EMI Security “Directions”

John White for EMI Security Area

Helsinki Insitute of Physics

March 1st, 2012

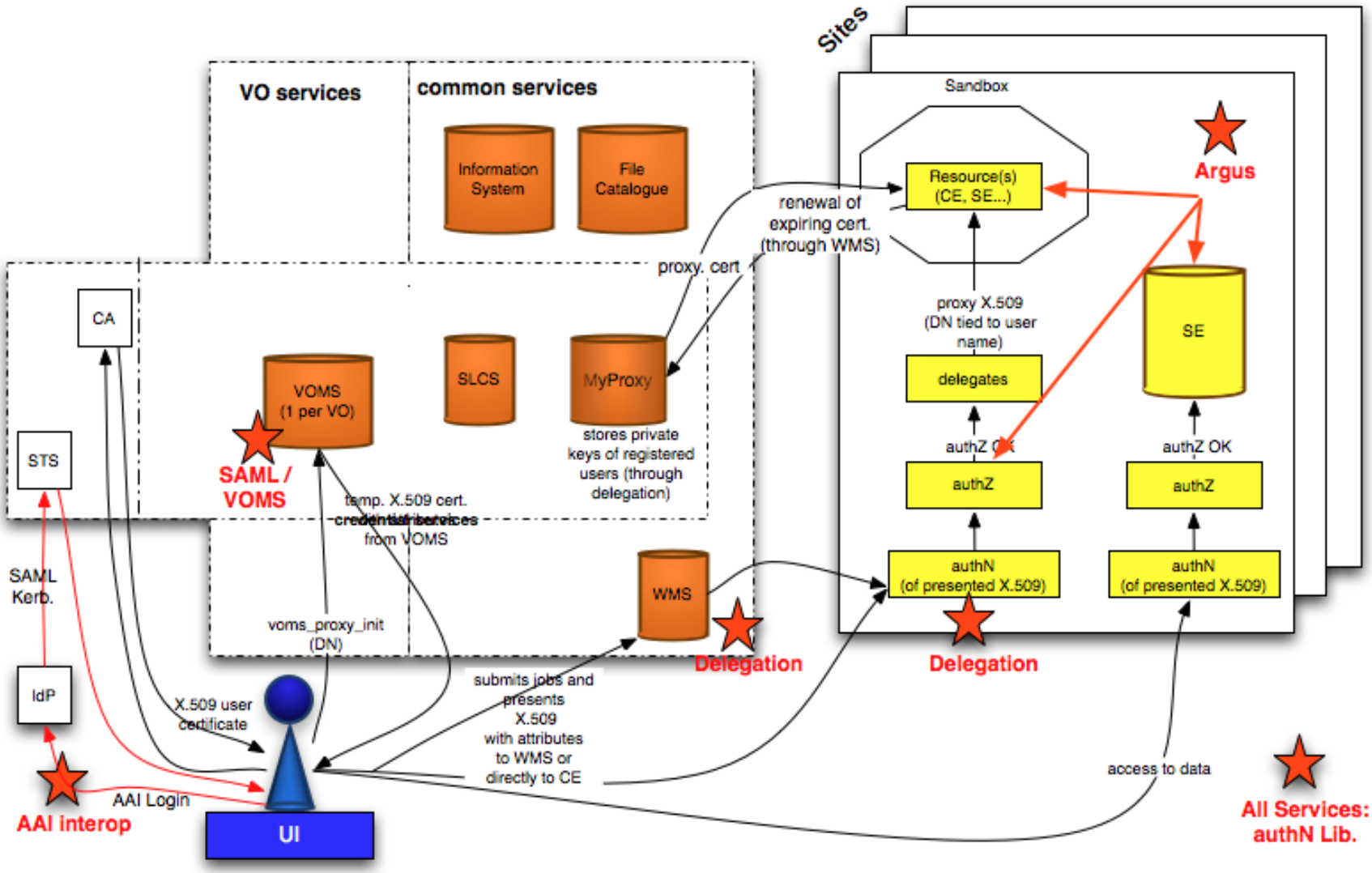
EMI INFSO-RI-261611

Overview

- **EMI project combines ARC, gLite and UNICORE stacks.**
  - Security models are similar not identical.
    - gLite, ARC based on X.509 credentials for AuthN/AuthZ [1].
    - UNICORE uses X.509 for AuthN, SAML attributes internally.
- Opportunity to improve the inter-operation.
- Unify and simplify the user credential handling.
- Provide common profiles and libraries for uniform operation.
  - Simplified credential handling
  - Common SAML profile
  - Common XACML profile
  - Common Authentication Libraries
  - Common Delegation method
  - Argus-EES.
- **The Security Area developments follow these directions.**

