Grid Security

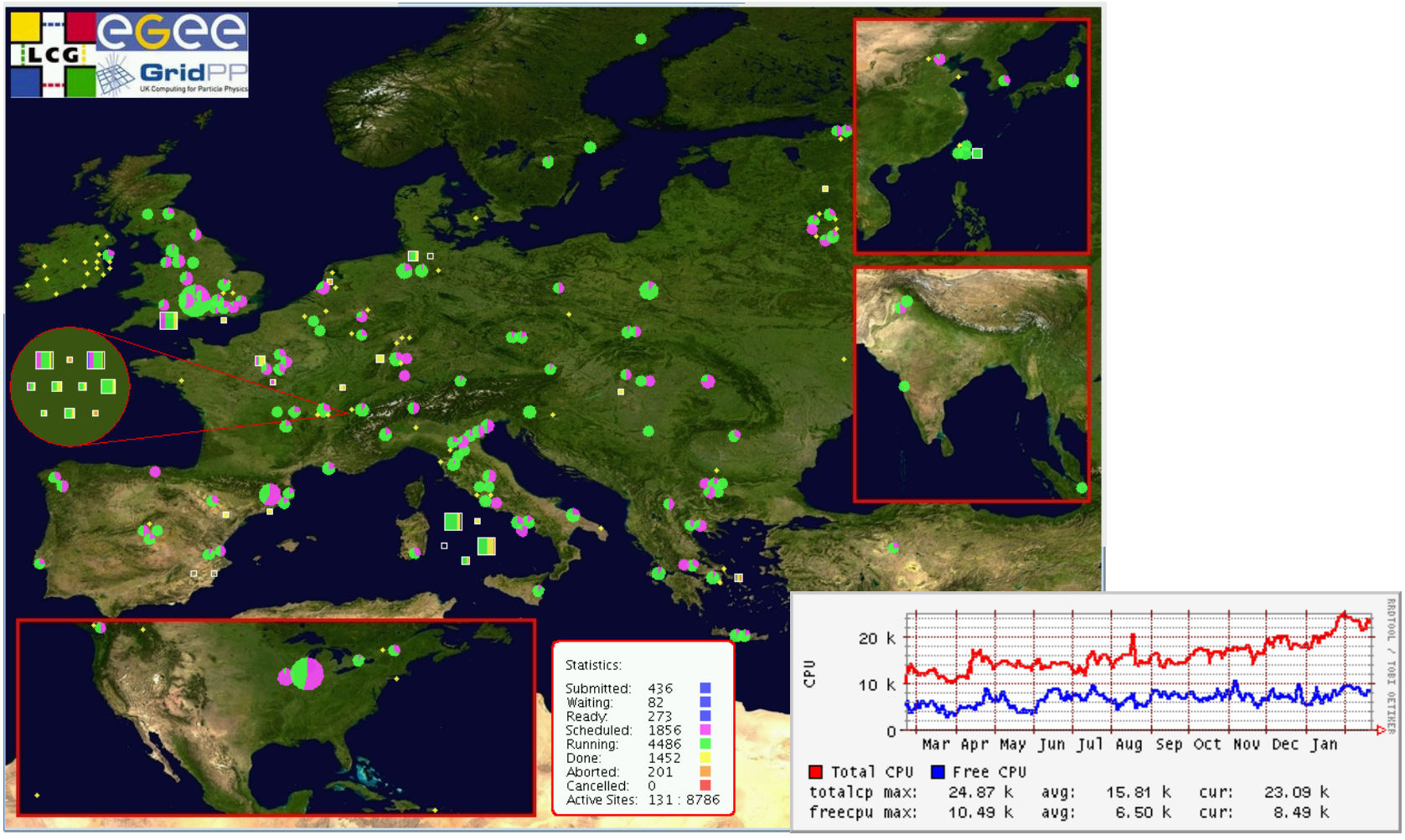
John White (Helsinki Institute of Physics)

EMI INFSO-RI-261611
GridKa School, Karlsruhe, Sept 10th, 2010

EMI Project

- European Middleware Initiative (EMI).
- EU-Funded for 3 years (until end April 2013).
  - Preceded by EGEE-I/II/III, UNICORE, NorduGrid.
- Includes middleware components from:
  - **ARC**
    - Client job brokering, VOMS, X.509, SAML
  - **gLite**
    - Centralized job brokering, VOMS, X.509, Data Management
  - **UNICORE**
    - HPC, Common FS, homogeneous env, VOMS, X.509, SAML
  - **dCache**
    - Widespread Data Management, Used by other projects.
- Provides a consistent middleware distribution to EGI and others.

WLCG (EGEE) Infrastructure



- 54 Countries, 267 Sites, 114k CPUs 20PB Storage.
- `http://gridportal.hep.ph.ic.ac.uk/rtm/`

WLCG (EGEE) Infrastructure

- Virtual Organizations on the EGEE infrastructure: ≈ 200
- Registered Virtual Organizations: 152
- Registered users: ≈ 16000
- Number of jobs: $\approx$ 150k jobs/day
- Application domains: more than 15

WLCG (EGEE) Infrastructure

- Archeology.
- Astronomy & Astrophysics.
- Civil Protection.
- Computational Chemistry.
- Computational Fluid Dynamics.
- Computer Science/Tools.
- Condensed Matter Physics.
- Earth Sciences.
- Finance.
- Fusion.
- Geophysics.
- High-Energy Physics.
- Life Sciences.
- Multimedia.
- Material Sciences.

Security for Grid Infrastructures

- An overall **Infrastructure** is composed of **Computing Resources.**
  - Universities, Institutes, Agencies.
- There are rules and policies on security.
  - (Inter)National, Institutional.
- Grid software must not compromise the resources.
  - eg. Securely coded services, Grid Users identified.
- The Grid software should (at least) answer:
  - **Who is the Grid User?**
  - **Where is the Grid User from?**
  - **What does the Grid User want to do?**
  - **What is the Grid User allowed do?**

Grid User Identity

- Grid User Identity based on a Credential:
  - PKI public/private key pair (X.509 cert/key).
  - Shibboleth (SAML Assertion)*.
  - Kerberos Ticket*.
  - OpenID*.
  - Short-Lived Credentials.
- A Grid User receives a credential from a recognized source.
  - Grid User requests a credential from a "national" Certificate Authority (CA).
  - Identity of the Grid User verified by CA.
  - CA signs certificate request for Grid User.
  - CA identity distributed to Grid resources via CA certificate.
  - Certificate/key pair uniquely identifies Grid User to all resources with CA certificate.

Grid User Identity

- Grid User Identity based on a Credential:
  - PKI public/private key pair (X.509 cert/key).
  - Shibboleth (SAML Assertion)*.
  - Kerberos Ticket*.
  - OpenID*.
  - Short-Lived Credentials.
- A Grid User receives a credential from a recognized source.
  - Grid User requests a credential from a "national" Certificate Authority (CA).
  - Identity of the Grid User verified by CA.
  - CA signs certificate request for Grid User.
  - CA identity distributed to Grid resources via CA certificate.
  - Certificate/key pair uniquely identifies Grid User to all resources with CA certificate.
- **Who the Grid User is and where they are from.**

Proxies

- **Grid User credentials cannot be passed to resources.**
  - **Security "risk"!**
- Credentials are written into a **proxy** certificate (ARC and gLite case).
  - Limited lifetime.
  - Better security risk.

```
#!/bin/sh
cd $HOME
cd .globus
userid=MY_LOCAL_USERID
openssl req -new -nodes -keyout proxy.key -newkey rsa:1024 \
     -subj "/O=Grid/O=NorduGrid/OU=hip.fi/CN=John White/CN=proxy" > proxy.csr
openssl x509 -CA ~/.globus/usercert.pem -CAkey ~/.globus/userkey.pem \
     -req -in proxy.csr -md5 -days 7 -set_serial 0xcafebabe01 \
     -extfile proxy_openssl.cnf -extensions proxy_ext > /tmp/x509up_u${userid}
chmod 600 /tmp/x509up_u${userid}
```

or...

