Open Geospatial Consortium Inc.

Date: 2009-06-30

Reference number of this OGC® project document**: 07-118r1**

Version: 0.0.4

Category: OGC™ Interoperability Program Report

Editors: R.Smillie, A.Cucumel SPACEBEL s.a.

User Management Interfaces for Earth Observation Services

Document type: OGC™ Interoperability Program Report
Document subtype: Candidate Implementation Specification
Document stage: Draft
Document language: English

Contents

Figures

Date: June 30, 2

i. Preface

This document explains how user and identity management information is included in the protocol specifications for EO (Earth Observation) services for catalogue access (OGC 06-131), ordering (OGC 06-141) and programming (OGC 07-018) in the EO DAIL and HMA operational interfaces.

The document was initially produced during the ESA HMA (Heterogeneous Missions Accessibility) project and refined during the FEDEO (Federated Earth Observation) Pilot. It is further refined in the ESA EODAIL Implementation project.

This document is not a new specification, however, it describes how existing specifications from W3C and OASIS can be used in combination to pass identity information to Web services some of which are based on OGC Best Practice specifications.

ii. Submitting organisations

The following organisations will submit the original document or its revisions to the OGC™ Security Working Group.

- **Spacebel s.a.**
- **ESA – European Space Agency**
- **Oracle**

The editors would like to acknowledge that this work is the result of collaboration and review of many organisations and would like to thank for the comments and contributions from:

- **Astrium**
- **Spot Image**
- **ASI**
- **CNES**
- **DLR**
- **Eumetsat**
- **EUSC**
- **MDA**

Note: this does not imply a complete endorsement from these organisations.

iii. Document contributor contact points

All questions regarding this document should be directed to the editor or the contributors:

Contact	Organisation	Email
Rowena Smillie	Spacebel	Rowena.Smillie@spacebel.be
Alexandre Cucumel	Spacebel	Alexandre.Cucumel@spacebel.be
Wouter Van de Weghe	Oracle	wouter.van.de.weghe@oracle.com

iv. Revision history

Date	Version	Editor	Sections modified	Description
15 September 2007	0.0.1 Draft	R.Smillie	All	Initialised Draft Document.
23 April 2008	0.0.2	R.Smillie		Updated in line with EO DAIL implementation project
07 Feb 2009	0.0.3	R.Smillie		Updated in line with EO DAIL implementation project SOAP version changed to 1.1 Authentication request does not use WS-Security Message examples added Encryption and signature descriptions improved

30 June 2009	0.0.4	R.Smillie		Updated in line with EO DAIL RID PRE-AR2#34: • Namespace in encrypted message example corrected to http://earth.esa.int/um/eop/saml <http://earth.esa.int/um/eop/saml> • decryptandCheckSignature removed from authentication service • authenticating identity correctly asserted in examples • authenticate and authenticateFederated merged into one operation • Attribute assertions updated in examples • WSDL provided for authentication service • Clarification made for the assertion element and schema attached • All schemas and references given in annex.

v. Foreword

This document, through its implementation profile, references several external standards and specifications as dependencies:

1. The Extensible Markup Language (XML), World Wide Web Consortium, http://www.w3.org/TR/1998/REC-xml-19980210
2. Simple Object Access Protocol (SOAP) Version 1.1 W3C Note 08 May 2000 , http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
3. WSDL, Web Services Description Language (WSDL) 1.1, http://www.w3.org/TR/wsdl
4. SAML, Security Assertion Markup Language 1.1, OASIS http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
5. WS-Security Web Services Security 1.1, OASIS http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open GIS Consortium, Inc. shall not be held responsible for identifying any or all such patent rights.

Introduction

This specification is complementary to a set of specifications that describe services for managing Earth Observation (EO) data products. These services include collection level, and product level catalogues, online-ordering for existing and future products, on-line access etc. and are put into context in an overall document (see HMA Architecture Technical Note [NR13]).

The intent of this specification is to describe a federated identity management interface that can be supported by many data providers (satellite operators, data distributors …), most of whom have existing (and relatively complex) facilities for the management of their data and users. The strategy is to specify a platform and provider independent interface using existing standards.

1 Scope

This proposed interface document describes the interfaces required to authenticate and authorise users in a federated system of Earth Observation services.

2 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.

3 References

3.1 Normative references

[NR1] W3C Recommendation January 1999, Namespaces In XML, http://www.w3.org/TR/2000/REC-xml-names

[NR2] W3C Recommendation 6 October 2000, Extensible Markup Language (XML) 1.0 (Second Edition), http://www.w3.org/TR/REC-xml

[NR3] W3C Recommendation 2 May 2001: XML Schema Part 0: Primer, http://www.w3.org/TR/2001/REC-xmlschema-0-20010502/

[NR4] W3C Recommendation 2 May 2001: XML Schema Part 1: Structures, http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

[NR5] W3C Recommendation 2 May 2001: XML Schema Part 2: Datatypes, http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/

[NR6] W3C Simple Object Access Protocol (SOAP) Version 1.1 W3C Note 08 May 2000 , http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[NR7] WSDL, Web Services Description Language (WSDL) 1.1, http://www.w3.org/TR/wsdl

[NR8] IETF RFC 2119, Keywords for use in RFCs to Indicate Requirement Levels, http://rfc.net/rfc2119.html

[NR9] WS-Security, SOAP Message Security V1.1 http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[NR10] SAML, Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[NR11] Web Services Security SAML Token Profile 1.1 http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

[NR12] Secure Hash Standards (SHA-1) National Institute of Standards and Technology http://csrc.nist.gov/cryptval/shs.htm

[NR13] HMA Architectural Design Technical Note version 1.6, 13/06/2007 http://services.eoportal.org/portal/system/HelpUI.jsp

[NR14] 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

[NR15] Java Cryptography Architecture API Specification & Reference

http://java.sun.com/j2se/1.5.0/docs/guide/security/CryptoSpec.html

[NR16] OGC 04-016r5, OWS Common Implementation Specification 2004/12/17

[NR17] XML encryption http://www.w3.org/TR/xmlenc-core/

[NR18] XML signature http://www.w3.org/TR/xmldsig-core/

[NR19] Apache XML Security http://santuario.apache.org/Java/index.html

3.2 Other references

[OR1] HMA Operational Scenarios Technical Note HMA-TN-ASU-SY-0001 http://services.eoportal.org/portal/system/HelpUI.jsp

[OR2] HMA-TN-SIE-EN-003 GMES Minimum User Profile 1.0c

[OR3] EO-DAIL User Management Specifications

DAIL-RS-ASU-EN-0002 1.1

[OR4] SOAP Version 1.2 http://www.w3.org/TR/soap12-part1/

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

4.1.
Authentication [NR14]
To confirm a system entity's asserted principal identity with a specified, or understood, level of confidence.

4.2.
circle of trust
A federation of service providers and identity providers within which service providers accept the authentication asserted by the identity provider.

4.3.
client
software component that can invoke an **operation** from a **server**

4.4.
external entity

This is the entity external to the DAIL owning the protected web service. For the EO DAIL project it is the various ground segments that perform this activity. The external entity can be both an identity provider and service provider. There can be many external entities.

4.5.
federated identity [NR14]
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.

4.6.
federating entity

This is the entity performing the federation of the identities. For the EO DAIL project it is the EO DAIL that performs this activity. The authentication request always passes through the federating entity. The federating entity can be both identity provider and service provider. There is only one federating entity.

4.7.
identifier
a character string that may be composed of numbers and characters that is exchanged between the client and the server with respect to a specific identity of a resource

4.8.
identity provider [NR14]
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.

4.9.
interface
named set of operations that characterise the behaviour of an entity [ISO 19119]

4.10.
operation
specification of a transformation or query that an object may be called to execute [ISO 19119]

4.11.
parameter
variable whose name and value are included in an operation **request** or **response**

4.12.
PEP
Policy enforcement point.

4.13.
principal [NR14]
A *system entity* whose identity can be authenticated.

4.14.
request
invocation of an **operation** by a **client**

4.15.
response
result of an **operation,** returned from a **server** to a **client**

4.16.
server
service instance
a particular instance of a **service** [ISO 19119]

4.17.
service
distinct part of the functionality that is provided by an entity through interfaces [ISO 19119]

capability which a service provider entity makes available to a service user entity at the interface between those entities [ISO 19104 terms repository]

4.18.
service interface
shared boundary between an automated system or human being and another automated system or human being [ISO 19101]

4.19.
service provider [NR14]
A role donned by a system entity where the system entity provides services to principals or other system entities.

4.20.
transfer protocol
common set of rules for defining interactions between distributed systems [ISO 19118]

5 Symbols and abbreviations

5.1 Symbols (and abbreviated terms)

Some frequently used abbreviated terms:

BPEL Business Process Execution Language

DAIL Data Access Integration Layer

EO Earth Observation

HMA Heterogeneous Missions Accessibility

HTTP HyperText Transport Protocol

IdP Identity Provider

ISO International Organisation for Standardisation

OGC Open GIS Consortium

SAML Security Assertion Markup Language

SOAP Simple Object Access Protocol

SP Service Provider

URI Uniform Resource Identifier

URL Uniform Resource Locator

URN Uniform Resource Name

WSDL Web Service Definition Language

W3C World Wide Web Consortium

XML eXtensible Markup Language

5.2 Document terms and definitions

This document uses the specification terms defined in Subclause 5.3 of [NR16].

6 System context

This section documents special requirements and describes the context of use.

6.1 Application domain

Web service requests are received by service providers (Ground segments). These service Providers should be able to identify who issued the request and react accordingly. The following approach is proposed:

1) An authentication Web service (accepting a user identifier password and optionally his identity provider) returns a SAML token which authenticates the user to the client (i.e. Web service consumer). (This authentication web service may federate the identity to another identity provider for authentication. At the interface context this is transparent, the federated identity request being identical to the initial request.)

2) Each subsequent service request by the client (Web service consumer) should include the SAML token in the SOAP header as described later in this document.

3) Each service provider accepts service requests only via a "policy enforcement point". The PEP decides based on the content of the message body, the contents of the message header (including authentication token) and the context (i.e. applicable policies) whether to accept or to refuse the service request or reroute it.

6.2 Protocol binding

To provide an overall coherent architecture within this context operations shall support the embedding of requests and responses in SOAP messages. Only SOAP messaging (via HTTP/POST or HTTPS/POST) with document/literal style shall be used. Messages should conform to SOAP 1.1 [NR6]. The message payload shall be in the body of the SOAP envelope. All authentication tokens shall be in the WS-Security element in the header of the SOAP envelope.

6.3 Libraries

The Santaurio Apache XML security Java library [NR19] has been used to implement the examples given from the DAIL implementation project.

6.4 Basic use cases

The use cases covered by this specification are shown in the following sequence diagram:

- 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 but is not limited to these. The service requests can be synchronous or asynchronous via ws-addressing. This is transparent for the current specification.

A mission ground segment may be either an identity provider (IdP), a service provider (SP) or both IdP and SP.

This specification covers identity federation whereby the receiving IdP(federating entity), if not the IdP for the request, resolves the IdP and passes the authentication request to the correct IdP.

Authorisation requests (service requests) may address more than one ground segment, to perform so-called multi-mission requests, these requests are orchestrated by a BPEL workflow.

The policy enforcement on the SP is non invasive meaning that it is independent of the SP implementation.

