HMA-S Project
User Management for EO Services
OGC 07-118r9

P. Jacques, Spacebel s.a.

P. Denis, Spacebel s.a.

Y. Coene, Spacebel s.a.

May 17, 2013

Outline

- Task 2: Goals and Topics
- Summary of changes to OGC 07-118r9
- Remaining and future work

Task 2: Identity Management - Specification

- Goals
  - Address pending issues/shortcomings of OGC 07-118 “User Management Interfaces for Earth Observation Services” v1.0 (OGC Best Practice)
  - Provide the specification for Task 2 demonstrator
  - Update ATS and ETS (Intecs)
- Output
  - Best Practice OGC 07-118 v1.1

Task 2: Identity Management - Specification

- Topics
  - I133: wsp:DelegateTo misused
    - goal : delegate RST to an external STS
    - → propose a new XML element for this purpose
  - I134: identification of RST coming from federating STS
    - allow to get SAML token unencrypted and not signed
    - proposition of U. Voges to be analyzed
    - → propose a new mechanism for this purpose
  - I135: Need to reconcile user IDs ?
    - User ID shall be known by one STS, the one that receives the “routed” request

Task 2: Identity Management - Specification

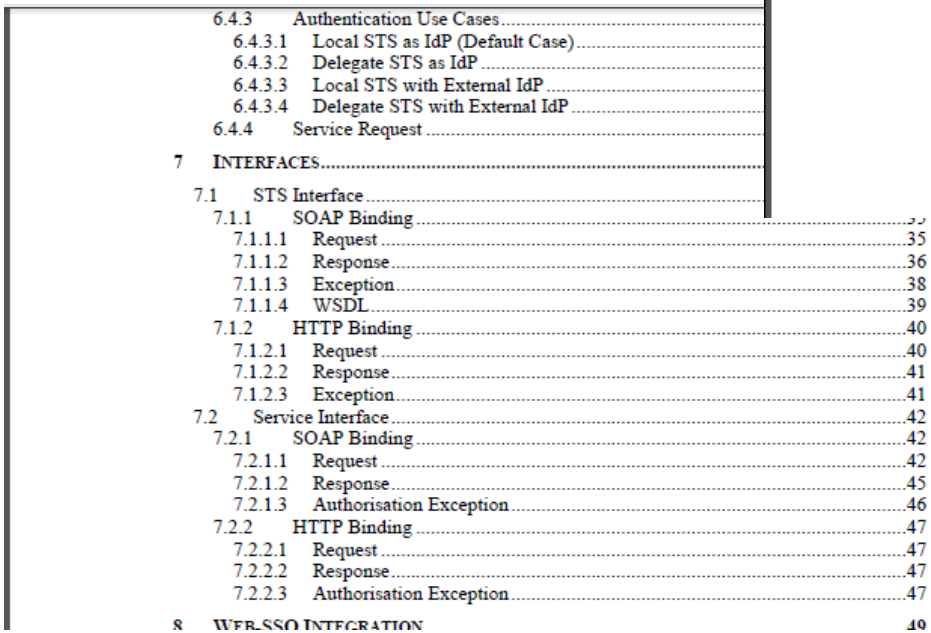
- Topics (cont'd)
  - I136: section "STS with trusted IdP"
    - received comment about the title
    - → add a clarification note
  - I137: wrong statements in section 7.1.3
    - → Obsolete paragraphs to be removed
  - I17: Propose a binding independent structure
    - Review description of uses cases, related to Web-SSO (e.g. EO-SSO)
    - Factorize the use cases according to two axes:

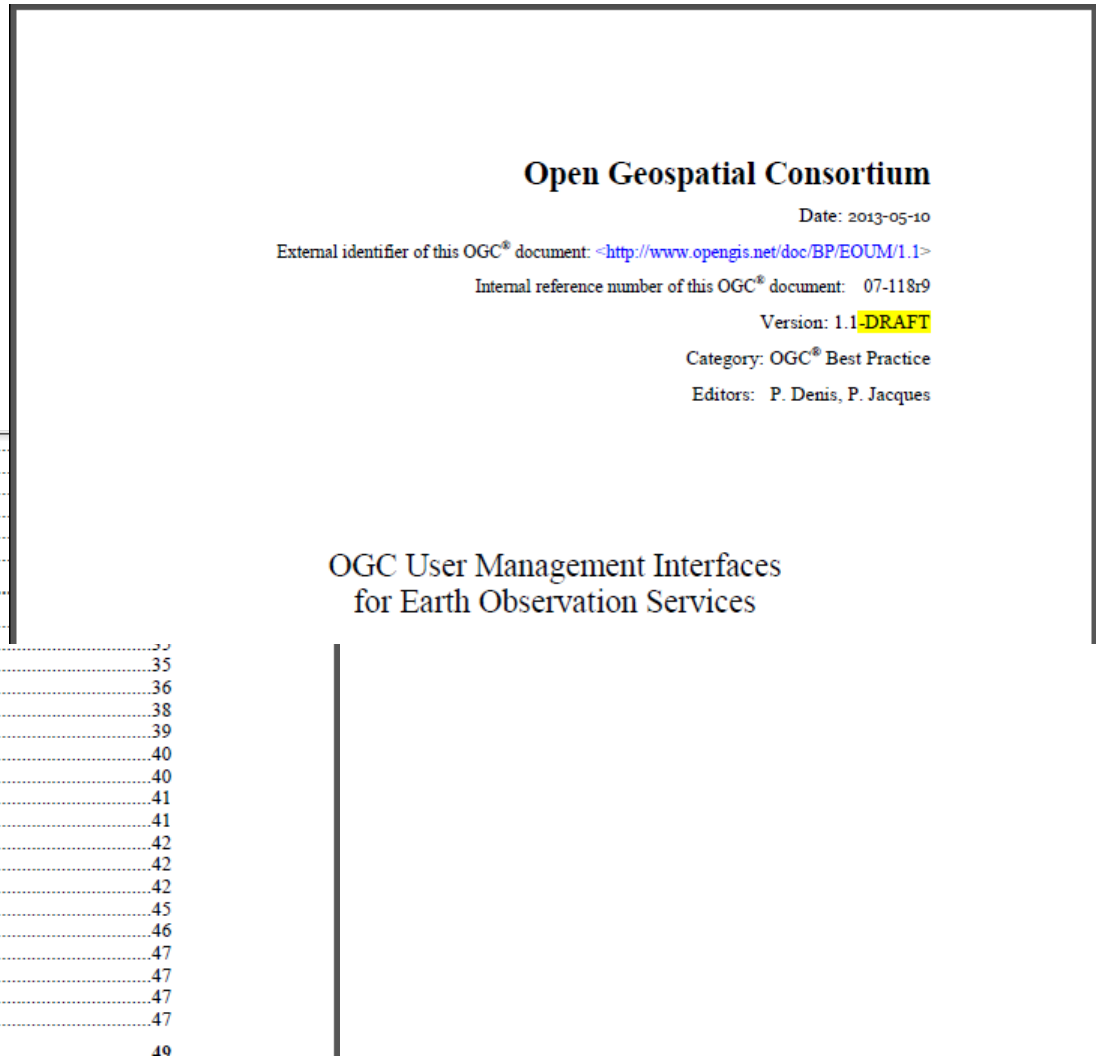
	Autonomous	**Delegation**
IdP = STS	1. STS as local IdP	2. STS as Federating IdP
IdP = Web-SSO	3. STS with trusted IdP	4. *Additional Case*

Summary of Changes to OGC 07-118r9

- General improvement of document structure and figures for enhanced clarity and readability
- Convergence towards new OGC template
- Split “STS with trusted IdP” use case into two cases, for the sake of uniformity on STS delegation
- Added HTTP protocol binding, for both
  - STS interface, and
  - Service interface
- Alignment of all examples with SOAP 1.2
- Alignment with OWS Common for authorisation exceptions on Service requests

OGC Template & Protocol Bindings





Open Geospatial Consortium

Date: 2013-05-10

External identifier of this OGC® document: <http://www.opengis.net/doc/BP/EOUM/1.1>

