EMI AAI Strategy & Plans

John White / Helsinki Institute of Physics

Federated Identity Systems for Scientific Collaborations Workshop

09.06.2011, CERN, Geneva, Switzerland

Content

- Background
- AAI WG use cases
- Security Token Service (STS)
- Current work plan

Background

- AAI workshop held at EGI TF (Sept. 2010) [1]
- Questionnaires for projects crossing national boundaries and National Grid Initiatives (NGIs)
  - 3 User communities
    - Biomed, Earth Sciences, HEP
  - 5 ESFRI projects
    - CLARIN, Lifewatch, ELIXIR, EuroFEL, ILL
  - 2 NGIs
    - Italy, U.K.

Results for the questionnaire [2]

- Grid users do not want to handle credentials themselves
- Grid users would like to obtain X.509 credentials and VOMS attributes from other credentials and vice-versa
- Projects would like to use federated identities
- Projects recognize that both national and international identity federations will become more important
- User identities and actions on a Grid should be protected (anonymized)
- Projects realize that access to the majority of Grid infrastructures requires and will require in the future X.509 credentials

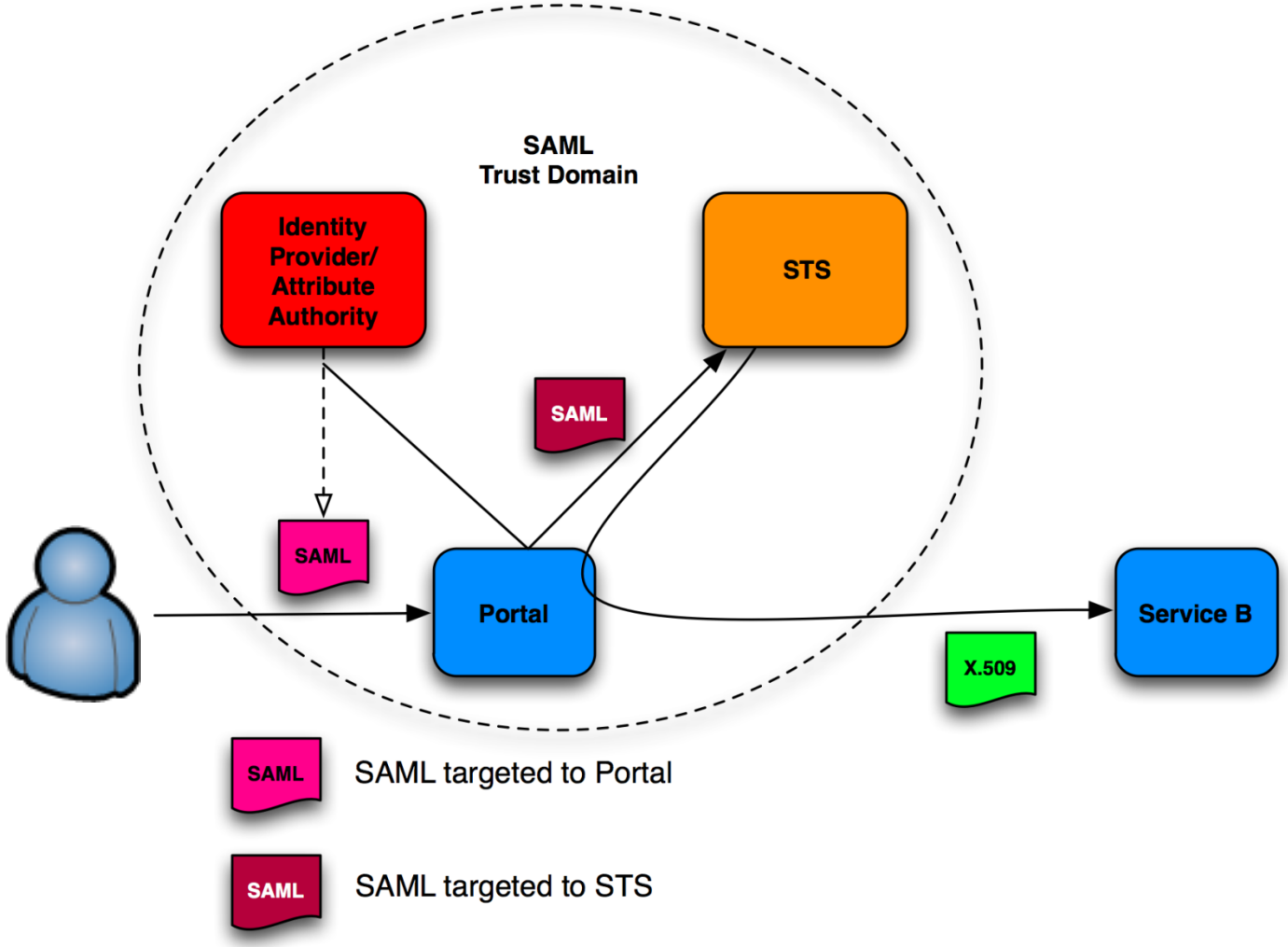
AAI WG use cases [2]