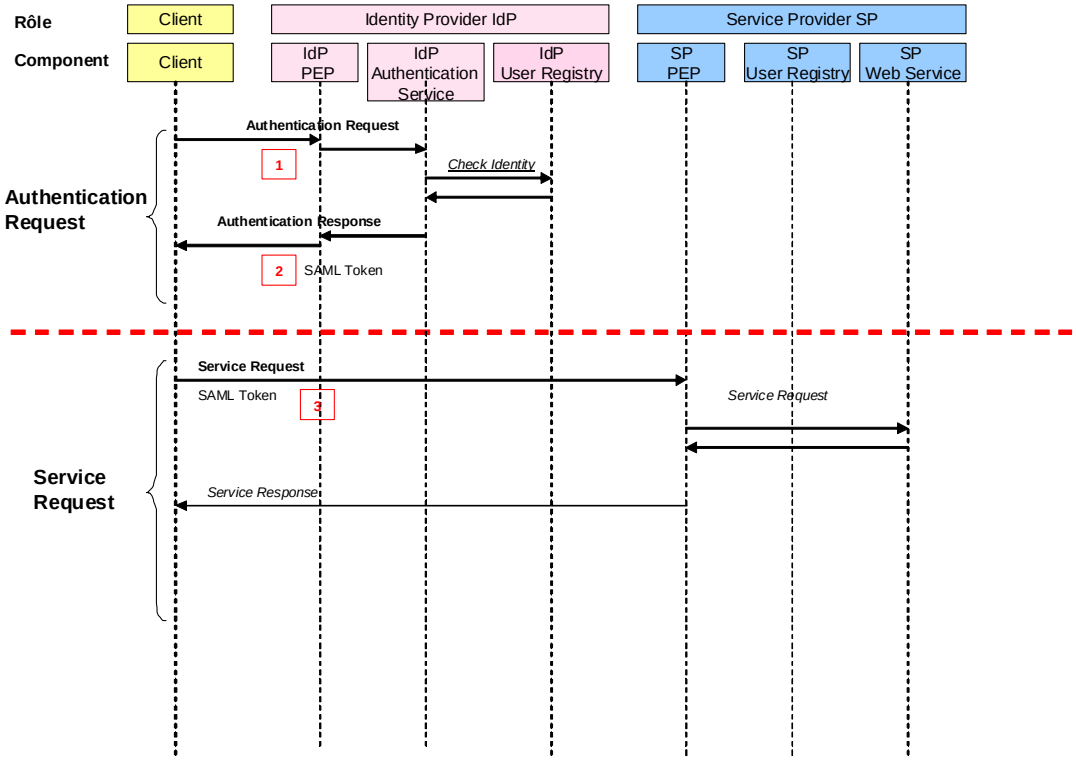

Figure 1 User Management Use Cases

The high level use case for authentication and authorisation is shown in the above figure. Following sections of this document further elaborate the detail of the authentication and authorisation.

1. The authentication request is sent by the client to the authentication service which in the DAIL is directly exposed as a web service and does not pass through the PEP. However, if required a request could equally be intercepted by the IdP PEP and routed.

2. The client receives the authentication response containing the SAML token

3. The client then sends a service request i.e. an authorisation request. This request contains the SAML token.

6.5 Security Model

The model is based on WS-Security SAML token profile [NR11]. The authentication request contains the name and password identifying the user plus an optional definition of the designated identity provider.

User credentials are sent in SOAP over an encrypted channel i.e. HTTPS. The signed and encrypted SAML token is returned as SOAP over HTTPS. The client is unable to decrypt the content.

6.5.1 Encryption

Encryption of the SAML token is performed by the authentication service during an authentication request and response. Decryption is performed by the PEP during the authorization request. The encryption algorithm used is the AES-128 as defined in [NR15]. The encryption process is as follows:

- The authentication service first creates the symmetric key using The AES-128 encryption algorithm.
- This symmetric key is then itself encrypted with the public key of the IdP (i.e. GS) using the RSA encryption algorithm to create a secret key.
- The SAML token is then encrypted with the generated secret key using the AES-128 encryption algorithm.
- The message is then built.

Example Authentication Request:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:q0="http://earth.esa.int/um/eop"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
      <q0:authenticate>
         <q0:username>TestUser</q0:username>
         <q0:password>TestUser42</q0:password>
         </q0:serverName>
      </q0:authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

Example Encrypted Authentication Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Body>
   <ns:authenticateResponse xmlns:ns="http://earth.esa.int/um/eop">
     <ns:return>
       <Assertion xmlns="http://earth.esa.int/um/eop/saml">
         <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Content">
           <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
           <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
             <xenc:EncryptedKey>
```

```
               <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
               <xenc:CipherData>

<xenc:CipherValue>cbE8viFOmyDuxR8N4EdwS9UUKpSoUbMrWSVprW7IypMwFZLeHR9Rxd4iw5
dUl4K+TffyNdRJ9Tr9PD8YIdpFLzCvYas63g5x4/XnyA1E2AU8ZBBpM2dtbr3g4IYMywfraWrI76
mHM+MERVZdHMVBWFrhqXhcS92m23m+amt14mk=</xenc:CipherValue>
               </xenc:CipherData>
             </xenc:EncryptedKey>
           </ds:KeyInfo>
           <xenc:CipherData>

<xenc:CipherValue>VEHlprDMQ+DqIpoPqx6TYi/mMX2dGV5JCJCrhDquZHRKqOiaIFfwqOMZvn
2HW2JDFvUxJ6LRTKdNujQI7sxc6h3IGBL7NXF7bx4jGwQ09wAA7nm6OoB4jiGdaqb8wTx0olnzn2
WqOWoVeTng1lwBi0rv2+iD1HWnXAUUHfJH8ALq4IU3hR0vjoqJH6Y21EuXPeXp/dYPUw3oIFn2FE
ID2u+8T+xOxbbq2ezQbU3z8n1LbgvDtN3ex5lUCo260pOOPn92nn7nYErT682eYd+bCKoiENpQSY
gHszvvyqFf9o6O0u87zk4AORWsRhQH74L2gG8wVOeHKyhEx0RsBkf4xZcQKBvQ9JHWQWpDEB51NZ
aJe1hSyaUk6T5gf9ArDnz6UwL0ZTDp6Dxgjha91u5qIMG3ECxVYKcnBv+O6Om1Q0HbL0ecbUDR56
evS+mf0U9JxduBKwFJLqta6D0wmwqYWcaF3ZrKd7SatV8Z2l0DmWTMe5R+x6O1RpbKltlduKl4bL
aSYFpaqaU758ZsmTDmjQQj8fn1qCZbDtp4SEVPWumoTg2k7RAOay2QtV5b+VA9wloSXoxVf2csLS
OOH/NDE1noBIpzgUb9Xm/YIPwikQKsxNPFM72yLrS0vjAho1Cxrg+8l7XIVcmowhPnLqSs6ZpvA0
1YP8EhsOFlN+0y+9EfAuoY4jYcScfwqDehth76lER+EyAdFLi10VhVxKW14VLbmksAydndIQaw6V
zGm1Qwoc3CeCaeq4q4GgFgiem1BmW9IeBaUBTX2wZmIKG8Z9Xhjv6MwT7hOeWH5fefipJs8JS8l6
wQBo8WAczzmw6s1j8JW9YDyAWosfoTPrtOwFTaaYSiaEXvPOnb5RgR/W4ivZ64ioA8FXyLFoWcNE
JJ6AgWHDLAbCDg/zvnVwEs7OdaSxRTxVNsc7cpclGspSmk/HzGYxPHInGhn/QPsac5iN6t6HlwnQ
UJgt81rI/tbFfSYqqtYqXKeNoEtw91/1DZVUi7mSc7Xj2e2Wb65h8PIoYeX3Nli+i4SrOoeAKaZr
HtpqP6f+pI4lpkANS4RFxFDiL9Ddxv1WKD//nMck0Su0HfIbPYUYF0GGvlHsv6IiwT8dj/f0MnCx
kAgegliGageZthQiNavOcURRC/94d+1jDZGayowurzdxmJhxyiEY5REQQt3hK4aAD89wMjndzxHd
tcQEuvXA5uSm3T9qgIm4Qdvuh54PW/SKptG9fDj4paTxVVlfZ+0f/1Vxjj4pPIKOVjE3e4ChBPkJ
XD/nXqZ8DdR+zPxOLWYyiqnMaxv3OInd/Iz2Lq36a09b0JEfMVz4e39sGtFzNDbxXgQnTx4L3jDY
Fdl5+gelUNduK9HtgklXDWfNIMWtY5xhdTX0m3Q8hBtNgKOHeg7BcBXF+uT30mqwgJu5cbJQl/1j
/QlMvromUaUQATN2ULu7mMiTWkoYoMTiijJGAizbKIi6O5xmHvF/jicd7lBcmSz+B+BnrnqxY5DM
/qQSFsnRoGmPKlJeiao2g+QuMD5x7H+pBUIq3B8lkMlUBg5VoKx2+kCHuP2lamGFskQl80PRGygQ
5adA2iWwKoIKoCdcYIc9C2sPVkJz+slExJXizl4L51GEWDlQ8VGsqNV7CzOyIt0uXIIBQW3j0aX/
/7QoYVfM681TiqvtaDEY7Ip4nSV839e5xnj3s+qgzXOpoK5rw5EThDLhthPy97CJiuSbsfcGf1Dv
WNE74x2E4b8HazacItRBIbx0GFDHIoqaHEih6zlhQaqwloLnUHRpL8vAQLVKiW3q94569e3GenoQ
bpjxKQ9F58VuQh3ZiZtJ+17XOxDx6ZDXcTiQDa+3nXiTgT7k9gGtpIv8vYLMuUHDEZx1zGd/rMzU
3JAbbfKO8+Cs3pMnb2KpGL4rLLgivee1P35rbHK04V8D0NbwDk0TOVnmFQWIRsgVtPwmEHXbFl3j
qIUTx4xdishXmkKcDCwaNfqYo4yzmgLUlbtchkDGF9YBA0mXv4gT7z0TiBb1jUFBhTnciL4DBkI9
K8wEjklHUi7w4LjvhCB5B15y1ZG/baIscoRrVu41HUp7crwbsdKjcWGE//dBTXN1vrXDm0maAkCo
nuYNPpMY0Cf+ikVITJO73UaXplFjOOtm+mkql6e5nTd8qGQXwHZl/nGJOEO/rMsXSoVybxIn5bg+
97CFCtAdsRRjAJZRQcrJIztenGJX81U0rvAX+OuoSNrgVpdxcwuH/1x80i+CY5kdUkg3EMkU0m4F
iNQ6CyXiiimVSBRB0sHfWW5/Em+qlYeRjrXCyJBYPo2mCuMtqQN42VeShEkQ1XPx6o09NTaaxXRM
pV2IHjzALLrR0Px6zqbp7CuEhPdLxTYcXetDKQJt/XHJuWdvETMgsJnyQ0cCJSPXp21xsrK6zYLY
cQ1M8rS9RHCmWvFdTZg49mX3QPANOUDPoPR0y3mOT19FWKFYOfQhHN2xPJZAPV6ZJeReeAeTBRkT
vgIJE/3BsQpmqsSusjgEDYCrK8MfaybAC6CpE5ZKnQwV99YlTcbPx7vVKPuU13j3Aj4FjtGjkFun
fCOpLX1AA0FSbBfOOCVeYd94bCGaW8f+j3NBB+29ELYMskew2tyCBiw2HodBrMoDiYVWHbD+bWw8
qMOOBurEQihVdNq5Tbi3R2fnnX9DpfbVljJeKFjyVwCLZA5OdGIYPuJxrXGKsaBI+abTgciL4n4W
bsG7LalURKCMe/HH1jVuy8VjevwJMB+u7CHoOc9jVCwR4YSPjH9fbxcIn9UIuECm1CryEUYB6kkh
BEeyxdQclP0amPYlyxVU80KN+Mxvle4//B6kwUtjS+/Rv943oXrXxaLXTCpeds49x0FWSRo/HCxy
nunzpkyqD4wBfUyB7hYggeRUaCb7aNVuIB1QZSY9EqF3F26Aootz1cYpr1CBtizZK9Q6Ez6N3iYW
1dMUB7dsNp4a4emAU3CfhHYh3JNv4pD21PbPASO/t89v7uMDrsI8SOp1nHqV0hYG2+JhxNyhYKV1
oXv54mKzbW+4vwsU/ySrrexUvmkTzLCsYBI7nSZT5uVprRA+MQJBLx6dKVVuzO1x8hzTv9T2LvJr
7rpd6Ban94JJ8vG7OUO0OaNP9HDrz+34xmCqQRi/f0TkmfSo4uFcsIfAmdQVbd6uu22ZBoWqolaz
lBXjt5Oe2AQV51Zma53dlArSBLpvbg/RoMM7cMhnGn33DkSBDYU9rN2iApw0zswa/KJ/p1r33Jrk
5YTL6wTTEuaG+UxVrtCxX4VHk7syaOjI5dshRELos3ZeIJeqKAgS45H6cK+gjCq0l3qWDDnFHcGm
zYoP1665lC7c9TOs8i5OBLM6hGqgEgcKEiTIp+tRUvDEhyN1v/YngT3izvWbsijV0QTTJcjsyFWq
DSJiw8G1WH4oFqZAzF2UzE6fzEeQbMVlPPxlnpUjipTqdtWcuayLH7tifX7diBl1fjlUOTqPK2+5
vz1HckVtzJMS4g0W7rWHAbTv5nfrby/1IJBHMDutjI2dh6J7nXbSgFOiT98TFL7upJCNc7T3AH4j
Ro1TzzXqODFShamQeYlooCyvStQxqj08rz74+7ery+GapNEPL4cPZ1qV0bfKCBwOQrTV8lIZXsFt
Jj9TV+7lT6ZcePnCFY6pWI78u5WWePZunmI9FFhz+odZd4vfh0C3VEISmeEN28T8XdvtHt8A78sr
4/SmrPteZpZhByZe2n50ZHQU+ukncDgZirtz5A4LIBedcDLCgeNfonHYCQTNYOKoDA+eq5sBczKP
mqFKjPnBq1533/lptWhsgou8CZfsEaY4kZvEzK8YTVrfVt4T407A851vKxBfHIyXKxFFi17Yddr2
SiqebAUjT3waPAoUwgdJelDYTnnKUQy0Zm25gGRDiE9LUwoOp7ys0H9m/xXJROx76gbljguU3ad9
fcwQIm8RTKZvXvKrVRBUsHutEL6/qZAb5VBQ1JHsa4tknAFTdwh7lsB1/l0lHtZ+HzBdgZ8kOvRm
HiCKYb+2p26WMVNy8SRhW8EeYxx3t79LMU3pIp9w4rCnuClwAYAXN6PP1Gf5GgsGS228ur3vwNKO
8YZIdMatmKJDy8Ufkm1Ljvy4Z0/3+XcGLDWyxRx6M2mLvMPvJIz9iGSr684PRfSydR3nq6W7gwYc
```