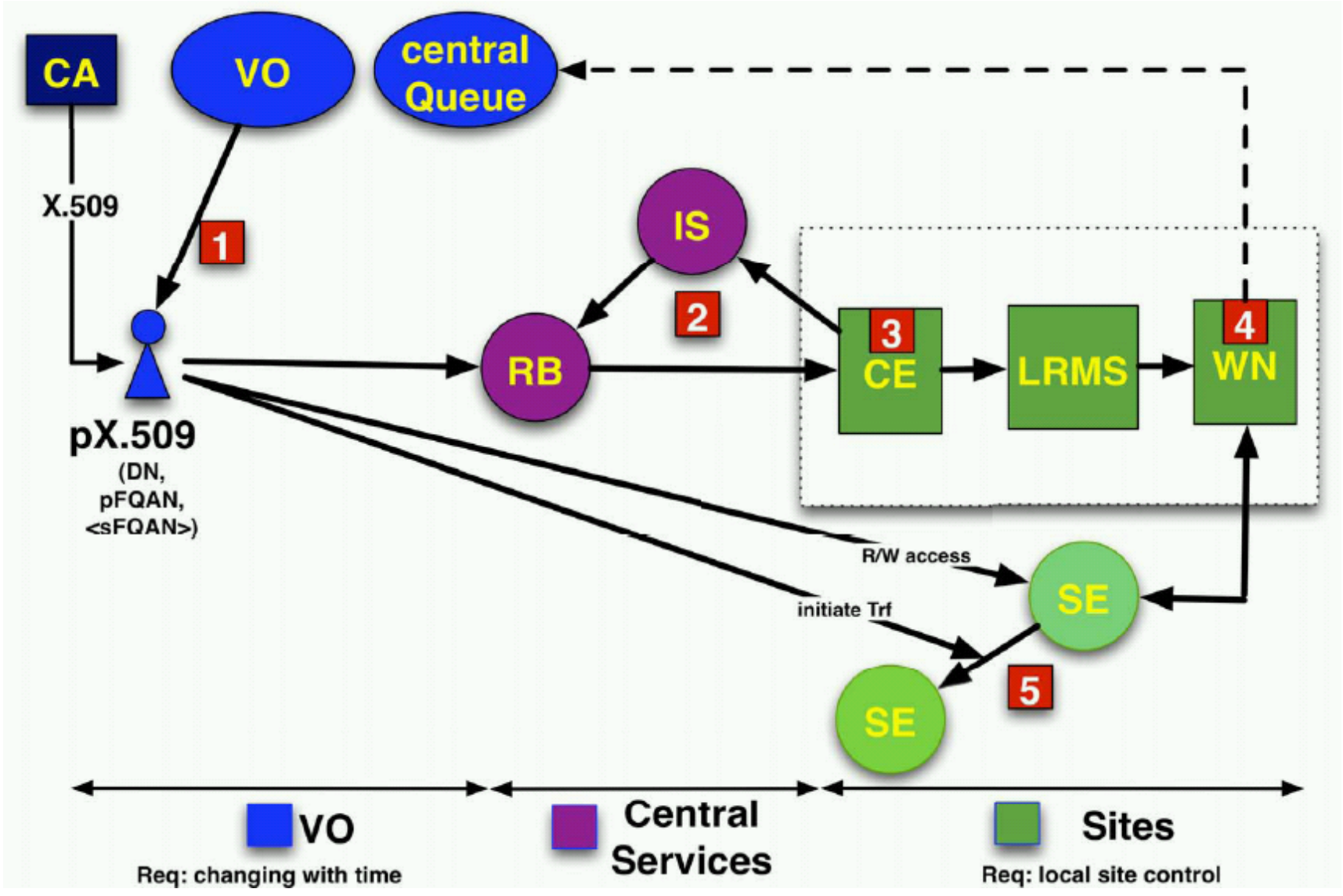
```
jwhite@pcppe01:~$ date;grid-proxy-init
Tue Apr 21 14:59:01 CEST 2009
Your identity: /O=Grid/O=NorduGrid/OU=hip.fi/CN=John White
Enter GRID pass phrase for this identity:
Creating proxy ..................................................................... Done
Your proxy is valid until: Wed Apr 22 02:59:04 2009
```

Proxies

```
jwhite@paha:~/.globus$ openssl x509 -in /tmp/x509up_u${userid} -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ca:fe:ba:be:01
        Signature Algorithm: md5WithRSAEncryption
        Issuer: O=Grid, O=NorduGrid, OU=hip.fi, CN=John White
        Validity
            Not Before: Apr  8 10:48:04 2009 GMT
            Not After : Apr 15 10:48:04 2009 GMT
        Subject: O=Grid, O=NorduGrid, OU=hip.fi, CN=John White, CN=proxy
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e4:7f:89:b8:89:48:71:2c:06:38:f7:56:c9:56:
                    2a:24:f8:8c:c5:27:68:2d:1c:a5:dc:1a:5b:27:21:
                    7d:6b:3a:d5:f4:8e:28:e7:1d:11:ce:19:cd:ec:43:
                    8a:a5:60:4a:f8:da:e6:98:a7:a0:19:9b:dc:26:21:
                    28:2d:e9:54:ec:8f:7c:95:63:12:64:ea:22:a7:70:
                    70:f4:e0:1a:31:ec:f1:a6:c9:c0:ff:4d:f5:68:ed:
                    fb:a7:41:8c:71:ad:67:de:c2:92:8f:73:fb:e7:90:
                    72:d3:28:51:f1:5c:b8:4e:03:d8:58:d5:18:5a:97:
                    f7:cc:74:77:e0:f9:4b:94:9d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Proxy Certificate Information: critical
                Path Length Constraint: infinite
                Policy Language: Any language

    Signature Algorithm: md5WithRSAEncryption
        92:43:ed:20:26:c9:e1:28:80:77:e7:c3:30:4f:9f:c7:8c:c9:
        62:0e:48:57:62:f3:02:ba:44:0e:fb:29:c9:55:1f:78:1f:c0:
        05:89:cc:59:4e:46:23:10:0c:7f:8f:14:92:e0:28:b8:65:61:
```