[1] AuthN - Authentication (who you are)
AuthZ - Authorization (what you can(not) do)

Credential Handling

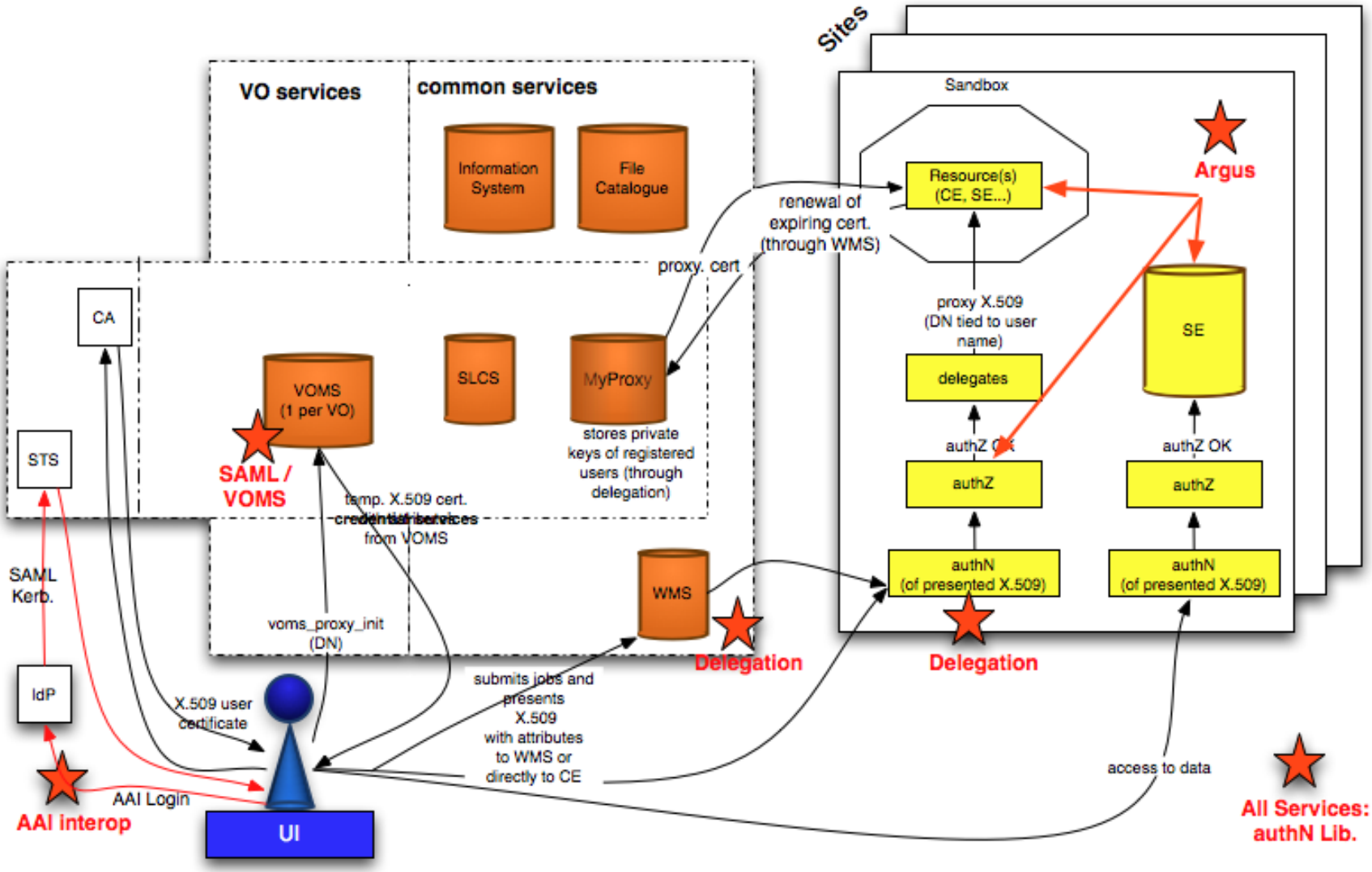


Credential Handling

- **Security Token Service "authenticates and authorizes" users based on security tokens.** [2]
- Aggregates the required information from external sources.
  - eg. The Identity Provider (IdP)
- Establishes a trust relationship between different security/application domains.
  - eg. Institute login $\rightarrow$ VO VOMS.
- First STS version will support the ISSUE operation that transforms an incoming security token into another security token.
  - Incoming formats: X.509, X.509 Proxy, SAML, Kerberos
  - Outgoing formats: X.509, using external online CA
    X.509 Proxy, exploiting VOMS
    SAML
    Kerberos
- **See next talk.**

[2] Security token: a collection of statements (or claims) about a user or resource, in this case: X.509 certificate, SAML assertion, Kerberos ticket, Username/Password

