EGEE Security

2nd EU Review

CERN December 6-7, 2005

Åke Edlund

EGEE Security Head

On behalf of the members of JRA3

and the EGEE Security groups

Content

- ✓ **Overview - EGEE Security**
- ✓ **Security Coordination and Collaboration** - the EGEE security workgroups and how they are used in the security coordination work and as an active part of the global collaboration on Grid security
- ✓ **Security Guiding Documents** - status, usage
- ✓ **gLite Security Modules** - current status and future plans
- ✓ **Q&A** - open sesssion for questions and answers

Overview - JRA3 Objectives

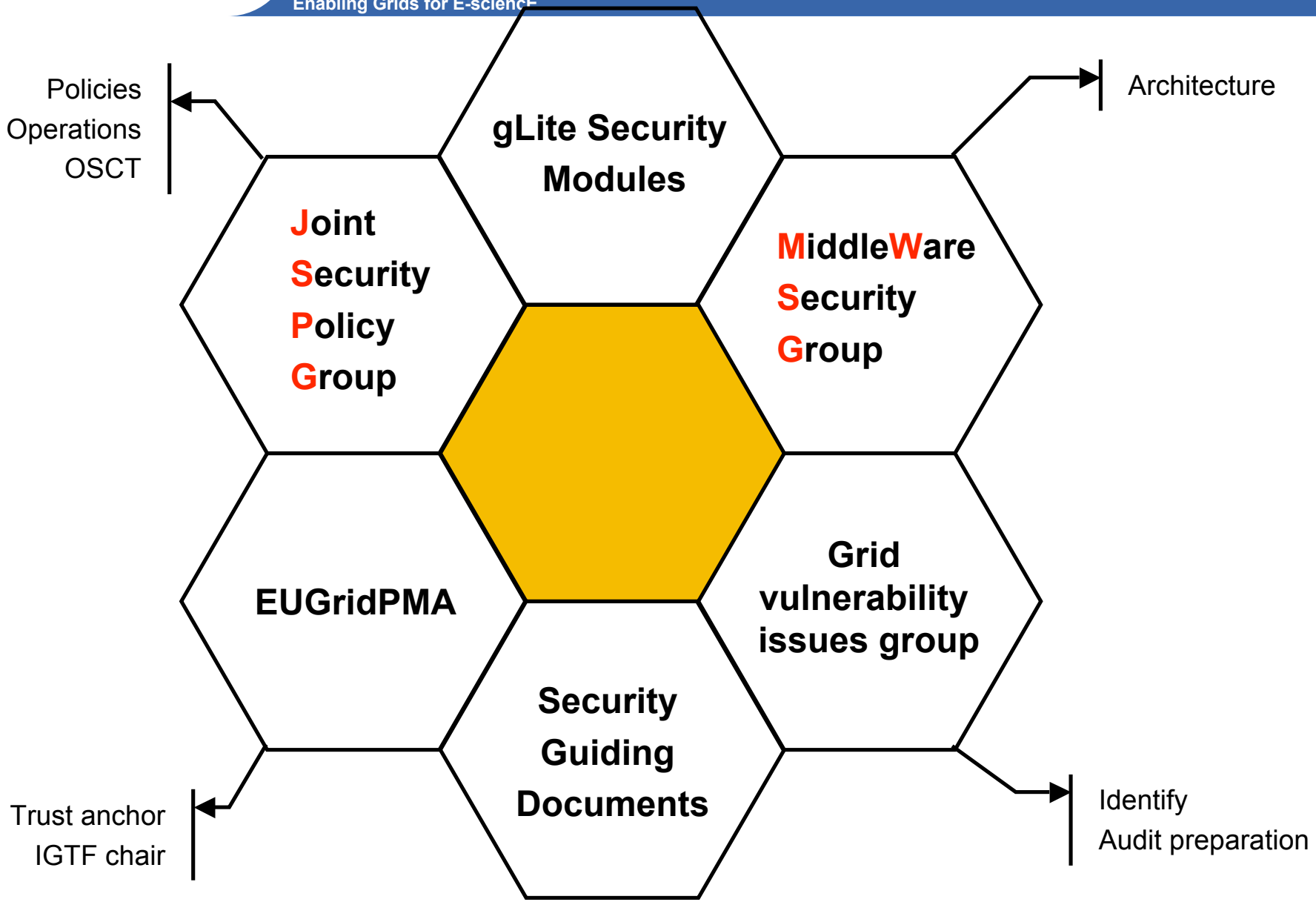
- **Enable secure operation of a European Grid infrastructure**
  - Develop security architectures, frameworks and policies
  - Definition of incident response methods and authentication policies
- **Consistent design of security mechanisms for all core Grid services**
  - Meet production needs of resource 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

Overview - JRA3 Achievements

- **Revised global security architecture. Secure credential storage procedures/recommendations document**
- **Middleware security group (MWSG) setting example for security interoperability between grid initiatives (EGEE, OSG, NAREGI)**
  - To be used for GGF work. Official MWSG meeting at GGF16
- **Actively contributing to the gLite middleware**
- **EUGridPMA continued work and was instrumental to**
- **IGTF launched,**
  - Chaired by David Groep (JRA3)
  - Coordinating European, Asian, and American GridPMAs
- **Vulnerability analysis database created**

- **For remaining 2005**
  - Reinforce middleware security component development and interoperability
  - Overview and recommendation document on accounting techniques
  - Second revision of security operational procedures document.
  - Assessment of security infrastructure – *Security Challenge*

Overview - EGEE Security



These groups are lead by the SA1 team, and are addressing all aspects of operational security.

These groups are all part of the overall EGEE security effort, and main contributors to the operational security guiding documents.

Chairs of these groups are members of the Security Coordination Group.

Extending Trust: IGTF – the International Grid Trust Federation

Enabling Grids for E-sciencE

EUGridPMA

All EU 6th framework e-Infrastructure projects

EGEE
DEISA
SEE-GRID

LHC Computing Grid Project ("LCG")
Open Science Grid (US)
National projects, like (non-exhaustive):

UK eScience programme
Virtual Lab e-Science, NL

APGridPMA

13 members from the Asia-Pacific Region

AIST (.jp)
APAC (.au)
BMG (.sg)
CMSD (.in)
HKU CS SRG (.hk)
KISTI (.kr)
NCHC (.tw)
NPACI (.us)
Osaka U. (.jp)
SDG (.cn)
USM (.my)
IHEP Beijing (.cn)
ASGCC (.tw)

Launched June 1st, 2004
4 'production-quality' CAs
Pioneered 'experimental'profile

TAGPMA

10 members to date

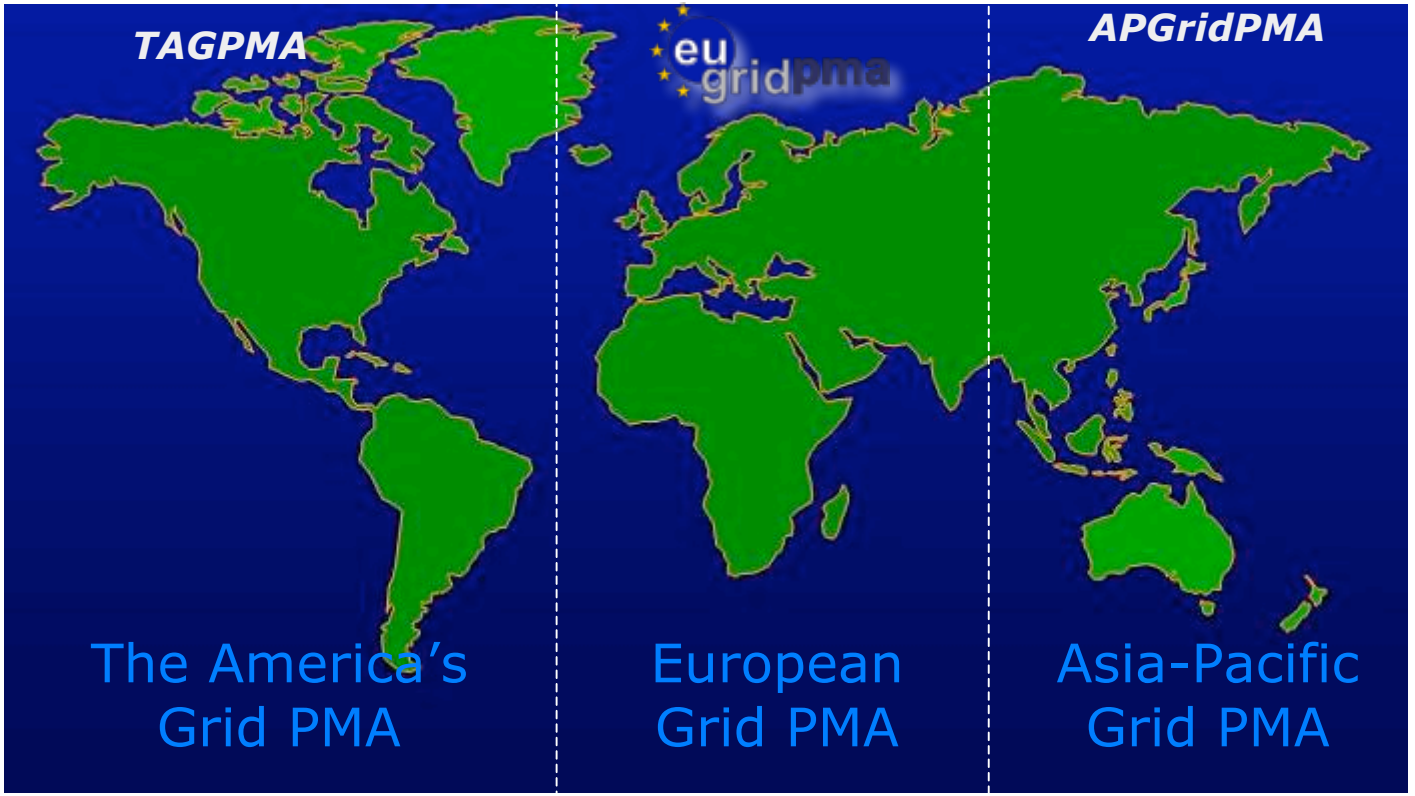
Canarie (.ca)
OSG (.us)
TERAGRID (.us)
Texas H.E. Grid (.us)
DOEGrids (.us)
SDSC (.us)
FNAL (.us)
Dartmouth (.us)
Umich (.us)
Brazil (.br)

Launched June 28th, 2005
Pioneered new "SLCGS" (Kerberos CA & al.)

