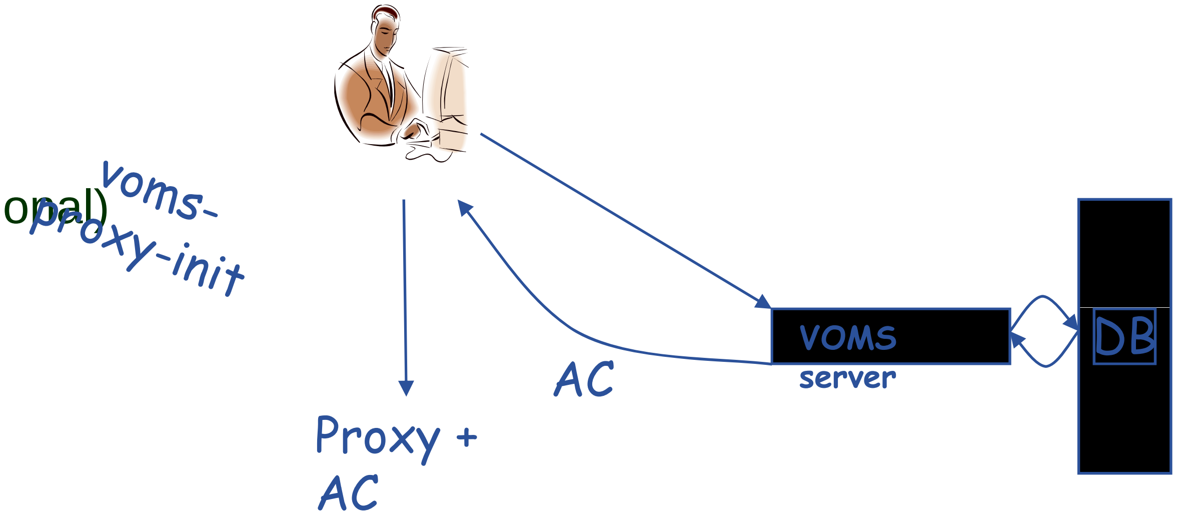
proxy certificate

- **voms-proxy-init**
  - a gLite command to
    - Contact the VOMS with user’s proxy certificate
    - Retrieve the certificate that contains VO information on it.

VOMS

- Virtual Organization Membership Service (VOMS)
- A service that keeps track of the members of a VO and grants them a set of attributes, that get included in the user's proxy certificate at proxy creation time.
- Attributes granted to users upon request (e.g. via voms-proxy-init) as AC and inserted as extension in user's proxy-certificate and used by RB, CE, SE....

VO name
Group membership
Role ownership (optional)

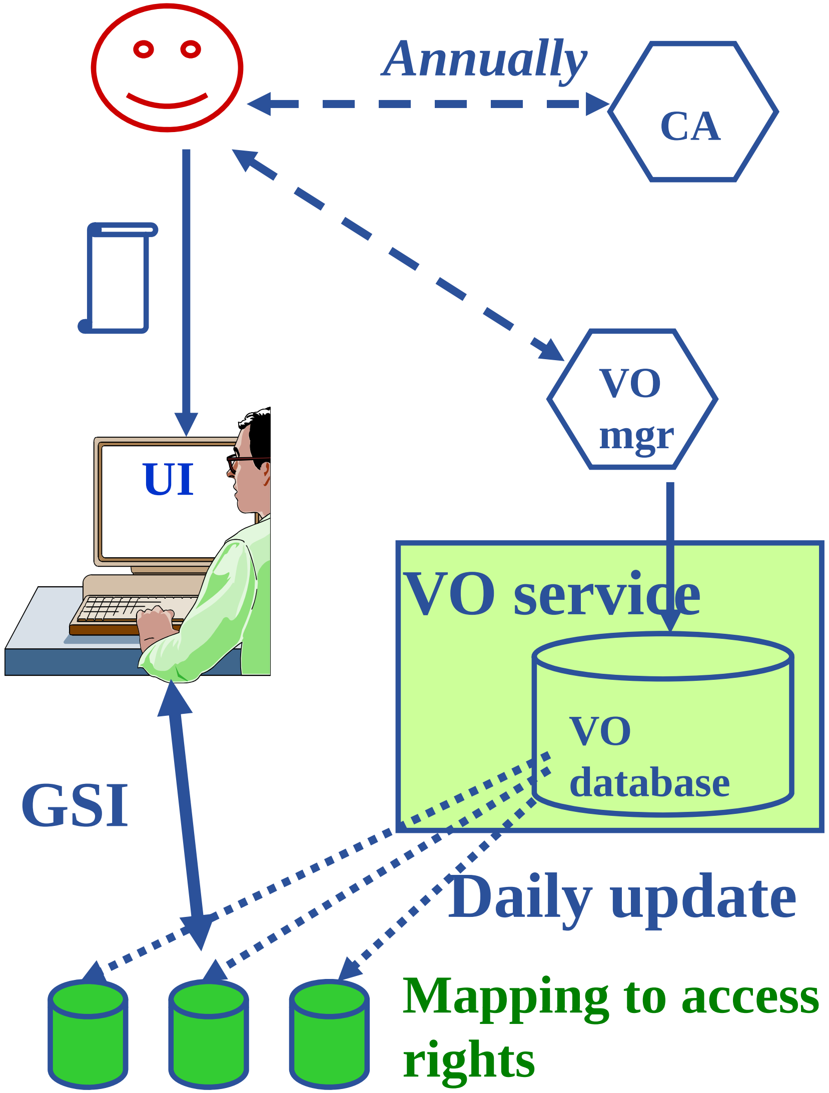


Summary of AA

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

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

  Credentials in proxy determine user's rights



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.

Reference

- **Grid Security**

  LCG Security: **http://proj-lcg-security.web.cern.ch/proj-lcg-security/**

  Globus Security: **http://www.globus.org/security/**

  Grid-it portal: **http://grid-it.cnaf.infn.it**

  LCG Registration**: http://lcg-registrar.cern.ch/**

- **Background**

  GGF Security**: http://www.gridforum.org/security/**

  IETF PKIX charter**: http://www.ietf.org/html.charters/pkix-charter.html**

  PKCS**: http://www.rsasecurity.com/rsalabs/pkcs/index.html**

Thanks for Your Listening