Common SAML profile

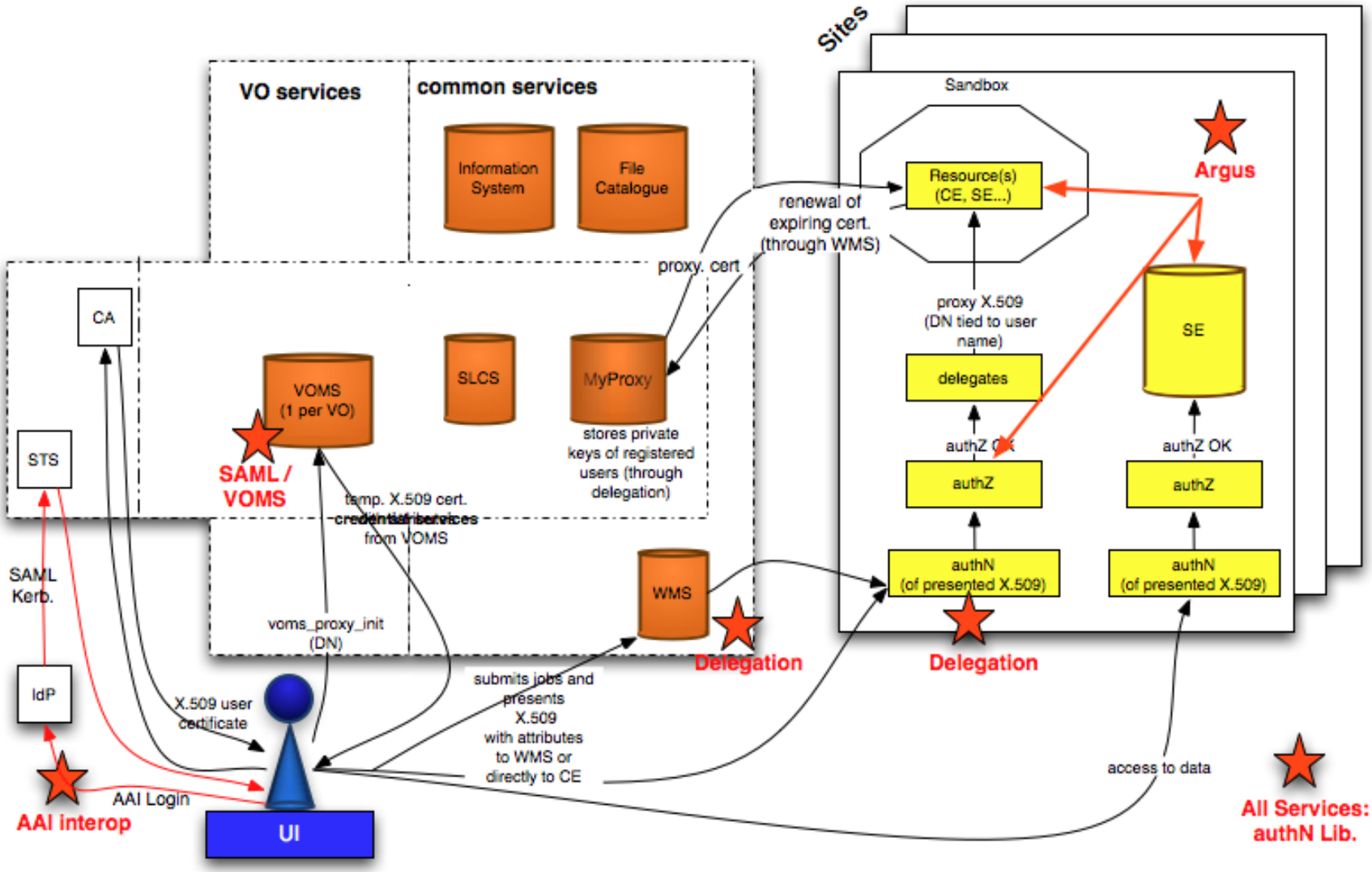


Common SAML profile

- **Common user attribute schema for AuthZ/AuthN.**
- Currently integrating UNICORE security with VOMS-SAML and Argus.
- UNICORE client fetches attributes from VOMS-SAML.
  - → Latest VOMS-SAML implements the profile.
- UNICORE services to fetch attributes for third parties from VOMS-SAML.
  - → VOMS-SAML to support third-party queries (EMI-2).
- UNICORE integrates with Argus.
  - → Support for extracting attributes from SAML assertion implemented in Argus.
  - → Argus SPL extended to express equality checks among XACML attributes.