TIMELINE

- **March 2005: IGTF Draft Federation Document GGF13**
- **June 28th: TAGPMA founded at GGF14**
- **July 27th : APGridPMA approved draft 0.7**
- **September: EUGridPMA meeting on approval**
- **October 3-4: formal foundation of the IGTF!**

- common, global best practices for trust establishment
- better manageability and response of the PMAs



Middleware Security Group (MWSG)

Objectives

To ensure the security architecture is updated with the user's requirements, coordinated with other grid initiatives and standardization efforts.

Members

Core security developers from EGEE
Operations representatives from EGEE
Representatives from the applications in EGEE
Core security representatives from OSG, FNAL, SLAC
(NEW) Security Architects from 5 other EU Grid initiatives
Also: NAREGI

MWSG meetings

MWSG1, May 5-6 '04, Gap Analysis - *"MWSG kick-off"*
MWSG2, June 16-17 '04, gLite Release Plan
MWSG3, Aug 25 '04, Security Architecture v1.0
MWSG4, Oct 15 '04, First release candidate planning
MWSG5, Feb 23-24 '05, Workplan update
MWSG at 3rd EGEE, EGEE/OSG/Naregi meeting
MWSG6, Sept 14-15 '05, OSG and EGEE interoperability
MWSG BOF at GGF15, Oct '05 'Good interop. example'
MWSG at 4th EGEE, Oct '05 GGF in Athens, Feb '06, New EU members

Next meeting: MWSG7, Dec 14-15 '05

Proposal on Interworking (OSG, EGEE)

Interop agreements list:

GSI/SSL Authentication
Authorization Attributes
Delegation
Proxy Renewal ?
Authorization Policy statements ?
What needed for auditing/accounting ?
- Request identifiers ?

Service Specifications

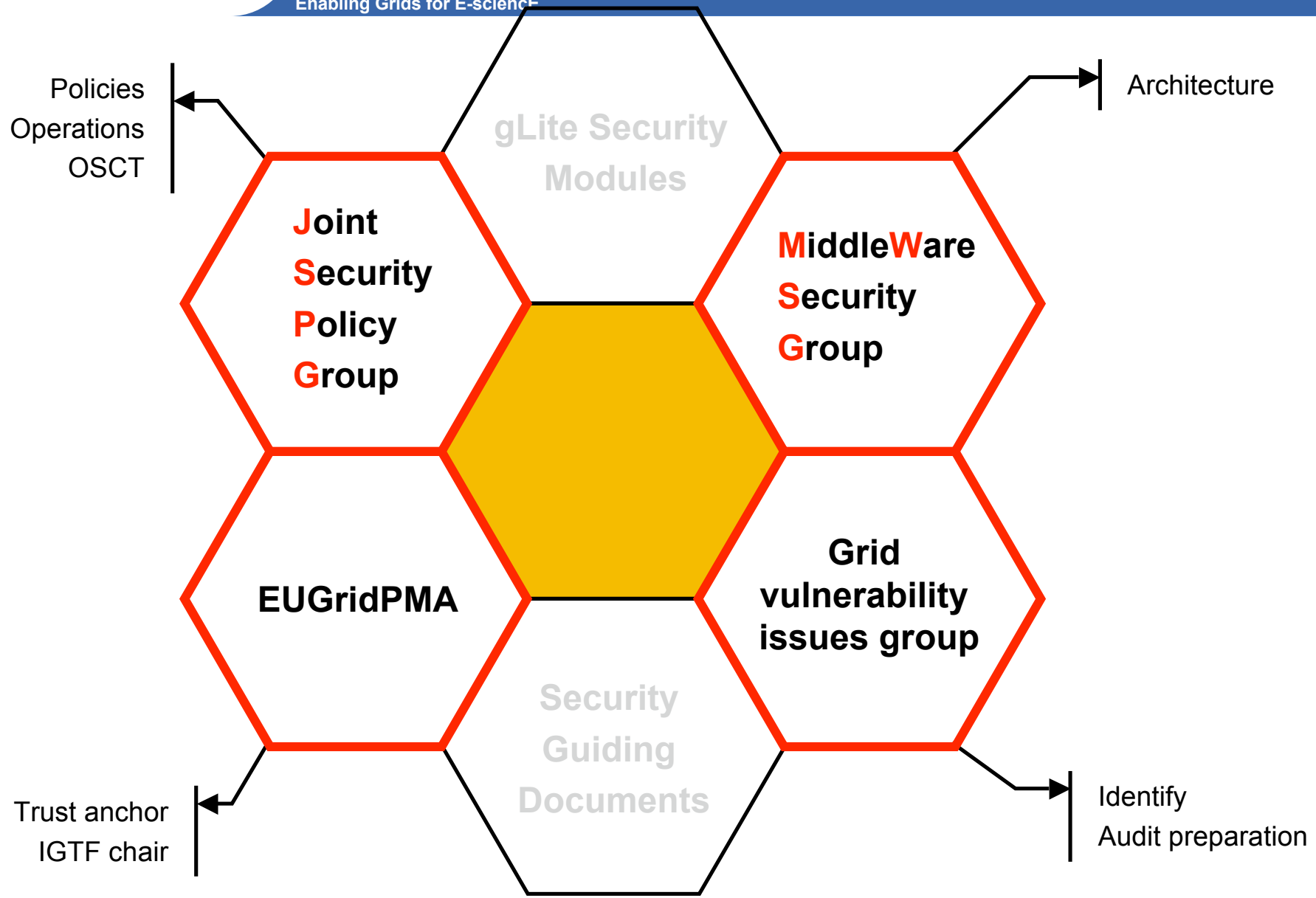
All service interface specifications have written specifications
- Pointer to authoritative document with product

Those internal to service documented with service
Those internal to project documented with project
Those exposed for grid interop documented in GGF

Make these lists public

We use GGF as intergrid info exchange
We work partnerships in pairwise meetings like MWSG

Security Coordination and Collaboration



Security Coordination

The Security Coordination Group (SCG)

is responsible for ensuring overall EGEE-II security coordination, includes architecture, deployment, standardisation and cross-project concertation.

The goal is to **ensure the relationship between the various security-related work** items inside the project do not:
- adversely overlap (leading to duplication of effort) or
- leave gaps that could be exploited.

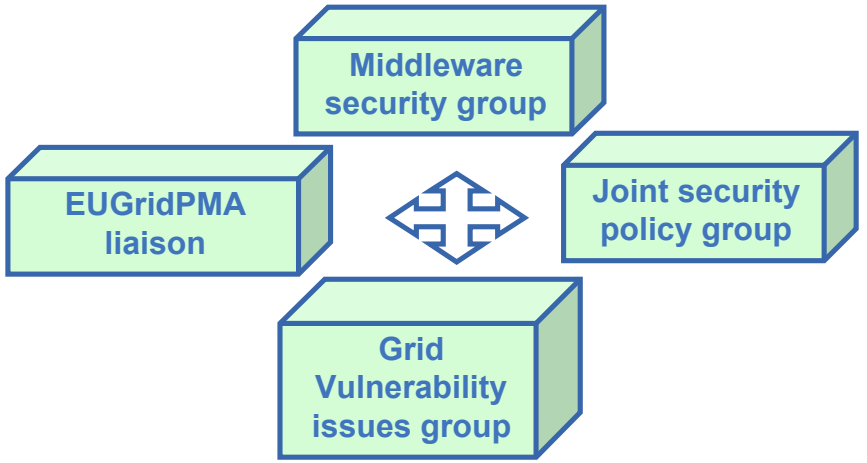
In addition, the SCG is to **coordinate a new security auditing activity**. This activity will monitor both operations and middleware for security issues and report periodically on status and progress of the issues identified.

The security audit will leverage the work of the Grid vulnerability issues group.

Security Coordination Group (SCG) members:

The Security Head, chair of the SCG (JRA2)

The chair of the Middleware Security Group (JRA1)
The chair of the Joint Security Policy Group (SA1)
The EUGridPMA liaison (SA1)
The chair of the Grid vulnerability issues group (SA1)

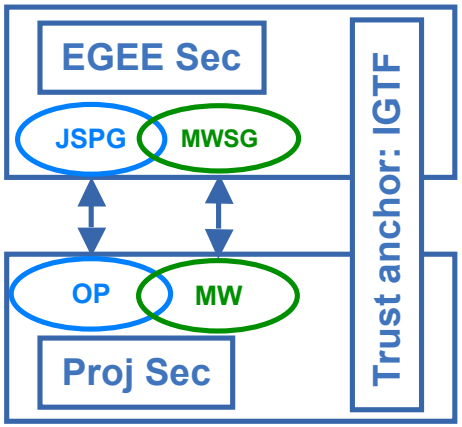


Security Collaboration

The security workgroups, MWSG and JSPG, are not only for internal EGEE security coordination, but also for collaboration with other grid initiatives, world-wide.

"Collaboration cook book"

New collaborations start off with identifying common interests, divided on security operations (JSPG handles these) and middleware (MWSG).



Grid projects not involved in inhouse reenginering, send their security representatives to JSPG to discuss common strategies, and reusage of requirements and policy documents.

At the same time, MWSG covers the various middleware interests, such as gLite, GLOBUS, UNICORE, by inviting representatives from these groups.

EGEE Security is not leading the standardization effort, but is closely following this, giving feedback and ideas.

EGEE is represented in a number of areas in GGF, leading the security area together with OSG.

The collaboration with OSG is close, from start. Together we have worked out a first suggestion on interoperability plans, something regarded by GGF as a "school book example" of interoperating grids, and something that will be further presented in GGF.

