User Management Interfaces for Earth Observation Services

OGC 07-118r1

Stresa 13/12/07

Rowena Smillie, Spacebel

Alexandre Cucumel, Spacebel

Wouter Van de Weghe, Oracle

Background

- Produced during the ESA HMA (Heterogeneous Missions Accessibility) project
  - refined during the FEDEO (Federated Earth Observation) Pilot.
- Existing specifications from W3C and OASIS are used in combination to pass identity information to Web services

- **Security Assertion Markup Language** (**SAML**)
  - OASIS Security Services Technical Committee XML standard for exchanging authentication and authorisation data between security domains, i.e. exchange between an identity provider (producer of assertions) and a service provider (consumer of assertions).

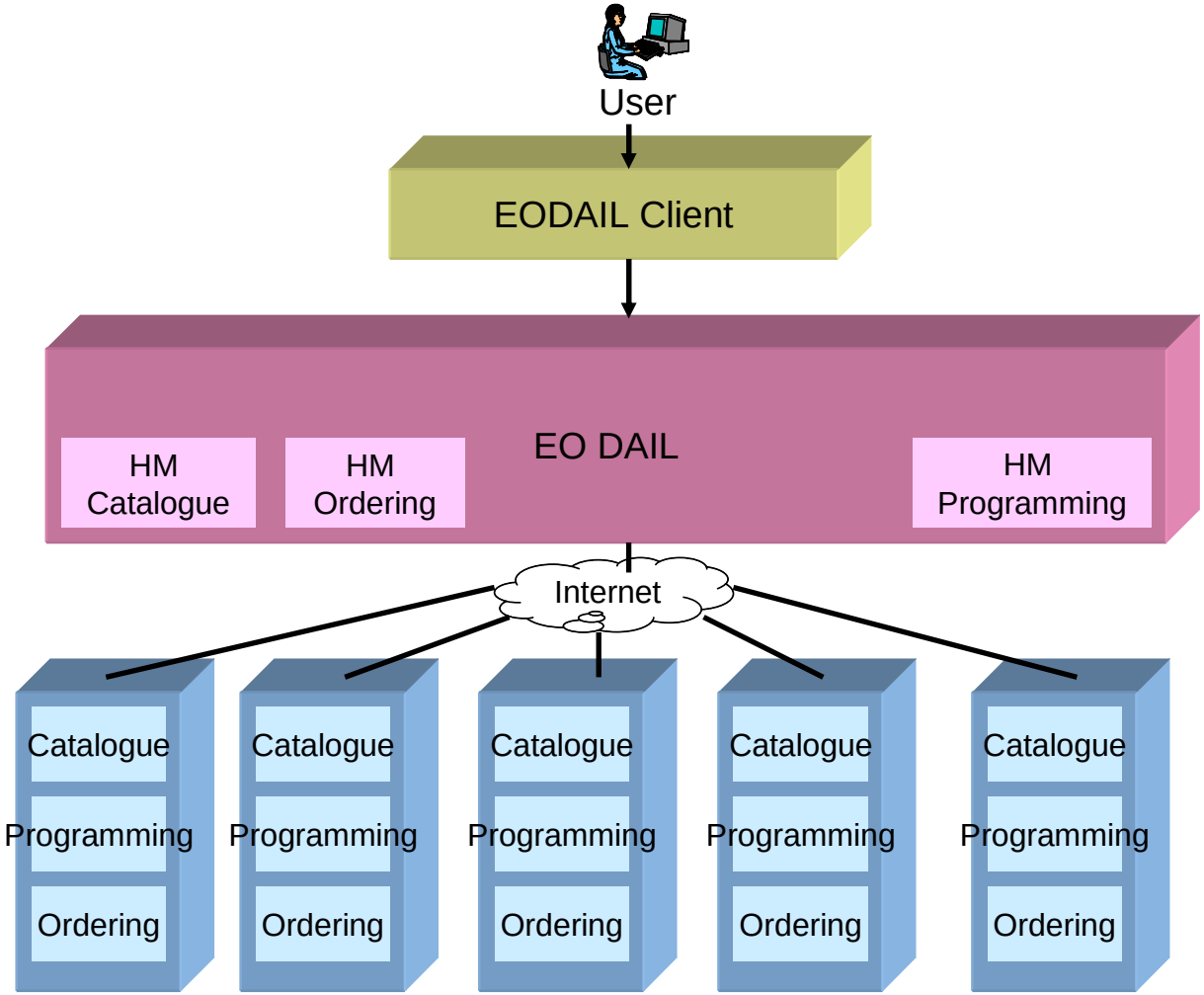
- **WS-Security**
  - **Web Services Security** from Oasis is a communications protocol providing for security of web services. WS-Security 1.0 was released on April 19 2004 and version 1.1 on February 17 2006.