`http://bit.ly/emi-vo-saml-profile`
`http://bit.ly/saml-authz-retrieval`

Common XACML profile

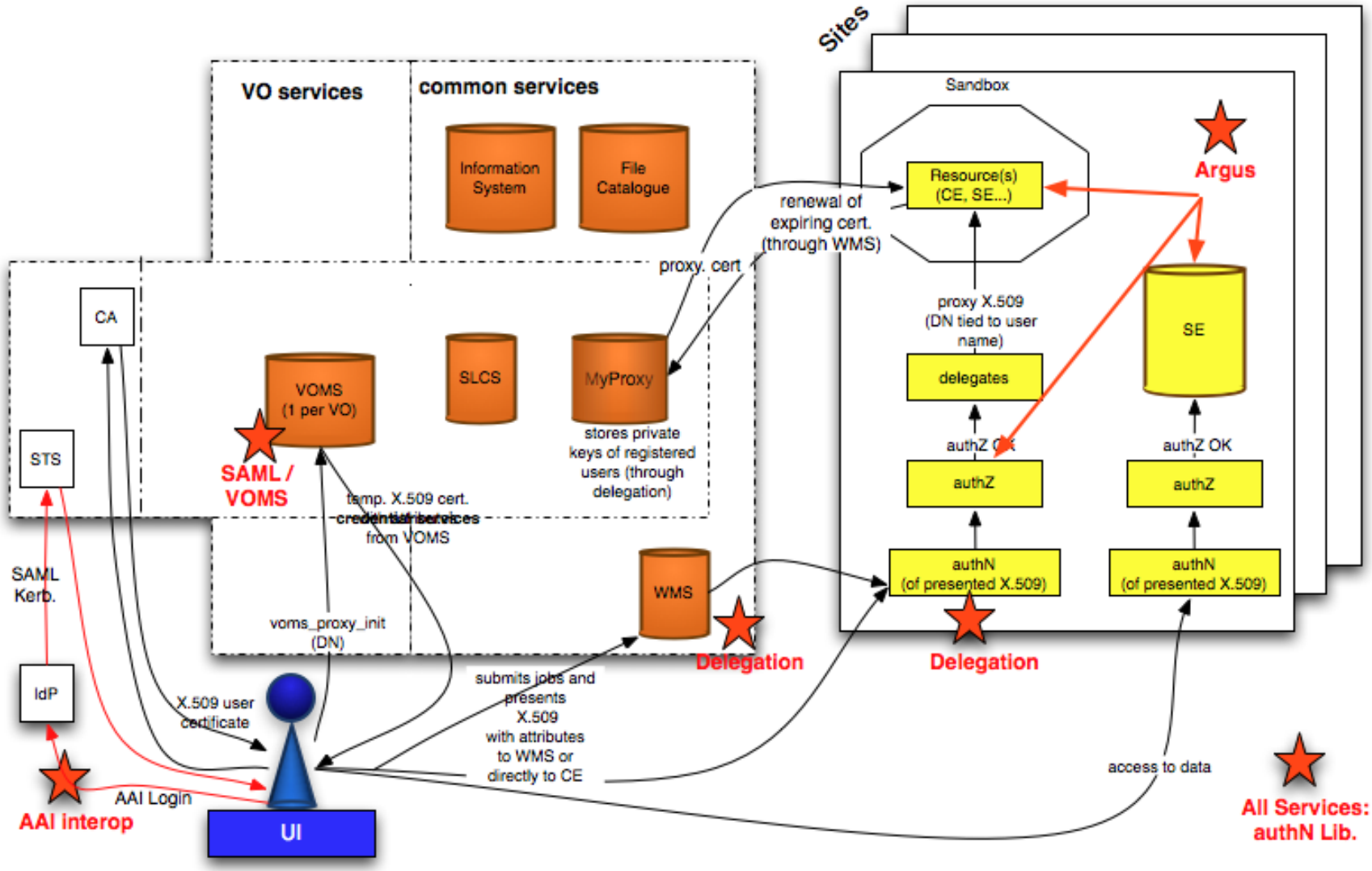


Common XACML profile

- Allows to write standard AuthZ schemes for services.
- Delivered: `http://bit.ly/common-xacml-profile`
- Adoption:
  - Argus PAP, PEP Server update (new profile and policies).
  - UNICORE* PDP callouts to Argus PAP.
  - ARC Security Handler callouts to Argus PEP Server.
  - **CREAM update/change existing profile. Discuss for EMI-3.**
  - **WMS - comes along with WMS integration with Argus (EMI-2).**