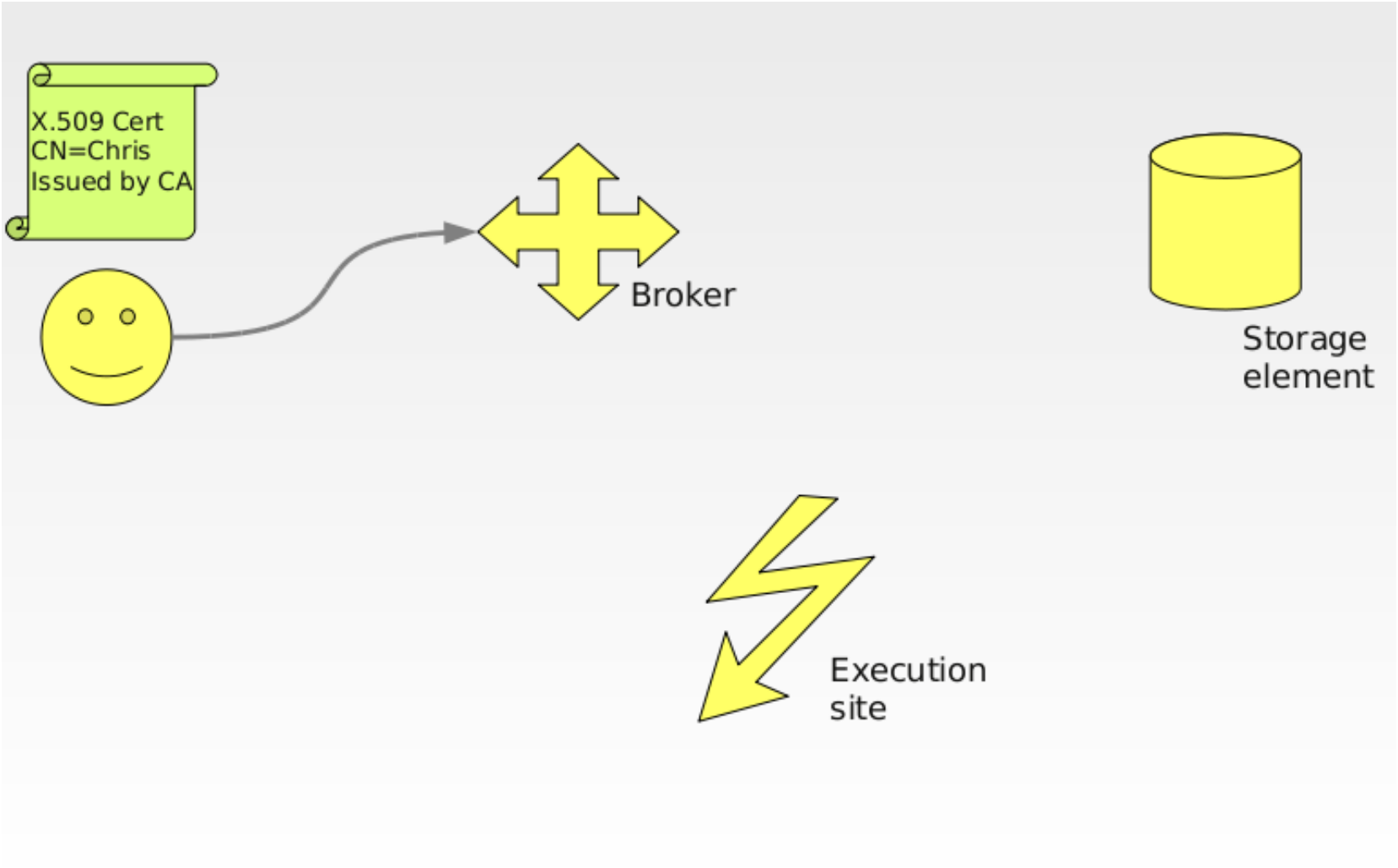
Security Domains



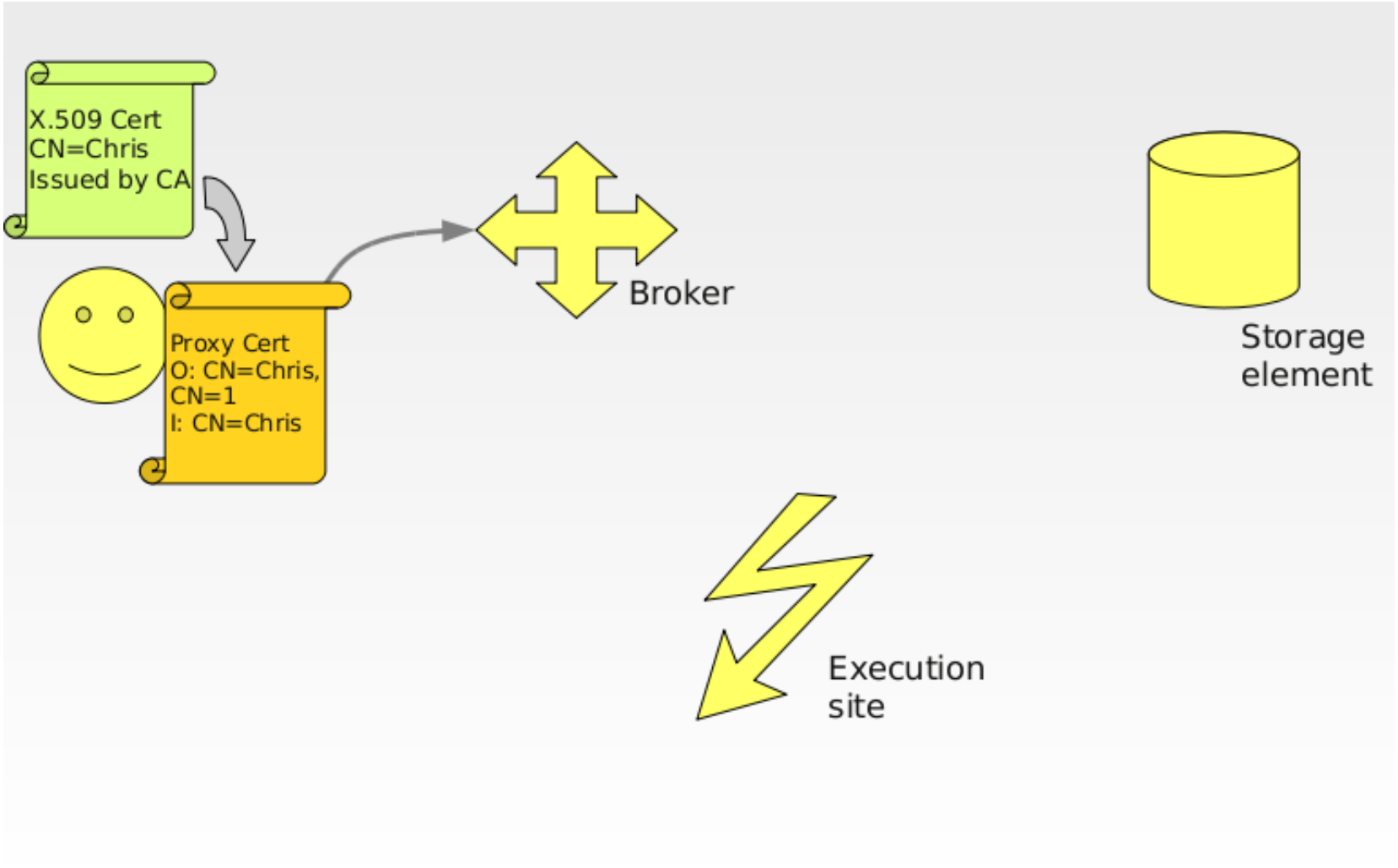
Sending Credentials to a Grid

- In gLite and ARC: user authentication, trust delegation achieved through Proxy Certificates.
  - Initial proxy certificate issued by the Grid User.
  - Contains new public key and corresponding private key.
  - Proxy is protected by the FS.
  - Private key is never encrypted.
- The middleware issues a proxy based on the initial proxy.
  - Used to initiate a SSL/TLS connection.
- This is **impersonation**.