```
Ohb62cmSLVWyECoaa+cqVFFGOKHcUT3ZS7Xlx0QkniCQI9d46XDEx64PFGeBXL/z4dj7ZYx6woX9
R+F5yOAdKoILV5N9m4xzauPO4EkmKakDBtsf9tzExrArDBoT664Xc7cVJ/2jTzX57Oms09Q7r+T8
hH0JNxhcXAqhxdbMitkcFSy7t0pBgrPXRhdXohbGlhuZPAOMVkWWDMf8x7Yc4k7F3l9ua67w5Z2Q
cDf8NBq5iYM3TkB+2qpmn16L7Pbp5qlAoIcB409+6VwxHiHQgBHOPGsP1xHNYGYyKcfR4VxaUUXf
5G18b5NOnx3S2VCBA9fJGXlHqW3RmtlMEP4dEQdCbhH7jw7jd5El0NabRA0fCBTAYR61vYa9Ov7S
DOIefy6NpDffg9sFltOa36ag==</xenc:CipherValue>
           </xenc:CipherData>
         </xenc:EncryptedData>
       </Assertion>
     </ns:return>
   </ns:authenticateResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

N.b. It should be noted that the "assertion" contained in the AuthenticateResponse is **not** a SAML assertion but is an element containing an encrypted SAML token. This is specified in dail-enc-schema.xsd (see Annexe). The tag enables identification of the element as an encrypted SAML assertion.

6.5.2 Message Digest

The secure hash SHA-1 digital signature message digest algorithm is proposed and is supported by [NR15]. The SAML token is signed before it is encrypted.

Example signed token before encryption.

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="oracle.security.xmlsec.saml.Assertion1955a65"
IssueInstant="2009-06-25T13:34:55Z" Issuer="http://earth.esa.int"
MajorVersion="1" MinorVersion="1">
           <saml:Conditions NotBefore="2009-06-25T13:33:55Z"
NotOnOrAfter="2009-06-25T13:39:55Z"/>

           <saml:AuthenticationStatement AuthenticationInstant="2009-06-
25T13:34:55Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">

                       <saml:Subject>


<saml:NameIdentifier>dail</saml:NameIdentifier>

                                   <saml:SubjectConfirmation>


<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:Confirm
ationMethod>

                                   </saml:SubjectConfirmation>

                       </saml:Subject>

           </saml:AuthenticationStatement>

           <saml:AttributeStatement>

                       <saml:Subject>


<saml:NameIdentifier>DAIL42</saml:NameIdentifier>

                                   <saml:SubjectConfirmation>
```

```
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:Confirm
ationMethod>

                                    </saml:SubjectConfirmation>

                        </saml:Subject>

                        <saml:Attribute AttributeName="hmaId"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>DAIL42</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="c"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>Italy</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="o"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>ESA</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="hmaProjectName"
AttributeNamespace="http://earth.esa.int/um/eop/saml">

                                    <saml:AttributeValue>HMA
imp</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="hmaAccount"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>dailsp</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="hmaServiceName"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>catalogue</saml:AttributeValue>

                        </saml:Attribute>

            </saml:AttributeStatement>

            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

                        <ds:SignedInfo>

                                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

                                    <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

```
                                    <ds:Reference URI="">

                                                <ds:Transforms>

                                                            <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

                                                            <ds:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

                                                <ds:Transforms>

                                                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>


<ds:DigestValue>nLkuqyqDggsxQnPiGzVDDckxaA0=</ds:DigestValue>

                                    </ds:Reference>

                        </ds:SignedInfo>


<ds:SignatureValue>oOkdc3KB2HwPB6YzhEa9MHx5yo1u/xqHp81wPj68uf5Ypet/5wHHEvfuN
hxD+S3ejT2f4lKIGkVDcsRNyUqaAn60CnJiN4RBpwcjcWQSUj5/XxesaR4nO4CtDylaLV6acLwww
lLN5PQ66UumASE=

                        </ds:SignatureValue>

                        <ds:KeyInfo>

                                    <ds:X509Data>


<ds:X509Certificate>UEBhMCQkUxETAPBgNVBAgTCEJlZWxsZXMxETAPBgNVBAoTCFNwYWNlYm
VsMREwDwYDVQQLEwhCUEAxMRQWxleGFuZHJlIENVQ1VNRUwwHhcNMDgwNjI1MDg0MTEwWhcNMDgw
MTEwWjB2MQswCQYDVQQGEwJCRTERMA8GA1UECBMIQmVsZ2lxdWUxEjAQBgNVBAcTCUJyGA1UEChM
IU3BhY2ViZWwxETAPBgNVBAsTCEJVIFNQQUNFMRowGAYDVQQDExFBYW5kcmUgQ1VDVU1FTDCBnzA
NBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAq4Vsyd7w1y+u53a7
S8Lyi+cuwRjySyxf3YYPdF+9BX2zfr/wGai0kYmkO1NzCWDTNn0gsd/EjLq0eReHrqhdbcrbA09A
9kA1MKo9SYQKDVM7oXU5rHqdbPdntoM4H2QzrgL4fyIV/Zimt31UrdgZ3ySEV/0CAwEAATANBgkq
hkiG9w0BAQQFAAOBgQAxwyN+gEsWh+tXEES9xUM/BHZ3aUsdh427IlJabJe2
bqlC+glYZD8JkLzHOP3lsxtuxWyg9kXKk0SUwOAPC2IjOEwhhL7WBhNpKYacrxmY6kgVe6g/+XRe
4pCQMARfwX22CyufDVSm3AM1nJTwEcw5OkM4pWFEdcjg==

                                                </ds:X509Certificate>

                                    </ds:X509Data>

                        </ds:KeyInfo>

            </ds:Signature>

</saml:Assertion>
```

The security model proposed requires that the authentication request is further decomposed into two cases as described in the following section.

6.5.3 Authentication Use Cases

6.5.3.1 Default Case - Local Entity is IdP

In this use case the authentication request contains an identifier specifying the local entity as IdP. This is the default case when no IdP is provided in the request.

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:q0="http://earth.esa.int/um/eop"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
      <q0:authenticate>
         <q0:username>TestUser</q0:username>
         <q0:password>TestUser42</q0:password>
      </q0:authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

Or

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:q0="http://earth.esa.int/um/eop"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
      <q0:authenticate>
         <q0:username>TestUser</q0:username>
         <q0:password>TestUser42</q0:password>
         </q0:serverName>
      </q0:authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

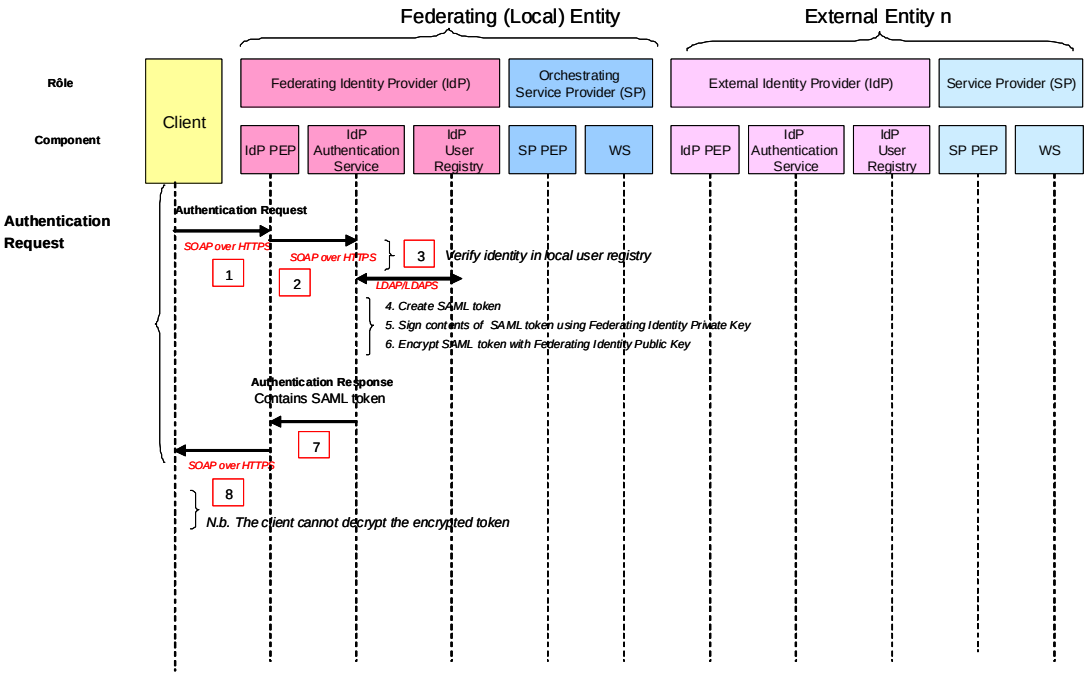

Figure 2 Federating (Local) Entity is request designated IdP (Default Case)

1. The authentication request is sent to the authentication service using SOAP over HTTPS. (May pass through the policy enforcement point (PEP) of the federating entity.)
2. (The PEP of the federating entity receives the request and forwards it to the authentication service of the federating entity.)
3. The authentication service verifies the identity in the **local** user registry over LDAP/LDAPS.
4. The authentication service creates a SAML token using the minimum profile attributes retrieved from the user registry. The SAML token is created containing assertion of the authentication and assertion regarding the value of the subset of attributes from the minimum user profile (see description in section 6.5.5).
5. The authentication service signs the SAML token using the Federating (local) Entity private key.
6. The authentication service encrypts the SAML token with the Federating (local) Entity public key.
7. The authentication response containing the encrypted and signed SAML token is returned to the client using SOAP over HTTPS.
8. The client is unable to decrypt the content.

