JRA3 Security

Åke Edlund, JRA3 Manager, KTH
On behalf of JRA3

EGEE 2nd EU Review
December 6-7, 2007
CERN, Switzerland

www.eu-egee.org
www.glite.org

Information Society and Media

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

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 since the 1st EU review

- **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**

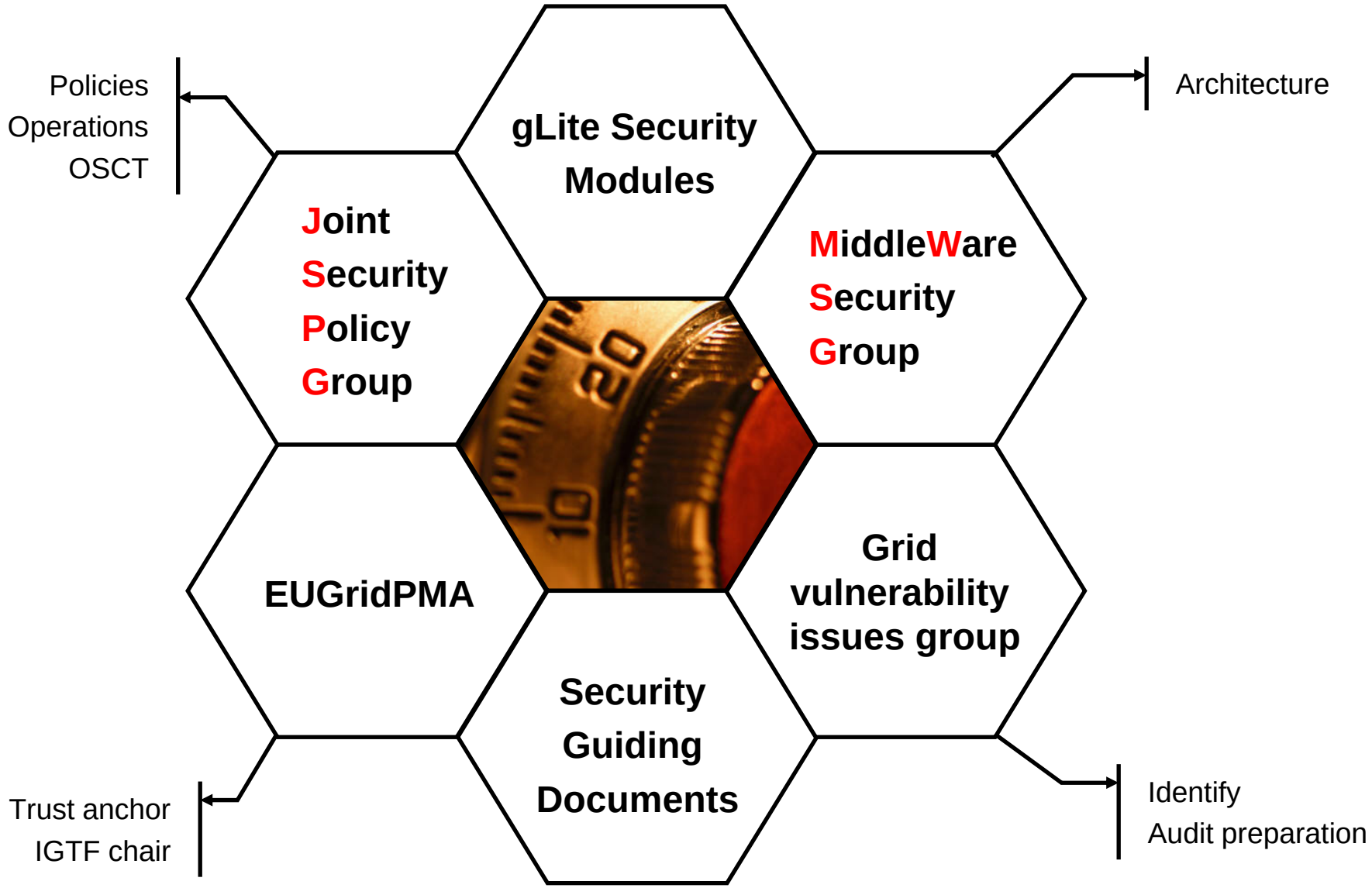
- **For remaining 2005**
  - Reinforce middleware security component development and interoperability
  - Overview and recommendation document on accounting techniques
  - Second revision of security operational procedures document.
  - Assessment of security infrastructure – *Security Challenge*

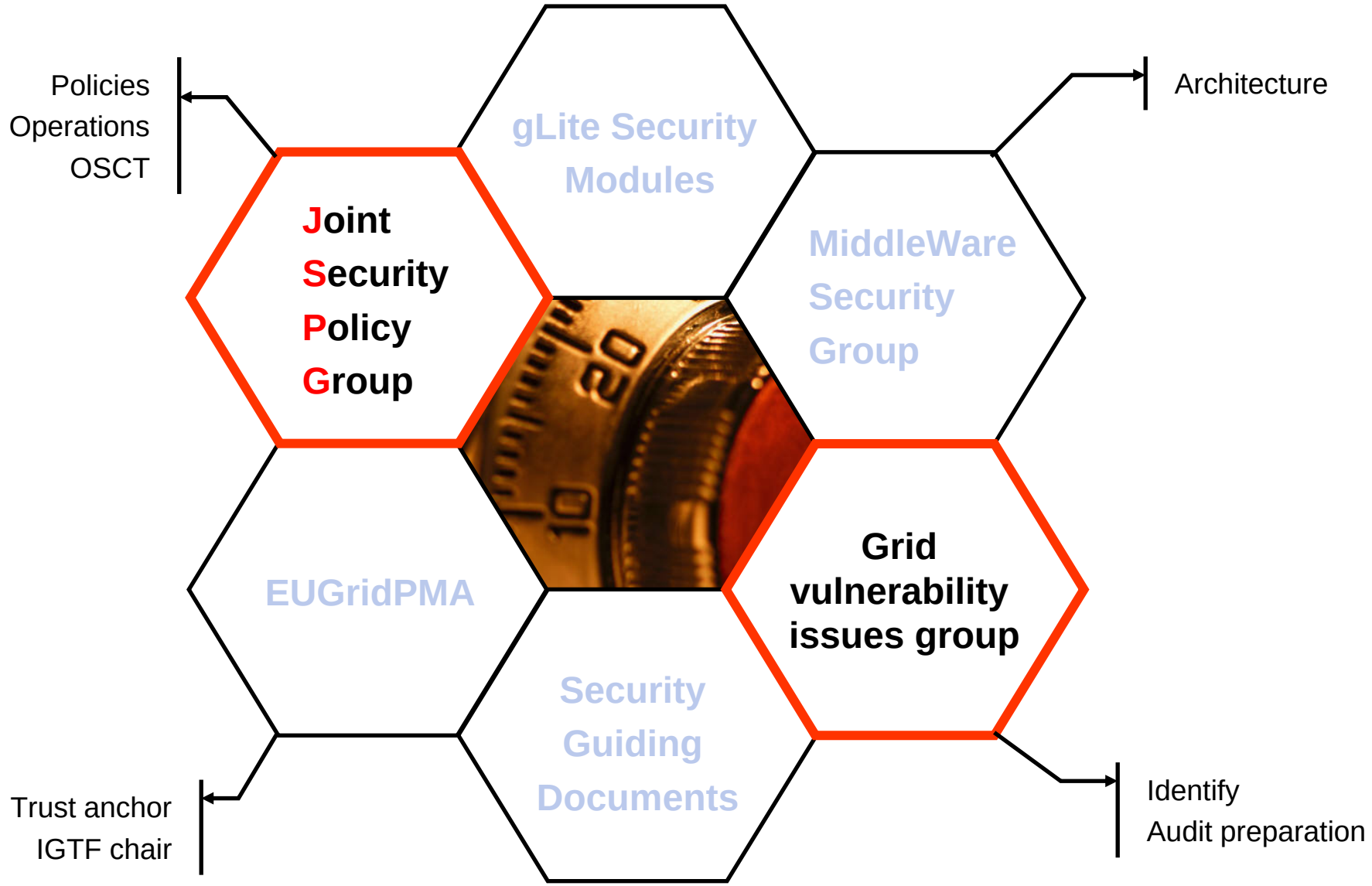
Overview - JRA3 issues and their mitigation

- **Geographically distributed teams**
  - Teams: Organized the team into two teams instead of four.
  - Cluster manager: For a development-intense period: two alternates for the JRA3 representation in the JRA1. Now: one point of contact in the TCG and EMT.
  - F2F meetings: Mainly MWSG and conferences.

- **Conflicting/challenging security requirements from applications and operations**
  - Proposed solutions meeting the sets of requirements as much as possible. Best example: Encrypted storage.

Overview - EGEE Security




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

Already covered by SA1 presentation on Day 1:

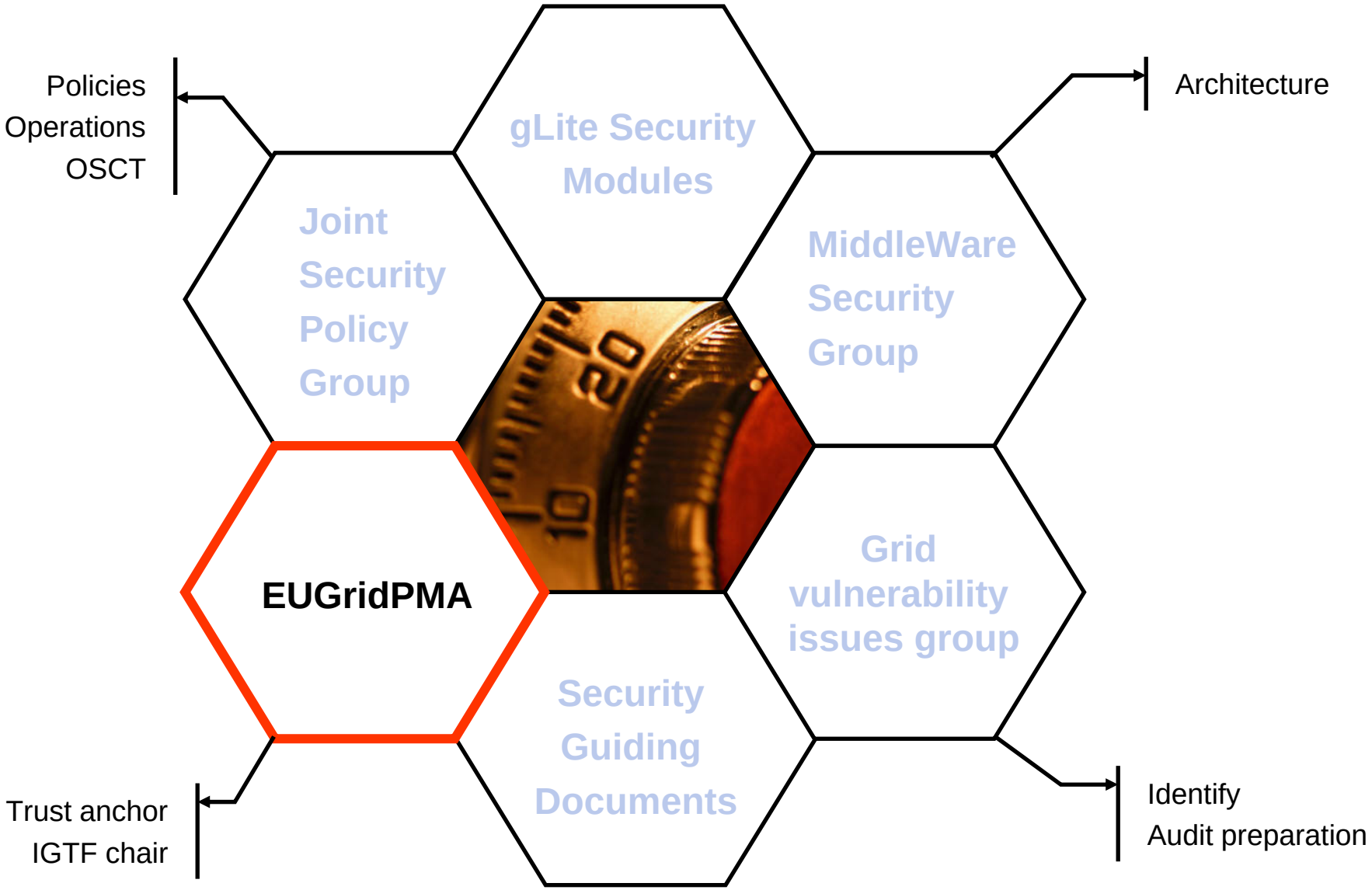
- Security Challenges
- Joint Security Policy Grop
- Operational Security Coordination Team
- Grid Vulnerability Issues Group