New collaborations have been established with 4 EU projects:

- DEISA
- SEEGRID
- DILIGENT
- GRIDCC

In Asia, we have met with NAREGI on a number of occasions, exchanging ideas and looking at future collaborations.

Security Guiding Documents

Deliverables

Security Architecture
Revised mid-term
MW OP

Site access control architecture
OP

Assessment of security infrastructure
Final report (ongoing)
MW OP

All these have been used in the ongoing security work, both on operational and reengineering level.
OP MW

Milestones

Completed user requirements survey defines effort redistribution over action lines.
MW OP

Set-up of the PMA for European CAs and liaison with the corresponding extra European ones (document + standing committee)
OP

Framework for policy evaluation accepted in GridPMA policies and determination of the CA service authorities for EGEE
OP

OGSA SEC service initial recommendations for reengineering
MW

Secure Credential Storage procedures (recommendations document)
MW OP

Security operational procedures
Two revisions
OP

Review and future recommendations on accounting techniques and distributed budgets
MW OP

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

Security Requirements - a horizontal activity, managed through central groups

- Lesson learned: reused and updated requirements from earlier projects
- Collecting (continuous process) the requirements from the activities - Middleware, Sites, Applications
- Share the requirements with other grid activities and get feedback, e.g. OSG
- Prioritization set in the security groups, with representatives from all involved activities
- Defining what security modules to deliver when

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

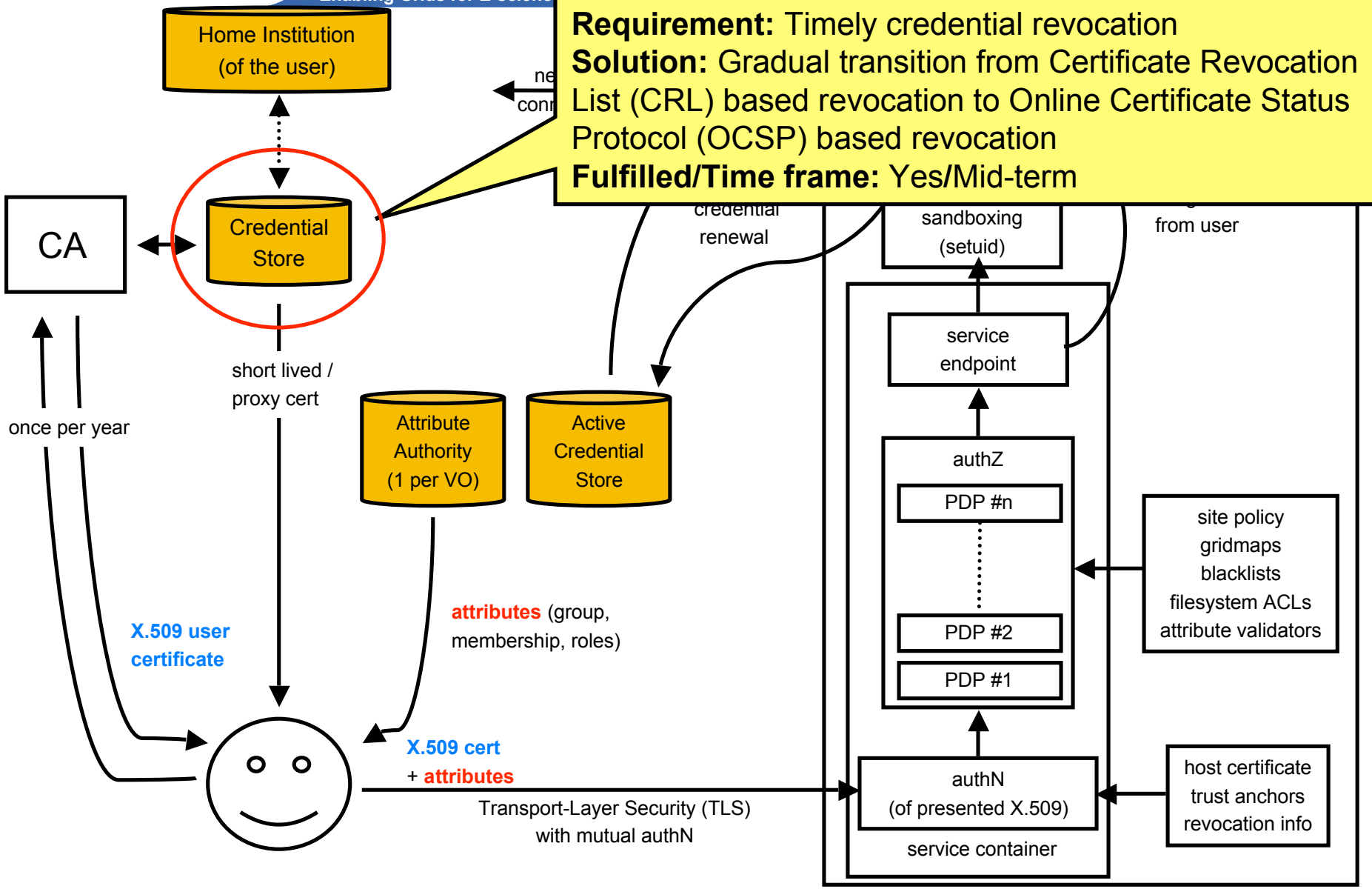
Will gLite be any better?

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

gLite Security Modules
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



gLite Security Modules Services - TLS vs MLS

Transport Level Security

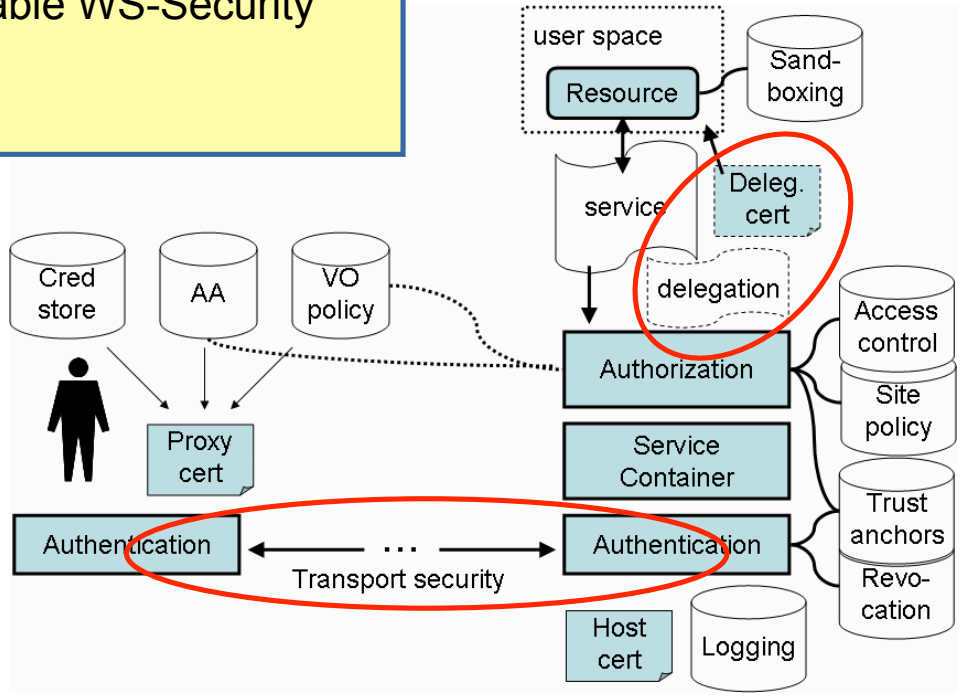
- Uses widely deployed TLS/SSL protocol
- Does not provides security through intermediate hosts (can be done using delegation, not yet delivered).

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

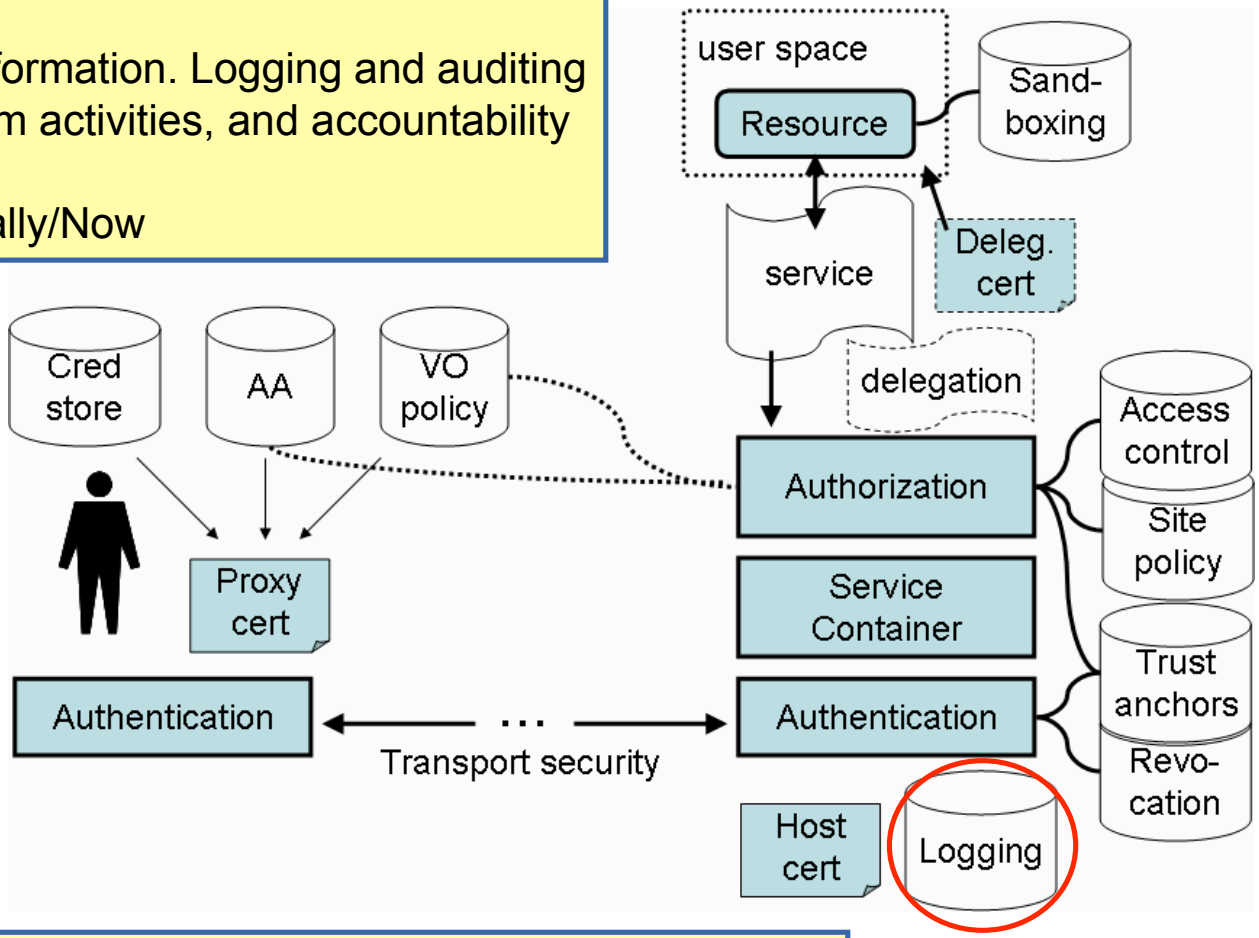
So, TLS for now

- 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)



