|  |  |
| --- | --- |
| **TITLE:**  | **OWS Common SecurityStandards Working Group Charter** |
| **Authors:** | **Andreas Matheus, Dave Wesloh** |
| **Email:** |  |
| **DATE:** | **16 July 2015** |
| **CATEGORY:**  | **SWG Charter** |

To:  OGC members & interested parties

A new OGC Standards Working Group is being formed. The OGC members listed below have proposed the OGC Open Web Services (OWS) Common Security Standards Working Group.  The SWG proposal provided in this document meets the requirements of the OGC TC Policies and Procedures.

The SWG name, statement of purpose, scope, list of deliverables, audience, and language specified in the proposal will constitute the SWG's official charter. Technical discussions may occur no sooner than the SWG's first meeting.

This SWG will operate under the OGC 2007 IPR Policy. The eligibility requirements for becoming a participant in the SWG at the first meeting (see details below) are that:

* You must be an employee of an OGC member organization or an individual
member of OGC;
* The OGC member must have signed the OGC Membership agreement;
* You must notify the SWG chair of your intent to participate to the first meeting. Members may do so by logging onto the OGC Portal and navigating to the Observer page and clicking on the link for the SWG they wish to join and;
* You must attend meetings of the SWG. The first meeting of this SWG is at the time and date fixed below. Attendance may be by teleconference.

Of course, participants also may join the SWG at any time. The OGC and the SWG welcomes all interested parties.

Non-OGC members who wish to participate may contact us about joining the OGC. In addition, the public may access some of the resources maintained for each SWG: the SWG public description, the SWG Charter, Change Requests, and public comments, which will be linked from the SWG’s page.

Please feel free to forward this announcement to any other appropriate lists. The OGC is an open standards organization; we encourage your feedback.

# **1. OWS Common Security**

A **spatial data infrastructure (SDI)** is a data infrastructure implementing a framework of geographic data, metadata, users and tools that are interactively connected in order to use spatial data in an efficient and flexible way ([Wikipedia - Spatial data infrastructure](http://en.wikipedia.org/wiki/Spatial_data_infrastructure)).

Common Security implements the relevant concepts in the ISO 10181 framework in a common fashion that can be used by OGC Standards supporting a SDI.

*Please note that ISO 10181-1 provides a summary and listing of the following frameworks.*

|  |
| --- |
| ***Authentication Framework****: ISO 10181-2 defines all basic concepts of authentication in Open Systems: It identifies different classes of authentication mechanisms, the services for their implementation and the requirements for supporting protocols. It further identifies requirements for the management of identity information.* |
| ***Access Control Framework****: ISO 10181-3 defines all basic concepts for access control in Open Systems and the relation to other frameworks such as the Authentication and Audit Frameworks.* |
| ***Non-repudiation Framework:*** *ISO 10181-4 refines and extends the concepts of non-repudiation, given in ISO 7598-2. It further defines general non-repudiation services and the mechanisms to provide these services.* |
| ***Confidentiality Framework****: ISO 10181-5 defines the basic concepts of confidentiality, identifies classes of confidentiality mechanisms and their maintenance. It further addresses the interactions of the confidentiality mechanisms with other services.* |
| ***Integrity Framework****: ISO 10181-6 defines the basic concepts of integrity, identical to the Confidentiality Framework.* |
| ***Security Audits and Alarms Framework****: ISO 10181-7 defines the basic concepts for security audit and alarms and the relationship to other security services.* |

From a standardization aspect, the following frameworks are out of scope as their implementation is not relevant to an SDI (for details please see OGC #15-022):

* Non-repudiation Framework (ISO 10181-4)
* Security Audits and Alarms Framework (ISO 10181-7)

# **2. Purpose of this Standards Working Group**

This SWG will create a Standard to define a common publication to declare that the Service instance (represented by a URL) is protected by the implementation of one or more security frameworks from ISO 10181.

**This SWG will normatively define how to make available to a client a description of the implementation of security framework(s). The SWG will not provide solutions to implement the frameworks, but will provide an** Implementation Standard or extension and a separate Best Practice or User Guide for deployment options, described in paragraph 5

**The type of standard is considered an extension to the existing OWS Common version 1.0, 1.1 and 2.0 to be able to add security by applying the extension. It shall be the goal of the SWG to minimize security-related Change Requests (CRs) to existing OGC Web Services standards or OWS Common.**

# **3. Business Value Proposition**

SWG Charter Members have recognized the need for OGC to act proactively with respect to web service security. The SWG sees Business Value in being able to use protected OGC services in an interoperable way to enable commercial and government use. The risks of data loss and theft continue to grow as mobile tools, cloud computing and social media go mainstream. As OGC-based services move to these platforms, a Common Security extension for OGC services based on mainstream IT becomes critical.

# **4. Scope of Work (Statement of Work, SoW)**

The SWG will concentrate on the development of a Security Extension to OWS Common 1.0, 1.1.0 and 2.0

The SWG will define the use of security code lists for ISO metadata in an informative annex.