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



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)

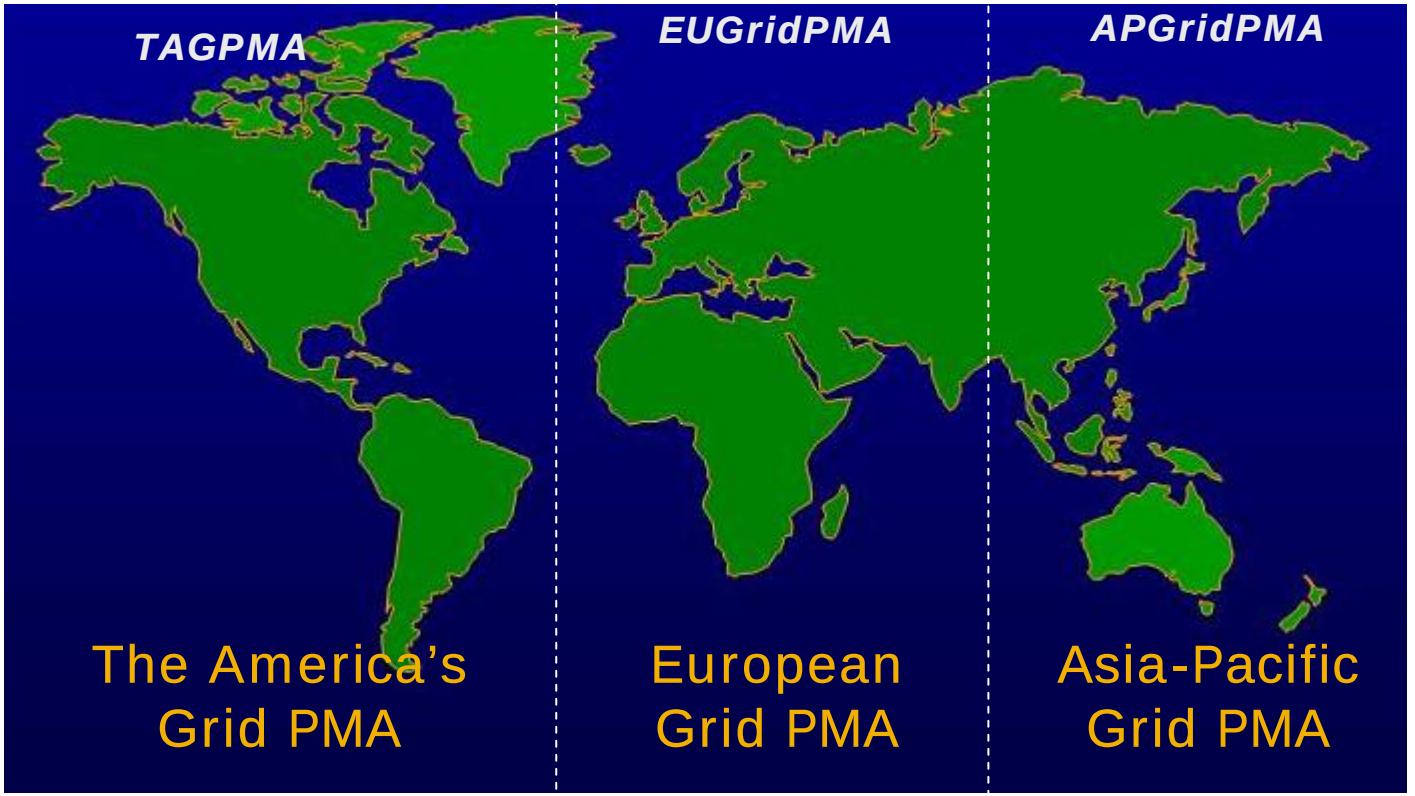
Launched June 28th, 2005
Pioneered new "SLCGS" (Kerberos CA & al.)

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!**

Extending Trust: IGTF – the International Grid Trust Federation

- **Common, global best practices for trust establishment**
- **Better manageability and response of the PMAs**



Middleware Security Group (MWSG)

Policies
Operations
OSCT

Architecture

gLite Security Modules

Joint Security Policy Group

MiddleWare Security Group

EUGridPMA

Grid vulnerability issues group

Security Guiding Documents

Trust anchor
IGTF chair

Identify
Audit preparation

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 4 other EU Grid initiatives. Also: NAREGI, UNICORE

- **MWSG output**

The meetings have addressed a number of middleware security issues and plans, e.g. gLite Security Release Plan, Security Architecture v1.0, First release candidate planning, Workplan update, EGEE/OSG/Naregi meeting, OSG and EGEE interop, Good interop. example' (GGF15 BOF), New EU members

Proposal on Interworking (OSG, EGEE)

- **Interop agreements list:**

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

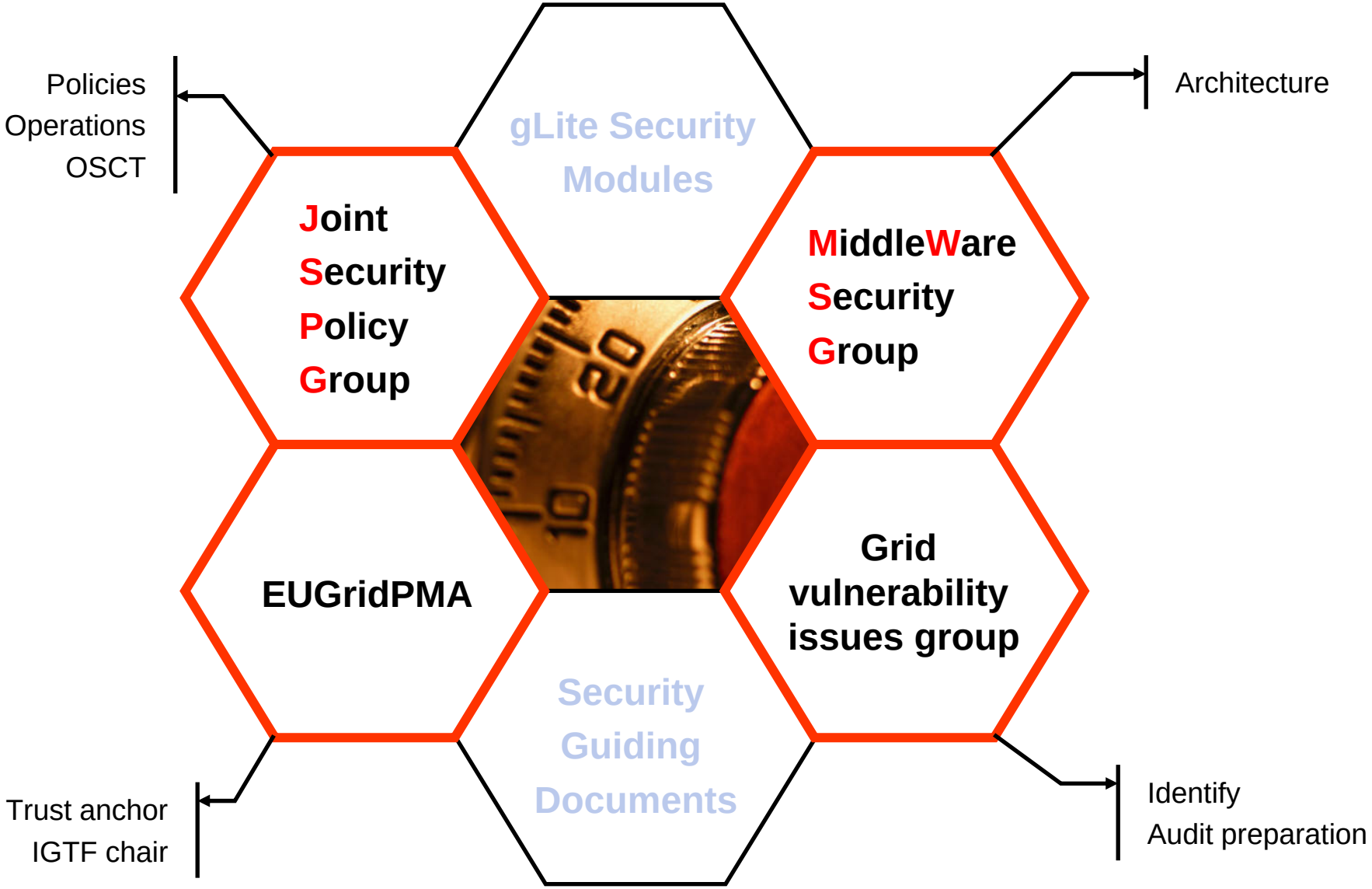
- **Service Specifications**

All service interface specifications have written specifications
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

NOW: The current security groups are successfully covering the various security aspects of the project.

NEXT: Formalizing the current security coordination work - The Security Coordination Group (SCG)

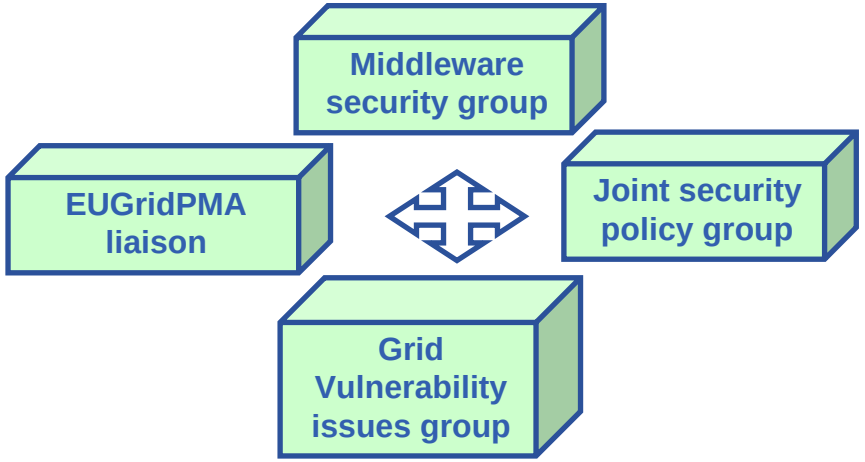
SCG will be responsible for ensuring overall EGEE-II security coordination, includes architecture, deployment, standardisation and cross-project concertation.

