Security Token Service
Transforming the Existing User Credentials for the Grid

Henri Mikkonen
Helsinki Institute of Physics

ISGC 2012, 26.2.-2.3.2012
Academia Sinica, Taipei
Content

• Background
  – Requirements from the DCIs
  – EMI AAI Use Cases

• Security Token Service (STS)
  – Terminology
  – Functionality

• (Some) STS Use Cases
Requirements from the DCIs

- **AAI needs of the DCIs** — workshop held at the EGI Technical Forum 9/2010
  - Questionnaires for the projects crossing national boundaries and NGIs

- **Participation & presentations from**
  - 3 user communities
    - *Biomed, Earth Sciences, HEP*
  - 5 ESFRI projects
    - *CLARIN, Lifewatch, ELIXIR, EuroFEL, ILL*
  - 2 NGIs (Italy & U.K.)
Highlights of the results

• Grid users do not want to handle multiple credentials
  – Users would like to obtain their Grid credentials using their existing user credentials

• DCIs would like to use federated identities
  – It is recognized that (inter)national federations are becoming more and more important

• X.509 certificates are and will be required by the majority of the Grid infrastructures for the foreseeable future
<table>
<thead>
<tr>
<th>Use case</th>
<th>Description</th>
<th>Current status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>X.509 issuance based on AAI credentials</td>
<td>“Solved”, but needs improvement</td>
</tr>
<tr>
<td>2</td>
<td>AAI-enabled portals to Grid infrastructures</td>
<td>Some solutions exist</td>
</tr>
<tr>
<td>3</td>
<td>AAI-enabled Grid information portals</td>
<td>Low priority</td>
</tr>
<tr>
<td>4</td>
<td>Security Token Service</td>
<td>New, general purpose service, high priority</td>
</tr>
<tr>
<td>5</td>
<td>Use of AAI attributes in the Grid</td>
<td>Interesting, potentially very important</td>
</tr>
<tr>
<td>6</td>
<td>Virtual Organization registration using AAI attributes</td>
<td>Low priority</td>
</tr>
</tbody>
</table>
• Security Token?
  — « A collection of statements (claims) about a user or a resource »
  • Anything that can be attached into a Web Service (SOAP) message
  • Example token formats: X.509 certificate, SAML assertion, Kerberos ticket, Username/Password, ...

• Security Token Service?
  — « A Web service used to issue, renew, validate and cancel security tokens »
STS ISSUE Functionality Overview

• Transforms the security token into another security token
  1. Validates the incoming security token
  2. Aggregates the required information & issues the new security token
  • Possibly by exploiting external sources / authorities
  3. Includes the new security token into the response message

• Establishes a trust relationship between different application domains
Username/Password to X.509

STS Client Tool

Username & Password

User Database

Verifies the token

Requests a certificate

Issues a certificate

CA

X.509 certificate -token

Username/Password -token

X.509 & Private key to the filesystem
SAML assertion to X.509

Username, Password, Home Institute

Username, Password

SAML assertion

SAML assertion -token

X.509 certificate -token

X.509 & Private key to the filesystem

Requests a certificate

Issues a certificate

Home Institute

STS

Client Tool

CA

01/03/2012

Henri Mikkonen @ ISGC 2012
SAML assertion to X.509

- STS Client Tool
  - Username, Password, Home Institute
  - SAML assertion
    - SAML assertion -token
    - X.509 certificate -token

- SAML Trust Domain
  - Home Institute

- X.509 Trust Domain
  - CA
    - Requests a certificate
    - Issues a certificate

- X.509 & Private key to the filesystem

01/03/2012
Henri Mikkonen @ ISGC 2012
SAML assertion to X.509 proxy

**STS**

- **Client Tool**
- **Username, Password, Home Institute**
- **SAML assertion**
- **SAML assertion -token**
- **X.509 proxy certificate -token**

**Home Institute**

**SAML Trust Domain**

**X.509 Trust Domain**

- **Requests a certificate**
- **Issues a certificate**
- **Requests attributes**
- **Issues an attribute certificate**

- **CA**
- **VOMS**

**X.509 proxy certificate chain & private key to the filesystem**

1. **Username, Password, Home Institute**
2. **SAML assertion**
3. **SAML assertion -token**
4. **X.509 proxy certificate -token**
SAML assertion to X.509 proxy

Username, Password
Web browser access

SAML assertion
SAML assertion -token

X.509 proxy certificate -token

Access Grid Services using the user’s proxy

Access Grid Services using the user’s proxy

Home Institute

Home Institute

SAML Trust Domain

SAML Trust Domain

X.509 Trust Domain

X.509 Trust Domain

Requests a certificate
Issues a certificate
Requests attributes
Issues an attribute certificate

CA

CA

VOMS

VOMS
• 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, ...
Thank you! Questions?

Henri Mikkonen
<henri.mikkonen@cern.ch>