
The EUMETSAT EO Portal User Management Concept







Second Workshop on the use of GIS/OGC standards in meteorology

Météo-France
International Conference Center
42 avenue Gaspard Coriolis, Toulouse, France
23.-25. November 2009

Marko Reiprecht
con terra GmbH, Germany

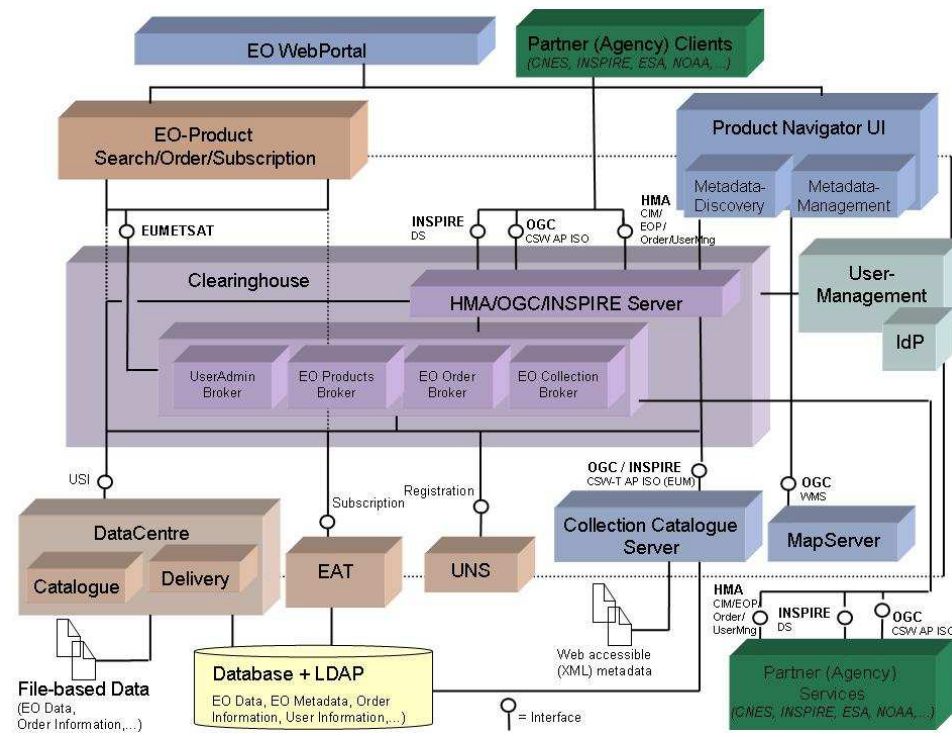
24. November 2009



-  **Introduction**
-  **Base Ideas**
-  **Components**
-  **Web application SSO**
-  **Web Service Integration**
-  **Summary**

- EO Portal provides a single point of online access to EUMETSAT data and dissemination services
 - Past: several applications with self contained user management
 - Users had to register with every application and to memorise different user ids and passwords
- EO Portal encapsulates the legacy applications and offers a harmonised user interface to discover, search, order / subscribe to data and services
- Clearinghouse:
 - allows users to access data and services of partner agencies (e.g. CNES Altimetry products, NOAA, WMO, ESA)
 - vice versa: allows partner agencies to discover, search, order and subscribe to EUMETSAT data and services via a set of programmatic, interoperable services
 - Services are based on OGC/HMA and INSPIRE EU specifications

- Some Services (e.g. ordering) require user details passed using security concepts
- In order to implement this between different organizations:
 - >> A harmonized, sophisticated, standards based security concept is required



 **Base Ideas**

- Brokered Trust via one or more trusted central authentication partners (Identity Provider)
- Integrate business partners as Service Provider entities
- Build up on already available federated user management and security specifications (SAML 2 + WS-Security)
- Explicit differentiation of web application SSO and the secure access to web services

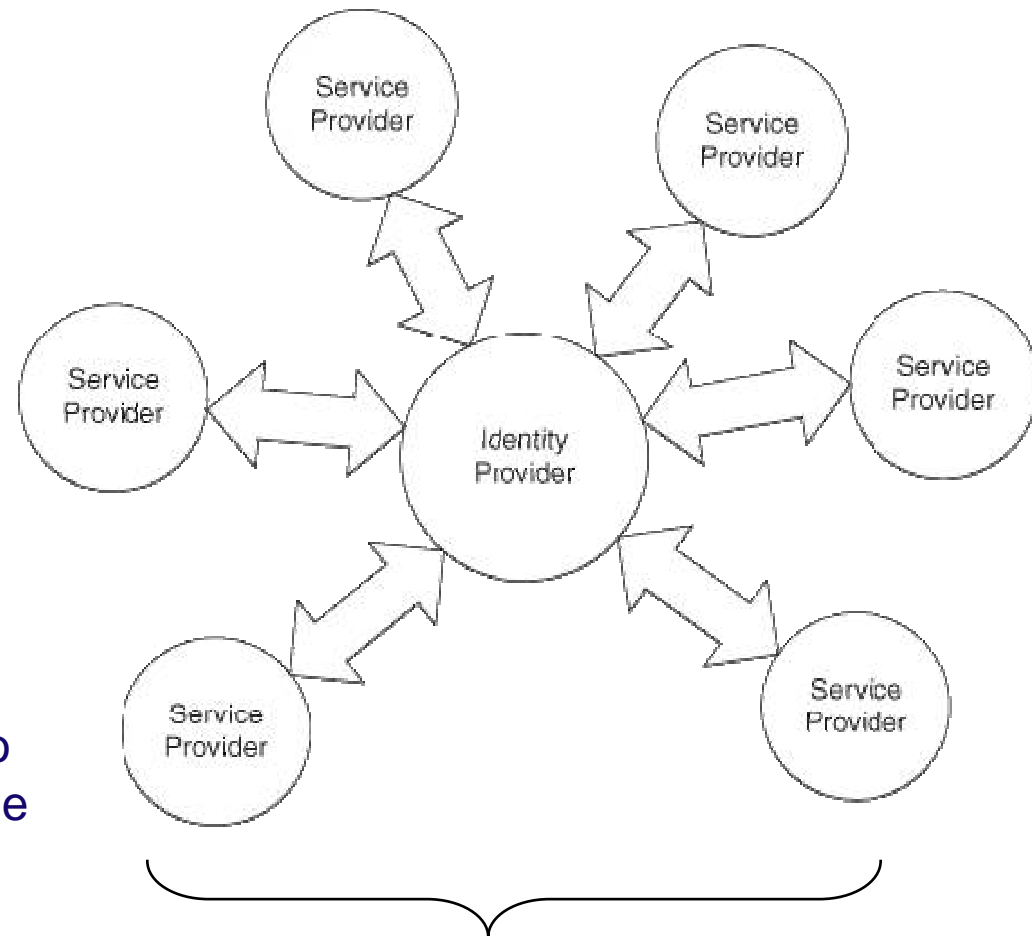


Terms

- Identity Provider (IdP)
 - Brokers the trust
 - Encapsulates user authentication
- Service Provider (SP)
 - Provides web services and web applications

