ESA EO Federated Identity Management Status Report

8th FIM4R

A. Baldi ESA: Andrea.Baldi@esa.int

M. Leonardi RHEA: M.Leonardi@rheagroup.com

ESA EO Identity Management Evolution

Authentication	Authorization	User Registration
Password Recovery	Secure Storage	User's Administration
Security Enforcement	Authentication for Java applications	Easy Deployment
Auditing	**Reporting**	**IT Redundancy**
Internal ESA EO Federation: Attribute Authority, ECP, STS	Short Term Internal/Inter federation ESA joining IDEM/EDUGAIN	Mid/Long Term Space Identity Management Federation

ESA EO Identity Management Evolution

Authentication	Authorization	User Registration
Password Recovery	Secure Storage	User's Administration
Security Enforcement	Authentication for Java applications	Easy Deployment
Auditing	Reporting	IT Redundancy
Internal ESA EO Federation: Attribute Authority, ECP, STS	Short Term Internal/Inter federation ESA joining IDEM/EDUGAIN	Mid/Long Term Space Identity Management Federation

Main Streams

1. Pilot Study with Siemens Romania:

    • Key topics relevant for future evolution

2. Internal Evolution Projects:

    • ESA new Online Dissemination Servers

    • ESA EO FIM

Siemens Pilot

- ECP prototypes:

  - Sample EO products Download Manager based on Java

  - Scripting languages for data retrieval via Perl and Bash

  - Still several limitations with shibboleth profile implementation and LDAP back-end not supported (only basic authentication)

Siemens Pilot

- ESA Internal Federation Prototype:

  - Split of EO domain into 2 new administrative domains:

    - ESA Multimission

    - ESA EU Copernicus

  - Deploy of Shibboleth native services

    - Multiple IDPs

    - Attribute Authority for shared profile management

    - Discovery Services

    - Metadata Aggregation

Siemens Pilot

- Prototype for an ESA Federation Management tool:

  - Assessment and tailoring of the Switch and Australian tools to fit ESA needs

  - Both could be used to simplify the current manual approach

  - The study recommended to use the Australian tool because less specific and rich of "general purpose functionalities"

Siemens Pilot

- IDEM/EDUGAIN Federation

  - Reuse of prototype for internal Federation

  - Implementation of EDUGAIN mandatory attributes in ESA IDP managed profile

  - First attempt to be compliant with Code of Conduct for the EO Landsat test dissemination server

  - Deploying of test SP and IDP in the cloud

  - First Successful test made with IDEM

AAI Ready for new generation EO Dissemination Servers

- SP specific profiles for EO dissemination to be used by Multi Mission and Copernicus