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.

Security Coordination Group (SCG) members - today's chairs of the security groups:

The Security Head, chair of the SCG

The chair of the MWSG
The chair of the JSPG
The EUGridPMA liaison
The chair of the Grid vuln. issues group

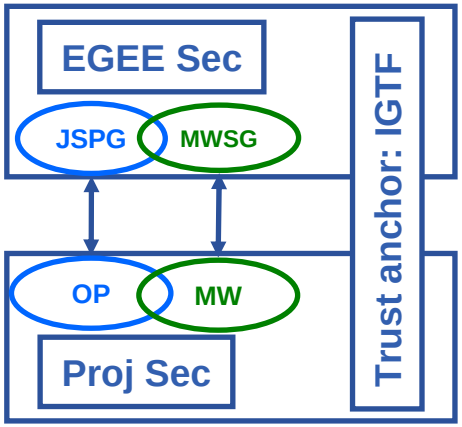


Security Collaboration

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).



Standardization work

- Leading the security area together with OSG, and being member of the GGF steering group.

- EUGridPMA (chair) and IGTF (chair).

The collaboration with OSG is close, from start.

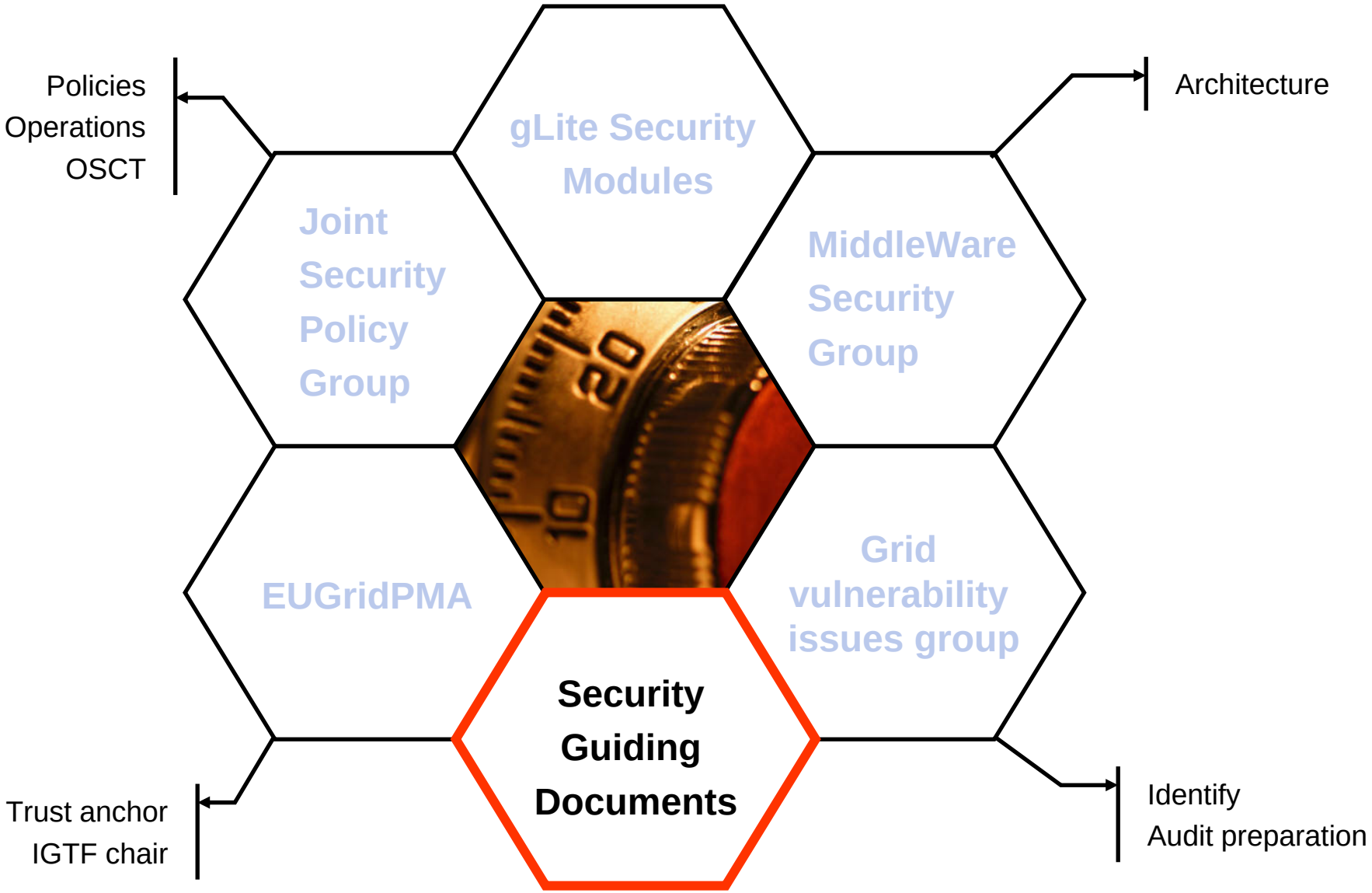
Together we have worked out a first suggestion on interoperability plans.

New collaborations have been established with 4 EU projects:

DEISA, SEEGRID, DILIGENT, and GRIDCC

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

Security Guiding Documents



Security Guiding Documents

Deliverables

Security Architecture MW OP
Revised mid-term

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

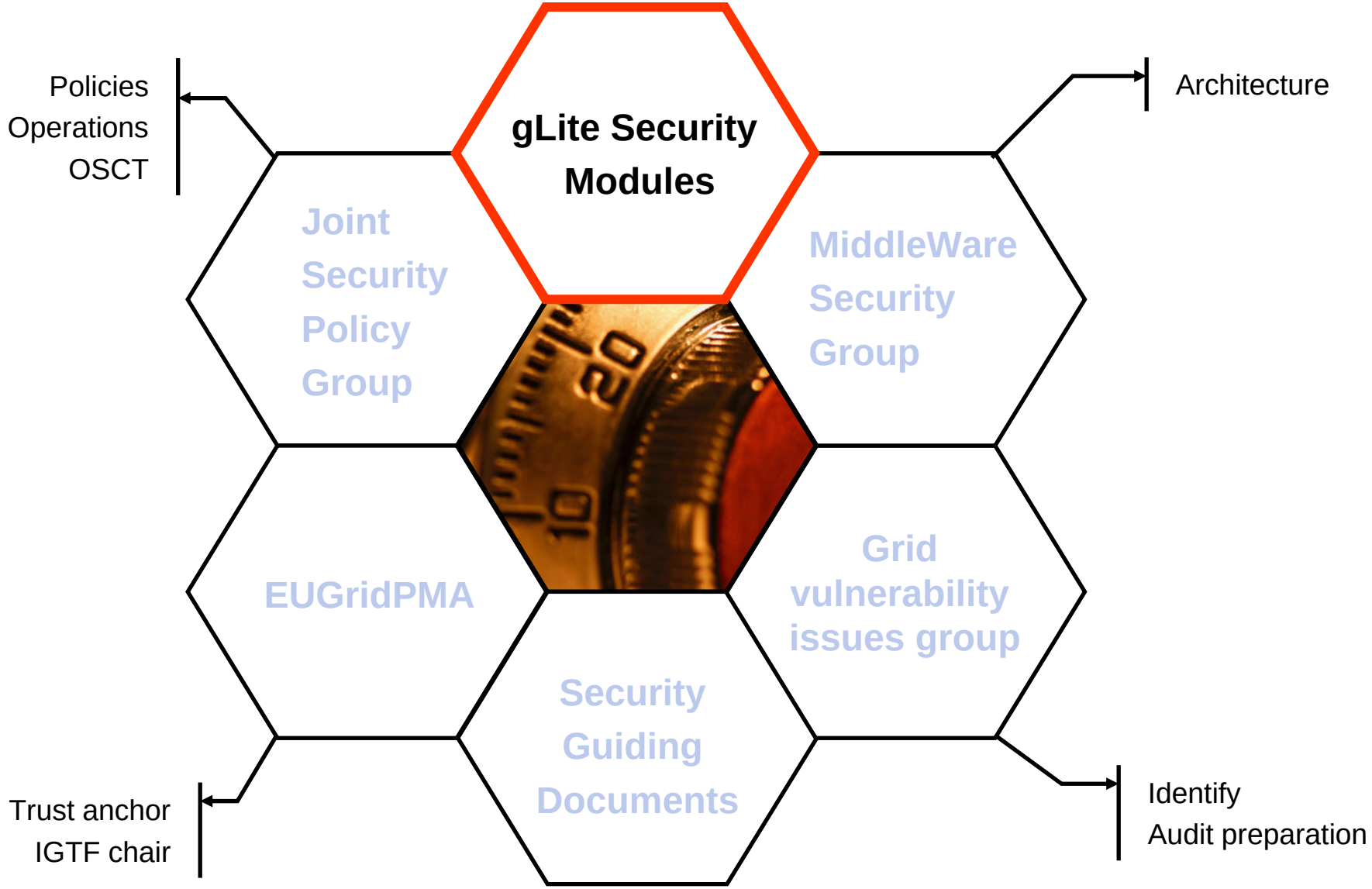
OGSA SEC service initial recommendations for reengineering MW