6.5.3.2 External Entity is IdP

In this use case the authentication request contains an identifier for the external entity authentication service. The relation table between identifiers and external entities authentication service url shall be stored on the server and configured at service deployment time. It must be done in this way for security as the system must deny access to untrusted authentication server.

Example Request with IdP:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:q0="http://earth.esa.int/um/eop"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
      <q0:authenticate>
         <q0:username>TestUser</q0:username>
         <q0:password>TestUser42</q0:password>
         <q0:serverName>spot</q0:serverName>
      </q0:authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

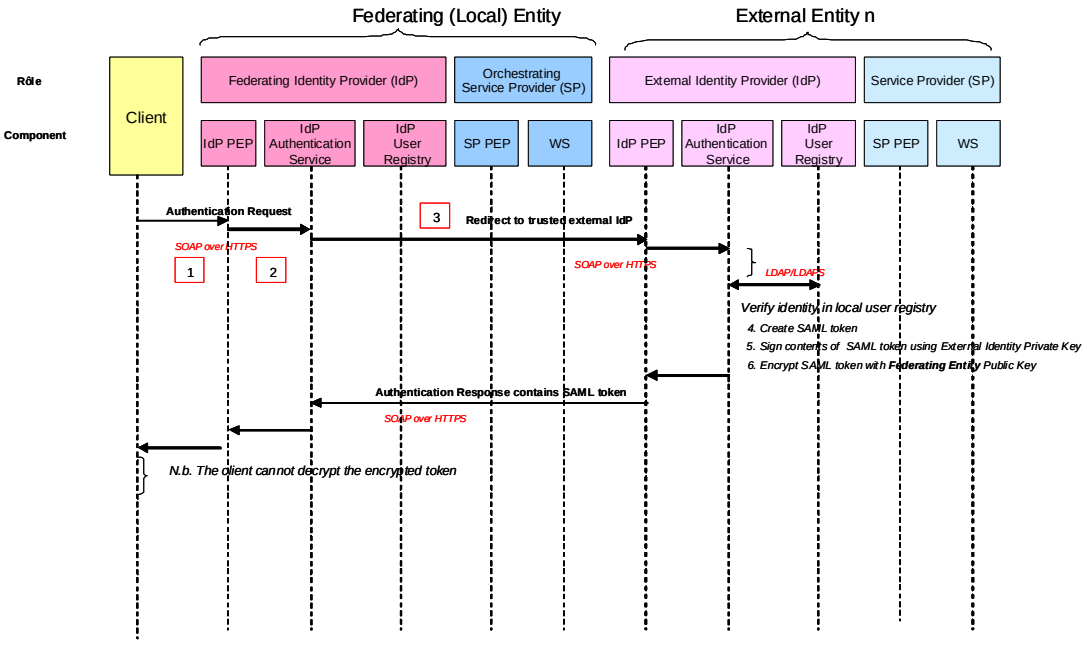

Figure 3 External Entity is request designated IdP

1. The authentication request is sent to the policy enforcement point (PEP) of the federating entity using SOAP over HTTPS.
2. The PEP of the federating entity receives the request and forwards it to the authentication service of the federating entity.
3. The authentication service redirects the authentication request to the PEP of the designated External IdP. The authentication service URL is extract from the table previously described.
4. The PEP of the external entity forwards the message to the authentication service of the external entity.
5. The authentication service verifies the user in the external entity user registry.
6. The authentication service creates the SAML token using the minimum profile attributes retrieved from the user profile in the user registry.
7. The authentication service signs the SAML token using the External Entity private key
8. The authentication service encrypts the SAML token with the Federating Entity public key.
9. The authentication response containing the SAML token in the SOAP body is returned.
10. The client receives but cannot decrypt the token.

6.5.4 Authorisation Request

The authorisation request may contain an encrypted SAML token in the WS-Security element of the SOAP header. This SAML token is obtained from an authentication request as previously described and is used to control access to services.

N.B. It is not mandatory that the authorisation request is preceeded by an authentication request as the SAML token is not mandatory in the service request. However, access to services is controlled by the policies applied in the PEP.

6.5.5 OASIS SAML

SAML (Security Assertion Markup Language) [NR11] is the 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).

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.

SAML includes mechanisms that allow providers to communicate privacy policy/settings from one to the other. For instance, a Principal's consent to some operation being performed can be obtained at one provider and this fact communicated to another provider through the SAML assertions and protocols.

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 [NR11] defines how SAML assertions are processed in SOAP messages.

SAML 1.1 is proposed to encode the user authentication token.

The following subset of attributes necessary to implement the basic EO DAIL policy steps are proposed to be included in the SAML token (see GMES Minimum User Profile [OR2]):

Minimum Profile	DAIL Part Profile	Mandatory data (not exported)	Description	inetOrgPerson mapping	Extended Class
hmaId			Unambiguous HMA identity	uid	
c			Country of origin	homePostalAddress	
o			Organisation	o	
hmaProjectNam			Names of projects with which user is		hmaProjectName

e			affiliated.		
hmaAccount			The HMA account number		hmaAccount
hmaServiceName			Associated services		hmaServiceName
	userProfile		Commercial/GMES/scientific		userProfile
	email		Email address	mail	
		password		password	
		state	Enabled/disabled. This information allows an administrator to disable a specific user.		state
	homePostalAddress		Home address	homePostalAddress	
	IdP		Identity provider		IdP

Table 1: Attributes in SAML Token

It should be noted that certain information such as password and the enabled/disabled state of a user is required to be held in the minimum user profile in the registry but shall not form a part of the data exported in the SAML token.

6.5.6 OASIS Ws-Security

Web Services Security [NR9] 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.

WS-Security is proposed to encode the SAML assertions in the SOAP header. WS-Security SAML Token Profile defines how SAML assertions are processed in SOAP messages and so it is proposed for this interface.

6.5.6.1 Encryption

Encryption is required to prevent the message content being read by someone other than the intended recipient. N.b. It does not prevent the message being modified, for this a digital signature is required.

The recipient, in this case the service providers “publish” their certificates allowing “anyone” to encrypt a message to them using the published public key. Only the recipient holding the corresponding private key can decrypt such a message.

6.5.6.2 Signature

WS-Security permits digital signatures to be used to prove that the message has not been changed since sending. A recipient can be sure that it is the user who has signed the message. The XML signature <ds:Signature> element of WS-Security can be used for signature.

a. Sender : Hash and signs (encrypts the hash code)

b. Receiver : Hash and verify hash (decrypts the hash)

c. Ensures that the message was sent by a known client and that the message arrived intact.

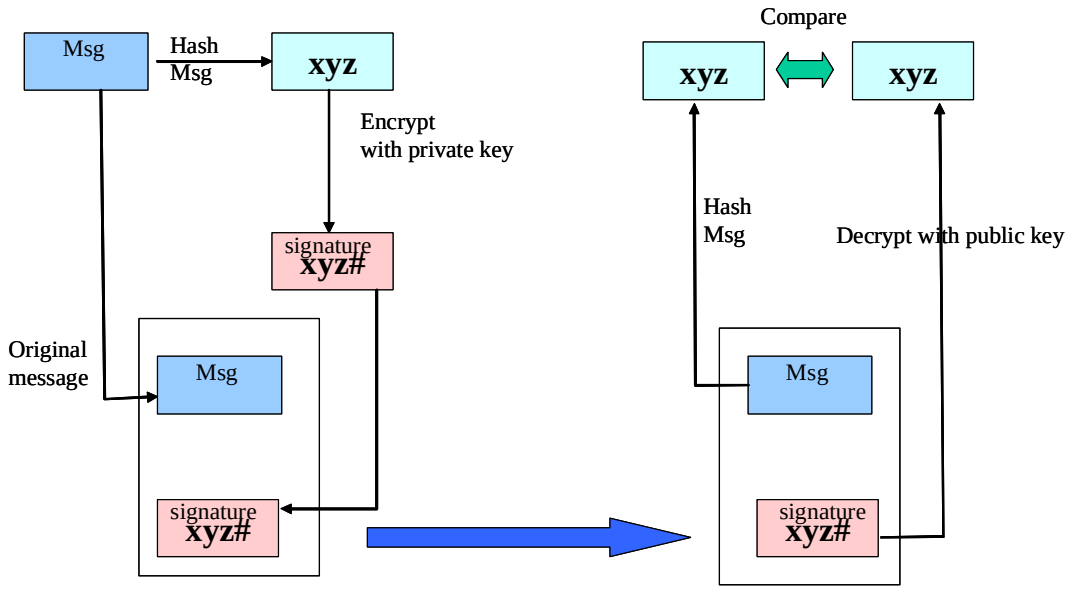

Figure 4 Digital Signature

Message encryption is not sufficient to guarantee that the message comes from a trusted client as this depends on how many people know the “encryption code”. It does not prevent someone from changing the message content.

SAML used with XML signature <ds:Signature> element of WS-Security allows signing the messages as well:

1. Sender : Hash and signs (encrypts the hash code)
2. Receiver : Hash and verify hash (decrypts the hash)

7 Interface

7.1 Authenticate

The Authenticate operation allows clients to retrieve authentication metadata from a nominated IdP server. The response to an Authenticate request should be an XML document containing authentication metadata about the authentication and requestor.

