

# Security Token Service

John White for EMI Security Area

Helsinki Institute of Physics

RAL, November 3rd, 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

AAI-enabled portals

AAI-enabled Grid portals

**Security Token Service (STS)**

Use of AAI attributes in the Grid

VO registration tied to AAI account

"Solved" (needs improvement)

Solutions exist, SAML delegation

Priority: low

Priority: high

Interesting, accounting?

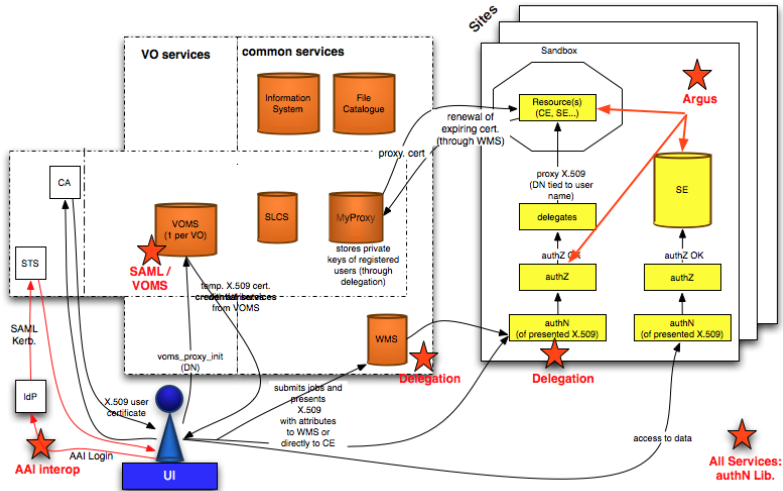
Priority: low

▶ 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



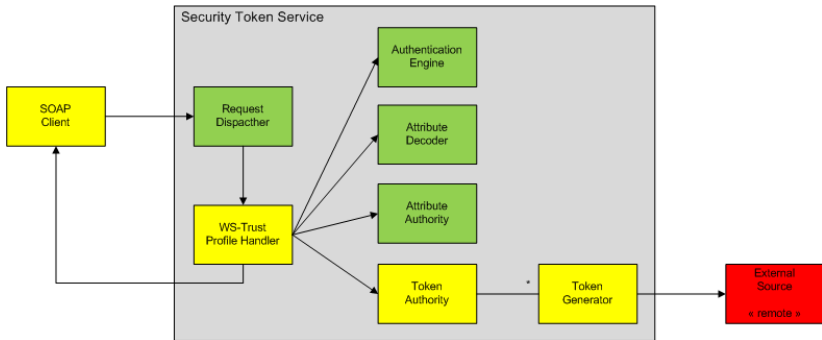
# STS Overview

- ▶ STS “authenticates and authorizes” users based on security tokens. <sup>1</sup>
- ▶ 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 → 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

---

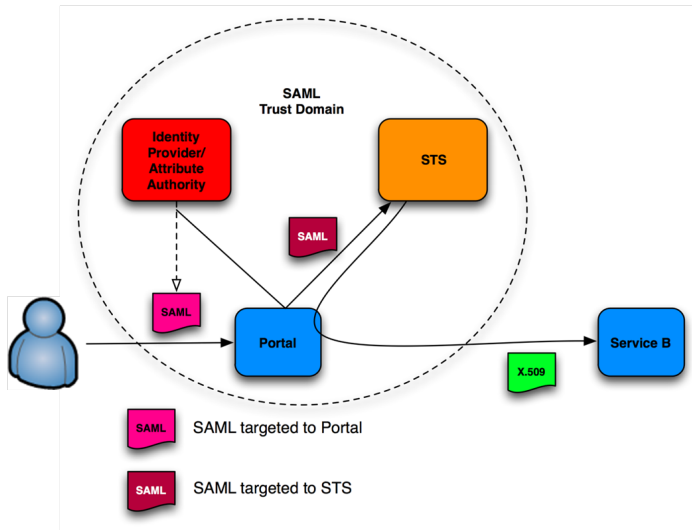
<sup>1</sup>Security token: a collection of statements (or claims) about a user or resource, in this case: X.509 certificate, SAML assertion, Kerberos ticket, Username/Password

# STS Overview



- ▶ Components in green boxes provided by Shib3
- ▶ Components in yellow boxes (to be) implemented.

# STS Overview



# Client Toolkit

## Client toolkit will be a Java-library, helping in:

- ▶ Generating the security tokens
  - ▶ From the file system: X.509 certificate, proxy
  - ▶ From an IDP: SAML assertion (ECP profile)
  - ▶ From a KDC: Kerberos ticket
- ▶ Generating the request messages
- ▶ Communicating the messages with STS
- ▶ Extracting the response messages
  - ▶ Storage of the security tokens
- ▶ Toolkit to be utilized in “a” client UI
- ▶ Integrated with services (e.g. portals)





# STS Timetable

- ▶ First version of STS: Q2 2012
  - ▶ OpenSAML3/Shib3\* Q4 2011
- ▶ 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
- ▶ Design document at:
- ▶ <https://twiki.cern.ch/twiki/bin/view/EMI/EmiJralT4AAI>

# STS Early Adopters

- ▶ Following success of Argus: early adopters.
  - ▶ Special mailing list set up for technical help
  - ▶ Mostly by bypassing bureaucracy
- ▶ Help to integrate STS to user portals possible
- ▶ Speed up acceptance and bug-finding





# Thank you!

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



# EMI Security Work