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



Architecture - Baseline assumptions

Security Architecture - Modular, Agnostic, Standard, Interoperable

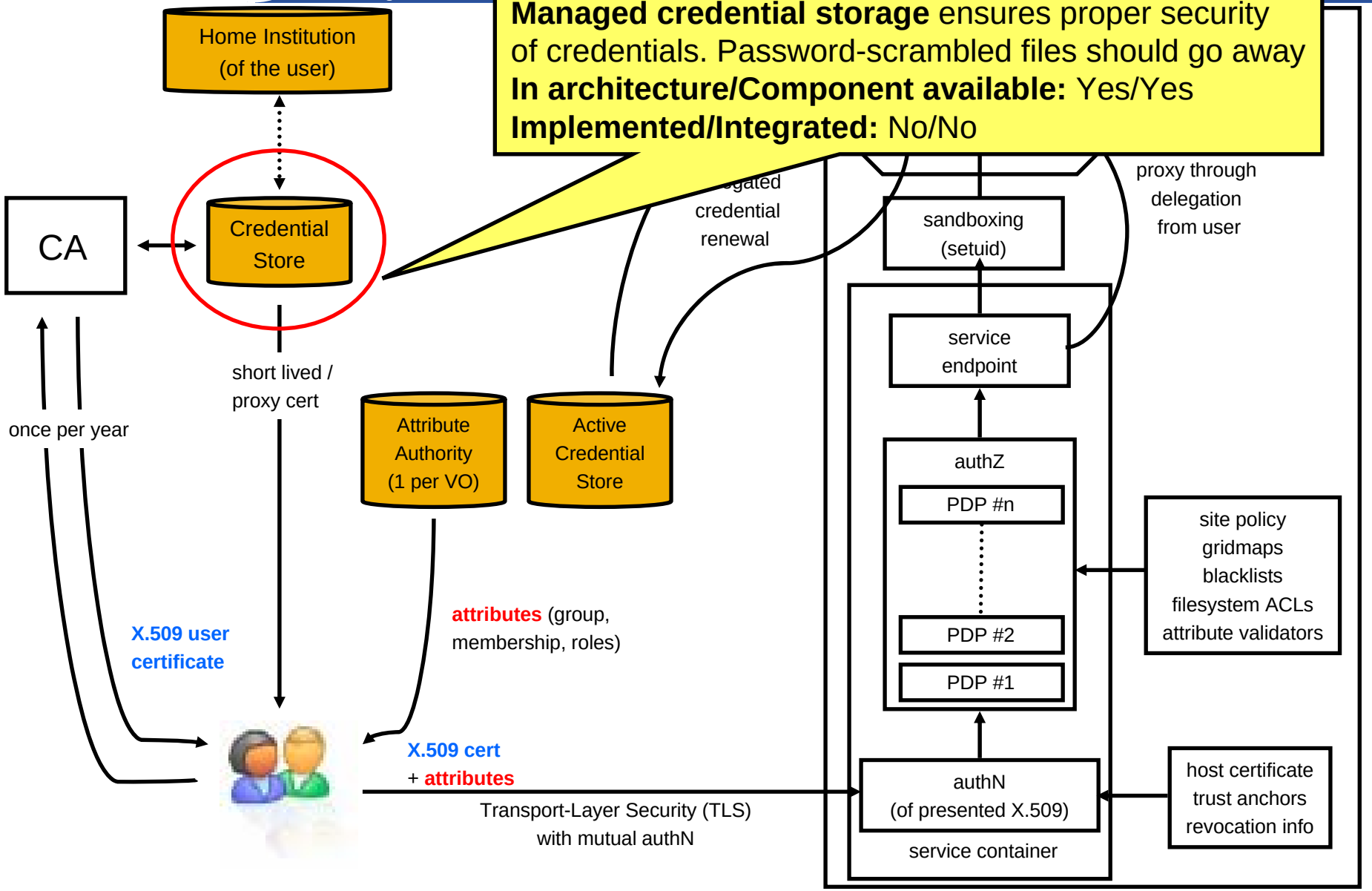
- Modular – possible to add new modules later
- Agnostic – implementation independent
- Standard – e.g. start with transport-level security but intend to move to message-level security when it matures
- Interoperable - at least for AuthN & AuthZ
- Applied to Web-services hosted in containers (Apache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

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
- Defining what security modules to deliver when

gLite Security Modules
Services - Authentication

Managed credential storage ensures proper security of credentials. Password-scrambled files should go away
In architecture/Component available: Yes/Yes
Implemented/Integrated: No/No



gLite Security Modules
Services - Authentication

Managed credential storage ensures proper security of credentials. Password-scrambled files should go away

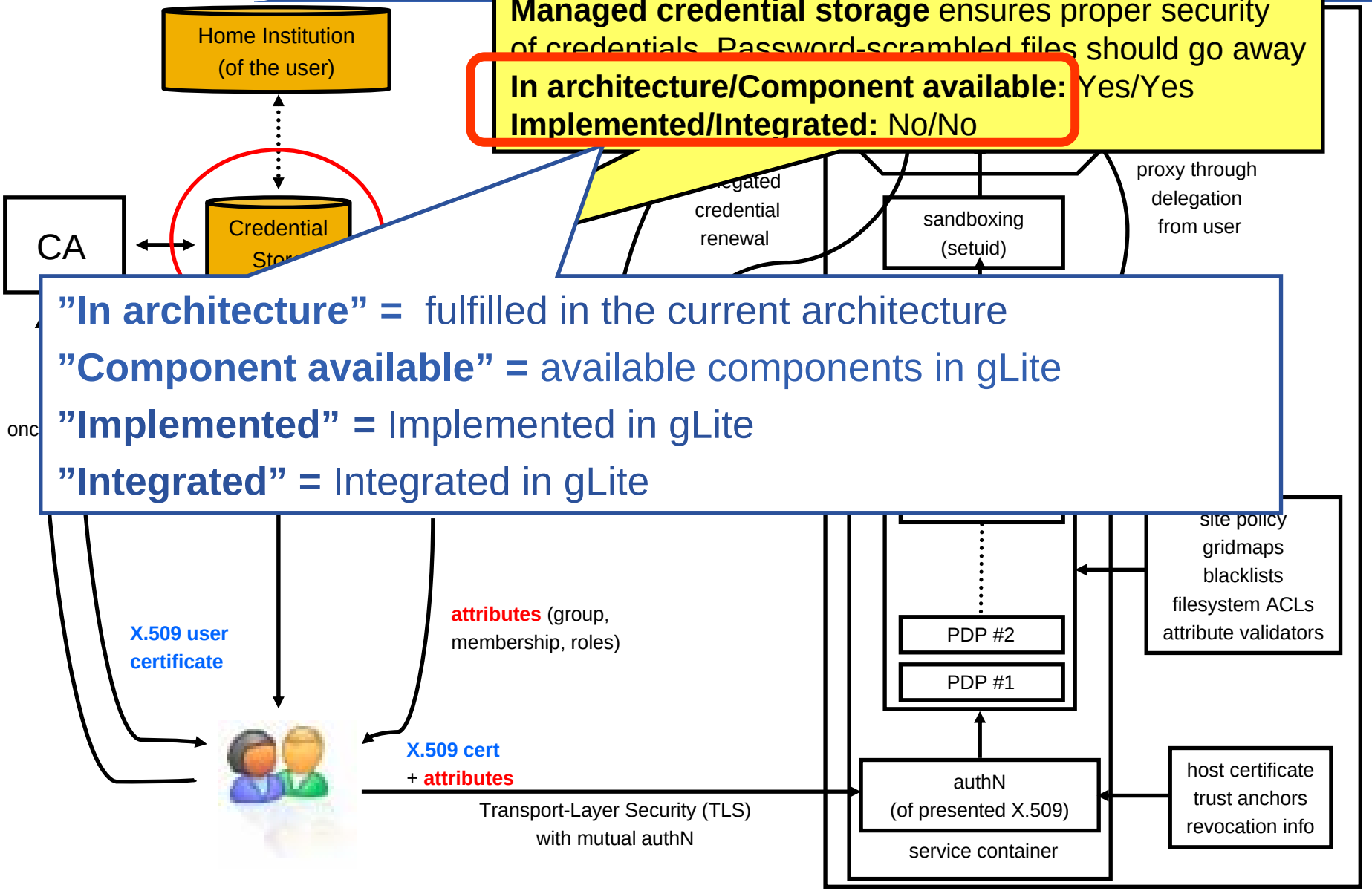
In architecture/Component available: Yes/Yes
Implemented/Integrated: No/No

"In architecture" = fulfilled in the current architecture

"Component available" = available components in gLite

"Implemented" = Implemented in gLite

"Integrated" = Integrated in gLite



gLite Security Modules Services - TLS vs MLS

Transport Level Security

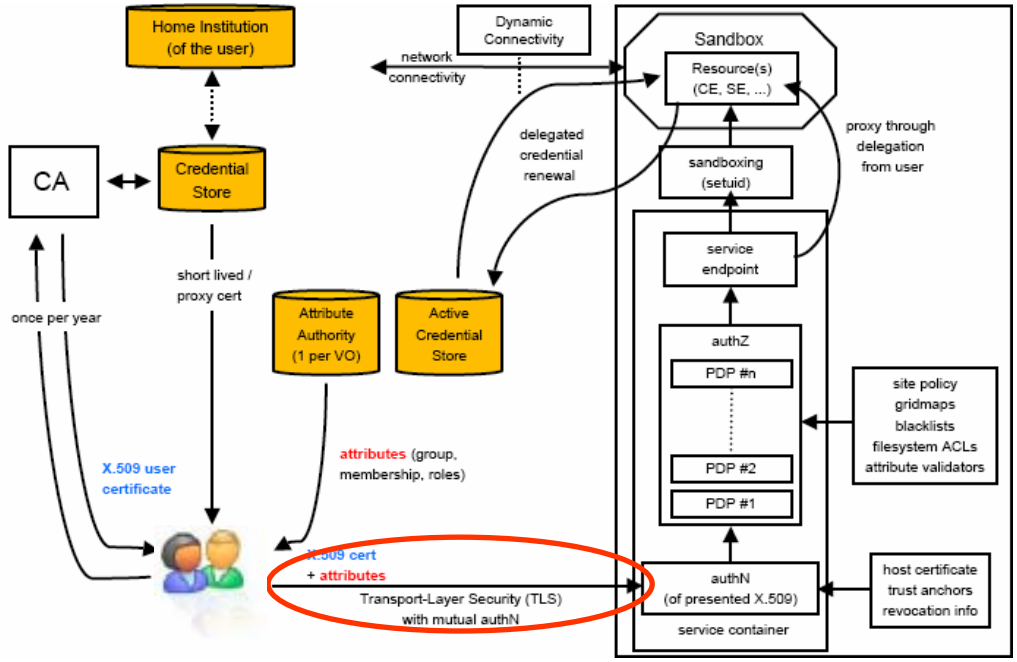
- Uses widely deployed TLS/SSL protocol
- Does not provides security through intermediate hosts (can be done using delegation, not yet delivered).

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

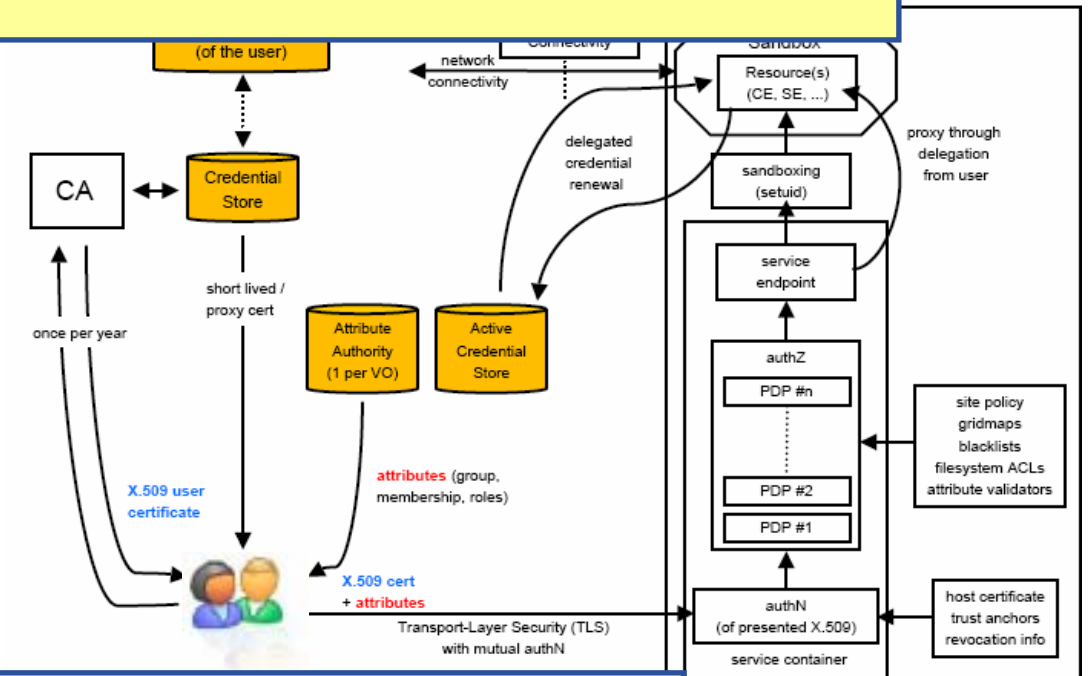
So, TLS for now

- SOAP over HTTPS with proxy cert supported path validation
- WS interface for delegation
- **Add MLS as we go along**
- Use cases for MLS exist already (DM)



