# INFORMATION, SERVICES AND RESEARCH ABOUT THE EARTH

NLS
NATIONAL
LAND SURVEY
OF FINLAND

# OGC WEB SERVICES SECURITY

NLS NATIONAL LAND SURVEY OF FINLAND

# BACKGROUND

- Information Assurance (IA) Controls for OGC Web Services (OWS) have been implemented for years.
- These implementations break interoperability, as they are not standardized by OGC Web Service standards.
- The goal of the OWS Common Security Standard is to allow the implementation of IA controls and to advertise their existence in an interoperable way **with minimal impact to existing implementations** using a backwards-compatible approach.

# OGC WEB SERVICES SECURITY

- Available at http://docs.opengeospatial.org/is/17-007r1/17-007r1.html
- Capabilities document must be publicly accessible

The following OGC standards are directly affected:

1. OWS Common 1.1.0, OGC 06-121r3 *OGC Web Services Common Specification, OGC® Implementation Standard*
2. OWS Common 2.0.0, OGC 06-121r9 *OGC Web Services Common Specification, OGC® Implementation Standard*
3. WMS 1.1.1, OGC 01-068r3 *Web Map Service Implementation Specification*
4. WMS 1.3.0, OGC 06-042 *OpenGIS Web Map Service (WMS) Implementation Specification*

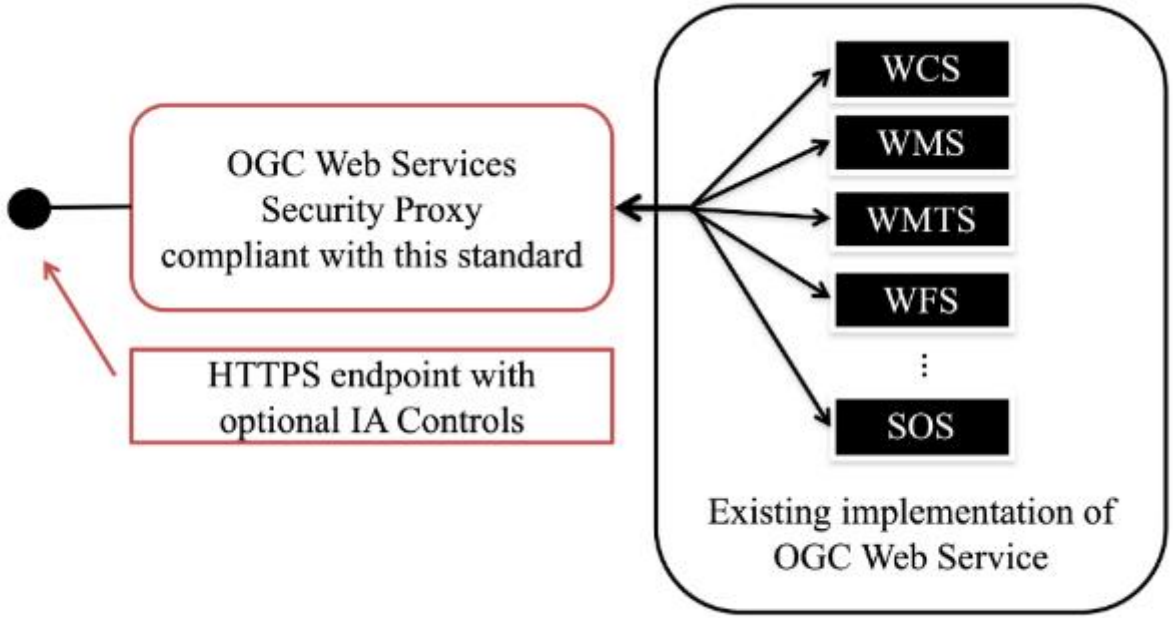


*Figure 2. Security Proxy to make Geoserver deployment compliant with this standard*

