AAI & STS Update

Henri Mikkonen / HIP

2nd EMI All-Hands Meeting

30.5.2011, Lund, Sweden

Content

- AAI use cases
- Introduction to WS-Trust
- WS-Trust profiles
- Security Token Service (STS)
- Next steps

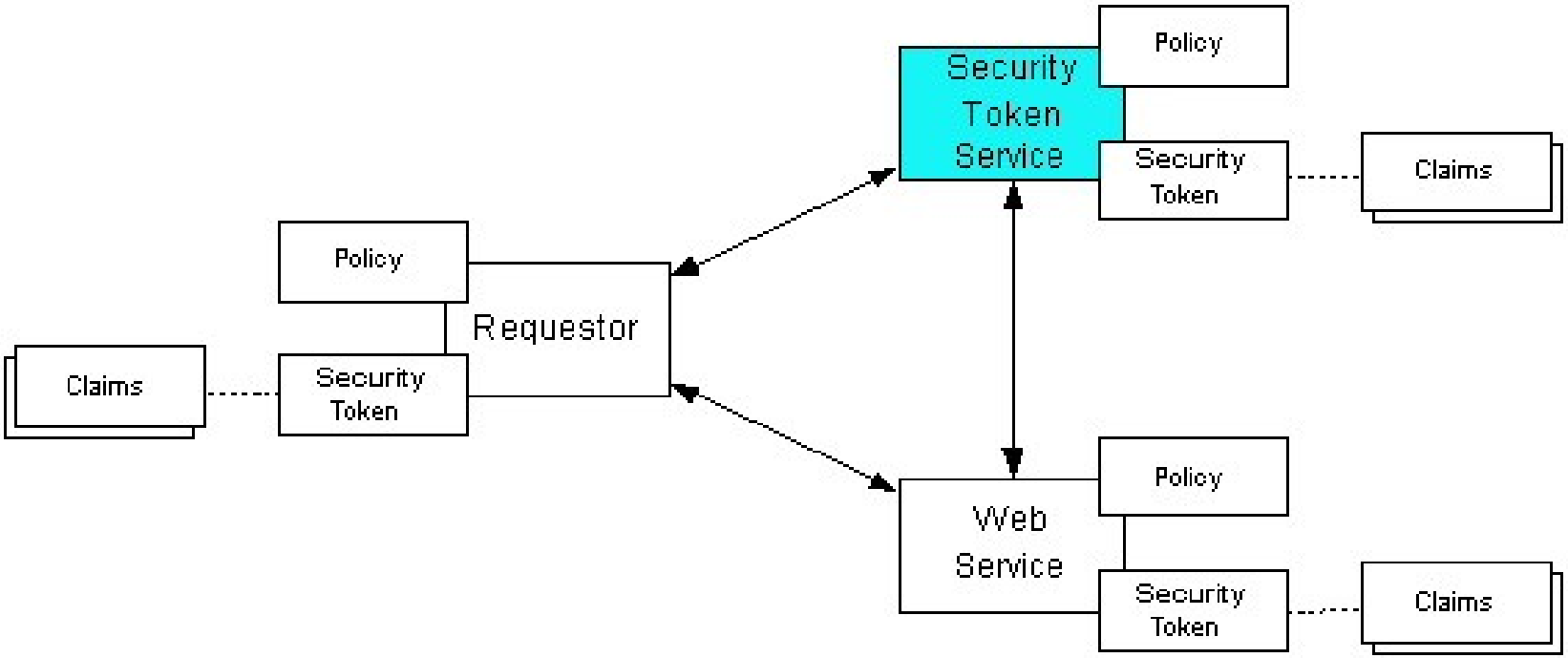
AAI use cases [1]

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 conversion	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

WS-Trust specification [2]

- Builds on WS-Security specification
  - Methods for issuing, renewing, validating, and canceling security tokens
  - Trust relationships brokering
- Security token: a collection of statements (claims) about a user or resource
  - X.509 certificate, SAML assertion, Kerberos ticket, Username/Password, …
- Security Token Service (STS): a service used to issue, renew, validate and cancel tokens