Scope

OGC 07-118 describes how user and identity management information was included in the protocol specifications for EO (Earth Observation) services for:

- catalogue access (OGC 06-131),
- ordering (OGC 06-141)
- programming (OGC 07-018) in the HMA prototype.

Scope



Partner GS

Submitting Organisations

- **Submitted by:**
  - **Spacebel s.a.**
  - **ESA – European Space Agency**
  - **Oracle**
- **Comments and contributions from:**
  - **Astrium**
  - **Spot Image**
  - **ASI**
  - **CNES**
  - **DLR**
  - **Eumetsat**
  - **EUSC**
  - **MDA**

Introduction

- 07-118 is complementary to a set of specifications that describe services for managing Earth Observation (EO) data products i.e. collection level, and product level catalogues, online-ordering for existing and future products, on-line access etc.

- Intent is to describe a federated identity management interface that can be supported by many data providers (satellite operators, data distributors …),
  - existing complex facilities for the management of data and users.

Introduction

- Specify a platform and provider independent interface using existing standards.
- This proposed interface document describes the interfaces required to:
  - authenticate
  - authorise users in a federated system of Earth Observation services.

Conformance

- Conformance:
  - This will be the subject of future work. In particular the extension of the CITE compliance tests for catalogue, ordering and programming to also check compliance to the current interfaces may be considered in future work.

Definitions

- Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

- **Authentication**
  - To confirm a system entity's asserted principal identity with a specified, or understood, level of confidence.

- **federated identity**
  - A principal's identity is said to be federated between a set of Providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the Principal.

Definitions

- **identity provider**
  - A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.

- **service provider**
  - A role donned by a system entity where the system entity provides services to principals or other system entities.

OASIS SAML

- Standard for exchanging authentication and authorisation data between security domains, i.e. exchange between an identity provider (producer of assertions) and a service provider (consumer of assertions).
- SAML is required to implement federated identity and identifies two roles; the identity provider (IdP) and the service provider. These communicate through SAML assertions. A SAML assertion is an XML document containing information about how the user was authenticated and can contain other user attributes. SAML bindings are defined for HTTP Post and SOAP.
- A SAML assertion is a package of information that supplies one or more statements made by a SAML authority.
- Authentication: The specified subject was authenticated by a particular means at a particular time. A typical authentication statement asserts Subject S authenticated at time t using authentication method m.
- Attribute: The specified subject is associated with the supplied attributes. A typical attribute statement asserts Subject S is associated with attributes X,Y,Z having values v1,v2,v3. Relying parties use attributes to make access control decisions
- WS-Security SAML Token Profile defines how SAML assertions are processed in SOAP messages.

Application Domain

- Ground segment (Service Provider) components receiving Web service requests should be able to identify who issued the request and react accordingly.
  - authentication Web service (accepting a user name and password) returns a SAML token which authenticates the user to the client (i.e. Web service consumer).
    - May federate
  - service requests by the client (Web service consumer) include the SAML token in the SOAP header.
  - Each service provider accepts service requests only via a "policy enforcement point".
    - decides based on the content of the message body, the contents of the message header (including authentication token) and the context.

