Access Control - Federation - relevance of OGC Best practice "OGC User Management Interfaces for Earth Observation Services”

Albrecht Schmidt (ESA) — Albrecht.Schmidt@esa.int
Marco Leonardi (Rhea) — M.Leonardi@rheagroup.com

Overview

- EO Single Sign-On (SSO) and moving towards Federated Identity Management
- Access Control - Federation
- OGC Best practice "OGC User Management Interfaces for Earth Observation Services”

Some facts about EO-SSO

- Operational System and Reference Platform
- Growing number of increasingly sophisticated services which rely on EO-SSO
- User Registration and Administration play an important role begin the scenes
- System evolved through requirements from Service Providers
- Formal Transfer-to-Operations process

ESA EO Identity Management Functions

Authentication

Single Sign On for all Web applications with inheritance of User community between Service Providers.

Authorisation

Exchange of authorisation statements for granting user access to the EO resources.

User Registration

Acquiring user's identity information before allowing user to login.

Password Recovery

The user is able to recover a forgotten password autonomously.

Secure Storage

Storage of sensitive identity information into secure registry via encryption.

User Administration

Administration of key profile information. More advanced administration functions for IM administrators.

Security Enforcement

Password strong security enforced upon registration and password management.

Auditing

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

Reporting

Reporting of user information for statistical utilisation via StatRep.

Authentication for Java Applications

Used to enable EOLI authentication.

Easy Deployment

Virtual Environment with ready to use components.

IT Redundancy

Geographically distributed for authentication infrastructure.

The FIM4R Vision

FIM4R (Federated Identity Management for Research Collaboration) *addresses the challenge of scientific laboratories and research organisations of making huge amounts of data accessible by expanding user bases in dynamic collaborations that cross organisational and national boundaries.*

- FIM4R objectives are:
  - Provide a **common policy and trust framework** for Identity Management based on existing structures and federations either presently in use by or available to the communities.
  - Provide researchers with **unique electronic identities** authenticated in multiple administrative domains and across national boundaries that can be used together with community defined attributes to authorise access to digital resources.
- FIM is designed to follow the institutional perspective.

Application areas of Federation

- ESA EO Internal Federation
- ESA EO Mirror Sites:
  - ESA data distributed by 3rd parties
  - ESA distributing other organisations' data
- Cooperative Scenario between ESA and other partners:
  - Cooperative data access
  - Cooperative LTDP access
  - Support to Thematic Exploitation Platforms

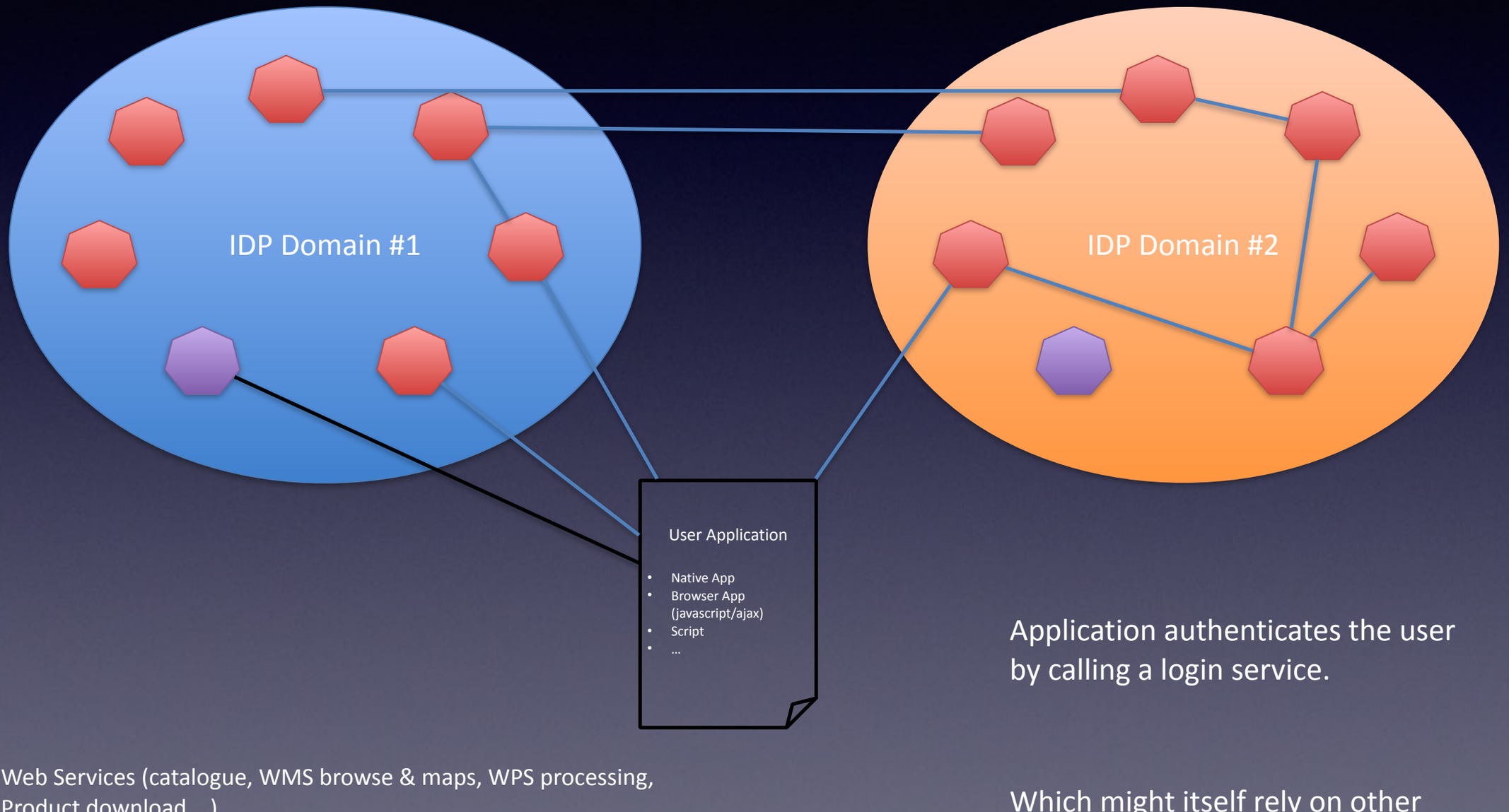
Working towards Federation (1)

- Architecture
  - Consolidation of current architecture
  - Addition of components such as Metadata Aggregator, Discovery Services, Security Token Service, Policy Enforcement Points, Attribute Authority
  - Reconsidering the concept of registration

Working towards Federation (11)

- Processes and concepts:
  - User Registration, ‘homeless’ users
  - Enhanced Client / Proxy Support for scripting/M2M solutions
  - Log-Out
  - Where is ‘home’ in a federation?
- Support to Thematic Exploitation Platforms

Web API authentication: Generic Scenario



Application authenticates the user by calling a login service.

Which might itself rely on other services…

Web Services (catalogue, WMS browse & maps, WPS processing, Product download,…)

Login Services (provides a token)

What else we are working on

- High-Availability architecture for SSO services
  - Note that any Service Provider requirements on availability implicitly impose availability requirements on the SSO.
- Security has to be reconsidered over time.
  - Again, subsystem requirements propagate up.
  - Ways to address the problem of bitrot.
- Design patterns for service providers

OGC User Management Interfaces for Earth Observation Services" (07-118r9)

- Document still relevant after so many years and updates.
- As a best-practice document it has to be read with the current context in mind.
- It provides a framework, terminology and tools that can be used to describe systems.

Conclusion

- Working towards Federated Identity Management by consolidating and evolving current technology.
  - STS, Metadata Aggregation, PEPs, etc.
  - Attribute Authority design and use
- Use existing technology and concept to arrive at Best Practices for current applications.
- Work will also include reviewing processes, procedures and maintenance.

Thank-You!