Security

David Fergusson

Material from:

Andrea Sciabà

Åke Edlund, JRA3 Manager, KTH

David Groep, EUGridPMA chair, NIKHEF

www.eu-egee.org

Overview

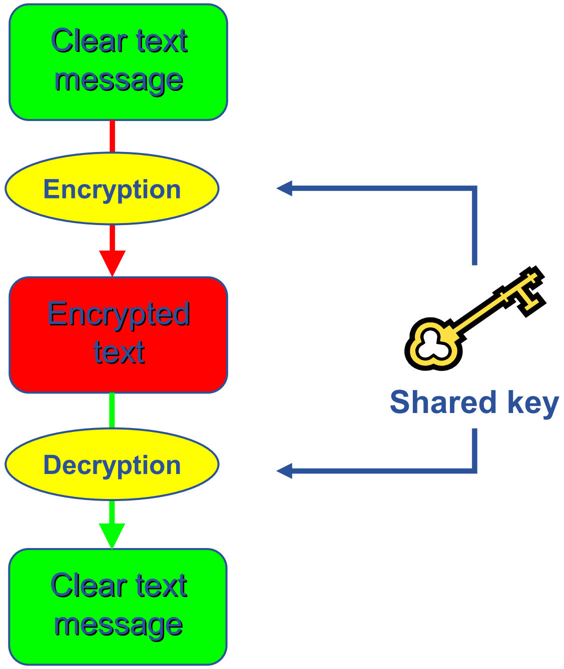
- Basic security concepts
- Certificates
- Virtual Organisations
- Command line interface

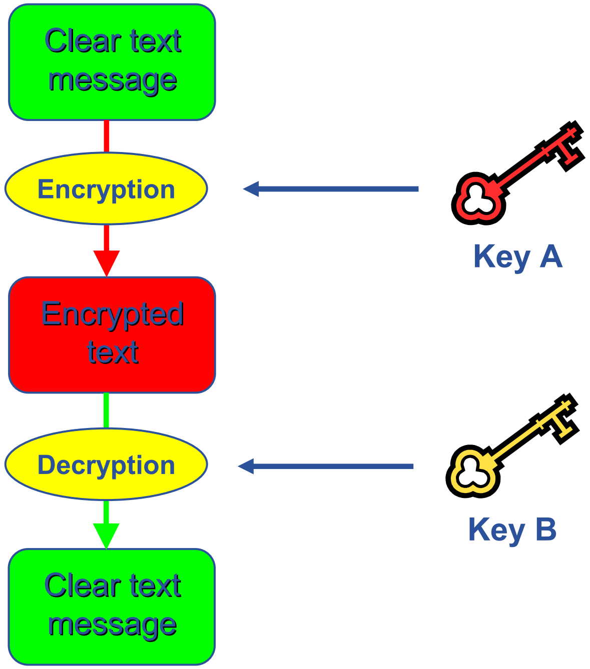
Basic security concepts

- Principal
  - An entity: a user, a program, or a machine
- Credentials
  - Some data providing a proof of identity
- Mechanism
  - software providing data authentication or confidentiality (e.g. Kerberos, GSI)
- Authentication
  - Verify the identity of the peer
- Authorization
  - Map an entity to some set of privileges
- Confidentiality
  - Encrypt the message so that only the recipient can understand it
- Integrity
  - Ensure that the message has not be altered in the transmission
- Non-repudiation
  - Impossibility of denying the authenticity of a digital signature

Encryption

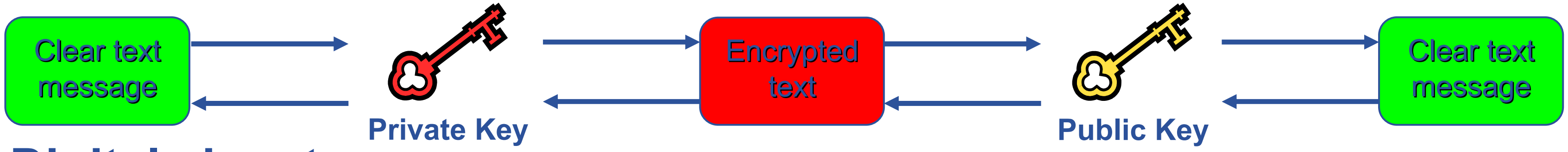
- **Symmetric encryption: same key (“secret”) used for encryption and decryption**
  - Kerberos, DES / 3DES, IDEA
- **Asymmetric encryption: different keys used for encryption and decryption**
  - RSA, DSA





Public Key Infrastructure

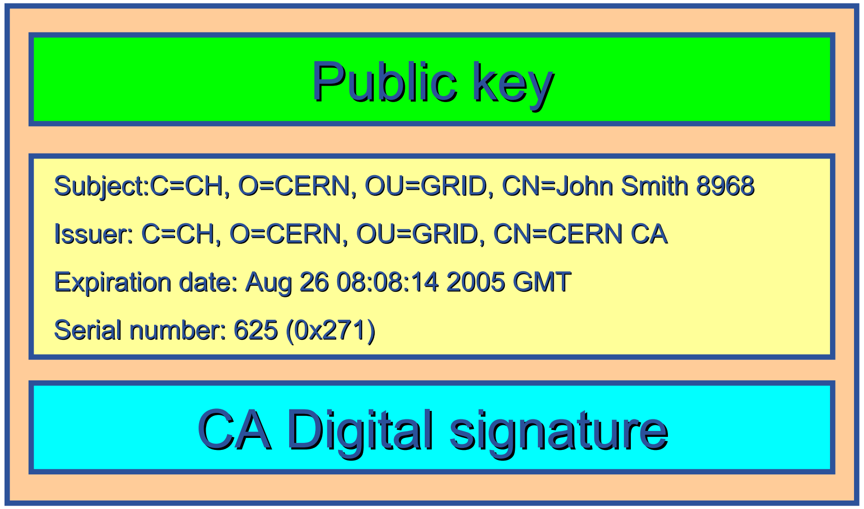
- Provides authentication, integrity, confidentiality, non-repudiation
- Asymmetric encryption



- Digital signatures
  - A hash derived from the message and encrypted with the signer's private key
  - Signature checked decrypting with the signer's public key
- Allows key exchange in an insecure medium using a **trust model**
  - Keys trusted only if signed by a trusted third party (Certification Authority)
  - A CA certifies that a key belongs to a given principal
- Certificate
  - Public key + information about the principal + CA signature
  - X.509 format most used
- PKI used by SSL, PGP, GSI, WS security, S/MIME, etc.

X.509 certificates and authentication

Structure of a X.509 certificate



Public key

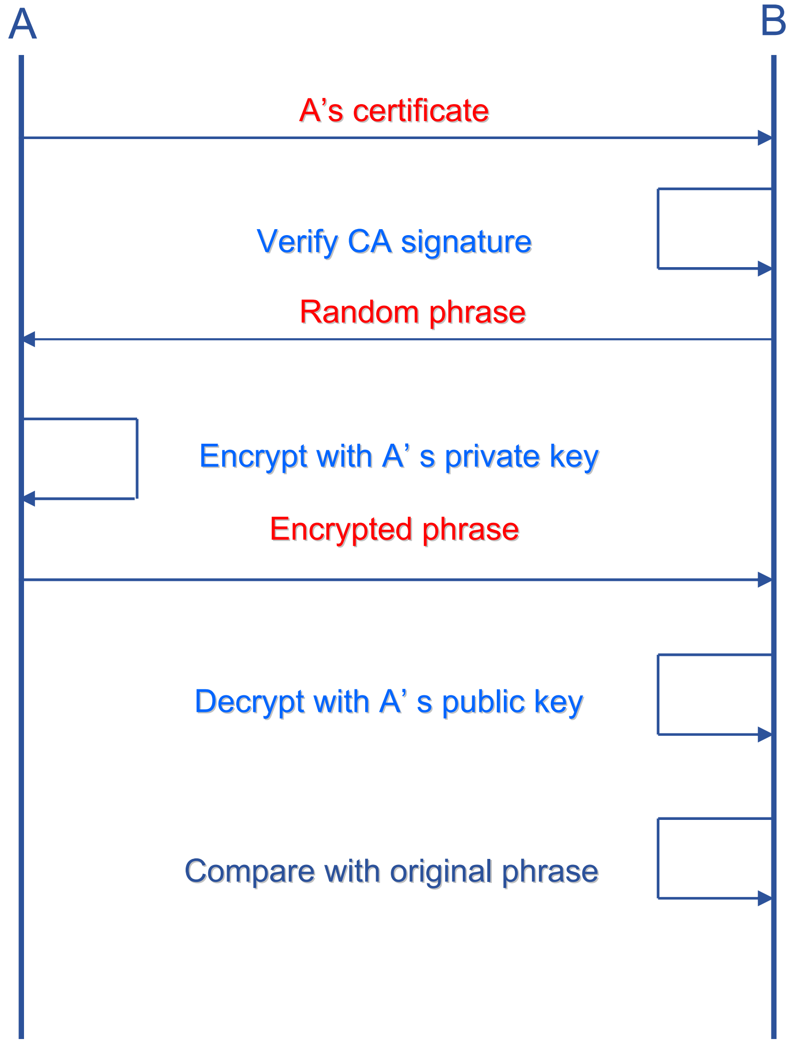
Subject:C=CH, O=CERN, OU=GRID, CN=John Smith 8968