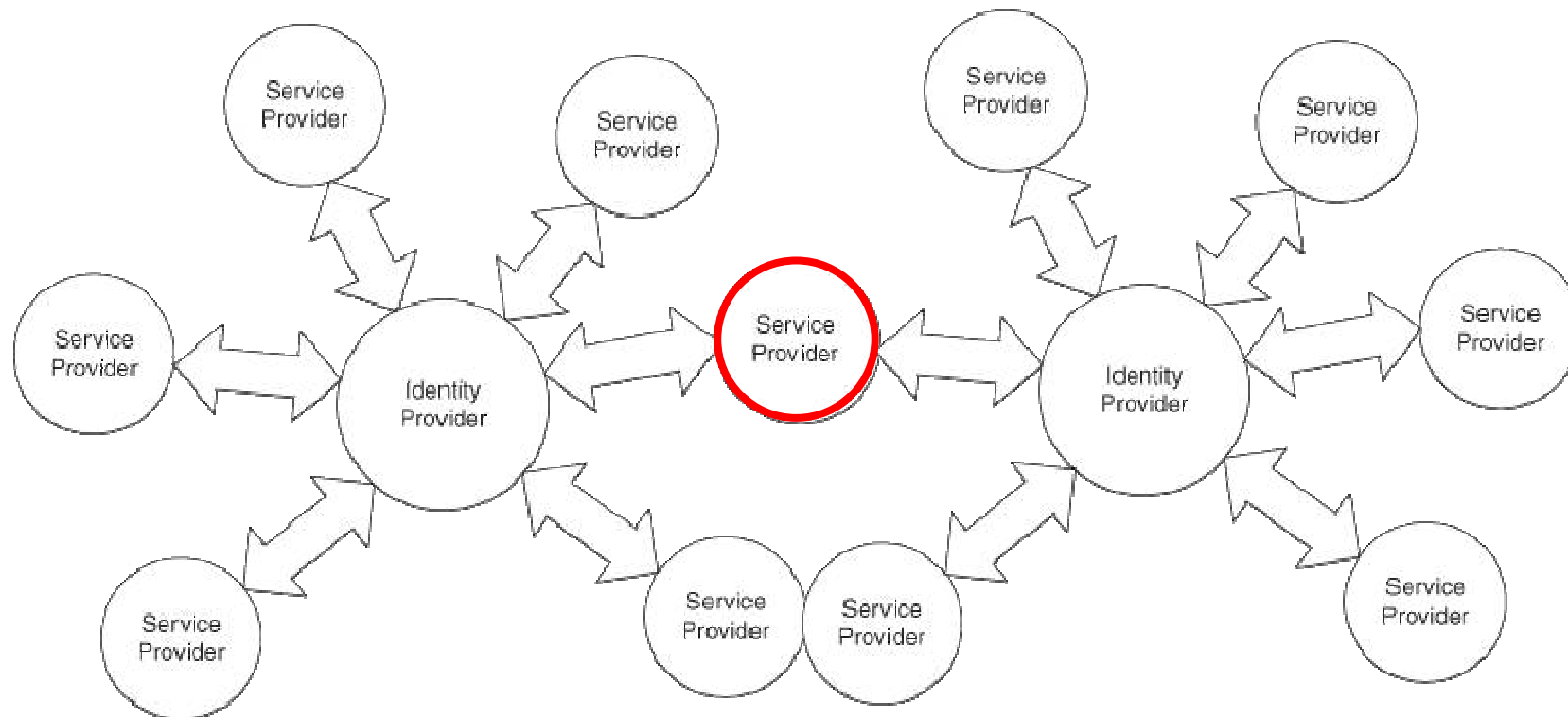
Both are Business Entities

- IdP and SPs work together to maximize their business volume

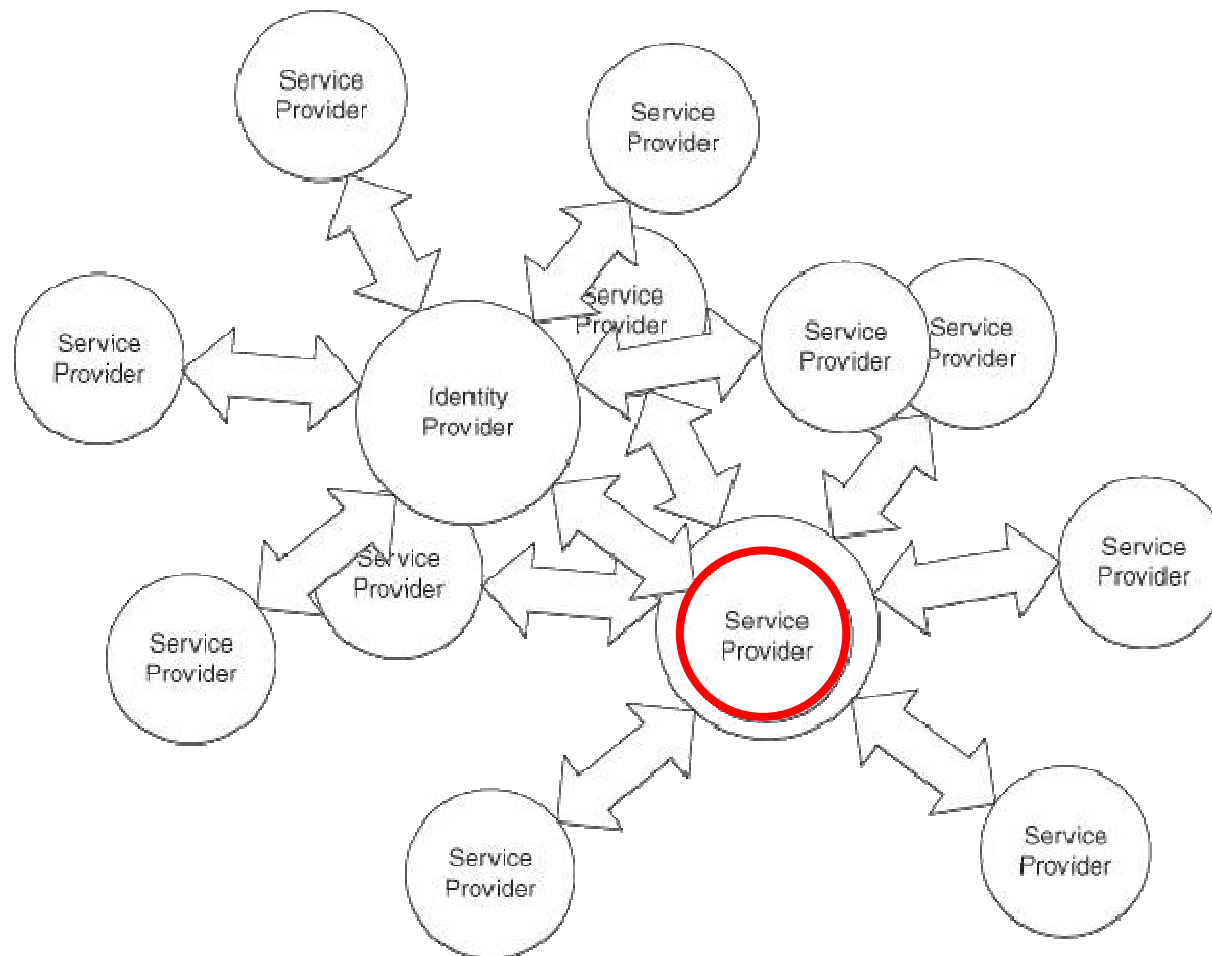


Circle of Trust

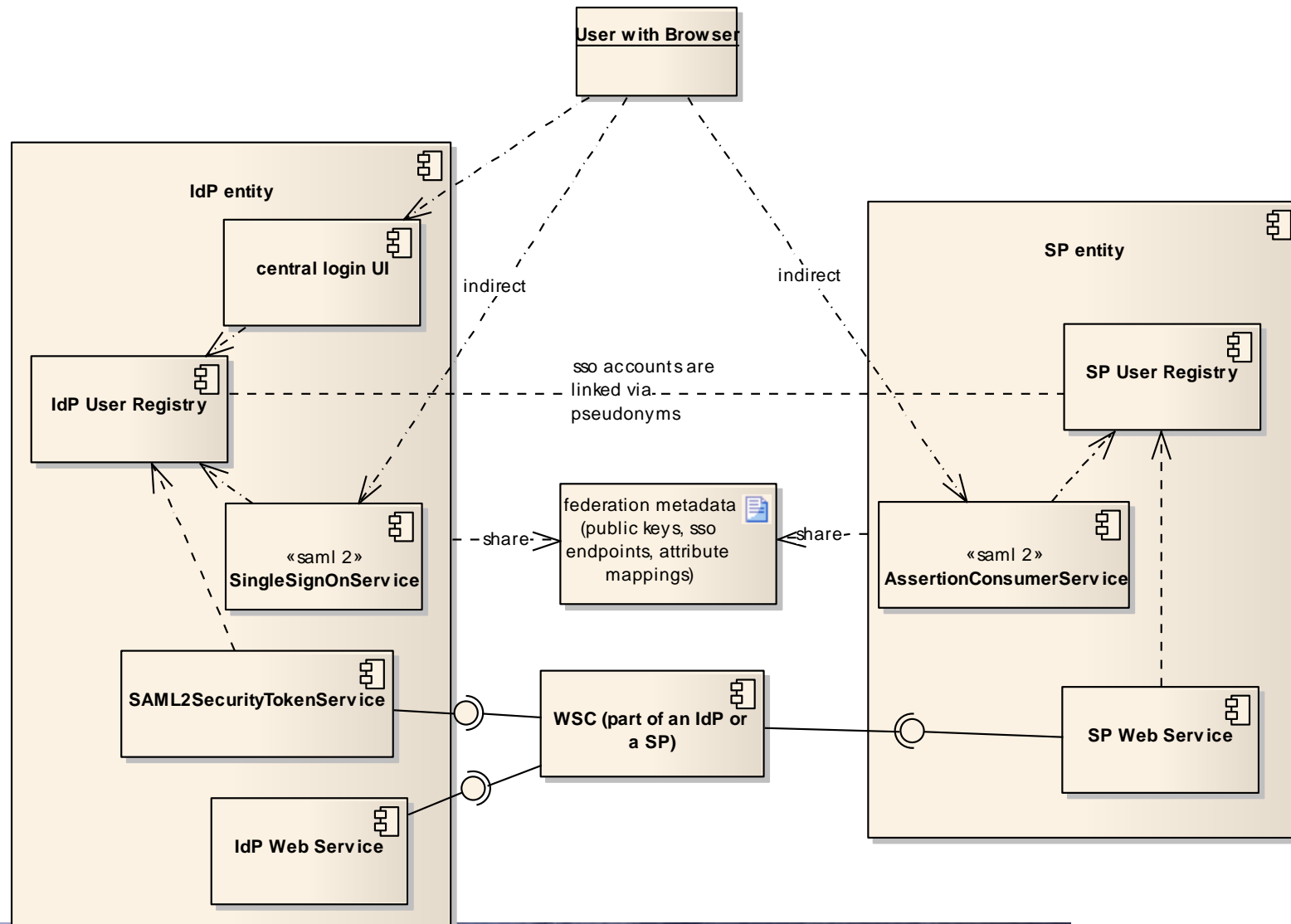
Complex Trust and Business Relationships



