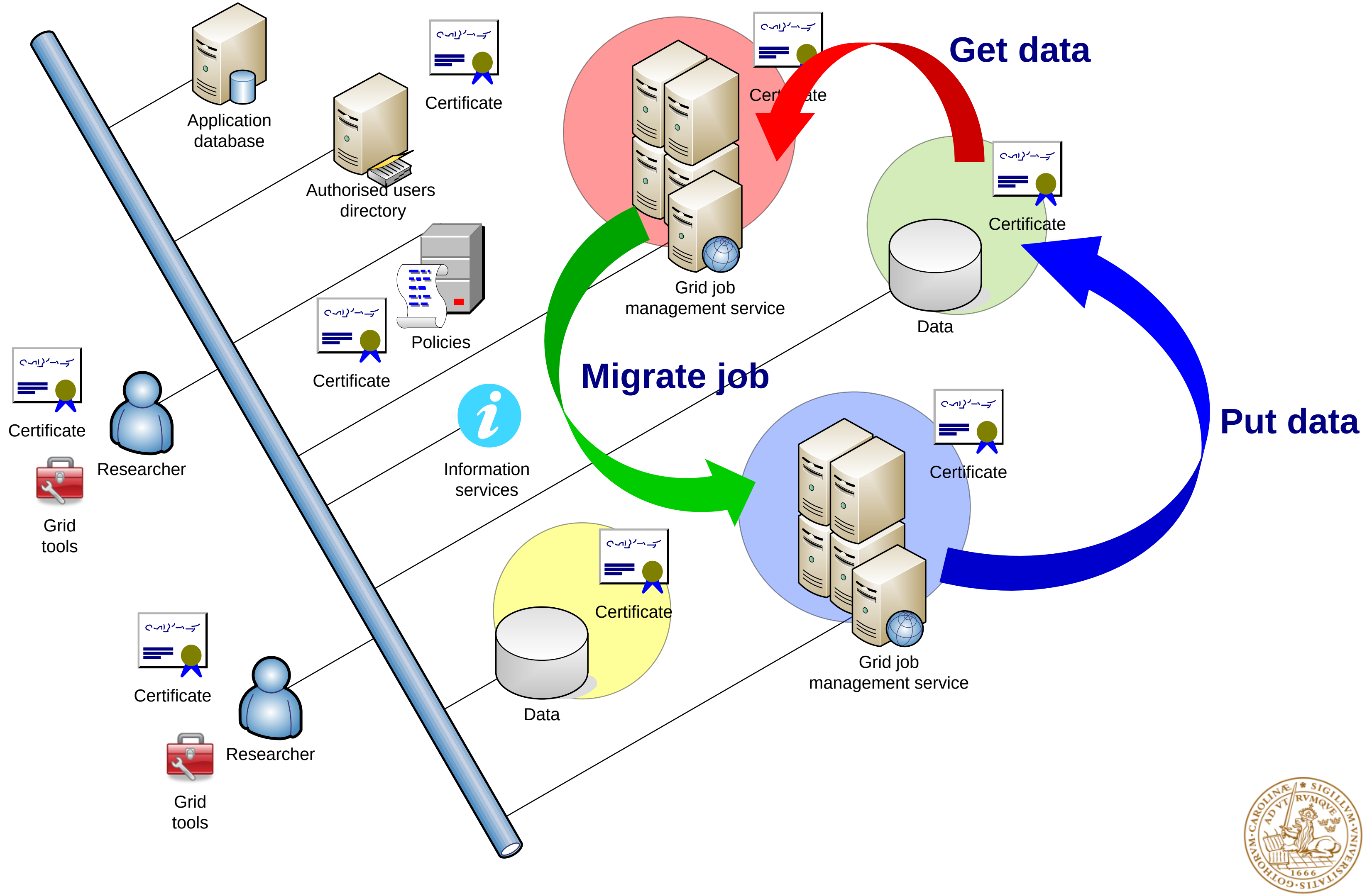
Delegation and authorisation

Grid services act on behalf of users



Why act on behalf of users?

