Security Token Service (STS)
Simplified Credential Management

Henri Mikkonen / UH.HIP

4th EMI All-Hands Meeting

8.-10.5.2012

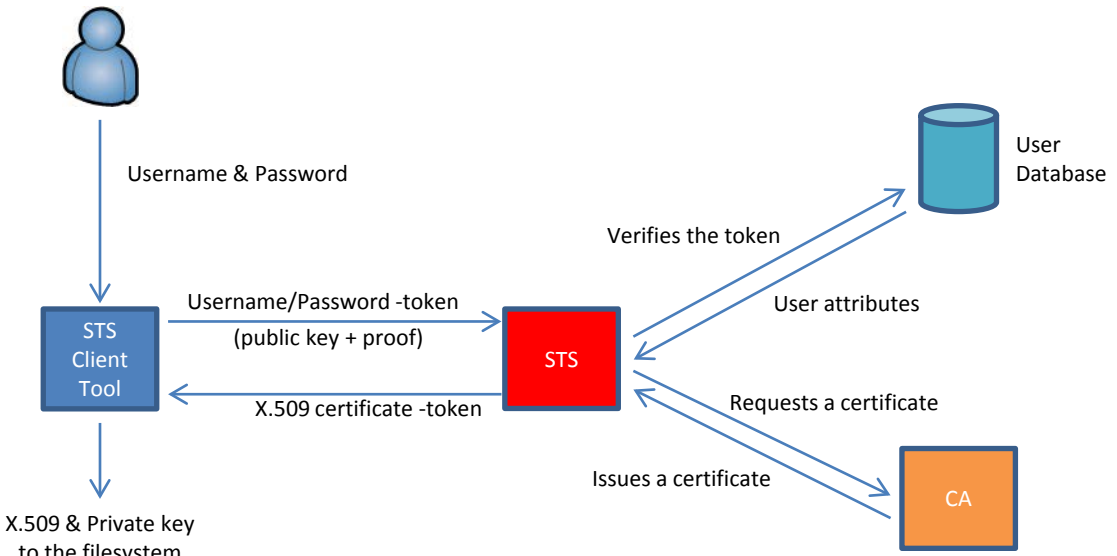
Hamburg, Germany

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

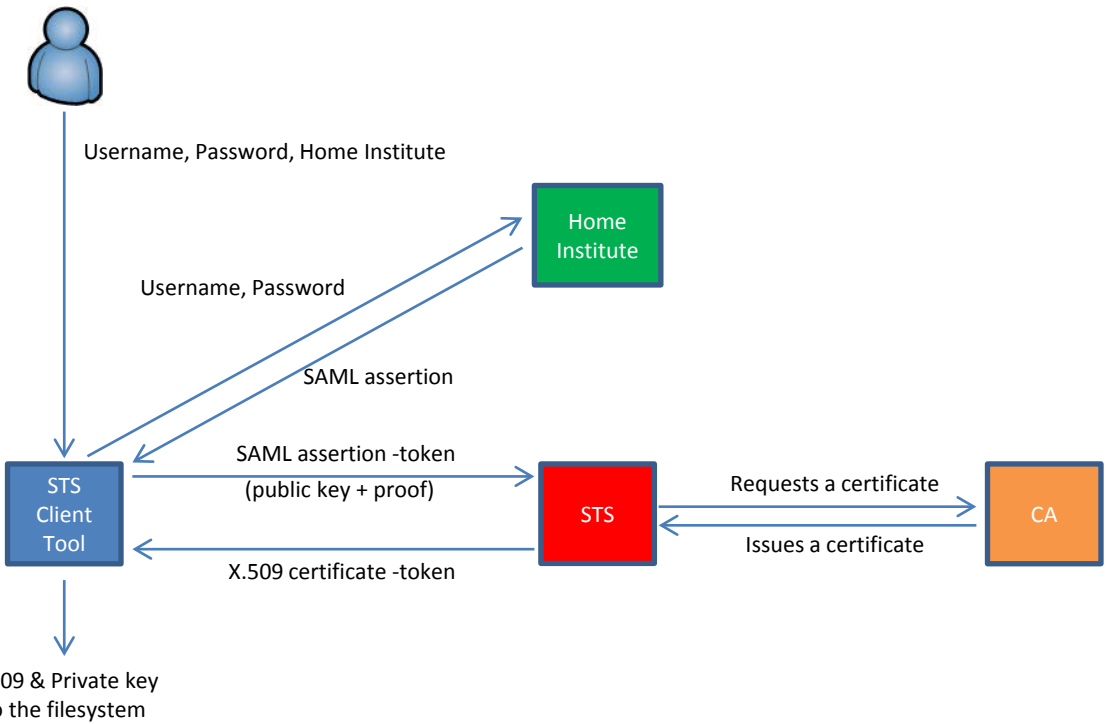
Content

- (Some) STS Use Cases
- Server-side Architecture
- Implementation Schedule

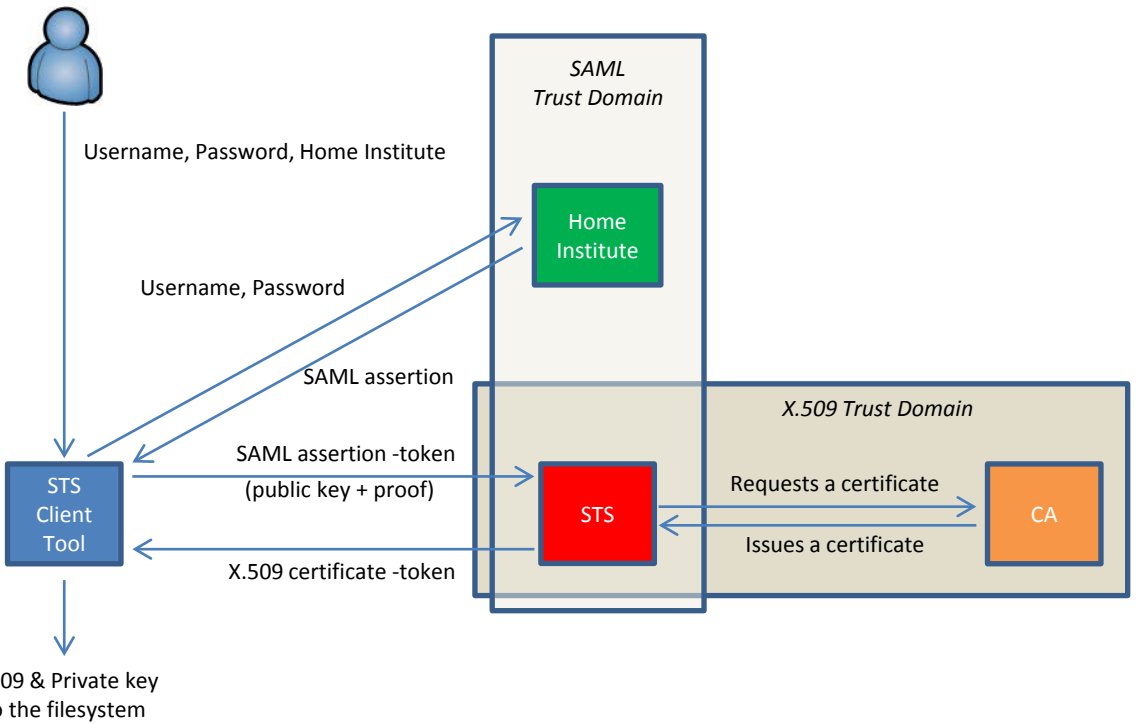
Username/Password to X.509



SAML assertion to X.509

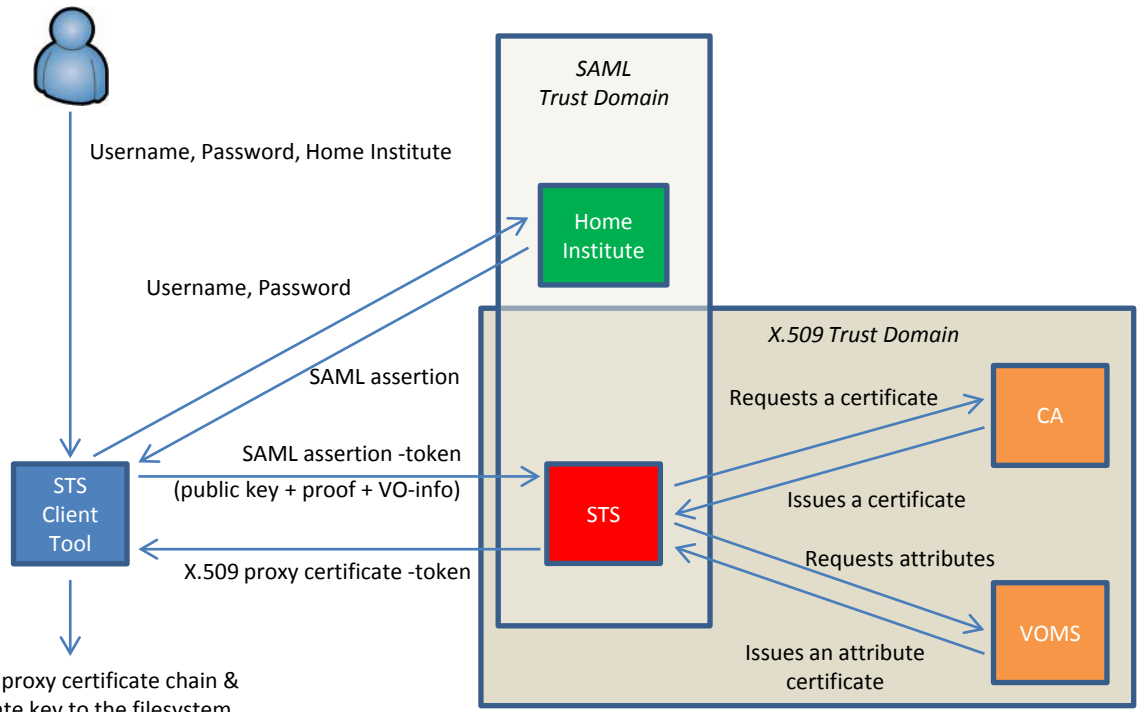


SAML assertion to X.509

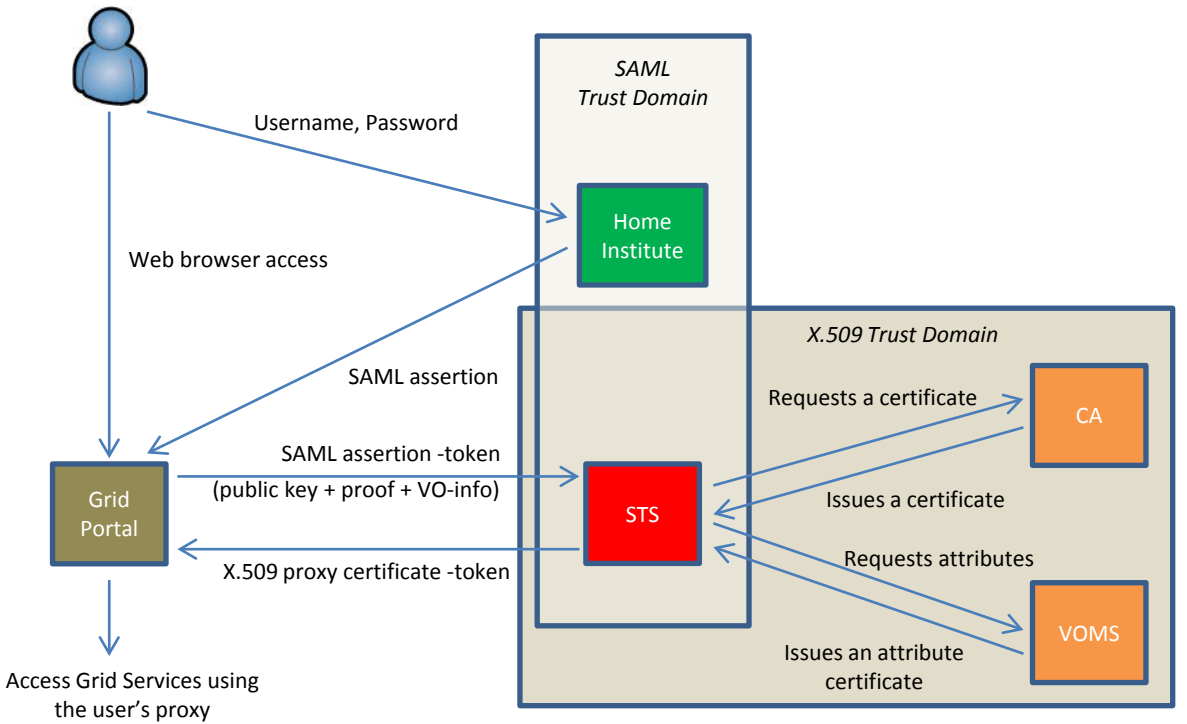


EMI INFSO-RI-261611

SAML assertion to X.509 proxy



SAML assertion to X.509 proxy



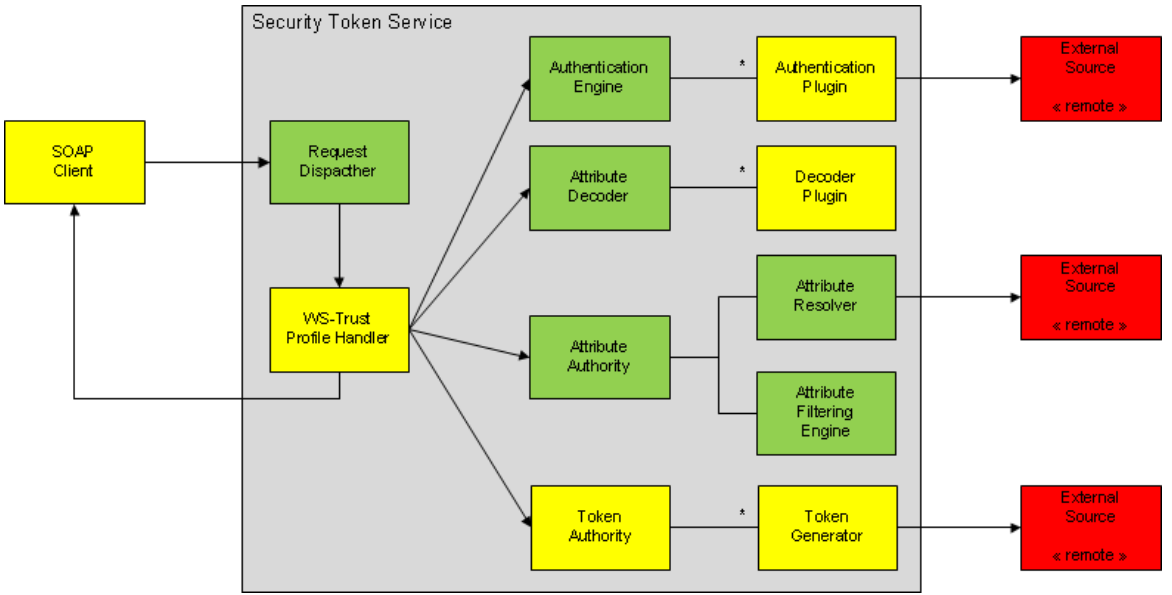