# WMS 1.1

*Table 4. Definition of the ExtendedSecurityCapabilities element for WMS 1.1.1*

```
<!DOCTYPE WMT_MS_Capabilities SYSTEM "http://schemas.opengis.net/wms/1.1.1/WMS_MS_Capabilities.dtd"[
<!--
============================================================
OWS Common Security Extension to annotate security
Definition of element ows:OperationsMetadata replicating the
definition from the OWS Common Schema to become available as DTD
============================================================
-->
<!ELEMENT VendorSpecificCapabilities (ows_security:ExtendedSecurityCapabilities)>

<!ELEMENT ows_security:ExtendedSecurityCapabilities (ows:OperationsMetadata+)>
<!ATTLIST ows_security:ExtendedSecurityCapabilities xmlns:ows_security CDATA #FIXED
"http://www.opengis.net/security/1.0">

<!ELEMENT ows:OperationsMetadata (ows:Operation*)>
<!ATTLIST ows:OperationsMetadata xmlns:ows CDATA #FIXED "http://www.opengis.net/ows/1.1">

<!ELEMENT ows:Operation (ows:DCP+) >
<!ATTLIST ows:Operation name CDATA #REQUIRED>

<!ELEMENT ows:DCP (ows:HTTP) >
<!ELEMENT ows:HTTP (ows:Get | ows:Post)+ >

<!ELEMENT ows:Get (ows:Constraint+)>
<!ATTLIST ows:Get xmlns:xlink CDATA #FIXED "http://www.w3.org/1999/xlink" xlink:type CDATA #FIXED "simple"
xlink:href CDATA #REQUIRED >

<!ELEMENT ows:Post (ows:Constraint+)>
<!ATTLIST ows:Post xmlns:xlink CDATA #FIXED "http://www.w3.org/1999/xlink" xlink:type CDATA #FIXED
"simple" xlink:href CDATA #REQUIRED >
```



NLS NATIONAL LAND SURVEY OF FINLAND

# WMS 1.3

*Table 9. Definition of the ExtendedSecurityCapabilities element for WMS 1.3.0*

```
<schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ows_security="http://www.opengis.net/security/1.0"
  xmlns:ows="http://www.opengis.net/ows/1.1"
    xmlns:wms="http://www.opengis.net/wms"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    targetNamespace="http://www.opengis.net/security/1.0"
    elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0.0">
    <import namespace="http://www.opengis.net/wms"
schemaLocation="http://schemas.opengis.net/wms/1.3.0/capabilities_1_3_0.xsd"/>
    <import namespace="http://www.opengis.net/ows/1.1"
schemaLocation="http://schemas.opengis.net/ows/1.1.0/owsOperationsMetadata.xsd"/>
    <xs:complexType name="ExtendedSecurityCapabilitiesType">
      <sequence>
        <element ref="ows:OperationsMetadata"/>
      </sequence>
    </xs:complexType>
    <element name="ExtendedSecurityCapabilities" type="ows_security:ExtendedSecurityCapabilitiesType"
substitutionGroup="wms:_ExtendedCapabilities"/>
</schema>
```