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

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

Serial number: 625 (0x271)

CA Digital signature



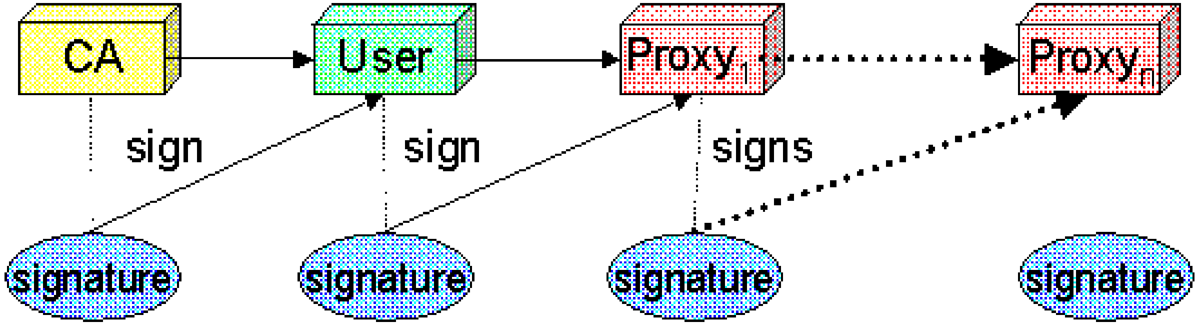
A
B
A’s certificate
Verify CA signature
Random phrase
Encrypt with A’ s private key
Encrypted phrase
Decrypt with A’ s public key
Compare with original phrase

Certification Authorities

- **Issue certificates for users, programs and machines**
- **Check the identity and the personal data of the requestor**
  - Registration Authorities (RAs) do the actual validation
- **Manage Certificate Revocation Lists (CRLs)**
  - They contain all the revoked certificates yet to expire
- **CA certificates are self-signed**
- **LCG-2 recognizes a given set of CAs**
  - https://lcg-registrar.cern.ch/pki_certificates.html

Globus Grid Security Infrastructure (GSI)

- *de facto* **standard for Grid middleware**
- **Based on PKI**
- **Implements some important features**
  - Single sign-on: no need to give one’s password every time
  - Delegation: a service can act on behalf of a person
  - Mutual authentication: both sides must authenticate to the other
- **Introduces proxy certificates**
  - Short-lived certificates including their private key and signed with the user’s certificate



More on proxy certificates and delegation

- **Delegation**
  - Allowing something else (eg. a file transfer service) to use my credentials
- **Proxies can be moved over a network**
- **Subject identifies the user:**
  - User subject: `/C=CH/O=CERN/OU=GRID/CN=Andrea Sciaba 8968`
  - Proxy subject: `/C=CH/O=CERN/OU=GRID/CN=Andrea Sciaba 8968/CN=proxy`
- **Full proxy**
  - A proxy created from a user certificate or another full proxy with normal delegation
- **Limited proxy**
  - A proxy created from a proxy with limited delegation, or from another limited proxy
- **What does that mean?**
  Entities can decide to accept only full proxies. Examples:
  - GridFTP accepts all proxies
  - Globus gatekeeper accepts only full proxies

Enabling Grids for E-sciencE

Virtual Organizations and authorization

- **LCG-2 users MUST belong to a Virtual Organization**
  - Sets of users belonging to a collaboration
  - Each VO user has the same access privileges to Grid resources
  - List of supported VOs:
    - https://lcg-registrar.cern.ch/virtual_organization.html
- **VOs maintain a list of their members**
  - The list is downloaded by Grid machines to map user certificate subjects to local "pool" accounts: only mapped users are authorized in LCG

```
...
"/C=CH/O=CERN/OU=GRID/CN=Simone Campana 7461" .dteam
"/C=CH/O=CERN/OU=GRID/CN=Andrea Sciaba 8968" .cms
"/C=CH/O=CERN/OU=GRID/CN=Patricia Mendez Lorenzo-ALICE" .alice
...
```

grid-mapfile

  - Sites decide which VOs to accept

GSI environment variables

- **User certificate files:**
  - Certificate: X509_USER_CERT (default: `$HOME/.globus/usercert.pem`)
  - Private key: X509_USER_KEY (default: `$HOME/.globus/userkey.pem`)
  - Proxy: X509_USER_PROXY (default: `/tmp/x509up_u<id>`)
- **Host certificate files:**
  - Certificate: X509_USER_CERT (default: `/etc/grid-security/hostcert.pem`)
  - Private key: X509_USER_KEY (default: `/etc/grid-security/hostkey.pem`)
- **Trusted certification authority certificates:**
  - X509_CERT_DIR (default: `/etc/grid-security/certificates`)
- **Location of the grid-mapfile:**
  - GRIDMAP (default: `/etc/grid-security/grid-mapfile`)

Command line interface: certificate and proxy management

- Get information on a user certificate
  - `grid-cert-info[-help] [-file certfile] [OPTION]...`

`-all`	whole certificate
`-subject │ -s`	subject string
`-issuer │ -I`	Issuer
`-startdate │ -sd`	Start of validity
`-enddate │ -ed`	End of validity

- Create a proxy certificate
  - `grid-proxy-init`
- Destroy a proxy certificate
  - `grid-proxy-destroy`
- Get information on a proxy certificate
  - `grid-proxy-info`