- A “normal” cluster usually has local storage
  - Same user identity for jobs and data access
- On the Grid, storage is usually remote
  - Every time a job needs to read or write data, authorised remote connection is required
- A Grid cluster’s own certificate is not enough
  - Users want to protect their data from unauthorised access
  - Users also don’t want everybody to write to their storage share
- A job may have to be migrated to another cluster
  - Not quite implemented in reality, yet

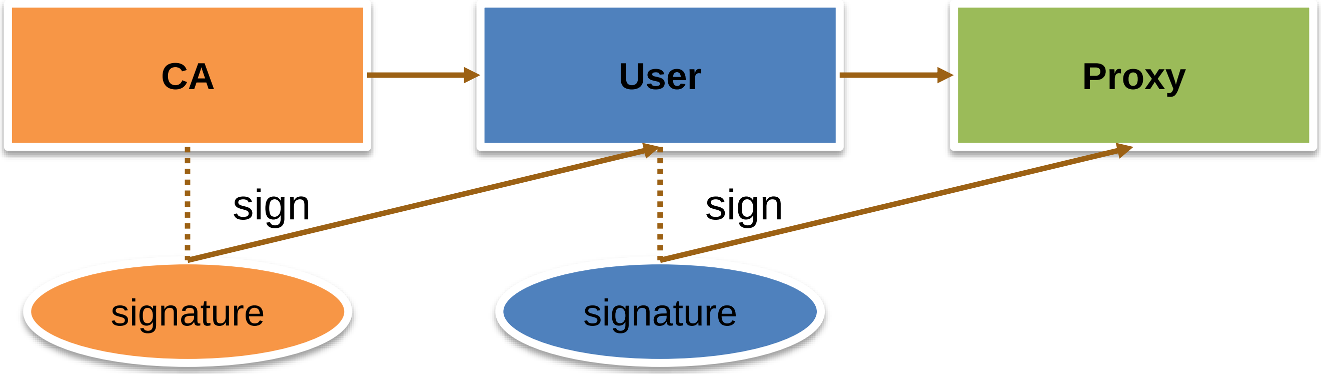
Delegation: Act by proxy

- In real life, you sign a **proxy** document and certify it by a notary
  - Document says what actions can be performed on your behalf
- On the Grid, a proxy document is a X.509 certificate signed by you
  - Since your certificate is in turn signed by a CA, proxy is also a trusted document
  - Proxy may contain a lot of additional information

PROXY AND WAIVER

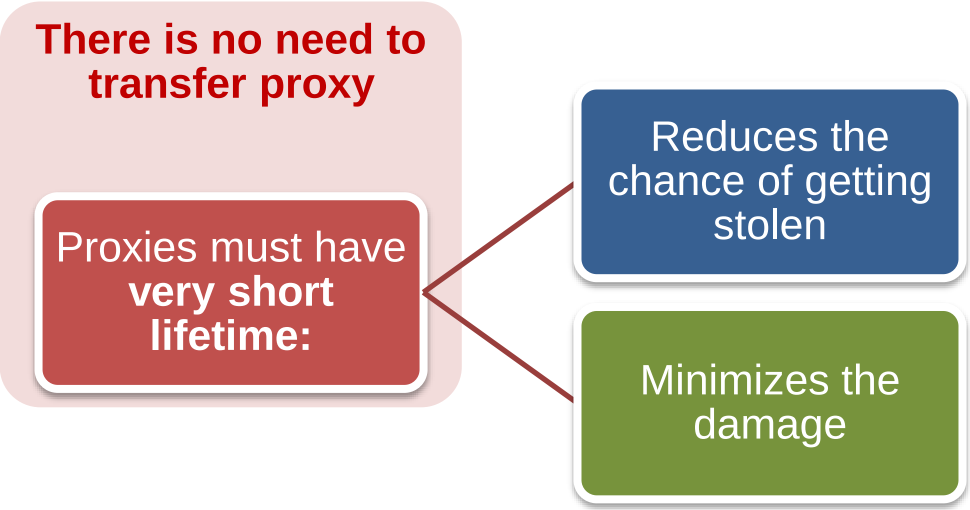
IRVING NATIONAL BANK

Know all Men by These Presents, [illegible]