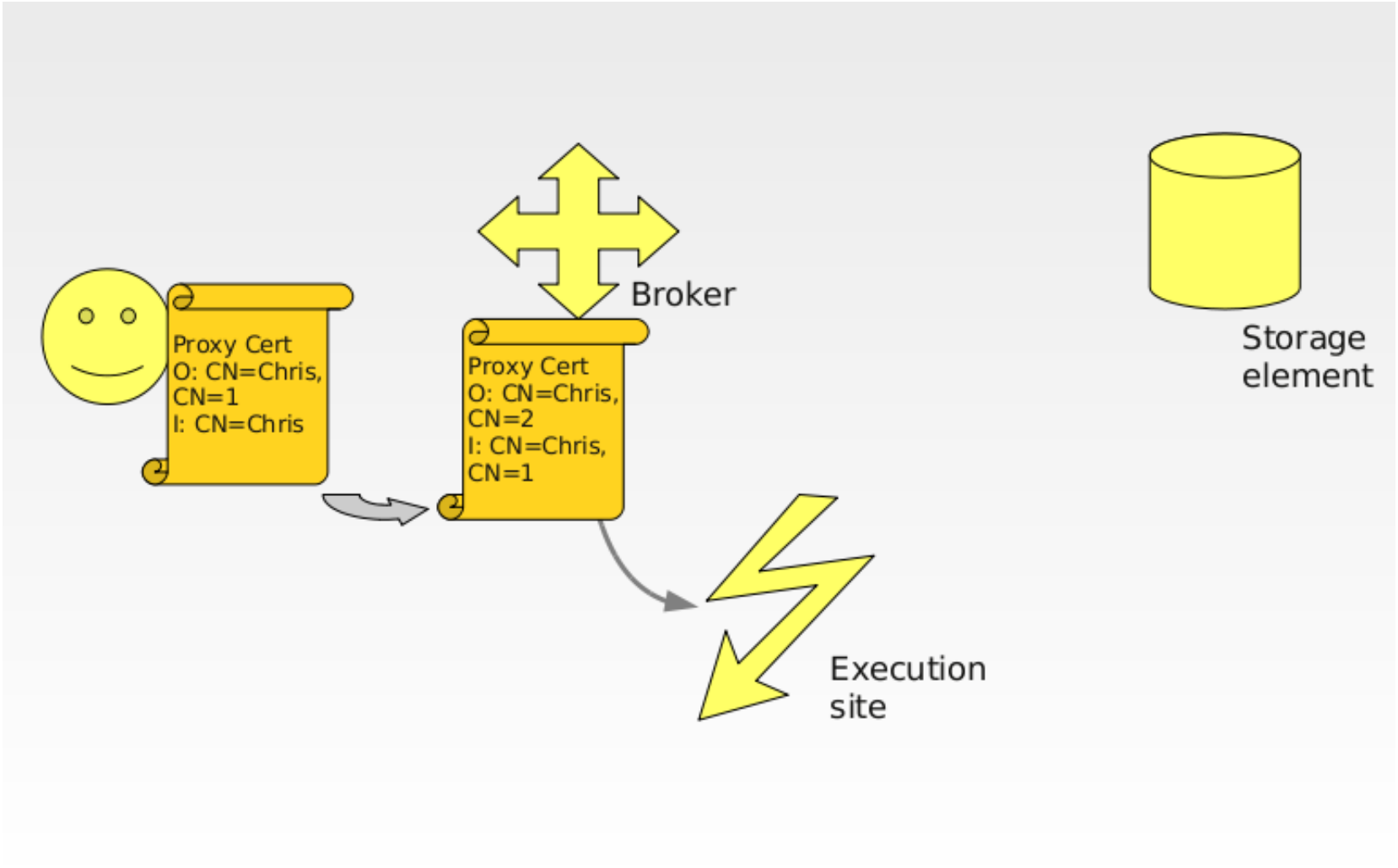
Using proxies



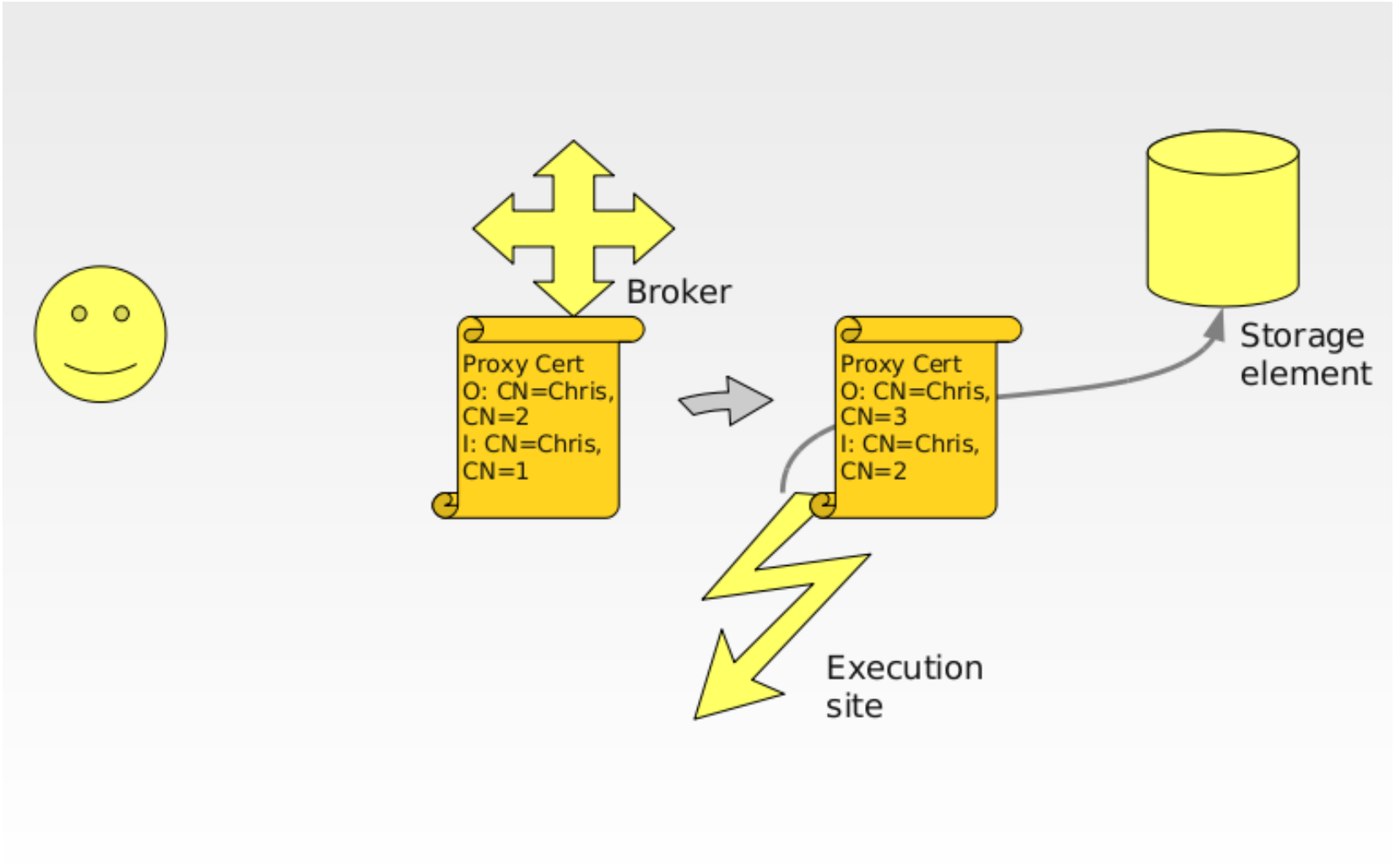
Using proxies



Using proxies



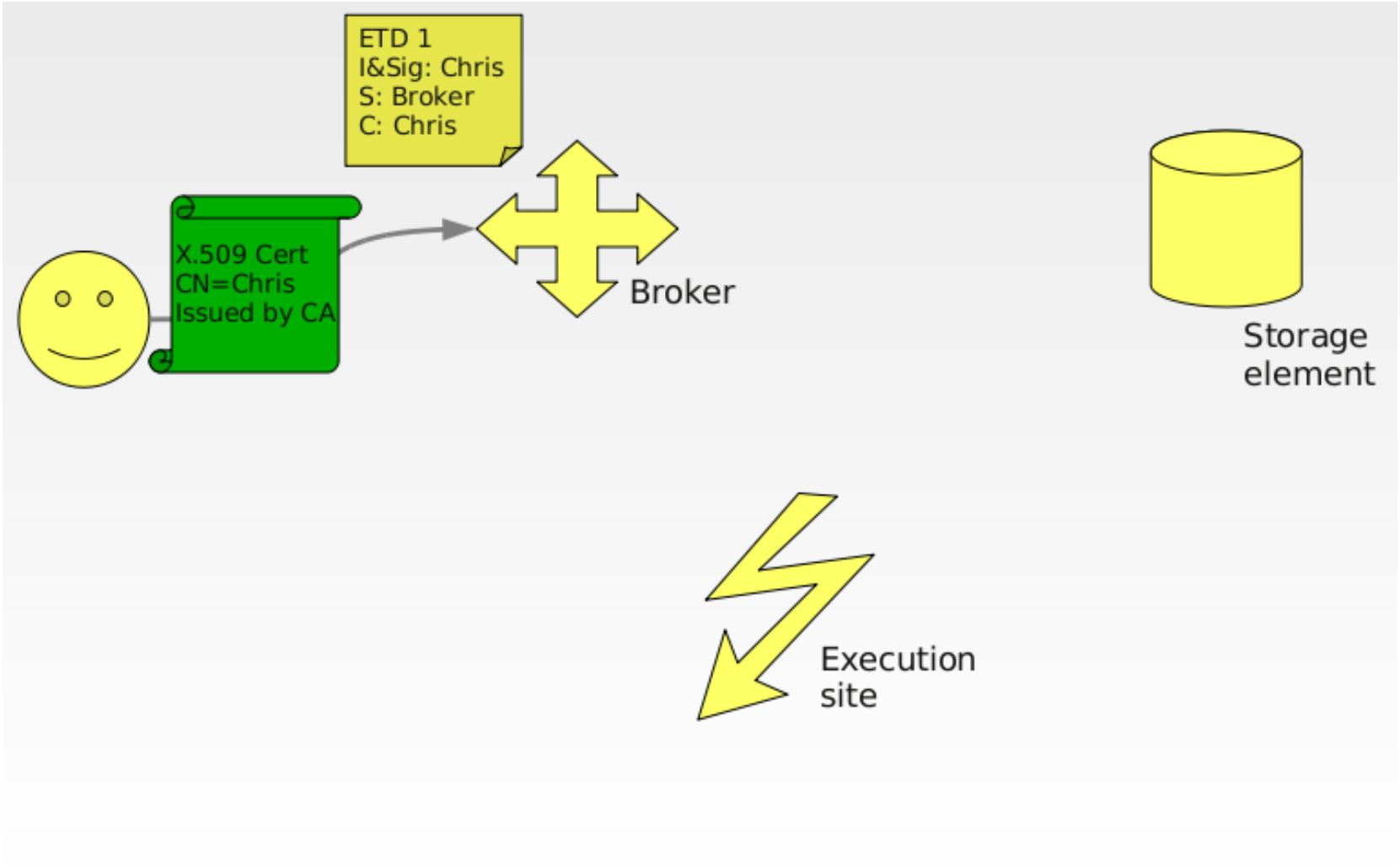
Using proxies



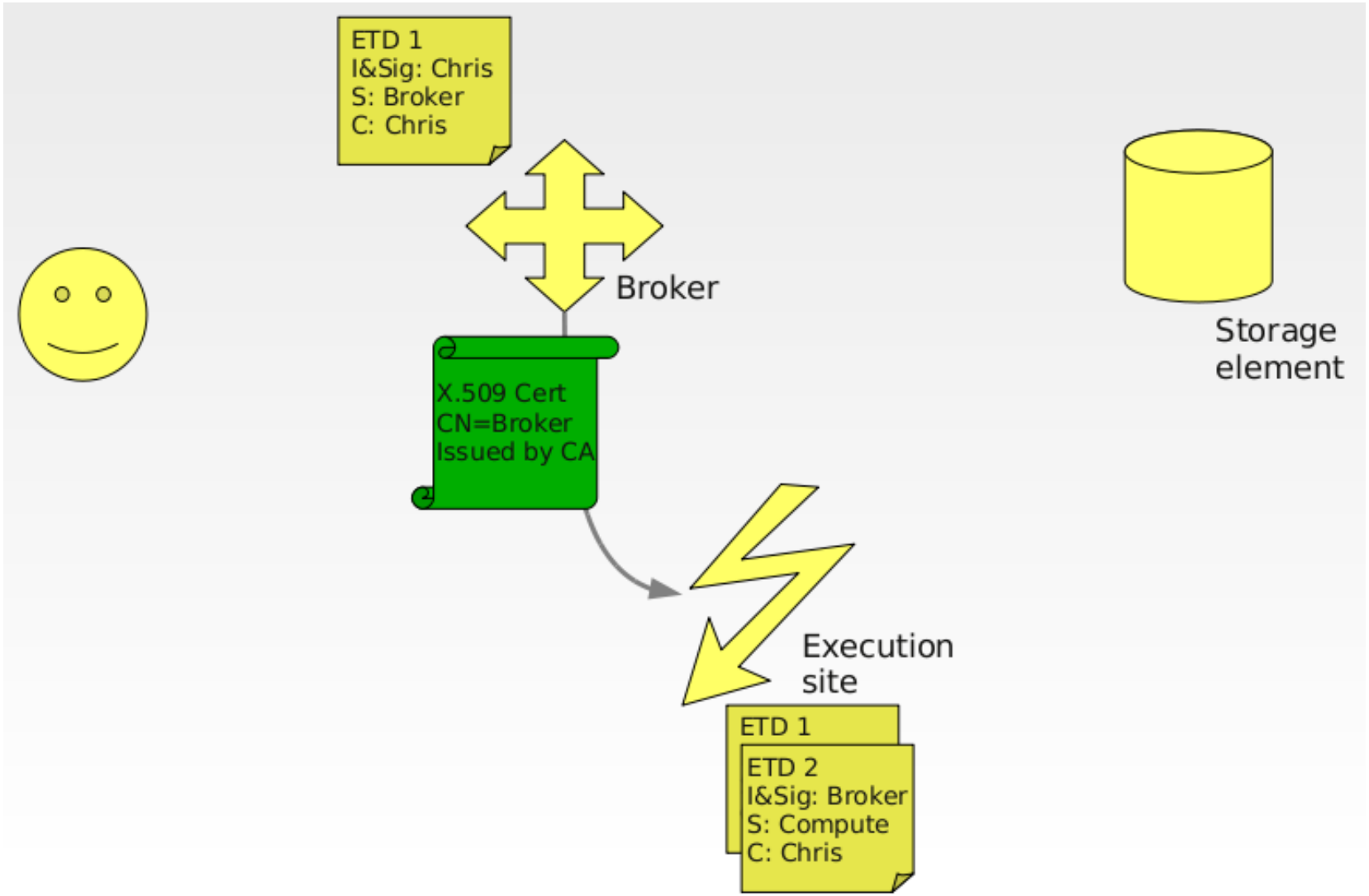
Sending Credentials to a Grid

- In UNICORE: trust delegation achieved through SAML assertions and Explicit Trust Delegation (ETD) model.
  - Client/Server model. X.509 SSLv3/TLS based AuthN.
  - User and Consignor roles are the primary concepts.
  - At the start User==Consignor