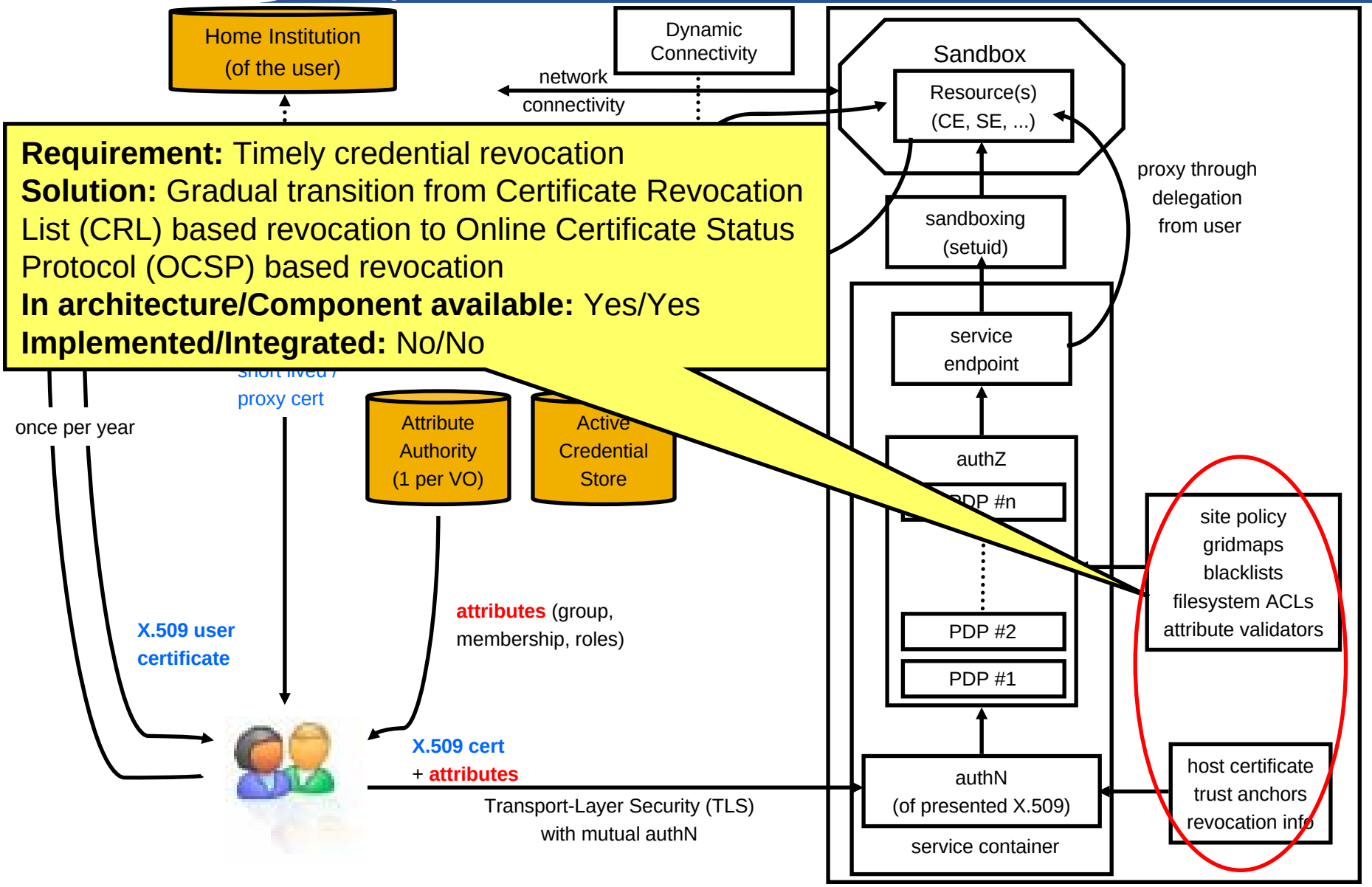
gLite Security Modules
Services - Logging and Auditing

Requirement: Audit ability
Solution: Meaningful log information. Logging and auditing ensures monitoring of system activities, and accountability in case of a security event
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes



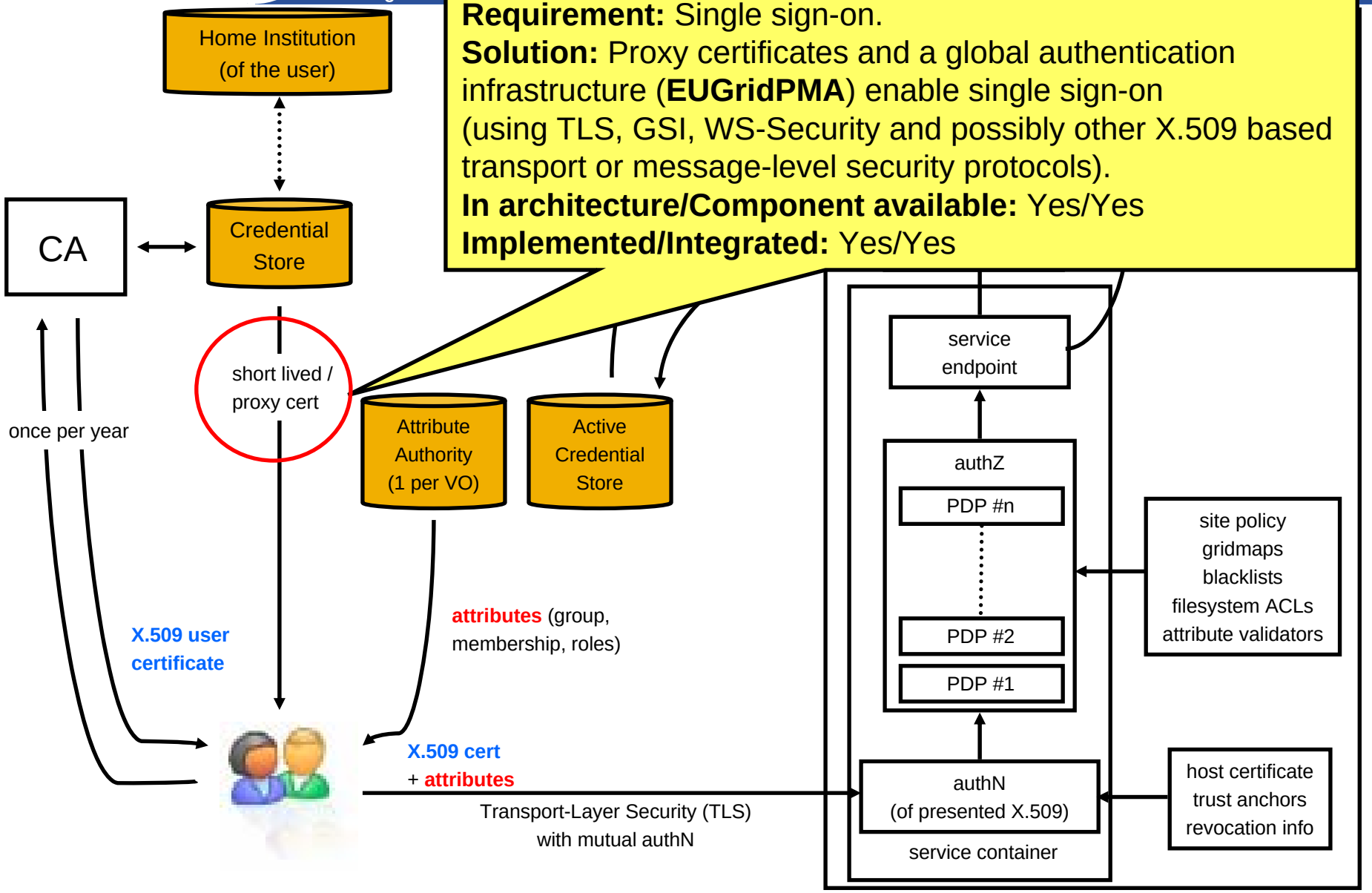
Requirement:. Accountability
Solution: All relevant system interactions can be traced back to a user
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes

gLite Security Modules Services - Authentication



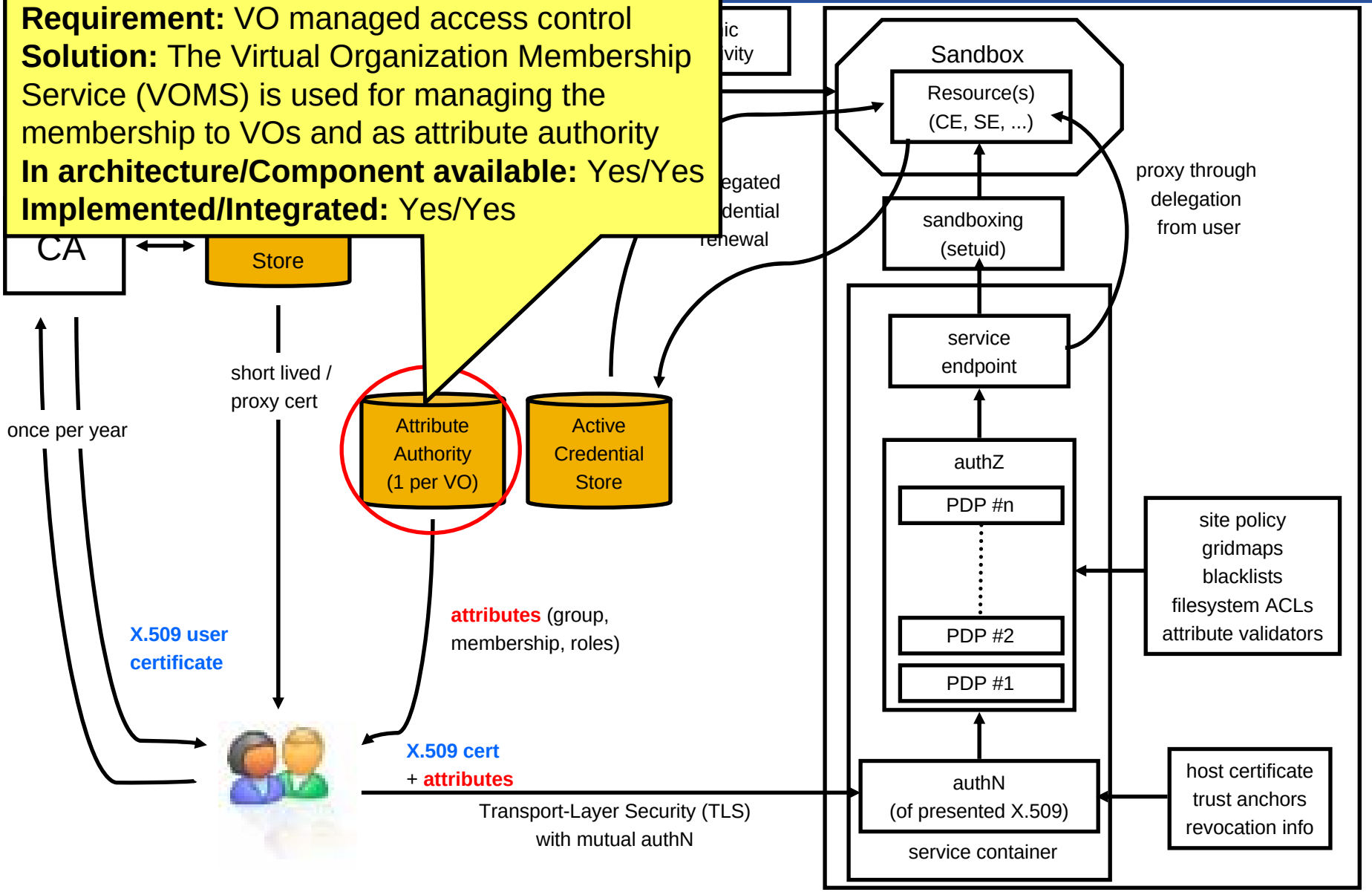
gLite Security Modules Services - Authentication