Proxy certificate

- Proxy is an extension of the SSL standard
- Proxy contains both public and private keys
  - Not the same as users' keys, but derived from them
- Proxy needs no password (unlike usual PKI certificates)
- Proxy can not be revoked
- Proxies are used by Grid services, to act on behalf of the proxy issuer



There is no need to transfer proxy

Proxies must have **very short lifetime:**

Reduces the chance of getting stolen

Minimizes the damage

Proxy creation

- A **new** private/public key pair is created for each proxy
  - When a proxy expires, a new one must be created to continue working
    - » Default expiration time is 12 or 24 hours
- A proxy is then constructed of:
  - Public certificate (with public key embedded)
    - » Certificate contains modified owner's Distinguished Name (has "*proxy*" appended to the name)
      - Owner's DN: **`/C=UK/O=Grid/OU=CenterA/L=LabX/CN=john doe`**
      - Proxy DN: **`/C=UK/O=Grid/OU=CenterA/L=LabX/CN=john doe/CN=proxy`**
    - » Certificate is signed by the proxy owner's **real** private key
    - » Certificate contains validity period
  - Private key
  - Optionally, Attribute Certificates – extensions containing additional information

The tale of two proxies

- A user always has to create a proxy certificate **P1**
  - Technically, it can be sent to the server, but it is a security breach
- The server gets itself a **<u>delegated</u> proxy P2** for each user:
  1. <u>Server</u> generates a **new** private/public key pair
  2. Server returns the generated public key as a <u>certificate request</u> to the user
  3. User’s tool signs that public key and inserts user information (DN etc), thus generating a public certificate. It uses the private key of <u>proxy</u> **P1** for performing signing operation.
     - » It can also use the actual private key, but that will require entering password every time!
  4. User’s tool sends the signed public certificate back to the server
  5. Server adds generated private key to that certificate and creates a <u>delegated</u> proxy **P2**

There can be even three proxies

- If a server needs a new proxy, and you are not available to sign it, a **MyProxy** server can act on your behalf
  - MyProxy is a technology provided with the Globus distribution
    - » MyProxy servers are offered by some Grids; none in the Nordics though
  - Of course, it needs a delegated proxy, too
- The procedure is as follows:
  1. A proxy **P1** is created by the user, as usual
  2. User contacts a MyProxy server, which creates a new key pair and then a **long-living** delegated proxy **P2**
  3. Another Grid service generates an own key pair, and requests MyProxy to create the certificate on your behalf; this leads to a short-living delegated proxy **P3**
     - » User has to provide a password to MyProxy

Do I have to do all this by hand?

- Luckily, all authentication and delegation procedures are a part of the protocol
- Before every Grid activity, you just have to create a proxy. Some common tools are:
  - By ARC: **`arcproxy`**
  - By Globus: **`grid-proxy-init`** and **`myproxy-init`**
  - By EMI VOMS: **`voms-proxy-init`**
- Proxies expire quickly!
  - Resist temptation to create long-living proxy: this will undermine your security
  - ARC has a tool to renew a proxy that has been sent away
    - Actually, an entirely new proxy is generated and sent to the job
  - MyProxy service can be used to deal with expiring proxies

Authorisation

- Authentication = passport; authorisation = visa
  - Having a valid passport is not enough to enter a country
  - Having a valid proxy is not enough to access computing or storage resources
- Authorisation can be by person or by group
  - By person: a person with Swedish visa can enter Sweden
  - By group: everybody with a EU/EEA/US passport can enter Sweden
- Authorisation on the Grid:
  - By person: your DN is in the list on a cluster (matched to your proxy DN)
  - By group: your DN is in the *Virtual Organisation (VO)* list
    - » Your proxy has this VO’s Attribute Certificate

LUND UNIVERSITY

Virtual Organisation

- A Grid Virtual Organisation (VO) is simply a group of people
- VO attributes:
  - VO must have a manager who approves membership
  - VO must have a set of rules – policies – regulating the membership
  - VO must have means of providing an up-to-date list of members' DNs to Grid services
  - VO may have groups and roles
    - Useful to define shares and privileges
  - VO may run a service that issues Attribute Certificates (AC)
    - An AC asserts VO membership of a user, as well as their role, group, or other attributes
    - An AC is digitally signed by the issuing VO
    - An AC is included into the proxy

Why use the VO concept?

