

# Open Geospatial Consortium, Inc.

Date: 2010-08-18

Reference number of this document: OGC 10-155

Category: Engineering Report

Editor: Andreas Matheus

## **OGC<sup>®</sup> OWS-7 Towards secure interconnection of OGC Web Services with SWIM**

Copyright © 2010 Open Geospatial Consortium, Inc.

To obtain additional rights of use, visit <http://www.opengeospatial.org/legal/>.

### **Warning**

This document is not an OGC Standard. This document is an OGC Public Engineering Report created as a deliverable in an OGC Interoperability Initiative and is not an official position of the OGC membership. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an OGC Standard. Further, any OGC Engineering Report should not be referenced as required or mandatory technology in procurements.

|                    |                                         |
|--------------------|-----------------------------------------|
| Document type:     | OpenGIS <sup>®</sup> Engineering Report |
| Document subtype:  | NA                                      |
| Document stage:    | Approved for public release             |
| Document language: | English                                 |

## License Agreement

Permission is hereby granted by the Open Geospatial Consortium, ("Licensor"), free of charge and subject to the terms set forth below, to any person obtaining a copy of this Intellectual Property and any associated documentation, to deal in the Intellectual Property without restriction (except as set forth below), including without limitation the rights to implement, use, copy, modify, merge, publish, distribute, and/or sublicense copies of the Intellectual Property, and to permit persons to whom the Intellectual Property is furnished to do so, provided that all copyright notices on the intellectual property are retained intact and that each person to whom the Intellectual Property is furnished agrees to the terms of this Agreement.

If you modify the Intellectual Property, all copies of the modified Intellectual Property must include, in addition to the above copyright notice, a notice that the Intellectual Property includes modifications that have not been approved or adopted by LICENSOR.

THIS LICENSE IS A COPYRIGHT LICENSE ONLY, AND DOES NOT CONVEY ANY RIGHTS UNDER ANY PATENTS THAT MAY BE IN FORCE ANYWHERE IN THE WORLD.

THE INTELLECTUAL PROPERTY IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE INTELLECTUAL PROPERTY WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE INTELLECTUAL PROPERTY WILL BE UNINTERRUPTED OR ERROR FREE. ANY USE OF THE INTELLECTUAL PROPERTY SHALL BE MADE ENTIRELY AT THE USER'S OWN RISK. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR ANY CONTRIBUTOR OF INTELLECTUAL PROPERTY RIGHTS TO THE INTELLECTUAL PROPERTY BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM ANY ALLEGED INFRINGEMENT OR ANY LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR UNDER ANY OTHER LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH THE IMPLEMENTATION, USE, COMMERCIALIZATION OR PERFORMANCE OF THIS INTELLECTUAL PROPERTY.

This license is effective until terminated. You may terminate it at any time by destroying the Intellectual Property together with all copies in any form. The license will also terminate if you fail to comply with any term or condition of this Agreement. Except as provided in the following sentence, no such termination of this license shall require the termination of any third party end-user sublicense to the Intellectual Property which is in force as of the date of notice of such termination. In addition, should the Intellectual Property, or the operation of the Intellectual Property, infringe, or in LICENSOR's sole opinion be likely to infringe, any patent, copyright, trademark or other right of a third party, you agree that LICENSOR, in its sole discretion, may terminate this license without any compensation or liability to you, your licensees or any other party. You agree upon termination of any kind to destroy or cause to be destroyed the Intellectual Property together with all copies in any form, whether held by you or by any third party.

Except as contained in this notice, the name of LICENSOR or of any other holder of a copyright in all or part of the Intellectual Property shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Intellectual Property without prior written authorization of LICENSOR or such copyright holder. LICENSOR is and shall at all times be the sole entity that may authorize you or any third party to use certification marks, trademarks or other special designations to indicate compliance with any LICENSOR standards or specifications.

This Agreement is governed by the laws of the Commonwealth of Massachusetts. The application to this Agreement of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded. In the event any provision of this Agreement shall be deemed unenforceable, void or invalid, such provision shall be modified so as to make it valid and enforceable, and as so modified the entire Agreement shall remain in full force and effect. No decision, action or inaction by LICENSOR shall be construed to be a waiver of any rights or remedies available to it.

None of the Intellectual Property or underlying information or technology may be downloaded or otherwise exported or reexported in violation of U.S. export laws and regulations. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use the Intellectual Property, and you represent that you have complied with any regulations or registration procedures required by applicable law to make this license enforceable.

| <b>Contents</b>                                                                   | <b>Page</b> |
|-----------------------------------------------------------------------------------|-------------|
| 1 Introduction.....                                                               | 1           |
| 1.1 Scope.....                                                                    | 1           |
| 1.2 Document contributor contact points.....                                      | 1           |
| 1.3 Revision history .....                                                        | 1           |
| 1.4 Future work.....                                                              | 1           |
| 1.5 Forward .....                                                                 | 2           |
| 2 References.....                                                                 | 2           |
| 3 Terms and definitions .....                                                     | 2           |
| 4 Conventions .....                                                               | 2           |
| 4.1 Abbreviated terms.....                                                        | 2           |
| 4.2 UML notation.....                                                             | 3           |
| 5 Towards Secure Integration of OGC Web Services .....                            | 3           |
| 5.1 Purpose and Scope .....                                                       | 4           |
| 5.2 Security Requirements .....                                                   | 4           |
| 5.3 Summary of The System’s Architecture.....                                     | 5           |
| 5.4 Implementation of security requirements in The System .....                   | 6           |
| 5.5 Evaluation of Security for the Boundary Protection.....                       | 11          |
| 5.5.1 Boundary Protection for NAS End System .....                                | 11          |
| 5.5.2 Boundary Protection for General Public Interaction Services Evaluation..... | 12          |
| 5.5.3 Boundary Protection for Support Services Evaluation .....                   | 14          |
| 5.6 Recommendations Towards Secure Interconnection with OGC Web Service.....      | 16          |
| 5.6.1 OGC Web Services classification (interaction and support services) .....    | 16          |
| 5.6.2 OGC Web Services to be used as Interaction Services.....                    | 17          |
| 5.6.3 OGC Web Services to be used as Support Services .....                       | 17          |
| 5.6.4 Recommendations to OGC Standardization towards security.....                | 18          |
| 5.6.4.1 Towards secure integration of OGC Services as Interaction Services .....  | 18          |
| 5.6.4.2 Towards secure integration of OGC Services as Support Services .....      | 19          |

| <b>Figures</b>                                                                               | <b>Page</b> |
|----------------------------------------------------------------------------------------------|-------------|
| <b>Figure 1 – NAS external boundary protection concepts ([1], p.5-51)</b>                    | <b>7</b>    |
| <b>Figure 2 – Boundary protection for General Public Interaction Services ([1], p.5-52)</b>  | <b>8</b>    |
| <b>Figure 3 – Boundary protection for Support Services ([1], p.5-56)</b>                     | <b>9</b>    |
| <b>Figure 4 – Communication of external sub-systems ([1], p.5-9)</b>                         | <b>12</b>   |
| <b>Figure 5 – Communication of external entities with Interaction Services ([1], p.5-52)</b> | <b>13</b>   |
| <b>Figure 6 – Communication of external entities with Support Services ([1], p.5-56)</b>     | <b>15</b>   |

| <b>Tables</b>                                                                        | <b>Page</b> |
|--------------------------------------------------------------------------------------|-------------|
| <b>Table 1 –Core routing and encryption options .....</b>                            | <b>11</b>   |
| <b>Table 2 –OGC Web Services categorization attempt based on functionality .....</b> | <b>17</b>   |
| <b>Table 3 –SOAP Interface Binding for OGC Web Services.....</b>                     | <b>18</b>   |

# OGC® OWS-7 Towards secure interconnection of OGC Web Services with SWIM

## 1 Introduction

### 1.1 Scope

This Engineering Report provides guidance and generate action items for the OGC standardization effort to properly enable security in the near future such that a seamless, interoperable but secure interconnection between OGC Web Services and FUSE ESB technology stack as selected by use in the System Wide Information Management (SWIM) System of the US Federal Aviation Administration (FAA) can be achieved.

