User Management Interfaces for Earth Observation Services – Abstract Test Suite

Primary Author
Andrew Woolf, STFC Rutherford Appleton Laboratory

Revision history

Version	Contributors	Date	Changes
0.1	Andrew Woolf	2009-01-31	First draft ATS for 07-118r1

Overview

The OGC specification 07-118r1 (User Management Interfaces for Earth Observation Services) specifies how EO protocol definitions (e.g. catalogue, ordering, programming) may be supplemented with user and identitiy management information. It describes how existing specifications (WS-Security, SOAP) may be used to implement authentication and authorisation for EO services.

This document specifies an Abstract Test Suite for the User Management Interfaces.

References

[ISO 19105] ISO 19105:2000, “Geographic information – Conformance and testing”
[07-118r1] OGC 07-118r1, “User Management Interfaces for Earth Observation Services”
[HMAT-TN-0001-IGN] IGN, “HMA-T Phase 2 Testing Policy”

Contents

Annex A: ABSTRACT TEST SUITE (NORMATIVE)

A.1 Conformance Test Class : The Core

A.1.1 Authentication: Federating Entity is request-designated IdP

The authentication request contains an identifier for the federating entity authentication service.

a) Test Purpose: For authentication purposes, the Identity provider (IdP) role may be fulfilled by the entity receiving the service request (the 'federating entity'). The request must include an identifier indicating this. This test verifies that such a request authenticates successfully.

b) Test Method: Send an authentication request with credentials (username and password) that are recognised and validated by the Federating Entity authentication service, and receive in return a SAML token encrypted and signed by the Federating Entity.

c) Reference: OGC 07-118r1, clause 6.4.3.1

d) Test Type: Basic

A.1.2 Authentication: External entity is request-designated IdP

The authentication request contains an identifier for the external entity authentication service.

a) Test Purpose: For authentication purposes, the Identity provider (IdP) role may be fulfilled by a named entity external to the Federating Entity. This test verifies that such a request authenticates successfully.

b) Test Method: Send an authentication request with credentials (username and password) that are recognised and validated by a specified External Entity separate from the federating IdP, and receive in return a SAML token encrypted and signed by the Federating Entity.

c) Reference: OGC 07-118r1, clause 6.4.3.2

d) Test Type: Basic

A.1.3 Authentication: No request-designated IdP – but Federating entity is resolved as IdP

In this use case there is no IdP specified in the authentication request. The authentication service resolves the IdP from the part profile stored in the local user registry which in this case contains an identifier for the local federating entity authentication service.

a) Test Purpose: For authentication purposes, the Identity provider (IdP) role may be fulfilled by the Federating Entity, even though not specified explicitly in the request. This test verifies that such a request authenticates successfully.

b) Test Method: Send an authentication request with credentials (username and password) that are recognised and validated by the local Federating Entity authentication service – even though not specified explicitly – and receive in return a SAML token encrypted and signed by the same Federating Entity.

c) Reference: OGC 07-118r1, clause 6.4.3.3

d) Test Type: Basic

A.1.4 Authentication: No request-designated IdP – but External entity is resolved as IdP

In this use case there is no IdP given in the authentication request. The authentication service resolves the IdP from the part profile stored in the local user registry which in this case contains an identifier for an external entity authentication service.

a) Test Purpose: For authentication purposes, the Identity provider (IdP) role may be fulfilled by an external entity, even though not specified explicitly in the request. This test verifies that such a request authenticates successfully.

b) Test Method: Send an authentication request with credentials (username and password) that are recognised and validated by an External Entity – unspecified in the request – separate from the federating authentication service and receive in return a SAML token encrypted and signed by the Federating Entity. The External Entity is resolved through a lookup on the local user registry.

c) Reference: OGC 07-118r1, clause 6.4.3.4

d) Test Type: Basic

A.1.5 Authentication: Test module for WS-Security

The security model is based on the WS-Security SAML token profile. An 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. An encrypted and signed SAML token is returned in the WS-Security element of SOAP header and returned over SOAP over HTTPS. The client is able to verify the signature but is unable to decrypt (and therefore modify) the content.

A.1.5.1 WS-Security: Encryption

Encryption and decryption of the SAML token is performed by the authentication service during an authentication request and response. It is performed by the Policy Enforcement Point during the authorization request and response. The encryption algorithm proposed is AES-128.

a) Test Purpose: Verification of correct encryption by Federating Entity.

b) Test Method: For the purpose of this test, the conformance test environment has a copy of the Federating Entity private key, as well as its public key. Send an authentication request with credentials (username and password) that are recognised and validated by the Federating Entity authentication service, and receive in return a SAML token encrypted and signed by the Federating Entity. Verify encryption using the Federating Entity private key.

c) Reference: OGC 07-118r1, clause 6.4.6.1

d) Test Type: Basic

A.1.5.2 WS-Security: Digital signature

The secure hash SHA-1 digital signature message digest algorithm is proposed.

a) Test Purpose: Verification of correct digital signature by Federating Entity.

b) Test Method: Send an authentication request with credentials (username and password) that are recognised and validated by the Federating Entity authentication service, and receive in return a SAML token encrypted and signed by the Federating Entity. Verify digital signature using Federating Entity public key.