  - Server verifies the Consignor request.
  - Issues an additional SAML Assertion to next server.
- ETD SAML Assertions are chained.
  - Do not carry a sensitive Grid User data.
  - The Trust path is more transparent.

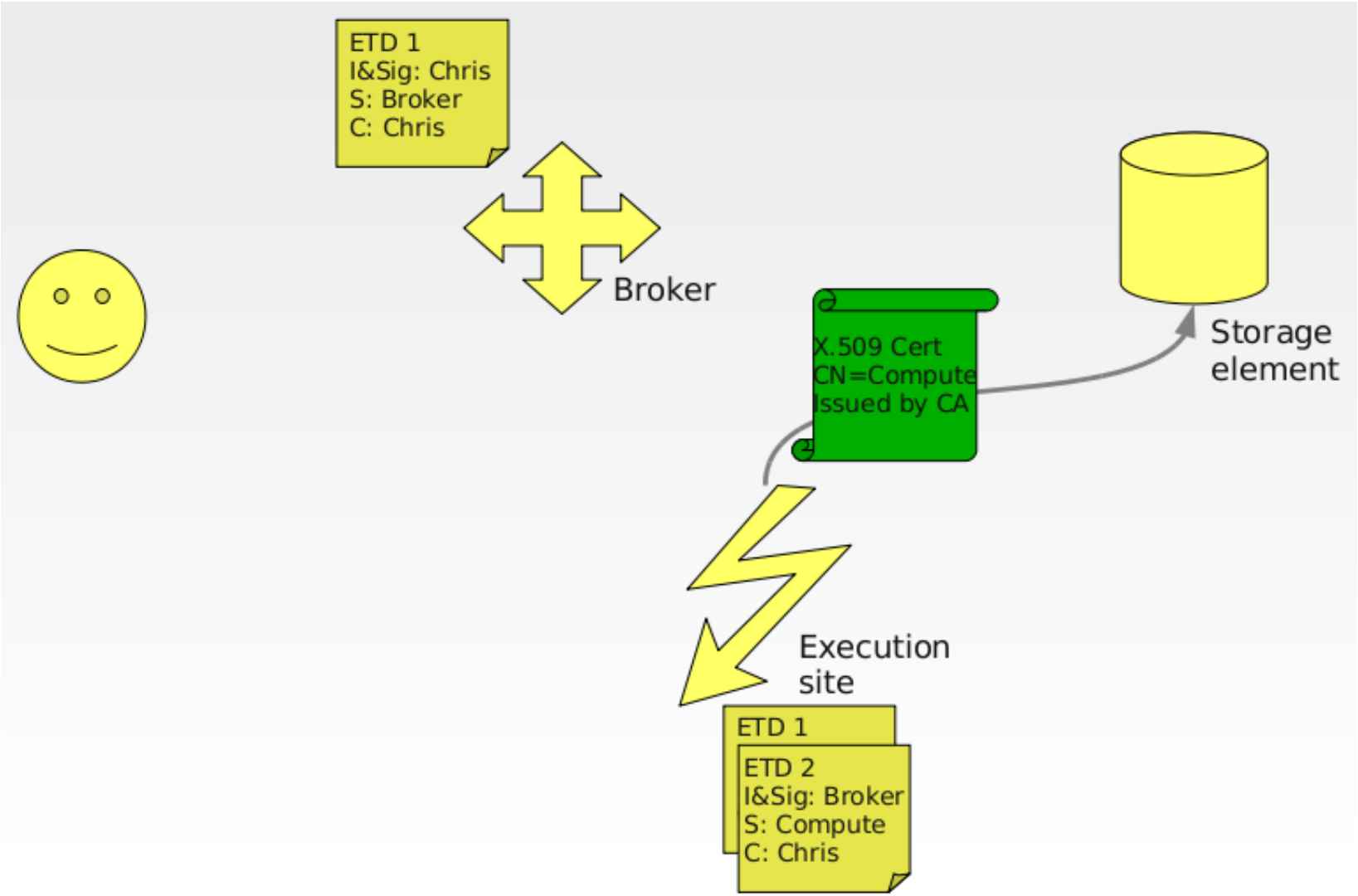
UNICORE


ETD 1
I&Sig: Chris
S: Broker
C: Chris
X.509 Cert
CN=Chris
Issued by CA
Broker
Storage
element
Execution
site

UNICORE


ETD 1
I&Sig: Chris
S: Broker
C: Chris
Broker
Storage
element
X.509 Cert
CN=Broker
Issued by CA
Execution
site
ETD 1
ETD 2
I&Sig: Broker
S: Compute
C: Chris