### 1.2 Document contributor contact points

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

| Name            | Organization                 |
|-----------------|------------------------------|
| Andreas Matheus | University of the Bundeswehr |
|                 |                              |
|                 |                              |

### 1.3 Revision history

| Date       | Release | Editor          | Primary clauses modified | Description |
|------------|---------|-----------------|--------------------------|-------------|
| 07/08/2010 | Draft   | Andreas Matheus |                          | First draft |
|            |         |                 |                          |             |
|            |         |                 |                          |             |

### 1.4 Future work

Improvements to this document are desirable to address open issues; to correct errors or enhance existing document content.

The understanding expressed in this report as well as the findings and recommendations of this report are derived from a theoretical exercise based on publically available documents. In order to gain a better understanding and to derive recommendations for an operational system, we like to recommend future work towards a prototype.

## 1.5 Forward

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.

## 2 References

The following documents are referenced in 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.

OGC 06-121r3, *OpenGIS<sup>®</sup> Web Services Common Standard*

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

FAA: *System Wide Information Management (SWIM), Segment 2 Technical Overview, Version 1.2*, 9 October 2009

FAA: *System Wide Information Management (SWIM), eXtensible Markup Language (XML) Gateway Requirements, Version 2.0*, September 21, 2009

## 3 Terms and definitions

For the purposes of this report, the definitions specified in Clause 4 of the OWS Common Implementation Specification [OGC 06-121r3] shall apply.

## 4 Conventions

### 4.1 Abbreviated terms

|      |                                   |
|------|-----------------------------------|
| CTS  | Coordinate Transformation Service |
| CSW  | Catalogue Service                 |
| ESB  | Enterprise Service Bus            |
| ER   | Engineering Report                |
| GIS  | Geo Information Systems           |
| HTTP | Hypertext Transfer Protocol       |
| OGC  | Open Geospatial Consortium        |

|        |                                           |
|--------|-------------------------------------------|
| SOA    | Service Oriented Architecture             |
| SOS    | Sensor Observation Service                |
| OpenLS | Location Services                         |
| OWS    | OGC Web Service                           |
| SAML   | Security Assertion Markup Language        |
| SPS    | Sensor Planning Service                   |
| STS    | Security Token Service                    |
| SWIM   | System Wide Information Management        |
| WCS    | Web Coverage Service                      |
| WFS    | Web Feature Service                       |
| WMS    | Web Map Service                           |
| WMTS   | Web Map Tiling Service                    |
| WPS    | Web Processing Service                    |
| XACML  | extensible Access Control Markup Language |
| XML    | Extensible Markup Language                |

## 4.2 UML notation

Most diagrams that appear in this document are presented using the Unified Modeling Language (UML) static structure diagram, as described in Subclause 5.2 of [OGC 06-121r3].

## 5 Towards Secure Integration of OGC Web Services

For the OGC OWS-7 initiative, the University of the Bundeswehr was tasked to perform a security evaluation for the integration of OGC Web Services with the FUSE ESB technology stack as selected by use in the System Wide Information Management (SWIM) System of the US Federal Aviation Administration (FAA); further on referred to as “The System”. As OGC Web Service specifications are currently silent about security, this evaluation surfs the purpose to provide guidance and generate action items for the OGC standardization effort to properly enable security in the near future such that a seamless, interoperable but secure interconnection between The System and OGC Web Services can be achieved. This provides the benefit for the FAA to enable geospatial data exchange by securely using OGC Web Services to safely exchange geospatial information. And it provides the benefit to OGC standardization to gain a good understanding of security use cases, motivated by this security analysis.

## 5.1 Purpose and Scope

It is the purpose of this Engineering Report to document the results of the security evaluation for the integration of OGC Web Services with The System undertaken during the OWS-7 initiative. The evaluation was undertaken upon information available in the Internet. These documents are listed in the sections “References” and “Bibliography”.

It is the overall concern of security to prevent unauthorized access to protected resources. For distributed systems like The System and OGC Web Services, the prevention of unauthorized access applies to information in storage and in transit. Protecting information in storage from unauthorized access requires appropriate control about physical access to the system (safety) as well as secure user account and key management. An evaluation of these topics is out of scope to this document.

In order to derive recommendations for the OGC standardization process regarding security, the main focus of this evaluation is to understand the architecture and the implementation of security requirements of interfaces that are relevant for The System to allow integration of external systems such as OGC Web Services.

## 5.2 Security Requirements

ISO 10181 (all parts) define a set of requirements in terms of a security framework for open systems. In order to protect the exchange of information between secured systems and the management of the stored data, the standard states that “... *security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.*”[4]. In subsequent parts of the standard, the requirements and the following security frameworks are defined:

- **Authentication Framework:** ISO 10181-2 (see [5]) 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 (see [6]) 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 (see [7]) 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 (see [8]) 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 (see [9]) defines the basic concepts of integrity, identical to the Confidentiality Framework.
- **Security Audits and Alarms Framework:** ISO 10181-7 (see [10]) defines the basic concepts for security audit and alarms and the relationship to other security services.
- **Availability:** This is a requirement that is in particular important in a Service Oriented Architecture. It is defined in ISO 7498-2 (see [11]) as „*The property of being accessible and useable upon demand by an authorized entity.*“ Adapting that to a Service means that the service shall be executable whenever there is a need.

### 5.3 Summary of The System’s Architecture

*Note: The following architecture summary is based on [1].*

The core of The System shall be implemented as an Enterprise Service Bus (ESB), routing messages between network endpoints, hence a destination. A destination is considered a logical combination of a message queue and a topic. The message format is XML (SOAP) and the protocol is HTTP or JMS. Three different kinds of message routing for the Core are supported:

- With **Content-Based Routing**, the destination of the message is determined from the content of the message.
- With **Context-Based Routing**, environment information determines the destination of the message.
- With **Itinerary-Based Routing**, the destination of the message is determined from metadata that is provided for the message itself.

The described architecture does naturally support communication between network endpoints which provides the capability to push relevant information from one source to many receivers based on the notification pattern. In order to achieve other types of communication such as communication with services based on the request/response pattern, message mediation services must be deployed. Other message mediation services shall perform transformation of other message formats to The System’s Core message format and vice versa. Network mediation services shall be used to support message traffic on different network protocols other than the core protocol.