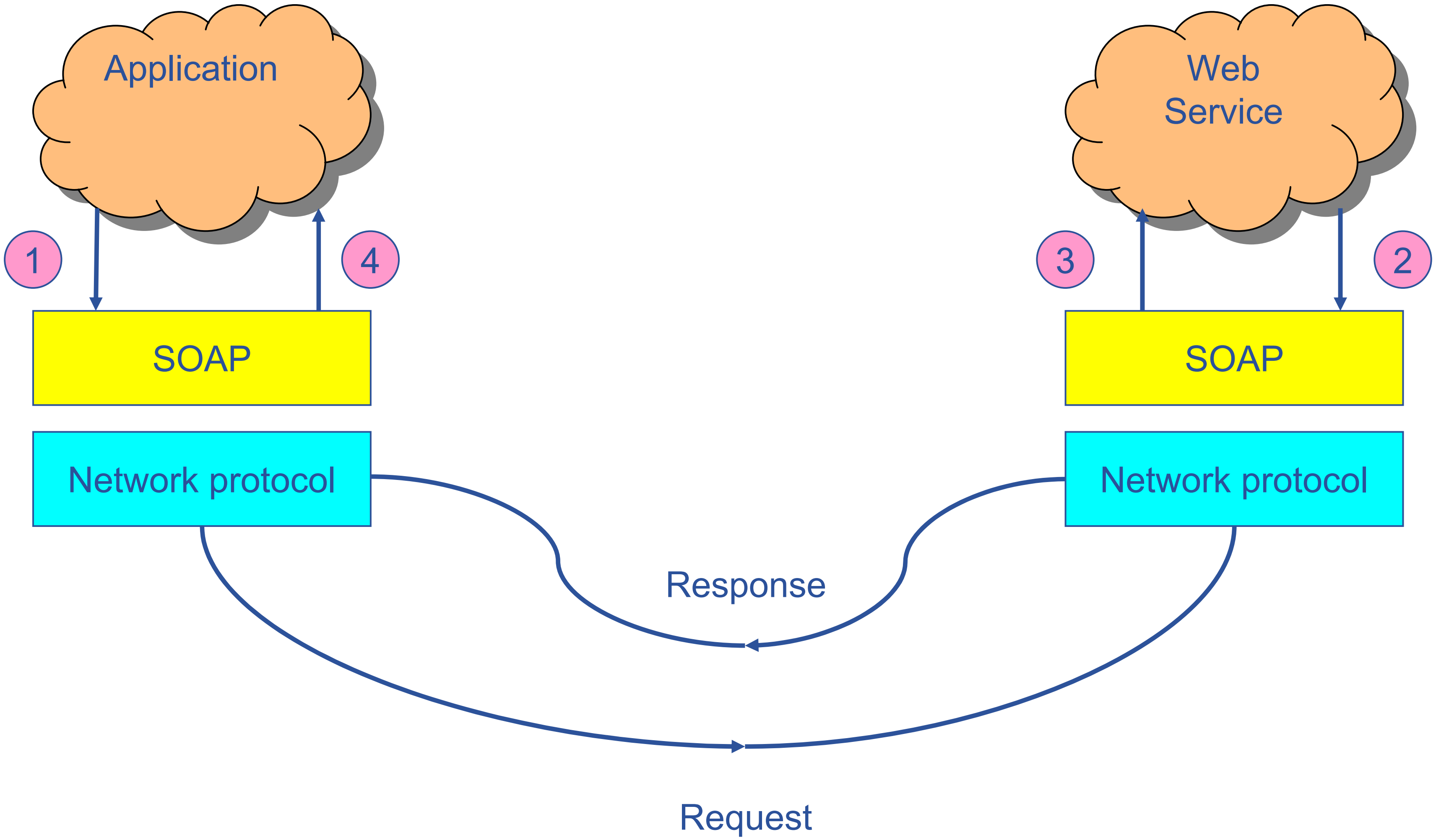
Long term proxy

- **Proxy has limited lifetime (default is 12 h)**
  - Bad idea to have longer proxy
- **However, a grid task might need to use a proxy for a much longer time**
  - Grid jobs in HEP Data Challenges on LCG last up to 2 days
- **myproxy server:**
  - Allows to create and store a long term proxy certificate:
  - `myproxy-init -s <host_name>`
    - `-s <host_name>` specifies the hostname of the myproxy server
  - `myproxy-info`
    - Get information about stored long living proxy
  - `myproxy-get-delegation`
    - Get a new proxy from the MyProxy server
  - `myproxy-destroy`
- **A service running continously can renew automatically a proxy created from a long term use proxy and use it to interact with the Grid**
  - Examples: automatic job dispatchers or data movers

Security APIs in LCG-2

- **Currently, there are no security APIs developed specifically by LCG**
- **The existing APIs come from other projects**
  - Authentication
    - Globus GSS-API, GSS Assist, COG Kits (Java and Python)
    - some gSOAP plugins (CERN, Lecce University)
  - Authorization
    - LCAS plugins
    - LCMAPS plugins
    - VOMS API
    - some gSOAP plugins (CERN, Lecce University)
- **The documentation is generally not good**

Web services



Web Service Security

- **Message level security**
  - WS-Security
    - set of SOAP extensions to implement integrity and confidentiality in Web Services
    - <Security> header contains the security-related information
    - http://www-128.ibm.com/developerworks/library/ws-secure/
  - WS-SecureConversation
    - defines how to establish secure contexts and exchange keys
  - Used in Globus Toolkit 3
- **Transport level security**
  - SOAP messages are transmitted encrypted
  - used by some gSOAP GSI plugins

EGEE JRA3 Objectives

- **Enable secure operation of a European Grid infrastructure**
  - Develop security architectures, frameworks and policies
  - Definition of incident response methods and authentication policies
- **Consistent design of security mechanisms for all core Grid services**
  - Meet production needs of resource providers with regard to identity, integrity and protection
- **Provide robust, supportable security components (as part of JRA1)**
  - Select, re-engineer, integrate identified Grid Services
- **Selection of security components is based on requirements of:**
  - Middleware developers
  - Applications
  - Grid operations

Introduction - Achievements, Issues and Mitigation

Major achievements

- Producing key security deliverables (well received in the community)
  - Global Security Architecture
  - Site Access Control Architecture
- Delivered a number of security modules, of which four will be part of gLite v1
- Driving community level agreements for middleware and policy
  - EUGridPMA

Major issues and mitigation

- Geographically distributed teams
  - Need to improve the handing over of security modules to the middleware developers. More F2F meetings.
  - Improve further contact with NA4, applications.
- Conflicting/challenging security requirements from applications and operations
  - Proposed solutions meeting the sets of requirements as much as possible.

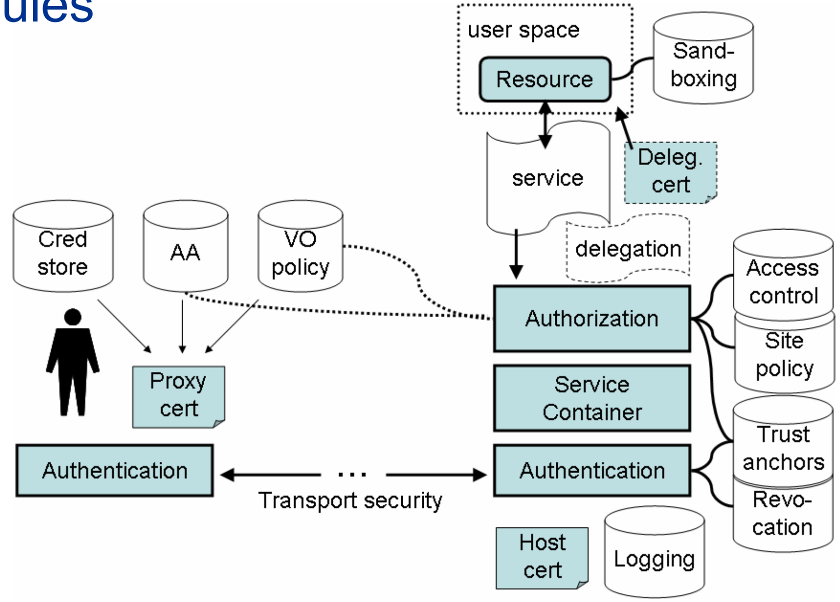
Architecture - Baseline assumptions

- **Security Architecture - Modular, Agnostic, Standard, Interoperable**
  - Modular – possible to add new modules later
  - Agnostic – implementation independent
  - Standard – e.g. start with transport-level security but intend to move to message-level security when it matures
  - Interoperable - at least for AuthN & AuthZ
  - Applied to Web-services hosted in containers (Apache Axis & Tomcat) and applications as additional modules

Requirement: Support for legacy and non-WS based software components

Solution: Modular authentication and authorization software suitable for integration

Fulfilled/Time frame: Yes/Now



Major security issues with current production service

Major issues

- Many of the services do not have authentication.
- Procedural issues, e.g. in incident handling
- No resource control on the local clusters
- Proliferation of network connectivity (especially outbound)
- Users store private credentials on NFS file systems

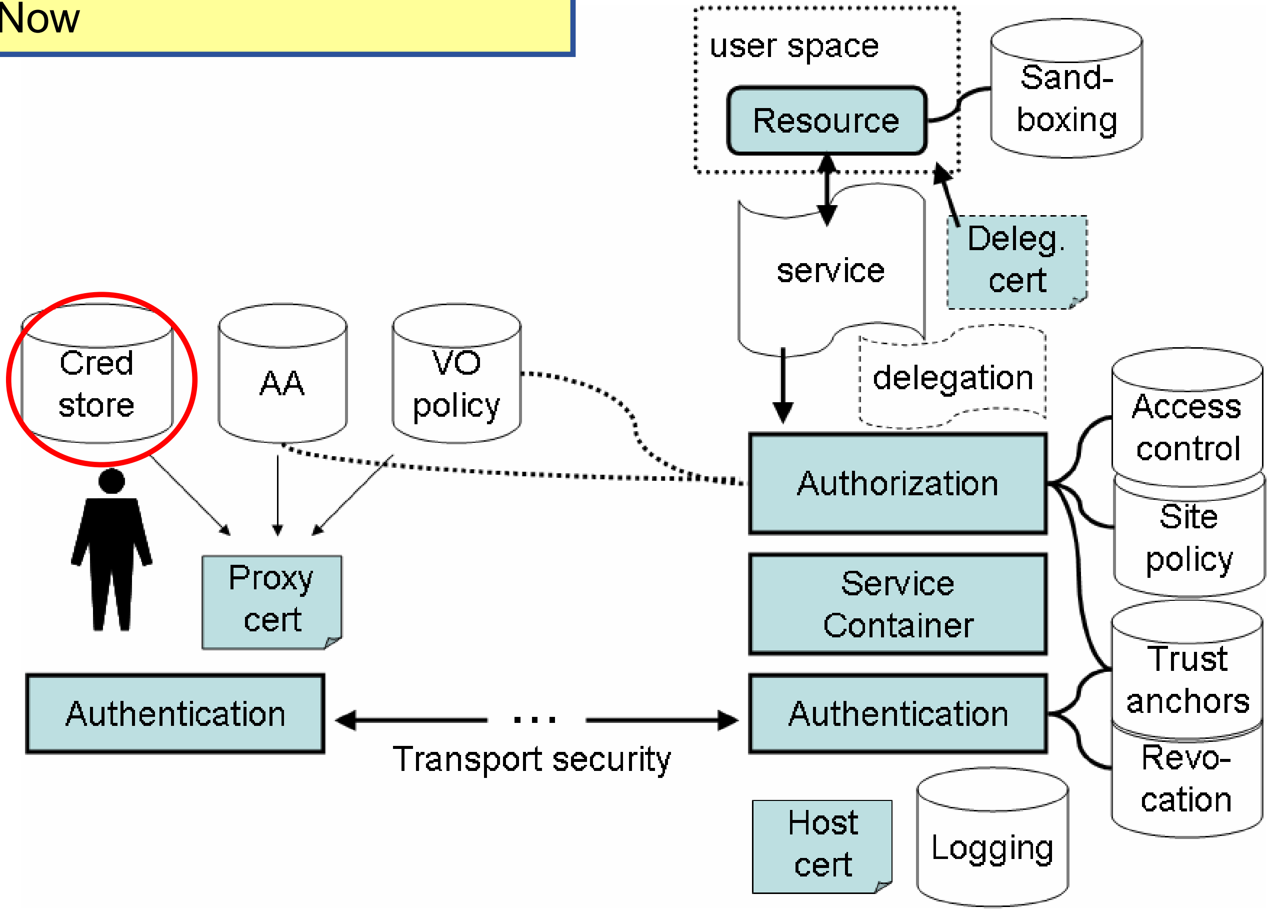
Will gLite be any better?