EMI INFSO-RI-261611

Use Cases Summary

- STS transforms an existing security token into another security token
  - Supported incoming formats: X.509, X.509 proxy, Username/Password, SAML, Kerberos
  - Supported outgoing formats: X.509, X.509 proxy, SAML
- STS is a SOAP-based Web Service
  - Any party capable of producing specified request messages and understanding response messages can act as a client
    - *Command-line clients, Web portals, Grid resources, …*

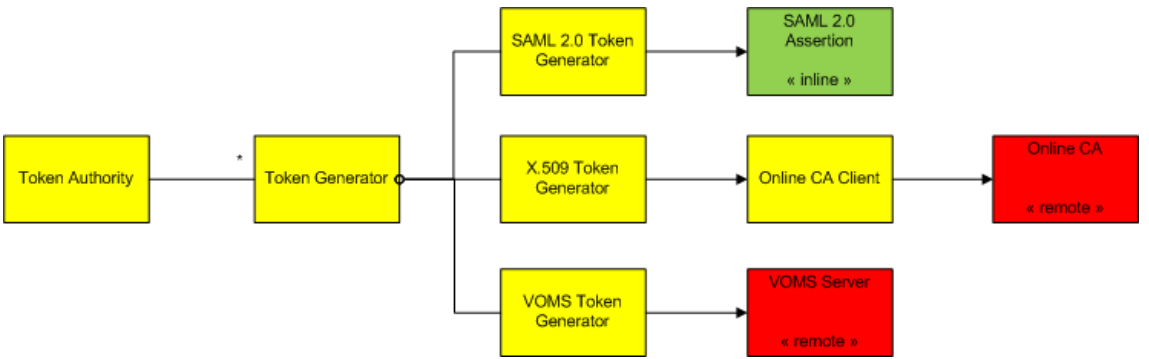
EMI INFSO-RI-261611

Server-side Architecture (1/2)



OpenSAML3 is used for producing and consuming the protocol messages
The *green* components are / will be provided by Shibboleth 3 Identity Provider