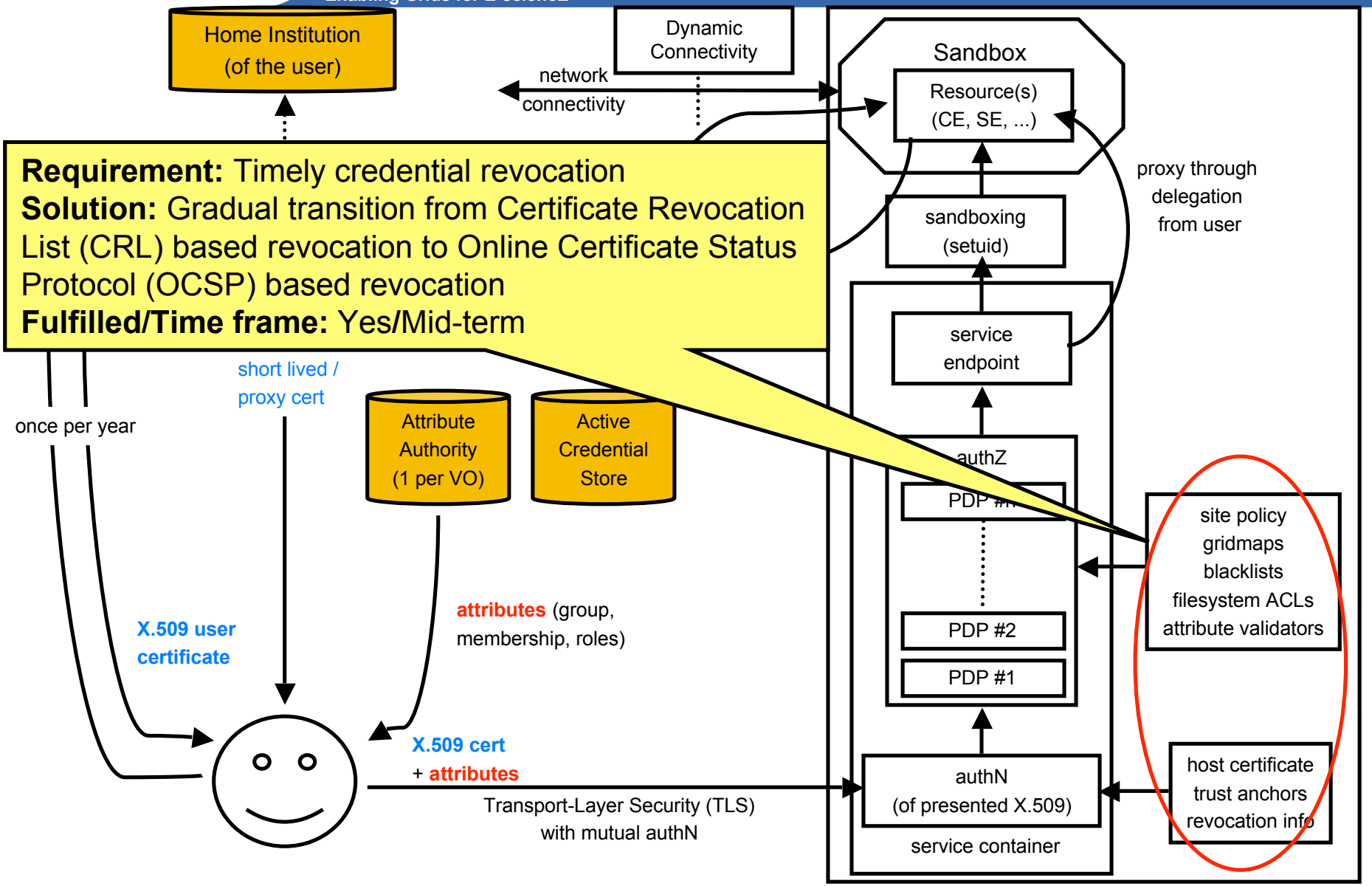
gLite Security Modules
Services - Logging and Auditing

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



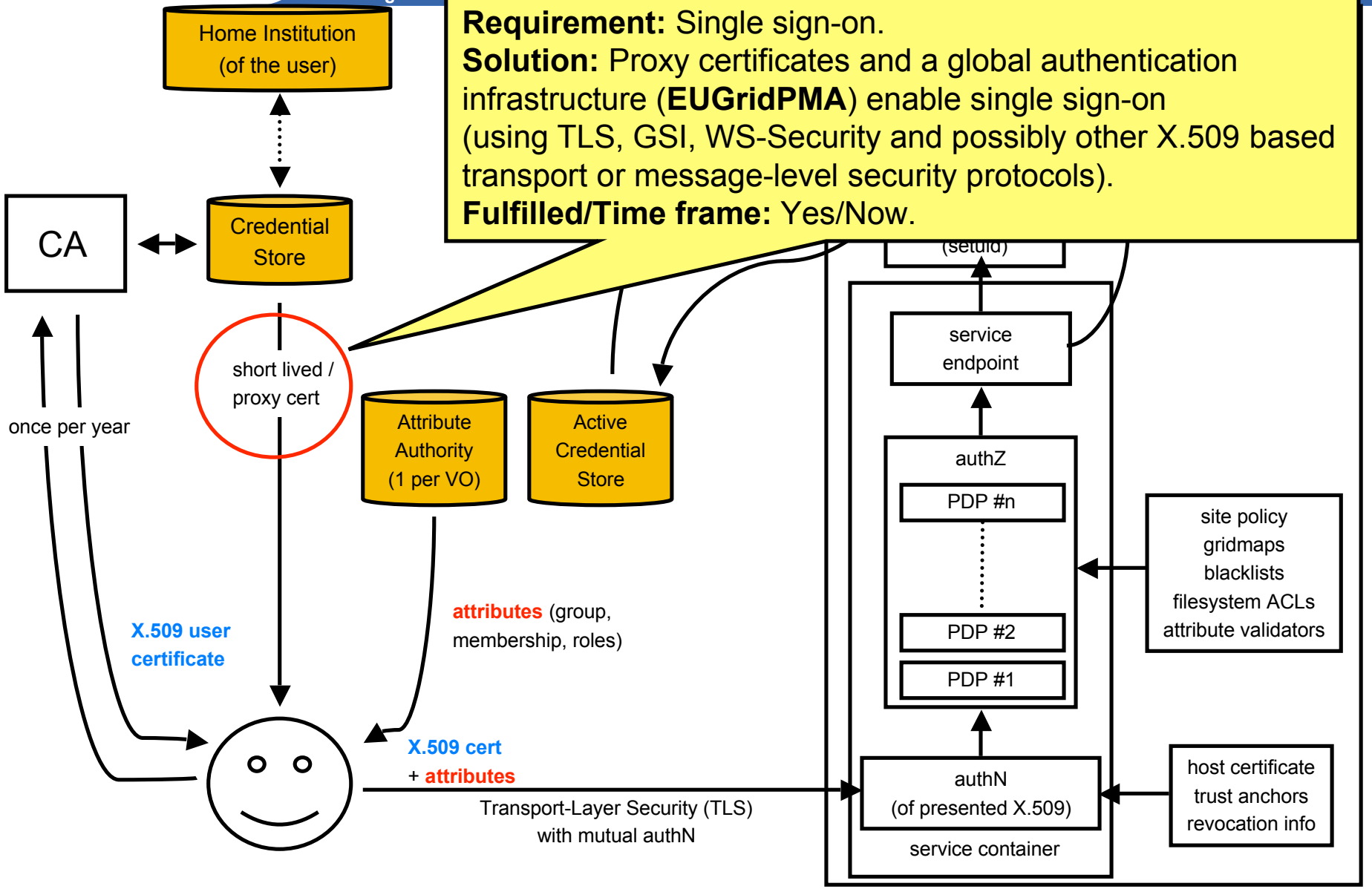
Requirement:. Accountability
Solution: All relevant system interactions can be traced back to a user
Fulfilled/Time frame: Yes/Now