`https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML`

Common Authentication Libraries



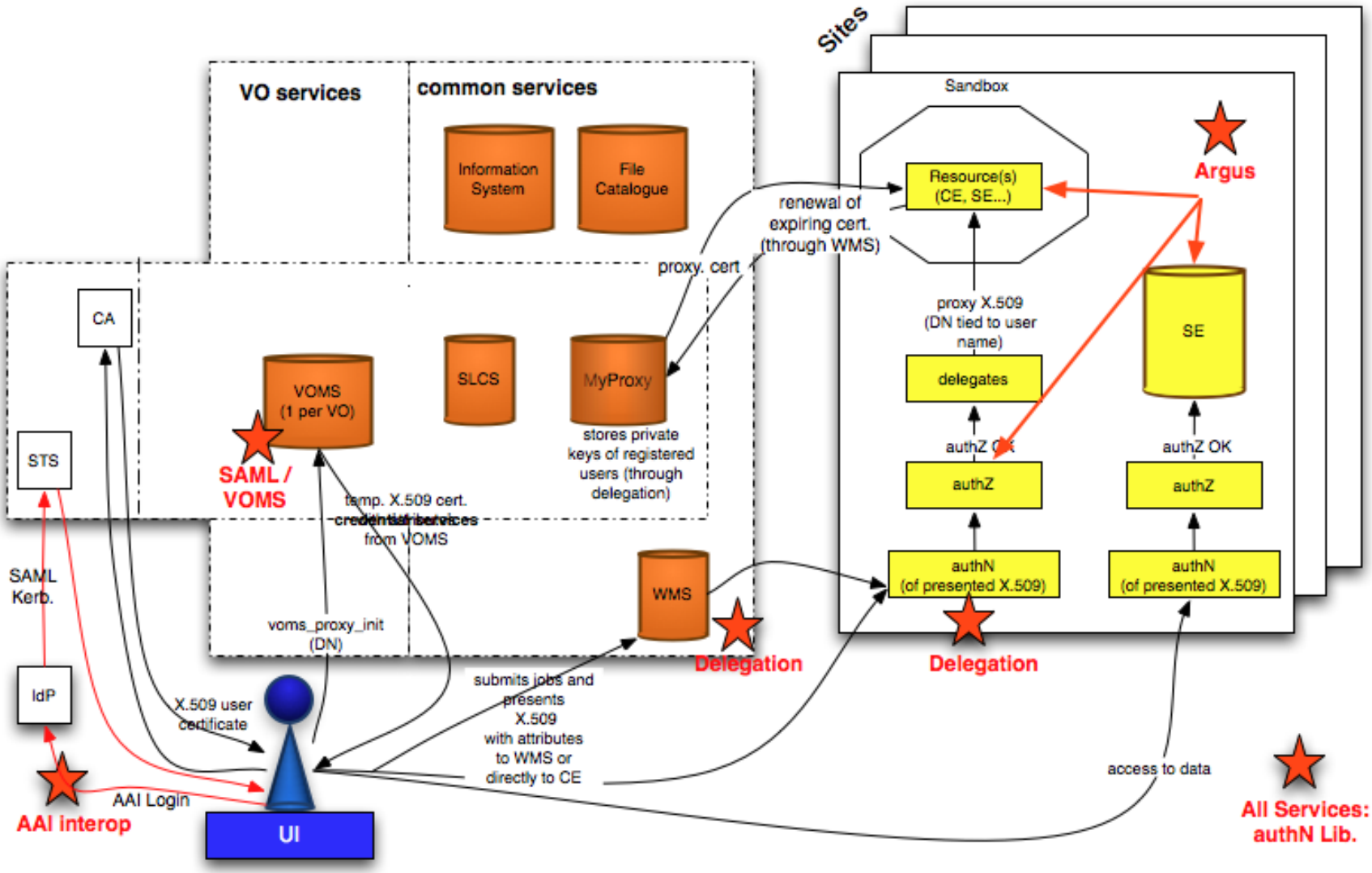
Common Authentication Libraries

Provide a uniform layer for AuthN decisions.

- C library :
  - Delivered. EMI-2
  - Sample client/server available.
- C++ :
  - Library delivered.
  - Still some details being worked out.
- Java :
  - Delivered.
  - Test coverage, Re-use of gLite Util-Java and VOMS tests.
  - Delivered with standards testing `http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html`

Common error messages. “Java” set proposed as the basis.
Libraries will be cross-tested.
Adoption by services in EMI-2.

Common Delegation Method



Common Delegation Method

- Participation: ARC and gLite, (compute, data and security)
  - Captured more Compute use-cases (gLite, ARC)
  - Identified areas where gLite and ARC have different usage.
  - Functional framework for delegation conformancy tests.
- No show-stoppers.
- Delegation agreement at:
  `https://discordia.desy.de:2880/paul/Delegation/`
- **Will proceed to form an OGF group.**