UNICORE

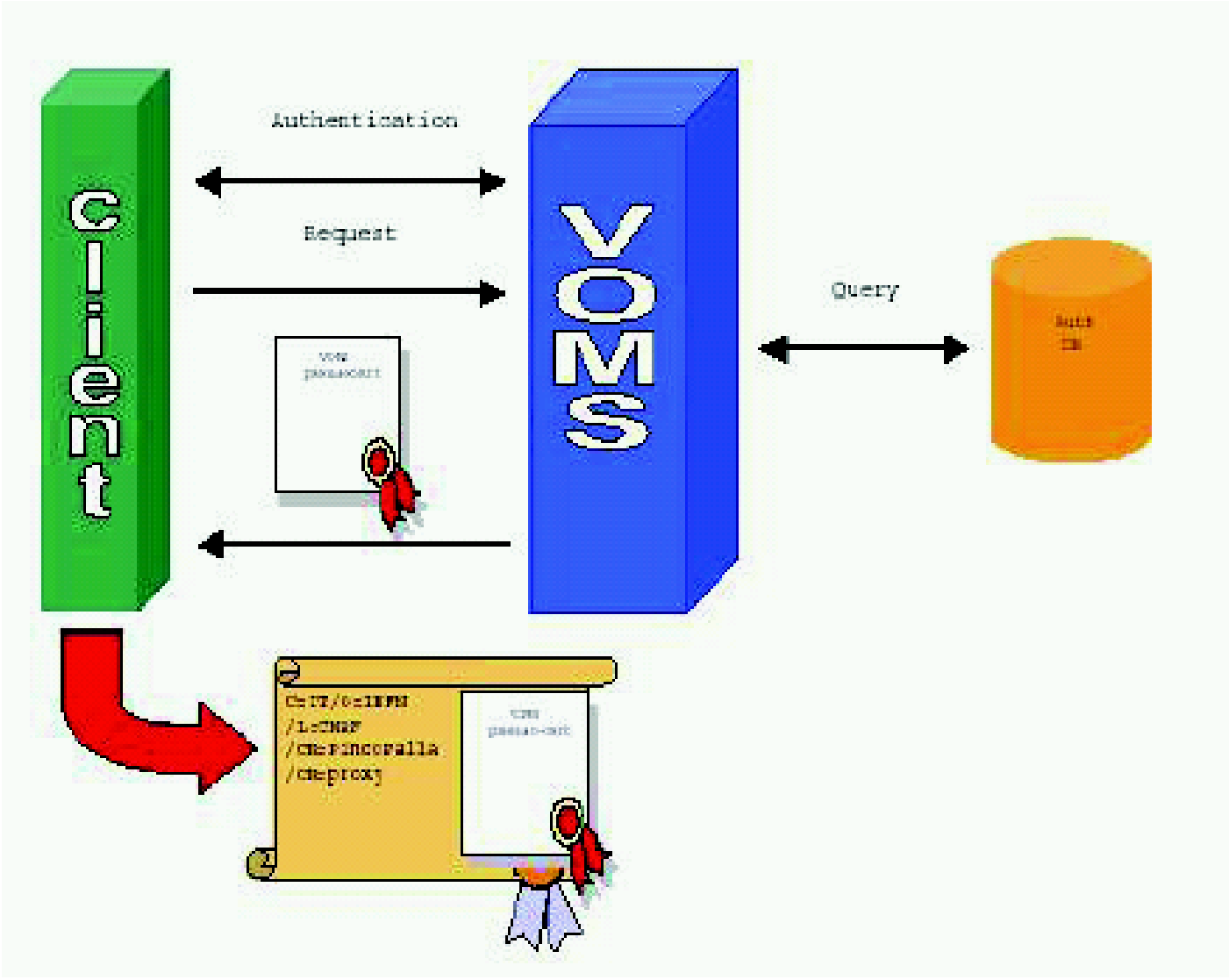

ETD 1
I&Sig: Chris
S: Broker
C: Chris
Broker
X.509 Cert
CN=Compute
Issued by CA
Storage
element
Execution
site
ETD 1
ETD 2
I&Sig: Broker
S: Compute
C: Chris

Virtual Organizations

Virtual Organization (VO): Collection of people/resources.

- Members of a VO can be grouped and hold roles.
- Membership in a VO managed by a system such as:
  - **Virtual Organization Management System (VOMS).**
  - **UNICORE Virtual Organisations System (UVOS).**
- VOMS consists:
  - VOMS server(s)
  - Administrative interface.
  - CLI clients and Java and C APIs.
- From the VO Admin point of view:
  - VOMS-Admin interface to add/delete members/groups/roles.
- From the VO member point of view:
  - Assigned to VO groups and assumes roles within groups.
  - CLI to generate proxies with VOMS groups/roles attributes.

VOMS

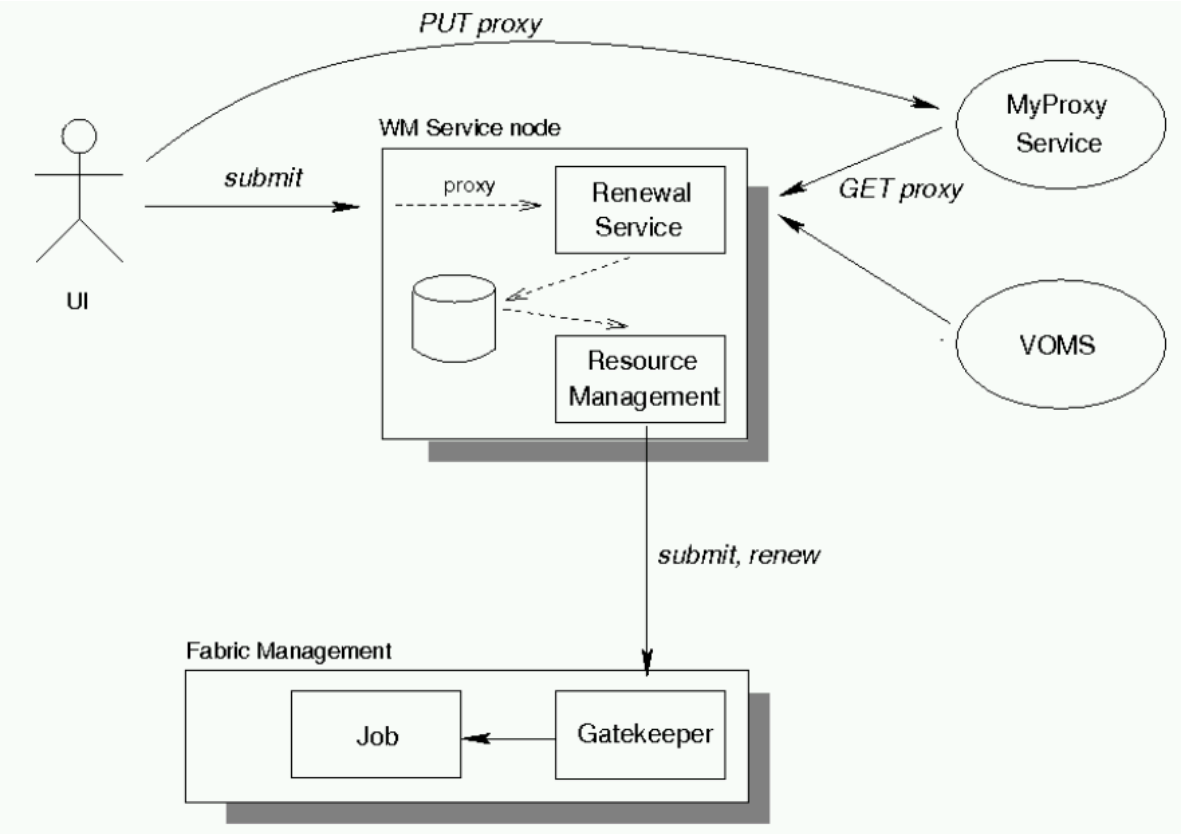


VOMS adds Attribute Certificate (AC) to your proxy!

