Standards applicable to Security Area

KJRA1.1 - "Standard compliance KPI":

Name: Number of EMI service interfaces and libraries passing standard compliance tests

Description: The metric measures how many EMI service interfaces and libraries are successfully tested for standard compliance. Standard compliance is defined broadly and also includes compliance with EMI internal agreements.

How to measure: The number is taken by checking the available test reports generated during the quarter by the Product Teams.

These are the standards used by each "component" in the Security Area. Assume that each component is supposed to test that they comply with the noted standard. Used the attached diagram as a guide.

Argus

- XACML
- X.509

VOMS

- SAML
- X.509

UVOS

- SAML
- X.509

UNICORE XUUDB

- X.509

UNICORE Services Environment

and everything built on top of it: UNICORE/X, Registry

- SAML (attributes)
- X.509
- XACML

UNICORE Gateway

- X.509

glexec/LCAS/LCMAPS

- X.509

STS

- X.509
- SAML
- Kerberos
- WS-Trust

Authentication Libraries (all)

- X.509

Delegation

- X.509

Hydra

- X.509
- WSDL?

Pseudonymity

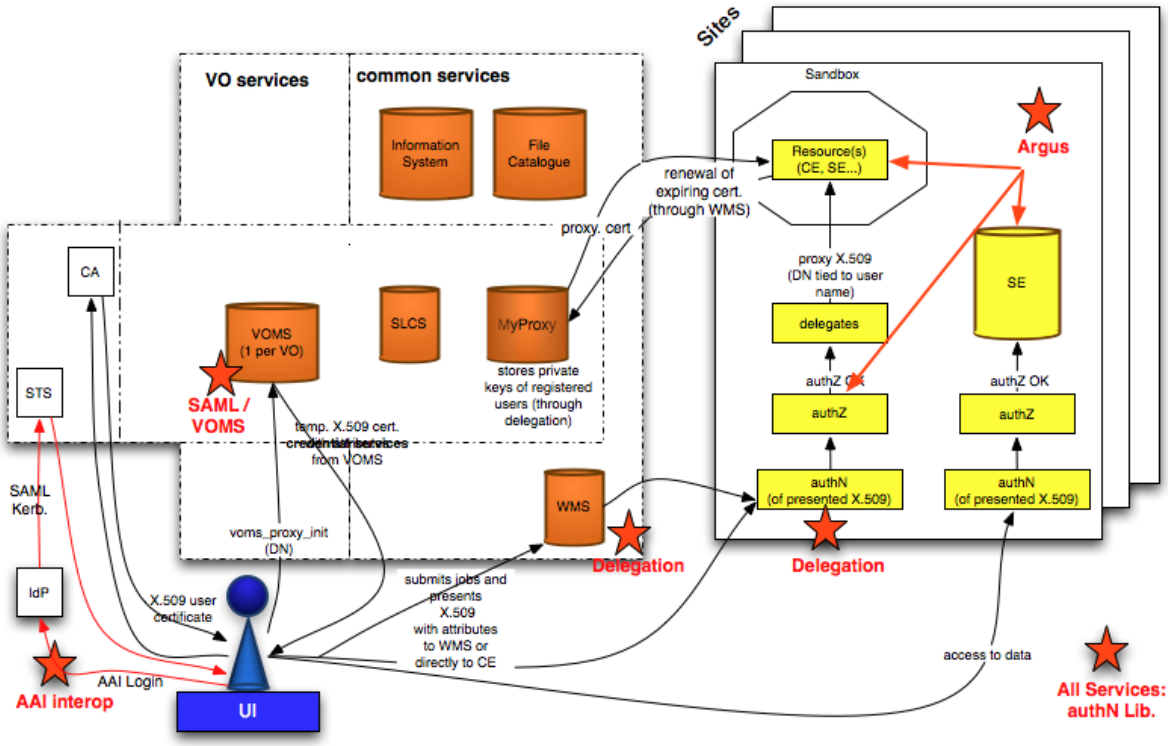
- X.509

ARC HED

- SSL/TLS/X.509
- VOMS (OGF GFD.182)
- XACML (partly)

-- JohnWhite - 11-Nov-2011

- emi_security_work_mod.png:



This topic: EMI > EmiJra1SecStandardsCompliance
Topic revision: r4 - 2011-11-11 - unknown