EMI Security Architecture.

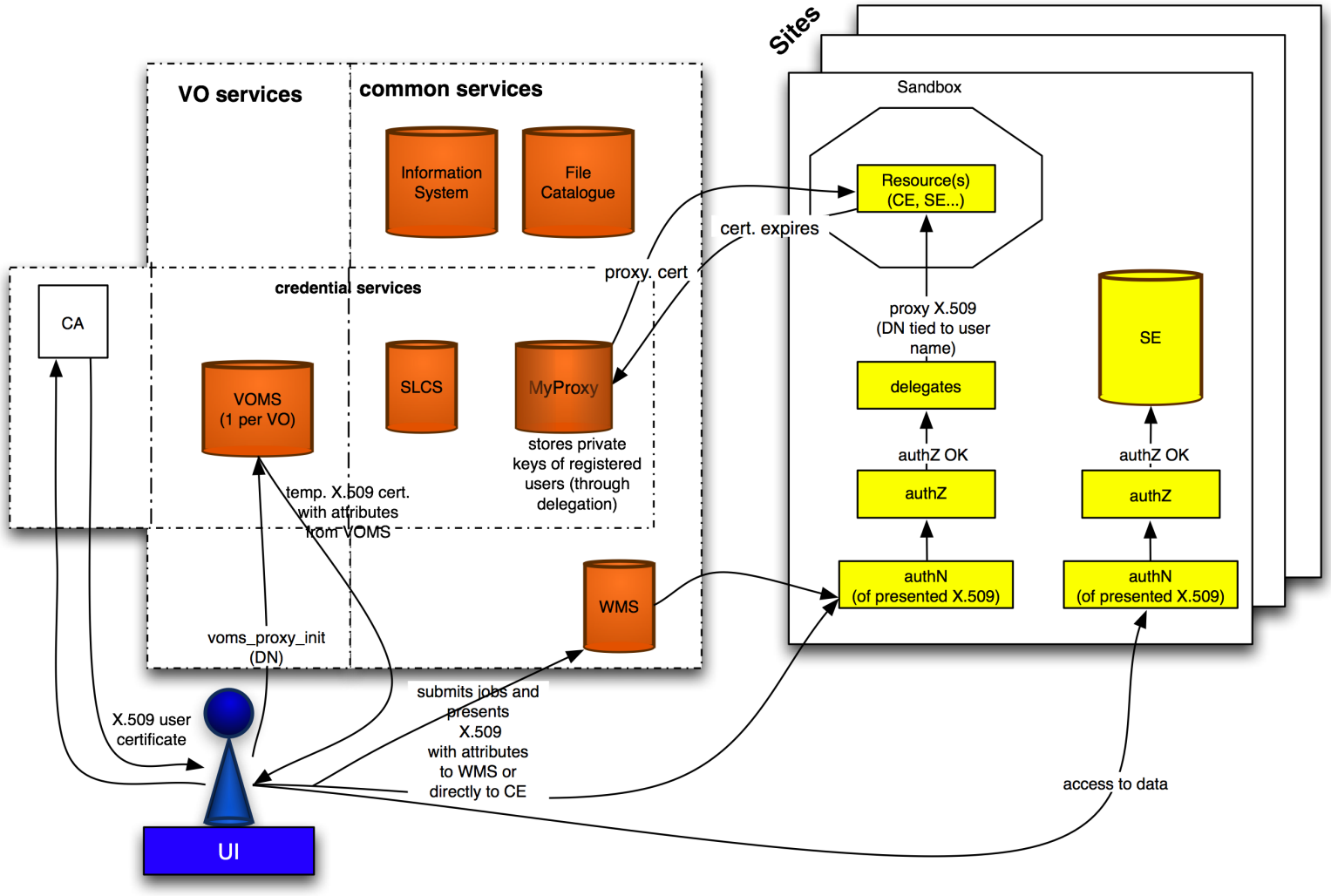
John White (for the EMI Security Task)

EMI INFSO-RI-261611
EMI All-Hands meeting, Nov 23rd 2010, Prague

Introduction

- **Security Architecture**
- What does Security "Architecture" mean?
- Not a rigid diagram of services.
- A collection of recommendations for middleware.
- Agreements that come from the working groups.
  - **Common Authentication Libraries.**
  - **Common Attribute Service with common profile.**
  - **Common Authorization system.**
  - **Common XACML profile for CEs.**
  - **Common delegation method.**
  - **Flexible AAI user interface.**

Security Overview



Common Authentication Libraries

All EMI components will be expected to use the common authentication libraries provided by the (to be formed) "AuthN lib" PT.

- Library form, languages and API determined by working group.
- Libraries primarily concerned with Authentication.
- APIs provided in C/C++ and Java.
- Agreement on the APIs has been reached at (or before) this meeting.