Proxy Renewal

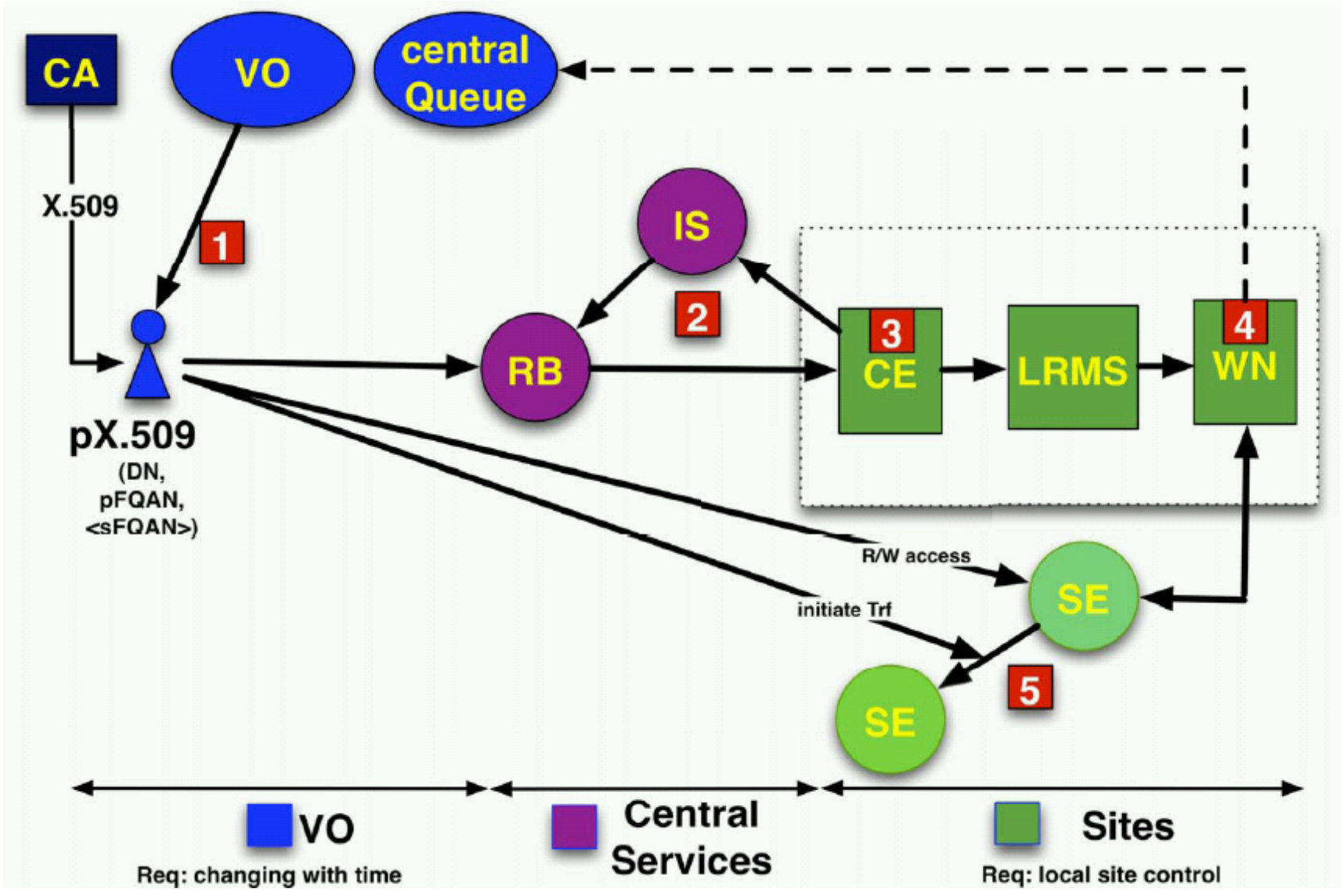
- Job broker determines correct computing element (CE).
  - gLite: **WMS.**
  - ARC: **Client Broker.**
  - UNCORE: **Not needed.**
- All phases of a job require a valid credential.
  - Submission.
  - Reading data.
  - Running on Worker Node.
  - Sending/storing results.
- Job's lifetime can easily exceed the lifetime of a proxy.
  - Overall job lifetime not known in advance.
- Inadvisable to submit a job with long-lived proxy credentials.
  - Violates the meaning of short-time proxies.
  - Increased risk if the credential is stolen.
  - Might be unacceptable for the end resources.
- **Grid User Proxy may need to be renewed.**

Job Submission



1. User puts proxy to MyProxy server (VO service).
2. Proxy is registered on the broker with job.
3. Broker contacts MyProxy for proxy renewal. (expiry near).
4. Broker contacts VOMS for Attribute Certificate.
5. Renewed credential sent to Compute Element.