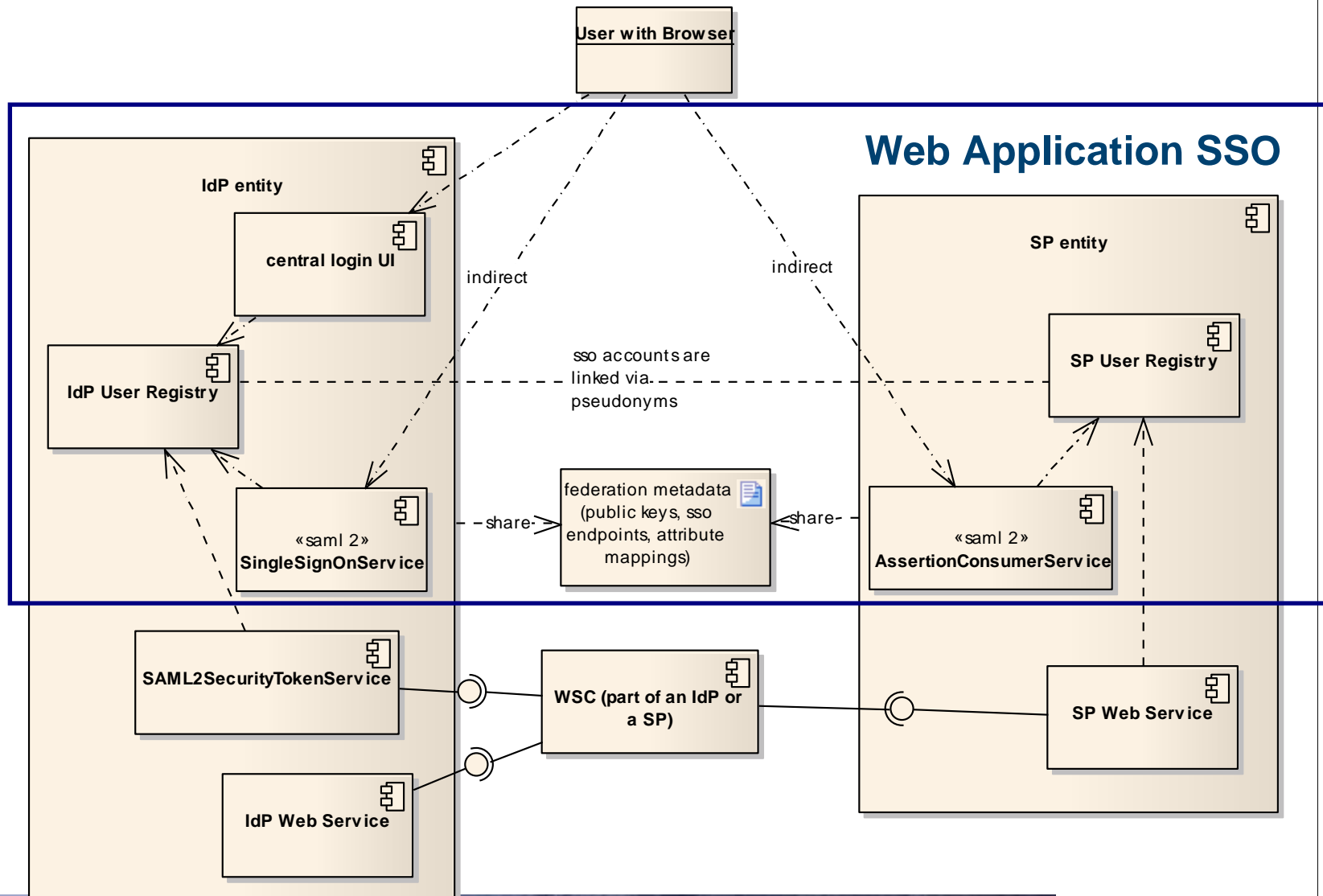
 **Complex Trust and Business Relationships**