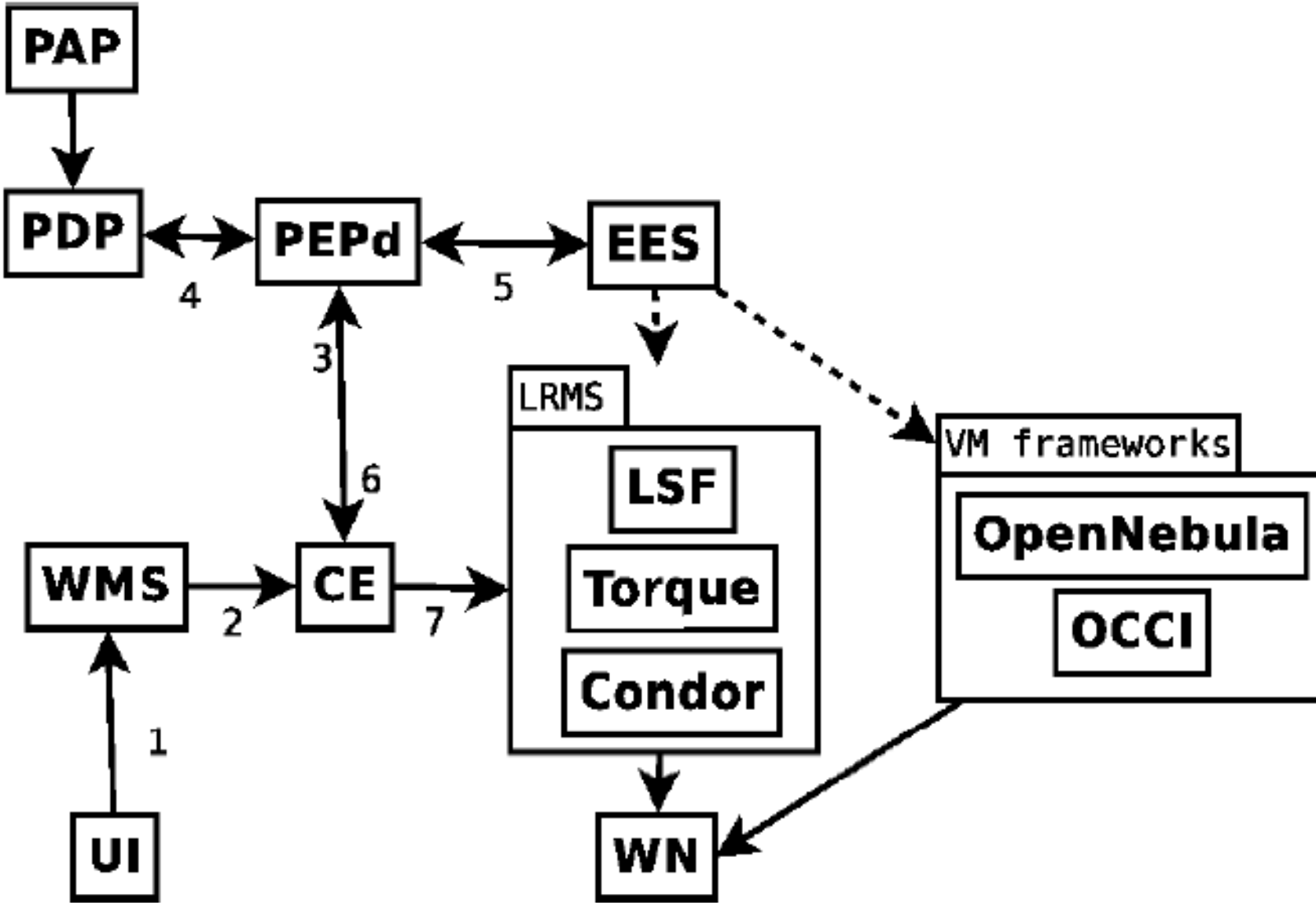
`https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi`

Argus EES

- "An obligation transformer used to ensure that an appropriate site-specific execution environment is procured based on the site-agnostic obligations and input attributes".
- A service that may co-exist with Argus to start VMs or send jobs to a Cloud*.
  - Argus-EES ready for EMI-2.
  - Tested with Argus. (PEPd)
  - OpenNebula will come as update for EMI-2
- No show-stoppers.