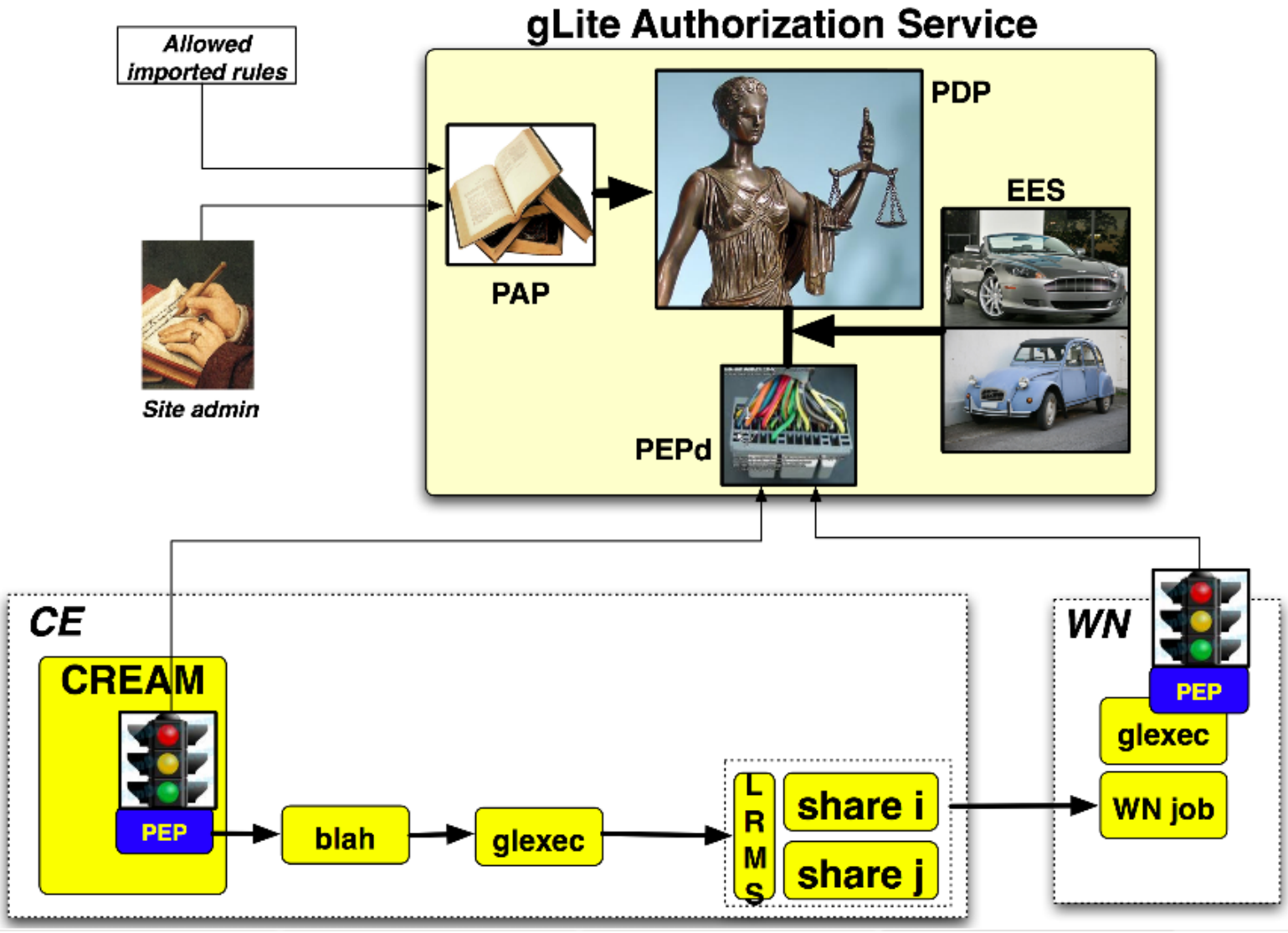
Security Domains



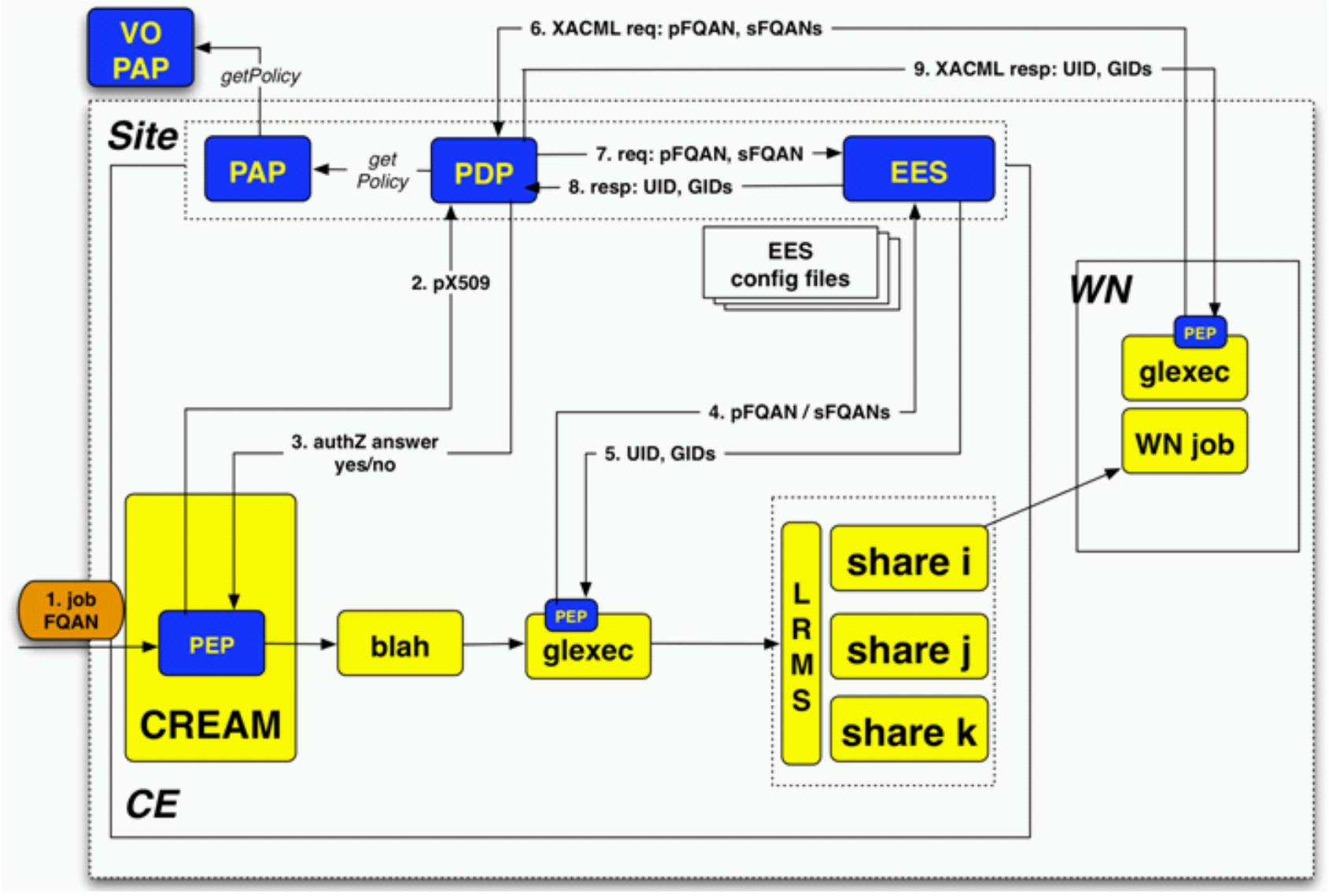
Compute Sites

- A Computing Element interacts with computing resources.
  - gLite: **CREAM.**
  - ARC: **ARC-CE**
  - UNICORE: **UNICORE/X or XNJS.**
- Interface to Local Resource Management System (LRMS).
  - Batch System eg PBS, LSF or Condor.
- LRMS sends jobs to (Grid-enabled) Worker Nodes (WNs).
- WNs receive jobs from CE and externally.
  - **Much computing power/storage available.**
  - **Potential for damage/misuse high.**
- What does the Grid User want to do?
- What is the Grid User allowed to do?
  - Authentication (AuthN).
  - Authorization (AuthZ).
- **General Authorization System... Argus.**

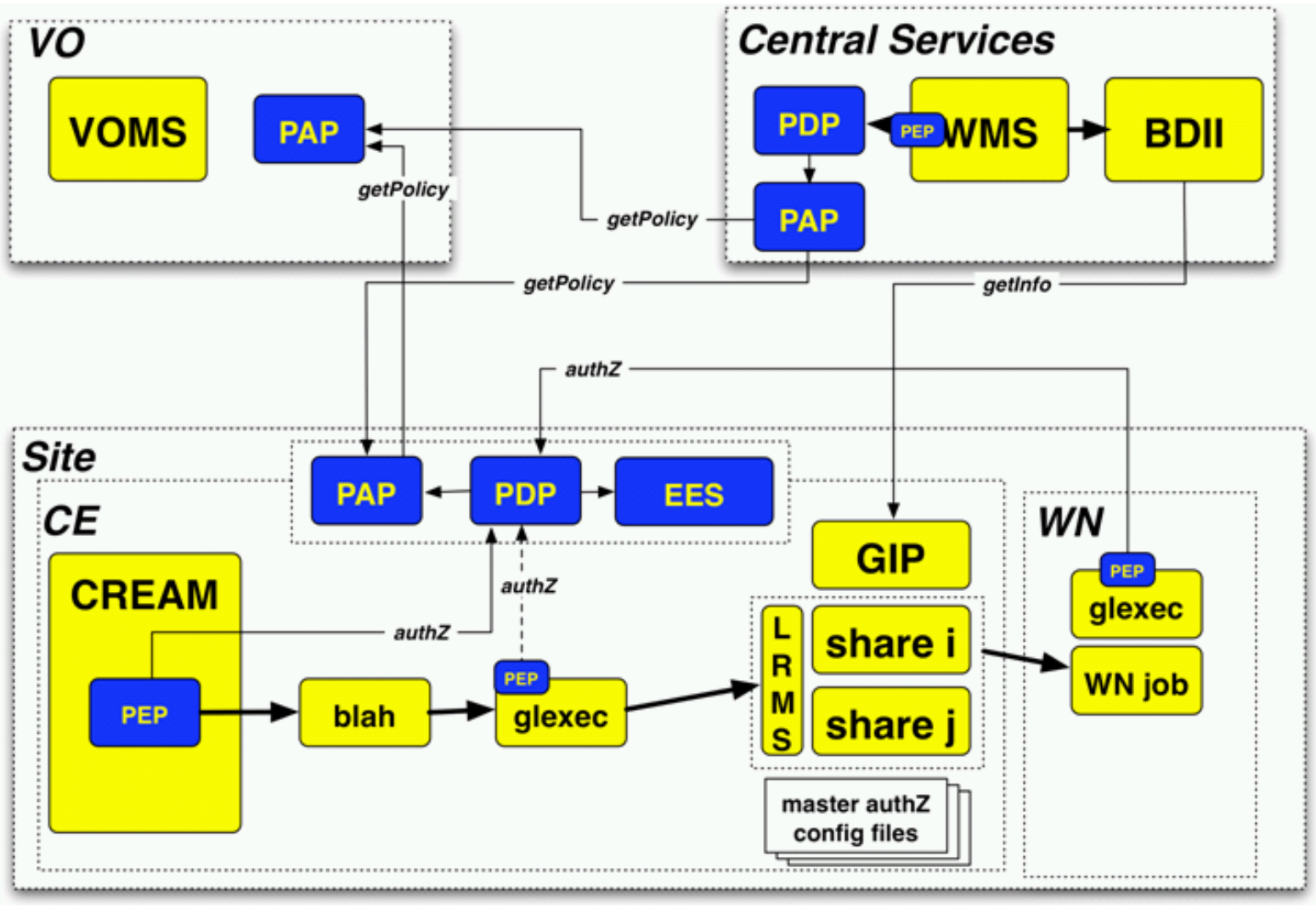
Argus AuthZ Service



Argus AuthZ Service



Argus Authorization



See: https://edms.cern.ch/document/887174/1

EMI Security

So how will Grid Security look in EMI?

- ARC, gLite and UNICORE will adopt common and standard solutions.
  - Adoption of SAML-enabled VOMS.
    - Already collaboration from UNICORE/OMII-Europe.
  - Adoption of Argus AuthZ system.
    - Common CE XACML profile.
  - Common AuthN libraries for all services.
    - Provides access to all credentials from AuthN.
  - Common SAML CE XACML profile.
    - UNICORE SAML profile starting point for common EMI profile.
  - Common solutions for other security tokens.
    - "AAI needs of DCIs" workshop next week at EGI TF.

EMI Security

So how will Grid Security look in EMI?

- ARC, gLite and UNICORE will adopt common and standard solutions.
  - Adoption of SAML-enabled VOMS.
    - Already collaboration from UNICORE/OMII-Europe.
  - Adoption of Argus AuthZ system.
    - Common CE XACML profile.
  - Common AuthN libraries for all services.
    - Provides access to all credentials from AuthN.
  - Common SAML CE XACML profile.
    - UNICORE SAML profile starting point for common EMI profile.
  - Common solutions for other security tokens.
    - "AAI needs of DCIs" workshop next week at EGI TF.

We still have work to do...