gLite Security Modules Services - Authentication



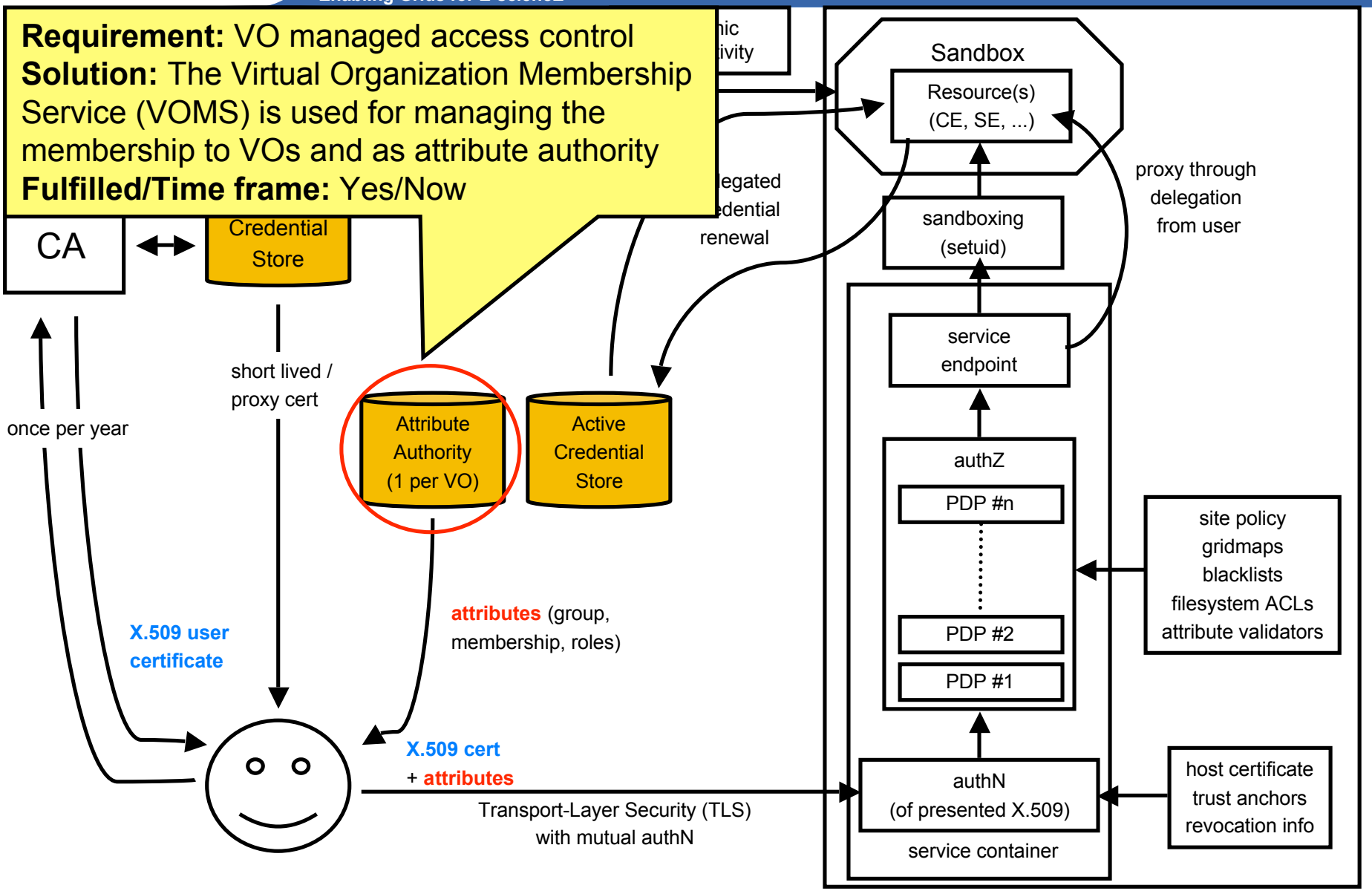
gLite Security Modules Services - Authentication

Requirement: Single sign-on.
Solution: Proxy certificates and a global authentication infrastructure (**EUGridPMA**) 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.



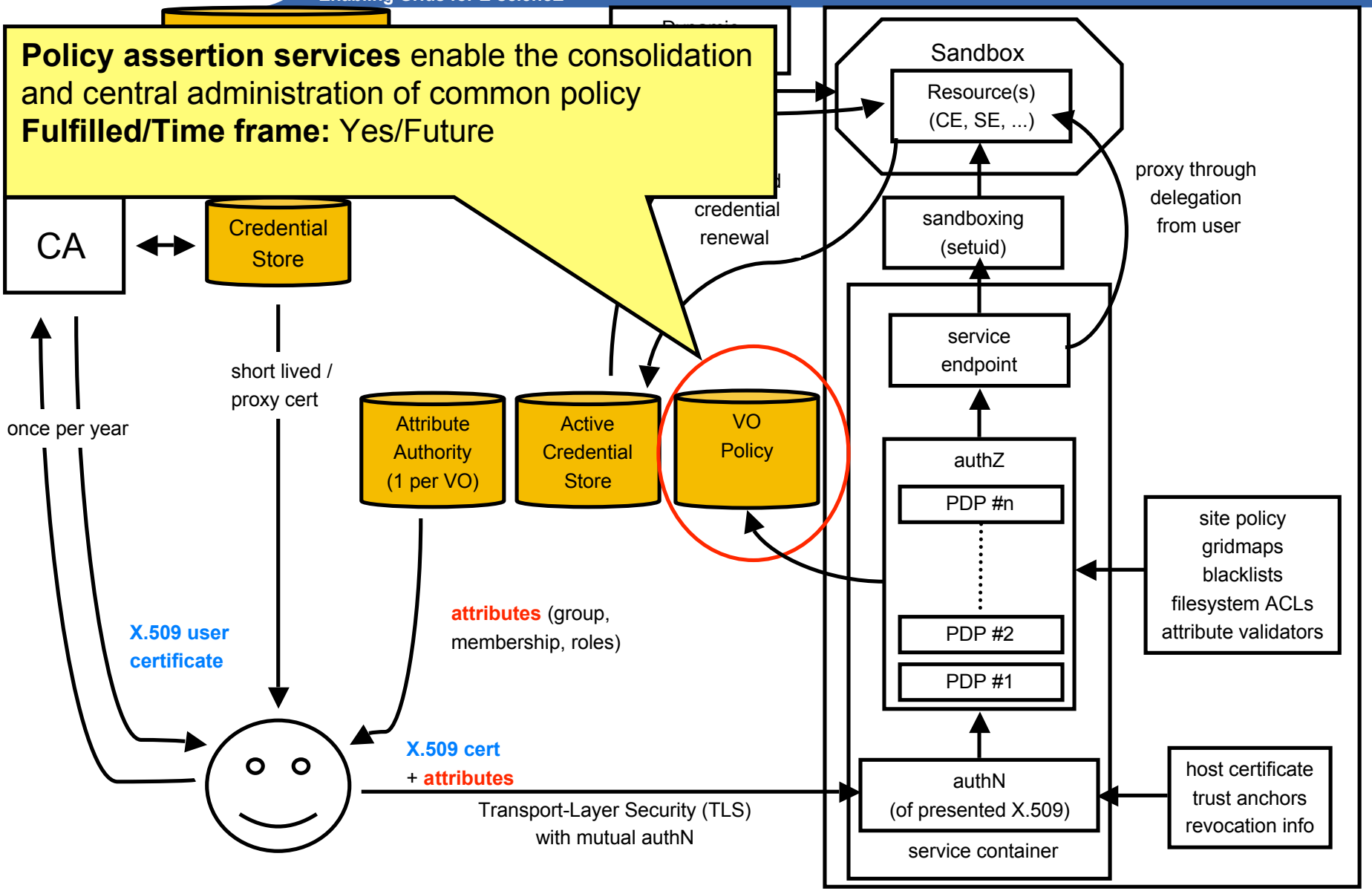
gLite Security Modules Services - Authorization

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



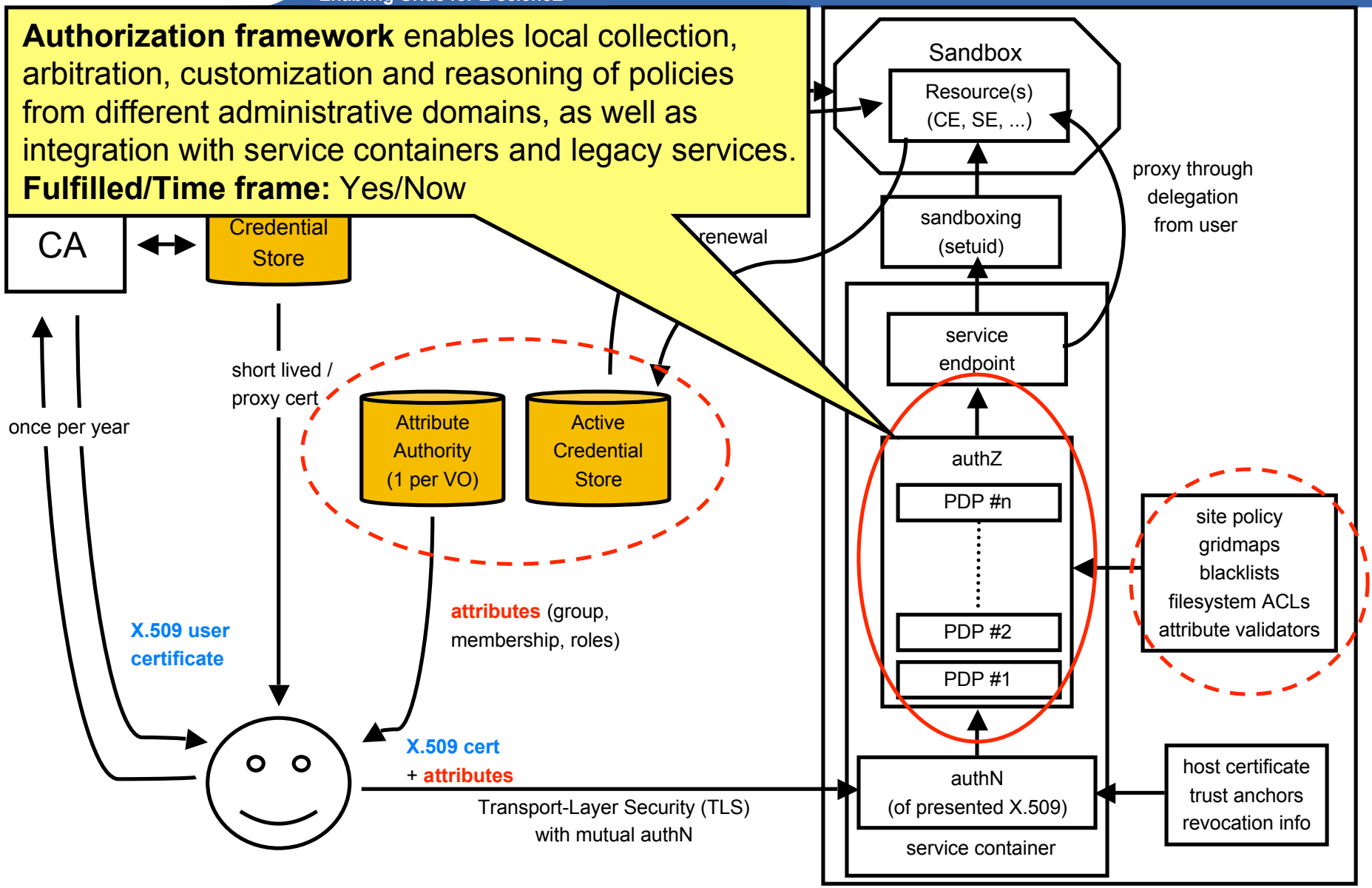
gLite Security Modules Services - Authorization