The architecture further comprises of security services that are relevant for this evaluation:

- **Boundary Protection** shall control and protect communication to and from external National Airspace Systems (NAS).

- **Information System Security Support Infrastructure** services shall provide functions for key management.
- **Service Policy Enforcement and Access Management** services shall control access to services and resources based on NAS policies. Rights in the policy are linked which the requesting entity's identity, it's role or any other attributes.
- **Security Monitoring** services shall log the activities of NAS services and the activities of subjects on resources to detect a security breach or unauthorized access. The logged information shall be forwarded to a trust center for further analysis.

#### 5.4 Implementation of security requirements in The System

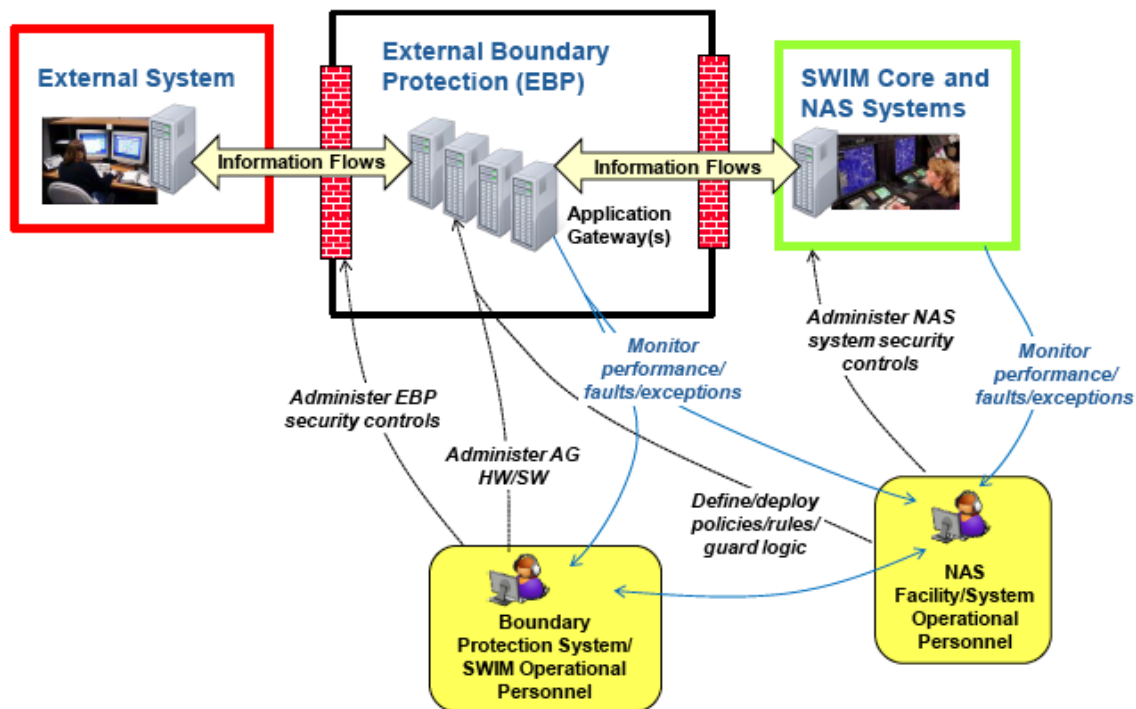
In [1], section 5.1.3.2.4 “Security”, states “*Authentication, authorization, and messaging security can be supported by a variety of mechanisms, including Java security APIs, username/password combination, or digital certificates (see Section 5.1.3.9).*”. Section 5.1.3.9 “Enterprise Messaging Security” is concerned with “*Messaging security as it applies to Message Brokers and Web Services (implemented in WSFs, ESBs, and Web based components) ...*”.

In a nutshell, The System's security architecture describes the implementation of requirements in a network agnostic fashion. It is the assumption that SOAP messages are protected towards integrity and confidentiality by applying WS-Security (see [14]). It is further recommended that the guarantee of delivery and the elimination of duplicate messages and correction of message order (as it potentially could occur in the defined Core) is implemented via WS-Reliable Messaging (see [13]). Access Control is twofold: It shall be implemented to control the flow of information from one destination to another destination and it shall be implemented as part of the boundary protection to prevent unauthorized access to The System's Core by external systems/services. The Core shall apply username/password or X.509 certificate based identification for direct and WS-Trust (see [15]) based identification for brokered authentication. The concept of a Security Token Service (STS) shall be used for establishing trust between communication / transaction parties.

Of particular concern to this evaluation is how The System is protected to external, non NAS systems, e.g. OGC Web Services. In [1], section 5.6.3.2 ff. “Boundary Protection ISS Capabilities”, the general approach of boundary protection is introduced and in sub-sections, specific types of boundary protection mechanisms are described for the following interaction pattern:

- Boundary Protection for General Public Interaction Services
- Boundary Protection for Support Services

Figure 1 – NAS external boundary protection concepts ([1], p.5-51) illustrates the general boundary protection (see [1], p. 5-51).



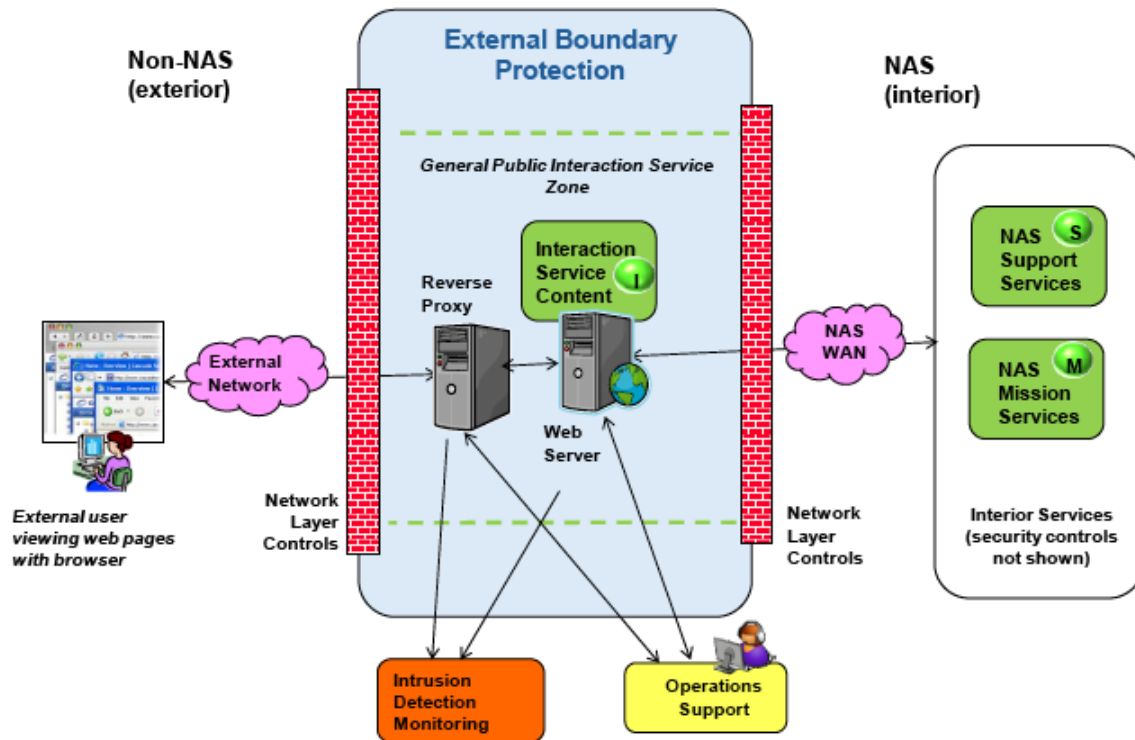
**Figure 5-21. General NAS External Boundary Protection Concepts**