c) Reference: OGC 07-118r1, clause 6.4.6.2

d) Test Type: Basic

A.1.5.3 WS-Security: SAML profile

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

SAML 1.1 is proposed to encode the user authentication token.

a) Test Purpose: Verification of correct construction of SAML token.

b) Test Method: For the purpose of this test, the conformance test environment has a copy of the Federating Entity private key, as well as its public key. Send an authentication request with credentials (username and password) that are recognised and validated by the Federating Entity authentication service, and receive in return a SAML token encrypted and signed by the Federating Entity. Decrypt SAML token using Federating Entity private key, and confirm structure of SAML token: valid SAML format, correct AuthenticationStatement, correct AttributeStatement.

c) Reference: OGC 07-118r1, clauses 6.4.5 and 7.1.3

d) Test Type: Basic

A.1.6 Authentication: Failed authentication request

A SOAP fault must be returned in response to an authentication request with invalid credentials (invalid username or password).

a) Test Purpose: Verification of fault response on failed authentication request.

b) Test Method: Send an authentication request with invalid credentials (invalid username or password), and receive in return an appropriate SOAP fault.

c) Reference: OGC 07-118r1, clause 7.1.4

d) Test Type: Basic

A.1.7 Authorisation: Synchronous response

Having obtained a SAML token from an authentication request, a user may submit an external service request to the Federating Entity. However, the service may not be invoked unless the requester is authorised to do so. Two

levels of policy enforcement may be applied – at both the Federating Entity (e.g. controlling access to the service), and at the (external) Service Provider (e.g. controlling invocation of the specific request). The process used at both stages is the same: verifying the signed request, decrypting and verifying the SAML token, retrieving user information from the local user registry, enforcing authorisation policy.

a) Test Purpose: Invocation of a requested service is not allowed unless the client has appropriate authorisation. This test verifies that an appropriately-authorised service request successfully completes.

b) Test Method: A service request is sent to the Federating Entity; it contains a SAML token previously obtained through an authentication request. The user is authorised both to access the requested service, and to make the specific service request. The request executes successfully and results are returned in a synchronous response.

c) Reference: OGC 07-118r1, clause 6.4.4.1

d) Test Type: Basic

A.1.8 Authorisation: Asynchronous response

Behaviour of a service request with asynchronous response is not completely defined by the User Management specification (07-118r1). Only internal behaviour is described, but interaction with a user/client is undefined. In particular, the response to the service request is first sent synchronously to the Federating Entity, which then processes the response with a 'dispatcher service', responsible for the asynchronous interaction with the client. As noted (07-118r1 clause 6.4.4.2), the response processing by the dispatcher service "is not further described as it is implementation dependent and the persistence and correlation management required is outside the scope of this document."

Since the interaction is implementation dependent, it is not appropriate to define a conformance test.

A.1.9 Authorisation: Test module for failed authorisation requests

A SOAP fault must be returned in response to a failed authorisation request. This may occur for any of a number of reasons: a non-present SAML token for a protected service, an invalid SAML token, an expired SAML token, not authorised to use service (determined by Federating Entity PEP), not authorised for specific service request (Service Provider PEP).

A.1.9.1 Authorisation: Failed authorisation request (SAML token not supplied)

a) Test Purpose: Verification of fault response authorisation request lacking required SAML token.

b) Test Method: Send an authorisation request (i.e. a service request) with no SAML token present and receive in return an appropriate SOAP fault.

c) Reference: OGC 07-118r1, clause 7.2.3

d) Test Type: Basic

A.1.9.2 Authorisation: Failed authorisation request (invalid SAML token)

a) Test Purpose: Verification of fault response on authorisation request with invalid SAML token.

b) Test Method: Send an authorisation request (i.e. a service request) with an incorrectly structured SAML token and receive in return an appropriate SOAP fault.

c) Reference: OGC 07-118r1, clause 7.2.3

d) Test Type: Basic

A.1.9.3 Authorisation: Failed authorisation request (expired SAML token)

a) Test Purpose: Verification of fault response on authorisation request with expired SAML token.

b) Test Method: Send an authorisation request (i.e. a service request) with an expired SAML token and receive in return an appropriate SOAP fault.

c) Reference: OGC 07-118r1, clause 7.2.3

d) Test Type: Basic

A.1.9.4 Authorisation: Failed authorisation request (not authorised to use service)

a) Test Purpose: Verification of fault response on service request to unauthorised service.

b) Test Method: Send a service request for a service the user is not authorised to access. An authorisation failure should be enforced by the Federating Entity PEP, and an appropriate SOAP fault returned.

c) Reference: OGC 07-118r1, clauses 6.4.4.1 and 7.2.3

d) Test Type: Basic

A.1.9.5 Authorisation: Failed authorisation request (specific request not authorised)

a) Test Purpose: Verification of fault response on unauthorised service request to allowed service

b) Test Method: Send an unauthorised service request to an allowed service (the request may be unauthorised due to its size, data access policies, etc.). An authorisation failure should be enforced by the Service Provider PEP, and an appropriate SOAP fault returned.

c) Reference: OGC 07-118r1, clauses 6.4.4.1 and 7.2.3

d) Test Type: Basic

Annex B: EXECUTABLE TEST SUITE (NORMATIVE)

This section tbd.