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

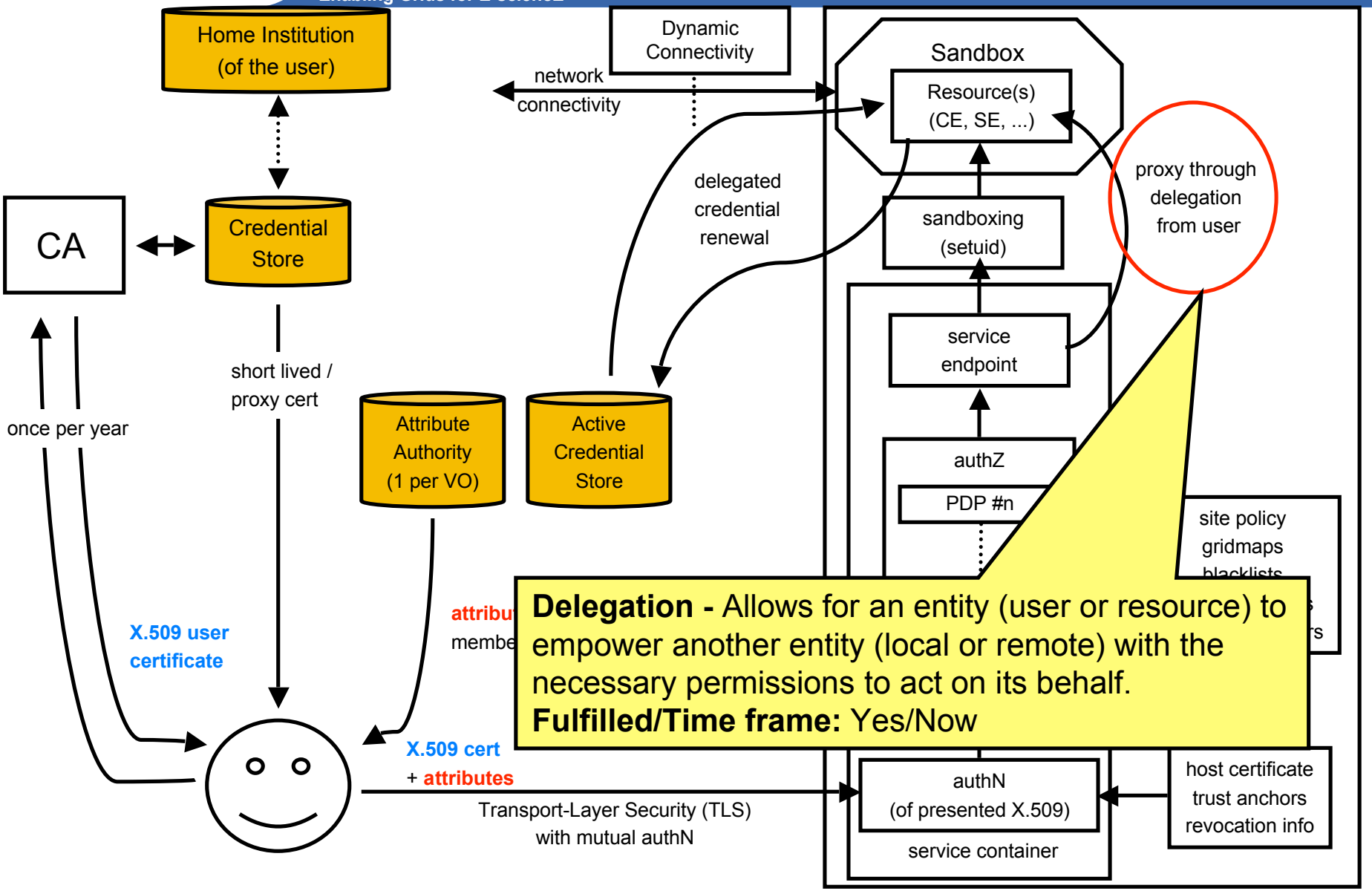


gLite Security Modules Services - Authorization

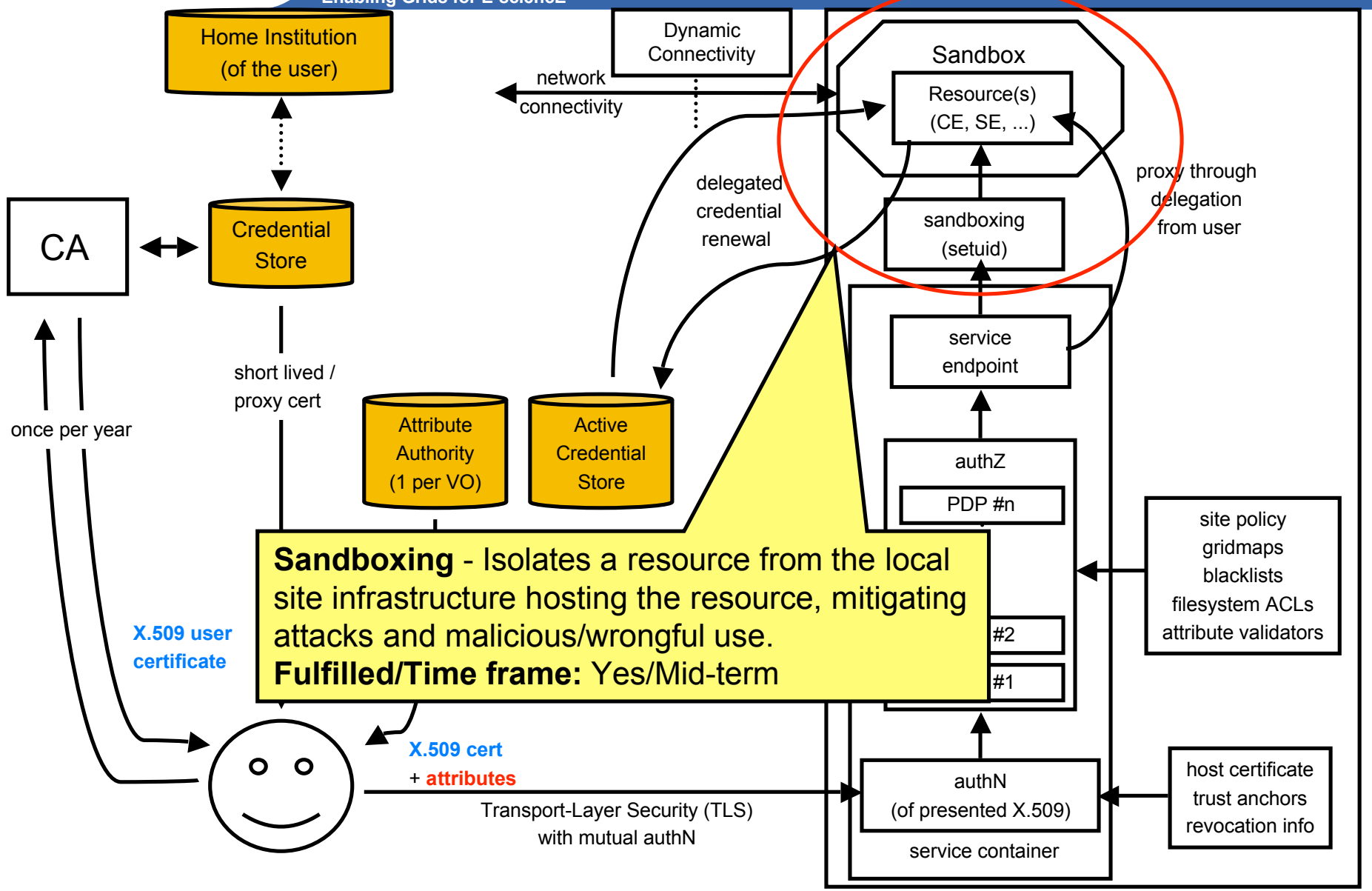
Authorization framework enables local collection, arbitration, customization and reasoning of policies from different administrative domains, as well as integration with service containers and legacy services.
Fulfilled/Time frame: Yes/Now