Internal reference number of this OGC® document: 07-118r9

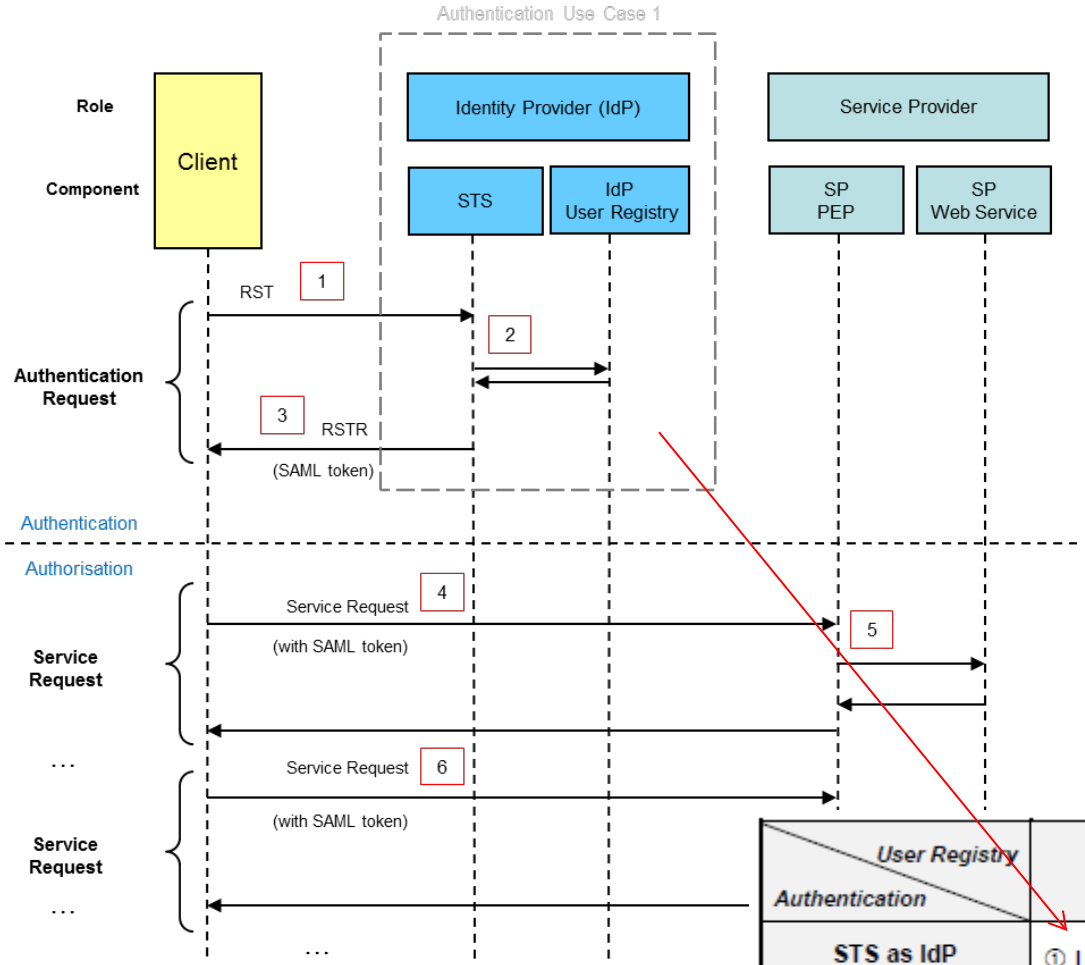
Version: 1.1-DRAFT

Category: OGC® Best Practice

Editors: P. Denis, P. Jacques

OGC User Management Interfaces
for Earth Observation Services

Authentication Use Cases



User Registry / Authentication	Local Registry	External registry (delegation)
STS as IdP	① Local STS as IdP	② Delegate STS as IdP
External IdP (Web-SSO)	③ Local STS with external IdP	④ Delegate STS with external IdP

HTTP Binding – Service Request

7.2.2.1 Request

Note: the present section aims at complying with the "Authorization Request Header Field" defined in OAuth 2.0 Authorization Framework (see NR31]).

The SAML token shall be put in the HTTP header of the request, in a field named "Authorization". The syntax shall obey the following rules, expressed in Augmented Backus-Naur Form (ABNF) (see [NR30]):

```
authorization = "Authorization" ":" 1*SP credentials

credentials = "Bearer" 1*SP b64token
```

The `b64token` element shall be the SAML token, i.e. the xenc:EncryptedData element extracted from the RSTR and converted by a Base64 encoding (see [NR28]).