NLS NATIONAL LAND SURVEY OF FINLAND

# EXAMPLES – KUDOS ANDREAS MATHEUS

WMS 1.3.0 (GetCapabilities)

```
<ows_security:ExtendedSecurityCapabilities xmlns:ows_security="http://www.opengis.net/security/1.0" xmlns:wms="http://www.opengis.net/wms"
xmlns:ows="http://www.opengis.net/ows/1.1">
  <ows:OperationsMetadata>
    <ows:Operation name="GetCapabilities">
      <ows:DCP>
        <ows:HTTP>
          <ows:Get xlink:type="simple" xlink:href="https://ogc.secure-dimensions.com:443/geoserver/ows?SERVICE=WMS&">
            <ows:Constraint name="urn:ogc:def:security:1.0:rc:cors">
              <ows:NoValues/>
            </ows:Constraint>
            <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-methods">
              <ows:AllowedValues>
                <ows:Value>GET</ows:Value>
                <ows:Value>OPTIONS</ows:Value>
              </ows:AllowedValues>
            </ows:Constraint>
          </ows:Get>
        </ows:HTTP>
      </ows:DCP>
    </ows:Operation>
    <ows:Operation name="GetMap">
      <ows:DCP>
        <ows:HTTP>
          <ows:Get xlink:type="simple" xlink:href="https://ogc.secure-dimensions.com:443/geoserver/ows?SERVICE=WMS&">
            <ows:Constraint name="urn:ogc:def:security:authentication">
              <ows:ValuesReference ows:reference="urn:ogc:def:security:authentication:ietf:6750:Bearer"/>
              <ows:Meaning ows:reference="https://ogc.secure-dimensions.com/authnCodelist#OAUTH2_BEARER_TOKEN"/>
            </ows:Constraint>
            <ows:Constraint name="urn:ogc:def:security:1.0:rc:cors">
              <ows:NoValues/>
            </ows:Constraint>
            <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-exception-handling">
              <ows:NoValues/>
            </ows:Constraint>
            <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-methods">
              <ows:AllowedValues>
                <ows:Value>GET</ows:Value>
                <ows:Value>OPTIONS</ows:Value>
              </ows:AllowedValues>
            </ows:Constraint>
            <ows:Constraint name="urn:ogc:def:security:1.0:rc:authorization">
              <ows:ValuesReference ows:reference="https://ogc.secure-dimensions.com/OWSCommonSecurityPolicy.xacml"/>
            </ows:Constraint>
          </ows:Get>
        </ows:HTTP>
      </ows:DCP>
    </ows:Operation>
```

# EXAMPLES – KUDOS ANDREAS MATHEUS

WFS 2.0.0 (GetCapabilities)

```
<ows:Operation name="GetCapabilities">
  <ows:DCP>
    <ows:HTTP>
      <ows:Get xlink:type="simple" xlink:href="https://ogc.secure-dimensions.com:443/geoserver/wfs">
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:cors">
          <ows:NoValues/>
        </ows:Constraint>
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-methods">
          <ows:AllowedValues>
            <ows:Value>GET</ows:Value>
            <ows:Value>OPTIONS</ows:Value>
          </ows:AllowedValues>
        </ows:Constraint>
      </ows:Get>
      <ows:Post xlink:type="simple" xlink:href="https://ogc.secure-dimensions.co
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:cors">
          <ows:NoValues/>
        </ows:Constraint>
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-methods">
          <ows:AllowedValues>
            <ows:Value>POST</ows:Value>
            <ows:Value>OPTIONS</ows:Value>
          </ows:AllowedValues>
        </ows:Constraint>
      </ows:Post>
    </ows:HTTP>
  </ows:DCP>
```

```
<ows:Operation name="DescribeFeatureType">
  <ows:DCP>
    <ows:HTTP>
      <ows:Get xlink:type="simple" xlink:href="https://ogc.secure-dimensions.com:443/geoserver/wfs">
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:cors">
          <ows:NoValues/>
        </ows:Constraint>
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-methods">
          <ows:AllowedValues>
            <ows:Value>GET</ows:Value>
            <ows:Value>OPTIONS</ows:Value>
          </ows:AllowedValues>
        </ows:Constraint>
      </ows:Get>
      <ows:Post xlink:type="simple" xlink:href="https://ogc.secure-dimensions.com:443/geoserver/wfs">
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:cors">
          <ows:NoValues/>
        </ows:Constraint>
        <ows:Constraint name="urn:ogc:def:security:1.0:rc:http-methods">
          <ows:AllowedValues>
            <ows:Value>POST</ows:Value>
            <ows:Value>OPTIONS</ows:Value>
          </ows:AllowedValues>
        </ows:Constraint>
      </ows:Post>
    </ows:HTTP>
  </ows:DCP>
```



NLS NATIONAL LAND SURVEY OF FINLAND


NLS
NATIONAL
LAND SURVEY
OF FINLAND

# SHOWING THE WAY

**MORE INFORMATION**
**JARI.REINI@NLS.FI**

NLS
NATIONAL
LAND SURVEY
OF FINLAND