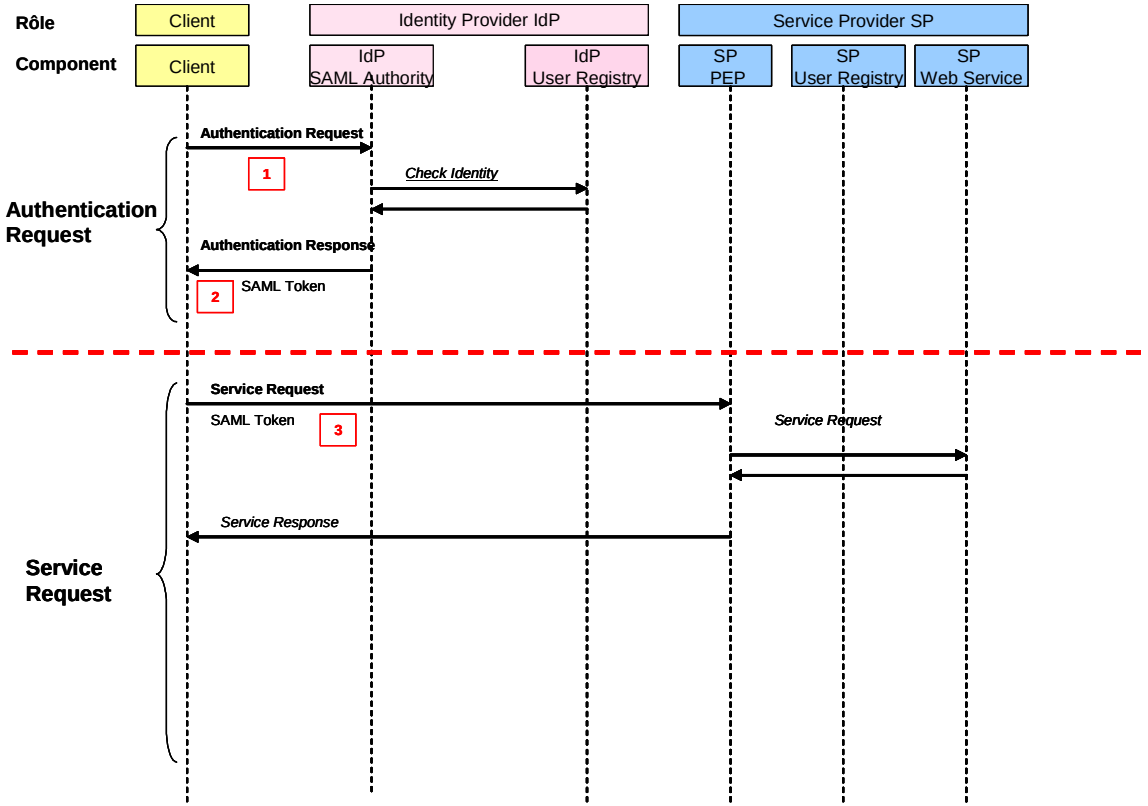
Protocol Binding

- ***Protocol binding***
  - Embedding of requests and responses in SOAP messages.
  - Only SOAP messaging (via HTTP/POST or HTTPS/POST) is be used.
  - Messages shall conform to SOAP 1.2

Basic Use Cases

- Authentication: An authentication request is first made to the identity provider (IdP).
- Authorisation: A service request sent to the service provider (SP). This service request is a call of any of the operations defined in the catalogue (OGC 06-131), ordering (OGC 06-141) or programming (OGC 07-018) specifications.
- A mission ground segment may be either an identity provider (IdP), a service provider (SP) or both IdP and SP.
- covers identity federation whereby the receiving IdP resolves the IdP and passes the authentication request to the correct IdP.
- Requests may address more than one ground segment, to perform so-called multi-mission requests