gLite will have less of these limitations, but we will still need to use and deploy the software correctly and within its limitations

- Better and more flexible tools for authorization and credential management
- Improved operational procedures and processes
- New services and solutions addressing the need of new applications

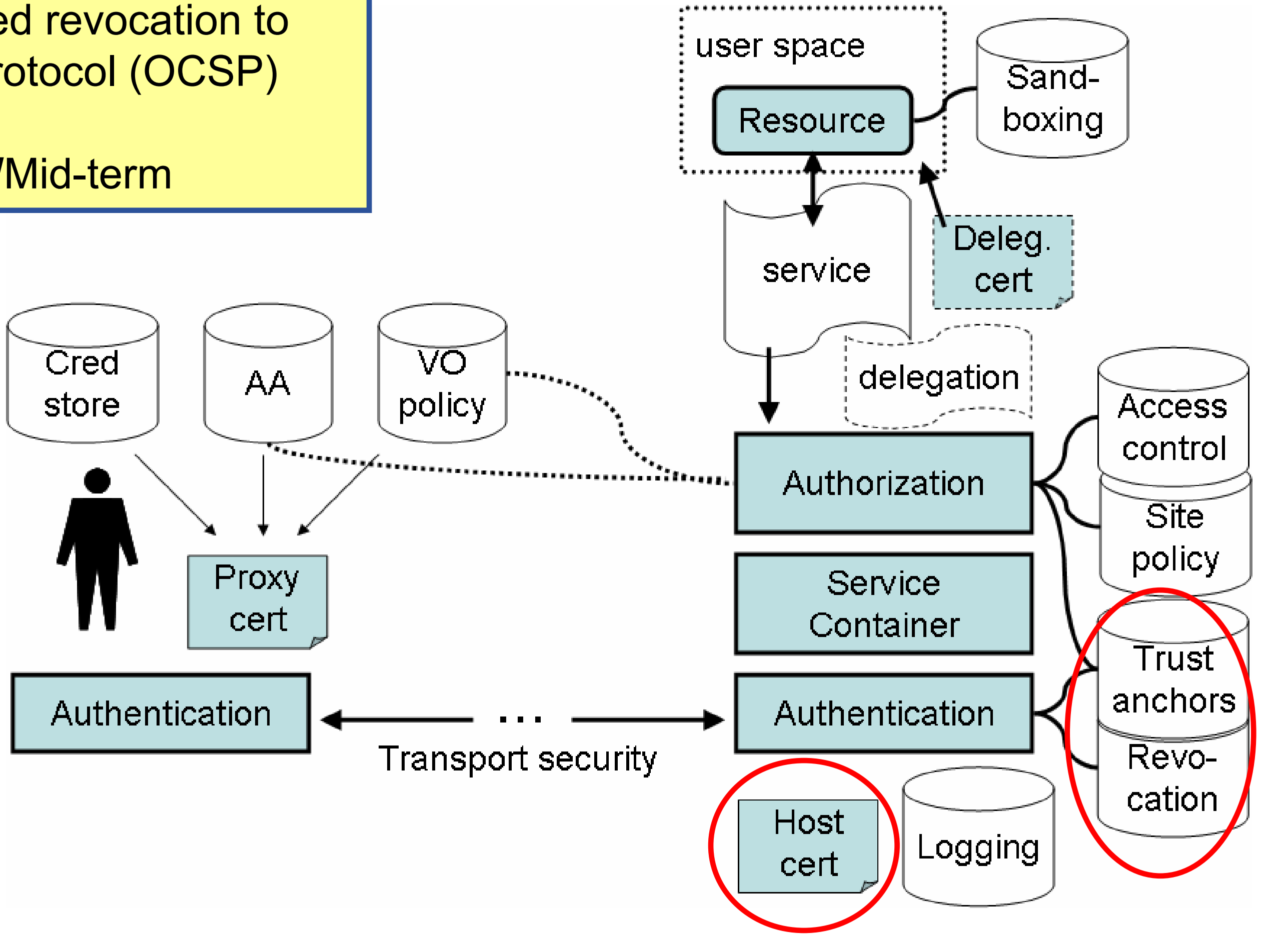
Services - Authentication

Managed credential storage ensures proper security of credentials. Password-scrambled files should go away
Fulfilled/Time frame: Yes/Now



Services - Authentication

Requirement: Timely credential revocation
Solution: Gradual transition from Certificate Revocation List (CRL) based revocation to Online Certificate Status Protocol (OCSP) based revocation
Fulfilled/Time frame: Yes/Mid-term



Services - TLS vs MLS

Transport Level Security

–Uses widely deployed TLS/SSL protocol

–Does not provides security through intermediate hosts (can be done using delegation, not yet delivered).