7.1.1 Request

Protocol: SOAP over HTTPS

7.1.2 XML encoding

The following XML-Schema fragment defines the XML encoding of the message body of the Authenticate operation.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:q0="http://earth.esa.int/um/eop"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
      <q0:authenticate>
         <q0:username>TestUser</q0:username>
         <q0:password>TestUser42</q0:password>
         <q0:serverName>spot</q0:serverName>
      </q0:authenticate>
   </soapenv:Body>
</soapenv:Envelope>
```

Figure 5: Example Authenticate Request

7.1.3 Response

The following XML shows an encrypted example response
The authenticate response message is always encrypted with the DAIL public key i.e. in both the use cases the client receives the same response:

- the federated response message to the federating entity authentication service and coming from an external Idp.
- The federated response message returned by the federating entity authentication service to a client.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Body>
   <ns:authenticateResponse xmlns:ns="http://earth.esa.int/um/eop">
     <ns:return>
       <Assertion xmlns="http://earth.esa.int/um/eop/saml">
         <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#Content">
           <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
           <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
             <xenc:EncryptedKey>
               <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
               <xenc:CipherData>

<xenc:CipherValue>cbE8viFOmyDuxR8N4EdwS9UUKpSoUbMrWSVprW7IypMwFZLeHR9Rxd4iw5
dUl4K+TffyNdRJ9Tr9PD8YIdpFLzCvYas63g5x4/XnyA1E2AU8ZBBpM2dtbr3g4IYMywfraWrI76
mHM+MERVZdHMVBWFrhqXhcS92m23m+amt14mk=</xenc:CipherValue>
               </xenc:CipherData>
             </xenc:EncryptedKey>
           </ds:KeyInfo>
           <xenc:CipherData>

<xenc:CipherValue>VEHlprDMQ+DqIpoPqx6TYi/mMX2dGV5JCJCrhDquZHRKqOiaIFfwqOMZvn
2HW2JDFvUxJ6LRTKdNujQI7sxc6h3IGBL7NXF7bx4jGwQ09wAA7nm6OoB4jiGdaqb8wTx0olnzn2
WqOWoVeTng1lwBi0rv2+iD1HWnXAUUHfJH8ALq4IU3hR0vjoqJH6Y21EuXPeXp/dYPUw3oIFn2FE
ID2u+8T+xOxbbq2ezQbU3z8n1LbgvDtN3ex5lUCo260pOOPn92nn7nYErT682eYd+bCKoiENpQSY
gHszvvyqFf9o6O0u87zk4AORWsRhQH74L2gG8wVOeHKyhEx0RsBkf4xZcQKBvQ9JHWQWpDEB51NZ
aJe1hSyaUk6T5gf9ArDnz6UwL0ZTDp6Dxgjha91u5qIMG3ECxVYKcnBv+O6Om1Q0HbL0ecbUDR56
evS+mf0U9JxduBKwFJLqta6D0wmwqYWcaF3ZrKd7SatV8Z2l0DmWTMe5R+x6O1RpbKltlduKl4bL
```

```
aSYFpaqaU758ZsmTDmjQQj8fn1qCZbDtp4SEVPWumoTg2k7RAOay2QtV5b+VA9wloSXoxVf2csLS
OOH/NDE1noBIpzgUb9Xm/YIPwikQKsxNPFM72yLrS0vjAho1Cxrg+8l7XIVcmowhPnLqSs6ZpvA0
1YP8EhsOFlN+0y+9EfAuoY4jYcScfwqDehth76lER+EyAdFLi10VhVxKW14VLbmksAydndIQaw6V
zGm1Qwoc3CeCaeq4q4GgFgiem1BmW9IeBaUBTX2wZmIKG8Z9Xhjv6MwT7hOeWH5fefipJs8JS8l6
wQBo8WAczzmw6s1j8JW9YDyAWosfoTPrtOwFTaaYSiaEXvPOnb5RgR/W4ivZ64ioA8FXyLFoWcNE
JJ6AgWHDLAbCDg/zvnVwEs7OdaSxRTxVNsc7cpclGspSmk/HzGYxPHInGhn/QPsac5iN6t6HlwnQ
UJgt81rI/tbFfSYqqtYqXKeNoEtw91/1DZVUi7mSc7Xj2e2Wb65h8PIoYeX3Nli+i4SrOoeAKaZr
HtpqP6f+pI4lpkANS4RFxFDiL9Ddxv1WKD//nMck0Su0HfIbPYUYF0GGvlHsv6IiwT8dj/f0MnCx
kAgegliGageZthQiNavOcURRC/94d+1jDZGayowurzdxmJhxyiEY5REQQt3hK4aAD89wMjndzxHd
tcQEuvXA5uSm3T9qgIm4Qdvuh54PW/SKptG9fDj4paTxVVlfZ+0f/1Vxjj4pPIKOVjE3e4ChBPkJ
XD/nXqZ8DdR+zPxOLWYyiqnMaxv3OInd/Iz2Lq36a09b0JEfMVz4e39sGtFzNDbxXgQnTx4L3jDY
Fdl5+gelUNduK9HtgklXDWfNIMWtY5xhdTX0m3Q8hBtNgKOHeg7BcBXF+uT30mqwgJu5cbJQl/1j
/QlMvromUaUQATN2ULu7mMiTWkoYoMTiijJGAizbKIi6O5xmHvF/jicd7lBcmSz+B+BnrnqxY5DM
/qQSFsnRoGmPKlJeiao2g+QuMD5x7H+pBUIq3B8lkMlUBg5VoKx2+kCHuP2lamGFskQl80PRGygQ
5adA2iWwKoIKoCdcYIc9C2sPVkJz+slExJXizl4L51GEWDlQ8VGsqNV7CzOyIt0uXIIBQW3j0aX/
/7QoYVfM681TiqvtaDEY7Ip4nSV839e5xnj3s+qgzXOpoK5rw5EThDLhthPy97CJiuSbsfcGf1Dv
WNE74x2E4b8HazacItRBIbx0GFDHIoqaHEih6zlhQaqwloLnUHRpL8vAQLVKiW3q94569e3GenoQ
bpjxKQ9F58VuQh3ZiZtJ+17XOxDx6ZDXcTiQDa+3nXiTgT7k9gGtpIv8vYLMuUHDEZx1zGd/rMzU
3JAbbfKO8+Cs3pMnb2KpGL4rLLgivee1P35rbHK04V8D0NbwDk0TOVnmFQWIRsgVtPwmEHXbFl3j
qIUTx4xdishXmkKcDCwaNfqYo4yzmgLUlbtchkDGF9YBA0mXv4gT7z0TiBb1jUFBhTnciL4DBkI9
K8wEjklHUi7w4LjvhCB5B15y1ZG/baIscoRrVu41HUp7crwbsdKjcWGE//dBTXN1vrXDm0maAkCo
nuYNPpMY0Cf+ikVITJO73UaXplFjOOtm+mkql6e5nTd8qGQXwHZl/nGJOEO/rMsXSoVybxIn5bg+
97CFCtAdsRRjAJZRQcrJIztenGJX81U0rvAX+OuoSNrgVpdxcwuH/1x80i+CY5kdUkg3EMkU0m4F
iNQ6CyXiiimVSBRB0sHfWW5/Em+qlYeRjrXCyJBYPo2mCuMtqQN42VeShEkQ1XPx6o09NTaaxXRM
pV2IHjzALLrR0Px6zqbp7CuEhPdLxTYcXetDKQJt/XHJuWdvETMgsJnyQ0cCJSPXp21xsrK6zYLY
cQ1M8rS9RHCmWvFdTZg49mX3QPANOUDPoPR0y3mOT19FWKFYOfQhHN2xPJZAPV6ZJeReeAeTBRkT
vgIJE/3BsQpmqsSusjgEDYCrK8MfaybAC6CpE5ZKnQwV99YlTcbPx7vVKPuU13j3Aj4FjtGjkFun
fCOpLX1AA0FSbBfOOCVeYd94bCGaW8f+j3NBB+29ELYMskew2tyCBiw2HodBrMoDiYVWHbD+bWw8
qMOOBurEQihVdNq5Tbi3R2fnnX9DpfbVljJeKFjyVwCLZA5OdGIYPuJxrXGKsaBI+abTgciL4n4W
bsG7LalURKCMe/HH1jVuy8VjevwJMB+u7CHoOc9jVCwR4YSPjH9fbxcIn9UIuECm1CryEUYB6kkh
BEeyxdQclP0amPYlyxVU80KN+Mxvle4//B6kwUtjS+/Rv943oXrXxaLXTCpeds49x0FWSRo/HCxy
nunzpkyqD4wBfUyB7hYggeRUaCb7aNVuIB1QZSY9EqF3F26Aootz1cYpr1CBtizZK9Q6Ez6N3iYW
1dMUB7dsNp4a4emAU3CfhHYh3JNv4pD21PbPASO/t89v7uMDrsI8SOp1nHqV0hYG2+JhxNyhYKV1
oXv54mKzbW+4vwsU/ySrrexUvmkTzLCsYBI7nSZT5uVprRA+MQJBLx6dKVVuzO1x8hzTv9T2LvJr
7rpd6Ban94JJ8vG7OUO0OaNP9HDrz+34xmCqQRi/f0TkmfSo4uFcsIfAmdQVbd6uu22ZBoWqolaz
lBXjt5Oe2AQV51Zma53dlArSBLpvbg/RoMM7cMhnGn33DkSBDYU9rN2iApw0zswa/KJ/p1r33Jrk
5YTL6wTTEuaG+UxVrtCxX4VHk7syaOjI5dshRELos3ZeIJeqKAgS45H6cK+gjCq0l3qWDDnFHcGm
zYoP1665lC7c9TOs8i5OBLM6hGqgEgcKEiTIp+tRUvDEhyN1v/YngT3izvWbsijV0QTTJcjsyFWq
DSJiw8G1WH4oFqZAzF2UzE6fzEeQbMVlPPxlnpUjipTqdtWcuayLH7tifX7diBl1fjlUOTqPK2+5
vz1HckVtzJMS4g0W7rWHAbTv5nfrby/1IJBHMDutjI2dh6J7nXbSgFOiT98TFL7upJCNc7T3AH4j
Ro1TzzXqODFShamQeYlooCyvStQxqj08rz74+7ery+GapNEPL4cPZ1qV0bfKCBwOQrTV8lIZXsFt
Jj9TV+7lT6ZcePnCFY6pWI78u5WWePZunmI9FFhz+odZd4vfh0C3VEISmeEN28T8XdvtHt8A78sr
4/SmrPteZpZhByZe2n50ZHQU+uknсDgZirtz5A4LIBedcDLCgeNfonHYCQTNYOKoDA+eq5sBczKP
mqFKjPnBq1533/lptWhsgou8CZfsEaY4kZvEzK8YTVrfVt4T407A851vKxBfHIyXKxFFi17Yddr2
SiqebAUjT3waPAoUwgdJelDYTnnKUQy0Zm25gGRDiE9LUwoOp7ys0H9m/xXJROx76gbljguU3ad9
fcwQIm8RTKZvXvKrVRBUsHutEL6/qZAb5VBQ1JHsa4tknAFTdwh7lsB1/l0lHtZ+HzBdgZ8kOvRm
HiCKYb+2p26WMVNy8SRhW8EeYxx3t79LMU3pIp9w4rCnuClwAYAXN6PP1Gf5GgsGS228ur3vwNKO
8YZIdMatmKJDy8Ufkm1Ljvy4Z0/3+XcGLDWyxRx6M2mLvMPvJIz9iGSr684PRfSydR3nq6W7gwYc
Ohb62cmSLVWyECoaa+cqVFFGOKHcUT3ZS7Xlx0QkniCQI9d46XDEx64PFGeBXL/z4dj7ZYx6woX9
R+F5yOAdKoILV5N9m4xzauPO4EkmKakDBtsf9tzExrArDBoT664Xc7cVJ/2jTzX57Oms09Q7r+T8
hH0JNxhcXAqhxdbMitkcFSy7t0pBgrPXRhdXohbGlhuZPAOMVkWWDMf8x7Yc4k7F3l9ua67w5Z2Q
cDf8NBq5iYM3TkB+2qpmn16L7Pbp5qlAoIcB409+6VwxHiHQgBHOPGsP1xHNYGYyKcfR4VxaUUXf
5G18b5NOnx3S2VCBA9fJGXlHqW3RmtlMEP4dEQdCbhH7jw7jd5El0NabRA0fCBTAYR61vYa9Ov7S
DOIefy6NpDffg9sFltOa36ag==</xenc:CipherValue>
          </xenc:CipherData>
        </xenc:EncryptedData>
      </Assertion>
    </ns:return>
  </ns:authenticateResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

Figure 6: Example Authenticate Response

7.1.3.1 Example Authentication Response Before Encryption

An example is given here for completeness of the fragment before encryption:

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="oracle.security.xmlsec.saml.Assertion1955a65"
IssueInstant="2009-06-25T13:34:55Z" Issuer="http://earth.esa.int"
MajorVersion="1" MinorVersion="1" >

          <saml:Conditions NotBefore="2009-06-25T13:33:55Z"
NotOnOrAfter="2009-06-25T13:39:55Z"/>

          <saml:AuthenticationStatement AuthenticationInstant="2009-06-
25T13:34:55Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">

                       <saml:Subject>


<saml:NameIdentifier>dail</saml:NameIdentifier>

                                  <saml:SubjectConfirmation>


<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:Confirm
ationMethod>

                                  </saml:SubjectConfirmation>

                       </saml:Subject>

          </saml:AuthenticationStatement>

          <saml:AttributeStatement>

                       <saml:Subject>


<saml:NameIdentifier>DAIL42</saml:NameIdentifier>

                                  <saml:SubjectConfirmation>


<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:Confirm
ationMethod>

                                  </saml:SubjectConfirmation>

                       </saml:Subject>

                       <saml:Attribute AttributeName="hmaId"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>DAIL42</saml:AttributeValue>

                       </saml:Attribute>

                       <saml:Attribute AttributeName="c"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>Italy</saml:AttributeValue>

                       </saml:Attribute>
```

```
                        <saml:Attribute AttributeName="o"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>ESA</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="hmaProjectName"
AttributeNamespace="http://earth.esa.int/um/eop/saml">

                                    <saml:AttributeValue>HMA
imp</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="hmaAccount"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>dailsp</saml:AttributeValue>

                        </saml:Attribute>

                        <saml:Attribute AttributeName="hmaServiceName"
AttributeNamespace="http://earth.esa.int/um/eop/saml">


<saml:AttributeValue>catalogue</saml:AttributeValue>

                        </saml:Attribute>

            </saml:AttributeStatement>

            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

                        <ds:SignedInfo>

                                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

                                    <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

                                    <ds:Reference URI="">

                                                <ds:Transforms>

                                                            <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

                                                            <ds:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

                                                <ds:Transforms>

                                                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>


<ds:DigestValue>nLkuqyqDggsxQnPiGzVDDckxaA0=</ds:DigestValue>

                                    </ds:Reference>

                        </ds:SignedInfo>
```

```
<ds:SignatureValue>oOkdc3KB2HwPB6YzhEa9MHx5yo1u/xqHp81wPj68uf5Ypet/5wHHEvfuN
hxD+S3ejT2f4lKIGkVDcsRNyUqaAn60CnJiN4RBpwcjcWQSUj5/XxesaR4nO4CtDylaLV6acLwww
lLN5PQ66UumASE=

                        </ds:SignatureValue>

                        <ds:KeyInfo>

                                    <ds:X509Data>


<ds:X509Certificate>UEBhMCQkUxETAPBgNVBAgTCEJlZWxsZXMxETAPBgNVBAoTCFNwYWNlYm
VsMREwDwYDVQQLEwhCUEAxMRQWxleGFuZHJlIENVQ1VNRUwwHhcNMDgwNjI1MDg0MTEwWhcNMDgw
MTEwWjB2MQswCQYDVQQGEwJCRTERMA8GA1UECBMIQmVsZ2lxdWUxEjAQBgNVBAcTCUJyGA1UEChM
IU3BhY2ViZWwxETAPBgNVBAsTCEJVIFNQQUNFMRowGAYDVQQDExFBYW5kcmUgQ1VDVU1FTDCBnzA
NBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAq4Vsyd7w1y+u53a7
S8Lyi+cuwRjySyxf3YYPdF+9BX2zfr/wGai0kYmkO1NzCWDTNn0gsd/EjLq0eReHrqhdbcrbA09A
9kA1MKo9SYQKDVM7oXU5rHqdbPdntoM4H2QzrgL4fyIV/Zimt31UrdgZ3ySEV/0CAwEAATANBgkq
hkiG9w0BAQQFAAOBgQAxwyN+gEsWh+tXEES9xUM/BHZ3aUsdh427IlJabJe2
bqlC+glYZD8JkLzHOP3lsxtuxWyg9kXKk0SUwOAPC2IjOEwhhL7WBhNpKYacrxmY6kgVe6g/+XRe
4pCQMARfwX22CyufDVSm3AM1nJTwEcw5OkM4pWFEdcjg==

                                                </ds:X509Certificate>

                                    </ds:X509Data>

                        </ds:KeyInfo>

            </ds:Signature>

</saml:Assertion>
```