The *yellow* components are currently being implemented in the STS project

Server-side Architecture (2/2)



- Three outgoing token formats promised in the EMI plans
  - SAML 2.0 assertion generation is provided “internally” by Shib IdP
  - The CMP protocol is initially supported for the Online CA connection
  - The VOMS token generation is very close to *voms-proxy-init* functionality

State of the Implementation

- OpenSAML3 and Shib IdP v3 starts to have most of the required functionality implemented
  - Their official schedule to be verified
- X.509 token generator using the CMP protocol is ready
  - Communication with EJBCA is tested to be working
  - Others (e.g. MyProxy) may be supported

Schedule

- Finish Username/Password to X.509 first
  - Client-side implementation coming from the UNICORE people
  - Planned to be ready by the end of June 2012
- The other promised token formats to follow
  - Order for the incoming token formats:
    - *X.509 certificate, VOMS proxy, SAML assertion, Kerberos*
  - And for the outgoing:
    - *VOMS proxy, SAML assertion*

EMI INFSO-RI-261611

Further Reading

- See STS Workshop slides from yesterday
  - Terminology
  - Functionality
  - Client Requirements
- STS Wiki Page
  - https://forge.switch.ch/redmine/projects/sts/wiki

EMI INFSO-RI-261611

Thank you! Questions?

Henri Mikkonen
<henri.mikkonen@cern.ch>

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