More information available at:

`https://twiki.cern.ch/twiki/bin/view/EMI/`

→ `EmiJra1T4SecurityCommonAuthNLib`

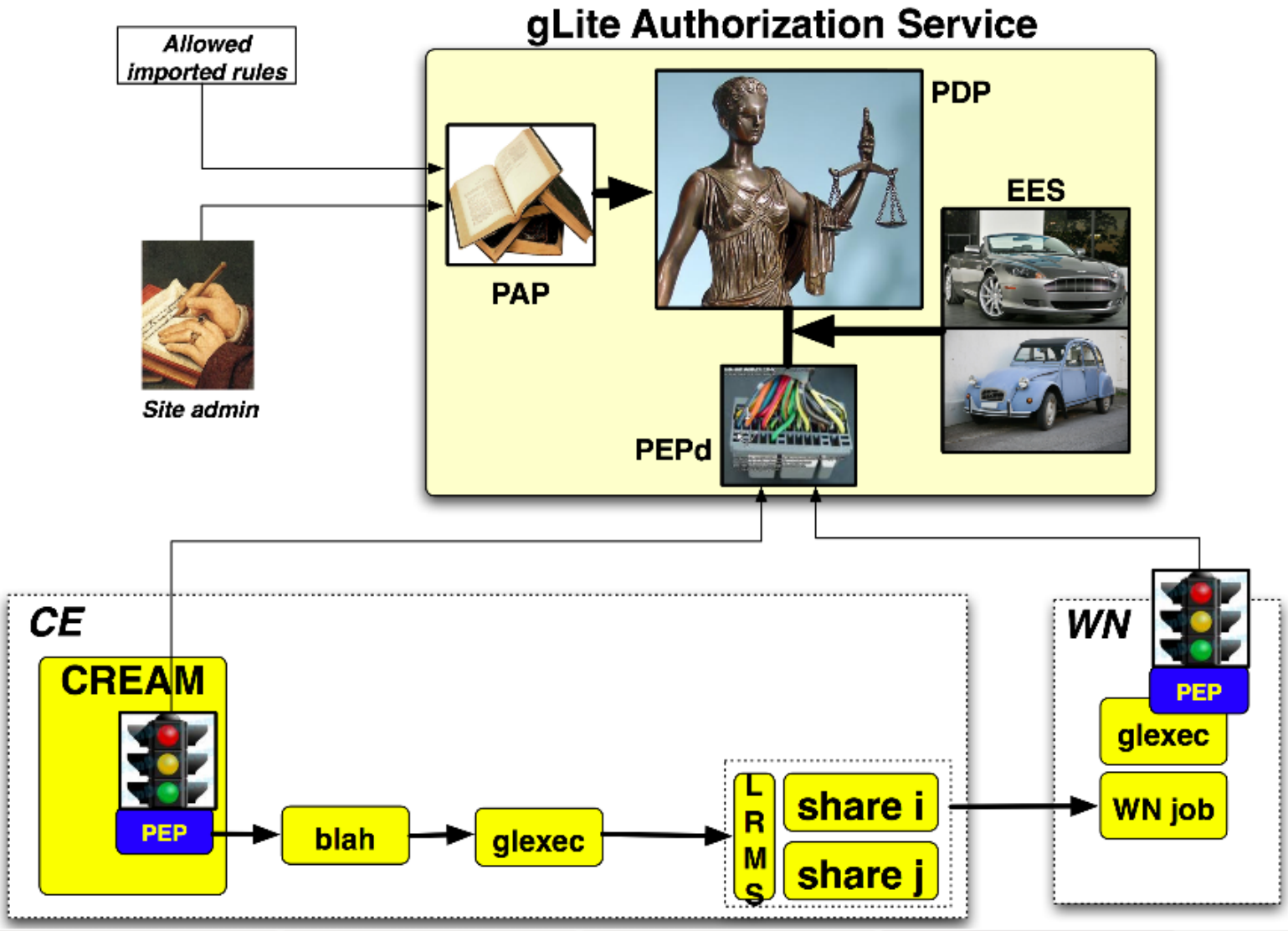
VOMS-SAML

A common Attribute service will be used. VOMS-SAML.

- Agreed to replace UNICORE UVOS with VOMS-SAML.
- Same VOMS-SAML version for gLite/ARC.
- Common SAML profile for all EMI stack.
- VOMS-SAML will issue attributes.

More information available at:
`https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML`

Argus AuthZ Service



Argus AuthZ Service

Argus will be taken as the common Authorization system.

- Starting with CEs.
- WMS and Data Management to follow.
- The common XACML profile will define the attributes passed.
  - Integration schedule to other components.
    - CE(s)
    - WMS
    - Data Management (DPM on the way, dCache started (EMI-1))
    - What else? Bolt on to a OCCI interface?

Common XACML profile

As Argus will be the common AuthZ solution, a common XACML profile for CEs is needed.

- Define XACML attributes for each CE to identify:
  - Users. (DN, FQAN, VO, CA, key-info)
  - Resources. (URN, URI, free id)
  - Actions. (??)
- gLite CE profile acts as basis.
- Expanded/clarified with attribs from ARC/UNICORE.

More information available at:
`https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML`

Delegation

EMI components that move proxies should use delegation. Delegation provided should move to the GSI-free and same WSDL.