gLite Security Modules Services - Delegation

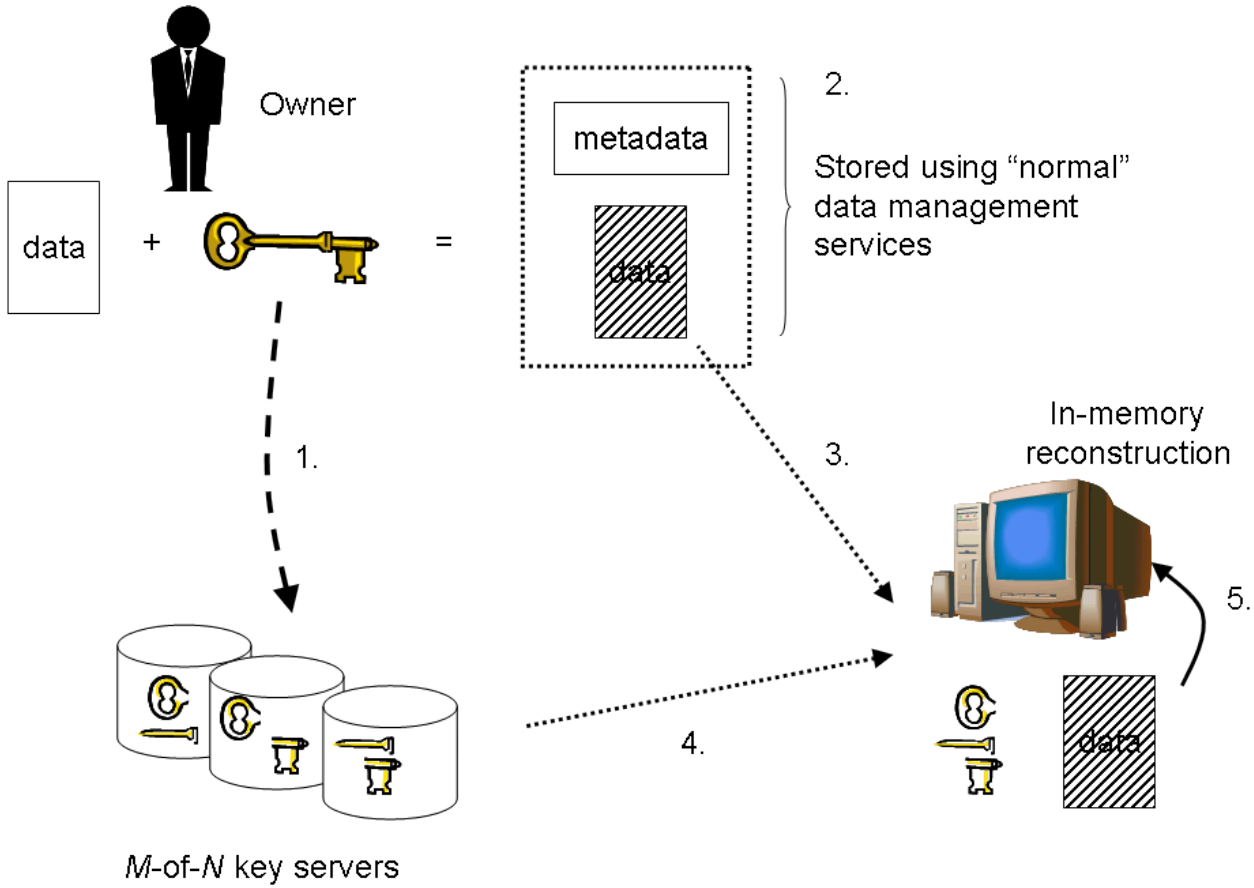


gLite Security Modules Services - Sandboxing



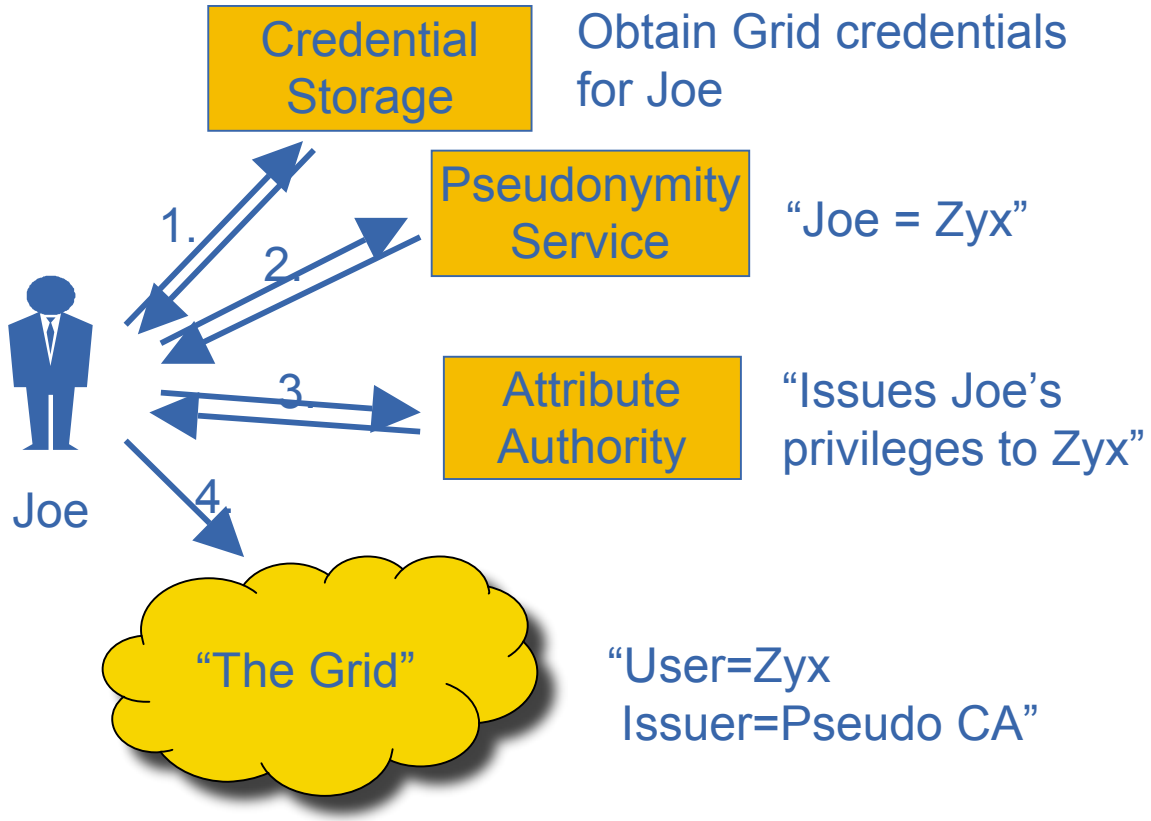
gLite Security Modules
Services - Encrypted Storage

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



gLite Security Modules Services - Pseudonymity

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



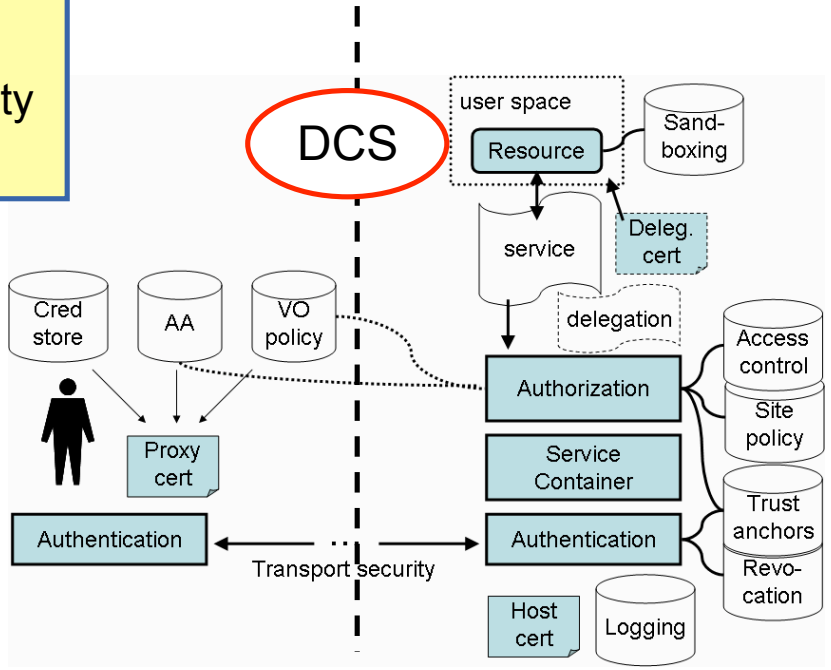
gLite Security Modules
Dynamic Connectivity Service

Requirement: Non-homogenous network access

Issue: Conflicting requirements:

Sites: ‘worker nodes’ shall have no global connectivity

Apps: ‘worker nodes’ must have global connectivity



One proposed solution, security-wise: Dynamic Connectivity Service

Enables applications to communicate despite heterogeneous and non-transparent network access:

- Policy-controlled connections to the outside world
- Compliant to work in JRA4

Fulfilled/Time frame: Yes/Future

Integration and development

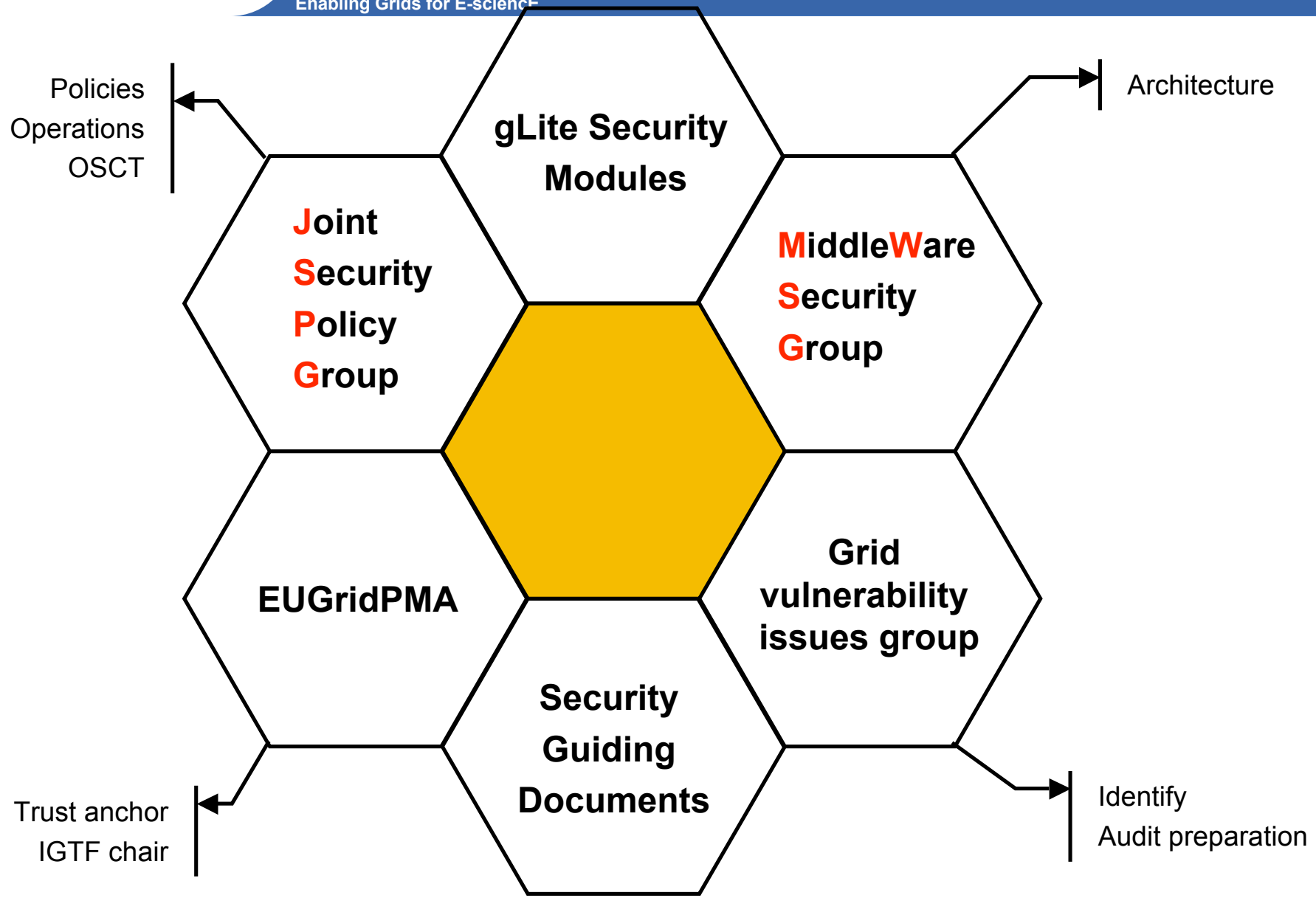
- **JRA3 is, from the start of the project, part of the JRA1 development - as the Northern Cluster**

- **All software re-engineering in JRA3 follows the processes of JRA1**
  - See previous presentation from JRA1

Plans and status – Next 4 months

- Continued gLite work (as part of JRA1)
- PM18 Second revision of the Security operational procedures document
- PM18 A documented assessment of the work and experience gathered with the basic accounting infrastructure already deployed. To highlight what remains to be done to provide a secure, deployable quota allocations and enforcement mechanism
- EGEE-II preparations

Summary

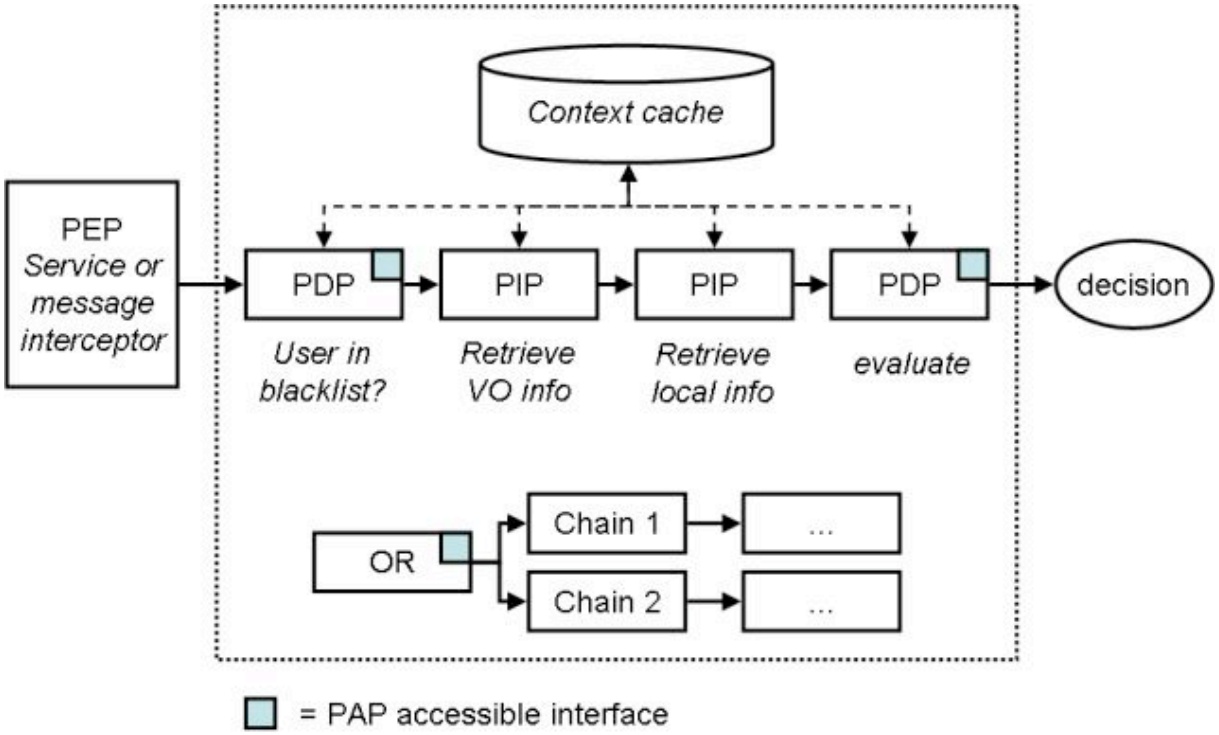

Policies
Operations
OSCT
gLite Security Modules
Architecture
Joint Security Policy Group
MiddleWare Security Group
EUGridPMA
Grid vulnerability issues group
Security Guiding Documents
Trust anchor
IGTF chair
Identify
Audit preparation

Questions and Answers

List of security modules, extra slides

org.glite.security.authz-framework-java

- Light-weight policy-engine chaining infrastructure, agnostic to back-end enforcers and evaluators.
- Avoids translating all policy services into XACML.
- The framework comprises:
  - chains, Policy Decision Points (PDPs), Policy Information Points (PIPs), Policy Administration Points (PAPs) and configuration back-ends.
- Reuses as much as possible in terms of standard Java XML and Security interfaces.
- Provides simple implementations of all components and algorithm implementations.



gLite Security Modules

org.glite.security.encrypted-storage-cpp

- This module contains the C++ code to perform the encrypt/decrypt of files.
- Contains the command line version
- Library provided
- Does simple key splitting along with Shamir splitting.

Has been used in the JRA1 Hydra and BioMed demonstrations.

org.glite.security.encrypted-storage-script

- Provides a set of scripts to perform the encrypt/decrypt of files.
- Useful for user-development purposes.

org.glite.security.gatekeeper

- Normal Globus gatekeeper with a a hook to include the LCAS in the authorization process.
- Provides in addition to the normal globus-gatekeeper, a hook to include the LCAS
- In addition it includes a callout to LCMAPS.

gLite Security Modules

org.glite.security.glexec

- Site-controlled component trusted by the site administration (can be run non-root).
- Grid ID has a meaning within their VO but not on a local site.
-Glexec switches a user's Grid ID to a local ID.is a site controlled component, i.e. it is trusted by the site-admin.
- Authorization and mapping are based on the user credential (proxy).

glexec is a fork of gsexec, which is a fork of suexec;
CREAM will be the first service to make use of glexec;
CondorC is to follow later, i.e. when WSS is supported (a.k.a. full mode vs. hybrid mode)

org.glite.security.jobrepository

- Job Repository is an optional plug-in to the LCMAPS framework.
- Stores all known information about the user-mapping in a relational database next to plain-text logs.
- store job information, detailed user information and detailed unix system mapping information.
  - Certificate chain (per certificate and no double entries).
  - VO Attributes used to launch a job.
  - Link the Grid ID to the Unix credentials (UID and GID).
- The database schema is open to include new service specific information.
- Can be used to extend an audit trail relationally across multiple services.

gLite Security Modules

org.glite.security.lcas
org.glite.security.lcas-interface
org.glite.security.lcas-plugins-basic
org.glite.security.lcas-plugins-voms
- Local Centre Authorization Service (LCAS).
- Handles the authorization to the local fabric using the users's certificate and the job RSL
- Certificate and RSL are passed to (plugin) authorization modules.
- Standard and VOMS plugins available.

org.glite.security.lcmaps
org.glite.security.lcmaps-interface
org.glite.security.lcmaps-plugins-afs
org.glite.security.lcmaps-plugins-basic
org.glite.security.lcmaps-plugins-jobrep
org.glite.security.lcmaps-plugins-voms
-Local Credential Mapping Service (LCMAPS) provides all local credentials needed for jobs allowed into the fabric.
- Can be accessed by the gatekeeper or other services as a shared library.
- Runs one or more 'credential mapping' plugins.
  - Plugin Manager loads and runs the plugins.
  - Evaluation Manager schedules the order of the plugins. Driven by policy engine.
- Based on the user credential and job JDL, either

gLite Security Modules

org.glite.security.test-utils

- Module provides:
  - Standard set of CA certificates.
  - A standard method to generate test certificates.
  - Method to re-generate all CAs.
- Generates many types of certificates (valid,expired,invalid etc).

Used widely in gLite standard testing procedures.

org.glite.security.trustmanager

-A replacement for the Java SSL implementations supplied with web containers and application servers.
- Allows the correct handling and authentication of Grid client proxy certificates.

Widely used in many Grid projects.

org.glite.security.util-java

- Provides the EGEE SSL socket factory and dependency.

Widely used in many Grid projects.

gLite Security Modules

org.glite.security.gsoap-plugin

org.glite.security.proxyrenewal

org.glite.security.voms
org.glite.security.voms-admin-client
org.glite.security.voms-admin-interface
org.glite.security.voms-admin-server
org.glite.security.voms-api
org.glite.security.voms-api-c
org.glite.security.voms-api-cpp
org.glite.security.voms-clients
org.glite.security.voms-config
org.glite.security.voms-mysql
org.glite.security.voms-oracle
org.glite.security.voms-server