Security Token Service

for EMI-2

John White for EMI Security Area

Helsinki Insitute of Physics

Padova, October 18th, 2011

EMI Security and AAI

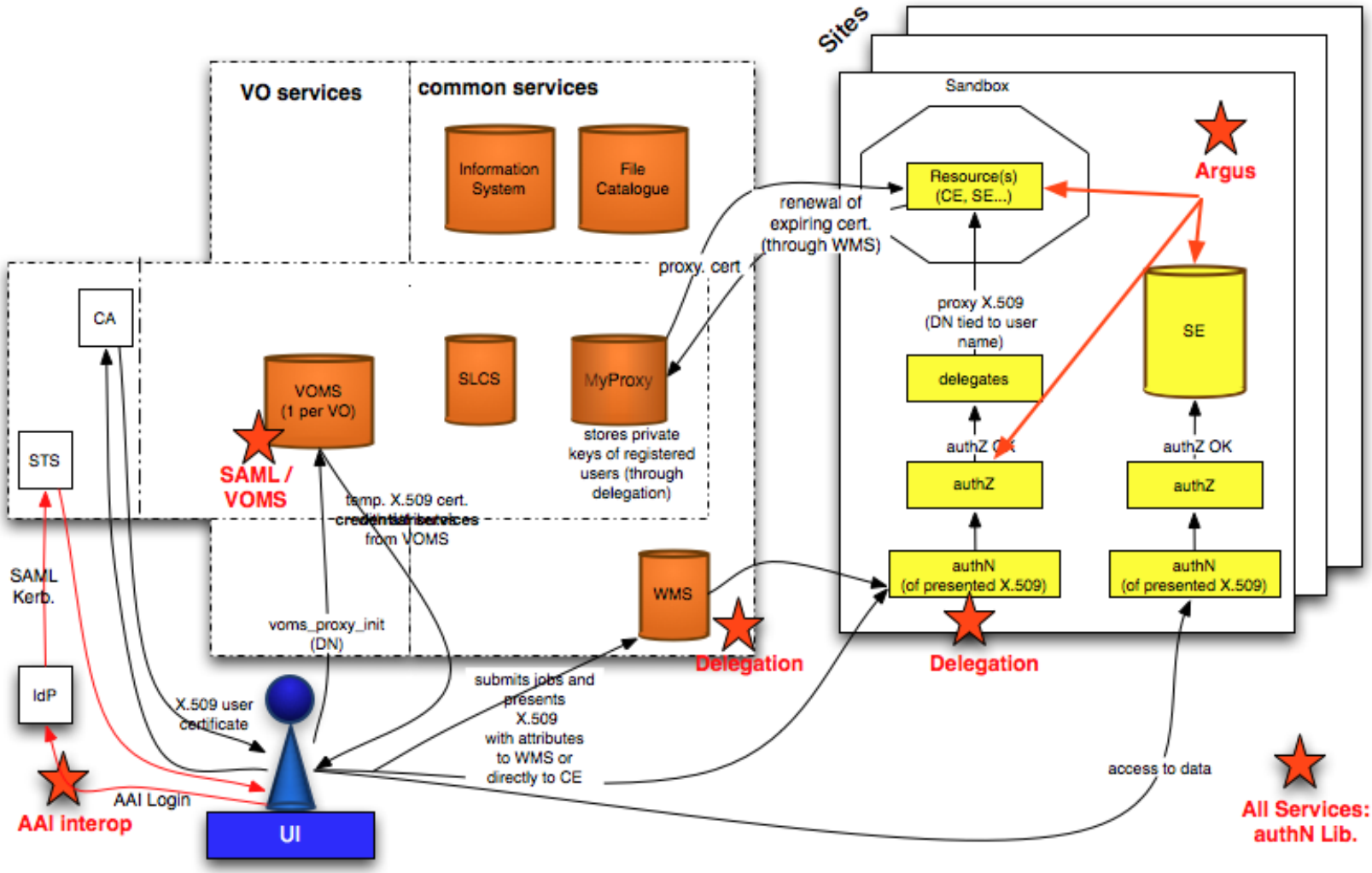
- Why STS?
- First workshop (AAI). EGI Amsterdam 2010. `https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI`
- 3 user communities, 5 ESFRI projects, 2 NGIs
- Questionnaire/answers:
  - **Grid users do not want to handle credentials.**
  - **Grid users want to obtain X.509 credentials and VOMS attributes from other credentials and vice-versa.**
  - Projects accept that access to the majority of Grid infrastructures require X.509 credentials in the medium term.
  - Projects recognize that both national and international federations are becoming more important.
  - User identities and actions on a Grid should be protected (anonymized).
- Set of Use-cases.