- UNICORE, does not use proxies, uses ETD.
- ARC does not need delegation service.
- Where is delegation used?
  - gLite: WMS to CE.
  - gLite: FTS.
  - gLite: CREAM (exposes a WS for delegation).
  - ARC: Client to CE.
  - Other: gridFTP (this is a ???).
  - UNICORE: Does have a service, if needed.

Please see: `https://twiki.cern.ch/twiki/bin/view/EMI/`
→ `EmiJra1T6Standardization`

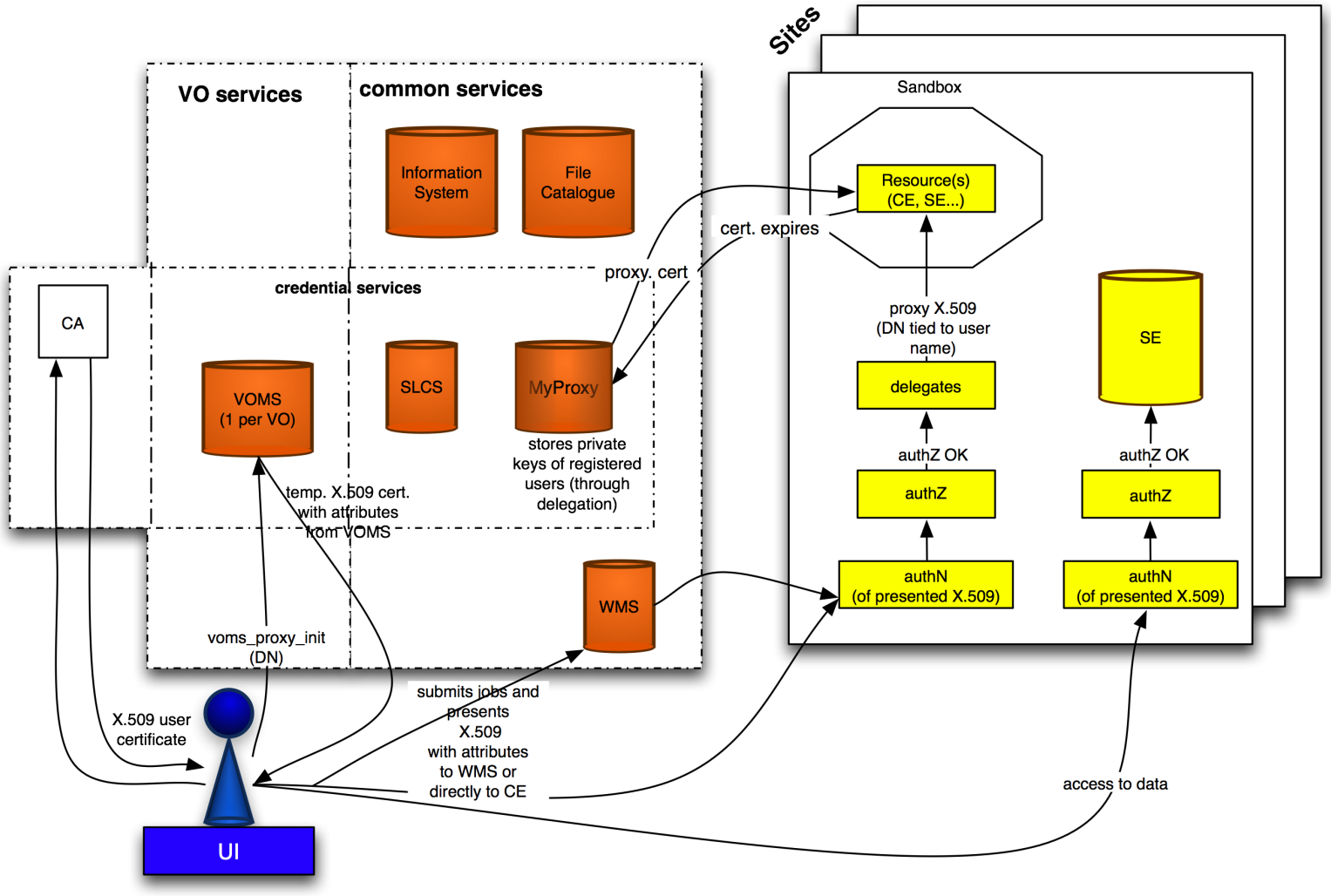
AAI Interface

"Users should be able to access EMI resources easily."

- Driven by requirements from users*.
- X.509 credentials passed for AuthN (and AuthZ*).
- SLCS, TCS or STS to issue credentials (from federated or not).

See the AAI report available at:
`https://twiki.cern.ch/twiki/bin/view/EMI/`
→ EmiJra1T4Security

Security Overview



What will improve?

- **Common Authentication Libraries.**
  - **Uniform AuthN response by all services.**
- **Common Attribute Service with common SAML profile.**
  - **Credentials and attributes issued throughout stacks.**
  - **Still not possible to submit WMS to UNICORE CE*.**
- **Common Authorization system.**
  - **Evident.**
- **Common XACML profile for CEs.**
  - **Common AuthZ for CEs.**
- **Common delegation method.**
  - **Evident.**
- **Flexible AAI user interface.**
  - **More users able to access resources.**