The following snippet of an HTTP POST request is provided as example.

```
POST http://aaa.bbb.gov/csw HTTP/1.1
Host: aaa.bbb.gov
…
Authorization: Bearer PHhlbmM6RW5jcnlwdGVkRGF0YSBUeXB1PSJodHRwOi8vd3d3LnczLm9yZy8yMDAx
LzA0L3htbGVuYyNFbGVtZW50IiB4bWxuczp4ZW5jPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGVuYy
MiPg … NEkA==
…
Content-Type: application/xml
Content-Length: …

<?xml version="1.0" encoding="UTF-8"?>
<csw:GetRecords maxRecords="10" … xmlns:wrs="http://www.opengis.net/cat/wrs/1.0">
   <csw:Query typeNames="rim:RegistryPackage rim:ExtrinsicObject
      …
   </csw:Query>
</csw:GetRecords>
```

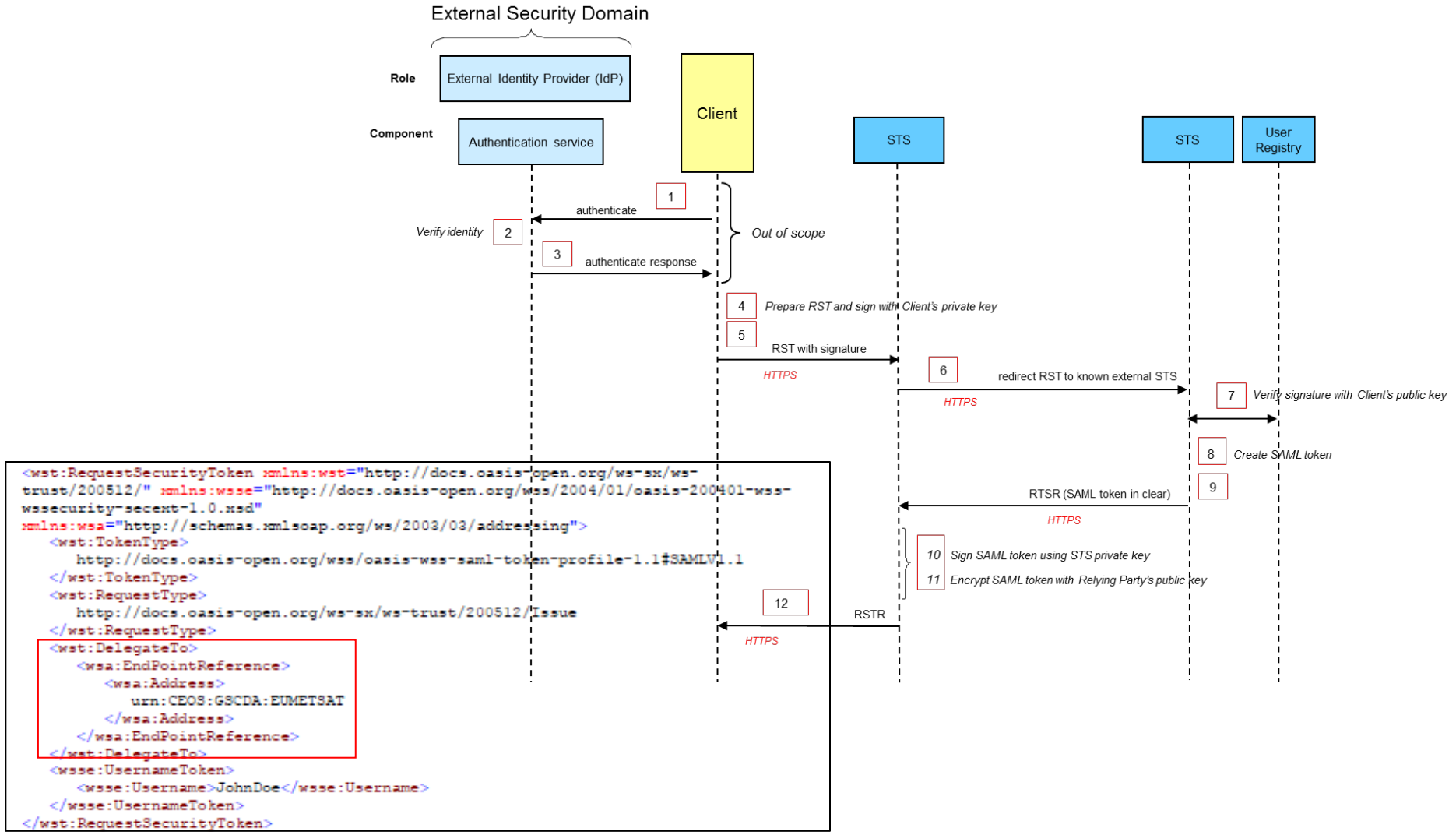
Note that the SAML token is neither included in the request line nor in the message body of the HTTP request. Also, the syntax is independent of the HTTP method used (i.e. GET, POST, etc).