**Figure 1 – NAS external boundary protection concepts ([1], p.5-51)**

An external system is connected to The System's Core via a Perimeter network hosting the Exterior Boundary Protection System, which provides two firewalls; one firewall to the external system and one firewall to the internal system and application gateways hosting the NAS Security Gateway services. These services provide the protection to prevent unauthorized messages to be forwarded to the Core by intercepting and inspecting incoming messages. Based on the content of the message, decisions are made whether or not the intercepted message shall be forwarded to the Core. Administrators of the boundary protection system define the overall control criteria for the decision making. As this decision making takes place on information concerning the application level, domain specific knowledge is required to maintain those rules and/or implement the decision making process.

**General Public Interaction Services** are to be used by human users and shall be made available to the general public in an anonymous fashion and to aviation partners where authorization depends on the requestors identity, approved through authentication. In general, the Interaction Services can be consumed via HTML pages or as RSS based feeds. As illustrated in Figure 2 – Boundary protection for General Public Interaction Services ([1], p.5-52), a Reverse Proxy shall control the incoming HTTP(S) requests to the Interaction Services, performing intrusion detection but also monitoring. It shall also undertake authentication and access control for ensuring aviation partners have legitimate access. OSAIS its Security Assertion Markup Language (SAML) (see [19]) and the eXtensible Access Control Markup Language (XACML) (see [21]) are named standards

to implement distributed authentication with the aviation partner(s) and to perform access control.



**Figure 5-22. Notional ISS Controls for General Public Interaction Service**

## **Figure 2 – Boundary protection for General Public Interaction Services ([1], p.5-52)**

**Support Services** shall be used by other services where no human user is present. Support Services shall be made available to aviation partners that want to further process FAA status information to be incorporated into planning and automation services. This communication shall be based on SOAP (see [16]) with optional WS-Security (see [14]) to ensure message integrity and confidentiality. As illustrated in Figure 3 – Boundary protection for Support Services ([1], p.5-56), for Support Services, the Reverse Proxy is replaced by a XML Gateway that shall inspect the incoming SOAP messages by verifying the integrity and the validity of the XML message.

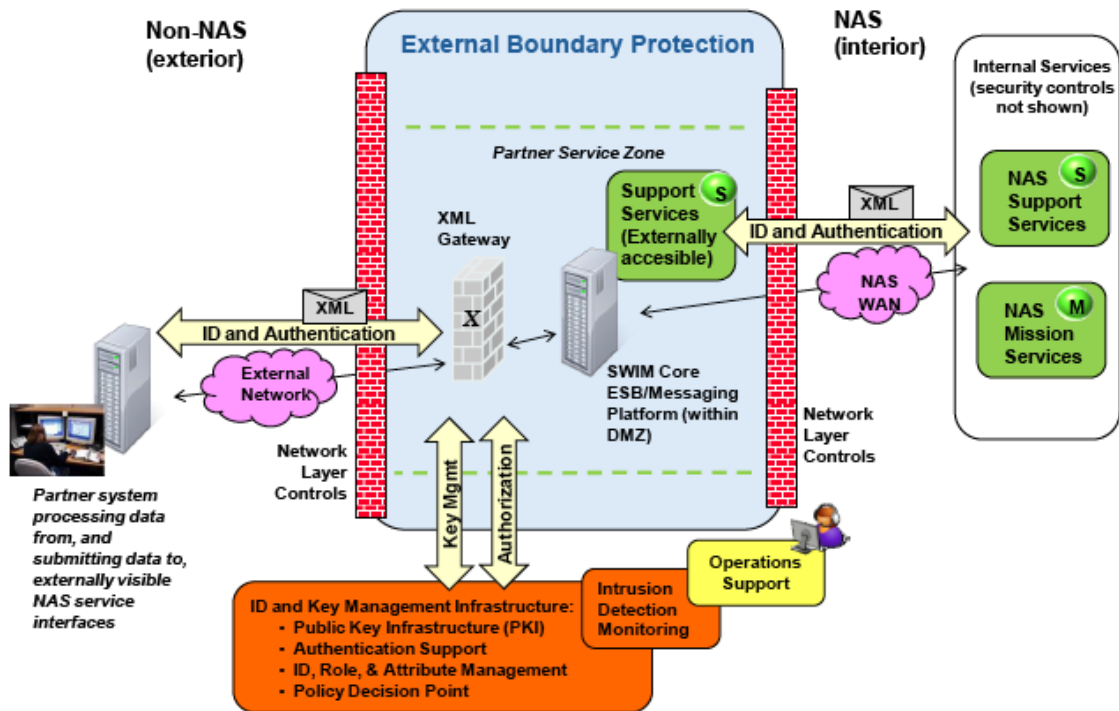


Figure 5-24. Boundary Protection Mechanisms for Support Services

Figure 3 – Boundary protection for Support Services ([1], p.5-56)

Requirements for the **XML Gateway** are defined in [3]. The communication shall be based on SOAP and the implementation of the following security requirements depend on the interaction scenario: Point-to-Point or Trusted Subsystem, Portal-to-Service, and Chained Service or Cross-Security Domain:

- Authentication
- Authorization
- Integrity
- Confidentiality
- Non-Repudiation

For the **Point-to-Point** interaction scenario, three different constellations occur:

- Client communicates with Service over HTTPS with mutual authentication based on X.509 certificates;
- Client communicates with Service and WS-Security Username Token is used for authentication;

- (iii) Client communicates with Service based on Security Token obtained from a STS to establish brokered trust. When a SAML Assertion based Token is used, it shall be possible to validate the chain of trust to the original assertion party.

For the **Portal-to-Service** interaction scenario, the client is a Web Browser and must establish a TLS based HTTPS communication based on mutual authentication. Optionally, the portal relays the request to the target service by attaching a SAML Token to the received request and adding its own credential to establish the “on behalf” aspect based on WS-Trust.

For the **Chained** interaction scenario, the Client interacts with the ESB instead of the Portal and the client is not a Web Browser. In order to fulfill a “on behalf” request, an optional STS shall be available that allows the client and the ESB to request and validate tokens.

For the **Cross-Domain** interaction scenario, the communication between the client and the service is mediated by two ESBs; one ESB in the domain of the client and one in the domain of the service. Both ESBs shall obtain security tokens from a trusted STS that resides in the service domain. The client domain is considered the Perimeter (DMZ) Network and the service domain is the NAS Network.