Message Level Security

–Uses Web Services or SOAP messages security technology

–Recommended by WS-I Consortium as preferable WS-Security solution

–Performance and support issues

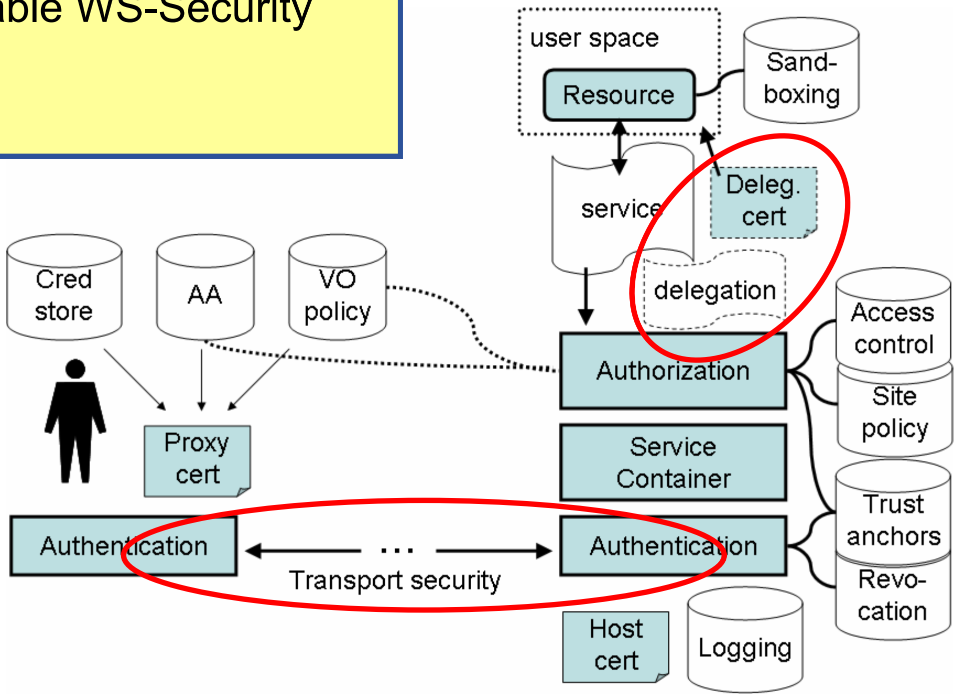
So, TLS for now

–SOAP over HTTPS with proxy cert supported path validation

–WS interface for delegation

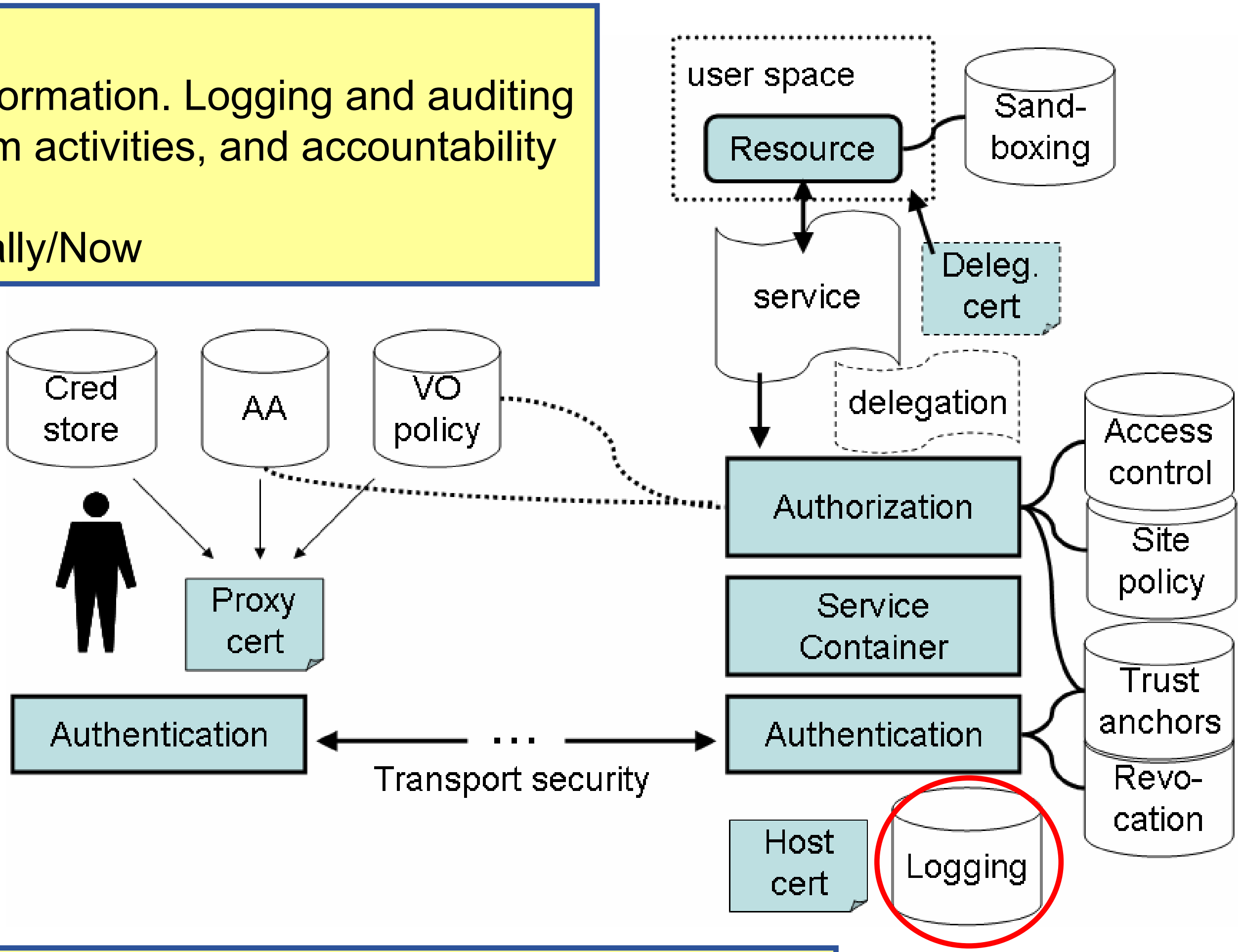
–**Move to MLS as we go along**

–Use cases for MLS exist already (DM)



Services - Logging and Auditing

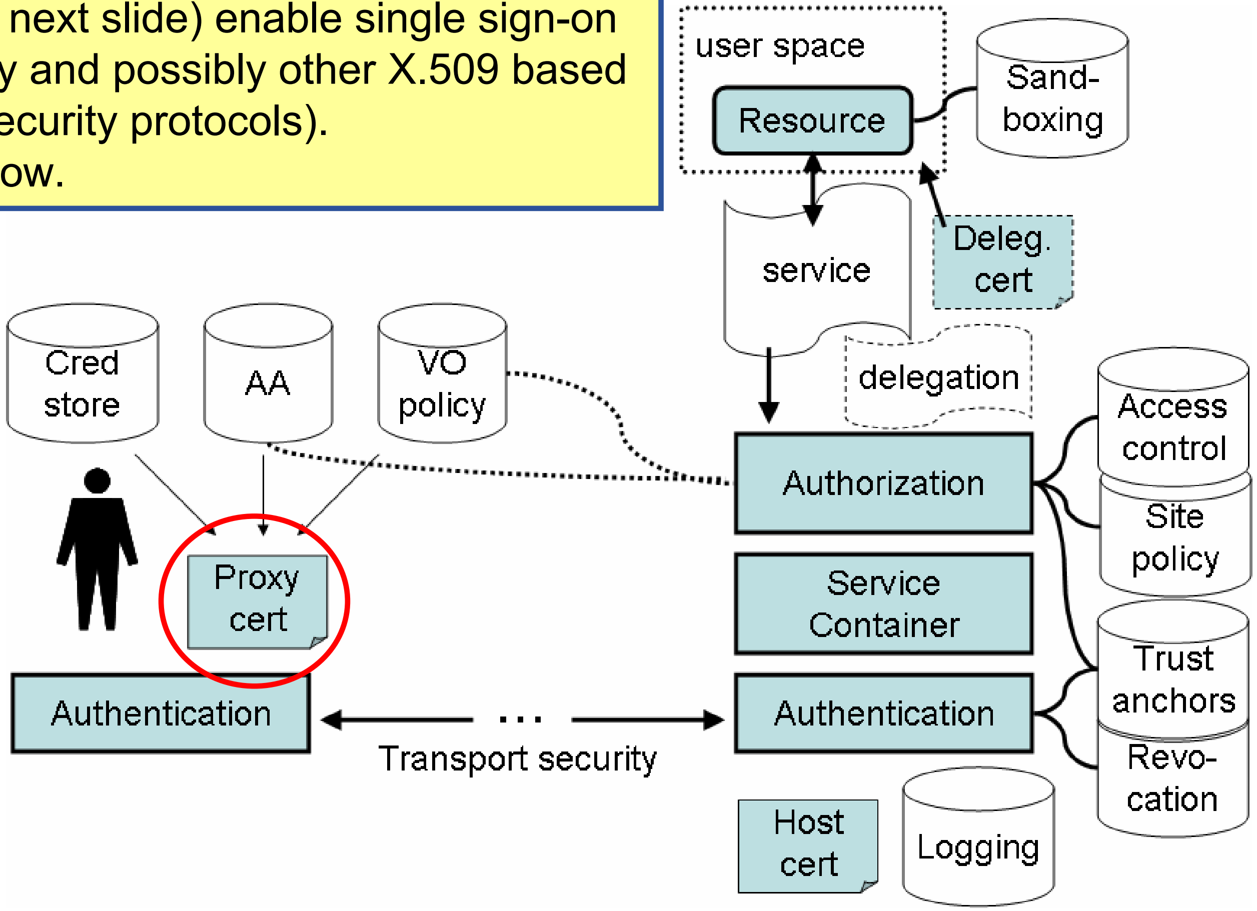
Requirement: Audit ability
Solution: Meaningful log information. Logging and auditing ensures monitoring of system activities, and accountability in case of a security event
Fulfilled/Time frame: Partially/Now



Requirement:. Accountability
Solution: All relevant system interactions can be traced back to a user
Fulfilled/Time frame: Yes/Now

Services - Authentication

Requirement: Single sign-on.
Solution: Proxy certificates and a global authentication infrastructure (**EUGridPMA** - next slide) enable single sign-on (using TLS, GSI, WS-Security and possibly other X.509 based transport or message-level security protocols).
Fulfilled/Time frame: Yes/Now.