Important caution: Although the HTTP specification does not enforce a limit on the size of header, there exist practical limits imposed by the implementations of HTTP servers. Since the size of the encoded SAML token is relatively large (~5 KB, in our example), it is important to ensure that it can be handled without error by the underlying transport layer, which usually relies on several HTTP servers. As a rule of thumb, the limit of 8 KB is quoted for the total size of HTTP request line and header; in any case, the set of attributes included in the SAML token should be narrowed to the strict authorization needs.

Summary of Changes to OGC 07-118r9

- Updates following issues/recommendations given by con terra on HMA Forum:
  - Correction on type of WS-Trust “DelegateTo” element
  - Mechanism for identification of delegate STS, based on WS-Trust “DelegateTo” element
  - Added missing WS-Trust “DelegateTo” in the ws-trust.xsd schema
  - Clarification on the concept of “STS with trusted IdP”
  - Removal of obsolete text in 7.1.3

STS Delegation

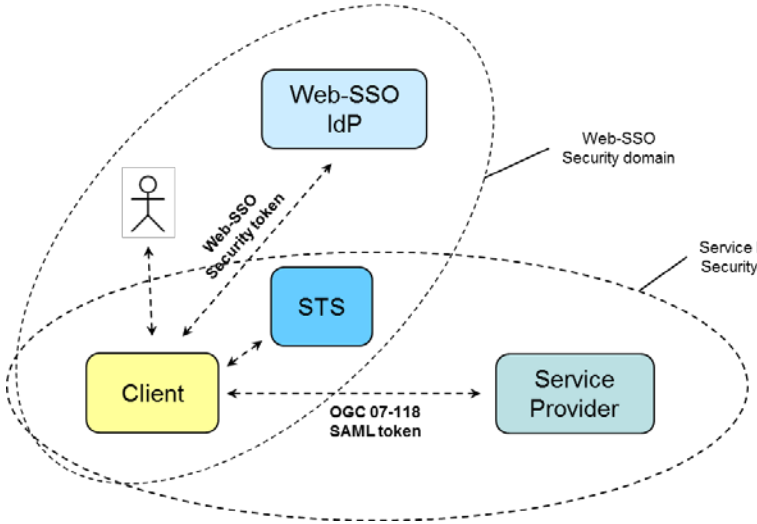


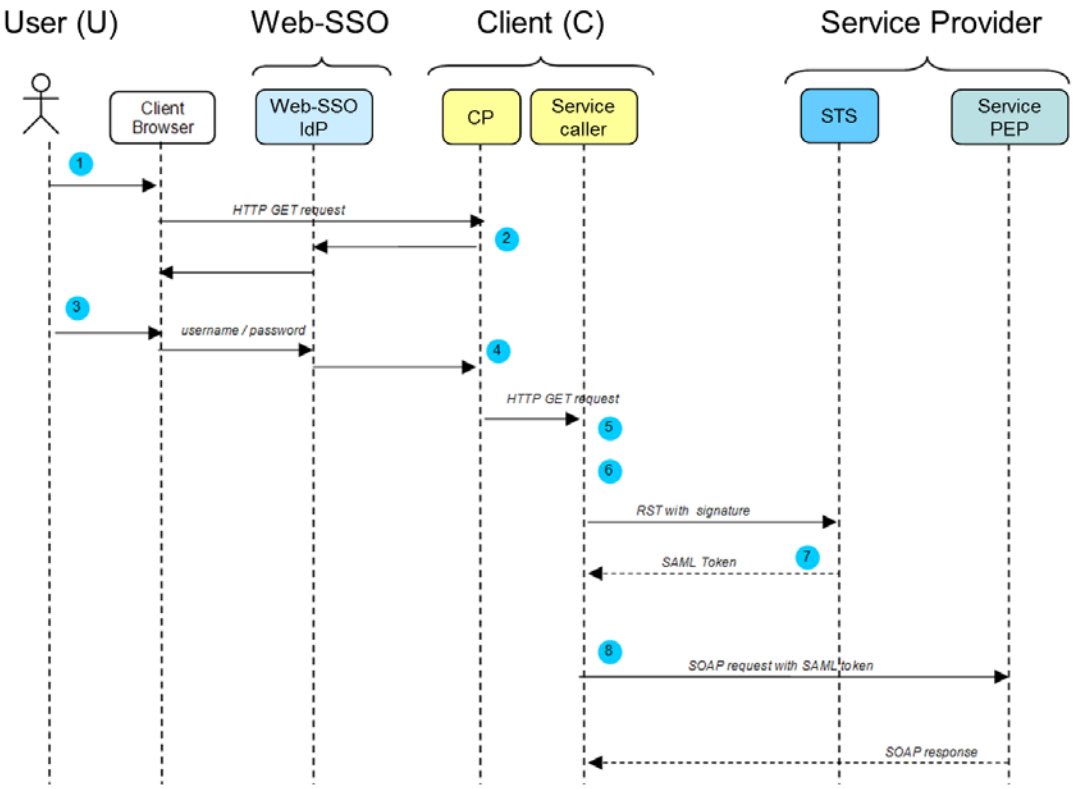

```
<wst:RequestSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-
trust/200512/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/addressing">
   <wst:TokenType>
      http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1
   </wst:TokenType>
   <wst:RequestType>
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
   </wst:RequestType>
   <wst:DelegateTo>
      <wsa:EndPointReference>
         <wsa:Address>
            urn:CEOS:GSCDA:EUMETSAT
         </wsa:Address>
      </wsa:EndPointReference>
   </wst:DelegateTo>
   <wsse:UsernameToken>
      <wsse:Username>JohnDoe</wsse:Username>
   </wsse:UsernameToken>
</wst:RequestSecurityToken>
```

