Building blocks for establishing federation with organizations like ESA

ESA Single Sign-on & OGC Authentication Standard

A. Baldi ESA: Andrea.Baldi@esa.int
M. Leonardi RHEA: M.Leonardi@rheagroup.com

Helsinki 02/10/2013
FIM4R
ESA EO IM introduced in 2011

- ESA EO Identity Management and the supporting AAI infrastructure for the creation, maintenance, and utilization of digital identities was introduced in beginning of 2011 after an initial study:
  - Initially based on Shibboleth 1 and then ported on Shibboleth 2 (current baseline) with few extensions
  - Consists of:
    - Redundant Identity providers (IDPs)
    - Redundant Identity Registries (LDAPs)
    - Multiple Service Provider (SPs) Check Points
  - Is based on a common “Minimal User Profile” derived from `inetOrgPerson` + a dedicated common EO SP profile for specific attributes.
Authentication
Single SSIgn On for all Web applications with inheritance of User community between SPs.

Authorization
Exchange of attributes for granting user access to the resources with SP profile synchronization with IDP.

Chained Multi Step Self Registration
Acquiring user’s identity information by IDP and SPs before issuing user credential.

Credentials Recovery
The user is able to self recover a forgotten password autonomously.

Secure Storage
Storage of sensitive identity information into secure registry (via encryption, owned by the IDP).

Administration
Self users administration of key profile information. More advanced administration functions across the enterprise for IM administrators.

Security Enforcement
Password strong security enforced upon registration and password management by the IDP.

Auditing
Auditing of user privileges, user access to resources, resource utilization.

Reporting
Reporting of user information for statistical utilization via a dedicated BI tool.

Authentication for Java Applications
JCL (Java Client Library) designed to offer an SSO API to Java applications.

Easy AAI Deployment
Virtual Environment with AAI infrastructure and IM template for SP.

AAI Robustness
Geographically Distributed Cluster for ESA AAI infrastructure.
Why FIM is important for ESA?

• Enable **Internal** Identity Federation:
  • split/model ESA user communities into smaller dedicated “domains” (e.g. ESA ONLY projects, ESA/EU projects, etc)

• Allow different organizations to interoperate and efficiently share data and services via **External** Identity Federation:
  • Enable ESA EO SSO users to access external resources operated by different space organizations.
  • Enable others space partners’ users to access to ESA EO resources.
# ESA Use Cases Details

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Source</th>
<th>Context</th>
<th>Description</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESA EO Federation</td>
<td>ESA/EU</td>
<td>GMES &amp; MM GS</td>
<td>Implementation of EO Federated Domains: different administrative Domains for i.e. EO ESA, EO EU. Users shall coexist with no duplication of accounts.</td>
<td>C2C</td>
</tr>
<tr>
<td>ESA EO Mirror Sites</td>
<td>ESA, Nasa, NOAA</td>
<td>Envisat Terra/Aqua</td>
<td>Joint dissemination with other space organizations (e.g. NASA/NOAA MODIS/MERIS): Nasa ~80000 Users, ESA ~12000 NASA selected users as ESA users (pilot?)</td>
<td>C2C</td>
</tr>
<tr>
<td></td>
<td>ESA VITO</td>
<td>PROBA V</td>
<td>VITO selected users as ESA PROBA V users</td>
<td>C2C</td>
</tr>
<tr>
<td></td>
<td>ESA Euro Image</td>
<td>3rd Party Missions</td>
<td>Independent distributor for ESA 3rd party mission data via ESA branded portal</td>
<td>C2C</td>
</tr>
<tr>
<td>Collaborative Scenarios</td>
<td>ESA DLR, UK Space Agency</td>
<td>LTDP</td>
<td>Each organization distributes its own long time data series (e.g. AVHRR) to the federation users. Authentication done by the Home organization</td>
<td>B2B C2C</td>
</tr>
<tr>
<td></td>
<td>ESA Eumetsat, DLR</td>
<td>HMA geo/fedeo</td>
<td>Federating WEB SSO with WEBServices based on OGC User Management Interfaces for Earth Observation Services STS between SAML based systems Pilot with Eumetsat &amp; DLR (~9000 Users)</td>
<td>C2B</td>
</tr>
</tbody>
</table>
Objective: Federating different users communities belonging to space agencies to easily share EO data by allowing cross authentication and authorization.

- ESA EO IM will use AuthZ/AuthN OGC Web services & Web SSO:
  3. Different Consumer to Consumer (C2C) Authentication & Authorization: ESA Web SSO shall interact with other space agencies Web SSO (e.g. ESA SSO with NASA SSO).
• Importance of IM was recognized in the context of the Heterogeneous Mission Accessibility (HMA) project.

• HMA is an ESA, ASI, CNES, CSA, DLR, EUSC, EUMETSAT collaboration to harmonize access to heterogeneous EO data systems.


• OGC 07-118 Specification submitted in 24th September 2013 as best practice to Open Geospatial Consortium (OGC) for approval as applicable standard.

• OGC 07-118 describes interfaces and scenarios for Authentication & Authorization in a federated system of OGC Web Services for Earth Observation. Expected approval by end of 2013.

• Implementation in the scope of new Federated Identity Management project 2014.
A Secure Token Service (STS) is a Web service that issues interoperable security tokens.

It makes assertions based on evidence of the user identity.

An STS receives some kind of credential and returns a token that represents the user’s identity.

Presenting the token, as proof of user identity, lets the user to be served outside of his security domain without providing credential.

A Web service itself can generate security tokens or it can rely on a separate STS to issue a security token.

The STS security model includes a Target Service, a Client and the Security Token Service.

There is an explicit trust relationship (PKI) between the Web service and the STS and between the client and the STS.

There is not an implicit trust between the client and service.
STS Security Model

1. RST (Request Security Token) with credentials
2. Validate identity in the local user registry
3. Create/Sign/Encrypt the SAML token
4. RSTR (Security Token Signed and Encrypted by the STS)
5. Service Request (Security Token)
6. Validate Security Token
7. Service Response

Basic case with the STS acting as Identity Provider (IDP)
**B2B Authentication Model**

1. **Client** sends credentials to **STS**
2. **Redirect RST to the client home organization IDP**
3. **Validate identity in the user registry**
4. **Create the SAML token**
5. **RSTR (SAML token)**
6. **Sign/Encrypt the SAML token**
7. **RSTR**
8. **Service Request (Security Token)**
9. **Validate Security Token**
10. **Service Response**
C2B Authentication Model

1. Protected Function call

2. Web Auth Request redirected to the client home organization IDP

3. Validate identity in the user registry

4. Create the SAML Artifact + attributes

5. Return the SAML Artifact + attributes

6. RST with Web Auth

7. Create/Sign/Encrypt the SAML token

8. RSTR

9. Service Request (Security Token)

10. Validate Security Token

11. Service Response
C2C Authentication Model

1a. Service request

2a. Federating user authentication process

3b. Validate identity in the user registry

4b. Create the Authentication statement

1b. Service request

2b. Federated user authentication process

User Home Organization IDP (Federated IDP, e.g. NASA)

Federating Domain (i.e. ESA)

Federating IM Infrastructure

WEB IDP

Users Registry

Federating Service Provider

Federation Gateway

Federated User Web Browser (i.e. NASA user)

Federated User Web Browser (i.e. ESA user)
Conclusions

- FIM is a challenge and it is essential:
  - to increase data exchange and collaboration with international partners
  - to enable EO organizations to increase data distribution via a simplified user access

- Scenario is complex and multi-faced

- Need to cope with different technologies, organizations and their constrains.

- Collaboration among organizations is essential to be able to get concrete results.

- Space organizations have agreed to start co-operate to establish common building blocks