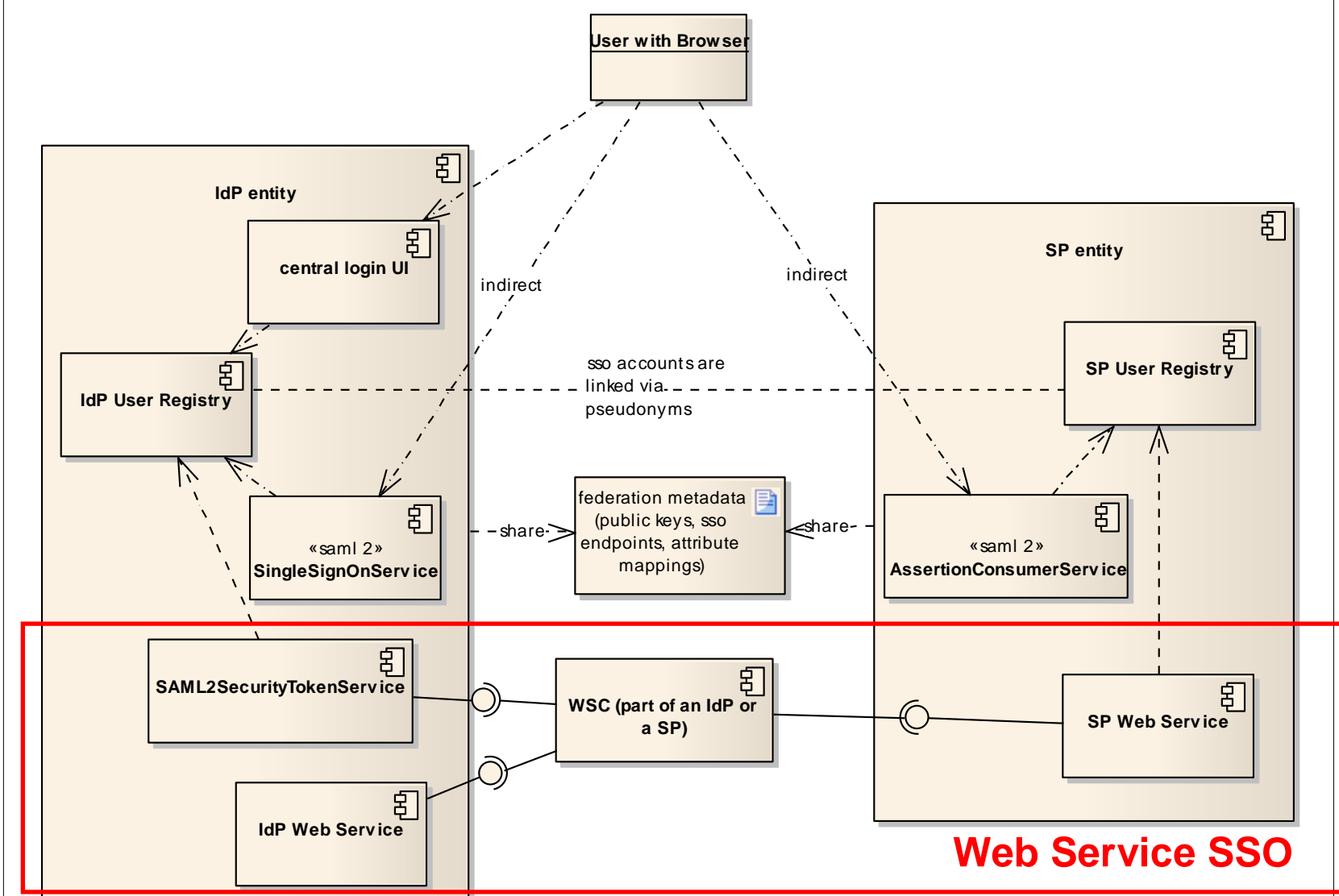
cmp eum usermanagement



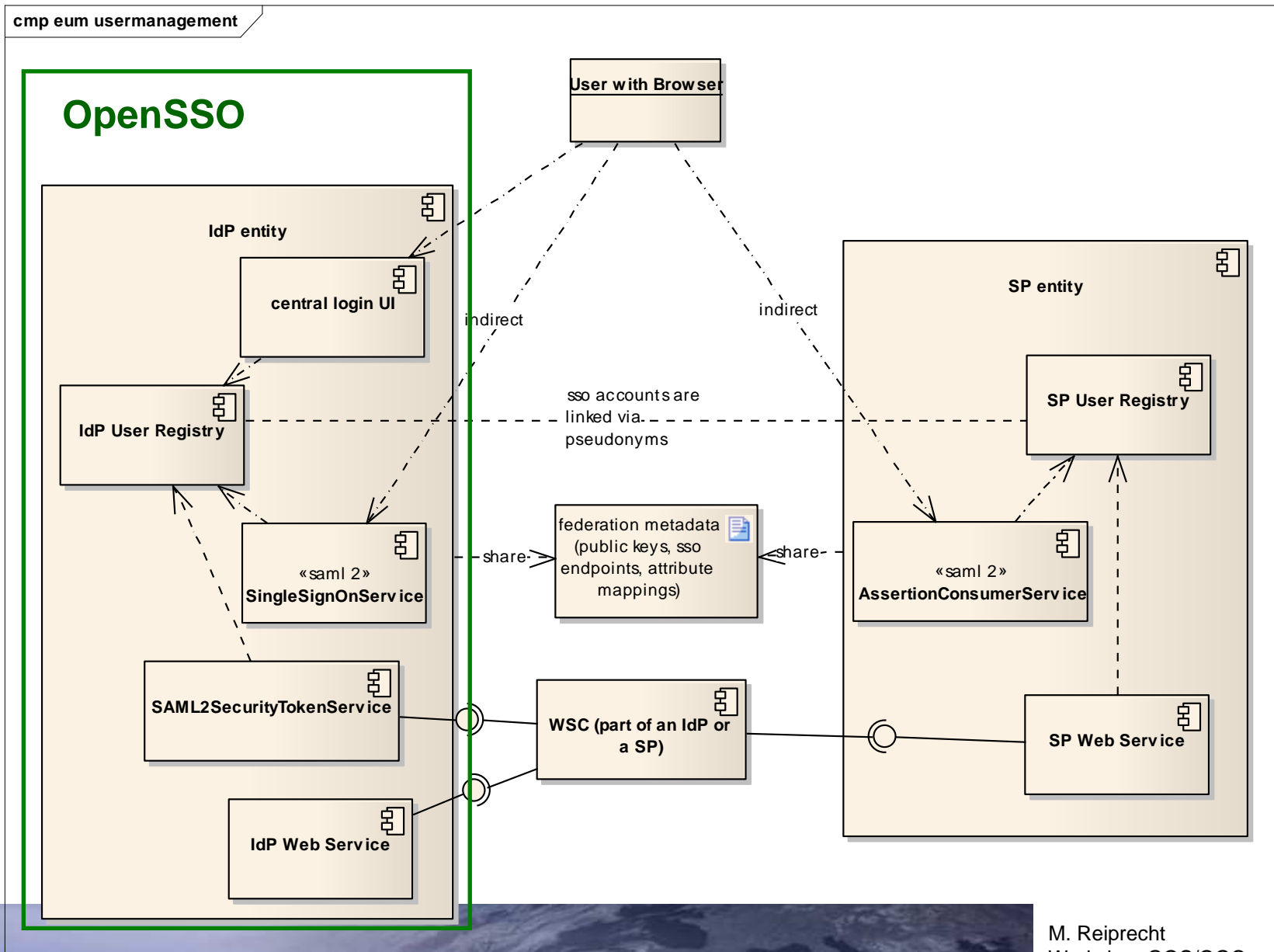
cmp eum usermanagement



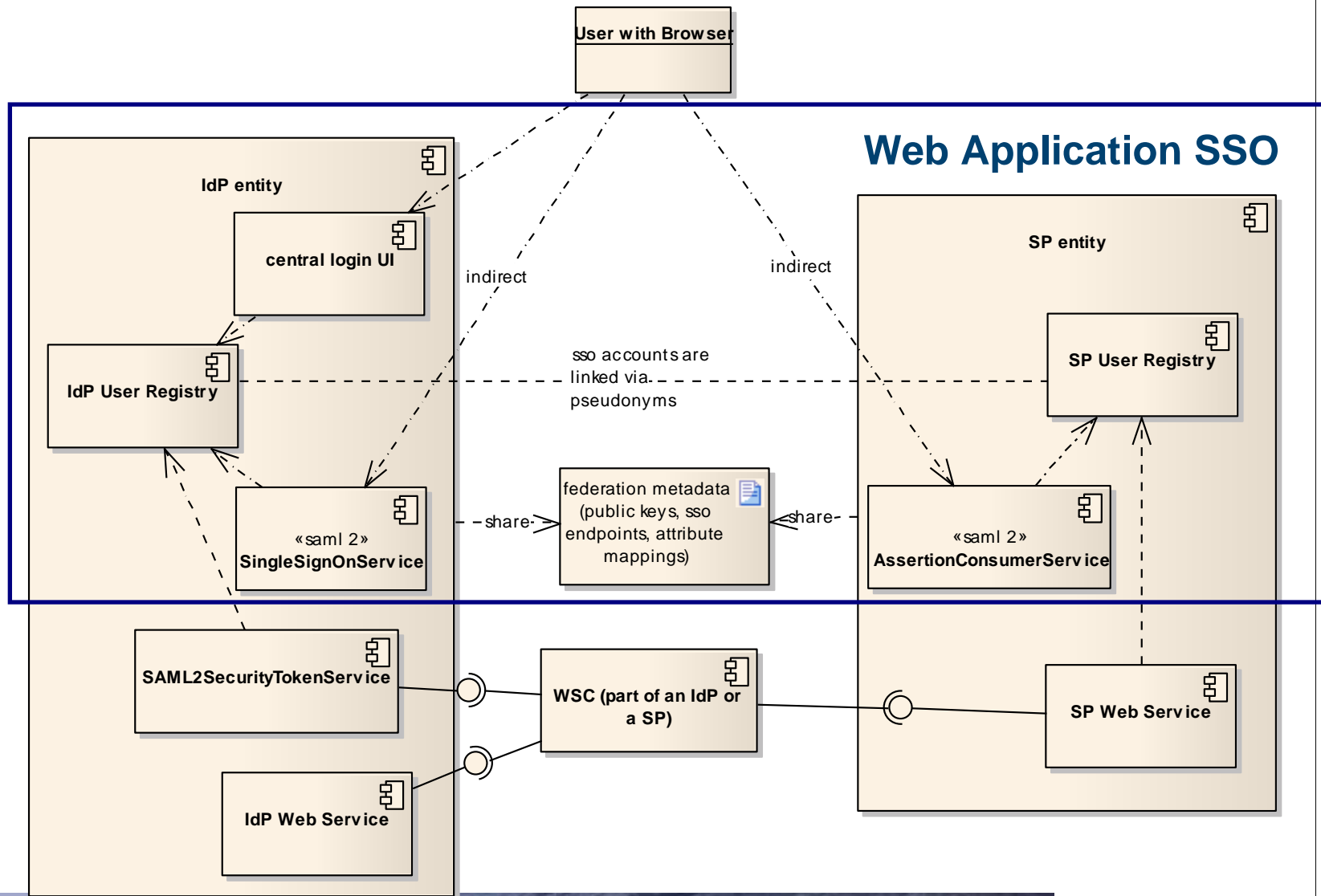
cmp eum usermanagement



Web Service SSO



cmp eum usermanagement