The System’s security outlined in [2] is concerned with Web Services security. It is concerned how to establish trust between Web Services based on the OASIS WS-Trust (see [15]) specification. As WS-Trust is based on SOAP and other security standards concerning message level based security, it can be used to overcome various Web Service / Client integration scenarios. In that sense, [2] illustrates in detail how to apply WS-Trust (and related standards) to achieve authentication, authorization, integrity by applying applicable processing to the messages. It also covers the delegation aspect by introducing a solution by verifying the chain of trust, based on SAML 2 (see [20]) assertions. In particular, [2] introduces security architectures and patterns to secure the following interactions:

- Portal-to-Service Interaction
- Chained Interaction
- Cross-domain Interaction

In order to implement these interaction scenarios, the document introduces three kinds of security profiles:

- SAML 1.1 Token Profile
- SAML 2 Token Profile
- WS-Security BinarySecurityToken Profile
- WS-Security UsernameToken Profile

- TLS Profile

## 5.5 Evaluation of Security for the Boundary Protection

This section describes the general security of the Boundary Protection in general and the security for Interaction and Support Services in particular. This, because we understand OGC Web Services as these types of services.

### 5.5.1 Boundary Protection for NAS End System

It is our understanding that communication between SIPs that do not belong to the same enclave cannot communicate to each other directly. The communication is routed via The System's Core as illustrated in Figure 4 – Communication of external sub-systems ([1], p.5-9). The Core supports three different kinds of routing: (i) Content based, (ii) Context based and (iii) Itinerary based routing. As the implementation of integrity and confidentiality is based on WS-Security, each SOAP message must be digitally signed to guarantee integrity and can optionally be encrypted to ensure confidentiality. For XML – hence SOAP messages – XML Encryption (see [18]) supports the following options of encryption: (i) encrypt a complete XML document, (ii) encrypt an element in an XML document, (iii) encrypt an element's content in an XML document.

As the encryption of (XML) messages is effective end-to-end (sender to the ultimate receiver), we see the following combinations for encryption option and routing to be possible:

|                              | Content based routing | Context based routing | Itinerary based routing |
|------------------------------|-----------------------|-----------------------|-------------------------|
| XML document encryption      | NO                    | MAY                   | YES                     |
| XML element encryption       | NO                    | YES                   | YES                     |
| XML element value encryption | NO                    | YES                   | YES                     |

**Table 1 –Core routing and encryption options**

It is not possible to use content based routing for received external messages that are protected towards confidentiality, because they are encrypted. It is possible to do Context (environment information) based routing of encrypted external messages regardless of encryption option. But this is bearing a risk as the encrypted messages cannot properly be inspected by the boundary inspection, depending on the encryption option.

- For document based encryption, it is not possible to verify the document structure and the origin of the message, as the related elements are encrypted.

- For element based encryption, it is not possible to verify the structure of the message content but it is possible to verify the origin of the message.
- For element value encryption, it is possible to verify the structure of the message content and the origin of the message. It is therefore possible to derive a solid decision if the message can be accepted or is to be rejected.
- Itinerary based routing relies on meta information available with the SOAP message that is typically available from the SOAP header that binds to information in the SOAP body of the same message. Assuming that the meta information conveyed in the SOAP header is ultimately attached to information in the SOAP body and that the metadata itself is protected by a digital signature, Itinerary based routing is acceptable for any encryption option. However, it is recommended for implementations of the boundary protection to follow the recommendations given by the W3C in [19].

