Open Geospatial Consortium

License-Based Access Control

Warning

Contents page

Table of Requirements

Req 1 <u>**Licence broker information:**</u>**A service that requires licences and/or other licence-related documents for use shall include in its capabilities document an tagged element** `<rightsInformation>` **whose content is a URI that links to any and all information that a client requires to obtain the needed licence, licences or other information. The type shall be expressed as a 'type' attribute of the** `<rightsInformation>` **element, containing another URI identifying the format of the referenced information.**

i.   Abstract

This Discussion Paper proposes model for license-based access control to SOAP services, based on OASIS SAML 2.0. This approach is a potential solution for license-based access control, which requires the possession of a valid license for getting access to a service. Use of digital licenses allow users to act on or with web services to which they are associated

This document re-uses content produced by the OGC GeoRM Common 1.0 Standards Working Group and combined that with the document OGC 10-125, which was posted to an internal OGC document archive (Pending Documents) but is not publicly available.

This document does not claim compliance to the GeoDRM reference model (ISO 19153), although the authors are not yet aware of any conflicts to it.

ii.   Keywords

ogcdoc, georm, saml, soap

iii.   Preface

Suggested additions, changes, and comments on this draft report are welcome and encouraged. Such suggestions may be submitted by email message or by making suggested changes in an edited copy of this document.

iv.   Document terms and definitions

This document uses the standard terms defined in Subclause 5.3 of [OGC 05-008], which is based on the **ISO/IEC Directives, Part 2. Rules for the structure and drafting of International Standards**. In particular, the word "shall" (not "must") is the verb form used to indicate a requirement to be strictly followed to conform to this standard.

v.   Submitting organizations

The following organizations submitted this document to the Open Geospatial Consortium.

Organization name(s)

con terra GmbH
University of Muenster - Institute for Geoinformatics

vi.   Document contributor contact points

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

Name	Organization
Rüdiger Gartmann,	con terra GmbH
Bastian Schäffer,	University of Muenster - Institute for Geoinformatics

vii.   Revision history

Date	Editor	Primary clauses modified	Description
10 Feb 2011	Rüdiger Gartmann	All	Merge from latest draft of GeoRM Common draft specifrication and pending document # 10-125
29 Mar 2011	Rüdiger Gartmann	4	Reference to terms and definitions from GeoDRM Reference Model

viii.   Changes to the OGC Abstract Specification

The OpenGIS® Abstract Specification does not require changes to accommodate the technical contents of this document.

ix.   Future work

This Discussion Paper proposes model for licence-based access control to SOAP services, based on OASIS SAML 2.0. This specification should be matured towards an Implementation Standard.

Foreword

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

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation

Introduction

This specification focuses on SOAP services and defines the following aspects:

- Use of digital licences that allow users to act on or with web services to which they are associated.
- The association of web service requests to specific licences and/or other licence-related documents.
- The verification of the licences and/or other licence-related documents and their combination with service requests to allow the execution of the requested actions.
- A licence model based on OASIS SAML 2.0, expressing access permissions to services.
- Extending service capabilities to include WS-Policy definitions of rights management-specific preconditions.
- Protocol extension to include rights management information in the SOAP header.

OpenGIS® License-Based Access Control

1 Scope

This document specifies the use of OASIS SAML for licence encoding, the implementation details for the use of this licence encoding for expressing access permissions to SOAP services, and the submission and evaluation of these licences with in service requests.

2 Compliance

There are three conformance classes in the abstract test suite concerning the licence model, the GetCapabilities extension, and the protocol extension defined in this specification:

A.1 Conformance Class: General Requirements
A.2 Conformance Class: Licence Model
A.3 Conformance Class: GetCapabilitiesextension
A.4 Conformance Class: SOAP Protocol

A compliant service must satisfy all requirements of this specification.

3 Normative references

The following normative documents contain provisions that, through reference in this text, constitute provisions of this document. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the normative document referred to applies.

ISO 19105:2000, *Geographic information — Conformance and Testing*

OGC 06-121r3, *OpenGIS® Web Services Common Specification[1]*

OASIS *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*

OASIS *Web Services Security: SOAP Message Security 1.1*

---

[1]This OWS Common Specification contains a list of normative references that are also applicable to this Implementation Specification.

OASIS *Web Services Security: SAML Token Profile 1.1*

OASIS*SAML 2.0 Profile of XACML,Version 2*

W3C*Web Services Policy 1.2 - Framework (WS-Policy)*

OASIS*WS-SecurityPolicy 1.2*

OGC 07-158,*Wrapping OGC HTTP-GET/POST Services with SOAP*

4 Terms and definitions

For the purposes of this standard, the definitions specified in Clause 4 of the OWS Common Implementation Specification [OGC 06-121r3] and in Clause 4 of the Geospatial Digital Rights Management Reference Model (GeoDRM RM) [OGC 06-004r4].

5 Conventions
5.1 Abbreviated terms

Some more frequently used abbreviated terms:

GeoRM   Geospatial Rights Management
OASIS   Organization for the Advancement of Structured Information Standards
SAML   Security Assertion Markup Language
SOAP   Formerly: Simple Object Access Protocol
XACML   eXtensible Access Control Markup Language

5.2 UML notation

Any UML used in this document will be conformant with UML 2.0.

6 General Requirements
6.1 Capabilities module

Since the licenced-protected service requires the user to acquire a licence, it is logically necessary that during the "find" process of the services "publish, find, bind, execute" cycle, the client needs to discover information on how to acquire this licence. This logically says that the "capabilities document" of the service (as defined in OWS common) should contain rights management information acquisition process information.

Req 2	**Licence broker information:A service that requires licences and/or other licence-related documents for use shall include in its capabilities document an tagged element `<rightsInformation>` whose content is a URI that links to any and all information that a client requires to obtain the needed licence, licences or other information. The type shall be expressed as a 'type' attribute of the `<rightsInformation>` element,**

      containing another URI identifying the format of the referenced information.

The actual acquisition of the licence may follow any "business model" appropriate, so the form of the target of the rights information URI is not fixed.

A request to a licence-protected service will have to contain both the request from the original non-protected service, and some number of licences and/or other licence-related documents. To assure that the association of the request and the licences are under the control of the licencee, this set of elements needs to be signed by all licencees whose licences are being used. Note that some licences use the same "public key holder" identity that are used in signatures, allowing the common use of this key-system pair to both sign the request and match signatory to licencee.

> **Req 3**   <u>Signature information:</u>**A valid service request shall include signatures for each distinct licencee whose licence is being used in the request. This signature shall cover the service interface, all licences and other**licence-related **information. The identity of the signatory shall be provably equal to the identity of the licencee.**

Recommendation: Identity Reuse In cases where it is possible, the identities used in the licences and the identities in the signature should be equal**.**

6.2 Enforcement point module

Once the request and the licenceare delivered to the services, the enforcement process validates the request. Once a licence-protected service receives a request and its associated licences and/or rights management-specific data, the service may invoke a rights decision process as described in the XACML specification that matches the request with the licences and/or other licence-related documents and other context information to derive an access decision that allows the execution of the services if the semantics of the request are a subset of the acts allowed by the context and personal licences and/or licence-related documents.

> **Req 4**   <u>Enforcement point</u>**: Once a licence-protected service receives a request and its associated licences, the service shall allow the process to proceed if and only if the request is verifiable against a combination of the public context and personal licences data supplied by the request.**

Note   If the request does not require a licence or other rights management data, the process verification decision is always to complete the request. This is essentially a "public licence" in the servers context for the enforcement point that is used by the Enforcement point whenever this type of request is received.

6.3   Error handling module

If the decision process does not authorize a request, the service may respond with a licence-specific error message. Alternatively, it may respond with any message allowed by the underlying service specification to avoid information leakage due to a licensing error. If a licensing-specific error message is used, it shall reflect the invalid licenceand/or other licence-related data

> **Req 5   Error handling: Whenever a licence-protected service receives a request that cannot be authorized, it shall respond either with a licensing error message or a response compliant to the underlying service specification. Licensing error messages shall either refer to insufficient rights, incomplete licences, or invalid licences.**

Note   This allows services to respond with a message that does not include the complete requested semantics without further notice. Nevertheless, this may be desired to protect a service against information leakage by revealing that the request touches restricted information.

6.4   Licence submission to SOAP services

In this profile, the licences and associated information are included as SOAP header elements or as subelements of a header element.

> **Req 6   SOAP with licence headers: For SOAP services, licences and/or other licence-related documents shall be included in the `<header>` element or a sub elements of the `<header>` element of the SOAP envelope.**

To achieve non-repudiation for requests to a licence-protected service, licences and/or other licence-related documents are associated with the request body by a common signature.

> **Req 7   Common signature for licence header and request body: The SOAP header shall contain a signature element, which signs the reuqest body and the licence header element and all related security header elements together in order to associate the licence element with the request body.**

Note: This does not affect the need for signing and/or encrypting the licences and/or other licence-related documents, if required by the licence specification.

For the handling of the headers all rules defined in the SOAP specification remain applicable.

7   SAML licence model

Licences are expressed based on OASIS SAML 2.0 assertions. Within these assertions, grants are expressed based on the OASIS SAML 2.0 Profile of XACML, Version 2.

7.1 SAML licence document

A licence expresses grants or rights of a subject on a certain resource. Additionally licences may include zero or more attributes as additional licence content.

Req 8   <u>Licence Encoding:</u>**A licence is expressed as a SAML 2.0 assertionand shall include an issuer element and an XACMLPolicyStatement based on the OASIS SAML 2.0 Profile of XACML, Version 2. It shall be compliant with the XML Schema in Annex B.1.**

It is recommended that the licence document is signed by the issuer to ensure authenticity, integrity and non-repudiation of the licence's existence. Furthermore it may contain an AttributeStatement including zero or more attributes, expressing licence attributes. Anenforcement point, however, is supposed to verify the licence's signature and then evaluate the XACMLPolicyStatement for the rights decision process.

The following XML Schema fragment defines the structure of a licence document:

```
<xs:elementname="Licence" type="lic:LicenceType" />
<xs:complexType name="LicenceType">
    <xs:complexContent>
        <xs:restriction base="saml:AssertionType">
            <xs:sequence>
                <xs:elementref="saml:Issuer" />
                <xs:elementref="ds:Signature"minOccurs="0" />
                <xs:elementref="saml:Subject"minOccurs="0" />
                <xs:elementref="saml:Conditions"minOccurs="0" />
                <xs:choicemaxOccurs="unbounded">
                    <xs:elementref="saml:Statement" />
                    <xs:elementref="saml:AttributeStatement" />
                </xs:choice>
            </xs:sequence>
        </xs:restriction>
    </xs:complexContent>
</xs:complexType>
```

It is recommended that a licence is only regarded as valid if retrieved from the licence issuer directly. This allows an easy licence revocation by the licence issuer at any time by simply not delivering the licence on an according request.

7.2 Licence reference document

Instead of submitting a complete licence within a request to a rights-managed service, a client can claim the possession of a licence by submitting a licence reference document. This refers to a licence being maintained by the licence issuer.

Req 9   <u>Licence Reference Encoding:</u>**The licence reference document shall be compliant with the XML Schema in Annex B.1 and consist of a**

> **SAML 2.0 assertion containing an AttributeStatement with the attribute names "LicenceProviderURI" and "LicenceID". The value for the "LicenceProviderURI" attribute shall be of the type "anyURI" and for the "LicenceID" attribute of the type "string".**

The following XML Schema fragment describes the structure of a licence reference document:

```xml
<xs:elementname="LicenceReference" type="lic:LicenceReferenceType" />
<xs:complexType name="LicenceReferenceType">
    <xs:complexContent>
        <xs:restriction base="saml:AssertionType">
            <xs:sequence>
                <xs:elementref="saml:Issuer" />
                <xs:elementref="ds:Signature"minOccurs="0" />
                <xs:elementref="saml:Subject"minOccurs="0" />
                <xs:choice>
                    <xs:elementref="saml:AttributeStatement" />
                </xs:choice>
            </xs:sequence>
        </xs:restriction>
    </xs:complexContent>
</xs:complexType>
```

7.3   Enforcement pointbehavior

The enforcement point uses the licence for its rights decision. To allow an easy revocation of licences, the enforcement point shall receive a licence reference from the client and request the licence directly from its issuer. This enables the licence issuer to hold back licences if they are regarded as revoked.

> **Req 10   <u>Enforcement Point Behavior:</u>Anenforcement point shall only accept licences if they are received from their issuer directly.**

Anenforcement point is supposed to verify the licence's signature and then evaluate the XACMLPolicyStatement for the rights decision process.

8   GetCapabilitiesextension
8.1   Introduction

A GeoRM-compliant service extends its capabilities document with a `<rightsInformation>` element, indicating the requirements for licences and/or other licence-related documents. This extension defines the types of these elements and the according information it links to.

Furthermore, the content of the capabilities may depend on the submitted licence and/or other licence-related documents. This section defines the behavior of the GetCapabilities operation depending on the submitted rights management information.

8.2   Rights information extension of service capabilities

To discover the rights management-specific requirements of a service, the <rightsInformation> node extends the standard capabilities document as specified in Req 1.This element links to a WS-Policy document describing all licensing-specific requirements, either globally for the complete service or individually for each operation.

> **Req 11   Rights Information Info Type:**The 'type' attribute of the `<rightsInformation>` element defined in Req1 shall contain the URI urn:ogc:def:georm:preconditions:ws-policy.
> **Req 12   Rights Information Info Value:**The value of the `<rightsInformation>` element defined in Req1 shall be a URI pointing to a WS-Policy version 1.2 document.

There are other means of retrieving a WS-Policy 1.2 description for a service, e. g. by using WS-MetadataExchange of linking the WS-Policy document from the service's WSDL description. However, it is recommended that either way leads to the same WS-Policy document.

8.3   Precondition encoding

The preconditions shall be encoded in a WS-Policy document. This document can include more requirements than needed for rights management only. A request shall only be accepted if all requirements from the WS-Policy document are fulfilled.

> **Req 13   Licence Precondition:**The referenced WS-Policy document from Req11 shall require a licence.
> **Req 14   Identity Precondition:**The referenced WS-Policy document from Req 12 shall require a an identity for authentication purposes. This identity precondition shall make use of one of the Identity preconditions specified in the WS-SecurityPolicy specification (such as i.e. SAML or X509 tokens).
> **Req 15   Precondition Schema:**The licence precondition shallcomply with the schema listed in Annex B.2.

8.4   Capabilities document of rights-managed services

Also access to the GetCapabilities request can be subject to protection and require a licence and/or other licence-related documents. This may lead to different capabilities contents depending on the submitted licences and/or other licence-related documents. However, it is recommended that the GetCapabilities request is in any case, even without any rights management-related information, responded with a capabilities document including at least the <rightsInformation> node as a means for bootstrapping the service.

Note   In any case a GetCapabilities request has to be answered with a capabilities document
             compliant to the specification of the underlying service or with an error message.

9   SOAP Protocol

This specification is designed for SOAP communication only. However, it is possible to
apply it to services with a HTTP-GET/Key-Value-Pair and a HTTP-POST/XML
parameter encoding if both the Gatekeeper component and the client support a protocol
transformation as specified in the OGC Discussion Paper "*Wrapping OGC HTTP-
GET/POST Services with SOAP*" (OGC document #07-158).

9.1   Embedding the licence element

**Req 16   Licence Embedding:The licence shall be embedded in the SOAP
             request header following Web Service Security: SAML Token
             Profile 1.1.**

9.2   Request signature

According to Req 6 of the GeoRM Common specification, the request shall include a
signature element signing the licence and/or other related documents in the SOAP header
together with the SOAP body.

**Req 17   Request Signature:The signature of the licence and the identity
             assertion together with the SOAP body shall be compliant to the
             WS-Security 1.1 specification.**

Note: This specification does neither prevent additional signatures in the request nor encryption of
             request elements.

Annex A
(normative)

Abstract test suite

A.1   Conformance Class: General Requirements
A.1.1 Licence broker information (Req 2)

A service that requires licences and/or other licence-related documents for use shall include in its capabilities document an tagged element `<rightsInformation>` whose content is a URI that links to any and all information that a client requires to obtain the needed licence, licences or other information.

    a) Test Purpose: Verify that this requirement is satisfied by the servers capabilities document.
    b) Test Method: Inspect the capabilities document to verify the proper use of these elements.
    c) Reference: Clause 6.1,
    d) Test Type: Conformance.

A.1.2 Signature information (Req 3)

A valid service request shall include signatures for each distinct licencee whose licence is being used in the request. This signature shall cover the service interface, all licences and other**r**licence-related information. The identity of the signatory shall be provably equal to the identity of the licencee.

    a) Test Purpose: Verify that this requirement is satisfied by the server and that all request will be answer completely only when there are sufficient signatures to validate the licences, the requests and their association.
    b) Test Method: Inspect the document to verify the above.
    c) Reference: Clause **Error! Reference source not found.**,
    d) Test Type: Conformance.

A.1.3 Enforcement Point (Req 4)

Once a licence-protected service receives a request and its associated licences, the service shall allow the process to proceed if and only if the request is verifiable against a combination of the public context and personal licences data supplied by the request.

    a) Test Purpose: Verify that this requirement is satisfied.
    b) Test Method: Inspect the document to verify the above.
    c) Reference: Clause 6.2,
    d) Test Type: Conformance.

A.1.4 Error handling: (Req 5)

Once a licence-protected service receives a request and its associated licences, the service shall allow the process to proceed if and only if the request is verifiable against a combination of the public context and personal licences data supplied by the request.

  a) Test Purpose: Verify that this requirement is satisfied.
  b) Test Method: Inspect the document to verify the above.
  c) Reference: Clause6.3
  d) Test Type: Conformance.

A.1.5 SOAP with licence headers (Req 6)

For SOAP services, licences and/or other licence-related documents shall be included in the `<header>` element or a sub elements of the `<header>` element of the SOAP envelope.

  a) Test Purpose: Verify that this requirement is satisfied.
  b) Test Method: Inspect the document to verify the above.
  c) Reference: Clause 6.4,
  d) Test Type: Conformance.

A.1.6 Common signature for licence header and request body (Req 7)

SOAP header shall contain a signature element, which signs the reuqest body and the licence header element and all related security header elements together in order to associate the licence element with the request body.

  a) Test Purpose: Verify that this requirement is satisfied.

  b) Test Method: the document to verify the above.

  c) Reference: Clause6.4.

  d) Test Type: Conformance.

A.2   Conformance Class: Licence Model
A.2.1 SAML licence document (Req 8)

Licence Encoding:A licence is expressed as a SAML 2.0 assertionand shall include an issuer element and an XACMLPolicyStatement based on the OASIS SAML 2.0 Profile of XACML, Version 2. It shall be compliant with the XML Schema in Annex B.1.

  a) Test Purpose: Verify that this requirement is satisfied.
  b) Test Method: Inspect the document to verify the above.
  c) Reference: Clause 7.1.

d) Test Type: Conformance.

A.2.2 Licence reference document (Req 9)

Licence Reference Encoding:The licence reference document shall be compliant with the XML Schema in Annex B.1 and consist of a SAML 2.0 assertion containing an AttributeStatement with the attribute names "LicenceProviderURI" and "LicenceID". The value for the "LicenceProviderURI" attribute shall be of the type "anyURI" and for the "LicenceID" attribute of the type "string".

    a) Test Purpose: Verify that this requirement is satisfied.
    b) Test Method: Inspect the document to verify the above.
    c) Reference: Clause7.2.
    d) Test Type: Conformance.

A.2.3 Enforcement pointbehavior (Req 10)

Enforcement Point Behavior:Anenforcement point shall only accept licences if they are received from their issuer directly.

    a) Test Purpose: Verify that this requirement is satisfied.
    b) Test Method: Use licence from another source than the issuer and verify that it is rejected.
    c) Reference: Clause7.3.
    d) Test Type: Conformance.

A.3   Conformance Class: GetCapabilitiesextension
A.3.1 Rights information type (Req 11)

Rights Information Info Type:The 'type' attribute of the `<rightsInformation>` element defined in Req1 shall contain the URI urn:ogc:def:georm:preconditions:ws-policy.

    a) Test Purpose: Verify that this requirement is satisfied.
    b) Test Method: Inspect the document to verify the above.
    c) Reference: Clause 8.2.
    d) Test Type: Conformance.

A.3.2 Rights information value(Req 12)

Rights Information Info Value:The value of the `<rightsInformation>` element defined in Req1 shall be a URI pointing to a WS-Policy version 1.2 document.

    a) Test Purpose: Verify that this requirement is satisfied.

    b) Test Method: Follow the URI and verify that it links to a WS-Policy version 1.2 document.

c) Reference: Clause 8.2.

d) Test Type: Conformance.

A.3.3 Licence precondition (Req 13)

Licence Precondition:The referenced WS-Policy document from Req11 shall require a licence.

a) Test Purpose: Verify that this requirement is satisfied.

b) Test Method: Inspect the document to verify the above.

c) Reference: Clause 8.3.

d) Test Type: Conformance.

A.3.4 Identity precondition (Req 14)

Identity Precondition:The referenced WS-Policy document from Req 12 shall require a an identity for authentication purposes. This identity precondition shall make use of one of the Identity preconditions specified in the WS-SecurityPolicy specification (such as i.e. SAML or X509 tokens).

a) Test Purpose: Verify that this requirement is satisfied.

b) Test Method: Send a request without anidentity element and verify that the request is rejected.

c) Reference: Clause 8.3.

d) Test Type: Conformance.

A.3.5 Schema compliance (Req 15)

Precondition Schema:The licence precondition shallcomply with the schema listed in Annex B.2.

a) Test Purpose: Verify that this requirement is satisfied.

b) Test Method: Inspect the document to verify the above.

c) Reference: Clause 8.3.

d) Test Type: Conformance.

A.4 Conformance Class: SOAP Protocol
A.4.1 Embedding the licence element (Req 16)

Licence Embedding:The licence shall be embedded in the SOAP request header following Web Service Security: SAML Token Profile 1.1.

   a) Test Purpose: Verify that this requirement is satisfied.
   b) Test Method: Send a request with the licence not embedded in header following Web Service Security: SAML Token Profile 1.1 and verify that the request is rejected.
   c) Reference: Clause 9.1.
   d) Test Type: Conformance.

A.4.2 Request signature (Req 17)

Request Signature:The signature of the licence and the identity assertion together with the SOAP body shall be compliant to the WS-Security 1.1 specification.

   a) Test Purpose: Verify that this requirement is satisfied.
   b) Test Method: Send a request without a WS-Security 1.1 compliant signature and verify that the request is rejected.
   c) Reference: Clause 9.2.
   d) Test Type: Conformance.

Annex B
(normative)
XML Schemas

B.1   Licence Schema

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schemaxmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xacml-
saml="urn:oasis:names:tc:xacml:1.1:profile:saml2.0:v2:schema:asse
rtion" xmlns:lic="http://www.conterra.de/licence"
targetNamespace="http://www.conterra.de/licence"
elementFormDefault="qualified"
attributeFormDefault="unqualified">
   <xs:import
namespace="urn:oasis:names:tc:xacml:1.1:profile:saml2.0:v2:schema
:assertion" schemaLocation="xacml-1.1-profile-saml2.0-v2-schema-
assertion-wd-5.xsd"/>
   <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd"/>
   <xs:importnamespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
   <xs:element name="Licence" type="lic:LicenceType"/>
   <xs:element name="LicenceReference"
type="lic:LicenceReferenceType"/>
   <xs:complexType name="LicenceType">
     <xs:complexContent>
       <xs:restriction base="saml:AssertionType">
         <xs:sequence>
           <xs:element ref="saml:Issuer"/>
           <xs:element ref="ds:Signature" minOccurs="0"/>
           <xs:element ref="saml:Subject" minOccurs="0"/>
           <xs:element ref="saml:Conditions" minOccurs="0"/>
           <xs:choicemaxOccurs="unbounded">
             <xs:element ref="saml:Statement"/>
             <xs:element ref="saml:AttributeStatement"/>
           </xs:choice>
         </xs:sequence>
       </xs:restriction>
     </xs:complexContent>
   </xs:complexType>
   <xs:complexType name="LicenceReferenceType">
     <xs:complexContent>
       <xs:restriction base="saml:AssertionType">
         <xs:sequence>
```

```
            <xs:element ref="saml:Issuer"/>
            <xs:element ref="ds:Signature" minOccurs="0"/>
            <xs:element ref="saml:Subject" minOccurs="0"/>
            <xs:choice>
                <xs:element ref="saml:AttributeStatement"/>
            </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
</xs:schema>
```

B.2   Licence Precondition Schema

```
<?xmlversion="1.0" encoding="UTF-8"?>
<xs:schemaxmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://www.opengis.net/wps/1.0.0"
xmlns:wsp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
   <xs:import namespace="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702" schemaLocation="http://docs.oasis-
open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-
1.2.xsd"/>
   <xs:importnamespace="http://www.w3.org/2005/08/addressing"
schemaLocation="http://www.w3.org/2006/03/addressing/ws-
addr.xsd"/>
   <xs:element name="LicenceToken" type="LicenceTokenType"/>
   <xs:complexType name="LicenceTokenType">
     <xs:sequence>
        <xs:element name="TokenType">
           <xs:simpleType>
              <xs:restriction base="xs:string">
                 <xs:enumeration
value="urn:oasis:names:tc:SAML:2.0:XACML"/>
              </xs:restriction>
           </xs:simpleType>
        </xs:element>
        <xs:element name="IssuingAuthority" minOccurs="1"
maxOccurs="unbounded">
           <xs:complexType>
              <xs:sequence>
                 <xs:element name="Issuer"
type="wsa:EndpointReferenceType"/>
                 <xs:element name="IssuerName"
type="xs:anyURI"/>
                 <xs:element name="IssuerType"
type="IssuerTypeType"/>
              </xs:sequence>
           </xs:complexType>
        </xs:element>
     </xs:sequence>
```

15

```
        <xs:attribute ref="wsp:IncludeToken" use="required"/>
    </xs:complexType>
    <xs:simpleType name="IssuerTypeType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="LicenceBroker"/>
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Annex C
(informative)
Examples

C.1   Sample licence document

```
<saml:Assertionxmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="someID" IssueInstant="2007-10-11T10:09:22.515+02:00"
Version="2.0">

   <saml:Issuer>http://www.52north.org/licman</saml:Issuer>
                <saml:Statementxsi:type="xacml-
saml:XACMLPolicyStatementType"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <xacml:PolicySetxmlns:xacml="urn:oasis:names:tc:xacml:2.0:poli
cy:schema:os"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-
combining-algorithm:first-applicable"
PolicySetId="urn:conterra:names:sdi-
suite:policy:interceptor:wms::TestRechte">

   <xacml:Description>Beschreibung</xacml:Description>
                      <xacml:Target>
                         <xacml:Subjects>
                            <xacml:AnySubject/>
                         </xacml:Subjects>
                         <xacml:Resources>
                            <xacml:AnyResource/>
                         </xacml:Resources>
                         <xacml:Actions>
                            <xacml:AnyAction/>
                         </xacml:Actions>
                      </xacml:Target>
                      <xacml:PolicyPolicyId="WMS_Recht"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:first-applicable">

   <xacml:Description>Beschreibung</xacml:Description>
                      <xacml:Target>
                         <xacml:Subjects>
                            <xacml:AnySubject/>
                         </xacml:Subjects>
                         <xacml:Resources>
                            <xacml:AnyResource/>
                         </xacml:Resources>
                         <xacml:Actions>
                            <xacml:AnyAction/>
                         </xacml:Actions>
                      </xacml:Target>
```

```
                                <xacml:Rule Effect="Permit"
RuleId="Zugriff_zugelassen">

    <xacml:Description>Beschreibung</xacml:Description>
                                <xacml:Target>
                                    <xacml:Subjects>
                                        <xacml:Subject>

    <xacml:SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:funct
ion:string-equal">
                                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">test</xacml:At
tributeValue>

    <xacml:SubjectAttributeDesignatorAttributeId="urn:oasis:names:
tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"/>
                                        </xacml:SubjectMatch>
                                    </xacml:Subject>
                                </xacml:Subjects>
                                <xacml:Resources>
                                    <xacml:Resource>

    <xacml:ResourceMatchMatchId="urn:oasis:names:tc:xacml:1.0:func
tion:string-equal">
                                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">imagery_high_r
es</xacml:AttributeValue>

    <xacml:ResourceAttributeDesignatorAttributeId="urn:oasis:names
:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
                                        </xacml:ResourceMatch>
                                    </xacml:Resource>
                                </xacml:Resources>
                                <xacml:Actions>
                                    <xacml:AnyAction/>
                                </xacml:Actions>
                            </xacml:Target>
                        </xacml:Rule>
                        <xacml:RuleEffect="Permit"
RuleId="Zugriff_zugelassen2">

    <xacml:Description>Beschreibung</xacml:Description>
                                <xacml:Target>
                                    <xacml:Subjects>
                                        <xacml:Subject>

    <xacml:SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:funct
ion:string-equal">
```

```
                                                <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Alice</xacml:A
ttributeValue>

    <xacml:SubjectAttributeDesignatorAttributeId="urn:oasis:names:
tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string"
SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"/>
                                        </xacml:SubjectMatch>
                                    </xacml:Subject>
                                </xacml:Subjects>
                                <xacml:Resources>
                                    <xacml:Resource>

    <xacml:ResourceMatchMatchId="urn:oasis:names:tc:xacml:1.0:func
tion:string-equal">
                                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">imagery_high_r
es</xacml:AttributeValue>

    <xacml:ResourceAttributeDesignatorAttributeId="urn:oasis:names
:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
                                        </xacml:ResourceMatch>
                                    </xacml:Resource>
                                </xacml:Resources>
                                <xacml:Actions>
                                    <xacml:Action>

    <xacml:ActionMatchMatchId="urn:oasis:names:tc:xacml:1.0:functi
on:string-equal">
                                            <xacml:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">GetCapabilitie
s</xacml:AttributeValue>

    <xacml:ActionAttributeDesignatorAttributeId="urn:oasis:names:t
c:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
                                        </xacml:ActionMatch>
                                    </xacml:Action>
                                </xacml:Actions>
                            </xacml:Target>
                        </xacml:Rule>
                        <xacml:Rule Effect="Deny"
RuleId="Verboten">
                            <xacml:Target>
                                <xacml:Subjects>
                                    <xacml:AnySubject/>
                                </xacml:Subjects>
                                <xacml:Resources>
                                    <xacml:AnyResource/>
                                </xacml:Resources>
```

```
                              <xacml:Actions>
                                  <xacml:AnyAction/>
                              </xacml:Actions>
                          </xacml:Target>
                      </xacml:Rule>
                  </xacml:Policy>
              </xacml:PolicySet>
          </saml:Statement>

    <ds:Signaturexmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:SignedInfo>
                      <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                      <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                      <ds:Reference URI="#someID">
                          <ds:Transforms>
                              <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                              <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                          </ds:Transforms>
                          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

    <ds:DigestValue>HhXaL4Ylj9u/28/AhgbaSh0YuPs=</ds:DigestValue>
                      </ds:Reference>
                  </ds:SignedInfo>

    <ds:SignatureValue>rDWzQR/GpXxqEV0e3qz/FDLdWbaqnYCydoqozmMalrS
0vBwPcB55XK7J932PX+eOGemfBO/Y6i6o
NlFnKFvHVTPLMtSUS9NP2bzuBwPpgqfBNnOH+QX50DF0ysG7LaOJ3GAIA76mZ1YVA
P8aN98xyk+G
O7n32Tp+jLckEbYOUW8=</ds:SignatureValue>
                  <ds:KeyInfo>
                      <ds:X509Data>

    <ds:X509Certificate>MIIC3jCCAkegAwIBAgIJAMmsOGGqzGCJMA0GCSqGSI
b3DQEBBQUAMIGOMRcwFQYDVQQDEw5IYXJh
bGQgSGVja2luZzEtMCsGCSqGSIb3DQEJARYeaGFyYWxkLmhlY2tpbmdAdW5pLW11Z
W5zdGVyLmRl
MQ0wCwYDVQQKEwRJRkdJMQ0wCwYDVQQLEwRJRkdJMQswCQYDVQQHEwJNUzEMMAoGA
1UECBMDTlJX
MQswCQYDVQQGEwJERTAeFw0wNzAzMjcxMzE1MDJaFw0wODAzMjYxMzE1MDJaMIGOM
RcwFQYDVQQD
Ew5IYXJhbGQgSGVja2luZzEtMCsGCSqGSIb3DQEJARYeaGFyYWxkLmhlY2tpbmdAd
W5pLW11ZW5z
dGVyLmRlMQ0wCwYDVQQKEwRJRkdJMQ0wCwYDVQQLEwRJRkdJMQswCQYDVQQHEwJNU
zEMMAoGA1UE
CBMDTlJXMQswCQYDVQQGEwJERTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAx
pRxb3dpdjdT
```

Ws6/BMqTffhwHVJuTgrW8maXLyIyW9NhSsMEX+HpTzTWxVfFCk0+gTK1zxDRZqDJG
gUVVmpmqnxX
FiJ697ZMiNhYFF9SkZODS9YAjwEuL1Q4NIrOMb7FUu0c1O8TUdpy94TB/AgDI1tX+
1XsmWp0ZrIN
WflkJs8CAwEAAaNCMEAwCQYDVR0TBAIwADALBgNVHQ8EBAMCAiQwEwYDVR0lBAwwC
gYIKwYBBQUH
AwEwEQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4GBACvHynRrUiWZd
hoi3BXqLoCW
udkEWa2/J/nKCyV7ohWuXy4OCbyQ6GGmbJT7Fi9gBxerVC7njbSRvHlaTqjAnSpii
8yGFGxXUoOM
jcvIZxXXj6K6SZQUq4ZkA98lZEIgxrynqS/tby8WCwkmB2UGBm/7FQCc4wTKOYj74
lOdz6wf</ds:X509Certificate>
                              <ds:X509IssuerSerial>

   <ds:X509IssuerName>C=DE,ST=NRW,L=MS,OU=IFGI,O=IFGI,1.2.840.113
549.1.9.1=#161e686172616c642e6865636b696e6740756e692d6d75656e7374
65722e6465,CN=Harald Hecking</ds:X509IssuerName>

   <ds:X509SerialNumber>14532052089746251913</ds:X509SerialNumber
>
                         </ds:X509IssuerSerial>
                       </ds:X509Data>
                    </ds:KeyInfo>
                 </ds:Signature>
              </saml:Assertion>

C.2   Sample licence reference document

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion ID="ID_1" Version="0.5.0" IssueInstant="2008-05-
15T09:30:47.0Z">
   <saml:Issuer>conterra</saml:Issuer>
   <saml:Subject>
<saml:NameID>customer</saml:NameID>  </saml:Subject>
   <saml:AttributeStatement>
      <saml:Attribute Name="LicenceManagerURI">

   <saml:AttributeValue>www.conterra.de</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="LicenceID">
         <saml:AttributeValue>916743582</saml:AttributeValue>
      </saml:Attribute>
   </saml:AttributeStatement>
</saml:Assertion>
```

C.3   Sample WS-Policy document including a licence requirement

```
<wsp:Policywsu:Id="SigOnly" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <wsp:ExactlyOne>
          <wsp:All>
```

```
   <sp:AsymmetricBindingxmlns:sp="http://schemas.xmlsoap.org/ws/2
005/07/securitypolicy">
                  <wsp:Policy>
                     <sp:InitiatorToken>
                        <wsp:Policy>
                           <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypo
licy/IncludeToken/AlwaysToRecipient">
                              <wsp:Policy>

   <sp:RequireThumbprintReference/>
                                 <sp:WssX509V3Token10/>
                              </wsp:Policy>
                           </sp:X509Token>
                        </wsp:Policy>
                     </sp:InitiatorToken>
                     <sp:RecipientToken>
                        <wsp:Policy>
                           <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypo
licy/IncludeToken/Never">
                              <wsp:Policy>

   <sp:RequireThumbprintReference/>
                                 <sp:WssX509V3Token10/>
                              </wsp:Policy>
                           </sp:X509Token>
                        </wsp:Policy>
                     </sp:RecipientToken>
                     <sp:AlgorithmSuite>
                        <wsp:Policy>
                           <sp:TripleDesRsa15/>
                        </wsp:Policy>
                     </sp:AlgorithmSuite>
                     <sp:Layout>
                        <wsp:Policy>
                           <sp:Strict/>
                        </wsp:Policy>
                     </sp:Layout>
                     <sp:IncludeTimestamp/>
                     <sp:OnlySignEntireHeadersAndBody/>
                  </wsp:Policy>
               </sp:AsymmetricBinding>

   <sp:SupportingTokensxmlns:sp="http://schemas.xmlsoap.org/ws/20
05/07/securitypolicy">
                  <wsp:Policy Id="LicensingPrecondition">
```

```
   <georm:LicenceTokenxmlns:georm="http://www.opengis.net/georm/1
.0.0" wsp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient"
xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:wsa="http://www.w3.org/2005/08/addressing">

   <georm:TokenType>urn:oasis:names:tc:SAML:1.1:XACML</georm:Toke
nType>
                                <georm:IssuingAuthority>
                                    <georm:Issuer>
                                        <wsa:EndpointReference>
                                            <wsa:Address>http://giv-
antlion.uni-
muenster.de:8080/LicenceBroker/services/LicenceBroker</wsa:Addres
s>

                                        </wsa:EndpointReference>
                                    </georm:Issuer>

   <georm:IssuerName>urn:ogc:LicenceBroker@giv-antlion.uni-
muenster.de</georm:IssuerName>

   <georm:IssuerType>urn:oasis:names:tc:SAML:1.1:XACML</georm:Iss
uerType>
                                </georm:IssuingAuthority>
                            </georm:LicenceToken>

                        </wsp:Policy>
                            <wsp:Policy Id="IdentityPrecondition">
                                <sp:SamlToken
sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                                    <sp:Issuer>
                                        <wsa:EndpointReference>
                                            <wsa:Address>http://giv-
antlion.uni-muenster.de:8080/sts/services/STS</wsa:Address>
                                        </wsa:EndpointReference>
                                    </sp:Issuer>
                                    <wsp:Policy>
                                        <sp:WssSamlV11Token10 />
                                    </wsp:Policy>
                                </sp:SamlToken>
                            </wsp:Policy>
                        </sp:SupportingTokens>
                <sp:Wss10
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
                    <wsp:Policy>
                        <sp:MustSupportRefKeyIdentifier/>
                        <sp:MustSupportRefIssuerSerial/>
                    </wsp:Policy>
                </sp:Wss10>
```

```
        <sp:SignedPartsxmlns:sp="http://schemas.xmlsoap.org/ws/2005/07
/securitypolicy">
                    <sp:Header
Namespace="http://schemas.xmlsoap.org/ws/2002/07/secext" />

                    <sp:Body/>
                </sp:SignedParts>
            </wsp:All>
        </wsp:ExactlyOne>
    </wsp:Policy>
```

C.4   Sample GeoRM service request including a licence reference

```
<soapenv:Envelopexmlns:soapenv="http://schemas.xmlsoap.org/soap/e
nvelope/">
    <soapenv:Headerxmlns:wsa="http://www.w3.org/2005/08/addressing
">
        <wsse:Security xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="Timestamp-28946925">
                <wsu:Created>2010-04-24T10:25:27.745Z</wsu:Created>
                <wsu:Expires>2010-04-24T10:30:27.745Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509v1" wsu:Id="CertId-
148082">MIICTDCCAbUCBEbJZMQwDQYJKoZIhvcNAQEEBQAwbDELMAkGA1UEBhMCT
EsxEDAOBgNVBAgTB1dlc3Rlcm4xEDAOBgNVBAcTB0NvbG9tYm8xDzANBgNVBAoTBk
FwYWNoZTEQMA4GA1UECxMHUmFtcGFydDEWMBQGA1UEAxMNU2FtcGxlIENsaWVudDA
gFw0wNzA4MjAwOTU0MTJaGA8yMDYyMDUyMzA5NTQxMlowbDELMAkGA1UEBhMCTEsx
EDAOBgNVBAgTB1dlc3Rlcm4xEDAOBgNVBAcTB0NvbG9tYm8xDzANBgNVBAoTBkFwY
WNoZTEQMA4GA1UECxMHUmFtcGFydDEWMBQGA1UEAxMNU2FtcGxlIENsaWVudDCBnz
ANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAhjQp2NJRUrAEsPYIlg26m34O16E6Wky
BWMbkSvy/FJQoNg2HSOtqF/DHmej7qqJCDtiHtdZqCTOo28cpyB3XJ0g6y23ADTy1
v7qUjYieF4Bn3p9QFtyznUmKyZ6hK4CjGraYvcDgjRlnPkfeyVnNamkzJB7TVRaLk
umRlxHgxm0CAwEAATANBgkqhkiG9w0BAQQFAAOBgQBNLSbNEaGBj8GBoXWBndY3JF
vblPvI2mDbtZsNiggGOCezyAufGe6RnR3s5DjR5YQqPcMiDtlskFQm4/SRN2Yh16E
6l7LfsOhGQsPiPrDrci4T18pz1eDLSrtJiiBah1NdeISaD0kpoUiaNKiQiu16JCnx
c8tGSw3nSPg44aLYmA==</wsse:BinarySecurityToken>

    <ds:Signaturexmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Id="Signature-6416415">
            <ds:SignedInfo>
```

```
                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#Id-5264648">
                        <ds:Transforms>
                            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

    <ds:DigestValue>fAkKMOzeZggQUSwMoBN9PYL3rtM=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#id-2906128">
                        <ds:Transforms>
                            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

    <ds:DigestValue>UCZ+fpVYn3rOuT5GoAxFZg2fFz0=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference
URI="#_091cec4cf83a9550d4322c873d4856ad">
                        <ds:Transforms>
                            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

    <ds:DigestValue>ljOWqsMqvfxeQAZJrT3Xj0gBam0=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#Timestamp-28946925">
                        <ds:Transforms>
                            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

    <ds:DigestValue>j2L/CQZt9e7zD5KWd/ExgXOmEx8=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>
fA/ILv7bwSXLCEpJguLA+KJrizXzoNsetDN1OEDesFSlXVOKFABgRGun6ueAOnitj
hKGiRjhbRl7
KBeODjcThxEcQznnRA8fio4LomPKrFZxXd017CiJkLdJcn8pirHJW2Yn43Kn/w6mN
5KyQS0SGJ0L
ySTtei5tZGZ1IAC9SlM=
</ds:SignatureValue>
```

```
                    <ds:KeyInfo Id="KeyId-2533023">
                        <wsse:SecurityTokenReference
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd" wsu:Id="STRId-25504895">
                            <wsse:Reference URI="#CertId-148082"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-x509-token-profile-1.0#X509v1"/>
                        </wsse:SecurityTokenReference>
                    </ds:KeyInfo>
                </ds:Signature>


    <LicenceReferencexmlns="http://www.52north.org/licence/0.3.2"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd" ID="R-bf674a75-541e-42c0-a831-
aabf7262d54f9c
5" IssueInstant="2010-04-24T12:21:59.773+02:00" Version="2.0"
wsu:Id="id-2906128">
            <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
Format="http://www.52north.org/licman">52N Licence
Manager</Issuer>

    <AttributeStatementxmlns="urn:oasis:names:tc:SAML:2.0:assertio
n">
            <Attribute
Name="!licencemanager.samlassertion.attributeStatement.prefix!Lic
enceManagerURL">

    <AttributeValue>http://www.52north.org/licman</AttributeValue>
            </Attribute>
        </AttributeStatement>

    <AttributeStatementxmlns="urn:oasis:names:tc:SAML:2.0:assertio
n">
            <Attribute
Name="!licencemanager.samlassertion.attributeStatement.prefix!Lic
enceID">
                <AttributeValue>DA1272104519695</AttributeValue>
            </Attribute>
        </AttributeStatement>
    </LicenceReference>
    <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd"
AssertionID="_091cec4cf83a9550d4322c873d4856ad"
IssueInstant="2010-04-24T10:22:00.870Z" Issuer="STS"
MajorVersion="1" MinorVersion="1"
wsu:Id="_091cec4cf83a9550d4322c873d4856ad">
        <Conditions NotBefore="2010-04-24T10:22:00.870Z"
NotOnOrAfter="2010-04-24T10:27:00.870Z"/>
```

```
            <AuthenticationStatementAuthenticationInstant="2010-04-
24T10:22:00.870Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
            <Subject>
                <NameIdentifier
Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">client</NameIdentifier>
                <SubjectConfirmation>

    <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
key</ConfirmationMethod>

    <KeyInfoxmlns="http://www.w3.org/2000/09/xmldsig#">
                        <X509Data
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <X509Certificate>MIICTDCCAbUCBEbJZMQwDQYJKoZIhvcNAQEEBQAwbDELM
AkGA1UEBhMCTEsxEDAOBgNVBAgTB1dlc3Rlcm4xEDAOBgNVBAcTB0NvbG9tYm8xDz
ANBgNVBAoTBkFwYWNoZTEQMA4GA1UECxMHUmFtcGFydDEWMBQGA1UEAxMNU2FtcGx
lIENsaWVudDAgFw0wNzA4MjAwOTU0MTJaGA8yMDYyMDUyMzA5NTQxMlowbDELMAkG
A1UEBhMCTEsxEDAOBgNVBAgTB1dlc3Rlcm4xEDAOBgNVBAcTB0NvbG9tYm8xDzANB
gNVBAoTBkFwYWNoZTEQMA4GA1UECxMHUmFtcGFydDEWMBQGA1UEAxMNU2FtcGxlIE
NsaWVudDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAhjQp2NJRUrAEsPYIlg2
6m34O16E6WkyBWMbkSvy/FJQoNg2HSOtqF/DHmej7qqJCDtiHtdZqCTOo28cpyB3X
J0g6y23ADTy1v7qUjYieF4Bn3p9QFtyznUmKyZ6hK4CjGraYvcDgjRlnPkfeyVnNa
mkzJB7TVRaLkumRlxHgxm0CAwEAATANBgkqhkiG9w0BAQQFAAOBgQBNLSbNEaGBj8
GBoXWBndY3JFvblPvI2mDbtZsNiggGOCezyAufGe6RnR3s5DjR5YQqPcMiDtlskFQ
m4/SRN2Yh16E6l7LfsOhGQsPiPrDrci4T18pz1eDLSrtJiiBah1NdeISaD0kpoUia
NKiQiu16JCnxc8tGSw3nSPg44aLYmA==</X509Certificate>
                        </X509Data>
                    </KeyInfo>
                </SubjectConfirmation>
            </Subject>
        </AuthenticationStatement>
        <AttributeStatement>
            <Subject>
                <NameIdentifier
Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">client</NameIdentifier>
            </Subject>
            <Attribute AttributeName="Name"
AttributeNamespace="https://rahas.apache.org/saml/attrns">
                <AttributeValue>Colombo/Rahas</AttributeValue>
            </Attribute>
        </AttributeStatement>

    <ds:Signaturexmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

```
                    <ds:Reference
URI="#_091cec4cf83a9550d4322c873d4856ad">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                    <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">

   <ec:InclusiveNamespacesxmlns:ec="http://www.w3.org/2001/10/xml
-exc-c14n#" PrefixList="code ds kind rwsamlsamlptypens #default
xsdxsi"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

   <ds:DigestValue>BH3I2aXC9g74CnbnrdAAnC+KDjk=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>
RrgrSGutLq/62QE1WrEdVgZS3amSGOVl3YN2fj00gg5eGJQcUr8lYDHKhcbDJ9SwW
OTYhtAhDxoC
mfq4VnxN95kn5oH5Zc4NuVoEnmztIEP0iP3zCXgeIUwOrXGcLQ557B1aZmtnkSCjl
EVsR3+myKpy
CCKzXgaMD2sOjh8b2v0=
</ds:SignatureValue>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>
MIICTjCCAbcCBEbJZQEwDQYJKoZIhvcNAQEEBQAwbTELMAkGA1UEBhMCTEsxEDAOB
gNVBAgTB1dl
c3R
9e6
lcm4xEDAOBgNVBAcTB0NvbG9tYm8xDzANBgNVBAoTBkFwYWNoZTEQMA4GA1UECxMH
UmFtcGFy
dDEXMBUGA1UEAxMOU2FtcGxlIFNlcnZpY2UwIBcNMDcwODIwMDk1NTEzWhgPMjA2M
jA1MjMwOTU1
MTNaMG0xCzAJBgNVBAYTAkxLMRAwDgYDVQQIEwdXZXN0ZXJuMRAwDgYDVQQHEwdDb
2xvbWJvMQ8w
DQYDVQQKEwZBcGFjaGUxEDAOBgNVBAsTB1JhbXBhcnQxFzAVBgNVBAMTDlNhbXBsZ
SBTZXJ2aWNl
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCDtgg6ess2lU1yOD48/iiAlWObB
0WwAQtFG4bb
2KyvOE9dRF7+d/aZrHti3QWs6dtHpGkVMLgpomoq7APEq1kQnRvduk2T6ln83Jw1E
pPDXH/emqeC
9OdNqHZj3eoyf34JMmgShuviYDqYaK4HkRmZMiJl3aPeZzPl60yBWydAuwIDAQABM
A0GCSqGSIb3
DQEBBAUAA4GBACVcoAqNbjO7+Jbm6+3pyYagQoBpdHZLnR8EU9/CRKmUGTj5qjXqY
tE+Eka6OYKB
zv/dHdYlB2X3yH3YlSx1OtA3+5xl4VIjYODlgh9Bs9Tbqj1tw0G37dLrlG97kJAVj
rkfm743N9EH
```

```
KFtFaX4iF1tWbGxa4+vIbbV4CaUG5s5x
</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
</Assertion>
</wsse:Security>
<ows6:OriginalBinding
xmlns:ows6="http://gatekeeper.service.security.n52.org"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://gatekeeper.service.security.n52.org
http://52north.org/schema/security/gatekeeper/KVP2XML.xsd">Post/X
ML</ows6:OriginalBinding>

    <wsa:To>http://localhost:8081/gatekeeper/services/gatekeeper</
wsa:To>

    <wsa:MessageID>urn:uuid:371BFBA99D171451521272104727777</wsa:M
essageID>
        <wsa:Action>method</wsa:Action>
    </soapenv:Header>
    <soapenv:Body xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="Id-5264648">
        <wps:Executexmlns:wps="http://www.opengis.net/wps/1.0.0"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:ows="http://www.opengis.net/ows/1.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
service="WPS" version="1.0.0"
xsi:schemaLocation="http://www.opengis.net/wps/1.0.0
http://schemas.opengis.net/wps/1.0.0/wpsExecute_request.xsd">

    <ows:Identifier>org.n52.wps.server.algorithm.SimpleBufferAlgor
ithm</ows:Identifier>
        <wps:DataInputs>
            <wps:Input>
                <ows:Identifier>data</ows:Identifier>
                <wps:Reference
schema="http://schemas.opengis.net/gml/2.1.2/feature.xsd"
xlink:href="http://giv-wps.uni-
muenster.de:8080/geoserver/ows?service=WFS&amp;version=1.0.0&amp;
request=GetFeature&amp;typeName=topp:tasmania_roads"/>
            </wps:Input>
            <wps:Input>
                <ows:Identifier>width</ows:Identifier>
                <ows:Title>Distance which people will walk to get
to a playground.</ows:Title>
                <wps:Data>
                    <wps:LiteralData>20</wps:LiteralData>
                </wps:Data>
            </wps:Input>
        </wps:DataInputs>
        <wps:ResponseForm>
```

```
            <wps:ResponseDocument>
               <wps:Output>
                  <ows:Identifier>result</ows:Identifier>
               </wps:Output>
            </wps:ResponseDocument>
         </wps:ResponseForm>
      </wps:Execute>
   </soapenv:Body>
</soapenv:Envelope>
```