 **Sample starting from SP**

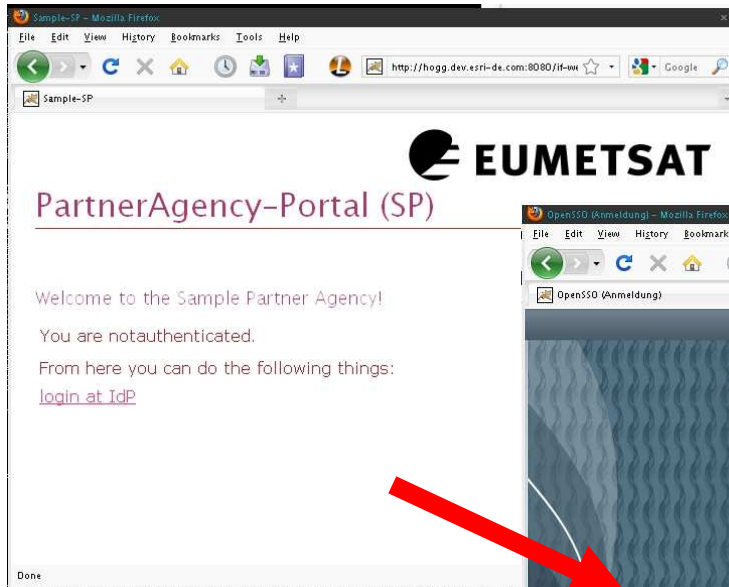


 **User not logged in**

 **Can perform anonymous tasks**



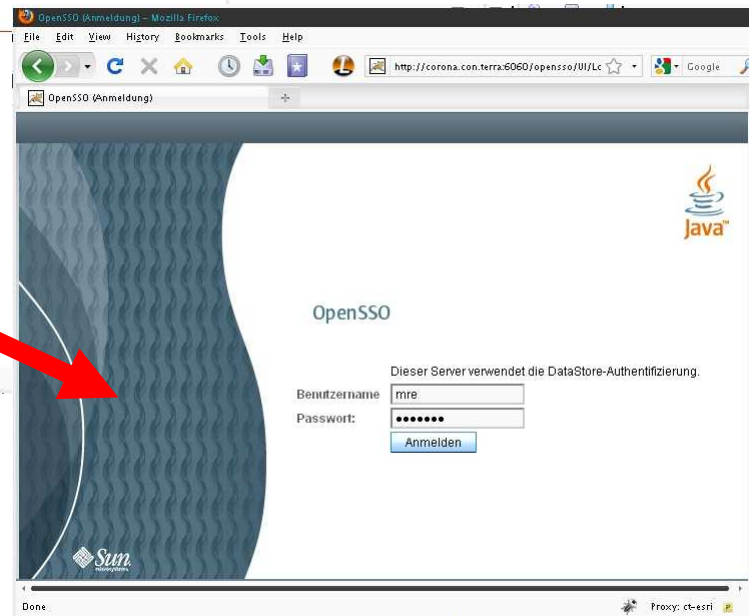
 **Sample starting from SP**



 **User clicks on “Login”**

 **Redirect to SingleSignOnService