The SWG will define implementation guidelines and requirements addressing the World Wide Web Consortium (W3C) Requests for Comments (RFCs) in the Security Extension. Implication for the extension is that the full RFC 2616 (including all HTTP verbs and status codes) use is permitted.

The SWG will provide deployment guidance regarding main stream IT use in Apache as an informative annex.

The SWG will mandate the use of HTTP over TLS (HTTPS) for the security extension. The implication is an extension to the OWS schema for HTTPS to become a valid protocol.

The SWG will develop additional guidance to address Authentication and Authorization requirements with examples on how to implement / deploy the proposed security extension (i.e., Proxy).

The SWG will evaluate the role of SOAP in the Common Security framework.

The SWG will provide example WSDL documents including guidance on how to embed WS-\* and WS-Policy when using SOAP.

The SWG will provide a common mechanism to transport binary or XML Schema data.

The SWG will develop recommendations on how to organize support for Common Security in conformance classes, including SOAP.

The SWG will develop recommendations on the usage of the “action" attribute on the application/soap+xml media type typically provided as part of the HTTP header.

The SWG will define and describe a Common Security framework for OGC Service Capabilities documents.

The SWG will submit a WFS 1.1.0 CR to normatively reference OWS Common 1.x or 2.0 allowing for the use of ows:Constraint for advertising the security constraints

The SWG will work on an alternate solution for WMS 1.3 (and WMS 1.1.x) to use ExtendedCapabilities as a placeholder for ows:Constraint.

The SWG will prepare security related Change Requests against OGC Service Standards on an as needed basis.

The SWG will define Client side requirements and implications for Security support including those needed for: (i) communication and (ii) processing.

## 4.1 Statement of relationship of planned work to the current OGC standards baseline

The OWS Common Security SWG will provide input on a Common Security extension to the new OWS Common SWG.

The OWS Common Security SWG will provide input to the suite of OGC Web Service SWGs through the development of Change Requests as needed.

## 4.2 What is Out of Scope?

Normative guidance on how to implement a specific security framework. This is up to each provider.

## 4.3 Specific Contribution of Existing Work as a Starting Point

The SWG will analyze the results and recommendations from OGC Testbed 11 related to Security requirements to include:

* 15-022 Testbed 11 Implementing Common Security Across the OGC Suite of Service Standards
* 15-077 Testbed-11 SOAP Interface
* 15-052 Testbed -11 REST Interface
* CR to WFS 1.1.0 to fix broken normative reference to OWS Common 0.0.3

## 4.4 Determination of SWG Completion

The OWS Common Security SWG work will be completed when all the tasks defined in paragraph 4. above have been completed, and the deliverables described in paragraph 5 produced.

## 4.5 Persistent SWG?

Yes

## 4.6 When can SWG be made inactive?

Upon completion of the tasks identified in Paragraph 4 have been accomplished.

# **5. Description of Deliverables**

The OWS Common Security SWG anticipates 2 deliverables: one Implementation Standard or extension and a separate Best Practice or User Guide for deployment options.

# **6. IPR Policy for this SWG**

x RAND-Royalty Free.  RAND for fee

# **7. Anticipated Participants**

Security DWG participants and OGC members which operate or want to operate secured OGC Web Services and any security experts of those members.

This is not meant as a limiting statement but instead is intended to provide guidance to interested potential participants as to whether they wish to participate in this SWG.

# **8. Other Informative Remarks about this SWG**

## a. Similar or Applicable Standards Work (OGC and Elsewhere).

The following standards and projects may be relevant to the SWG's planned work, although none currently provide the functionality anticipated by this committee's deliverables:

* ISO 10181
* IETF RFC 2818, 2617, 6256 (obsoletes 2965 and 2109)
* OGC OWS Common 1.x and 2.0

The SWG intends to seek and if possible maintain liaison with each of the organizations maintaining the above works.

## b. Details of the First Meeting

The first meeting of the SWG will be held during the September 2015 Technical Committee Meetings in Nottingham UK.

## c. Projected On-going Meeting Schedule

The SWG anticipates a regular bi-weekly telecon schedule until such time that this will no longer be necessary.

## d. Supporters of the Proposal (Charter Members)

The following people support this proposal and are committed to the Charter and projected meeting schedule. These members are the Charter members. The charter members agree to the SoW (Clauses 4 and 5) and IPR terms (Clause 6) as defined in this charter. The charter members have voting rights beginning the day the SWG is officially formed. Charter Members are shown on the public SWG page.

|  |  |
| --- | --- |
| **Name** | **Organization** |
| Frank Terpstra | Geonovum, NL |
| Satish Sankaran | Esri, USA |
| Don Sullivan | NASA, USA |
| Michael Leedahl | DigitalGlobe, USA |
| Arnaud Cauchy | Airbus Defence & Space, F |
| Jean-Baptiste Henry | Thales, F |
| Andreas Matheus | University of the Bundeswehr, D |
| David Wesloh | NGA, USA |

## e. Convener(s)

The conveners who started this SWG process are Dave Wesloh, NGA and Andreas Matheus, University of the Bundeswehr