Global authentication infrastructure

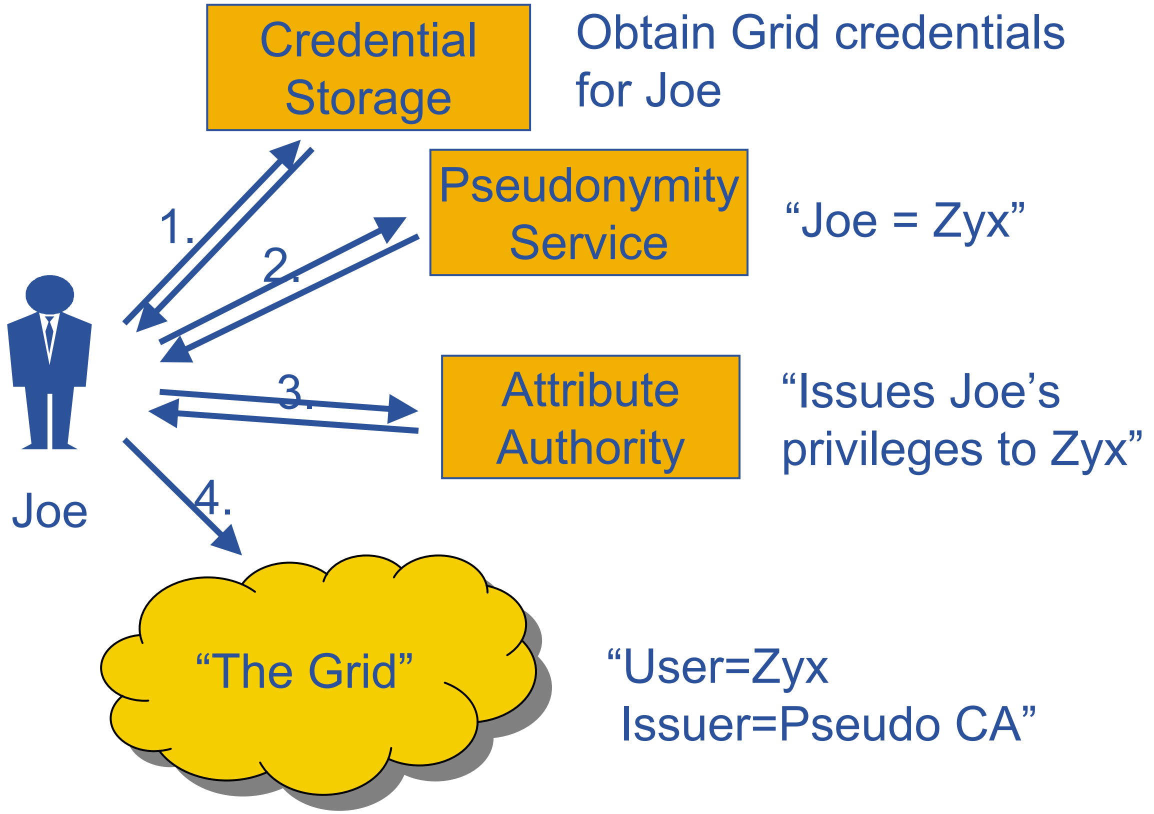
EUGridPMA (Chair: David Groep, JRA3)

European **Grid** Authentication **P**olicy
Management **A**uthority for e-Science

- Setting **guidelines and minimum requirements** for Grid authentication for e-Science
- Now a Global federation of grid identity providers, based on EUGridPMA requirements: **the International Grid Federation (IGF)**
- **EUGridPMA was the driving example** for similar groups in Asian-Pacific and the Americas
- Coverage of Europe almost complete
  - **30 accredited members**
  - 7 non-EU countries + 1 treaty organization
- **Initiative strongly encouraged by the eInfrastructures Reflection Group (eIRG)**

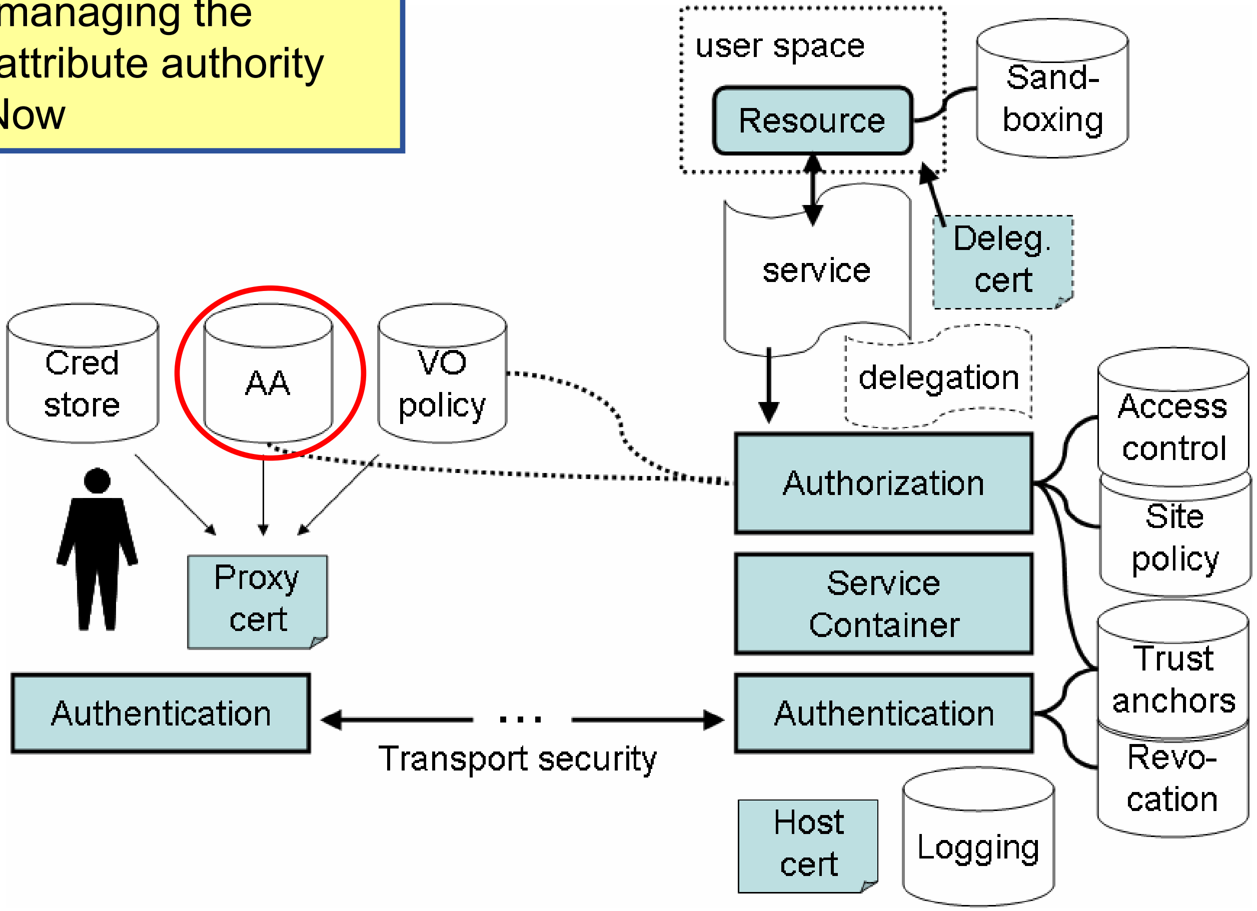
Services - Authentication

Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
Fulfilled/Time frame: Partially/Mid-term



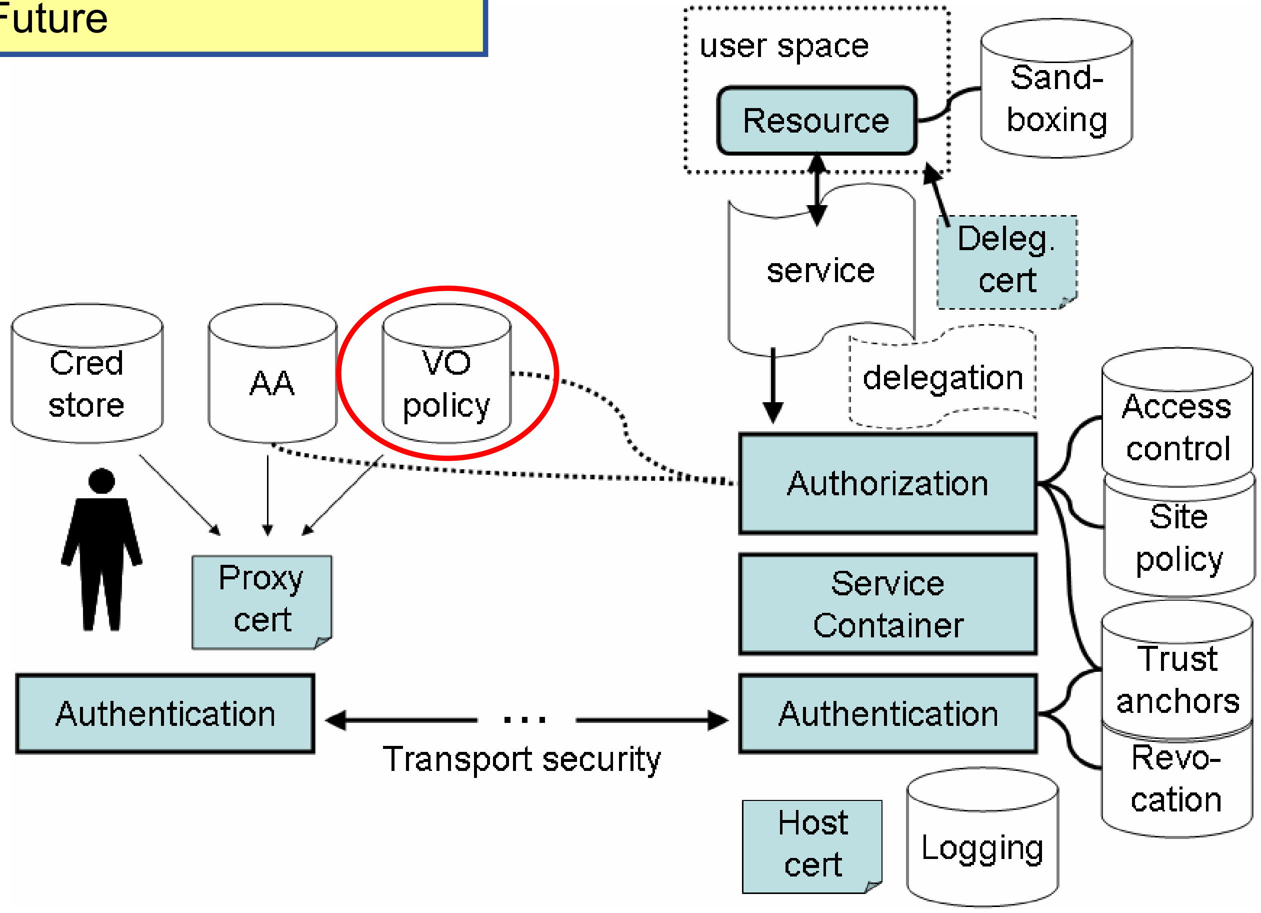
Services - Authorization

Requirement: VO managed access control
Solution: The Virtual Organization Membership Service (VOMS) is used for managing the membership to VOs and as attribute authority
Fulfilled/Time frame: Yes/Now



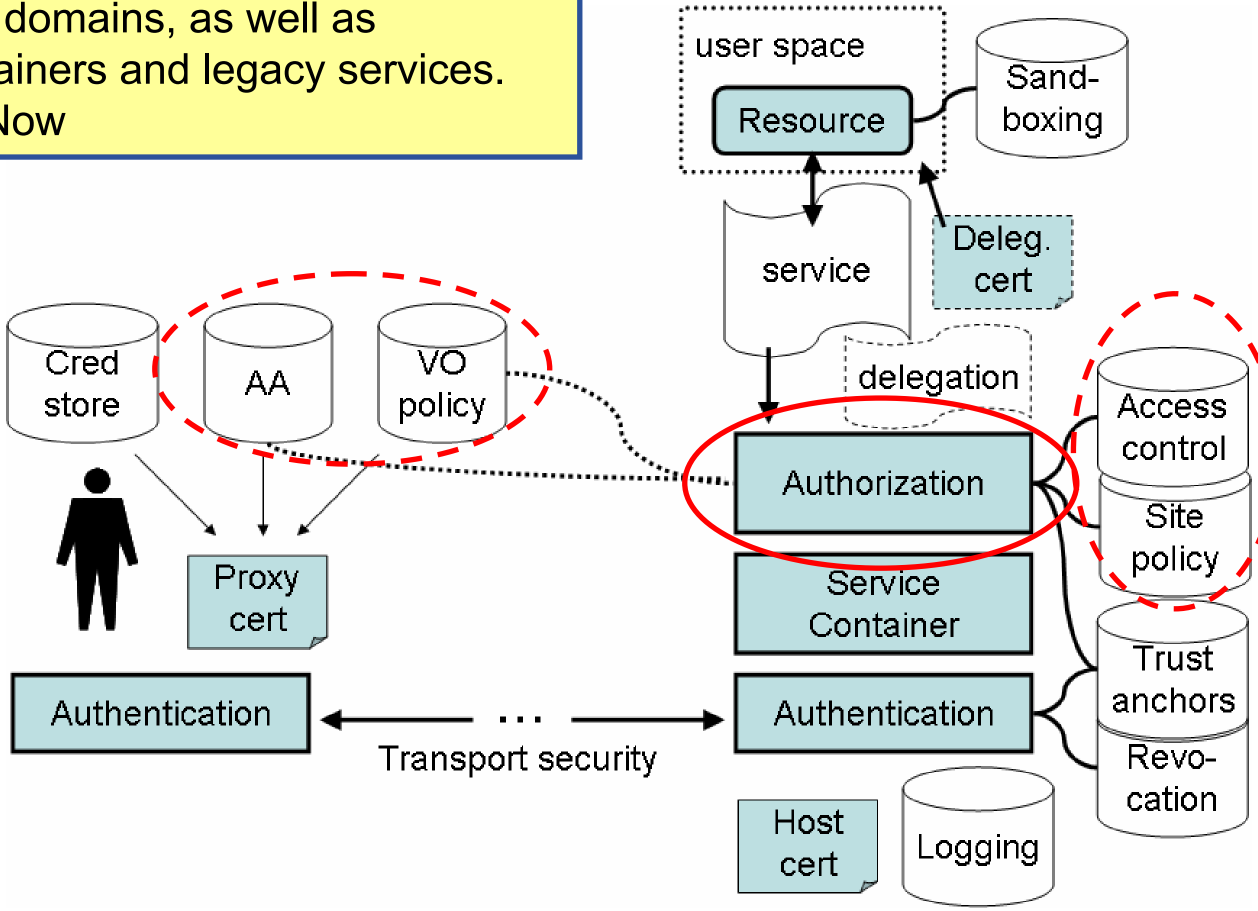
Services - Authorization

Policy assertion services enable the consolidation and central administration of common policy
Fulfilled/Time frame: Yes/Future



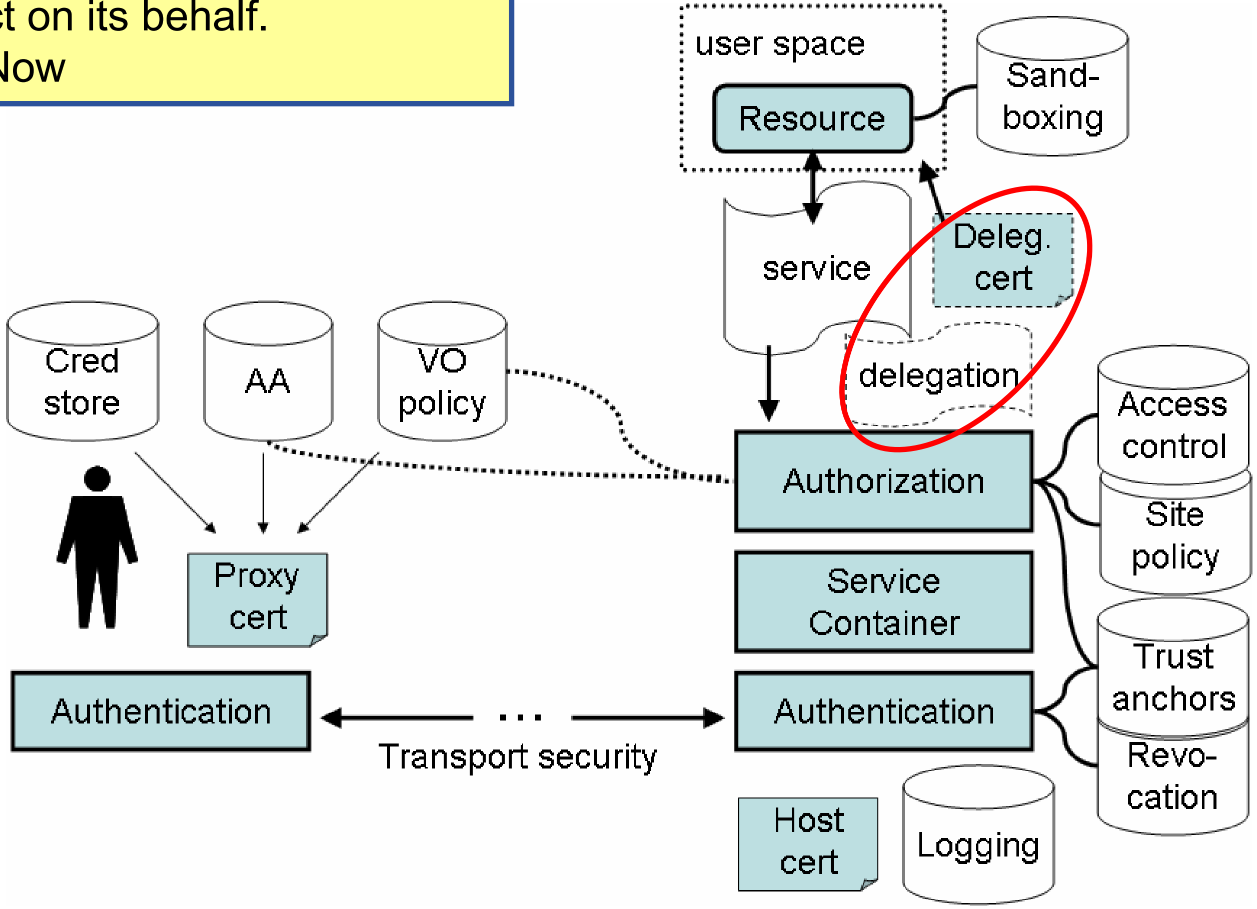
Services - Authorization

Authorization framework enables local collection, arbitration, customization and reasoning of policies from different administrative domains, as well as integration with service containers and legacy services.
Fulfilled/Time frame: Yes/Now