`http://www.eu-emi.eu/products/-/asset_publisher/z2MT/content/argus-ees`

Argus Execution Environment Service



Argus EES

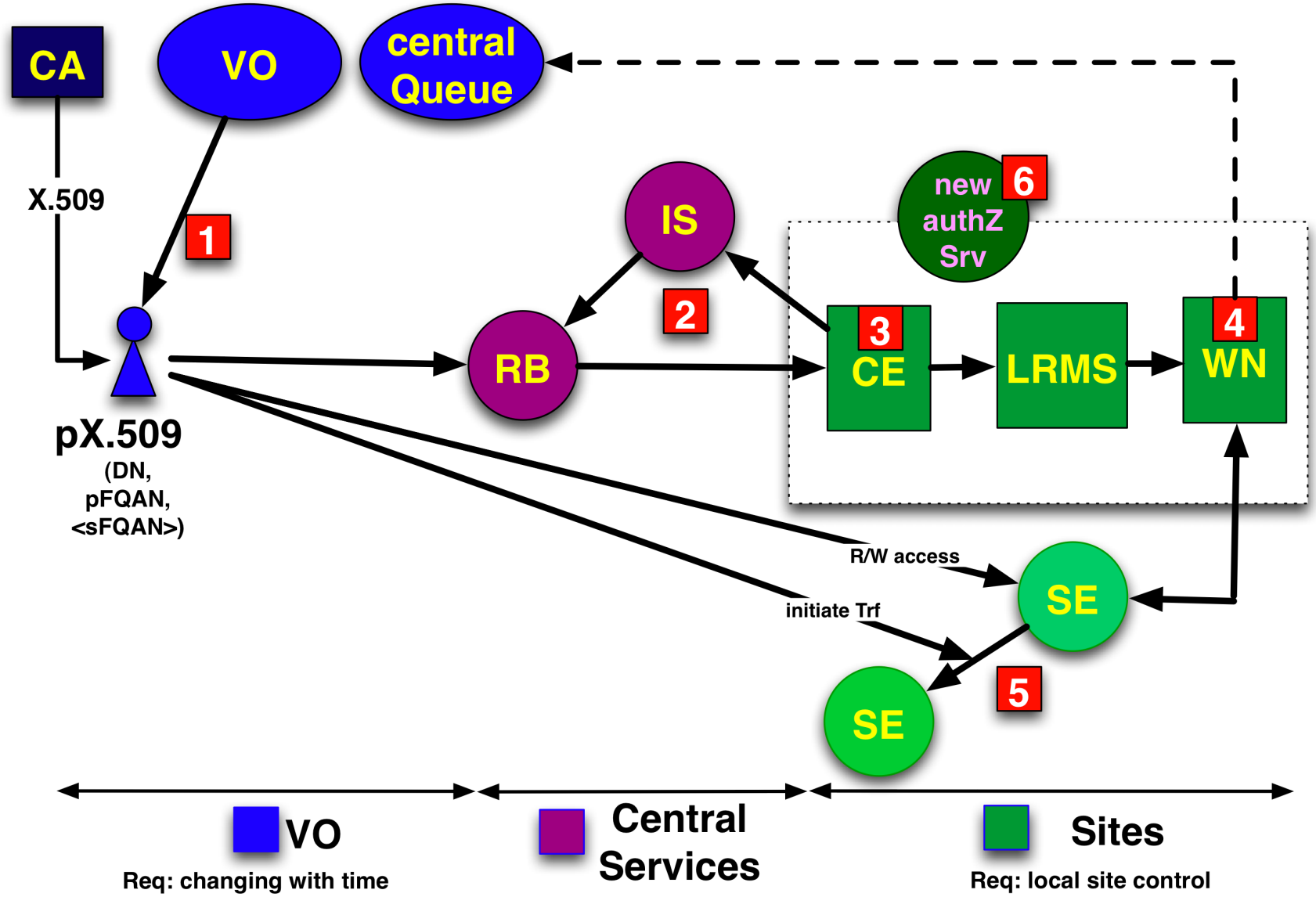
- "An obligation transformer used to ensure that an appropriate site-specific execution environment is procured based on the site-agnostic obligations and input attributes".
- A service that may co-exist with Argus to start VMs or send jobs to a Cloud*.
  - Argus-EES ready for EMI-2.
  - Tested with Argus. (PEPd)
  - OpenNebula will come as update for EMI-2
- No show-stoppers.

`http://www.eu-emi.eu/products/-/asset_publisher/z2MT/content/argus-ees`

Thank you!

EMI is partially funded by the European Commission under Grant Agreement RI-261611

Security Domains



EMI Security Pages

- First workshop (AAI). EGI Amsterdam 2010.
  https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI
- Common SAML profile
  https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SAML
- Common XACML profile
  https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML
- Common Authentication Libraries
  https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4SecurityCommonAuthNLib
- Common Delegation method
  https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi