HMA for Science Kickoff Meeting

KO Meeting
24 January 2013, ESRIN Frascati

Yves Coene, SPACEBEL
Pierre Denis, SPACEBEL
Overview

- **Specification Activities**
  - Task 2: Identity Management

- **Demonstrators**
  - Task 2: Identity Management
  - Task 3: EO Metadata
  - Task 5: Enhancement ebRIM EP

- **Task 8: HMA-S Testbed**

- **Technical Coordination**
  - Task 9: Coordination and harmonisation
Introduction
Task 2: Demonstrator Identity Mgt

- Task inputs:
  - OGC 07-118 v1.1 (see Task 2 specification activity)
  - HMA-T Identity and Access Management Guidance Document v 1.0
  - HMA Skeleton 2.2
  - Intecs Policy Enforcement Point
  - Spacebel STS Implementation
Goal:

- Demonstrator for the 3 use cases of OGC 07-118:
  1. STS as local IdP
  2. STS as Federating IdP
  3. STS with trusted IdP (e.g. Web-SSO)

- STS implementation shall be updated to cover use case 2.

- Need to validate the correction of “DelegateTo” issue

RST with password

RST with signature
Use case 1: STS as local IdP
Task 2: Demonstrator Identity Mgt

- Use case 2: STS as Federating IdP (DelegateTo)
Use case 3: STS with trusted IdP

- **External IdP**
- **Client**
  - Client Keystore
    - Client private key
    - Signature of RST
  - SOAP/HTTPS
  - RST with signature
- **STS**
  - STS Keystore
    - STS private key
    - Signature of SAML token
    - Relying Party’s public key
    - Encryption of SAML token
    - Trusted Client’s public key
    - Verification of RST signature
  - SOAP/HTTPS
  - RSTR (SAML Token) or SOAP fault
- **PEP** (Relying Party)
  - PEP Keystore
    - PEP private key
    - Encryption of SAML token
    - STS public key
    - Verification of SAML token signature
  - SOAP/HTTPS
  - Service request
- **Service**
  - JNDI
  - LDAP User Registry

Web-SSO, e.g. Shibboleth
Task 2: Demonstrator Identity Mgt

HMA Skeleton (OGC 07-118 - RST)

HMA Skeleton (version 2.2 build 1004131448)
Task 2: Demonstrator Identity Mgt

- HMA Skeleton (OGC 06-131 GetRecords)
Task 2: Identity Mgt - Demonstrator

➢ Outputs:

• D2000.2: Open-source Demonstrator
  ▪ Policy Enforcement Point (Intecs)
  ▪ Client – HMA Skeleton (Spacebel)
  ▪ Updated Security Token Service (Spacebel)

• D2000.3: Demonstrator TN including
  ▪ Description of native interfaces
  ▪ User Manual

H2.1 – HMA Skeleton (Client)
H2.2 – STS
H2.3 – PEP

Updated HMA-T Guidance Document
Task 2: Identity Mgt - Demonstrator

Issues:

• Integration with Web SSO as part of Demonstrator?

• Alternatives:
  ▪ Online (test) UM-SSO IDP available at ESA to connect to?
  ▪ UM-SSO IDP to be made available by ESA?
  ▪ Shibollet IDP instead of UM-SSO IDP?