Summary of Changes to OGC 07-118r9

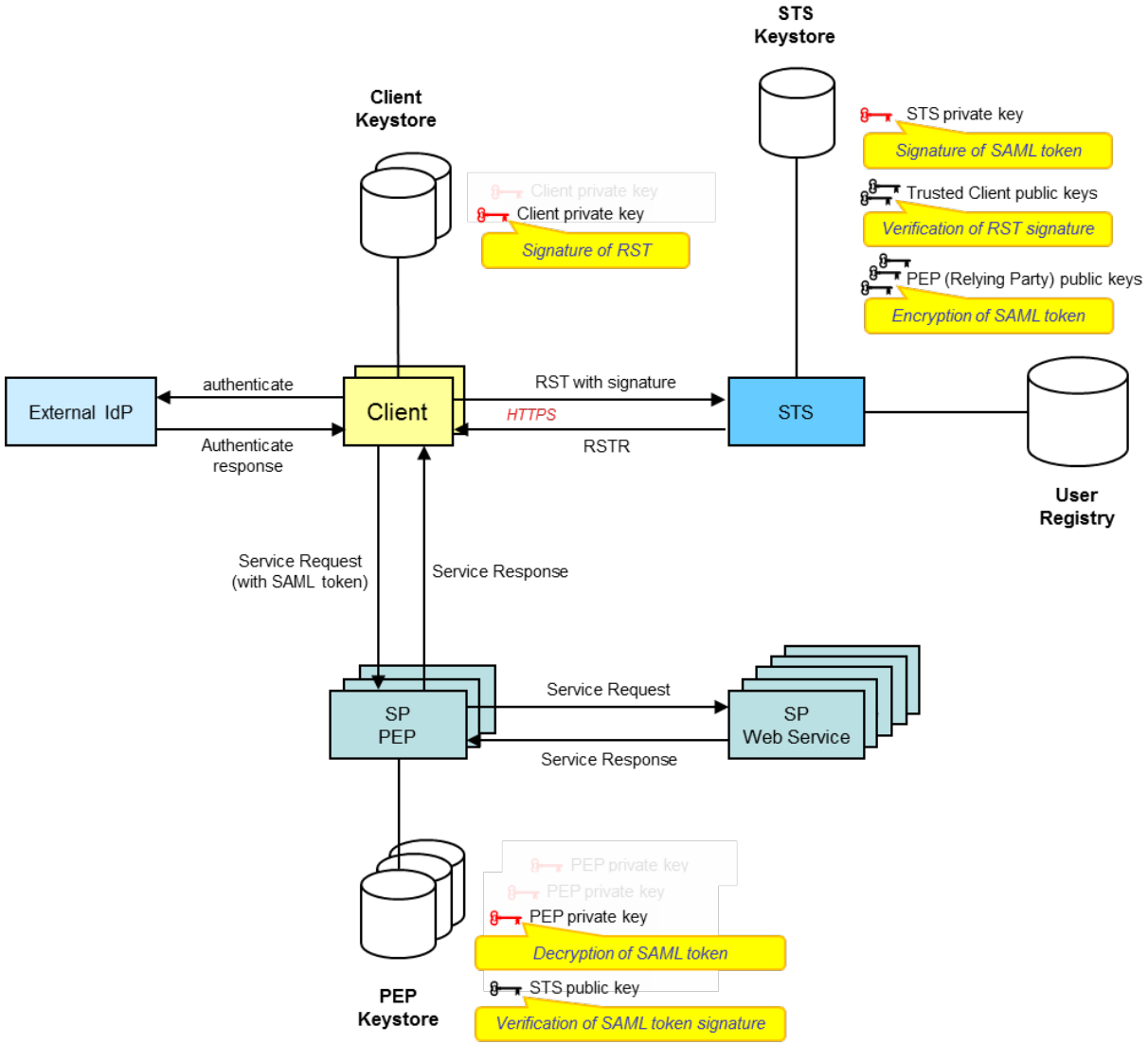
- Updates to address most comments (RIDs) raised by ESA (Andrea Baldi), in particular:
  - Term Client clarified (SW component, service consumer)
  - HL-REQ060 and Web-SSO integration (section 8) clarified
  - Added note on “user id” extracted or derived from Web-SSO attributes (authentication with External IdP)
  - Added note on possible use of different SAML attributes in a multi-PEP configuration (based on AppliesTo in RST)
  - Support for both SAML 1.1 and 2.0
  - Added Figure 4 illustrating the use of keys
  - Removal of HMA specific “minimum profile”
  - Use of OWS Common exception format and definition of authorisation specific exception codes
  - Colour coding and indentation of all XML figures

Web-SSO Integration





Key Management



Service Authorisation Exception

7.2.1.3 Authorisation Exception

When a SOAP request is unauthorised on a server, this server shall respond with a SOAP fault indicating the failure reason (e.g. missing SAML token, invalid SAML token, insufficient privileges, etc). As with all OGC services, the exception report message shall be returned as specified in section 8 of the OGC Web Services Common Standard document [OGC 06-121r9]. However, the HTTP status code value shall be set to 401 Unauthorized.

The authorisation specific exception codes are defined in the table below.

"exceptionCode" value	Meaning of code	"locator" value
MissingToken	Request does not contain a SAML token.	Omit locator parameter
InvalidToken	Request does not contain a valid SAML token, or the token cannot be decrypted, or the token signature is invalid, or the token expired.	Omit locator parameter
TokenVersion	Request contains a SAML token with an unsupported version.	URI of SAML version supported
AuthorisationFailed	Request is for an operation that is not authorised by (the PEP of) this server.	Name of SAML attribute causing the authorisation failure

Table 1: Authorisation Exception Codes

Use HTTP status code **403 Forbidden** for this one?

An example is given below:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Body>
      <soapenv:Fault>
         <soapenv:Code>
            <soapenv:Value>soap:Receiver</soapenv:Value>
         </soapenv:Code>
         <soapenv:Reason>
            <soapenv:Text xml:lang="en">A server exception was
encountered.</soapenv:Text>
         </soapenv:Reason>
         <soapenv:Detail>
            <ows:ExceptionReport xmlns:ows="http://www.opengis.net/ows/2.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.opengis.net/ows/2.0
http://schemas.opengis.net/ows/2.0/owsExceptionReport.xsd" version="1.0.0"
xml:lang="en">
               <ows:Exception exceptionCode="AuthorisationFailed" locator="o">
                  <ows:ExceptionText>Country of origin not
authorised</ows:ExceptionText>
               </ows:Exception>
            </ows:ExceptionReport>
         </soapenv:Detail>
      </soapenv:Fault>
   </soapenv:Body>
</soapenv:Envelope>
```

Remaining and Future Work

- Remaining work
  - Implement remaining RIDs (e.g. from DLR)
  - Authorisation exception for non-OGC services
  - Update Annex A: ATS (Intecs)
  - Improve Annex C (explain all diffs between SOAP 1.1 & 1.2)

- Future work
  - Optional encryption of SAML token
  - Compression of SAML token (HTTP binding, Service interface)
  - SAML token in URL using KVP (...?Bearer=...&...)

When confidentiality of attributes not required
or
When using encrypted attributes in SAML 2.0

SAML token (encrypted or not)
➔ compress (e.g. deflate)
➔ Base64 encoding

same +
➔ URL encoding