Web Services Trust Model [2]



WS-Trust schema overview

- RequestSecurityToken (RST) and RequestSecurityTokenResponse (RSTR)

```
<wst:RequestSecurityToken Context="..." Any="...">
    <wst:TokenType>...</wst:TokenType>
    <wst:RequestType>...</wst:RequestType>
    <wst:SecondaryParameters>...</wst:SecondaryParameters>
    <Any>...</Any>
</wst:RequestSecurityToken>
```

```
<wst:RequestSecurityTokenResponse Context="..." Any="...">
    <wst:TokenType>...</wst:TokenType>
    <wst:RequestedSecurityToken>...</wst:RequestedSecurityToken>
    <Any>...</Any>
</wst:RequestSecurityTokenResponse>
```

WS-Trust profiles [3]

- The specification provides an open content model for messages
  - Provides maximal extensibility, but theoretically infinite number of messages can be compliant
  - Profiles need to be defined for achieving interoperability
- This effort was already started by Chad in 2008 (EGEE-III)
  - WS-Trust interoperability profile
  - Token-specific profiles (X.509, SAML, Username)

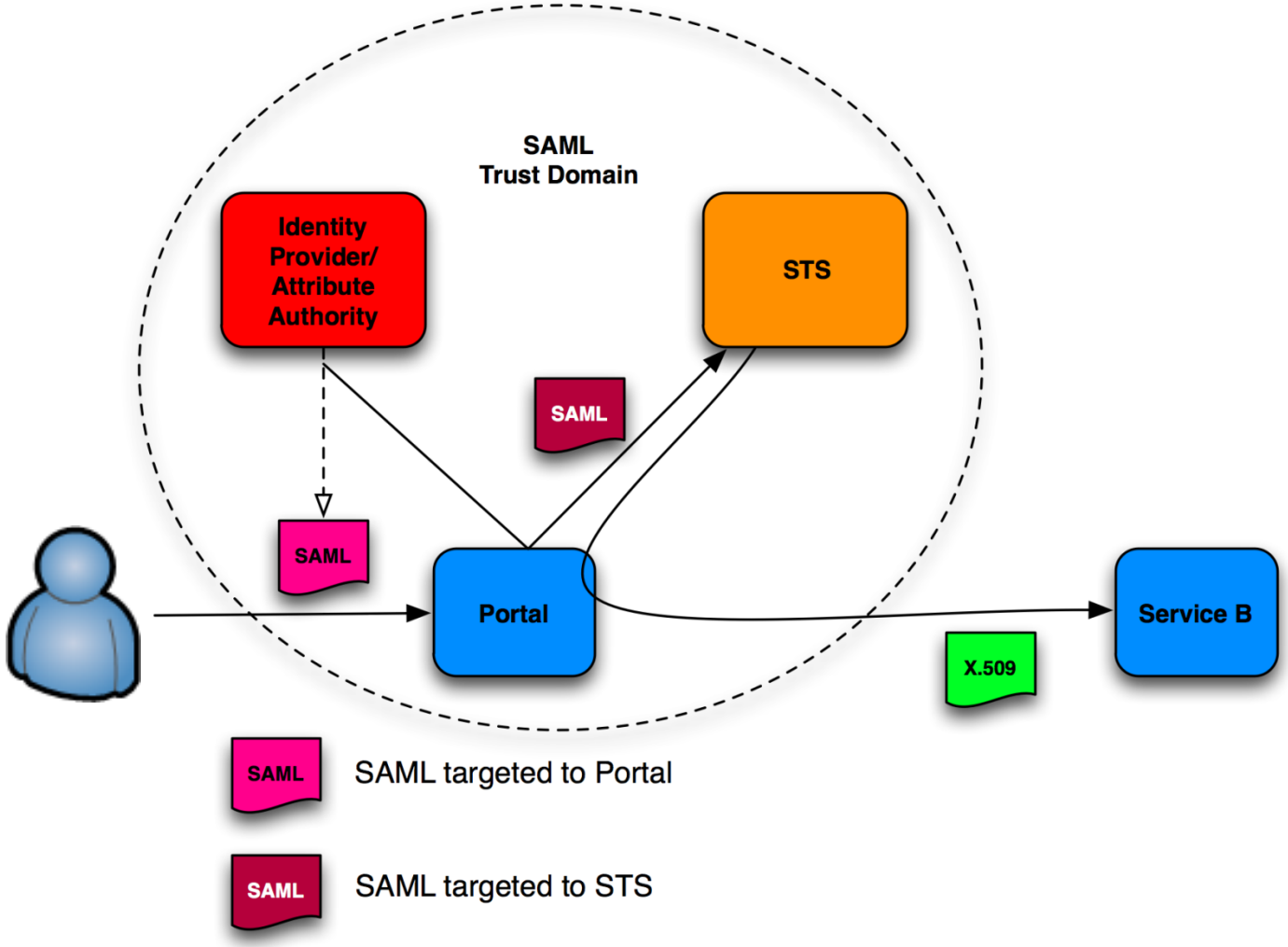
WS-Trust Interoperability profile

- Base protocol requirements
  - SOAP-binding, common message format requirements and processing rules
- Operation-specific requirements
- Also, profiles for
  - XML-Signature
  - XML-Encryption
  - Proof of key possession
  - Message security (integrity / confidentiality)