7.1.4 Failed Authentication Request

Security considerations require that full error information is not returned to the user. An example is given below:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring>Exception occurred while trying to invoke service method
Authenticate</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

7.1.5 WSDL

The WSDL is given below for the authentication web service used by the identity provider.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
xmlns:ns1="http://org.apache.axis2/xsd"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:ns="http://earth.esa.int/um/eop"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
targetNamespace="http://earth.esa.int/um/eop">
   <wsdl:documentation>AuthenticationService</wsdl:documentation>
   <wsdl:types>
          <xs:schema attributeFormDefault="qualified"
elementFormDefault="qualified"
targetNamespace="http://earth.esa.int/um/eop">
           <wsdl:import namespace="http://earth.esa.int/um/eop"
schemaLocation="./authentication.xsd"/>
       </xs:schema>
   </wsdl:types>
   <wsdl:message name="authenticateRequest">
       <wsdl:part name="parameters" element="ns:authenticate"/>

   </wsdl:message>
   <wsdl:message name="authenticateResponse">
       <wsdl:part name="parameters" element="ns:authenticateResponse"/>
   </wsdl:message>
   <wsdl:portType name="AuthenticationServicePortType">
       <wsdl:operation name="authenticate">
           <wsdl:input message="ns:authenticateRequest"
wsaw:Action="urn:authenticate"/>
           <wsdl:output message="ns:authenticateResponse"
wsaw:Action="urn:authenticateResponse"/>
       </wsdl:operation>

   </wsdl:portType>
   <wsdl:binding name="AuthenticationServiceSoap11Binding"
type="ns:AuthenticationServicePortType">
       <soap:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document"/>
       <wsdl:operation name="authenticate">
           <soap:operation soapAction="urn:authenticate" style="document"/>
           <wsdl:input>
               <soap:body use="literal"/>

           </wsdl:input>
           <wsdl:output>
               <soap:body use="literal"/>
           </wsdl:output>
       </wsdl:operation>

   </wsdl:binding>
   <wsdl:binding name="AuthenticationServiceSoap12Binding"
type="ns:AuthenticationServicePortType">
       <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document"/>
       <wsdl:operation name="authenticate">

           <soap12:operation soapAction="urn:authenticate"
style="document"/>
           <wsdl:input>
               <soap12:body use="literal"/>
           </wsdl:input>
           <wsdl:output>
               <soap12:body use="literal"/>
           </wsdl:output>
       </wsdl:operation>

   </wsdl:binding>

   <wsdl:binding name="AuthenticationServiceHttpBinding"
type="ns:AuthenticationServicePortType">
       <http:binding verb="POST"/>
       <wsdl:operation name="authenticate">
           <http:operation location="AuthenticationService/authenticate"/>
           <wsdl:input>
```

```
                <mime:content type="text/xml" part="authenticate"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="text/xml" part="authenticate"/>

            </wsdl:output>
        </wsdl:operation>

    </wsdl:binding>
    <wsdl:service name="AuthenticationService">
        <wsdl:port name="AuthenticationServiceHttpSoap11Endpoint"
binding="ns:AuthenticationServiceSoap11Binding">
            <soap:address
location="http://172.16.5.36:8080/AxisService/services/AuthenticationService
.AuthenticationServiceHttpSoap11Endpoint"/>
        </wsdl:port>
        <wsdl:port name="AuthenticationServiceHttpSoap12Endpoint"
binding="ns:AuthenticationServiceSoap12Binding">
            <soap12:address
location="http://172.16.5.36:8080/AxisService/services/AuthenticationService
.AuthenticationServiceHttpSoap12Endpoint"/>