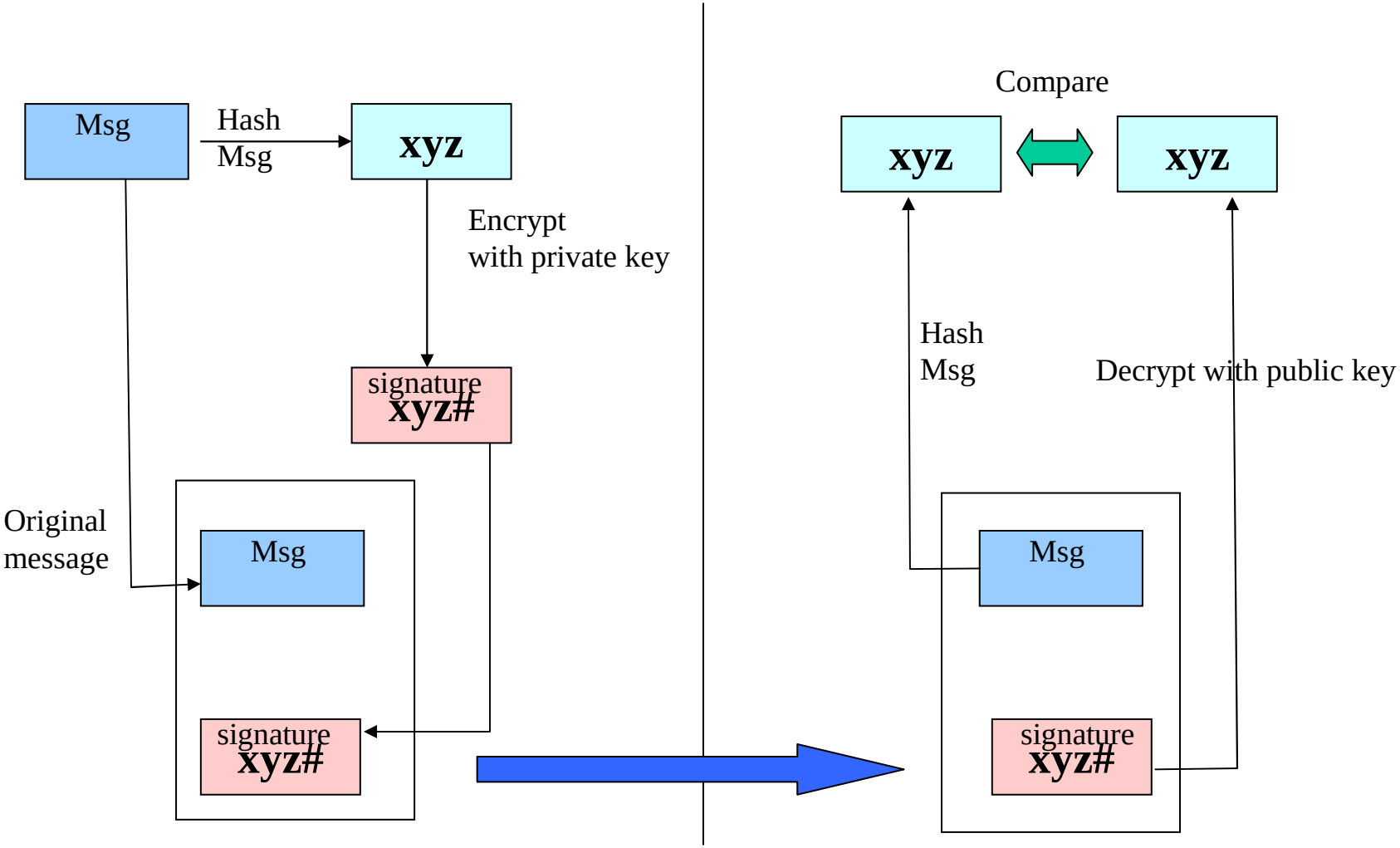
User Management Use Cases



Seurity Model

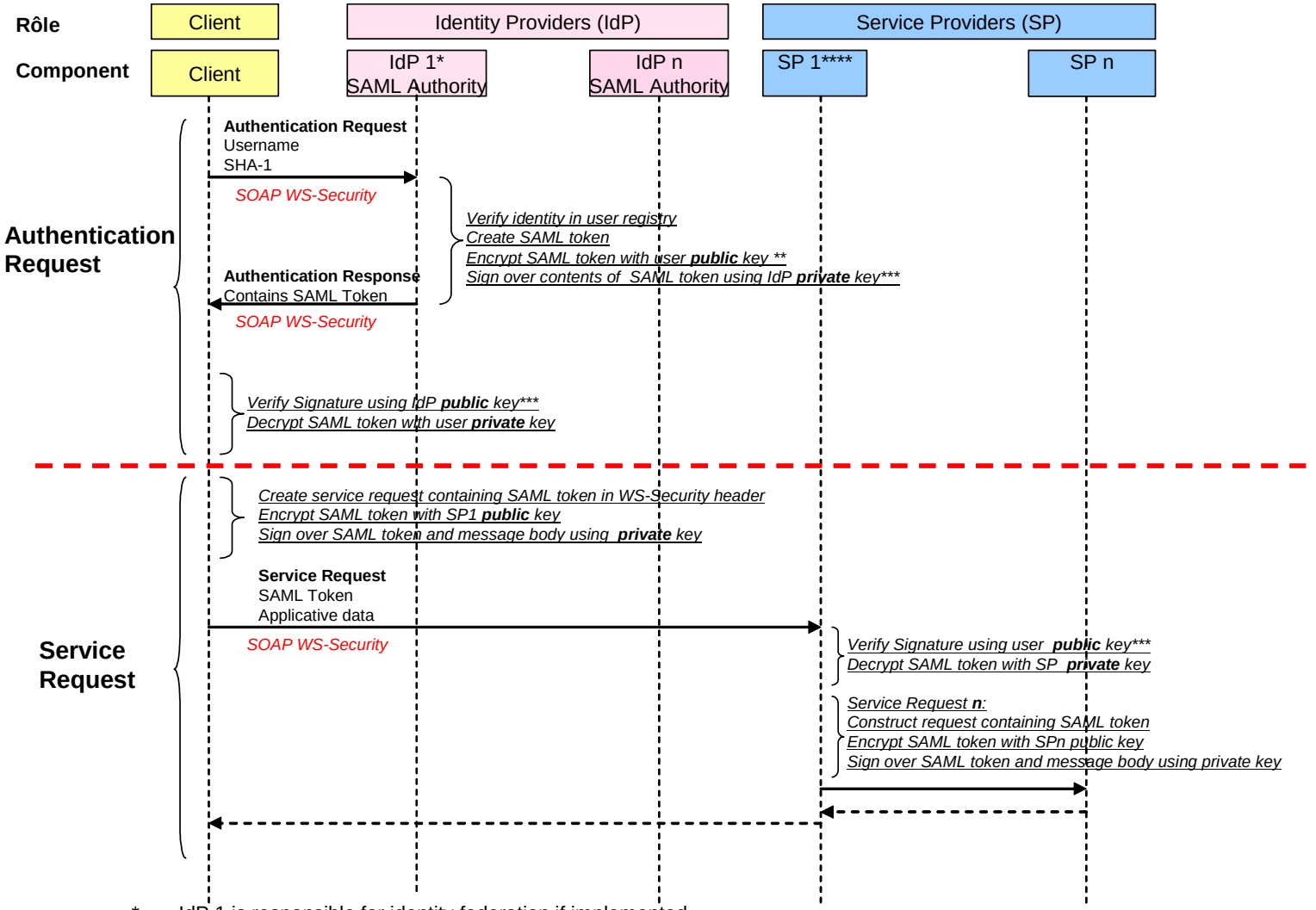
- The model is based on WS-Security SAML token profile.
- Option 1: Name and password sent in clear over encrypted channel i.e. HTTPS. SAML token returned in clear over HTTPS.
  - Used for HMA
- Option 2: Encrypted password sent over HTTP using WS-Security. Encrypted and signed response using WS-Security.

Security Model - Digital Signature



http://www.w3.org/TR/xmldsig-core/
XML-Signature Syntax and Processing
W3C Recommendation 12 February 2002

Security Model



* IdP 1 is responsible for identity federation if implemented

** Public key of user is retrieved from the X.509 certificate which the user provides at registration with the IdP

*** In order to subsequently verify the signature a user must know his IdP

**** SP 1 is responsible for workflow orchestration if implemented

Security Model

- **Authentication**:
  - Client:
    - The authentication request is sent to the authentication web service of the identity provider.
    - The password is provided as a SHA-1 hash
  - IdP Authentication Web Service:
    - The receiving authentication web service federates the identity if required and the authentication web service of the identity provider verifies the username and password in the user registry.
      - SAML token is created containing assertion of the authentication and assertion regarding the value of the subset of attributes from the minimum user profile
      - SAML token is encrypted with the user public key provided in the X.509 certificate provided by the user at registration.
    - SAML token is digitally signed using the private key of the IdP.
    - SAML token, encryption and digital signature are inserted in the WS-Security reply
  - Client:
    - client verifies the signature using the public key of his IdP.
    - client decrypts the SAML token with the user private key.

Security Model

Service Request:

- Client:
  - client creates the service request. The SAML token is put in the WS-Security header, encrypted using the public key of the service provider
  - SAML token and message body are signed using the private key of the user.
- SP Policy Enforcement Point:
  - signature is verified using the user public key and the SAML token is decrypted with the private key of the SP.

OASIS SAML

- The following subset of attributes necessary to implement the basic HMA policy steps are proposed to be included in the SAML token:
  - hmaId (unambiguous HMA identity)
  - c (Country of origin)
  - o (Organisation)
  - userCertificate (X.509 certificate)
  - hmaProjectName (names of projects with which the user is affiliated)
  - hmaServiceName (associated services)
  - hmaOperatorName (associated operators)

WS-Security

- WS-Security SAML Token Profile defines how SAML assertions are processed in SOAP messages.