at IdP**

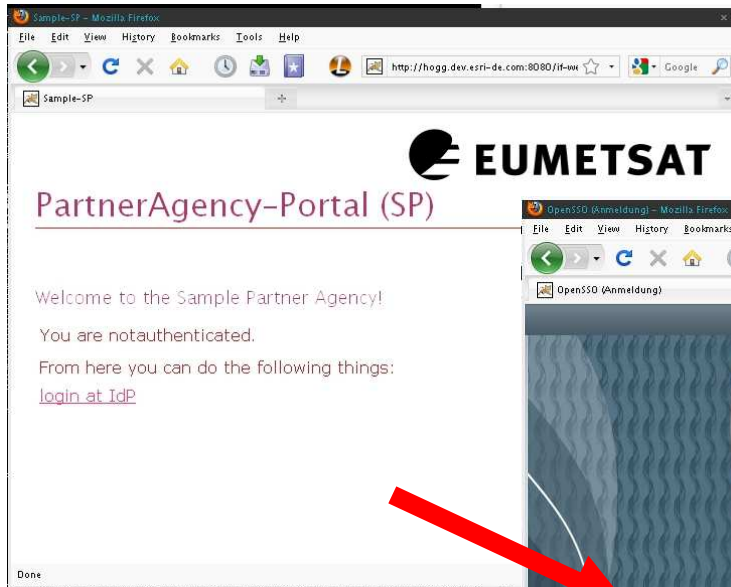
Central login UI



 **form-based redirect**

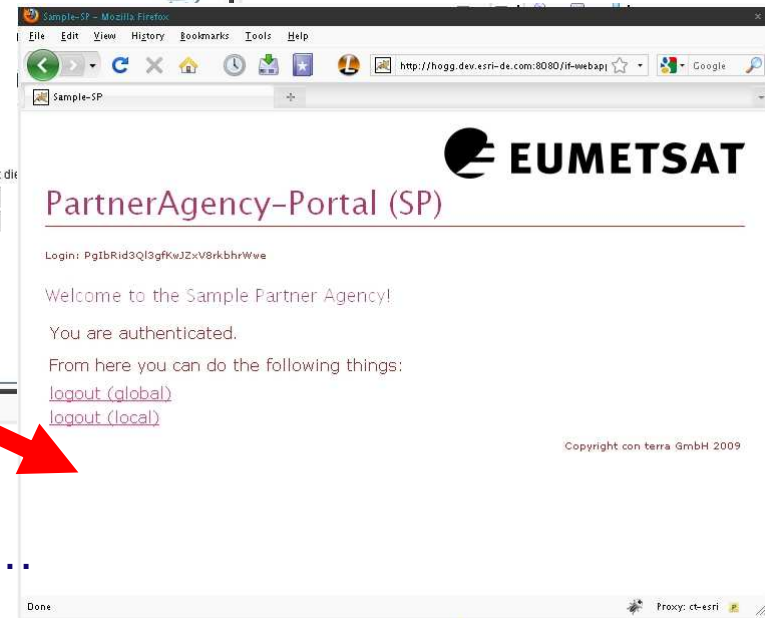
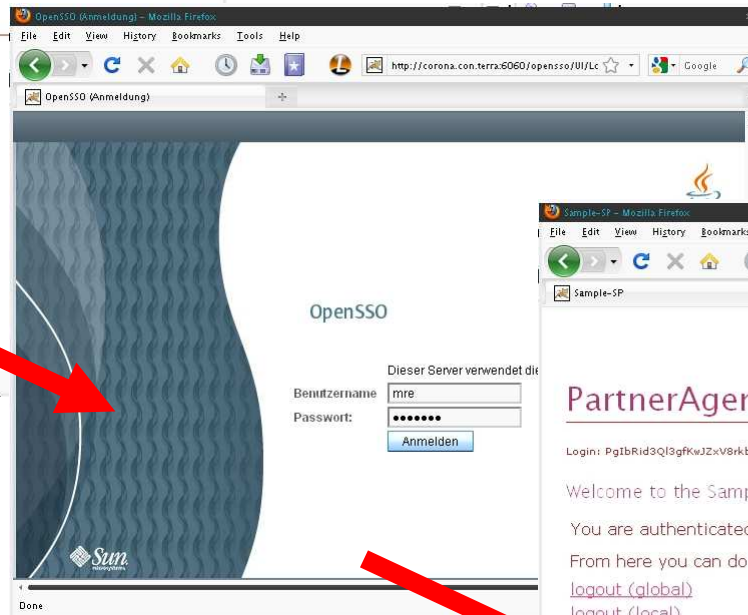
- SAMLRequest = <saml2:AuthnRequest/>
- RelayState = <start-url>

Sample starting from SP



Redirect to the AssertionConsumerService of the SP

- Now the user is authenticated



form-based redirect

- SAMLResponse = ...<saml:Assertion/>...
- RelayState = <start-url>



Web application SSO

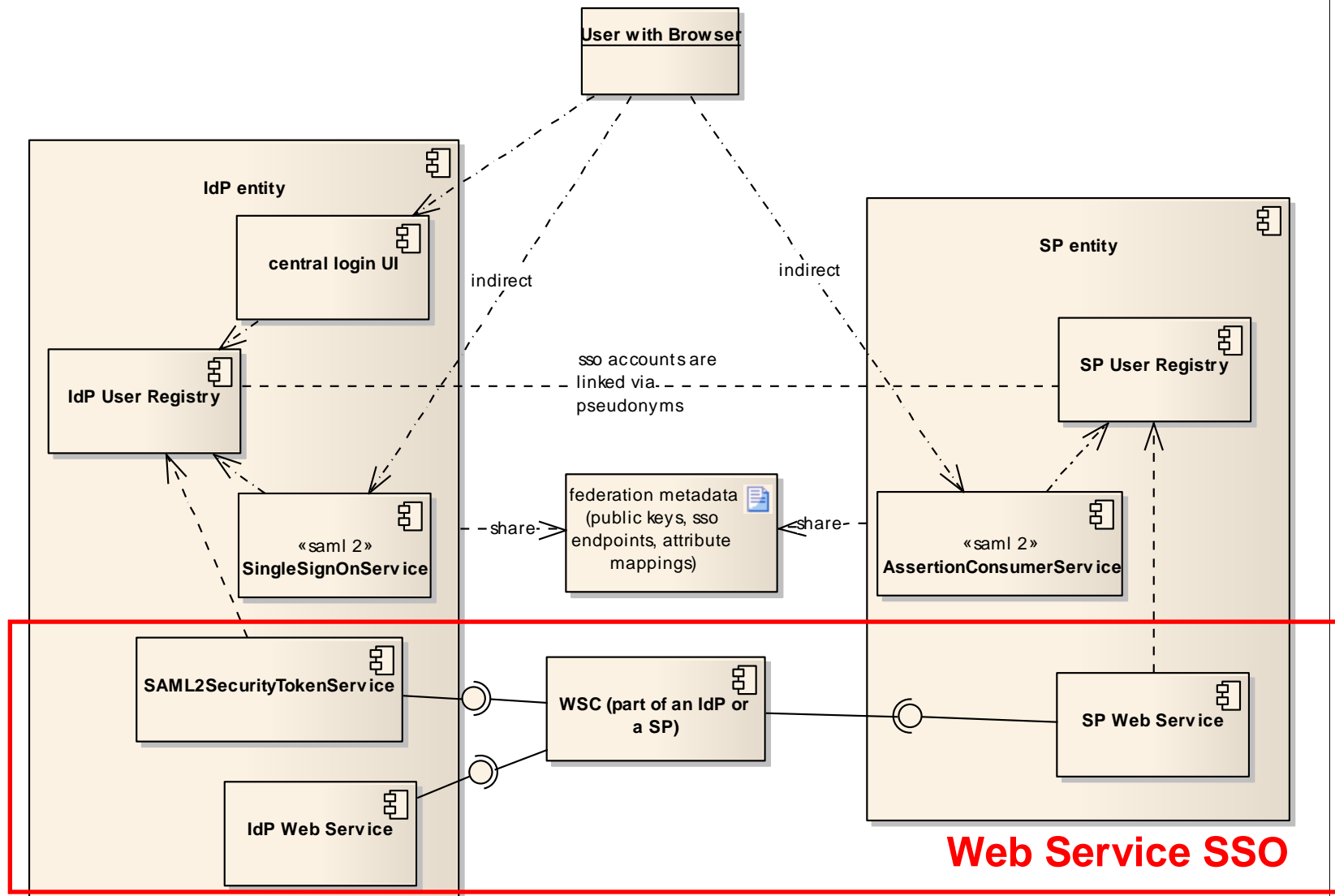
- SAML 2 Web Browser SSO Profile
 - HTTP-Redirect mechanism (HTTP-Post and/or Artifact Binding)
 - Central login at the EO-Portal

- A user has a personal account at least at one identity provider and optional accounts on service provider level, these accounts are linked via special ids (pseudonyms) per IdP/SP pair

- The user accounts can be linked dynamically, during a user initiated web application SSO process or via offline batch processing



cmp eum usermanagement



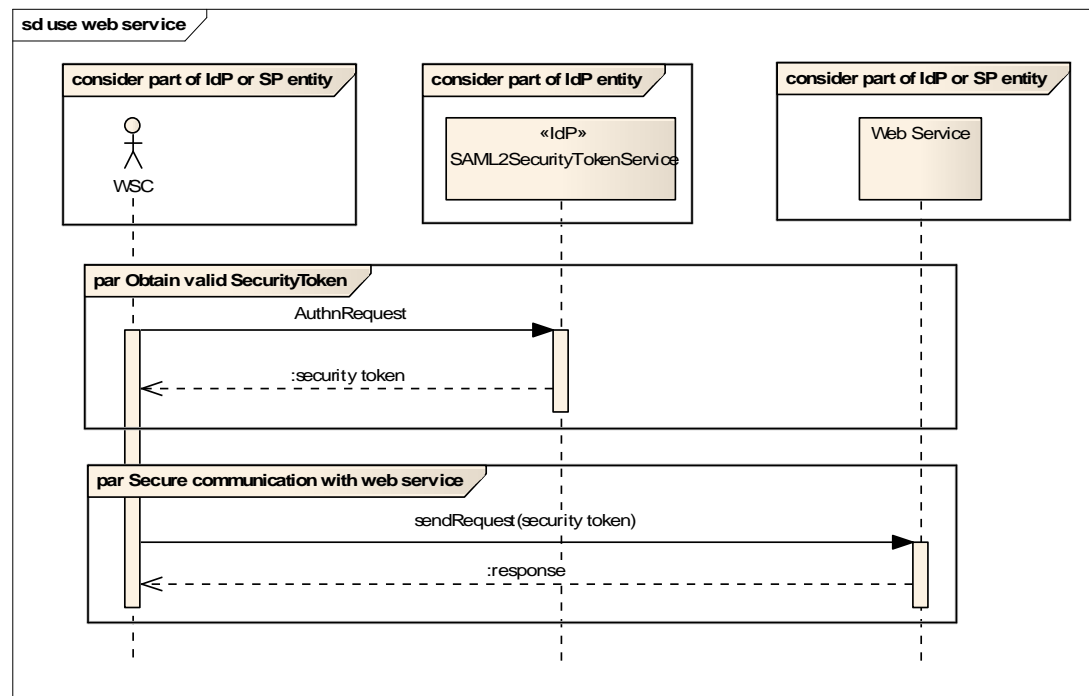
Web Service SSO

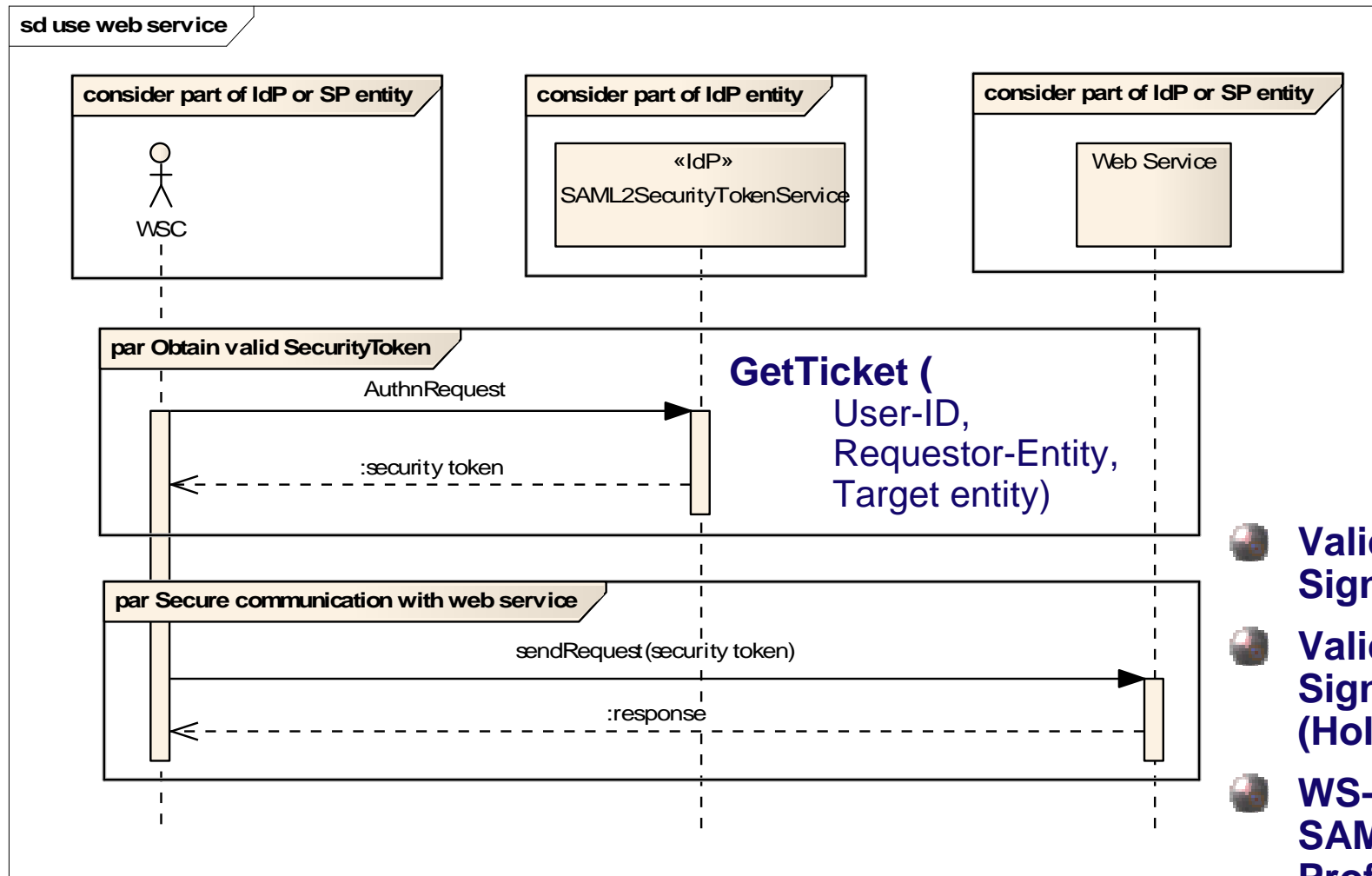
Result of Web Application SSO

- Authenticated User at a Web Service Client (WSC)

Problem:

- How to retrieve a valid security token for an user to authenticate the user at the target web service?





REST Service Integration

- Proprietary Mechanism due to the lack of official specifications

- HTTP-Header “SAML2Token”
 - base 64 encoded <saml2:Assertion/>
 - doesn't change any domain protocols
 - not visible within URLs

- Additional Request Parameter “SAML2Token”
 - base 64 encoded <saml2:Assertion/>
 - only useable if Key-Value-Pair encoding is used
 - visible in URLs

EO-Portal Supports the Specification OGC 07-118r1 User Management Interfaces for Earth Observation Services V0.0.4

- Extension of the OpenSSO Server to support the HMA-AuthenticationService interface
- Support for the HMA Security Token Format (SAML1)
- EO-Portal Services can be consumed by HMA-Clients



-
- **Based on OASIS SAML 2 and WS-Security**
 - **Identity Federation Approach**
 - **Web Application SSO (SAML2 & Domain Cookie)**
 - **SOAP/REST Web Service Integration**
 - **HMA User Management Integration**
 - **Flexible and Extensible Security Model**

 **Thank you!**

 **Questions?**