Use-case	Description	Status
1	X.509 issuance based on AAI (another security domain)	„Solved“ (but needs improvement!)
2	AAI-enabled portals to Grid infrastructures	Solutions exist SAML delegation new
3	AAI-enabled Grid information portals	Low priority
4	Security Token Service (STS)	New, general purpose service, high priority
5	Use of AAI attributes in Grid	Interesting, potentially very important
6	VO registration using AAI (identity vetting)	Low priority

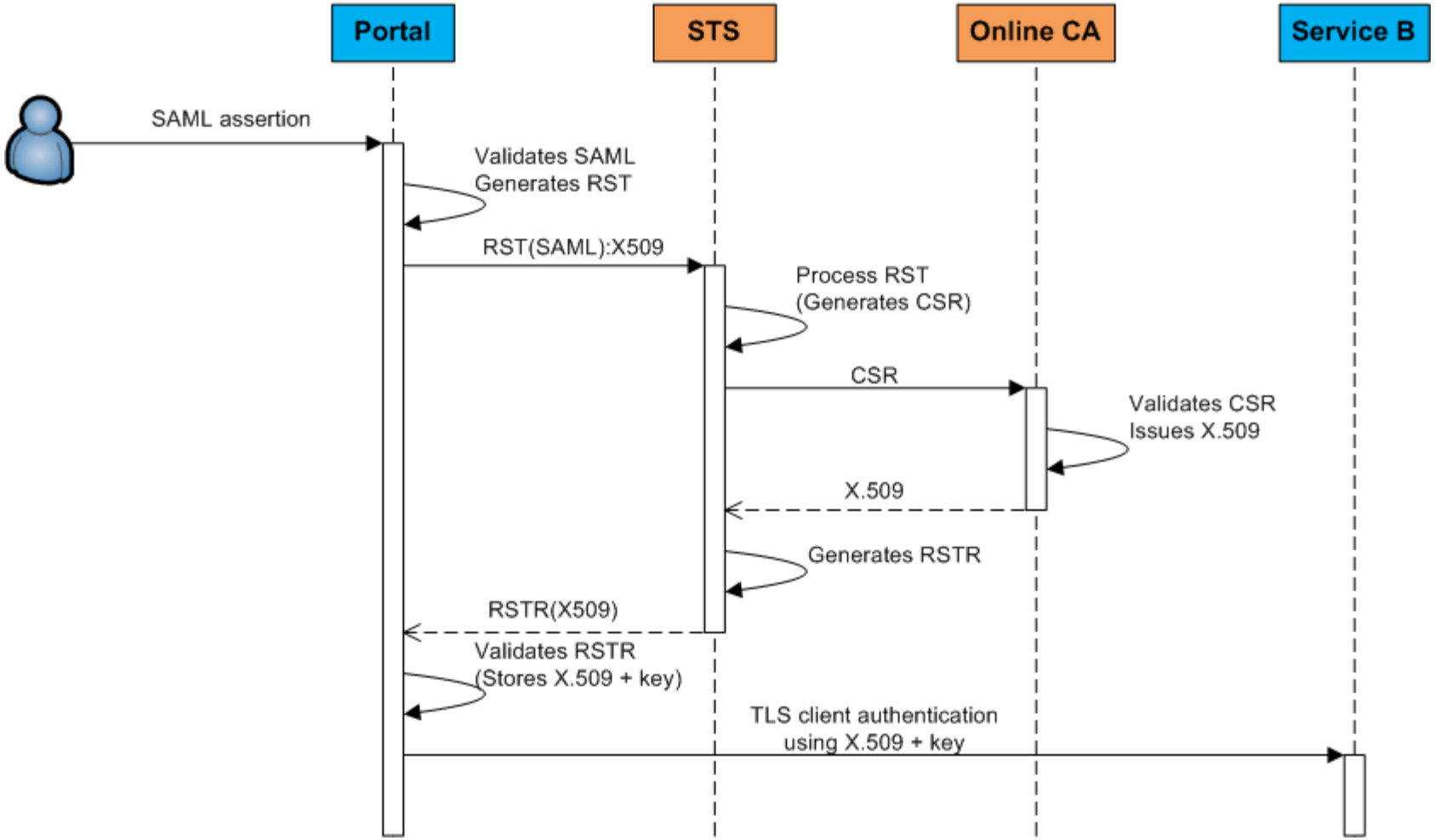
STS functionality overview

- Security Token Service (STS) is defined in the WS-Trust specification [3]
  - Authenticates and “authorizes” users based on security tokens
  - Transforms the security token into another security token
  - Aggregates required information from external sources
  - Establishes a trust relationship between different application domains

STS Example Use Case (1/2)



STS Example Use Case (2/2)



(Some) issues in the previous sequence

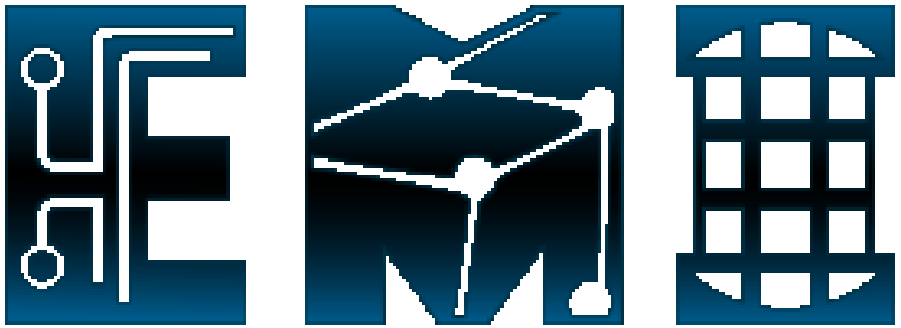
- SAML token must be targeted for both Portal and STS
- Who generates the key pair and stores the private key?
  - Depending on the online CA, key pair can be theoretically generated by any party
- WS-Trust [3] profile definitions
- How about if the STS is accessed directly via a (non-browser) client tool?

Current work plan

- Continue the WS-Trust interoperability profile [4] effort started in EGEE-III
- Define the other profiles missing in the sequence
  - E.g. for SAML, the building blocks include SAML delegation and ECP profile
- STS service- and client-side implementations
  - Service implementation is based on the upcoming Shibboleth Identity Provider v3

References

- [1] EGI TF 2010: AAI needs of the DCIs
  - https://www.egi.eu/indico/sessionDisplay.py?sessionId=11&confId=48#20100914
- [2] EMI AAI Working Group
  - https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI
- [3] OASIS Standard: WS-Trust 1.3
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512
- [4] Chad La Joie / SWITCH: WS-Trust 1.3 Interoperability profile
  - http://www.switch.ch/grid/support/documents/



Thank you!

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