WS-Security

```
<S12:Envelope xmlns:S12="...">
  <S12:Header>
    <wsse:Security xmlns:wsse="...">
     <saml:Assertion xmlns:saml="..."
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer="www.opensaml.org"
        MajorVersion="1"
        MinorVersion="1">
       <saml:AuthenticationStatement>
          <saml:Subject>
            <saml:NameIdentifier
              NameQualifier="www.example.com"
              Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
              uid=joe,ou=people,ou=saml-demo,o=baltimore.com
            </saml:NameIdentifier>
            <saml:SubjectConfirmation>
              <saml:ConfirmationMethod>
                urn:oasis:names:tc:SAML:1.0:cm:bearer
              </saml:ConfirmationMethod>
            </saml:SubjectConfirmation>
          </saml:Subject>
        </saml:AuthenticationStatement>

      </saml:Assertion>

 </wsse:Security>
  </S12:Header>
  <S12:Body>
    . . .
  </S12:Body>
</S12:Envelope>
```

Protoype WS-Security

```
<wsse:Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse
="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
  <Assertion xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" AssertionID="_3033cb9dc297af58d72cca838340b337" IssueInstant="2007-06-19T08:41:53.708Z" Issuer="http://www.spacebel.be"
MajorVersion="1" MinorVersion="1"><Conditions NotBefore="2007-06-19T07:41:53.707Z" NotOnOrAfter="2007-06-20T08:41:53.707Z" />
    <AuthenticationStatement AuthenticationInstant="2007-06-19T08:41:53.707Z" AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
      <Subject>
        <NameIdentifier>esa_sci</NameIdentifier>
        <SubjectConfirmation>
          <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>
        </SubjectConfirmation>
      </Subject>
    </AuthenticationStatement>
    <AttributeStatement>
      <Subject>
        <NameIdentifier>esa_sci</NameIdentifier>
        <SubjectConfirmation>
          <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>
        </SubjectConfirmation>
      </Subject>
      <Attribute AttributeName="mail" AttributeNamespace="http://www.oasis-open.org/RSA2004/attributes">
        <AttributeValue xsi:type="xsd:string">esasci@esa.int</AttributeValue>
      </Attribute>
      <Attribute AttributeName="employeetype" AttributeNamespace="http://www.oasis-open.org/RSA2004/attributes">
        <AttributeValue xsi:type="xsd:string">scientific</AttributeValue>
      </Attribute>
      <Attribute AttributeName="registeredaddress" AttributeNamespace="http://www.oasis-open.org/RSA2004/attributes">
        <AttributeValue xsi:type="xsd:string">ITALY</AttributeValue>
      </Attribute>
      <Attribute AttributeName="givenname" AttributeNamespace="http://www.oasis-open.org/RSA2004/attributes">
        <AttributeValue xsi:type="xsd:string">esaScientificUser</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</wsse:Security>
```

WS-Security

- SAML can be encrypted content within <xenc> element of WS-Security
  - Helps to ensure that only the target service can read the message – However:
    - Can't be sure that the message came from a trusted client.
    - Depends on how many people know the "encryption code"
    - Does not prevent someone from changing the message content.
- SAML used with XML signature <ds:Signature> element of WS-Security
    - Sender : Hash and signs (encrypts the hash code)
    - Receiver : Hash and verify hash (decrypts the hash)
    - Ensures that the message was sent by a known client and that the message arrived intact.
    - Include a timestamp in the signed message to prevent replay attacks.

➢ *Authenticate*

- The Authenticate operation allows clients to retrieve authentication metadata from a server. The response to an Authenticate request should be an XML document containing authentication metadata about the authentication and requestor.
  - **Request**
    - Protocol: SOAP over HTTPS
    -
    - <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
    - xmlns:xsd="http://accessGate.spacebel.be/xsd">
    - <soap:Header/>
    - <soap:Body>
    - <xsd:authenticate>
    - <xsd:username>acl</xsd:username>
    - <xsd:password>*******</xsd:password>
    - </xsd:authenticate>
    - </soap:Body>
    - </soap:Envelope>