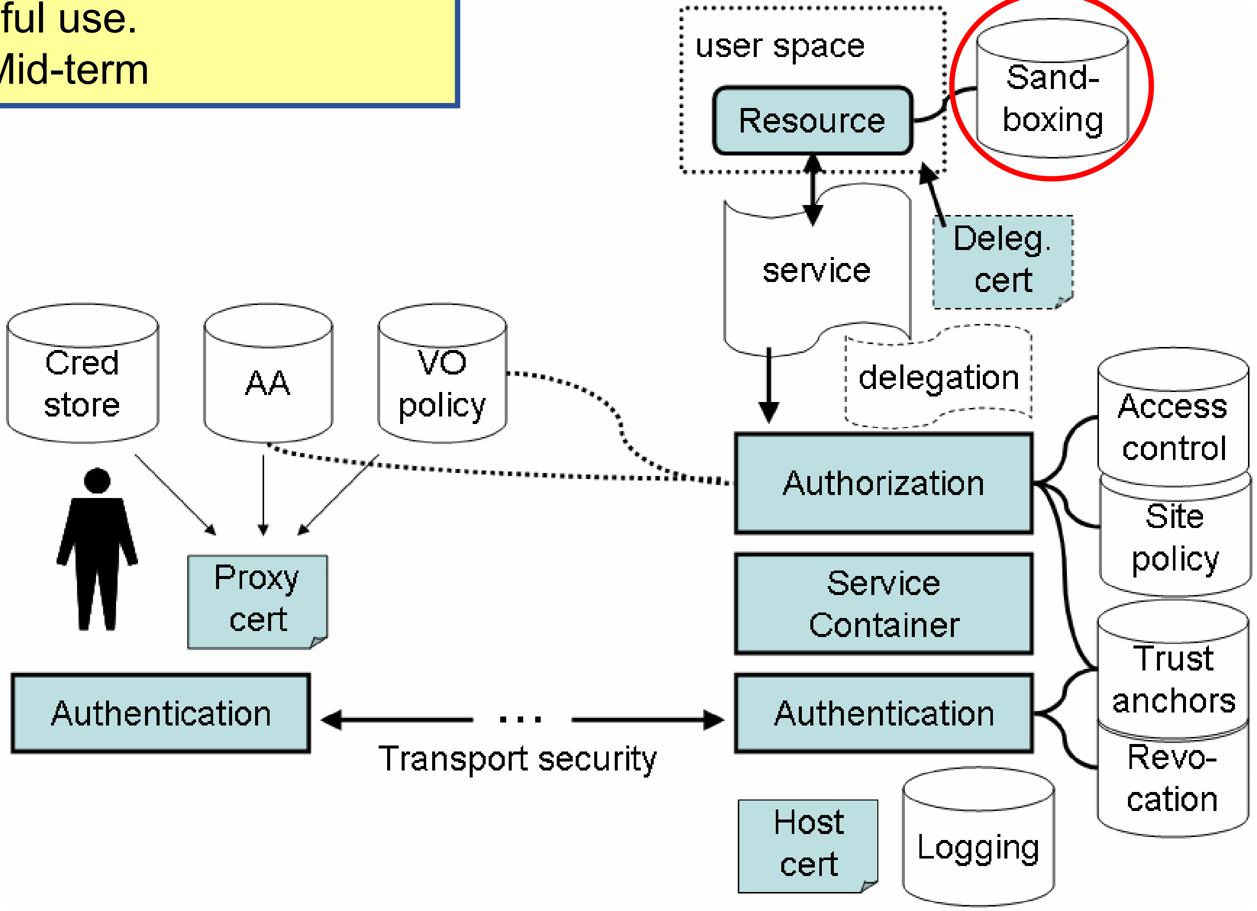
Services - Delegation

Delegation - Allows for an entity (user or resource) to empower another entity (local or remote) with the necessary permissions to act on its behalf.
Fulfilled/Time frame: Yes/Now



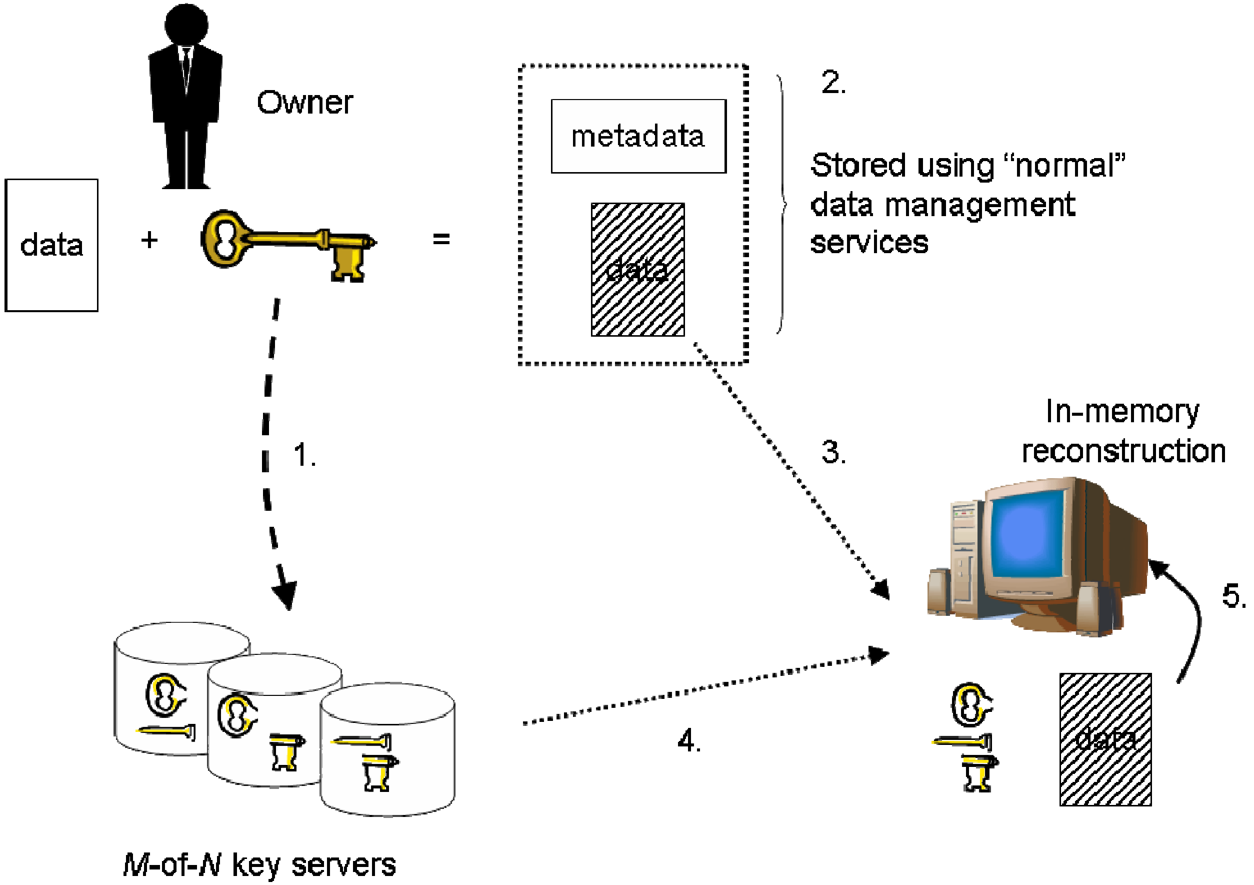
Services - Sandboxing

Sandboxing - Isolates a resource from the local site infrastructure hosting the resource, mitigating attacks and malicious/wrongful use.
Fulfilled/Time frame: Yes/Mid-term



Services - Data Key Management

Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
Fulfilled/Time frame: Partially/Mid-term



Plans and status - gLite release 1

Module candiates for gLite release 1:

- **SOAP over HTTPS**
  - Implements transport layer security for web services
- **Authorization framework**
  - A java rendering of the pluggable authorization framework
- **VOMS support for authorization**
  - The Virtual Organization Membership Service (VOMS) is used for managing the membership to VOs and as attribute authority
- **Resource Access Control (LCAS, LCMAPS, gatekeeper)**
  - Resource access control is based on Local Centre AuthZ Service (LCAS) and Local Credential MAPping Service (LCMAPS). The Globus WorkSpace Service (WSS) is used for account management