AAI Use-Cases

X.509 issuance based on AAI	"Solved" (needs improvement)
AAI-enabled portals	Solutions exist, SAML delegation
AAI-enabled Grid portals	Priority: low
Security Token Service (**STS**)	Priority: high
Use of AAI attributes in the Grid	Interesting, accounting?
VO registration tied to AAI account	Priority: low

- STS solves:
  - “A Grid service obtains a user-request from another security domain and based on the token obtains a X.509 certificate with which it communicates to other grid services”
  - “A User obtains a X.509 certificate based on a security token from another domain”

EMI Security

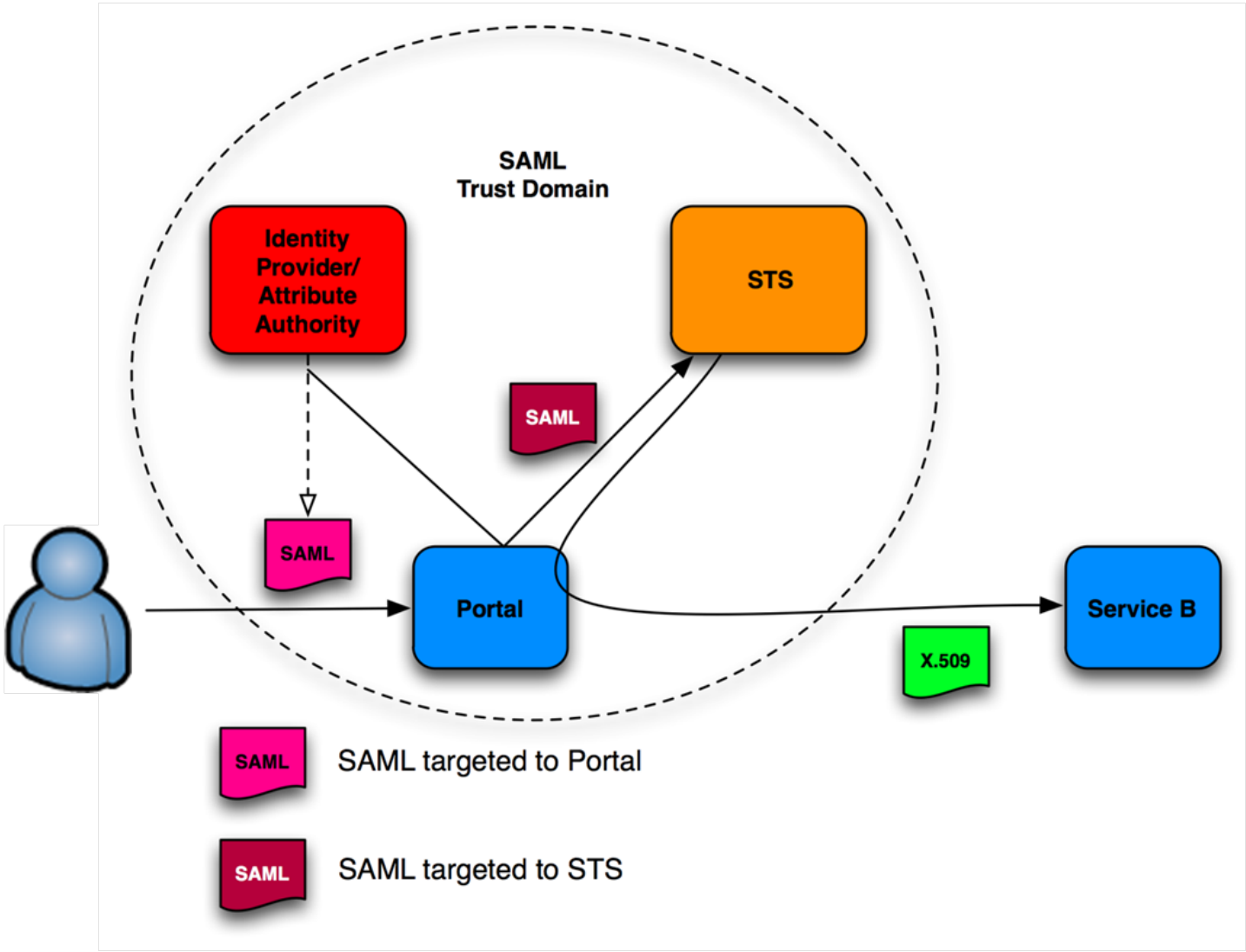


STS Overview

- STS "authenticates and authorizes" users based on security tokens. [1]
- ISSUE operation transforms an incoming security token into another security token.
- 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.
  - Incoming formats: X.509, X.509 Proxy, SAML, Kerberos
  - Outgoing formats: X.509, using external online CA
    X.509 Proxy, exploiting VOMS
    SAML
    Kerberos

[1] 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

STS Overview



STS Timetable

- First version of STS: Q2 2012
  - OpenSAML3/Shib3* Q4 2011
  - UH/HIP 0.6 FTE
  - SWITCH 0.3 FTE*
- Deployment strategy
  - Identify the most likely deployment situation(s).
  - VO, national, institutional, site, service.
  - Basis on Security Tokens attractive.
- Please see the more technical talk and
- Design document at:
  `https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI`

Thank you!

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

EMI Security Work