➢ *ServiceRequest*

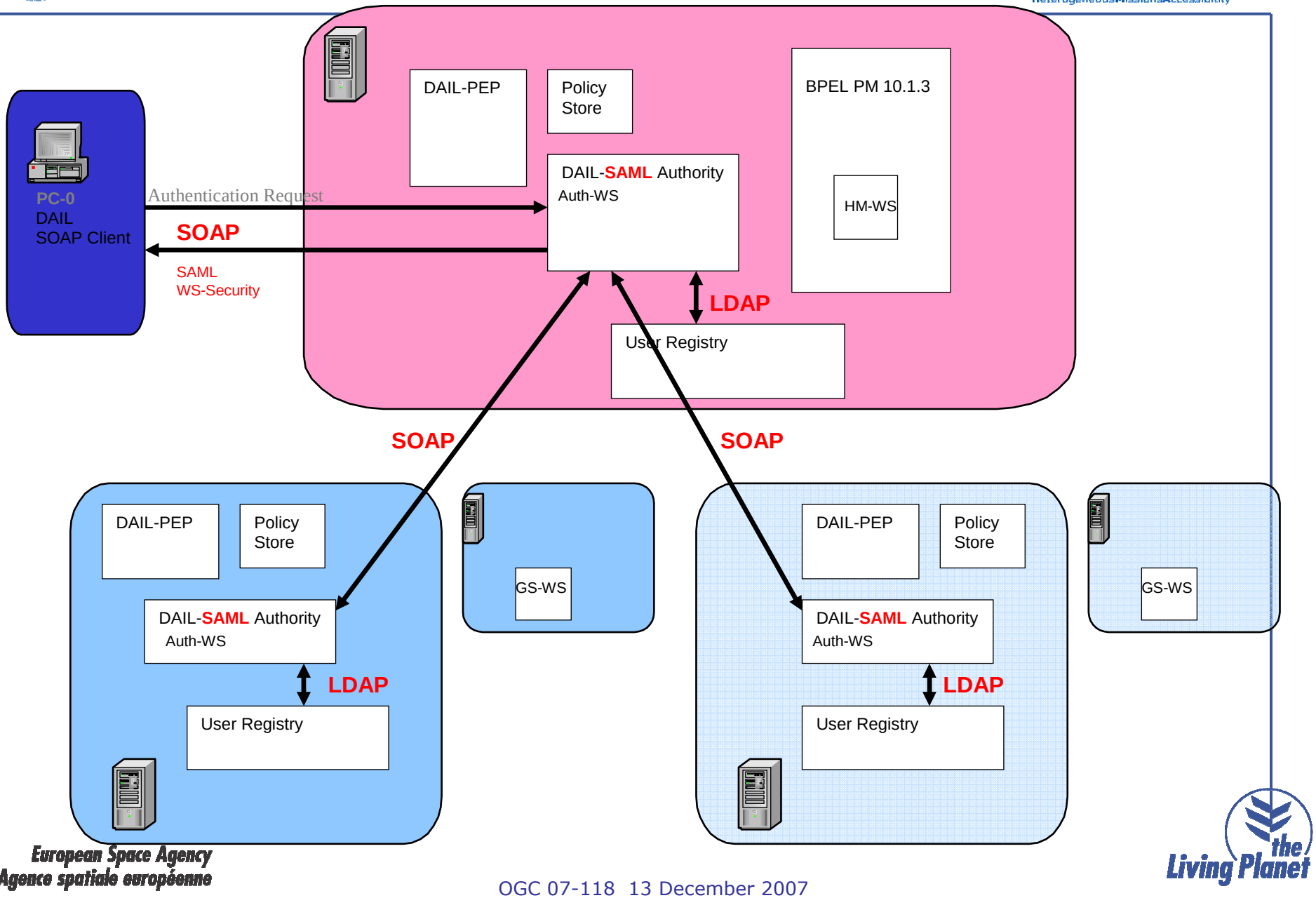
- Through the implementation of this interface to the ServiceRequest (i.e. the service operations such as the catalogue GetRecords, the programming GetFeasibility etc.) authenticated clients will send requests to a server controlling access to the final service. The request is made using WS-Security containing the SAML token previously returned in the AuthenticationResponse.

- Protocol: SOAP WS-Security over HTTP.