- Simplicity
  - It is easier to authorise a VO than all its members individually
    - » To authorise users individually, all their DNs must be known
    - » To authorise a VO, only its URL is needed
- Flexibility
  - VO members may come and go, and Grid services don’t have to change a thing
- Scalability
  - It is easier to negotiate service levels with few VO managers than with all individual users
    - » Different VOs may have different quotas or shares
    - » Different roles inside a VO may have different privileges
- Delegation of responsibility
  - VO managers are responsible to check eligibility of users
  - Resource owners trust VO managers
    - » If some VO users misbehave, entire VO can lose access

VO Management Service (VOMS)

- A trivial VO can be simply a file on the Web with user DNs
- For large VOs, dedicated **VO Management Service (VOMS)** exists (distributed with EMI)
  - Has a database of users
    - Each user can have a number of VO-specific attributes: group, role, alias etc
    - VO membership can be time-limited
  - Has a management interface
    - Registration form for new users
    - Management tools for administrators
  - Has a capability to issue Attribute Certificates upon request
- VOMS, like any Grid service, has a certificate and operates over a secure connection

How to make use of VOMS

- A Grid cluster administrator may use VOMS database to synchronise the list of authorised DNs
  - Alternatively, a cluster can be configured to check every user's proxy for VOMS extensions
- A Grid user must become a member of a VO
  - If none exists for you, just set it up
- If VO uses a VOMS server, VOMS-extended proxies must be created
  - The proxy creation tool must be pointed to a VOMS server
  - Upon proxy creation, the tool contacts VOMS and receives an AC asserting VO membership, role etc
  - The AC is then embedded into proxy, and everything is signed by the owner's private key
    - AC can not be embedded in normal PKI certificates or keys
    - AC lifetime can be different from that of the proxy itself

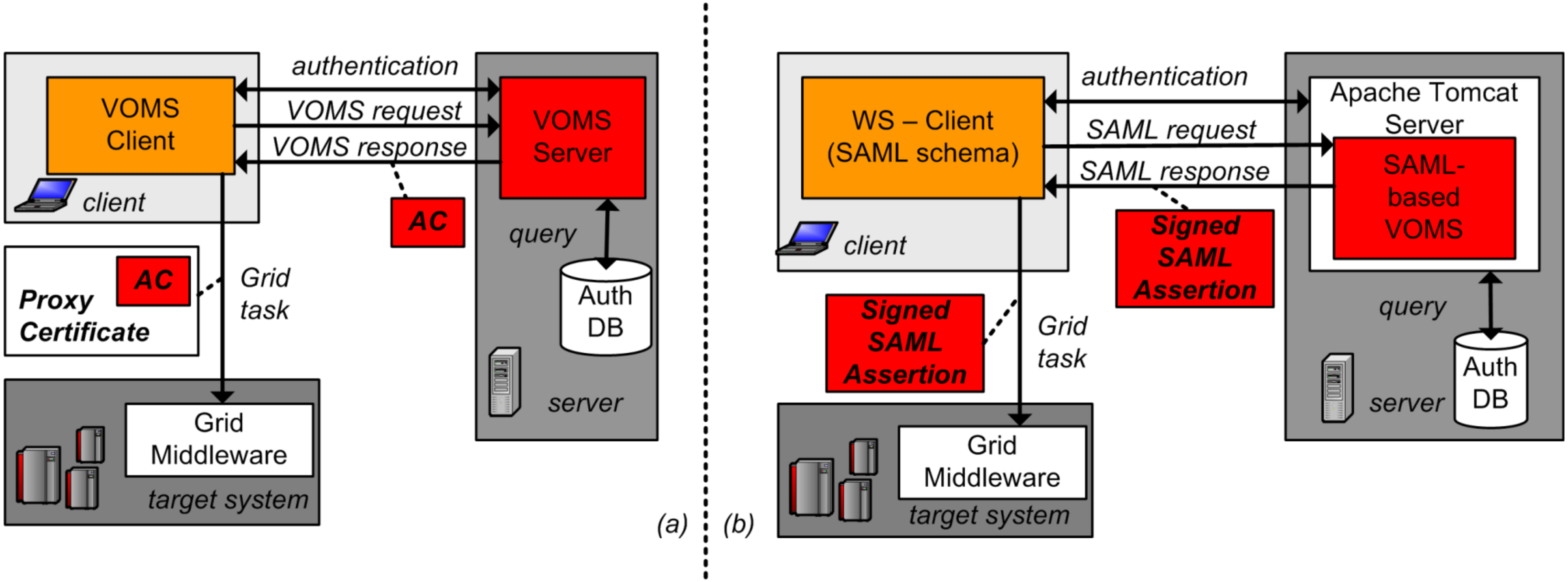
Groups and roles

- VOMS-extended proxy is used for authentication, authorisation and delegation just like a normal proxy
- Groups and roles are some of the most frequently used attributes in VOMS
  - A group is a subset of the VO (e.g., all students)
  - A user can be a member of any number of groups, all of them will be listed in the AC
  - A role is indication of a privilege (e.g. a VO manager)
  - Roles are attached to groups (e.g. each group may have a manager role)
- Groups and roles are specified in a Fully Qualified Attribute Name (FQAN)
  - FQAN format: **`<group name>[/Role=<role name>]`**
  - FQAN example: **`/physics/astro/Role=tester`**
  - FQANs are used to assign agreed priorities, quotas etc on clusters and storage

When VOMS proxy is not needed

- Working with storage usually needs no delegation
  - A normal X.509 certificate could well be sufficient in many cases
  - But if a VO wants to limit access to its data, storage may still be configured to inspect VOMS AC
    - » A proxy will be needed because AC can not be embedded into a normal certificate
- Instead of an AC, a VO management service can issue assertions using Security Assertion Markup Language (SAML)
  - SAML assertions are documents that can be transferred along with normal X.509 credentials
  - Not widely used on the Grid (yet)
- Authorisation can even rely on an external policy decision point (PDP)
  - Grid cluster or storage will only need yes/no answer from a PDP

VOMS AC compared to SAML



Graphics by the VOMS team

Exercises

- Create a simple proxy using **`arcproxy`**
  - Need to know the location of your certificate (both .pem or .p12 format OK)
    - Default location: **`$HOME/.globus/`** , create it and copy your keys there
    - Default names: **`userkey.pem`** for the private key, and **`usercert.pem`** – for the certificate
  - Need to know the location of the trusted CA files
    - Default location: **`/etc/grid-security/certificates`** , check that it exists
  - If defaults locations and names are used, **`arcproxy`** will work right away; if not, issue the full command with all the necessary parameters specified explicitly:

```
arcproxy -C certfile_path  -T CAfiles_path -P proxyfile
```

- Inspect your proxy with **`arcproxy -I`**
  - Compare certificate DN and proxy DN
  - Locate the proxy file, check proxy permissions, compare with key permissions
- Generate proxy with one hour lifetime: use **`-c validityPeriod=3600`**

Exercises

- Join NorduGrid VO:
  - Load your .p12 certificate into the browser and make sure you can read your email
  - Visit http://www.nordugrid.org → “Grid access” → “User groups (VOs) → nordugrid.org → “Membership request”
- Create a file containing the VOMS server contact string (e.g. **`my.vomses`**)
  - Default file: **`$HOME/.voms/vomses`** (there are other defaults, but this one is most common)
  - Copy the `VOMSES string` from the “Configuration Info” at the VOMS Admin web site
- Create a VOMS-extended proxy (extended proxy with VO information):

```
arcproxy -S nordugrid.org -P /tmp/my_voms_proxy1
```

  - For advanced users who don’t like defaults:

```
arcproxy -C your_certfile -P /tmp/voms_proxy1 –V my.vomses -S
nordugrid.org
```

- Request a proxy with a non-granted role, check how your request is rejected:

```
arcproxy -S nordugrid.org:/nordugrid.org/Role=VO-Admin
```

- inspect a NorduGrid-extended proxy; pay attention to proxy lifetime and VOMS AC lifetime:

```
arcproxy -I -P /tmp/my_voms_proxy1
```