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).
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes



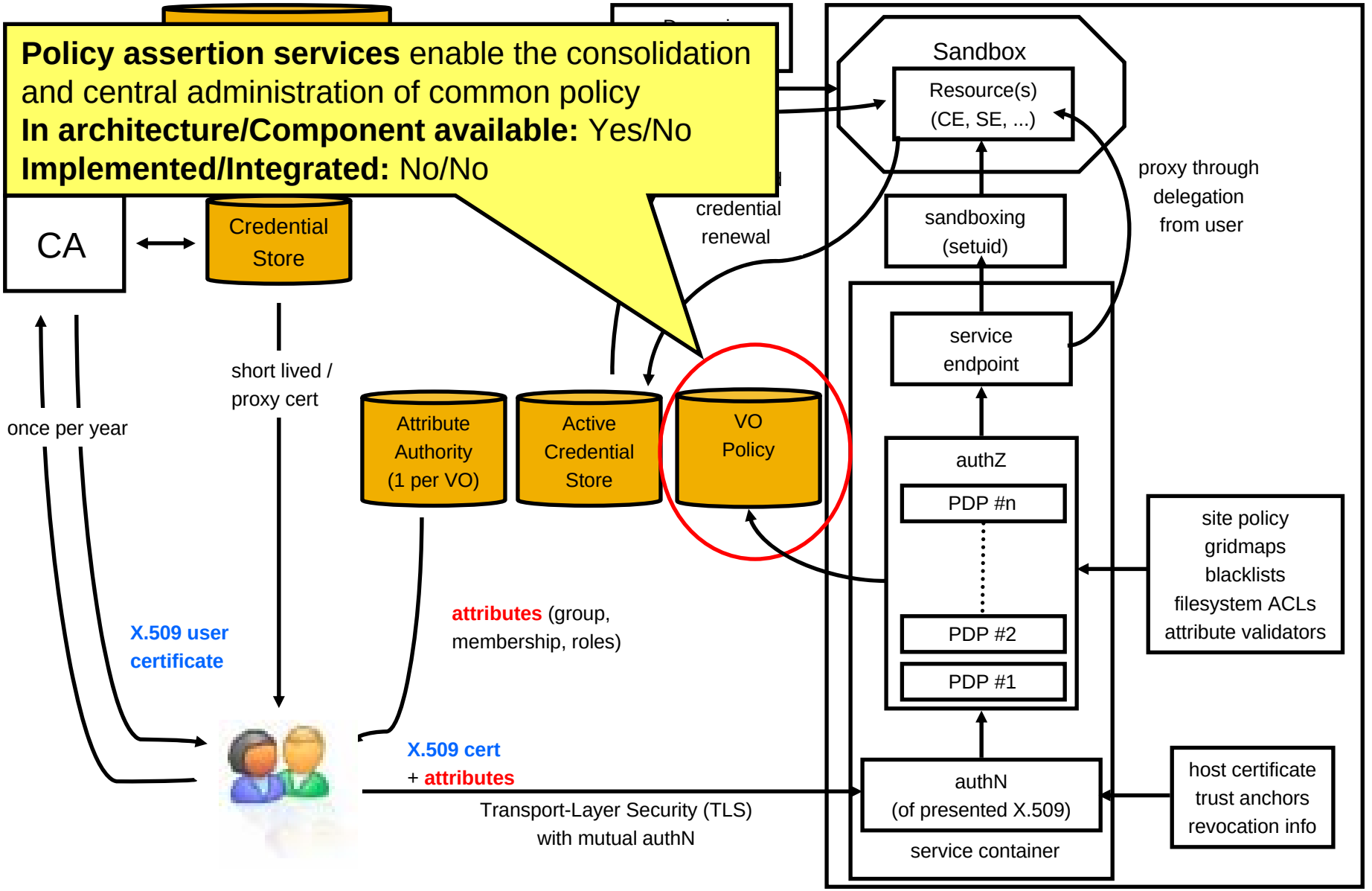
gLite Security Modules Services - Authorization

Requirement: VO managed access control
Solution: The Virtual Organization Membership Service (VOMS) is used for managing the membership to VOs and as attribute authority
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes



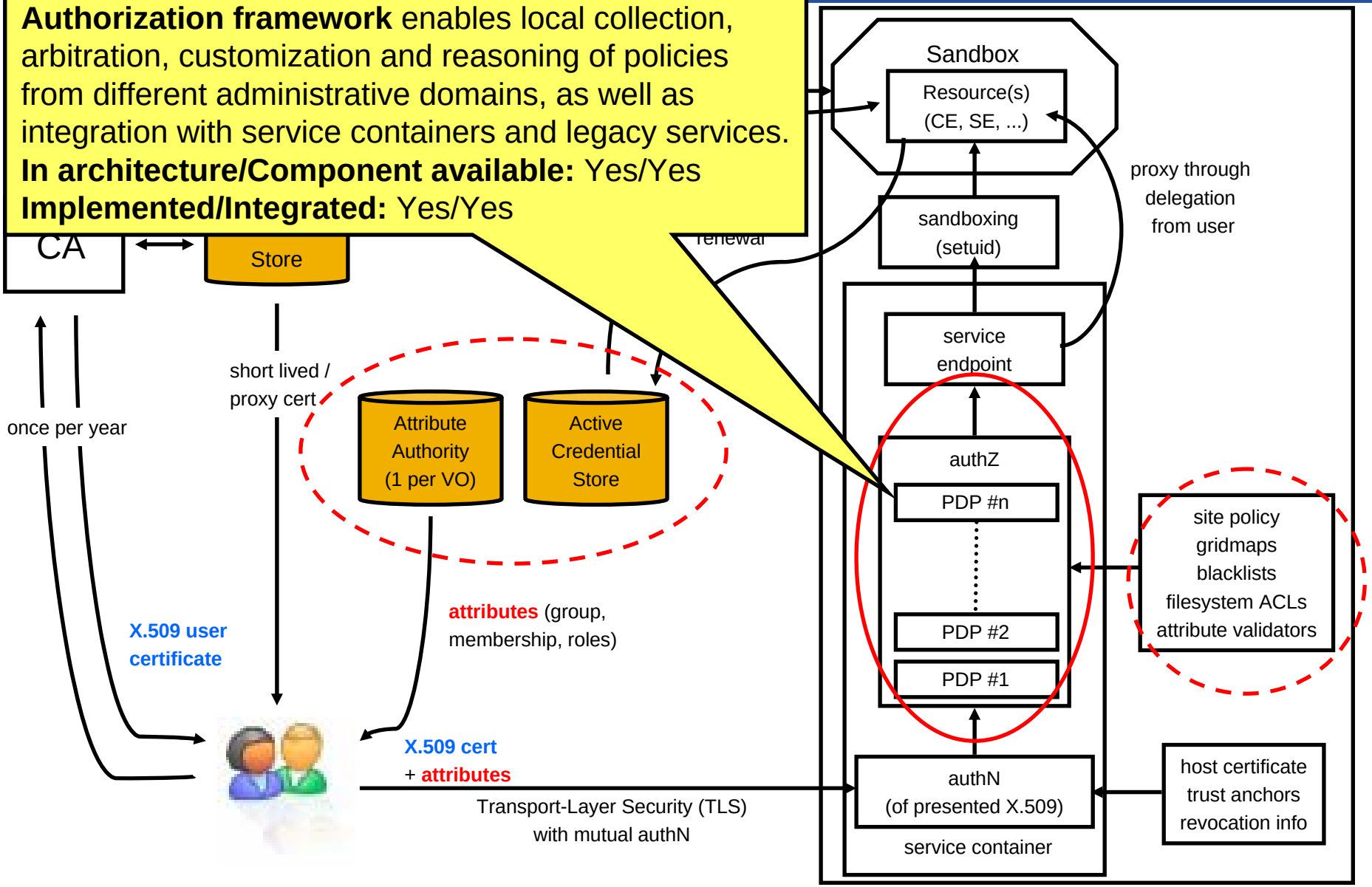
gLite Security Modules Services - Authorization

Policy assertion services enable the consolidation and central administration of common policy
In architecture/Component available: Yes/No
Implemented/Integrated: No/No

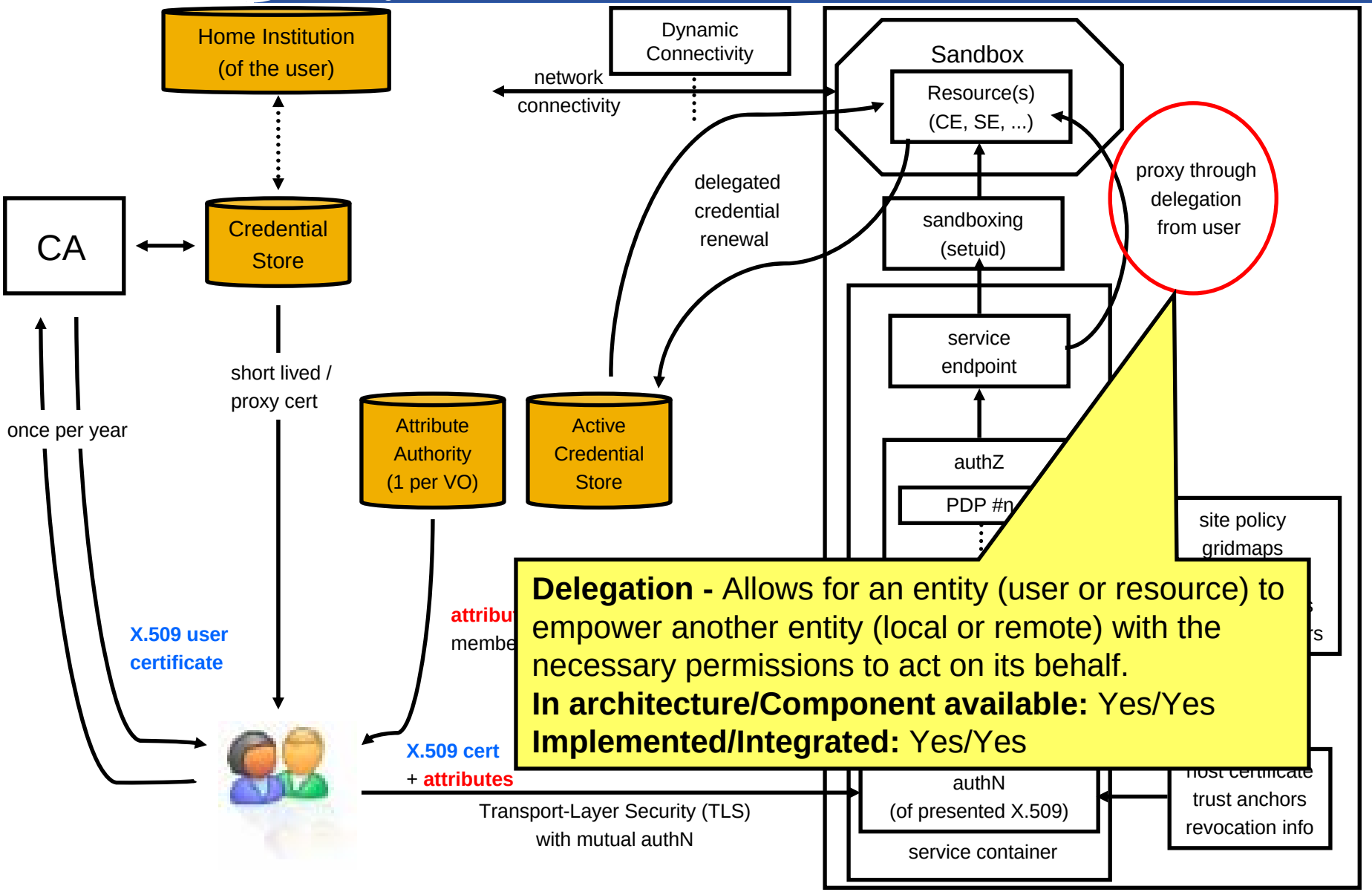


gLite Security Modules Services - Authorization

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.
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes

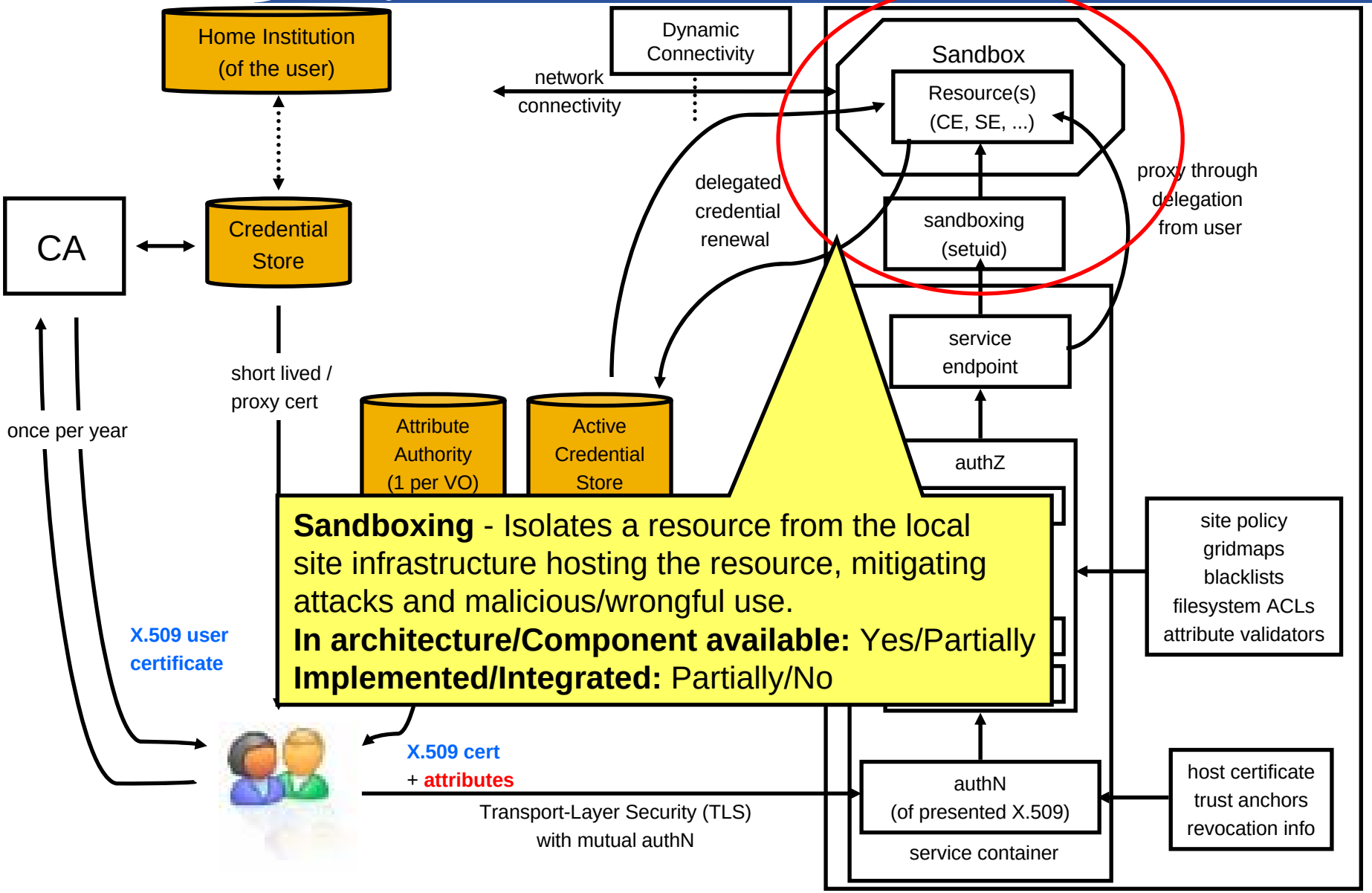


gLite Security Modules Services - Delegation



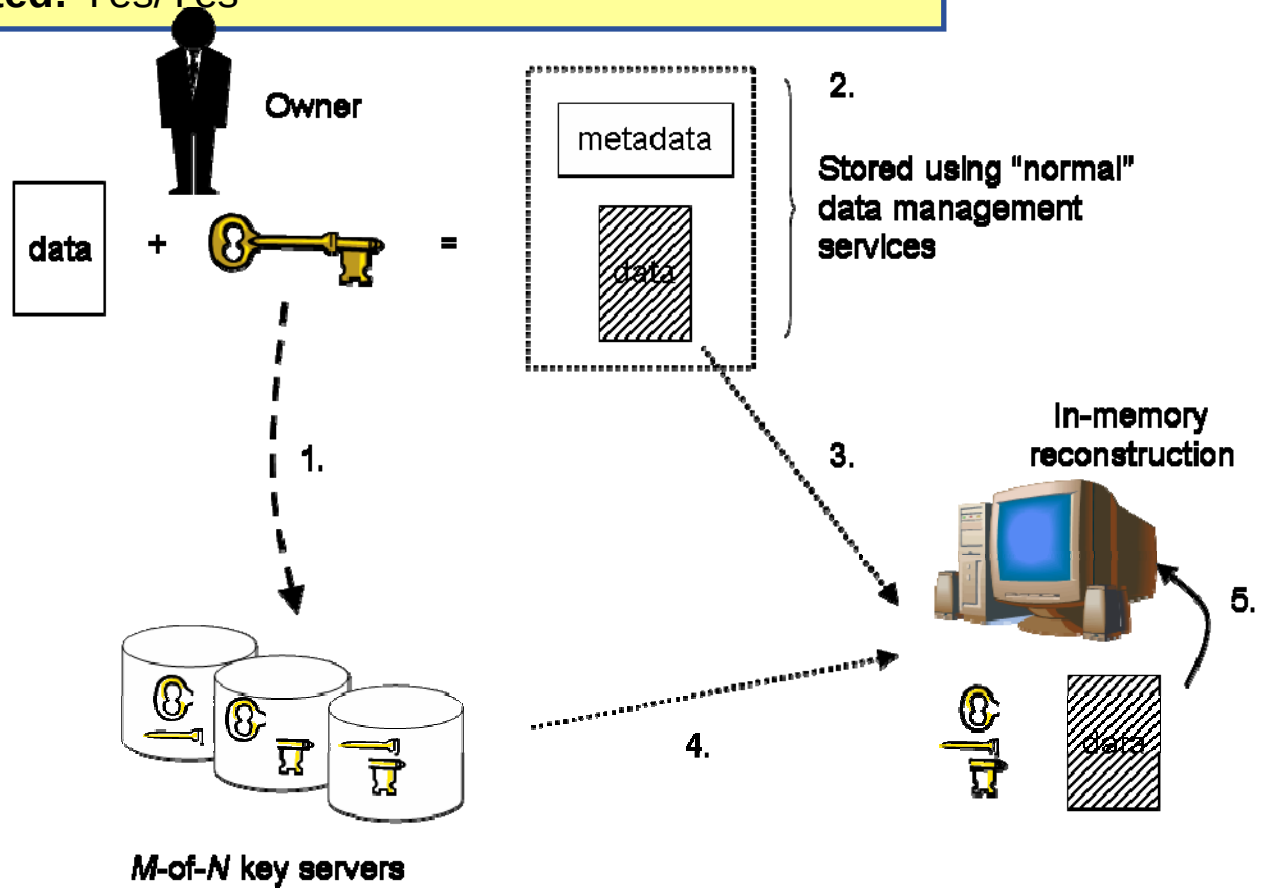
Delegation - Allows for an entity (user or resource) to empower another entity (local or remote) with the necessary permissions to act on its behalf.
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes

gLite Security Modules Services - Sandboxing



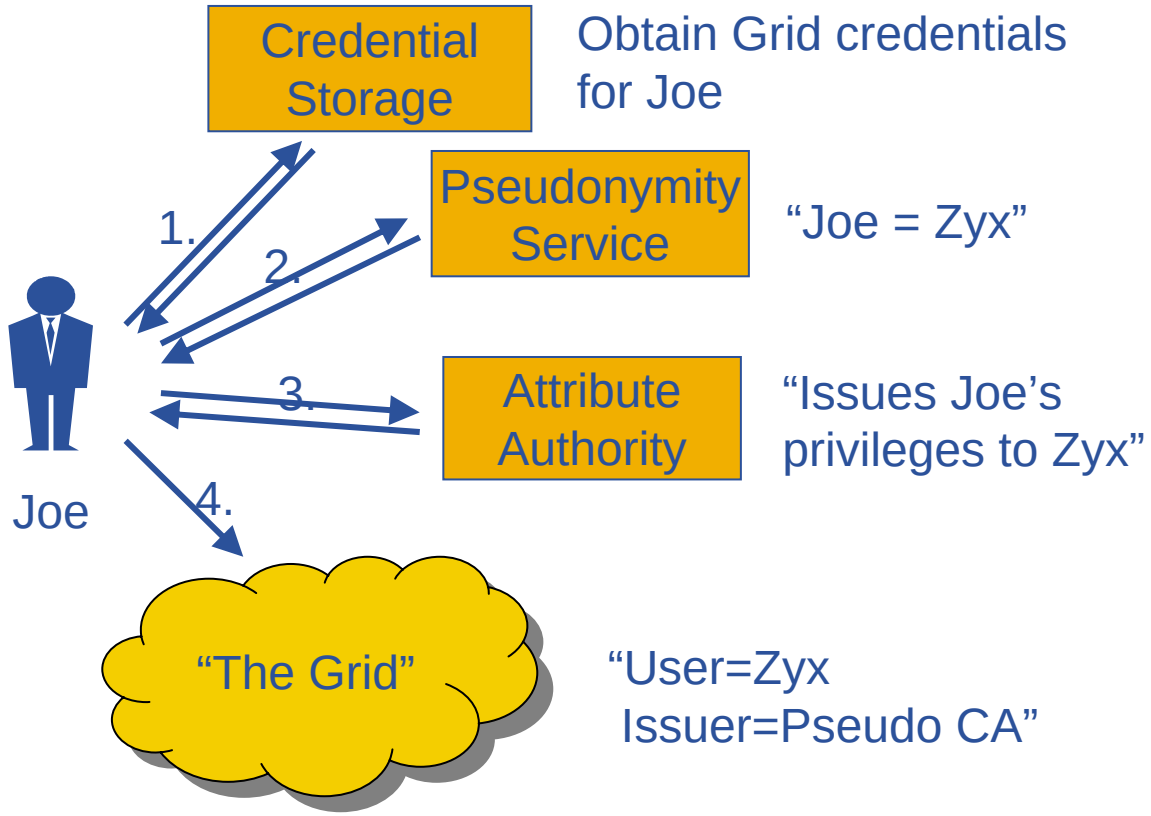
gLite Security Modules
Services - Encrypted Storage

Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
In architecture/Component available: Yes/Yes
Implemented/Integrated: Yes/Yes



gLite Security Modules Services - Pseudonymity

Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
In architecture/Component available: Yes/No
Implemented/Integrated: No/No



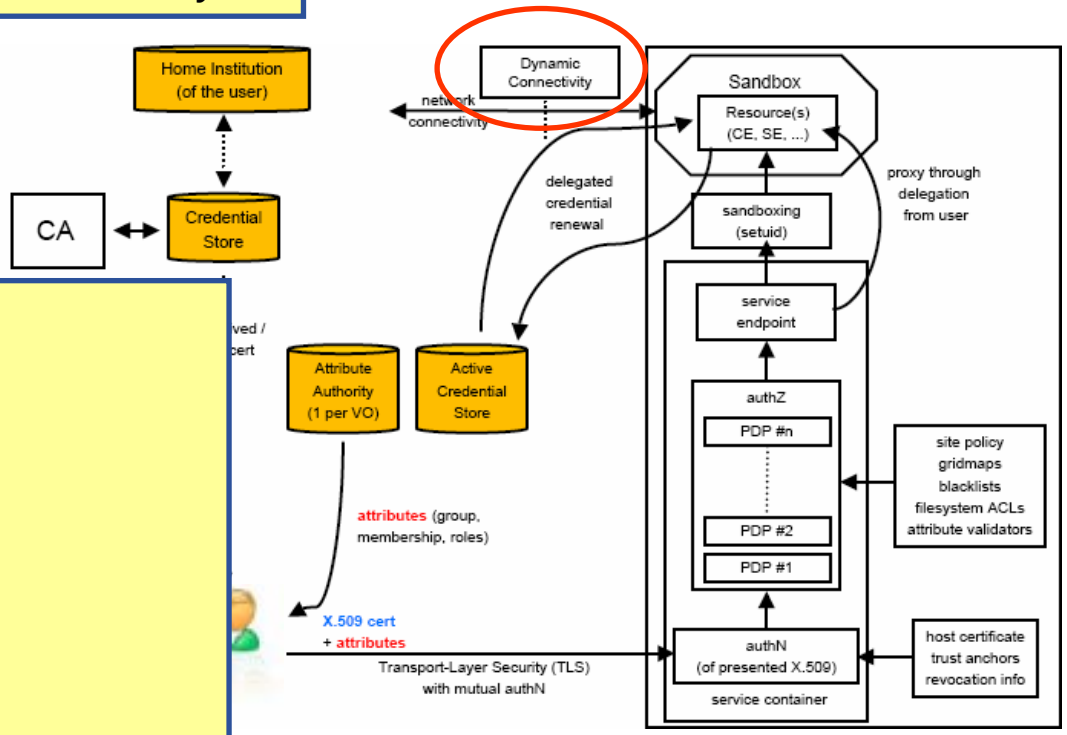
gLite Security Modules
Dynamic Connectivity Service

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

In architecture/Component available: Yes/No

Implemented/Integrated: No/No

- **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

Next couple of slides: a list of the s/w produced by JRA3

Released gLite Security Modules

Authz framework (java)
Generic, pluggable policy-engine chaining infrastructure.

Encrypted storage (C++ and Script)
File encryption and secret sharing library and example of usage.

Grid enhancements for OpenSSL
Implemented support for Grid proxies. Added to OpenSSL main line.

glexec
Designed to switch identity from the grid user to a local user, “sudo for grids”.

Jobrepository
Stores all known information about the user-mapping

Security test utils
Simplifying testing of security modules. Used widely in gLite standard testing procedures.

Trustmanager
Grid proxy support and enhancement for java SSL.

LCAS - Local Centre Authorization Service
Handles the authorization to the local fabric based on the user's proxy certificate and the job description in RSL format.

LCMAPS - Local Credential Mapping Service
Provides the local credentials needed for jobs allowed into the local fabric, in particular the unix uid and gids.

Gatekeeper
Globus gatekeeper, extended with call-outs to LCAS and LCMAPS.

gsoap plugin
Grid proxy support and ssl for gSOAP SOAP library

proxyrenewal
Grid proxy support and ssl for gSOAP SOAP library

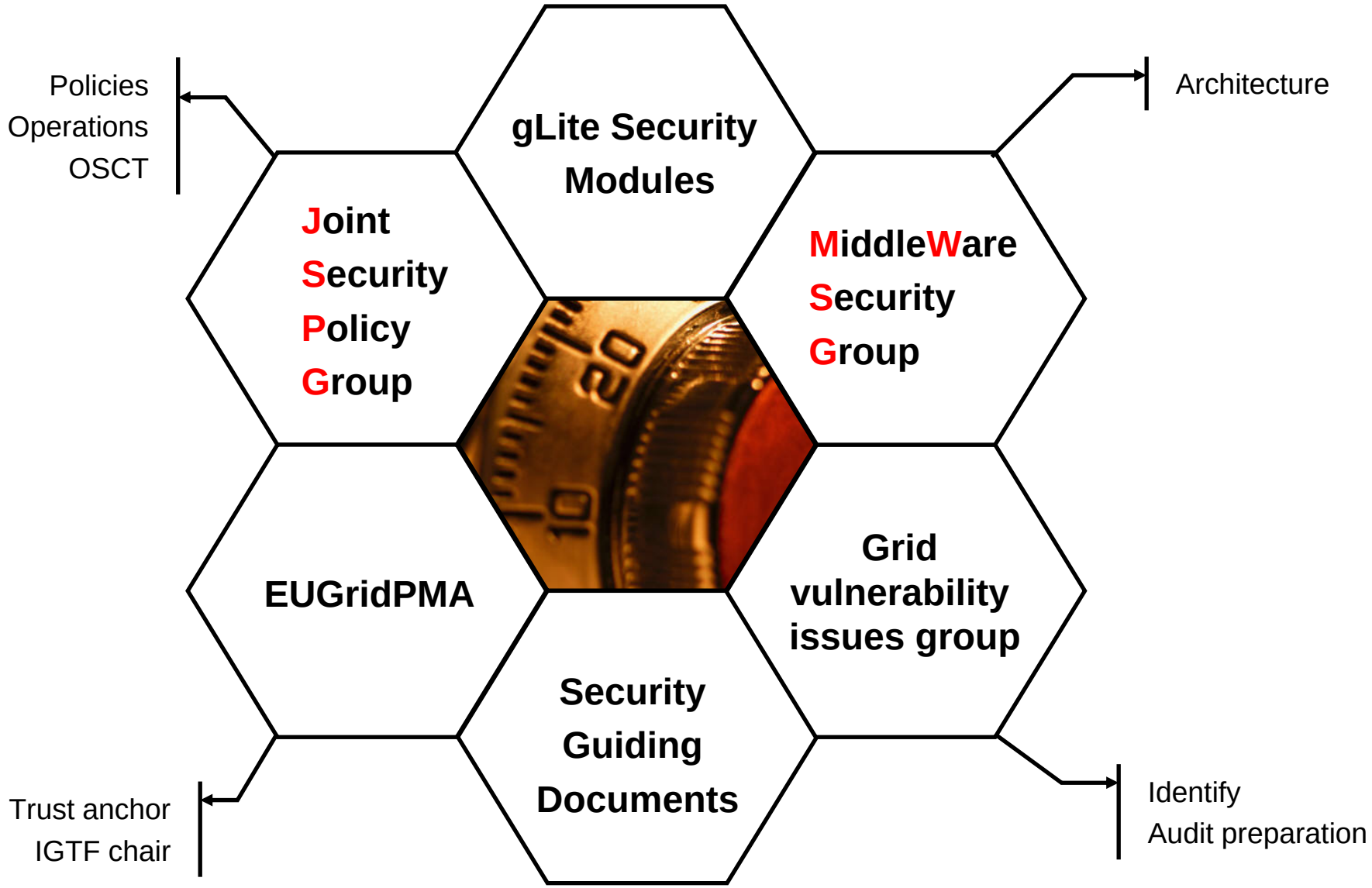
Util (java)
Security utilities for java.

Also contributing to the VOMS work

Plans and status – Next 4 months

- Continued gLite work (as part of JRA1)
- PM21 Second revision of the Security operational procedures document
- PM22 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

Summary - Security services

Requirement	In architecture	Solution/ Technology/Service	Component Available	Implemented	Integrated
Single sign-on	Yes	Proxy certificates and a global authentication infrastructure	Yes	Yes	Yes
User Privacy	Partially	Pseudonymity services	Yes	No	No
Data Privacy	Partially	Encrypted Storage	Yes	Yes	Yes
Audit ability	Partially	Meaningful log information	Yes	Yes	Yes
Accountability	Yes	All system interactions can be traced back to a user	Yes	Yes	Yes
Combining policy from different administrative domains	Partially	Authorization framework	Yes	Yes	Yes
VO managed access control	Yes	VOMS	Yes	Yes	Yes
Support for legacy and non-WS based software components	Yes	Modular authentication and authorization sofware suitable for integration	Yes	No	No
Non-homogenous network access	Yes	Dynamic Connectivity Service	No	No	No

Summary - Security modules

Module	Component available	Implemented	Integrated
AuthZ framwork (java)	Yes	gLite1.0	Yes
Grid enhancement for OpenSSL	Yes	No	Yes, in openssl-0.9.7g
glexec	Yes	gLite3.0	No
Jobrepository	Yes	gLite1.5	No
Security test utils	Yes	gLite1.3	Yes
Trustmanager	Yes	gLite1.0	Yes
LCAS	Yes	gLite1.0	Yes
LCMAPS	Yes	gLite1.0	Yes
Gatekeeper	Yes	gLite1.0	Yes
Delegation	Yes	gLite1.2/1.5	Yes
gsoap plugin	Yes	gLite1.2(not JRA3)	Yes

Conclusion

- JRA3 has released and is supporting a number of security related software modules in gLite.
- The EGEE security groups have been successfully moved towards an agreed security infrastructure with OSG, expanding towards EU grids and NAREGI.
- EUGridPMA was the leading partner in the establishment and has the first chair of IGTF.
- Secure Credential Storage procedures was added to the list of security guiding documents.
- A first revision was made of the Global security architecture.
- Assessment document of accounting infrastructure and analysis of what is missing to provide secure quota-based resource access was prepared.

Questions and Answers