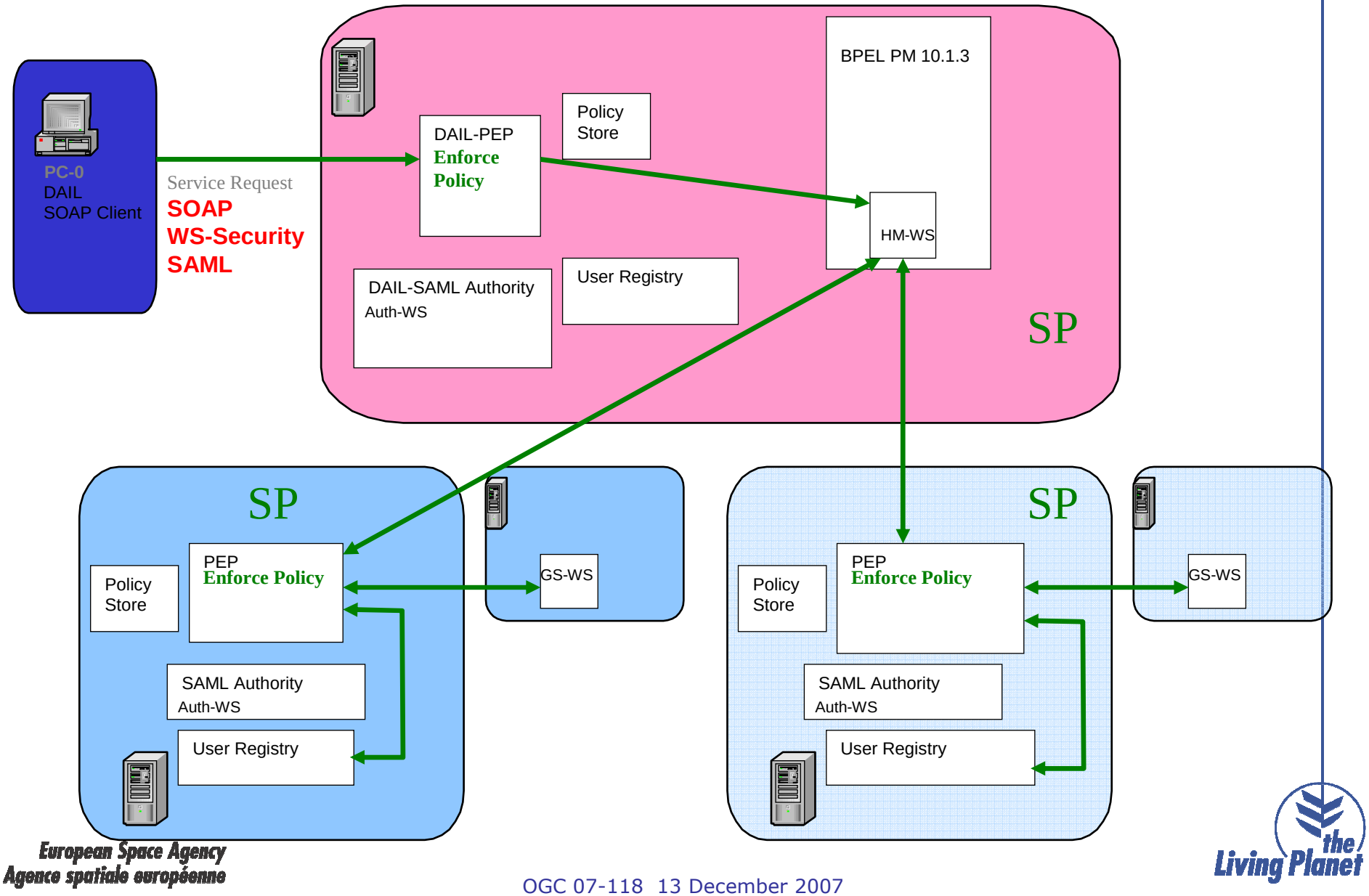
Prototype

- Challenges
  - User Mgt for Heterogeneous and distributed environment
  - Support multiple scenarios
  - Fit in a Service Oriented Architecture
  - Scalable
  - non intrusive
  - respect data protection and privacy laws of each country
  - Ensure that resources are not used by unauthorised entities
  - Ensure message confidentiality
  - Ensure message Integrity

User requests authentication



Authenticated user requests HM Service



Architecture - Challenges

- Challenges
  - User Mgt for Heterogeneous and distributed environment ✓
  - Support multiple scenarios ✓
  - Fit in a Service Oriented Architecture ✓
  - Scalable ✓
  - Installation must be non intrusive ✓
  - Installation shall respect data protection and privacy laws of each country ✓

Architecture - Challenges

- Challenges
  - Access Control ✓
    - Ensuring that resources are not used by unauthorised entities
      - Authentication
      - Authorisation
  - Message Confidentiality
    - Ensuring that information only accessible to authorised entities ✓
  - Message Integrity
    - Prevent modification of data ✓

Thank you