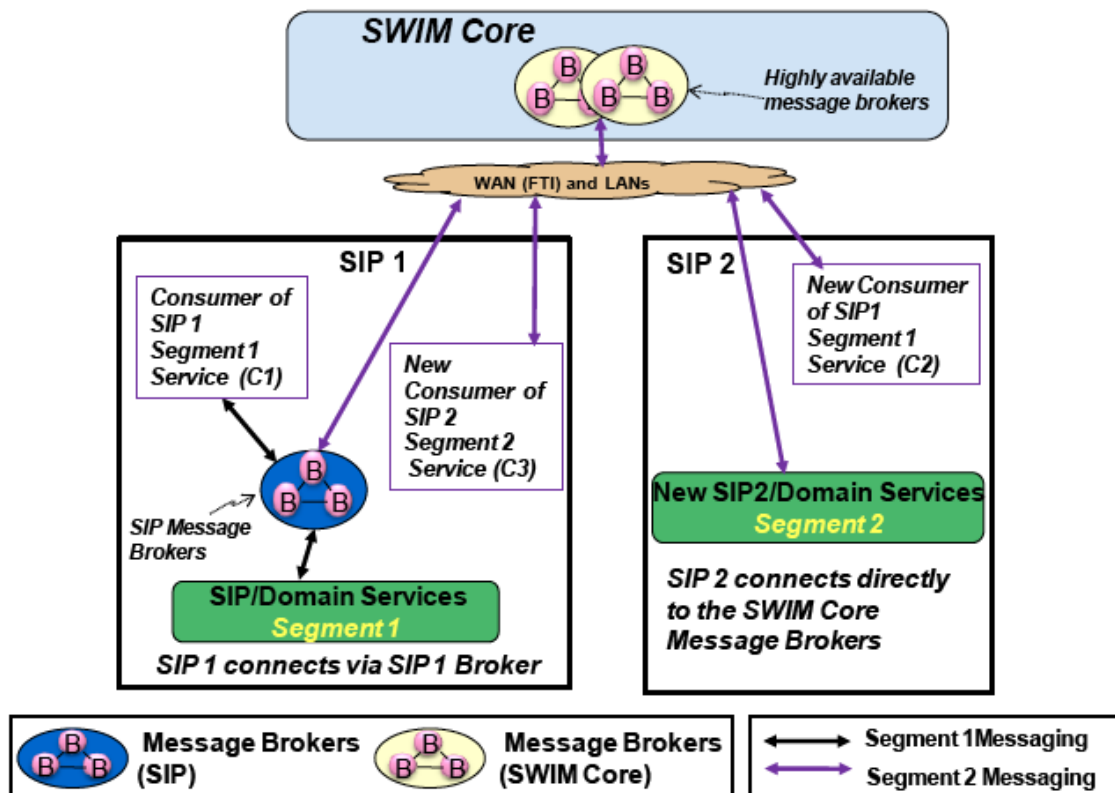


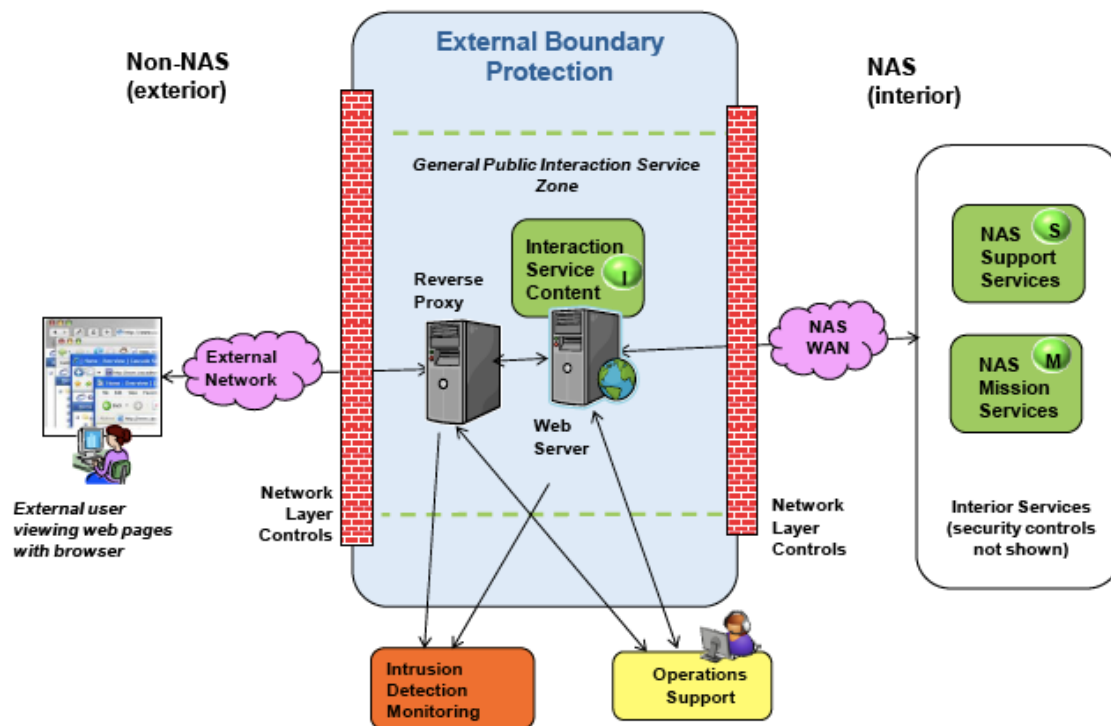
Figure 5-6. Transition Paths for Segment 1 Messaging to Segment 2 Message Brokers

Figure 4 – Communication of external sub-systems ([1], p.5-9)

### 5.5.2 Boundary Protection for General Public Interaction Services Evaluation

NAS Interaction Services are made available to non-NAS entities that reside outside the NAS (The System) and consume the information with a web browser via HTTPS. Protection for The System is anticipated through External Boundary Protection where the

perimeter network is separated with two independent firewalls from the external and internal network. The general architecture is illustrated in the figure below.



**Figure 5-22. Notional ISS Controls for General Public Interaction Service**

### **Figure 5 – Communication of external entities with Interaction Services ([1], p.5-52)**

The most important functionality in the boundary protection is that – beside the firewalls – the communication from the external user clients to the NAS Interaction Services is routed via a Reverse Proxy and a Web Server functions as a mediator. This ensures that no direct communication can be established from the external client to the internal Interaction Services.

Towards Authentication, two different user methods to establish a secure communication via HTTPS including mutual authentication shall be supported: Username / Password and X.509 certificates and maintain revocation lists. This requires that a X.509 certificate management is in place to release and revoke user certificates. SAML is mentioned as an additional mechanism to establish brokered authentication in a distributed environment. This becomes necessary if the user accounts are not stored inside the external boundary protection (e.g. at the Reverse Proxy).

Access Control can be established either in the Reverse Proxy based on configuration and environment information. [1] elaborates on p. 5-53 where enforcement of access restrictions shall be based on XACML policies following the proposed logical separation of enforcement and decision making as outlined in the XACML specification. The document foresees a Policy Enforcement and Policy Decision Point as part of the Access

Control Systems illustrated in the architecture (see Figure 5 – Communication of external entities with Interaction Services ([1], p.5-52)).

External entities that wish to interact with the NAS Interaction Services in a confidential or integrity protected communication, a secure network connection can be established with the Reverse Proxy using HTTPS.

Towards security audit and alarms, it is anticipated that the Reverse Proxy and the Mediation Service, as part of the Boundary Protection, provide the functionality to monitor the communication between the external user clients and the NAS Interaction Services. And because the communication confidentiality and integrity ends with the Reverse Proxy, the monitoring – as the prerequisite for audits and alarms – can be established.

### 5.5.3 Boundary Protection for Support Services Evaluation

NAS Support Services are made available to other services of non-NAS entities using SOAP over HTTPS. Similar to the protection of Interaction Services, the protection of Support Services is ensured by External Boundary Protection, where the external and the internal network are separated by two independent firewalls. This prevents direct communication from the external services to the NAS Support Services and enforces a routed and mediated communication. The incoming communication is handled by the XML Gateway which then – after inspection – forwards the requests to The System's Core Messaging Platform that is deployed in the perimeter network; hence inside the security domain of the External Boundary Protection. The architecture is illustrated in the figure below.

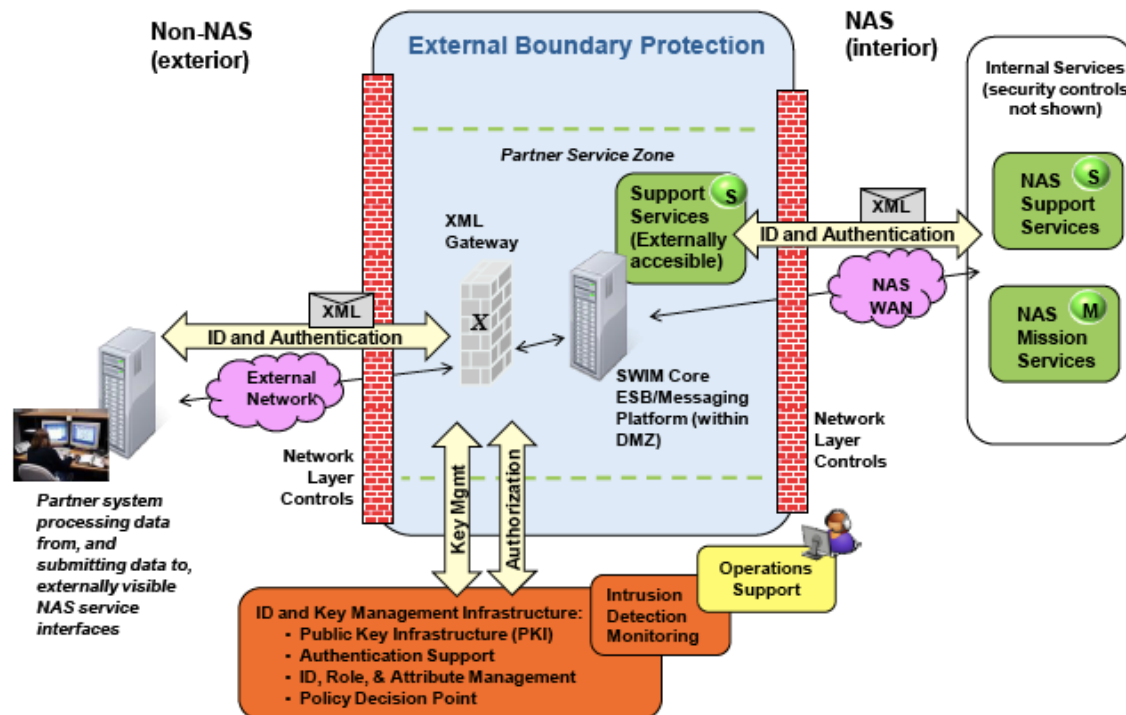


Figure 5-24. Boundary Protection Mechanisms for Support Services

### **Figure 6 – Communication of external entities with Support Services ([1], p.5-56)**

In this setup, the entire intrusion detection, establishment of secure communication (protected towards confidentiality and integrity) as well as access control and authentication is all handled by the XML Gateway. This component therefore is mission critical and must be implemented with care based on solid requirements.

*Note: For the evaluation of the XML Gateway, we have used [3] as a supplement.*

According to [1], authentication can be performed by either mutual HTTPS communication or by leveraging WS-Security with SOAP messages. As HTTPS provides a secure communication channel between systems, it should be the intention to use mutual authentication based on X.509 certificates representing the digital identities of the peer systems only, to establish a secure communication channel. As the communication from the external systems with the Support Services is based on SOAP, it is good practice to use WS-Security (and WS-Trust) – as described in the document - to enable application-to-service (end-to-end) authentication.

According to [1], confidentiality can be established on either connection level (HTTPS) or message level (XML encryption and WS-Security). We like to point out that there are fundamental differences between confidentiality established by HTTPS and XML Encryption on a SOAP message, causing side effects to overcome additional security requirements.

With HTTPS communications, the confidentiality of the information ends at the receiving entity which is not necessarily the same entity consuming the information. This raises the concern that the communication with the consuming entity must also be secured. Even when there is another secure communication with the consuming entity, the information is available in the clear at the receiving entity.

With confidentiality at the message level (encrypted SOAP body), the information is only available to the ultimate consumer and any other intermediary cannot read the information. This strength has a drawback on routing the incoming message, received by the XML Gateway to the appropriate consumer. Also, the encrypted message cannot be inspected at the XML Gateway so the ultimate consumer will process the message despite correct or malicious content.

According to [1], integrity can be established on either connection level (HTTPS) or message level (XML digital signatures and WS-Security). We like to point out that there are fundamental differences between integrity established by HTTPS and XML Digital Signature on a SOAP message. When applying HTTPS, it is possible for the XML Gateway to inspect the incoming message and create additional (meta) information to the inspected message before forwarding to the ultimate consuming entity, because the message itself is not protected. When applying integrity to the SOAP message, it is still possible for the XML gateway to inspect the incoming message but depending how the digital signature was applied to the message, it is or it is not possible to extend the message with the own (meta) information.

## 5.6 Recommendations Towards Secure Interconnection with OGC Web Service

We understand that OGC Web Services can be integrated to The System as service of trusted partners. As such, the connection of the OGC Web Services could technically be achieved by leveraging The System's Boundary Protection. The Boundary Protection basically allows to securely connect two different types of services: Interaction Services and Support Services. The former is technically connected through HTTP (e.g. RFC 1616) and secure extensions of HTTP such as HTTP+TLS/SSL, (e.g. RFC 2818). In order to analyse the ways OGC Web Services can be integrated, it is important to categorize existing OGC Web Service specifications and match them to be a support or interaction type service. The next step is to verify the existing interface to determine if the required binding and encoding is provided; hence HTTP and SOAP.

### 5.6.1 OGC Web Services classification (interaction and support services)

Categorization of OGC Web Services towards interaction and support services is potentially not a straight forward approach. Therefore, we introduce a table with three columns:

- √ at column #1 means that we put the OGC Service functionality to match the description of an interaction service
- √ at column #2 means that we put the OGC Service functionality to match the description of a support service
- √ at column #1 and #2 means that OGC Service is potentially both; an interaction and a support service

| OGC Service       | Interaction Service | Support Service |
|-------------------|---------------------|-----------------|
| CSW (see [22])    | √                   |                 |
| CTS (see [23])    |                     | √               |
| OpenLS (see [24]) | √                   | √               |
| SOS (see [25])    | √                   |                 |
| SPS (see [26])    | √                   |                 |
| WCS (see [27])    | √                   | √               |
| WFS (see [28])    | √                   | √               |
| WMS (see [29])    | √                   |                 |
| WMTS (see [30])   | √                   |                 |

|                |  |   |
|----------------|--|---|
| WPS (see [31]) |  | √ |
|----------------|--|---|

**Table 2 –OGC Web Services categorization attempt based on functionality**

### 5.6.2 OGC Web Services to be used as Interaction Services

The secure integration of Interaction Services according to the use case foresees a communication via HTTPS and a user is consuming the service with a web browser or web browser based client. According to the OGC Abstract Topic 12, this is considered Transparent Service Chaining. In order to achieve this, it is sufficient for the service to provide a simple interface binding supporting RFC 2616 and RFC 2818.

All OGC Web Service provide an interface binding that enables the service to be integrated with The System via a Boundary Protection System for Interaction Services using a Reverse Proxy. Because the support for HTTPS (HTTP+TLS or HTTP+SSL) is a feature of the deployment and not of the actual implementation of the service, no implications for OGC standardization exist.

### 5.6.3 OGC Web Services to be used as Support Services

The secure integration of Support Services according to the use case foresees a communication via HTTP or HTTPS and SOAP, where potentially the implementation of communication security (e.g. integrity and confidentiality) is ensured by securing SOAP messages according to WS-Security, and the service is “consumed” by another service and not used with a client operated by a human. Therefore, the OGC Web Service must provide a SOAP binding in order to be used as a Support Service. Also, the implementation of the service must support WS-Security and potentially WSDL+WS-Policy or WS-SecurePolicy to enable the service to advertize its security restrictions in such a way that it can automatically be consumed by the service, functioning as an automated client with no human interaction.

Not all OGC Web Services at the moment provide SOAP interfaces. The following table gives an overview which current versions provide SOAP interfaces.

| OGC Service | Version | Support Service | SOAP Interface |
|-------------|---------|-----------------|----------------|
| CSW         |         |                 | Yes            |
| CTS         |         | √               | No             |
| OpenLS      |         | √               | No             |
| SOS         |         |                 | No             |
| SPS         |         |                 | No             |

|      |  |   |     |
|------|--|---|-----|
| WCS  |  | √ | Yes |
| WFS  |  | √ | Yes |
| WMS  |  |   | No  |
| WMTS |  |   | Yes |
| WPS  |  | √ | Yes |

**Table 3 –SOAP Interface Binding for OGC Web Services**

#### 5.6.4 Recommendations to OGC Standardization towards security

For an operational use of OGC Web Services as outlined in this document, it is important that all relevant security requirements are implemented. Also, we recommend that OGC Web Services define fail state behavior that can be instantiated in case an error occurred from an attack. This is important to prevent harm to the asset.

In addition to this document, we like to point out that a detailed security assessment report for OGC Sensor Web Services can be found in the OWS-6 Secure Sensor Web Engineering Report (see [32]).

The following recommendation must be seen in the context of the question how to integrate OGC Web Services with The System in a securely manner to ensure the safe exchange of geospatial information. As outlined in previous sections, different security requirements must be implemented in order achieve this effort. As The System provides different integration strategies for Interaction and Support Services, we like to separate the recommendation accordingly.

##### 5.6.4.1 Towards secure integration of OGC Services as Interaction Services

- **Authentication**

For Interaction Services, it is essential to know the identity of the user. Various technologies of the underlying network protocol, such as HTTP, exist that can be used without affecting the OGC standardization, as the services interfaces do not need to change.

However, making a service require authentication implies that certain failure semantics are defined. As this is not done sufficiently in most OGC Service specifications, we recommend to address this issue for the next revision.

- **Access Control**

Denying or allowing access to an OGC Service requires that the service specifications defines corresponding error codes. For interaction services with the purpose to instruct the user of what to do next.

We recommend that OGC Service specification revisions address this issue.