- Attributes Authority for specific SP profiles for service authorisation

- Implementation of standard profile attributes required by EDUGAIN

- Metrics for user management and service statistics
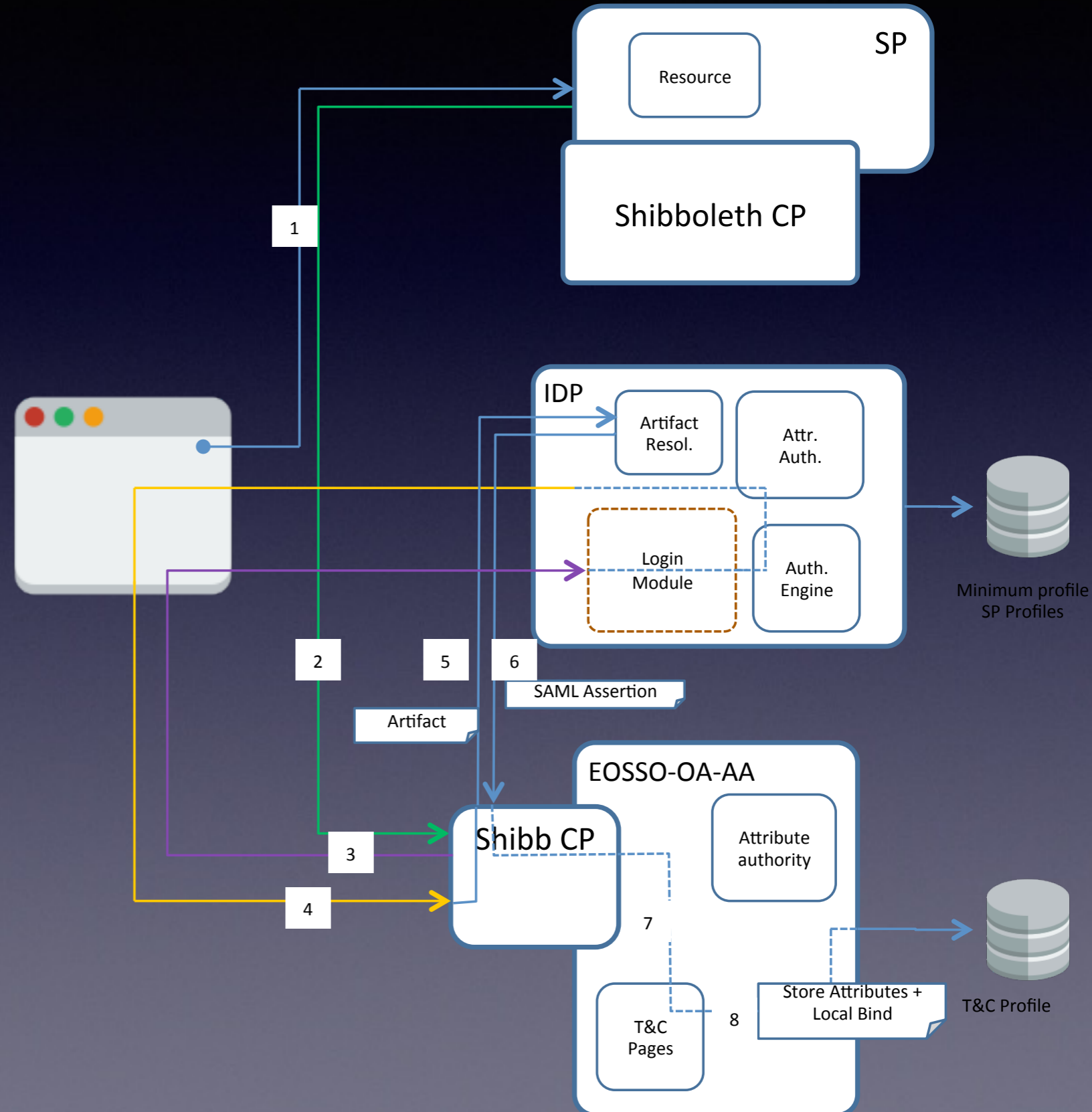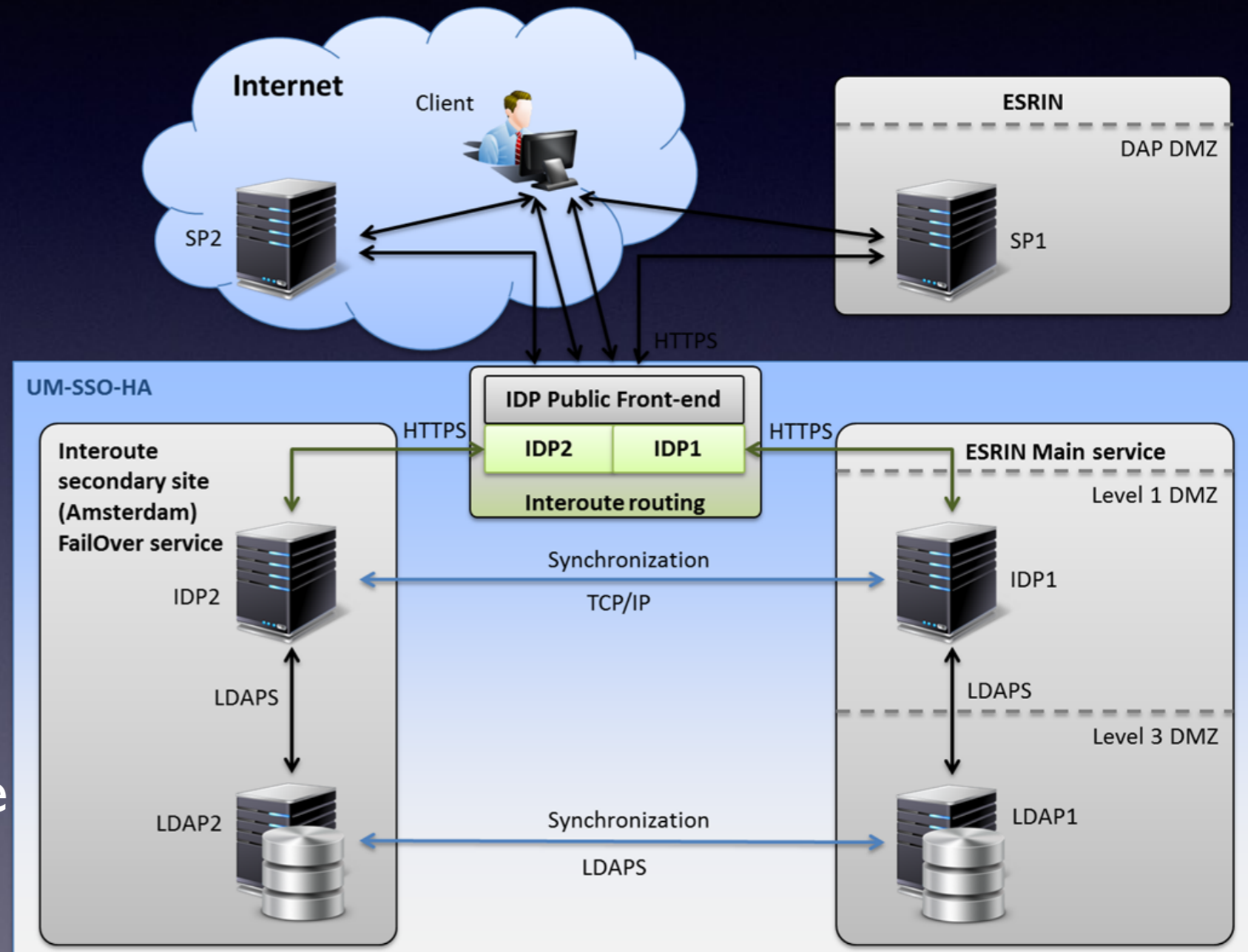
AAI Infrastructure redundancy for High Availability

- **High Availability AAI:**

  - Multiple IDPs/LDAPs distributed on geographical basis

    - Synchronisation of IDPs and LDAPs

    - IDP session data synchronization is obtained serializing them into memcached service attached to a distributed database.

ESA EO FIM
- EO SSO V3 -

- **New Generation of EO SSO shall include:**

  - **Main functionalities piloted by Siemens with production quality**

  - **Based on Shibboleth V3 shall support for ESA EO scenarios:**

    - **Internal Federation**

    - **Mirros Sites**

    - **Cooperative Multilateral**

EO FIM Project Bid Process

- EO FIM project procurement approach:
  - **Open Competition Tender in Europe via ESA EMITS (http://emits.sso.esa.int) open to Industry and Research Institutes.**
    - **Required skill in FIM domani, and related standards and technology:**
      - **SAML, STS, Shibboleth, etc**
  - **ESA Industrial geographical return policy promote the following countries:**
    - **Ireland, Poland, Luxembourg, Norway, Finland, Sweden, Czech Republic, Romania**
  - **Input to the BID :**
    - **Use Cases Specifications**
    - **Technical Requirements**
    - **Current Technical Baseline**
  - **ITT Budget : ~ 750K€ with two independent companies selected.**
    - **BID Publishing : March 2015**
    - **bidder proposal submission (bid Publishing + 6 weeks)**
    - **Evaluation (bidder proposal submission + 4 weeks)**
    - **Kick-off (Evaluation + 4 weeks)**