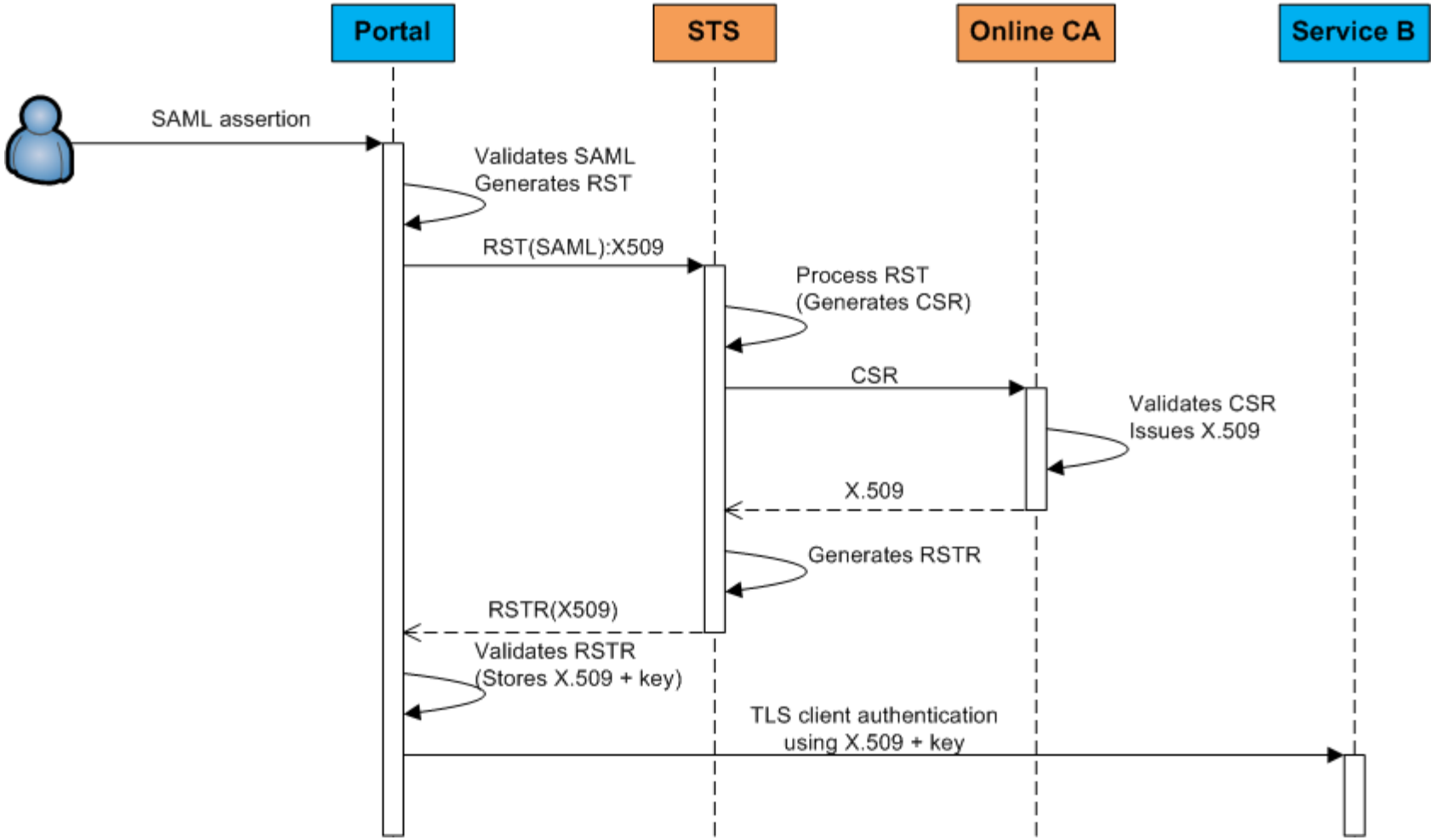
STS functionality overview

- 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 to the previous sequence

- SAML token must be targeted to both Service A and STS
  - By default the SAML assertions are targeted to one service provider
- Who generates the key pair and stores the private key?
  - Depending on the online CA, key pair can be theoretically generated by any party
- How about if the STS is accessed via a (non-browser) client tool?

Next steps

- Revise the WS-Trust interoperability profiles
  - Kerberos is missing from the existing profiles, but is mentioned in the EMI plans
- Define the profiles missing from the whole sequence (e.g. the previous slide)
  - E.g. for SAML, the building blocks include SAML delegation and ECP profile
- STS service- and client-side implementations

(Current) STS implementation plan (1/2)

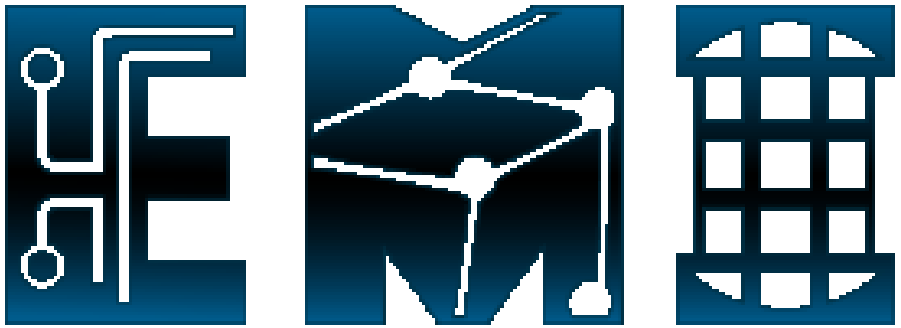
- Implementation is based on the upcoming Shibboleth IDP & OpenWS/SAML v3 (Shib3)
  - They provide most building blocks, widely used and well supported
    - pluggable authentication engine, attribute authority
- Currently Shib3 is under development and we are waiting for them to progress
  - Stable APIs & full functionality expected to September 2011, first release 2012Q1

(Current) STS implementation plan (2/2)

- What will be implemented by us:
  - WS-Trust profile handler
    - Orchestrates the process (vs. SAML2 profile handlers)
    - At first, only ISSUE operation will be supported
  - Authentication support for the incoming tokens
    - Plug-ins to the authentication engine
  - Token Authority for the outgoing tokens
    - Pluggable token resolvers (X.509, Proxies, SAML)
- First version scheduled to 2012Q2

References

- [1] EMI AAI Working Group
  - https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4AAI
- [2] OASIS Standard: WS-Trust 1.3
  - http://docs.oasis-open.org/ws-sx/ws-trust/200512
- [3] 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