        </wsdl:port>
        <wsdl:port name="AuthenticationServiceHttpEndpoint"
binding="ns:AuthenticationServiceHttpBinding">
            <http:address
location="http://172.16.5.36:8080/AxisService/services/AuthenticationService
.AuthenticationServiceHttpEndpoint"/>
        </wsdl:port>
    </wsdl:service>
</wsdl:definitions>
```

Figure 7: Authentication Service WSDL

7.2 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.

N.b. The service requests from a client to the DAIL or from the DAIL to a service provider are the same.

7.2.1 Request

Protocol: SOAP plus WS-Security over HTTP/HTTPS.

7.2.2 XML encoding

The following XML-Schema fragment defines the XML encoding of an example ServiceRequest operation

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Header>
```

```
      <wsa:MessageID
xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/addressing"/>
      <wsa:ReplyTo
xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/addressing">
         <wsa:Address/>
      </wsa:ReplyTo>
      <Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd">
         <Assertion xmlns="http://earth.esa.int/um/eop/saml">
            <xenc:EncryptedData
Type="http://www.w3.org/2001/04/xmlenc#Content"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
               <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
               <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <xenc:EncryptedKey>
                        <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                        <xenc:CipherData>

   <xenc:CipherValue>k4kkm+nBkutOsmP9Lm6v4gpPvtJqxOOJLEOoKCQfE4Q7qp1yOBkKRlu
j9zb7Y07cNdJf8OhzGaHFGz7OIfM9Tpl5QEntkoeOT9wg/PsYqlIaAsCRoDsYjJoQrqpHdIpv3wl
Cck8iysQus4LpqdK
Hc6pWRk0Gk9022z/3U=</xenc:CipherValue>
                        </xenc:CipherData>
                  </xenc:EncryptedKey>
               </ds:KeyInfo>
               <xenc:CipherData>

   <xenc:CipherValue>+X0OFMae+FV8zOr0pPA02icglYf4AKcaml/jNfP8gdmjIh/dB/utVIC
YxKtarBRSAlptozGoI92r+bwUwmAyIY3D7gX0h6EC0P3LqhojKiMRrNbvCaotOPWoMherMp1SUbx
eYgxdZVlpXa77mNHHEkjhcmNXHydgz4DJoLxzHUIdWm9Lv+UTufH+D680JicO0SCnGdIC6KEpM68
h+3x/PRRNdmzy
QRpS9WZ03DAADBokRmW8IbG5YlUG4NjZDhkPDRlFhaHBTn4ZDP4LEd98KXZclwAlAB9XIICTeNFh
9t0itufclexX0zu/icAM8ws/sEAh7NmLyw+k8MRI7lMXeldnqftBYYj5NzYZqUd87XXqTe6ytnS3
SwbZXgdkgKylqdp0p0FcJVOGb4obfP/6irwzf1ujK2DMJb+9+mTQzfdNIIXimegV5wY2r1Wsg7Xt
xiVU6TFMI6VA5CH1MkmgYyYFqgI2MoiNXW3c3sgAs6+QlRoPMR3uNzvtB7NKy0m9BET+zqxCRgPt
GPstjX5ATvJ7tbcAlSKGyHubEIE9Am1Q2nGv3ChGzPPw+rwtow1D8xeSnxWOKpp/whmXcN9AEQ/z
5HtDCmbw1+ExRTM8Xy1NWp135If/6ooxcJtOf5vavo5Mx1OQto8TieF35+5FXA0rUiCn//yJzJRz
2mXEMJfoO1HfwPpfGWxwId4yuhWeylNAA4sKWt2OVDc/zkZpRTIHOoOWuut2LdsZS1fBZ+RMnpt/
u8tivsRITLyd2htTILLXKIenNpdRWeUD4d23RxcFFt+bGh
yrbHnsrT+DIZJD0PfS0zxigXu+NG4wy+Plhj11h4pn2AosIP5v0ZXN/tObgsQonwKyjFwgqGH8js
Ik/96PLnu1ODRRYVIBOGlcV9K7NrHeqCkM1157HCwu/rflTXK61jzRsZ8/hzC8ADiOXQnpk8K4EO
AFs/A6LY54A8MFQndHkAHN6NEK0nbAkqhOTur99PHrXQtYfsf26Mrd8rTKhkP5zd3pdfzvhnqOnx
OSe2FuWX3WHwUTgAzMBlJC2PRzHM4Q4q/pHFyK+UrLE2QLYsBn6VzouHfcI3dikR/0d2RQPsrQKQ
PB8WXMjJxK7v05jRBjZaNYpmsFk08zweM1OWuVB8L57zSzAfb7CKpPgsgRk4ezLWrPVK7Z2UuQ+z
/UH66S3a9dYsneQMaDMh7wYQtLe3fEeUhbBYrjRBZWHriOnhxoN7Rll8bnKOXoJUJJMZqyZyvN7q
HTLUxG98KUncu3HYwKSIgZEog
ZhHsfbqp9jee0tx4MhW+t8z9Upsh7TPhWcEvaFxpn5pfz4c704nsM7Tmcq4IijlnW8m3kX/mBR/O
TFcjWh2mV8XZoa/Hro7Rj69HVjELBTlF/W+S7pNsN+hoErRDlWxuHqC6v7KDMakaLF/Cekz
WA27ozxm7z1+6a/BeiXSTNojoodOybmv7hxjObWg53RUp5H3rejnN52+7IDHJwik2DONIErqL5GP
Soy3+adE5mSnAQklZ4zeErsl/A82ySgovaQNskuqa+6aBLvhHQ9CPeQmlddOfyU6HebMSN2mE8OZ
2yejwhujnT5ha4KoefrE21bwi5xWkNDobJbfBPXgg7Wdf4M6n3zsRTT6ixugXrkdRhnYyTzpRJ6E
PpL5Cdunh2gyQHiyJbcCh37rzTcsx0CiWHfak0ObqDRUeJ8tPyOS5PhyxcNknQ4p3RCI0QJTxUYG
3jpWntAK7ZU3d0Bmk+DAaPGGGJ44fKZ3HZTWjnFTcqWxwYOXxsiJ/kKE8ZVcDJ6IL4pf4dTnJHaa
8hT09LVutVZJrqcYbI5q/QL1hcMclPBByoaP4EmFPxX3dpbap0uf2qbX80G+jjVtsHd9rhEmyoc6
tJjj27Z2B0ANPAI53AMDXGF5HHHzzficfizN0vK48EO/xk34EEylSmCIInrf72m54f7wh8RojgoO
zIWZkIU+tpCfO2HTcxRUT/rd6Wfb624YE9ov20+T1U0Yc9nyj
zoNDNBjCXh7+tr4FkUoZGyzqm5OlYkfkKvkwkp6rH8RzUhqKewHjWb7zdlYHEH8XkMtcHneYgeQ
pDQ/E8bshTuLILOELUtRODjszaTXyrm4xlhCzJ7mWlZa+viTV4PzHdRQCVByGxOsFfhJGtrOOrx
SUnyUNVDBbKxiTe7tzuTtZ9demhjAE17svhCxh5tIWg5NMJ3FeG4HzOL9UUoah4gwjyvFa/0azdt
1ZWaYc6SPufQIWk9I2HWRb1m4waiA24LkLBXvYMjWTto+DsVWPP3WQXtPaSBNtnD/VEbM+2bbPER
A1+drMTui6Gvl/iHNQ9uq+UrmXPoR9NtfSEAh/M5BdSH75zGifd369R1eFJqBuBWile2R7ryqnPP
BbVf89md0nhYe3RzdD0DKbJen5/r3eicrc3PculW8cGJDqtuEI9kC1xULyXuhWmpEACgTabmNmw3
T+3LnzEuKU97DtLpgqlJoAqXHBBImDsPmzX
JIDOoNc7J8ouh53L8ZM6jZwFXGqQBteV0HsDPwxTBSGE+tuPQHj/cWvovOBeltewUuBskG0EwsDt
kYwmP5yNlbY4vn0ouL+4tlprZr2oNSitv3Lle/usE5ps70ALpQYvzG369DAqf2T+m3Ld5HaKZ/N+
```

```
cWtQSt/EJGjjBTTodrzbkAe7Mkz/euMxU0Pj5Gv4kyLysfivPPuvar+ZuRos/jm5N+mHUQUzWd2i
zk4BvBuyWHNe3Jq45H/ELAND0OEZRoXCRbpz0io+a9C6T44BlOECJyXI1gp/m9lsbb5iSv0HpMSv
4xsLpM1AuXLpKmeqdsHO/zEnLUOhR2Dpk6hoqpnPvK+QbVO0c/YdJ+lkeGIz6C2OsrbbsiO+cUou
l+7mJ6WG7VqifJWNX8mzd6RklCntt0W1CgBk93vzOspDJfnvBkHSZ1VmuiWLWpesttUrYCwF77lc
SLDR3Rvqa29hUORrV4BRHl1LAuf9ofAyg9r3vb2TjlrG58FOekzRxomjP/rTL0jteYiBf6YwoMEw
g2chC3lhRoaTpzTpMSbAoByuI3VCsqMN81JwEAUOtXmjRFg/C8Cnc1/Zg8tYfNtIymNbzH9S5Mmo
Qy2oEUaM/RmAU1yhqEE+J1q4wBfJb933T8oPOQBgbNjntcDsJXwQt1xa/QxDs7d1TaGMkzbY6YxZ
Qxt0s6cTwyda2XwqO6Bd9pugluF4c4l218g+42PTzwHWpTcXbqOaQDLVITfM5LWK7JvAEK5fai9X
c2dooFiNiR+QgU3SwRrZ4GZ1d4wWgOJsPexgEkYOKQuwo6S1vl0WNZtuYC7/+ct4qiHzA2tk+5HB
vMoZ1WyxUQNXo/sfhRx5xK7lT2vHqBx0k1gwoZW7l8/IPPbo0frpdKT2iOGLB/YH46GkWztp0Ft8
+7uPbFebu76teSF04ei3utFf9h+UmcxgNmtGR1BuILEs5ERKI2KDLfr90+ltKhDZu6gOBrcOWxik
x+bhojouvj0o+LdZt9zjSaNPZTkym01zPoFv24xyAA3OUAc1WESHKcuPbwO18LIopmURoEROB3dY
N8veuTfekmYPv3tHOaLdZaL66oJklarJBcHWYlr/ob0/gElFmn+20y/kK7oq9vEP/oOSMYgtiyCW
mBEgcnm6rIQvklFxzt9FFMz06+2I5/W0OSRnr371Pb1nukHFXHJC5bDRMbnR7JobKhPAcDibzl2i
Nt/uWNX3K7L3Ddh1hCHFF/Dl+won2HJsfItOvbfxVoL3fs1Rk6+FXvO5QRqcrQVOKN/z2cn2Y8N/
bLIr86AH3+J7r4fGAspyqx985VMKzzl5OHvi+DzGDmmuzgtHpB3/R0NRbWgbW5
ebpeduehhmzGQ4vL3KbrrbH+QkU2DIlcp+DOYysnVNtDxlFJVSDfvHxBAeOYwm9sjzvrslpHMqkl
tSmiqOnuU/shfPtAdYyxoTTDV11R+TJNQo80Mq7cJUd9NeiYi+TjorpN5qtJW9/XQIPQjO
riuWkK3d/mv4dwGWQkS14CJ/5Em4ONdEJnJzwU4FndrLGh76IWczBM+3grhCVWBWf5EohxV8rMEJ
D7m3HeP6koPo4uxTylRkhSFO8GgP0aFR5cEGsjnIhyPVcf7ad1L9t+A3ajzpPW9m+pcdgWqvamCT
47B/Uc6S/nN8VA+7bIdXVCqTsNiyyNoNSEplk8Qi97nz2ZF6/UcxdoD6aVD/HvJA53usmluCKuyl
nFbFX9eIyOF0DGppo3RsP8ka61pSt+jXrn95xkisO1u/Efmt8lb0bhrPET+NEkA==</xenc:Ciph
erValue>
                </xenc:CipherData>
             </xenc:EncryptedData>
          </Assertion>
       </Security>
   </env:Header>
   <env:Body>
      <csw:GetRecords maxRecords="10" outputFormat="application/xml"
outputSchema="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
resultType="results" service="CSW" startPosition="1" version="2.0.2"
xmlns:aoi="http://www.esa.int/xml/schemas/mass/aoifeatures"
xmlns:common="http://exslt.org/common"
xmlns:csw="http://www.opengis.net/cat/csw/2.0.2"
xmlns:gml="http://www.opengis.net/gml"
xmlns:ogc="http://www.opengis.net/ogc"
xmlns:portal="http://www.esa.int/mass" xmlns:rim="urn:oasis:names:tc:ebxml-
regrep:xsd:rim:3.0" xmlns:serviceNs="http://www.opengis.net/cat/wrs/1.0"
xmlns:wrs="http://www.opengis.net/cat/wrs/1.0">
         <csw:Query typeNames="rim:RegistryPackage rim:ExtrinsicObject
rim:ExtrinsicObject rim:ExtrinsicObject_acquisitionPlatform
rim:ExtrinsicObject_dataLayer rim:Association_acquisitionPlatAsso
rim:Association_dataLayerAsso rim:Classification rim:ClassificationNode">
            <csw:ElementSetName
typeNames="rim:RegistryPackage">full</csw:ElementSetName>
            <csw:Constraint version="1.1.0">
               <ogc:Filter>
                  <ogc:And>
                        <ogc:BBOX>

   <ogc:PropertyName>/rim:ExtrinsicObject/rim:Slot[@name=&quot;urn:ogc:def:e
bRIM-Slot:OGC-06-
131:multiExtentOf&quot;]/wrs:ValueList/wrs:AnyValue[1]</ogc:PropertyName>
                                    <gml:Envelope srsName="EPSG:4326"
xmlns="http://www.esa.int/xml/schemas/mass/aoifeatures"
xmlns:sch="http://www.ascc.net/xml/schematron"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                                          <gml:lowerCorner>23.1368 -
40.7547</gml:lowerCorner>
                                          <gml:upperCorner>58.3726
32.2642</gml:upperCorner>
                                    </gml:Envelope>
                              </ogc:BBOX>
                              <ogc:PropertyIsEqualTo>
```

```
   <ogc:PropertyName>/rim:ExtrinsicObject/rim:Slot[@name=&quot;urn:ogc:def:e
bRIM-Slot:OGC-06-
131:parentIdentifier&quot;]/rim:ValueList/rim:Value[1]</ogc:PropertyName>

   <ogc:Literal>urn:ogc:def:EOP:ESA:SIMU.EECF.ENVISAT_MER_FR_xS</ogc:Literal
>
                           </ogc:PropertyIsEqualTo>
                           <ogc:PropertyIsEqualTo>

   <ogc:PropertyName>/rim:ExtrinsicObject/@objectType</ogc:PropertyName>
                                 <ogc:Literal>urn:x-ogc:specification:csw-
ebrim:ObjectType:EO:EOProduct</ogc:Literal>
                           </ogc:PropertyIsEqualTo>
                           <ogc:PropertyIsGreaterThanOrEqualTo>

   <ogc:PropertyName>/rim:ExtrinsicObject/rim:Slot[@name=&quot;urn:ogc:def:e
bRIM-Slot:OGC-06-
131:beginPosition&quot;]/rim:ValueList/rim:Value[1]</ogc:PropertyName>
                                 <ogc:Literal>2009-06-
26T00:00:00.000</ogc:Literal>
                           </ogc:PropertyIsGreaterThanOrEqualTo>
                           <ogc:PropertyIsLessThanOrEqualTo>

   <ogc:PropertyName>/rim:ExtrinsicObject/rim:Slot[@name=&quot;urn:ogc:def:e
bRIM-Slot:OGC-06-
131:endPosition&quot;]/rim:ValueList/rim:Value[1]</ogc:PropertyName>
                                 <ogc:Literal>2009-06-26T23:59:59.000

                                 </ogc:Literal>
                           </ogc:PropertyIsLessThanOrEqualTo>
                           <ogc:PropertyIsEqualTo>

   <ogc:PropertyName>$acquisitionPlatform/@objectType</ogc:PropertyName>
                                 <ogc:Literal>urn:x-ogc:specification:csw-
ebrim:ObjectType:EO:EOAcquisitionPlatform</ogc:Literal>
                           </ogc:PropertyIsEqualTo>
                           <ogc:PropertyIsEqualTo>

   <ogc:PropertyName>$acquisitionPlatAsso/@sourceObject</ogc:PropertyName>

   <ogc:PropertyName>/rim:ExtrinsicObject/@id</ogc:PropertyName>
                           </ogc:PropertyIsEqualTo>
                           <ogc:PropertyIsEqualTo>

   <ogc:PropertyName>$acquisitionPlatAsso/@associationType</ogc:PropertyName
>
                                 <ogc:Literal>urn:x-ogc:specification:csw-
ebrim:AssociationType:EO:AcquiredBy</ogc:Literal>
                           </ogc:PropertyIsEqualTo>
                           <ogc:PropertyIsEqualTo>

   <ogc:PropertyName>$acquisitionPlatAsso/@targetObject</ogc:PropertyName>

   <ogc:PropertyName>$acquisitionPlatform/@id</ogc:PropertyName>
                           </ogc:PropertyIsEqualTo>
                        </ogc:And>
                     </ogc:Filter>
                  </csw:Constraint>
               </csw:Query>
            </csw:GetRecords>
   </env:Body>
</env:Envelope>
```

Figure 8: Service Request Example

7.2.3 Failed Request

An example is given below:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>AuthorisationFailed</faultcode>
      <faultstring>Country of origin not authorised</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

7.3 ServiceResponse

7.3.1 Synchronous

The service response is as defined in the corresponding catalogue, ordering and programming ICDs.

7.3.2 Use Case: User logs in at client and makes Synchronous Service Request to HM Service

In this case the sequence is as follows:

1. A user already registered in the local (DAIL) user registry logs in at the client (DAIL Client or an external client).
2. The client authenticates the user through the DAIL authentication service.
3. The DAIL authentication service:
   - validates the user,
   - creates the SAML assertions from the information held in the user registry
   - signs the SAML assertion with the DAIL private key.
   - encrypts the signed SAML assertion with the DAIL public key.
4. The DAIL authentication service returns the authentication response containing the encrypted SAML token.
5. The user is given confirmation of login.
6. The user selects a service.
7. The client constructs the service request and inserts the encrypted SAML assertion in the request. (N.b. The client should manage the token validity as it is possible that the token has expired and will therefore not pass the PEP checks . To ensure the token has not expired an authentication request could be be requested at each service request).
8. The service request is sent.
9. The DAIL PEP decrypts the token using the DAIL private key and applies policy checks.

10. The request is forwarded to the DAIL HM service.
11. GS service requests are constructed and the SAML token in the header is encrypted with the GS public key.
12. The service request is sent to the GS PEP.

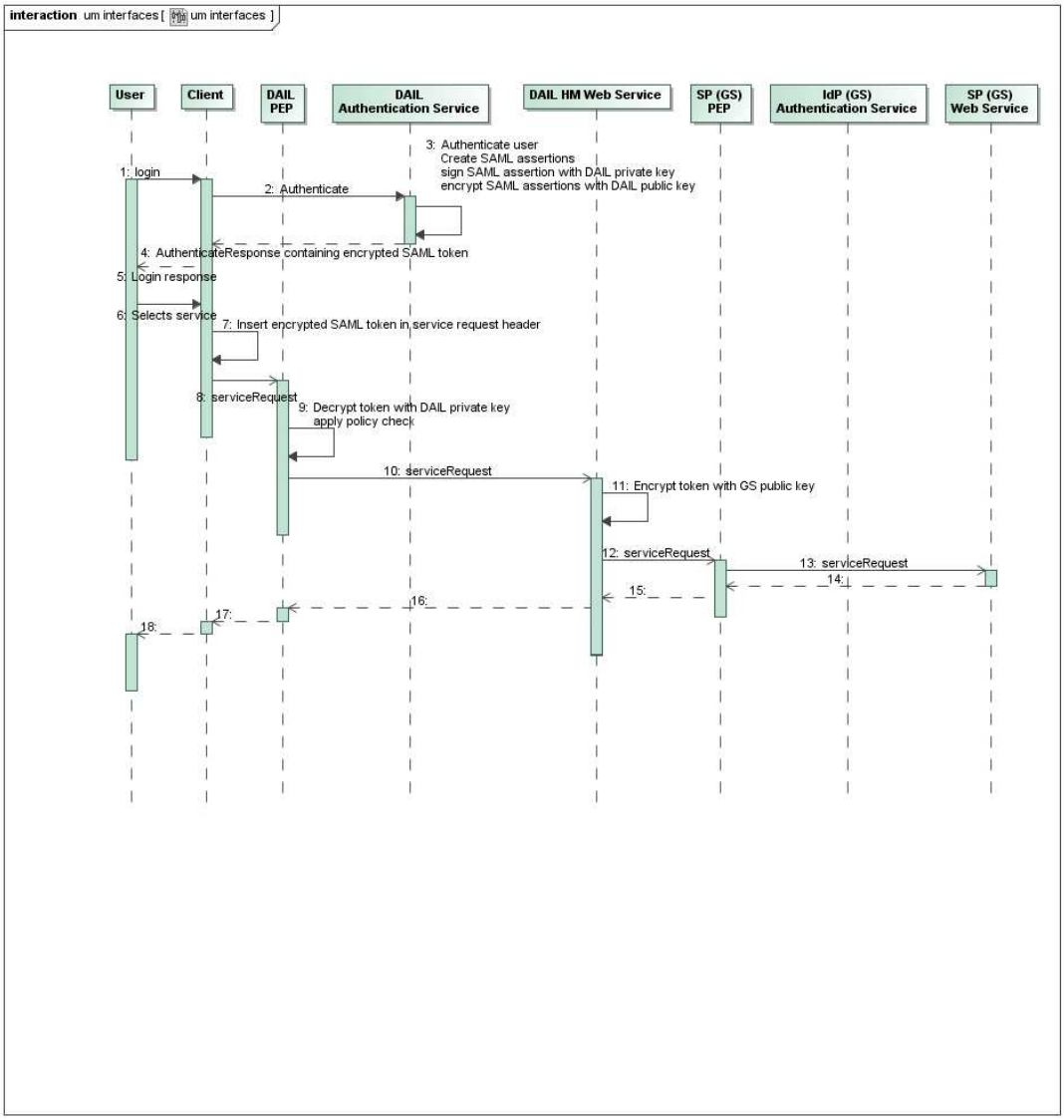

Figure 9 DAIL Sequence Diagram Showing Client Request with synchronous Response

7.3.3 Asynchronous

The asynchronous service response is as defined in the corresponding catalogue, ordering and programming ICDs. This response may be protected by the same encryption and signature as defined for the service request and authentication. The sequence is as follows:

1. The SP prepares the response to the endpoint mentioned in the WS_Addressing.
2. The service provider creates a token authenticating himself i.e. GS and signs it with his private key. This is then encrypted with the public key of the DAIL and inserted into the asynchronous response in the same way as previously described for a service request
3. The asynchronous response is returned to the address provided in the ws_addressing of the request. This will normally be the address of a PEP.

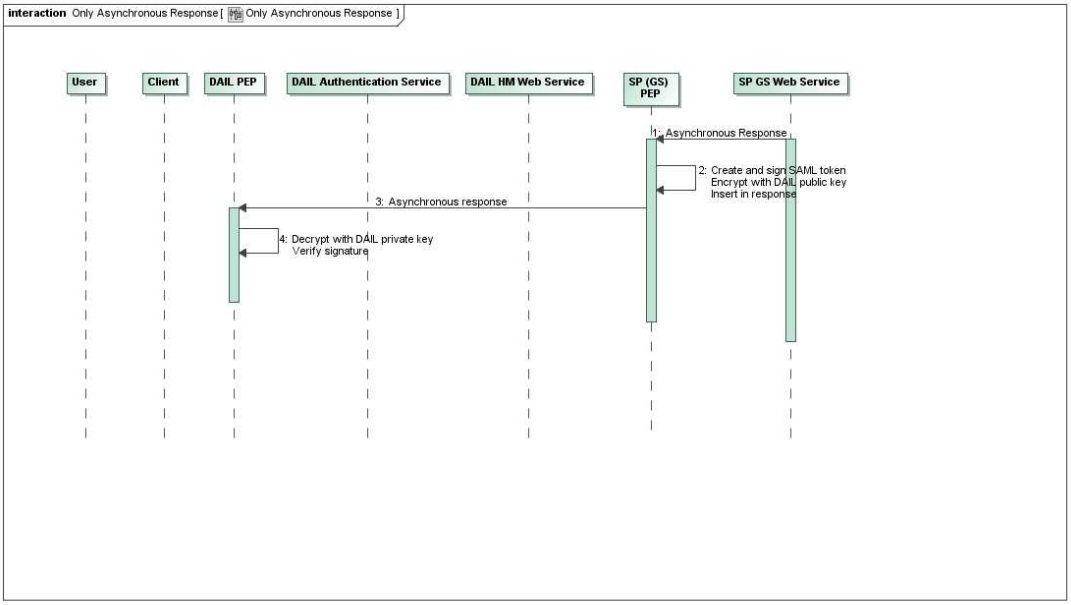

Figure 10 Sequence Diagram showing asynchronous request

Annex - Schemas

authentication.xsd

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns="http://earth.esa.int/um/eop" xmlns:saml="http://earth.esa.int/um/eop/saml"
targetNamespace="http://earth.esa.int/um/eop" elementFormDefault="qualified">
        <xs:import namespace="http://earth.esa.int/um/eop/saml"
schemaLocation="./dail-enc-schema.xsd"/>
        <xs:element name="authenticateResponse">
```

```
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="return">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element ref="saml:Assertion"
minOccurs="0"/>
                                                </xs:sequence>
                                        </xs:complexType>
                                </xs:element>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>
        <xs:element name="authenticate">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="username" type="xs:string"
nillable="true"/>
                                <xs:element name="password" type="xs:string"
nillable="true"/>
                                <xs:element name="serverName" type="xs:string"
nillable="true" minOccurs="0"/>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>

</xs:schema>
```

dail-enc-schema.xsd

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--W3C Schema generated by XMLSpy v2006 sp2 U (http://www.altova.com)-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
targetNamespace="http://earth.esa.int/um/eop/saml"
elementFormDefault="qualified">
        <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"
schemaLocation="http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd"/>
        <xs:element name="Assertion">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element ref="xenc:EncryptedData"/>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>

</xs:schema>
```

oasis-200401-wss-wssecurity-secext-1.0.xsd

http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

oasis-sstc-saml-schema-assertion-1.1.xsd

http://www.oasis-open.org/committees/download.php/3408/oasis-sstc-saml-schema-assertion-1.1.xsd