Another facet of access control is filtering the result according to the interaction of the protected resources that the user requests and the resources the user has rights for. To our understanding, current OGC specifications do not allow the silent modification of a service request or response. We think it is therefore relevant to discuss ways forward how filtering becomes possible.

- **Non-repudiation**

The implementation of non-repudiation is out of scope for OGC Web Service specifications as it is a property of the deployment.

- **Confidentiality**

The implementation of confidentiality for OGC Services providing a “pure” HTTP binding is limited to communication channel security. However, for this type of interface binding, we do not see any recommendations that effect OGC standardization.

- **Integrity**

Same as confidentiality.

- **Security Audits and Alarms**

We understand the implementation of security audit as a deployment and use case specific issue which is independent from OGC Web Service specifications.

Alarming as a trigger for audit is application – hence OGC Web Service – specific. In order to enable a common set of alarms, we recommend to define a standard set of rules for the different operations and OGC Web Service types.

- **Availability**

One aspect of ensuring availability for OGC Web Services requires the appropriate inspection of service requests. We think it would be helpful to define a common set of rules - perhaps as a best practices approach - that allows a standard way of request inspection.

#### 5.6.4.2 Towards secure integration of OGC Services as Support Services

As Support Services are not consumed by clients controlled by humans, it is important to enable a fully automatic find & bind & execute. For protected OGC Web Services, we think it is important to start discussions if this is fully supported and how specifications

need to be adopted to ensure the approach. This includes the description of service endpoints including security conditions, how to bind and execute including error handling. It is important to describe how a service chain can undertake rollback if possible to prevent harm to assets.

- **Authentication**

In contrast to Interaction Services, the use of OGC Web Services as Support Services requires to maintain the identity of different entities that take part in the workflow and make the identity available to services down the chain. Another aspect for workflows is the support for “on behalf” statements. We understand that both requirements can be supported by using SOAP + WS-Security or WS-Trust as outlined in The System’s architecture.

The implication to OGC standardization is to ensure that for Support Services, the use of the SOAP header is no limited. We actually like to recommend that SOAP interfaces support WS-Security and allow whatever the WS-Security specification allows.

- **Access Control**

As Support Services are consumed by other services, it is required that service exceptions that result from missing access rights and the follow-up processing are standardized. In particular, we think it is mandatory to define the actions to be undertaken by the calling service in order to either report the failure to the end user or to automatically recover from the failure and proceed.

We recommend that OGC standardization addresses these issues for the next revision of service specifications.

- **Non-repudiation**

For SOAP messages, direct mechanisms exist for implementing non-repudiation, or at least to extend messages as such that non-repudiation becomes possible.

We like to recommend that the OGC community discusses the issue and evaluate a consensus of how to enable non-repudiation for workflows. We see this topic inside the Workflow or Decision Support DWG.

- **Confidentiality**

For services that support SOAP interfaces, it is possible to ensure confidentiality for the request and response message itself, independent from security provided by the underlying communication protocol.

In order to ensure that confidentiality can be applied to SOAP (request and response) messages, we recommend that the OGC standardization provides support for WS-Security.

- **Integrity**

Same as confidentiality.

- **Security Audits and Alarms**

As a Security Audits and Alarms for Interaction Services.

- **Availability**

For SOAP based interfaces, we think it extremely important to define common rules for the verification of service requests to ensure prevention or strong mitigation of corrupted requests that aim to reduce the availability of the service.

## Bibliography

- [1] FAA: System Wide Information Management (SWIM), Segment 2 Technical Overview, Version 1.2, 9 October 2009, FAA, 800 Independence Avenue, Washington D.C. 20591
- [2] FAA: U.S. Department of Transportation, Federal Aviation Administration, Specification, SWIM Web Service Security ( DRAFT ), FAA-XXXXX, March 5 2010, FAA, 800 Independence Avenue, Washington D.C. 20591
- [3] FAA: System Wide Information Management (SWIM), eXtensible Markup Language (XML) Gateway Requirements, September 21, 2009, Version 2.0, Federal Aviation Administration, 800 Independence Avenue SW, Washington, DC 20591
- [4] ISO/IEC 10181-1: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview, ISO 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=24404](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24404)
- [5] ISO/IEC 10181-2: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework, ISO 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=18198](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18198)
- [6] ISO/IEC 10181-3: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework, ISO 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=18199](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199)
- [7] ISO/IEC 10181-4: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework, ISO 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=23615](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=23615)
- [8] ISO/IEC 10181-5: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Confidentiality framework, ISO 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=24329](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24329)
- [9] ISO/IEC 10181-6: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Integrity framework, ISO 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=24330](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24330)
- [10] ISO/IEC 10181-7: Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework, ISO

- 1996:  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=18200](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18200)
- [11] ISO/IEC 7498-1: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 1: The Basic Model, [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=20269](http://www.iso.org/iso/catalogue_detail.htm?csnumber=20269)
  - [12] ISO/IEC 7498-2: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=14256](http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256)
  - [13] OASIS: WS-Reliable Messaging: Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2, Committee Draft, 28 February 2008: <http://docs.oasis-open.org/ws-rx/wsrn/200702/wsrn-1.2-spec-cd-01.pdf>
  - [14] OASIS: Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) – OASIS Standard Specification, 1 February 2006: <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>
  - [15] OASIS: WS-Trust 1.3, OASIS Standard, 19 March 2007: <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf>
  - [16] W3C: SOAP, W3C Recommendation (Second Edition) 27 April 2007: <http://www.w3.org/TR/soap/>
  - [17] W3C: XML Digital Signature: XML-Signature Syntax and Processing – W3C Recommendation 12 February 2002: <http://www.w3.org/TR/xmldsig-core/>
  - [18] W3C: XML Encryption: XML Encryption Syntax and Processing – W3C Recommendation 10 December 2002: <http://www.w3.org/TR/xmlenc-core/>
  - [19] W3C: XML Signature Best Practices, W3C Working Draft 04 February 2010, <http://www.w3.org/TR/xmldsig-bestpractices/>
  - [20] OASIS: SAML: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
  - [21] OASIS: XACML: eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 Feb 2005: [http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)
  - [22] OGC : CSW (Catalogue Service): <http://www.opengeospatial.org/standards/specifications/catalog>
  - [23] OGC : CTS (Coordinate Transformation Service): <http://www.opengeospatial.org/standards/ct>

- [24] OGC : OpenLS (Location Services): <http://www.opengeospatial.org/standards/ols>
- [25] OGC : SOS (Sensor Observation Service):  
<http://www.opengeospatial.org/standards/sos>
- [26] OGC: SPS (Sensor Planning Service):  
<http://www.opengeospatial.org/standards/sps>
- [27] OGC: WCS (Web Coverage Service):  
<http://www.opengeospatial.org/standards/wcps>
- [28] OGC: WFS (Web Feature Service): <http://www.opengeospatial.org/standards/wfs>
- [29] OGC: WMS (Web Map Service): <http://www.opengeospatial.org/standards/wms>
- [30] OGC: WMTS (Web Map Tiling Service):  
<http://www.opengeospatial.org/standards/wmts>
- [31] OGC: WPS (Web Processing Service):  
<http://www.opengeospatial.org/standards/wps>
- [32] OGC: OWS-6 Secure Sensor Web Engineering Report, OGC #08-176r1, June 2009: