

Enclosure 3

**EUROCONTROL Specification  
for  
SWIM TI Yellow Profile**

DOCUMENT IDENTIFIER : EUROCONTROL-SPEC- #####

<b>Edition Number</b>	:	<b>0.2</b>
<b>Edition Date</b>	:	<b>18 May 2017</b>
<b>Status</b>	:	<b>Draft</b>
<b>Intended for</b>	:	<b>General Public</b>
<b>Category</b>	:	<b>EUROCONTROL Specification</b>

## DOCUMENT CHARACTERISTICS

TITLE			
<b>EUROCONTROL Specification for SWIM TI Yellow Profile</b>			
			<b>Publication Reference:</b> SPEC-
			<b>ISBN Number:</b> xx
<b>Document Identifier</b>		<b>Edition Number:</b>	0.2
EUROCONTROL-SPEC-xx		<b>Edition Date:</b>	18 May 2017
Abstract			
<p>This specification contains requirements for system interfaces (e.g. protocols) and for IT infrastructure capabilities required to enable a reliable, secure and efficient exchange of information in the context of Initial System Wide Information Management (iSWIM). This contributes to technical interoperability.</p>			
Keywords			
SWIM	Technical Infrastructure	Service Interface Binding	Interoperability
System Wide Information Management			
Contact Person(s)		e-mail	Unit
Pedro Fernandez		swim@eurocontrol.int	ATM/STR/SWM

STATUS, AUDIENCE AND ACCESSIBILITY					
Status	Intended for			Accessible via	
Working Draft	<input type="checkbox"/>	General Public	<input checked="" type="checkbox"/>	Intranet	<input type="checkbox"/>
Draft	<input checked="" type="checkbox"/>	EUROCONTROL	<input type="checkbox"/>	Extranet	<input type="checkbox"/>
Proposed Issue	<input type="checkbox"/>	Restricted	<input type="checkbox"/>	Internet (www.eurocontrol.int)	<input checked="" type="checkbox"/>
Released Issue	<input type="checkbox"/>				

# DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.1	31 March 2017	Released for Specification Package consistency review.	All
0.2	18 May 2017	Update following internal review	All

### Publications

EUROCONTROL Headquarters  
96 Rue de la Fusée  
B-1130 BRUSSELS

Tel: +32 (0)2 729 4715  
Fax: +32 (0)2 729 5149  
E-mail: [publications@eurocontrol.int](mailto:publications@eurocontrol.int)

# CONTENTS

<b>DOCUMENT CHARACTERISTICS</b> .....	<b>2</b>
<b>DOCUMENT APPROVAL</b> .....	<b>3</b>
<b>DOCUMENT CHANGE RECORD</b> .....	<b>4</b>
<b>CONTENTS</b> .....	<b>5</b>
<b>LIST OF FIGURES</b> .....	<b>7</b>
<b>LIST OF TABLES</b> .....	<b>8</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>9</b>
<b>1. Introduction</b> .....	<b>10</b>
1.1 Purpose.....	10
1.2 Scope .....	10
1.3 Applicability .....	11
1.4 Target Audience .....	11
1.5 Conventions .....	11
1.6 Abbreviations .....	12
1.7 Definitions.....	15
1.8 Reference material .....	18
1.9 Document Structure.....	18
1.10 Maintenance of the Specification.....	19
<b>2. Conformance</b> .....	<b>20</b>
2.1 Interface Binding Conformance .....	20
2.2 Profile Part Conformance .....	21
<b>3. Interface Binding Specifications</b> .....	<b>24</b>
3.1 Interface Bindings Catalogue .....	24
3.1.1 Service Interface Bindings.....	24
3.1.1.1 WS Light .....	26
3.1.1.2 WS SOAP .....	26
3.1.1.3 WS SOAP with Basic Message Security.....	27
3.1.1.4 WS SOAP with Message Security .....	27
3.1.1.5 WS SOAP with Federated Security .....	28
3.1.1.6 WS-N SOAP .....	29
3.1.1.7 WS-N SOAP with Basic Message Security.....	30
3.1.1.8 WS-N SOAP with Message Security .....	31
3.1.1.9 WS-N SOAP with Federated Security .....	32
3.1.1.10 AMQP Messaging.....	33

3.1.2	<b>Network Interface Bindings .....</b>	<b>33</b>
3.1.2.1	IPv4 Unicast .....	33
3.1.2.2	IPv4 Secure Unicast.....	33
3.1.2.3	IPv6 Unicast .....	34
3.1.2.4	IPv6 Secure Unicast.....	34
3.2	<b>Interface Binding Requirements.....</b>	<b>34</b>
<b>4.</b>	<b>Profile Part Specifications .....</b>	<b>51</b>
4.1	<b>Core Profile Part .....</b>	<b>51</b>
4.1.1	Messaging .....	51
4.1.2	Security .....	51
4.1.3	Monitoring .....	61
4.1.4	Performance Efficiency .....	62
4.1.5	Reliability .....	63
4.2	<b>Extended Profile Part .....</b>	<b>63</b>
4.2.1	Messaging .....	63
4.2.2	Monitoring .....	65
4.2.3	Reliability .....	67
4.3	<b>Security+ Profile Part .....</b>	<b>68</b>
4.4	<b>Security+2 Profile Part .....</b>	<b>74</b>
<b>ANNEX A –</b>	<b>List of Contributors .....</b>	<b>80</b>

# LIST OF FIGURES

**Figure 1 – Conformance Overview ..... 20**

## LIST OF TABLES

<b>Table 1 – Requirement structures.....</b>	<b>12</b>
<b>Table 2 – List of abbreviations.....</b>	<b>14</b>
<b>Table 3 – List of terms with definitions .....</b>	<b>17</b>
<b>Table 4 – Bindings Overview.....</b>	<b>25</b>
<b>Table 5 – List of subject matter experts .....</b>	<b>80</b>



## EXECUTIVE SUMMARY

This specification contains requirements for the implementation of technical infrastructure supporting information exchanges in Initial System Wide Information Management (iSWIM).

It enables technical interoperability by specifying standardised technical interfaces (e.g. protocols) and the capabilities required to enable a reliable, secure and efficient exchange of information.

This specification is modular and provides different implementation options based on mainstream technology, taking into account a wide range of information exchange needs (e.g. security).

This specification is intended for use by technical experts designing and implementing systems and services.

# 1. Introduction

## 1.1 Purpose

This specification contains requirements for the implementation of technical infrastructure in the context of Initial System Wide Information Management (iSWIM) in Europe. The requirements are necessary for technical interoperability, enabling IT systems to communicate and exchange data.

In order to achieve technical interoperability, it is essential that IT systems use standardised interfaces and have the capabilities required to enable a reliable, secure and efficient exchange of information.

## 1.2 Scope

This specification focuses on technical interoperability, providing requirements for:

- The specification of IT system interfaces that enable the exchange of information based on standardised protocols. More specifically, it focuses on the interfaces of services that enable the exchange of information between ATM organisations, providing interconnectivity requirements, hereinafter referred to as Service Interface Binding Specifications.
- The specification of IT infrastructure capabilities that determine the required functional and non-functional technical capabilities for exchanging information in SWIM, hereinafter referred to as SWIM Technical Infrastructure Profile Specifications.

Among the IT infrastructure capabilities considered in this specification:

1. **Messaging**: Fundamental capability of the technical infrastructure responsible for the effective exchange of information.
2. **Security**: (All requirements in this category are traced to existing security standards<sup>1</sup>)
  - **Authentication**: Ensuring that the identity of a subject can be proved to be the one claimed.
  - **Authorization**: Granting of rights and, based on these rights, the granting of access.
  - **Integrity**: Protecting information from modification by unauthorized parties.
  - **Confidentiality**: Protecting information from disclosure to unauthorized parties.
  - **Data Protection**: Ensuring that the integrity and confidentiality of data is preserved and that its origin can be traced back to the relevant identity.
  - **Recording**: Ensuring that security-related events are recorded for real-time or deferred analysis.
3. **Monitoring** (of infrastructure components and services).
4. **Performance efficiency** (focused on throughput and time behaviour).
5. **Reliability** (focused on availability, fault tolerance and recoverability).

This specification relates to, but does not include, requirements for interfacing with infrastructure services shared among various organisations, e.g. Public Key Infrastructure (PKI), Security Token Infrastructure (STI)<sup>2</sup>, and Service Registry<sup>3</sup>. These are important areas for technical interoperability and are candidates for becoming self-standing standards.

---

<sup>1</sup> Security requirements are traced to NIST SP 800-53 rev4, (Appendix H) of said standard provides a traceability table to ISO/IEC 27001:2013. NIST SP 800-53 takes a more system-oriented point of view for the security controls which is a better fit to the scope of this Specification.

<sup>2</sup> PKI and STI were addressed in SESAR as part of the SWIM TI Identity Management Technical Specifications.

<sup>3</sup> Service Registry was addressed in SESAR and further worked is planned in SESAR 2020

## 1.3 Applicability

iSWIM supports “*information exchanges that are built on standards and delivered through an internet protocol (IP)-based network by SWIM enabled systems* [RD 1] It lists four areas for information exchanges:

- Aeronautical information exchange
- Meteorological information exchange
- Cooperative network information exchange
- Flight information exchange

The Pilot Common Project Regulation (PCP) [RD 1] requires the use of the SWIM Technical Infrastructure (TI) Yellow Profile specification for the implementation of the above-listed information exchanges.

Satisfying the requirements of this specification can be considered as a means of compliance for the implementation of the iSWIM ATM functionality as defined by the PCP [RD 1] in relation to IT system interfaces and IT infrastructure capabilities.

For exchanges related to “*flight information between ATC centres and between ATC and Network Manager*” the PCP [RD 1] requires the use of the SWIM TI Blue Profile<sup>4</sup>.

Beyond the PCP context, this specification is applicable to a wide variety of information exchanges, including those that require:

- Use of mainstream technology
- Cost-efficient implementation for the consumers
- Security over private networks as well as the internet.

## 1.4 Target Audience

The target audience for this specification includes, but is not limited to:

- Operational stakeholders implementing services supporting the exchange of information over SWIM. More specifically, technical experts designing and implementing systems and services;
- Oversight authorities.

## 1.5 Conventions

In this specification:

- Requirements using the operative verb **shall** indicate that they must be implemented to achieve the minimum objectives of this specification.
- Requirements using the operative verb **should** indicate that they are recommended to achieve the best possible implementation of this specification.
- Requirements using the operative verb **may** indicate options.

Each requirement is detailed in a table with the following structure.

<b>Title</b>	Title of the requirement, used as a short name for the requirement for mnemonic and readability purposes.
--------------	---

<sup>4</sup> The SWIM TI Blue Profile is an alternative specification to the SWIM TI Yellow Profile focused on real time communications requiring extremely high availability. At the time of this writing, the SWIM TI Blue profile is still in a research phase and not ready for standardisation.

<b>Identifier</b>	Unique identifier of the requirement.
<b>Requirement</b>	The statement expressing the requirement.
<b>Clarification</b>	Additional information providing the rationale, a particular interpretation of the requirement, a reference to similar requirements, as well as an example or any other description that facilitates understanding of the requirement.
<b>Verification</b>	<p>Providing an indication of the method to be used to verify the proper satisfaction of the requirement. The following verification methods are used:</p> <ol style="list-style-type: none"> <li>1) Document Inspection</li> <li>2) Configuration Inspection</li> <li>3) Demonstration</li> <li>4) Test</li> <li>5) Analysis</li> </ol>

**Table 1 – Requirement structures**

## 1.6 Abbreviations

Abbreviation	Term
<b>ABAC</b>	Attribute Based Access Control
<b>AIRM</b>	ATM Information Reference Model
<b>AMQP</b>	Advanced Message Queuing Protocol
<b>ATC</b>	Air Traffic Control
<b>ATM</b>	Air Traffic Management
<b>CAVP</b>	Cryptographic Algorithm Validation Program
<b>CMVP</b>	Cryptographic Module Validation Program
<b>COTS</b>	Commercial Off The Shelf
<b>CTR</b>	Common Time Reference
<b>DoS</b>	Denial of Service
<b>DDoS</b>	Distributed Denial of Service
<b>ERAF</b>	EUROCONTROL Regulatory and Advisory Framework
<b>HMI</b>	Human Machine Interface
<b>HTTP</b>	Hypertext Transfer Protocol

Abbreviation	Term
<b>ICMP</b>	Internet Control message Protocol
<b>IP</b>	Internet Protocol
<b>ISO</b>	International Organization for Standardization
<b>ISO/IEC</b>	International Standards Organization / International Electrotechnical Committee
<b>iSWIM</b>	Initial System Wide Information Management
<b>IT</b>	Information Technology
<b>MAC</b>	Message Authentication Code
<b>MEP</b>	Message Exchange Pattern
<b>MTOM</b>	Message Transmission Optimisation Mechanism
<b>NIST</b>	National Institute of Standards and Technology
<b>OASIS</b>	Organization for the Advancement of Structured Information Standards
<b>PCP</b>	Pilot Common Projects
<b>PKI</b>	Public Key Infrastructure
<b>QoS</b>	Quality of Service
<b>RBAC</b>	Role Based Access Control
<b>SESAR</b>	Single European Sky ATM Research
<b>SOAP</b>	Simple Object Access Protocol
<b>STI</b>	Security Token Infrastructure
<b>SWIM</b>	System Wide Information Management
<b>TCP</b>	Transmission Control Protocol
<b>TI</b>	Technical Infrastructure
<b>TLS</b>	Transport Layer Security Protocol
<b>VPN</b>	Virtual Private Network
<b>W3C</b>	World Wide Web Consortium
<b>WS</b>	Web Services
<b>WSDL</b>	Web Services Description Language

Abbreviation	Term
XML	Extensible Markup Language
YP	Yellow Profile

***Table 2 – List of abbreviations***

## 1.7 Definitions

Term	Definition	Source
<b>access control</b>	A procedure used to determine whether an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.	ITU X.1252:2010 [RD 4]
<b>accountability</b>	The degree to which the actions of an entity can be traced uniquely to the entity.	ISO/IEC 25010:2011 [RD 5]
<b>analysis (verification method)</b>	Technique based on analytical evidence obtained without any intervention on the submitted element using mathematical or probabilistic calculation, logical reasoning (including the theory of predicates), modelling and/or simulation under defined conditions to show theoretical compliance. Mainly used where testing to realistic conditions cannot be achieved or is not cost-effective.	SEBoK:2017 [RD 10]
<b>authenticity</b>	The degree to which the identity of a subject or resource can be proved to be the one claimed.	ISO/IEC 25010:2011 [RD 5]
<b>availability</b>	The degree to which a system, product or component is operational and accessible when required for use.	ISO/IEC 25010:2011 [RD 5]
<b>capability</b>	A functional or non-functional ability for performing a particular task.	–
<b>confidentiality</b>	The degree to which a product or system ensures that data is accessible only to those authorized to have access.	ISO/IEC 25010:2011 [RD 5]
<b>configuration inspection (verification method)</b>	Verification method for a system whereby information used by the system to specify system behaviour or characteristics of its components is analysed to assess proper compliance with a requirement.	–
<b>demonstration</b>	Verification method for a product or system that consists in using it as intended, confirming that the results are as planned or expected.	–
<b>digital identity</b>	A digital representation of the information known about a specific individual, group or organization.	ITU X.1252:2010 [RD 4]
<b>document inspection (verification method)</b>	Verification method for a product or system whereby information describing the product or system is analysed to assess proper compliance with a requirement.	–
<b>entity</b>	Something that has separate and distinct existence and that can be identified in context.  <i>Note: An entity can be a physical person, an animal, a juridical person, an organization, an active or passive</i>	ITU X.1252:2010 [RD 4]

Term	Definition	Source
	<i>thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.</i>	
<b>identity</b>	A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context.	ITU X.1252:2010 [RD 4]
<b>information service</b>	A type of service that provides an information exchange capability.	–
<b>integrity</b>	The degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data.	ISO/IEC 25010:2011 [RD 5]
<b>interface binding</b>	Specification of the protocols and data format to be used in transmitting messages defined by the associated interface.	W3C Web Services Description Requirements: 2002, [RD 6]
<b>interoperability</b>	The ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge.	–
<b>IT infrastructure</b>	All the hardware, software, networks, facilities, etc. required to develop, test, deliver, monitor, control or support applications and IT services. The term includes all the information technology but not the associated people, processes and documentation.	ITIL v3:2007
<b>message</b>	A message is a discrete unit of communication intended by the source for consumption by a given recipient or group of recipients.	–
<b>message exchange pattern (MEP)</b>	A Message Exchange Pattern (MEP) is a template, devoid of application semantics, that describes a generic pattern for the exchange of messages between agents. It describes relationships (e.g. temporal, causal, sequential, etc.) of multiple messages exchanged in conformance with the pattern, as well as the normal and abnormal termination of any message exchange conforming to the pattern.	W3C Web Services Glossary [RD 7]
<b>non-repudiation</b>	The degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	ISO/IEC 25010:2011 [RD 5]
<b>performance efficiency</b>	The performance relative to the amount of resources used under stated conditions. It includes time behaviour, resource utilization and capacity.	ISO/IEC 25010:2011 [RD 5]
<b>protocol</b>	A set of semantic and syntactic rules for exchanging information.	ISO/IEC 14519:2001



Term	Definition	Source
		[RD 8]
<b>reliability</b>	The degree to which a system, product or component performs specified functions under specified conditions for a specified period of time. It includes maturity, availability, fault tolerance and recoverability.	ISO/IEC 25010:2011 [RD 5]
<b>security</b>	The degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization. It includes confidentiality, integrity, non-repudiation, accountability, authenticity.	ISO/IEC 25010:2011 [RD 5]
<b>security token</b>	Something that a claiming entity possesses and controls (typically a cryptographic module or password) that is used to authenticate the entity's identity.	NIST SP 800-63-2:2013 [RD 11]
<b>service</b>	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface.	OASIS (2006) [RD 9]
<b>service description</b>	The information needed in order to use, or consider using, a service.	–
<b>service interface</b>	The means by which the underlying capabilities of a service are accessed. <i>Note: the service interface is the means for interacting with a service.</i>	OASIS (2006) [RD 9]
<b>SWIM TI</b>	A technical infrastructure conformant to one or more SWIM TI specifications (e.g. SWIM TI YP Specification).	–
<b>SWIM TI Profile</b>	Specification defining an implementation of the SWIM TI. Multiple SWIM TI Profiles can coexist, each of them focused on the implementation of technical infrastructure but with different scope and applicability.	–
<b>SWIM TI Profile Part</b>	A consistent grouping of related technical infrastructure requirements. A SWIM TI Profile is composed of one or more Profile Parts.	–
<b>technical infrastructure (TI)</b>	The software and hardware used in an organization that enables the provision of information services. <i>Note: Technical infrastructure is a subset of IT Infrastructure.</i>	–
<b>test (verification method)</b>	Technique performed onto the submitted element by which functional, measurable characteristics, operability, supportability, or performance capability is quantitatively verified when subjected to controlled conditions that are real or simulated. Testing often uses special test equipment or instrumentation to obtain accurate quantitative data to be analysed.	SEBoK:2017 [RD 10]

**Table 3 – List of terms with definitions**

## 1.8 Reference material

- [RD 1]** Commission Implementing Regulation (EU) No 716/2014 of 27 June 2014 on the establishment of the Pilot Common Project supporting the implementation of the European Air Traffic Management Master Plan
- [RD 2]** EUROCONTROL Specification for SWIM Information Definition, Ed. Xx, *date*
- [RD 3]** EUROCONTROL Specification for SWIM Service Description, Ed.xx, *date*
- [RD 4]** International telecommunication Union X.1252: Baseline identity management terms and definitions, April 2010
- [RD 5]** International Organization for Standardization - ISO/IEC 25010:2011 – Systems and software engineering – Systems and Software Quality Requirements and Evaluation (SQuaRE) – System and Software quality models
- [RD 6]** World Wide Web Consortium (W3C) Web Services Description Requirements (2002), <http://www.w3.org/TR/ws-desc-reqs/>
- [RD 7]** World Wide Web Consortium (W3C) Web Services Glossary (2004), <http://www.w3.org/TR/ws-gloss/>
- [RD 8]** International Organization for Standardization - ISO/IEC 14519:2001 – Information Technology – POSIX Ada Language Interfaces – Binding for System Application Program Interface (API)
- [RD 9]** OASIS Reference Model for Service Oriented Architecture 1.0 (2006), <http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf>
- [RD 10]** Guide to the Systems Engineering Body of Knowledge (SEBoK) [http://sebokwiki.org/wiki/Guide\\_to\\_the\\_Systems\\_Engineering\\_Body\\_of\\_Knowledge\\_\(SEBoK\)](http://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK))
- [RD 11]** NIST Electronic Authentication Guideline (2013), <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>

Note: This specification is based on the work carried out in SESAR related to the SWIM TI Yellow Profile.

## 1.9 Document Structure

The “Specification for SWIM TI YP” is composed of different sets of requirements that can be understood from an implementation point of view as different sub-specifications. The modularity provided by the different sub-specifications enables fit-for-purpose implementation adapted to specific information exchange needs.

Chapter 1 introduces this document, including its purpose, scope and audience.

Chapter 2 defines the Conformance Statements which specify how to conform to the SWIM TI YP Specification taking into account the alternatives and composability of its sub-specifications. There are two main categories of sub-specifications:

- SWIM TI Interface Bindings (chapter 3) provide requirements for the implementation of system interfaces. Each Interface Binding specification represents an alternative for interconnecting systems and satisfies different information exchange needs.
- SWIM TI Profile Parts (chapter 4) provide requirements for the implementation of a Technical Infrastructure. The implementation of these different and complementary specifications enables different technical infrastructure capabilities.

Annex A lists contributing subject matter experts.

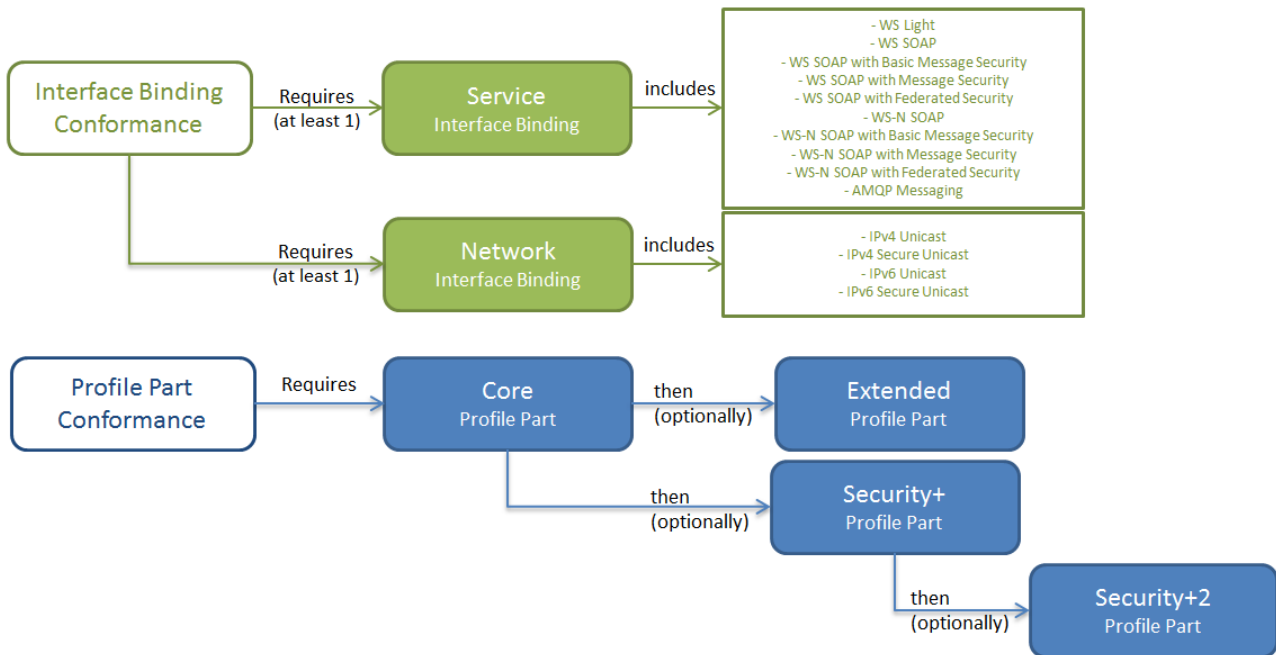
## **1.10 Maintenance of the Specification**

This EUROCONTROL Specification has been developed under the EUROCONTROL Advisory Framework (ERAF) and is maintained by EUROCONTROL in accordance with this framework.

## 2. Conformance

The SWIM TI YP provides requirements that are grouped into Interface Bindings (section 3) and Profile Part specifications (section 4). Each of these sub-specifications included in the SWIM TI YP is intended for a different purpose and addresses different exchange needs. To be conformant to the SWIM TI YP, it is not required to be conformant to all its sub-specifications as some of these are optional. Conformance to a sub-specification implies satisfying all its requirements as indicated by the operative verbs described in section 1.5 (shall, should, may). Requirements that are only part of optional sub-specifications are considered optional (may) for claiming conformance to the SWIM TI YP and their associated operative verb is only relevant when claiming conformance to the sub-specification they belong.

The figure below summarizes the process of identifying sub-specifications. Firstly, based on the functional and non-functional requirements of a service, the most appropriate Interface Bindings are identified both for service and network communication. Then, given that the Core Profile Part is always mandatory, there is a need to identify whether extra Profile Parts are desired, based on the capabilities they provide.



**Figure 1 – Conformance Overview**

### 2.1 Interface Binding Conformance

Interface Binding conformance statements specify the minimum required and options available to conform to the Interface Binding specifications of the SWIM TI YP (section 3). These statements are related to the objectives of the SWIM TI YP for the implementation of system interfaces, requiring:

1. The technical infrastructure to be able to support the implementation of standardised service interfaces and network interfaces as specified in the Interface Bindings of this document.
2. Services to implement standardised interfaces as specified in the Interface Bindings of this document.

<b>Title</b>	TI Conformance with Service Interface Bindings
<b>Conformance Statement</b>	A SWIM TI YP implementation <b>shall</b> be conformant with at least one of the Service Interface Bindings included in the SWIM TI YP Specification.
<b>Clarification</b>	The SWIM TI YP specification standardises, from a TI perspective, different types of service interfaces to address different exchange needs. These are the Service Interface Binding specifications. This conformance statement mandates the implementation of at least one Service Interface Binding for an implementation of the SWIM TI YP to be conformant.

<b>Title</b>	TI Conformance with Network Interface Bindings
<b>Conformance Statement</b>	A SWIM TI YP implementation <b>shall</b> be conformant with at least one of the Network Interface Bindings included in the SWIM TI YP Specification.
<b>Clarification</b>	The SWIM TI YP uses a network to effectively exchange information with other systems. In order to ensure that the SWIM TI YP can interface with the network, it has to support at least one of the Network Interface Bindings included in the SWIM TI YP specification.

<b>Title</b>	Service Conformance with Service Interface Bindings
<b>Conformance Statement</b>	An implementation of a SWIM Service interface <b>shall</b> use one of the Service Interface Bindings included in the SWIM TI YP specification.
<b>Clarification</b>	The SWIM TI YP specification standardises, from a TI perspective, different types of service interfaces that address different exchange needs. These are the Service Interface Binding specifications.

<b>Title</b>	Service Conformance with Network Interface Bindings
<b>Conformance Statement</b>	An implementation of a SWIM Service interface <b>shall</b> use one of the Network Interface Bindings included in the SWIM TI YP specification.
<b>Clarification</b>	The SWIM TI YP specification standardises, from a TI perspective, different types of network interfaces that address different exchange needs. These are the Network Interface Binding specifications.  A SWIM Service is required to use conformant Network Interface Bindings for its interfaces.

## 2.2 Profile Part Conformance

Profile part conformance statements detail how to conform to the Profile Part specifications of SWIM TI YP (section 4). Each of these Profile Part specifications focuses on different capabilities of a SWIM technical infrastructure and does not share requirements with other Profile Parts. Certain Profile Parts require as a prerequisite the implementation of other Profile Parts. There is a conformance statement for each Profile Part highlighting the intended purpose:

1. Conformance with the Core Profile Part implies an infrastructure with at least a minimum set of capabilities for the secure exchange of information.
2. Conformance with the Extended Profile Part implies an infrastructure with capabilities in addition to those specified in the core, focusing on additional reliability controls and extra messaging capabilities.

3. Conformance with the Security+ Profile Part implies an infrastructure with additional security capabilities in addition to those included in the core.
4. Conformance with the Security+2 Profile Part implies an infrastructure with additional security capabilities in addition to those included in Security+.

<b>Title</b>	TI Conformance to Core Profile Part
<b>Conformance Statement</b>	A SWIM TI YP implementation <b>shall</b> conform to the SWIM TI YP Core Profile Part Specification.
<b>Clarification</b>	<p>The Core Profile Part specification is a sub-specification of the SWIM TI YP that specifies the minimum set of requirements (excluding interface requirements) for the implementation of a technical infrastructure.</p> <p>A SWIM TI YP implementation is conformant with a Profile Part if it satisfies its included requirements in accordance with the operative verbs defined in section 1.5.</p>

<b>Title</b>	TI Conformance to Extended Profile Part
<b>Conformance Statement</b>	A SWIM TI YP implementation <b>may</b> conform to the Extended Profile Part Specification.
<b>Clarification</b>	<p>The Extended Profile Part specification is a sub-specification of the SWIM TI YP that specifies optional requirements for the implementation of a technical infrastructure. The Extended Profile Part requires the implementation of capabilities that are required in more sophisticated information exchange scenarios than those addressed by the core.</p> <p>A SWIM TI YP implementation is conformant with a Profile Part if it satisfies its included requirements in accordance with the operative verbs defined in section 1.5.</p>

<b>Title</b>	TI Conformance to Security+ Profile Part
<b>Conformance Statement</b>	A SWIM TI YP implementation <b>may</b> conform to the Security+ Profile Part Specification.
<b>Clarification</b>	<p>The Security+ Profile Part specification is a sub-specification of the SWIM TI YP that specifies optional requirements for the implementation of a technical infrastructure security. The Security+ Profile Part requires the implementation of capabilities that go beyond the most common security needs.</p> <p>A SWIM TI YP implementation is conformant with a Profile Part if it satisfies its included requirements in accordance with the operative verbs defined in section 1.5.</p>

<b>Title</b>	TI Conformance to Security+2 Profile Part
<b>Conformance Statement</b>	A SWIM TI YP implementation <b>may</b> conform to the Security+2 Profile Part Specification if it also conforms to the Security+ Profile Part.
<b>Clarification</b>	<p>The Security+2 Profile Part specification is a sub-specification of the SWIM TI YP that specifies optional requirements for the implementation of a technical infrastructure security. The Security+2 Profile Part requires the implementation of sophisticated capabilities aimed at satisfying strict security</p>

	<p>needs.</p>
--	---------------

	<p>A SWIM TI YP implementation is conformant with a Profile Part if it satisfies its included requirements in accordance with the operative verbs defined in section 1.5.</p>
--	---

## 3. Interface Binding Specifications

An Interface Binding specification is a consistent, self-contained grouping of interface requirements. Interface requirements focus mainly on the protocols and configuration options to be used for the transmission of messages. The SWIM TI YP includes a variety of Interface Binding specifications covering different technologies and capabilities which provide different alternatives to implementers.

### 3.1 Interface Bindings Catalogue

This section provides an overview of all Interface Binding specifications included in the SWIM TI YP, describing their main differentiating characteristics. Bindings are grouped into two categories:

1. Service Interface Bindings that enable services to exchange data with consuming applications based on the capabilities of the SWIM TI. The Service Interface Binding specifications are to be considered during the design of services.
2. Network Interface Bindings that enable the SWIM TI to exchange data with the network.

As explained in the scope section, interfaces with infrastructure services such as PKI and Registry do not fall within the scope of this document. Infrastructure services are expected to have their corresponding specifications.

#### 3.1.1 Service Interface Bindings

Service Interface Bindings can be differentiated from each other based on the messaging and security capabilities they provide.

- Exchange cardinality describes whether the information is intended to be sent from one endpoint to another or to several ones during the exchange (1 to 1, 1 to N).
- Time Decoupling determines whether the participating entities need to be available at the same time in order to exchange information.
- Process Decoupling determines whether the process originating the exchange remains blocked until there is a response from the entity addressed.
- Supported/Specified MEP describes the capability to implement (support<sup>5</sup>) or the availability of a concrete specification to implement (specified) a certain MEP:
  - R/R, Request Reply (1 to 1, time and processed coupled)
  - aR/R, asynchronous Request Reply (1 to 1, time but not process coupled)
  - P/S, Publish Subscribe, which can be further specialized into push and pull. (1 to N decoupled)
  - FF, Fire and Forget (1 to 1).
- Messaging QoS describes the capability to ensure a certain type of delivery (e.g. at most once, at least once, exactly once).
- Bandwidth Efficiency provides an estimate of the bandwidth overhead of each of the protocol selections.
- Security: Information exchanges are cryptographically protected ensuring their confidentiality and integrity and enforcing user authentication and authorization access. Based on the different Interface Bindings available, the SWIM TI provides different options to secure information, applying security at different levels:
  - Transport Level Security: Uses transport protocols (i.e. TLS) to secure communications. Providing point-to-point security and an efficient information exchange.

<sup>5</sup> Certain bindings are based on technology that does not specify concretely how to implement a particular MEP; however this can be implemented as a combination of other more basic MEPs.



- o **Message Level Security:** Uses message security protocols (e.g. SOAP Message Security, XML encryption) to secure messages individually and independently of the transport. It is suitable when information is routed through intermediary systems and security needs to be ensured end-to-end.

The below table provides an overview of all service bindings, highlighting the main differentiating characteristics.

	MEP		Performance		Security			Binding
	Pattern Supported <sup>6</sup>	Pattern Specified <sup>7</sup>	Messaging QoS Capability	Bandwidth Efficiency	Confidentiality	Integrity	Authentication	
HTTP	R/R	R/R	No	++	Transport	Transport	Transport (X.509 Server or X.509 Mutual)	<b>WS Light</b>
SOAP WS	R/R	R/R	Yes	+	Transport	Transport	Transport (X.509 Server or X.509 Mutual)	<b>WS SOAP</b>
					Transport	Transport	Transport (X.509 Server or X.509 Mutual) Message (Username/Password)	<b>WS SOAP with Basic Message Security</b>
					Message (Optional)	Message	Message (X.509)	<b>WS SOAP with Message Security</b>
					Message (Optional)	Message	Message (X.509 or SAML)	<b>WS SOAP with Federated Security</b>
SOAP WS-N	P/S	P/S	Yes	+	Transport	Transport	Transport (X.509 Server or X.509 Mutual)	<b>WS-N SOAP</b>
					Transport	Transport	Transport (X.509 Server or X.509 Mutual) Message (Username/Password)	<b>WS-N SOAP with Basic Message Security</b>
					Message Optional	Message	Message (X.509)	<b>WS-N SOAP with Message Security</b>
					Message Optional	Message	Message (X.509 or SAML)	<b>WS-N SOAP with Federated Security</b>
AMQP	(a)R/R, P/S, FF	FF	Yes	+++	Transport	Transport	Transport (X.509 Server with SASL Client or X.509 mutual)	<b>AMQP Messaging</b>

**Table 4 – Bindings Overview**

The following sub-sections specify the interface bindings, stating the requirements they include and their corresponding conformance level as described in section 1.5. (Mandatory, Recommended, Optional). When a requirement needs to be satisfied when a condition is met, a “Conditional” suffix

<sup>6</sup> “Pattern Supported” refers to message exchange patterns which the protocol can participate in or that can be built on top of the protocol.

<sup>7</sup> “Pattern Specified” refers to message exchange patterns which are explicitly defined as part of the protocol specification.

will be added (e.g. Mandatory Conditional).

### 3.1.1.1 WS Light

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">TLS Authentication</a>	SWIM-TIYP-0041	Mandatory
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">HTTP over TLS</a>	SWIM-TIYP-0007	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TLS</a>	SWIM-TIYP-0005	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.2 WS SOAP

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding- specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">TLS Authentication</a>	SWIM-TIYP-0041	Mandatory
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP over TLS</a>	SWIM-TIYP-0007	Mandatory

<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TLS</a>	SWIM-TIYP-0005	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.3 WS SOAP with Basic Message Security

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">TLS Mutual Authentication</a>	SWIM-TIYP-0049	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">WS Security Username Token</a>	SWIM-TIYP-0027	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">SOAP Message Security</a>	SWIM-TIYP-0023	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP over TLS</a>	SWIM-TIYP-0007	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TLS</a>	SWIM-TIYP-0005	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.4 WS SOAP with Message Security

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
-------------------	----------------	-------------------

<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">SOAP Encryption</a>	SWIM-TIYP-0045	Optional
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">SOAP Message Signing</a>	SWIM-TIYP-0039	Mandatory
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">WS Security X509</a>	SWIM-TIYP-0028	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">XML Signatures</a>	SWIM-TIYP-0025	Mandatory
<a href="#">XML Encryption</a>	SWIM-TIYP-0024	Mandatory Conditional
<a href="#">SOAP Message Security</a>	SWIM-TIYP-0023	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.5 WS SOAP with Federated Security

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Addressing</a>	SWIM-TIYP-0022	Mandatory
<a href="#">WS Secure Conversation</a>	SWIM-TIYP-0020	Mandatory
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">WS Security Token Profiles</a>	SWIM-TIYP-0046	Mandatory
<a href="#">SOAP Encryption</a>	SWIM-TIYP-0045	Optional

<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">WS Federation</a>	SWIM-TIYP-0031	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">WS Trust</a>	SWIM-TIYP-0021	Mandatory
<a href="#">SOAP Message Signing</a>	SWIM-TIYP-0039	Mandatory
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">XML Signatures</a>	SWIM-TIYP-0025	Mandatory
<a href="#">XML Encryption</a>	SWIM-TIYP-0024	Mandatory Conditional
<a href="#">SOAP Message Security</a>	SWIM-TIYP-0023	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.6 WS-N SOAP

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">WS Notification</a>	SWIM-TIYP-0013	Mandatory
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">TLS Authentication</a>	SWIM-TIYP-0041	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory

<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">WS Security Username Token</a>	SWIM-TIYP-0027	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP over TLS</a>	SWIM-TIYP-0007	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TLS</a>	SWIM-TIYP-0005	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.7 WS-N SOAP with Basic Message Security

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">WS Notification</a>	SWIM-TIYP-0013	Mandatory
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">TLS Mutual Authentication</a>	SWIM-TIYP-0049	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">WS Security Username Token</a>	SWIM-TIYP-0027	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">SOAP Message Security</a>	SWIM-TIYP-0023	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory

<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP over TLS</a>	SWIM-TIYP-0007	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TLS</a>	SWIM-TIYP-0005	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.1.8 WS-N SOAP with Message Security

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">WS Notification</a>	SWIM-TIYP-0013	Mandatory
<a href="#">SOAP Encryption</a>	SWIM-TIYP-0045	Optional
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">SOAP Message Signing</a>	SWIM-TIYP-0039	Mandatory
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">WS Security X509</a>	SWIM-TIYP-0028	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">XML Signatures</a>	SWIM-TIYP-0025	Mandatory
<a href="#">XML Encryption</a>	SWIM-TIYP-0024	Mandatory Conditional
<a href="#">SOAP Message Security</a>	SWIM-TIYP-0023	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory

<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory
---------------------	----------------	-----------

### 3.1.1.9 WS-N SOAP with Federated Security

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">WS Addressing</a>	SWIM-TIYP-0022	Mandatory
<a href="#">WS Secure Conversation</a>	SWIM-TIYP-0020	Mandatory
<a href="#">WS Reliable Messaging</a>	SWIM-TIYP-0032	Optional
<a href="#">WS Notification</a>	SWIM-TIYP-0013	Mandatory
<a href="#">WS Security Token Profiles</a>	SWIM-TIYP-0046	Mandatory
<a href="#">SOAP Encryption</a>	SWIM-TIYP-0045	Optional
<a href="#">HTTP POST</a>	SWIM-TIYP-0044	Mandatory
<a href="#">HTTP Reason Phrase Header</a>	SWIM-TIYP-0043	Mandatory
<a href="#">HTTP Status Code Header</a>	SWIM-TIYP-0042	Mandatory
<a href="#">WS Federation</a>	SWIM-TIYP-0031	Mandatory
<a href="#">WS Policy</a>	SWIM-TIYP-0019	Optional
<a href="#">WS Trust</a>	SWIM-TIYP-0021	Mandatory
<a href="#">SOAP Message Signing</a>	SWIM-TIYP-0039	Mandatory
<a href="#">HTTP Header Transfer Encoding</a>	SWIM-TIYP-0038	Mandatory
<a href="#">HTTP Header Content Encoding</a>	SWIM-TIYP-0037	Mandatory
<a href="#">HTTP Content Type Header</a>	SWIM-TIYP-0030	Mandatory
<a href="#">XML Schema Validation</a>	SWIM-TIYP-0029	Mandatory
<a href="#">XML</a>	SWIM-TIYP-0026	Mandatory
<a href="#">XML Signatures</a>	SWIM-TIYP-0025	Mandatory
<a href="#">XML Encryption</a>	SWIM-TIYP-0024	Mandatory Conditional
<a href="#">SOAP Message Security</a>	SWIM-TIYP-0023	Mandatory
<a href="#">WS-I Security</a>	SWIM-TIYP-0012	Mandatory
<a href="#">WSI</a>	SWIM-TIYP-0011	Mandatory
<a href="#">WSDL</a>	SWIM-TIYP-0010	Mandatory
<a href="#">MTOM</a>	SWIM-TIYP-0009	Recommended
<a href="#">SOAP</a>	SWIM-TIYP-0008	Mandatory
<a href="#">HTTP</a>	SWIM-TIYP-0006	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory



### 3.1.1.10 AMQP Messaging

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">Data Compression</a>	SWIM-TIYP-0040	Optional
<a href="#">AMQP Content Encoding Header</a>	SWIM-TIYP-0048	Mandatory
<a href="#">AMQP Content Type Header</a>	SWIM-TIYP-0047	Mandatory
<a href="#">AMQP</a>	SWIM-TIYP-0033	Mandatory
<a href="#">TLS</a>	SWIM-TIYP-0005	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory
<a href="#">AMQP Transport Security Authentication</a>	SWIM-TIYP-0036	Mandatory

## 3.1.2 Network Interface Bindings

### 3.1.2.1 IPv4 Unicast

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">DNSSEC</a>	SWIM-TIYP-0034	Optional
<a href="#">Satisfactory Bandwidth</a>	SWIM-TIYP-0035	Mandatory
<a href="#">RFC 950</a>	SWIM-TIYP-0017	Mandatory
<a href="#">ICMP</a>	SWIM-TIYP-0016	Mandatory
<a href="#">RFC 1122</a>	SWIM-TIYP-0015	Mandatory
<a href="#">IPv4</a>	SWIM-TIYP-0003	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.2.2 IPv4 Secure Unicast

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">DNSSEC</a>	SWIM-TIYP-0034	Optional
<a href="#">Satisfactory Bandwidth</a>	SWIM-TIYP-0035	Mandatory
<a href="#">RFC 950</a>	SWIM-TIYP-0017	Mandatory
<a href="#">ICMP</a>	SWIM-TIYP-0016	Mandatory
<a href="#">RFC 1122</a>	SWIM-TIYP-0015	Mandatory
<a href="#">IPv4</a>	SWIM-TIYP-0003	Mandatory
<a href="#">IPsec</a>	SWIM-TIYP-0002	Mandatory

<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory
---------------------	----------------	-----------

### 3.1.2.3 IPv6 Unicast

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">DNSSEC</a>	SWIM-TIYP-0034	Optional
<a href="#">IPv6 Node Requirements</a>	SWIM-TIYP-0014	Mandatory
<a href="#">Satisfactory Bandwidth</a>	SWIM-TIYP-0035	Mandatory
<a href="#">RFC 1122</a>	SWIM-TIYP-0015	Mandatory
<a href="#">IPv6</a>	SWIM-TIYP-0004	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

### 3.1.2.4 IPv6 Secure Unicast

The following table makes reference to all interface requirements that need to be satisfied in order to claim conformance to this interface binding specification.

Requirement Title	Requirement ID	Conformance Level
<a href="#">DNSSEC</a>	SWIM-TIYP-0034	Optional
<a href="#">IPv6 Node Requirements</a>	SWIM-TIYP-0014	Mandatory
<a href="#">Satisfactory Bandwidth</a>	SWIM-TIYP-0035	Mandatory
<a href="#">RFC 1122</a>	SWIM-TIYP-0015	Mandatory
<a href="#">IPv6</a>	SWIM-TIYP-0004	Mandatory
<a href="#">IPsec</a>	SWIM-TIYP-0002	Mandatory
<a href="#">TCP</a>	SWIM-TIYP-0001	Mandatory

## 3.2 Interface Binding Requirements

This section contains a consolidated list of all requirements that are included by the Interface Binding specifications.

### TCP

<b>Identifier</b>	SWIM-TIYP-0001
<b>Title</b>	TCP
<b>Statement</b>	The Service Interface Binding <b>shall</b> support IETF RFC 793 (Transmission Control Protocol).
<b>Clarification</b>	This requirement mandates the use of the Transmission Control Protocol. + IETF RFC 793 (TCP): <a href="http://tools.ietf.org/html/rfc793">http://tools.ietf.org/html/rfc793</a>
<b>Verification</b>	Test, Configuration Inspection

**IPsec**

<b>Identifier</b>	SWIM-TIYP-0002
<b>Title</b>	IPsec
<b>Statement</b>	The Network Interface Binding <b>shall</b> support IPsec according to IETF RFC 5406.
<b>Clarification</b>	<p>This requirement mandates support of IPsec in accordance to IETF RFC 5406. IPsec admits certain variability and optionality in its use which needs to be properly selected and documented. IETF RFC 5406 provides considerations for these aspects and guidance towards documenting the existing optionality.</p> <p>+ IETF RFC 5406: <a href="https://www.ietf.org/rfc/rfc5406.txt">https://www.ietf.org/rfc/rfc5406.txt</a></p> <p>The IPsec protocol itself is defined in IETF RFC 4301.</p> <p>+ IETF RFC 4301: <a href="https://www.ietf.org/rfc/rfc4301.txt">https://www.ietf.org/rfc/rfc4301.txt</a></p> <p>While different algorithms and configuration options are defined in IETF RFC 4302 to IETF RFC 4309.</p> <p>Related NIST SP 800-53 rev4 Security Control: SC-8.</p>
<b>Verification</b>	Test, Document Inspection

**IPv4**

<b>Identifier</b>	SWIM-TIYP-0003
<b>Title</b>	IPv4
<b>Statement</b>	The Network Interface Binding <b>shall</b> support IETF RFC 791 (Internet Protocol v4).
<b>Clarification</b>	<p>This requirement mandates the use of IETF RFC 791 (Internet Protocol v4).</p> <p>+ IETF RFC 791 (Internet Protocol v4): <a href="http://tools.ietf.org/html/rfc791">http://tools.ietf.org/html/rfc791</a></p>
<b>Verification</b>	Test, Configuration Inspection

**IPv6**

<b>Identifier</b>	SWIM-TIYP-0004
<b>Title</b>	IPv6
<b>Statement</b>	The Network Interface Binding <b>shall</b> support IETF RFC 2460 (Internet Protocol v6).
<b>Clarification</b>	<p>This requirement mandates the use of IETF RFC 2460 (Internet Protocol v6).</p> <p>+ IETF RFC 2460 (Internet Protocol v6): <a href="http://tools.ietf.org/html/rfc2460">http://tools.ietf.org/html/rfc2460</a></p>
<b>Verification</b>	Test, Configuration Inspection

**TLS**

<b>Identifier</b>	SWIM-TIYP-0005
<b>Title</b>	TLS

<b>Statement</b>	The Service Interface Binding <b>shall</b> support the following versions of the Transport Layer Security Protocol (TLS): + IETF RFC 4346 (TLS v1.1) + IETF RFC 5246 (TLS v1.2)
<b>Clarification</b>	TLS is a widespread protocol to secure communications at the transport layer. + IETF RFC 4346 (TLS v1.1): <a href="http://tools.ietf.org/html/rfc4346">http://tools.ietf.org/html/rfc4346</a> + IETF RFC 5246 (TLS v1.2): <a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> Related NIST SP 800-53 rev4 Security Control: SC-8.
<b>Verification</b>	Test, Configuration Inspection

## HTTP

<b>Identifier</b>	SWIM-TIYP-0006
<b>Title</b>	HTTP
<b>Statement</b>	The Service Interface Binding <b>shall</b> support HTTP/1.1.
<b>Clarification</b>	This requirement specifies the use of the HTTP/1.1 protocol. HTTP/1.1 is defined across 7 IETF RFCs spanning from RFC 7230 to RFC 7237. + IETF RFC 7230: <a href="http://tools.ietf.org/html/rfc7230">http://tools.ietf.org/html/rfc7230</a> ... + IETF RFC 7237: <a href="http://tools.ietf.org/html/rfc7237">http://tools.ietf.org/html/rfc7237</a>
<b>Verification</b>	Test, Configuration Inspection

## HTTP over TLS

<b>Identifier</b>	SWIM-TIYP-0007
<b>Title</b>	HTTP over TLS
<b>Statement</b>	The Service Interface Binding <b>shall</b> comply with IETF RFC 2818 (HTTP over TLS).
<b>Clarification</b>	This requirement mandates compliance with the interoperability standard for the use of HTTP over TLS (HTTPS). + IETF RFC 2818 (HTTP over TLS): <a href="http://tools.ietf.org/html/rfc2818">http://tools.ietf.org/html/rfc2818</a> Related NIST SP 800-53 rev4 Security Control: SC-8.
<b>Verification</b>	Test, Configuration Inspection

## SOAP

<b>Identifier</b>	SWIM-TIYP-0008
<b>Title</b>	SOAP
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the following versions of SOAP: + SOAP 1.1 + SOAP 1.2.

<b>Clarification</b>	Service Providers that use an Interface Binding that uses SOAP has to support versions 1.1 and 1.2. + Simple Object Access Protocol 1.1: <a href="http://www.w3.org/TR/2000/NOTE-SOAP-20000508/">http://www.w3.org/TR/2000/NOTE-SOAP-20000508/</a> + SOAP 1.2 Part 1: <a href="http://www.w3.org/TR/soap12-part1/">http://www.w3.org/TR/soap12-part1/</a> + SOAP 1.2 Part 2: <a href="http://www.w3.org/TR/2007/REC-soap12-part2-20070427/">http://www.w3.org/TR/2007/REC-soap12-part2-20070427/</a>
<b>Verification</b>	Test, Configuration Inspection

**MTOM**

<b>Identifier</b>	SWIM-TIYP-0009
<b>Title</b>	MTOM
<b>Statement</b>	The Service Interface Binding <b>should</b> support MTOM encoding for the following versions of SOAP: + SOAP 1.1 Binding for MTOM + SOAP 1.2 Binding for MTOM.
<b>Clarification</b>	Service Providers that use an Interface Binding that contains the Simple Access Protocol are recommended to support the Message Transmission Optimization Mechanism. + MTOM 1.0 Binding for SOAP 1.1: <a href="http://www.w3.org/Submission/soap11mtom10/">http://www.w3.org/Submission/soap11mtom10/</a> + MTOM 1.0 Binding for SOAP 1.2 <a href="http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/">http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/</a>
<b>Verification</b>	Test, Configuration Inspection

**WSDL**

<b>Identifier</b>	SWIM-TIYP-0010
<b>Title</b>	WSDL
<b>Statement</b>	The Service Interface Binding <b>shall</b> support at least one of the following versions of the Web Services Description Language (WSDL): + WSDL 1.1 + WSDL 2.0.

<b>Clarification</b>	This requirement specifies the accepted versions of the Web Service Description Language used to specify in a machine-process able manner a SOAP Web Service. + WSDL 1.1: <a href="http://www.w3.org/TR/wsdl">http://www.w3.org/TR/wsdl</a> + WSDL 1.1 SOAP 1.2 Binding: <a href="https://www.w3.org/Submission/wsdl11soap12/">https://www.w3.org/Submission/wsdl11soap12/</a> + WSDL 2.0 Part 1: <a href="http://www.w3.org/TR/wsdl20/">http://www.w3.org/TR/wsdl20/</a> + WSDL 2.0 Part 2: <a href="http://www.w3.org/TR/2007/REC-wsdl20-adjuncts-20070626/">http://www.w3.org/TR/2007/REC-wsdl20-adjuncts-20070626/</a> + WSDL 2.0 SOAP 1.1 Binding: <a href="http://www.w3.org/TR/wsdl20-soap11-binding/">http://www.w3.org/TR/wsdl20-soap11-binding/</a> Related NIST SP 800-53 rev4 Security Control: SI-10.
<b>Verification</b>	Test, Configuration Inspection

## WSI

<b>Identifier</b>	SWIM-TIYP-0011
<b>Title</b>	WSI
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the following version of the OASIS WSI Basic Profile: + WSI Basic Profile Version 1.2 + WSI Basic Profile Version 2.0.
<b>Clarification</b>	WSI Basic Profile consists of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability. It also contains a set of executable test assertions for assessing the conformance to the profile. + OASIS WSI Basic Profile Version 1.2: <a href="http://ws-i.org/profiles/basicprofile-1.2-2010-11-09.html">http://ws-i.org/profiles/basicprofile-1.2-2010-11-09.html</a> + OASIS WSI Basic Profile Version 2.0: <a href="http://ws-i.org/profiles/basicprofile-2.0-2010-11-09.html">http://ws-i.org/profiles/basicprofile-2.0-2010-11-09.html</a>
<b>Verification</b>	Test, Configuration Inspection

## WS-I Security

<b>Identifier</b>	SWIM-TIYP-0012
<b>Title</b>	WS-I Security
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the OASIS WS-I Basic Security Profile 1.1.
<b>Clarification</b>	To enable interoperability for SOAP Web Services using WS-Security it is required to satisfy the OASIS WS-I Basic Security Profile 1.1. + OASIS WS-I Basic Security Profile 1.1: <a href="http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1">http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1</a> Related NIST SP 800-53 rev4 Security Control: SC-8 (1).
<b>Verification</b>	Test, Configuration Inspection

## WS Notification

<b>Identifier</b>	SWIM-TIYP-0013
<b>Title</b>	WS Notification
<b>Statement</b>	The Service Interface Binding <b>shall</b> support OASIS Web Services Notification 1.3.
<b>Clarification</b>	WS-Notification is a family of related specifications that define a standard Web services approach to notification using a topic-based publish/subscribe pattern. + OASIS Web Services Base Notification 1.3: <a href="http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.htm">http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.htm</a> + OASIS Web Services Brokered Notification 1.3: <a href="http://docs.oasis-open.org/wsn/wsn-ws_brokered_notification-1.3-spec-os.pdf">http://docs.oasis-open.org/wsn/wsn-ws_brokered_notification-1.3-spec-os.pdf</a> + OASIS Web Services Topics 1.3: <a href="http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf">http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf</a>
<b>Verification</b>	Test, Configuration Inspection

### IPv6 Node Requirements

<b>Identifier</b>	SWIM-TIYP-0014
<b>Title</b>	IPv6 Node Requirements
<b>Statement</b>	The Network Interface Binding <b>shall</b> support IETF RFC 6434 (IPv6 Node Requirements).
<b>Clarification</b>	This requirement mandates the support of IETF RFC 6434 (IPv6 Node Requirements). + IETF RFC 6434 (IPv6 Node Requirements): <a href="http://tools.ietf.org/html/rfc6434">http://tools.ietf.org/html/rfc6434</a>
<b>Verification</b>	Test, Configuration Inspection

### RFC 1122

<b>Identifier</b>	SWIM-TIYP-0015
<b>Title</b>	RFC 1122
<b>Statement</b>	The Network Interface Binding <b>shall</b> support IETF RFC 1122 (Internet Standard, Requirements for Internet Hosts- Communication Layers).
<b>Clarification</b>	This requirement mandates the use of IETF RFC 1122 Internet Standard, Requirements for Internet Hosts - Communication Layers. + IETF RFC 1122 Internet Standard, Requirements for Internet Hosts - Communication Layers: <a href="http://tools.ietf.org/html/rfc1122">http://tools.ietf.org/html/rfc1122</a>
<b>Verification</b>	Test, Configuration Inspection

### ICMP

<b>Identifier</b>	SWIM-TIYP-0016
<b>Title</b>	ICMP
<b>Statement</b>	The Network Interface Binding <b>shall</b> support the Internet Control Message Protocol

	(ICMP).
<b>Clarification</b>	This requirement mandates the use of IETF RFC 792 (Internet Control Message Protocol). + IETF RFC 792 (Internet Control Message Protocol): <a href="http://tools.ietf.org/html/rfc792">http://tools.ietf.org/html/rfc792</a> + IETF RFC 6918 (Formally Deprecating Some ICMPv4 Message Types): <a href="http://tools.ietf.org/html/rfc6918">http://tools.ietf.org/html/rfc6918</a>
<b>Verification</b>	Test, Configuration Inspection

## RFC 950

<b>Identifier</b>	SWIM-TIYP-0017
<b>Title</b>	RFC 950
<b>Statement</b>	The Network Interface Binding <b>shall</b> support IETF RFC 950 (Internet Standard Sub netting Procedure).
<b>Clarification</b>	This requirement mandates the use of IETF RFC 950 (Internet Standard Sub netting Procedure). + IETF RFC 950 (Internet Standard Sub netting Procedure): <a href="http://tools.ietf.org/html/rfc950">http://tools.ietf.org/html/rfc950</a>
<b>Verification</b>	Test, Configuration Inspection

## WS Policy

<b>Identifier</b>	SWIM-TIYP-0019
<b>Title</b>	WS Policy
<b>Statement</b>	The Service Interface Binding <b>may</b> include general service policies expressed using W3C Web Service Policy 1.5.
<b>Clarification</b>	Web Service Policy allows to express, using a formalised and machine-processable language, the capabilities and requirements of a Web Service. A Service Provider may choose to express the capabilities and requirements of a service using WS-Policy, where applicable this requirement complements the use of specific WS-Policy extensions like WS-SecurityPolicy or WS-ReliableMessagingPolicy to provide general purpose service policies. + W3C Web Service Policy 1.5 - Framework: <a href="https://www.w3.org/TR/2007/REC-ws-policy-20070904/">https://www.w3.org/TR/2007/REC-ws-policy-20070904/</a> + W3C Web Services Policy 1.5 - Attachment: <a href="http://www.w3.org/TR/ws-policy-attach/">http://www.w3.org/TR/ws-policy-attach/</a>
<b>Verification</b>	Test, Configuration Inspection

## WS Secure Conversation

<b>Identifier</b>	SWIM-TIYP-0020
<b>Title</b>	WS Secure Conversation
<b>Statement</b>	The Service Interface Binding <b>shall</b> support WS-SecureConversation 1.4.



<b>Clarification</b>	Establishment of a Security Session at message level through WS-SecureConversation helps reduce the performance overhead of message level security in case many messages are exchanged securely. Establishment of a Security Session at message level through WS-SecureConversation allows independence of equivalent transport level functionality. + OASIS Standard WS-SecureConversation 1.4: <a href="http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.html">http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.html</a> Related NIST SP 800-53 rev4 Security Control: SC-23.
<b>Verification</b>	Test, Configuration Inspection

### WS Trust

<b>Identifier</b>	SWIM-TIYP-0021
<b>Title</b>	WS Trust
<b>Statement</b>	The Service Interface Binding <b>shall</b> support WS-Trust 1.4.
<b>Clarification</b>	WS-Trust extends WS-Security providing a framework for requesting and issuing security tokens, and to broker trust relationships. + OASIS WS-Trust 1.4: <a href="http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html">http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html</a> Related NIST SP 800-53 rev4 Security Control: IA-4 (6).
<b>Verification</b>	Test, Configuration Inspection

### WS Addressing

<b>Identifier</b>	SWIM-TIYP-0022
<b>Title</b>	WS Addressing
<b>Statement</b>	The Service Interface Binding <b>shall</b> support WS-Addressing 1.0.
<b>Clarification</b>	WS-Addressing provides transport-neutral mechanisms to address Web services and messages. WS-Addressing enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner. + W3C Recommendation Web Services Addressing 1.0 - Core: <a href="https://www.w3.org/TR/2006/REC-ws-addr-core-20060509/">https://www.w3.org/TR/2006/REC-ws-addr-core-20060509/</a> + W3C Recommendation Web Services Addressing 1.0 - SOAP Binding: <a href="https://www.w3.org/TR/ws-addr-soap/">https://www.w3.org/TR/ws-addr-soap/</a>
<b>Verification</b>	Test, Configuration Inspection

### SOAP Message Security

<b>Identifier</b>	SWIM-TIYP-0023
<b>Title</b>	SOAP Message Security
<b>Statement</b>	The Service Interface Binding <b>shall</b> support OASIS Web Services Security SOAP Message Security 1.1.1.

<b>Clarification</b>	<p>To enable interoperability for SOAP Web Services using WS-Security it is required to satisfy the OASIS Web Services Security SOAP Message Security 1.1.1. A Service Interface Binding supporting OASIS WS-Security has to provide and be able to process a policy description using WS-SecurityPolicy. The WS-SecurityPolicy document is recommended to be included as an attachment to the WSDL of the service, as this promotes reusability of the policy.</p> <p>+ OASIS Web Services Security: SOAP Message Security Version 1.1.1:  <a href="http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html">http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html</a></p> <p>+ OASIS WS-SecurityPolicy 1.3: <a href="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html">http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html</a>  Related NIST SP 800-53 rev4 Security Control: SC-8 (1).</p>
<b>Verification</b>	Test, Configuration Inspection

### XML Encryption

<b>Identifier</b>	SWIM-TIYP-0024
<b>Title</b>	XML Encryption
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the W3C XML Encryption Syntax and Processing 1.1 if message confidentiality is needed.
<b>Clarification</b>	<p>XML Encryption and Processing provides the capability to encrypt XML messages, thus adding confidentiality at message level.</p> <p>+ XML Encryption Syntax and Processing 1.1: <a href="https://www.w3.org/TR/xmlenc-core1/">https://www.w3.org/TR/xmlenc-core1/</a>  Related NIST SP 800-53 rev4 Security Control: SC-8 (1).</p>
<b>Verification</b>	Test, Configuration Inspection

### XML Signatures

<b>Identifier</b>	SWIM-TIYP-0025
<b>Title</b>	XML Signatures
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the W3C XML Signature Syntax and Processing (Second Edition).
<b>Clarification</b>	<p>XML Signature Syntax and Processing provides the capability to sign XML messages, thus adding integrity and origin authentication at message level.</p> <p>+ XML Signature Syntax and Processing (Second Edition):  <a href="http://www.w3.org/TR/xmldsig-core/">http://www.w3.org/TR/xmldsig-core/</a>  Related NIST SP 800-53 rev4 Security Control: SC-8 (1).</p>
<b>Verification</b>	Test, Configuration Inspection

### XML

<b>Identifier</b>	SWIM-TIYP-0026
<b>Title</b>	XML

<b>Statement</b>	The Service Interface Binding <b>shall</b> support the Extensible Mark-up Language (XML) 1.0.
<b>Clarification</b>	This requirement specifies support for XML 1.0. + Extensible Mark-up Language (XML) 1.0 (Fifth Edition): <a href="https://www.w3.org/TR/2008/REC-xml-20081126/">https://www.w3.org/TR/2008/REC-xml-20081126/</a>
<b>Verification</b>	Test, Configuration Inspection

### WS Security Username Token

<b>Identifier</b>	SWIM-TIYP-0027
<b>Title</b>	WS Security Username Token
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the WS-Security Username Token Profile 1.1.
<b>Clarification</b>	This requirement specifies support for a username/password token to be used with WS-Security. + OASIS Web Services Security Username Token Profile 1.1: <a href="https://www.oasis-open.org/committees/download.php/13392/wss-v1.1-spec-pr-UsernameTokenProfile-01.htm">https://www.oasis-open.org/committees/download.php/13392/wss-v1.1-spec-pr-UsernameTokenProfile-01.htm</a> Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9.
<b>Verification</b>	Test, Configuration Inspection

### WS Security X509

<b>Identifier</b>	SWIM-TIYP-0028
<b>Title</b>	WS Security X509
<b>Statement</b>	The Service Interface Binding <b>shall</b> support one of the following versions of WS-Security X.509 Token Profile: + WS-Security X.509 Token Profile 1.0 + WS-Security X.509 Token Profile 1.1.1
<b>Clarification</b>	This requirement specifies support for a X.509 certificate token to be used with WS-Security, both versions are supported. Service Providers are free to choose which version of the X.509 Token Profile to use and have to document it in their respective WS-SecurityPolicy. + WS-Security X.509 Token Profile 1.0: <a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf</a> + WS-Security X.509 Token Profile 1.1.1: <a href="http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html">http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html</a> Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
<b>Verification</b>	Test, Configuration Inspection

### XML Schema Validation

<b>Identifier</b>	SWIM-TIYP-0029
-------------------	----------------

<b>Title</b>	XML Schema Validation
<b>Statement</b>	The Service Interface Binding <b>shall</b> support XML Schema validation.
<b>Clarification</b>	This requirement specifies the use of XML Schema Validation. Validation techniques allow to verify syntax and semantics of message payloads follow specified definitions of format and content. + XML Schema Part 1: <a href="https://www.w3.org/TR/2004/REC-xmlschema-1-20041028/">https://www.w3.org/TR/2004/REC-xmlschema-1-20041028/</a> + XML Schema Part 2: <a href="https://www.w3.org/TR/2004/REC-xmlschema-2-20041028/">https://www.w3.org/TR/2004/REC-xmlschema-2-20041028/</a> Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17, SI-10.
<b>Verification</b>	Test, Configuration Inspection

### HTTP Content Type Header

<b>Identifier</b>	SWIM-TIYP-0030
<b>Title</b>	HTTP Content Type Header
<b>Statement</b>	The Service Interface Binding <b>shall</b> use the HTTP <i>Content-Type</i> header to specify the Media Type.
<b>Clarification</b>	This requirement specifies the use of the Content-Type header of HTTP. Possible values include: + IANA registered Media Types + Protocol specific extensions + Vendor proprietary extensions. IANA registered Media Types: <a href="http://www.iana.org/assignments/media-types/media-types.xhtml">http://www.iana.org/assignments/media-types/media-types.xhtml</a>
<b>Verification</b>	Test, Configuration Inspection

### WS Federation

<b>Identifier</b>	SWIM-TIYP-0031
<b>Title</b>	WS Federation
<b>Statement</b>	The SWIM-TI Interface <b>shall</b> support WS-Federation 1.2
<b>Clarification</b>	WS-Federation framework builds on WS-Security, WS-Trust, and the WS-* family of specifications to provide an extensible mechanism for federation, allowing authorized access to resources across different security realms. + Web Services Federation Language (WS-Federation) Version 1.2: <a href="http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html">http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html</a> Related NIST SP 800-53 rev4 Security Control: IA-4 (6).
<b>Verification</b>	Test, Configuration Inspection

### WS Reliable Messaging

<b>Identifier</b>	SWIM-TIYP-0032
<b>Title</b>	WS Reliable Messaging

<b>Statement</b>	The Service Interface Binding <b>may</b> support WS-ReliableMessaging 1.2.
<b>Clarification</b>	<p>WS-ReliableMessaging allows reliable transfer of messages between nodes in the presence of software component, system, or network failures. The use of this WS specification is optional, a SWIM Service Provider has the freedom to utilize it for selected Service Interface Bindings. A Service Interface Binding supporting WS-ReliableMessaging has to provide and be able to process a policy description using WS-ReliableMessagingPolicy. The WS-ReliableMessagingPolicy document is recommended to be included as an attachment to the WSDL of the service, as this promotes reusability of the policy.</p> <p>+ OASIS Standard Web Services Reliable Messaging 1.2: <a href="https://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-os.html">https://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-os.html</a></p> <p>+ WS-ReliableMessaging Policy 1.2: <a href="http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-os.html">http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-os.html</a></p>
<b>Verification</b>	Test, Configuration Inspection

## AMQP

<b>Identifier</b>	SWIM-TIYP-0033
<b>Title</b>	AMQP
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the Advanced Message Queuing Protocol (AMQP) 1.0.
<b>Clarification</b>	<p>The Advanced Message Queuing Protocol (AMQP) 1.0 is an open internet protocol for business messaging. It defines a binary wire-level protocol that allows for the reliable exchange of business messages between two parties.</p> <p>+ ISO/IEC 19464:2014 Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification:  <a href="http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64955">http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64955</a></p>
<b>Verification</b>	Test, Configuration Inspection

## DNSSEC

<b>Identifier</b>	SWIM-TIYP-0034
<b>Title</b>	DNSSEC
<b>Statement</b>	The Network Interface Binding <b>may</b> support IETF RFC 4033 (DNSSEC).
<b>Clarification</b>	<p>This requirement mandates the support of IETF RFC 4033 (DNSSEC).</p> <p>+ IETF RFC 4033 (DNSSEC): <a href="http://tools.ietf.org/html/rfc4033">http://tools.ietf.org/html/rfc4033</a>  Related NIST SP 800-53 rev4 Security Control: SC-20, SC-21.</p>
<b>Verification</b>	Test, Configuration Inspection

## Satisfactory Bandwidth

<b>Identifier</b>	SWIM-TIYP-0035
-------------------	----------------

<b>Title</b>	Satisfactory Bandwidth
<b>Statement</b>	The Network Interface Binding <b>shall</b> support the bandwidth required by capacity management estimates.
<b>Clarification</b>	The network has to be able to support the capacity of the services it supports. Implementers are required to determine the throughput and implement the SWIM TI accordingly. Throughput can be described by specifying the number of messages, or amount of data, processed/transmitted during a particular time frame, taking into account certain processing considerations (e.g. encryption, compression). (e.g. 100 Mbps, or 10 messages per second having an avg. size of 1MB, with no compression )
<b>Verification</b>	Test, Analysis, Document Inspection

### AMQP Transport Security Authentication

<b>Identifier</b>	SWIM-TIYP-0036
<b>Title</b>	AMQP Transport Security Authentication
<b>Statement</b>	The Service Interface Binding <b>shall</b> support one of the following authentication methods: + TLS server authentication and SASL PLAIN + TLS mutual authentication and SASL ANONYMOUS + TLS mutual authentication and SASL PLAIN.
<b>Clarification</b>	This requirement specifies the supported authentication methods of the AMQP 1.0 Service Binding. Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
<b>Verification</b>	Test, Configuration Inspection

### HTTP Header Content Encoding

<b>Identifier</b>	SWIM-TIYP-0037
<b>Title</b>	HTTP Header Content Encoding
<b>Statement</b>	The Service Interface Binding <b>shall</b> use one of the following values of the HTTP header <i>Content-Encoding</i> if HTTP compression is needed: + deflate + gzip + exi
<b>Clarification</b>	HTTP compression performs on the fly compression. The compression can only be requested by the client. The server can ignore the request by the client and return non-compressed data if deemed appropriate. + DEFLATE Compressed Data Format Specification version 1.3: <a href="https://www.ietf.org/rfc/rfc1951.txt">https://www.ietf.org/rfc/rfc1951.txt</a> + GZIP File Format Specification 4.3: <a href="https://tools.ietf.org/html/rfc1952">https://tools.ietf.org/html/rfc1952</a> + Efficient XML Interchange (EXI) Format 1.0: <a href="http://www.w3.org/TR/2014/REC-exi-20140211/">http://www.w3.org/TR/2014/REC-exi-20140211/</a>
<b>Verification</b>	Test, Configuration Inspection

**HTTP Header Transfer Encoding**

<b>Identifier</b>	SWIM-TIYP-0038
<b>Title</b>	HTTP Header Transfer Encoding
<b>Statement</b>	The Service Interface Binding <b>shall</b> support the following values of the HTTP header <i>Transfer-Encoding</i> : + chunked
<b>Clarification</b>	The sender of a message may not know in advance the length of the message that will be sent. The HTTP/1.1 protocol provides for the mechanism to send the payload chunked.
<b>Verification</b>	Test, Configuration Inspection

**SOAP Message Signing**

<b>Identifier</b>	SWIM-TIYP-0039
<b>Title</b>	SOAP Message Signing
<b>Statement</b>	The SWIM-TI <b>shall</b> digitally sign SOAP messages.
<b>Clarification</b>	This requirement ensures integrity and data origin verification of the messages sent. Related NIST SP 800-53 rev4 Security Control: SC-8.
<b>Verification</b>	Test, Demonstration

**Data Compression**

<b>Identifier</b>	SWIM-TIYP-0040
<b>Title</b>	Data Compression
<b>Statement</b>	The Service Interface Binding <b>may</b> support data compression.
<b>Clarification</b>	The Service Interface Binding provides the possibility to transmit compressed data. Providers are free to choose if they want to implement it and for which data exchanges to use it.
<b>Verification</b>	Test, Demonstration

**TLS Authentication**

<b>Identifier</b>	SWIM-TIYP-0041
<b>Title</b>	TLS Authentication
<b>Statement</b>	The Service Interface Binding <b>shall</b> support one of the following authentication mechanisms for TLS: + Mutual authentication with X.509 certificates + Server authentication with X.509 and Client authentication with HTTP Basic or HTTP Digest.
<b>Clarification</b>	This requirement specifies the supported TLS authentication methods.

	Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
<b>Verification</b>	Test, Configuration Inspection

### HTTP Status Code Header

<b>Identifier</b>	SWIM-TIYP-0042
<b>Title</b>	HTTP Status Code Header
<b>Statement</b>	The Service Interface Binding <b>shall</b> be able to use the HTTP <i>Status-Code</i> header.
<b>Clarification</b>	This requirement specifies the need to use the Status-Code header of HTTP. The <i>Status-Code</i> rules and semantics are defined as part of the HTTP/1.1 specification. + IETF RFC 2616 (HTTP/1.1): <a href="http://tools.ietf.org/html/rfc2616">http://tools.ietf.org/html/rfc2616</a>
<b>Verification</b>	Test, Configuration Inspection

### HTTP Reason Phrase Header

<b>Identifier</b>	SWIM-TIYP-0043
<b>Title</b>	HTTP Reason Phrase Header
<b>Statement</b>	The Service Interface Binding <b>shall</b> be able to use the HTTP <i>Reason-Phrase</i> header.
<b>Clarification</b>	This requirement specifies the need to use of the Reason-Phrase header of HTTP. The <i>Reason-Phrase</i> rules and semantics are defined as part of the HTTP/1.1 specification. + IETF RFC 2616 (HTTP/1.1): <a href="http://tools.ietf.org/html/rfc2616">http://tools.ietf.org/html/rfc2616</a>
<b>Verification</b>	Test, Configuration Inspection

### HTTP POST

<b>Identifier</b>	SWIM-TIYP-0044
<b>Title</b>	HTTP POST
<b>Statement</b>	The Service Interface Binding <b>shall</b> use the following HTTP methods: + POST
<b>Clarification</b>	SOAP Web Services rely on HTTP's POST method.
<b>Verification</b>	Test, Configuration Inspection

### SOAP Encryption

<b>Identifier</b>	SWIM-TIYP-0045
<b>Title</b>	SOAP Encryption
<b>Statement</b>	The SWIM-TI <b>may</b> encrypt any combination of body blocks, header blocks and any of these sub-structures of a SOAP message.



<b>Clarification</b>	Message level encryption is able to ensure end-to-end confidentiality of the exchanged messages. Message encryption results in an inherent overhead (processing time and payload size) which needs to be taken into account and conflated with the confidentiality benefits that it provides. This requirement enables a Service Provider to use (if desired) message encryption of SOAP messages for part or the complete message. Related NIST SP 800-53 rev4 Security Control: SC-8.
<b>Verification</b>	Test, Demonstration

### WS Security Token Profiles

<b>Identifier</b>	SWIM-TIYP-0046
<b>Title</b>	WS Security Token Profiles
<b>Statement</b>	The Service Interface Binding <b>shall</b> support one of the following Token Profiles: + WS-Security X.509 Token Profile 1.0 + WS-Security X.509 Token Profile 1.1.1 + WS-Security SAML Token Profile 1.1.1
<b>Clarification</b>	This requirement specifies support for a X.509 certificate or SAML tokens to be used with WS-Security. Service Providers are free to select which Token Profile to use, it is worth noting that SAML Token Profile 1.1.1 allows for SAML 1.0 and SAML 2.0 tokens. + WS-Security X.509 Token Profile 1.0: <a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf</a> + WS-Security X.509 Token Profile 1.1.1: <a href="http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html">http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html</a> + WS-Security SAML Token Profile 1.1.1: <a href="http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SAMLTOKENProfile-v1.1.1.html">http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SAMLTOKENProfile-v1.1.1.html</a> Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
<b>Verification</b>	Test

### AMQP Content Type Header

<b>Identifier</b>	SWIM-TIYP-0047
<b>Title</b>	AMQP Content Type Header
<b>Statement</b>	The Service Interface Binding <b>shall</b> allow the use of the AMQP 1.0 <i>content-type</i> header to specify Media Type values.
<b>Clarification</b>	This requirement specifies the possible use of the content-type header of AMQP 1.0. Possible values include: + IANA registered Media Types + Protocol specific extensions + Vendor proprietary extensions. IANA registered Media Types: <a href="http://www.iana.org/assignments/media-types/media-types.xhtml">http://www.iana.org/assignments/media-types/media-types.xhtml</a>
<b>Verification</b>	Test

**AMQP Content Encoding Header**

<b>Identifier</b>	SWIM-TIYP-0048
<b>Title</b>	AMQP Content Encoding Header
<b>Statement</b>	The Service Interface Binding <b>shall</b> allow the use of the AMQP 1.0 <i>Content-Encoding</i> header to specify Media Type values.
<b>Clarification</b>	This requirement specifies the possible use of the content-encoding header of AMQP 1.0. Possible values include: + IANA registered Media Types + Protocol specific extensions + Vendor proprietary extensions. IANA registered Media Types: <a href="http://www.iana.org/assignments/media-types/media-types.xhtml">http://www.iana.org/assignments/media-types/media-types.xhtml</a>
<b>Verification</b>	Test

**TLS Mutual Authentication**

<b>Identifier</b>	SWIM-TIYP-0049
<b>Title</b>	TLS Mutual Authentication
<b>Statement</b>	The Service Interface Binding <b>shall</b> support one of the following authentication mechanisms for TLS: + Mutual authentication with X.509 certificates + Server authentication with X.509 certificate.
<b>Clarification</b>	This requirement specifies the supported authentication methods of Service Interface Bindings utilizing TLS and WS Username Token. Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
<b>Verification</b>	Test, Configuration Inspection

## 4. Profile Part Specifications

A Profile Part specification is a consistent grouping of technical infrastructure requirements. Contrary to the Interface Binding specification, the Profile Parts do not specify the interfaces between systems. The SWIM TI YP includes different Profile Part specifications that focus on different capabilities of a technical infrastructure. Profile parts do not share requirements with other Profile Parts.

### 4.1 Core Profile Part

This section contains the requirements that are included in the Core Profile Part specification.

#### 4.1.1 Messaging

##### Common Time Reference

<b>Identifier</b>	SWIM-TIYP-0069
<b>Title</b>	Common Time Reference
<b>Statement</b>	The SWIM-TI <b>shall</b> rely on a Common Time Reference (CTR) for time synchronisation.
<b>Clarification</b>	For the SWIM environment, each SWIM-TI function that uses time information must be synchronised to a time reference that satisfies precision requirements (e.g. a geographically close Stratum 2 or Stratum 1 time server).  For instance, security and identity tokens are checked for freshness in order to ensure that they are still within their valid lifetimes. Related NIST SP 800-53 rev4 Security Control: AU-8.
<b>Verification</b>	Test, Demonstration

##### Prioritise Use of COTS

<b>Identifier</b>	SWIM-TIYP-0082
<b>Title</b>	Prioritise Use of COTS
<b>Statement</b>	The SWIM-TI <b>shall</b> prioritise Commercial Off-The-Shelf (COTS) products for its implementation when these are suitable and available.
<b>Clarification</b>	Commercial Off-The-Shelf (COTS) products are prioritised as part of the SWIM-TI Standardisation for their combination of maturity, reliability, cost-effectiveness and suitability for the SWIM-TI scope.
<b>Verification</b>	Configuration Inspection

#### 4.1.2 Security

##### Overload Protection

<b>Identifier</b>	SWIM-TIYP-0050
<b>Title</b>	Overload Protection
<b>Statement</b>	The SWIM-TI <b>shall</b> provide overload protection mechanisms for its provided services.
<b>Clarification</b>	<p>This requirement prevents a single consumer from using all available resources, allowing other consumers requests to be processed.</p> <p>Due to the broad scope of uses applicable to the SWIM-TI Yellow Profile there is no single mechanism that can fit all implementations. Implementers are required to have some form of overload protection, the details of which are not specified to accommodate the different use cases.</p> <p>Common examples of such protection mechanisms include (from easier to implement to more sophisticated mechanisms):</p> <ul style="list-style-type: none"> <li>+ Limitation of the total number of requests each Service Consumer may be able to consume in certain time window</li> <li>+ Software firewalls</li> <li>+ Hardware solutions like routers and firewalls</li> </ul> <p>Related NIST SP 800-53 rev4 Security Control: SC-5 (1), AC-23.</p>
<b>Verification</b>	Test, Analysis

### Administrative Remote Encrypted Connection

<b>Identifier</b>	SWIM-TIYP-0053
<b>Title</b>	Encrypted Connections for Remote Administrative Access
<b>Statement</b>	The SWIM-TI <b>shall</b> use an encrypted connection if remote access to its administrative functionality is needed.
<b>Clarification</b>	<p>Remote connections from external networks (e.g. the Internet) might pose a security risk. This requirement ensures certain security controls such as using an encrypted virtual private network (VPN) and/or transport secured connections are present.</p> <p>Related NIST SP 800-53 rev4 Security Control: AC-17.</p>
<b>Verification</b>	Configuration Inspection

### Obscure Password Typing

<b>Identifier</b>	SWIM-TIYP-0054
<b>Title</b>	Obscure Password Typing
<b>Statement</b>	The SWIM-TI <b>shall</b> obscure screen typing feedback of passwords.

<b>Clarification</b>	<p>This requirement ensures that the feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms.</p> <p>This requirement prevents the threat often referred to as shoulder surfing, if the threat is not present (e.g. the system does not rely on passwords for authentication) or the risk is mitigated in other ways (e.g. physical security restrictions prevent shoulder surfing) the requirement can be considered satisfied.</p> <p>Related NIST SP 800-53 rev4 Security Control: IA-6.</p>
<b>Verification</b>	Demonstration

### Regulations Compliance

<b>Identifier</b>	SWIM-TIYP-0055
<b>Title</b>	Regulations Compliance
<b>Statement</b>	The SWIM-TI <b>shall</b> comply with applicable national and international regulations.
<b>Clarification</b>	<p>The SWIM-TI Yellow Profile Specification does not limit or circumvent in any way the satisfaction of any other applicable national or international regulations. Applicable regulations may include (but are not limited to) Information Technology systems, Electronic Communications or Air Traffic Management.</p> <p>Note: In the case of contradicting requirements between this specification and applicable regulations, regulatory requirements prevail.</p>
<b>Verification</b>	Document Inspection, Demonstration

### Role Based Access Control

<b>Identifier</b>	SWIM-TIYP-0058
<b>Title</b>	Role Based Access Control
<b>Statement</b>	The SWIM-TI <b>shall</b> support Role Based Access Control (RBAC).
<b>Clarification</b>	<p>Role based access control enables to provide access to a particular resource (e.g. service) based on the roles associated to an identity.</p> <p>Related NIST SP 800-53 rev4 Security Control: AC-3 (8).</p>
<b>Verification</b>	Test, Configuration Inspection

### Least Privileged Principle Access

<b>Identifier</b>	SWIM-TIYP-0059
-------------------	----------------

<b>Title</b>	Least Privileged Principle Access
<b>Statement</b>	The SWIM-TI <b>shall</b> rely on the principle of least privilege to grant access to its resources.
<b>Clarification</b>	Least privilege principle ensures that users and processes operate using privilege levels not higher than those necessary for the proper execution of their tasks. The principle of least privilege provides a first layer of mitigation against potential attacks by preventing access to critical functionality to users and processes that do not strictly require it for their normal operation. Related NIST SP 800-53 rev4 Security Control: AC-6, SC-3.
<b>Verification</b>	Demonstration, Analysis

### Automatic Sessions termination

<b>Identifier</b>	SWIM-TIYP-0060
<b>Title</b>	Automatic Sessions termination
<b>Statement</b>	The SWIM-TI <b>shall</b> terminate network connections associated to a communication session: + At the end of the session or, + After a configurable amount of idle time.
<b>Clarification</b>	Unneeded network connections are a source of potential security breaches, termination of such connections minimizes said risk.  Related NIST SP 800-53 rev4 Security Control: SC-10.
<b>Verification</b>	Test, Configuration Inspection

### Trusted Software

<b>Identifier</b>	SWIM-TIYP-0061
<b>Title</b>	Trusted Software
<b>Statement</b>	The SWIM-TI <b>shall</b> be composed of software components whose origin authenticity and integrity can be verified.
<b>Clarification</b>	This construction requirement guarantees integrity and authenticity of software used for the implementation of SWIM-TI components. Examples of mechanisms that can be used to verify the integrity include checksums and hash functions, cryptographic signatures can be used to verify authenticity. Related NIST SP 800-53 rev4 Security Control: SI-7.

<b>Verification</b>	Configuration Inspection
---------------------	--------------------------

### Verification of Signed Messages Integrity

<b>Identifier</b>	SWIM-TIYP-0063
<b>Title</b>	Verification of Signed Messages Integrity
<b>Statement</b>	The SWIM-TI <b>shall</b> verify, prior to any processing or data transformation, the integrity of cryptographically signed messages.
<b>Clarification</b>	Cryptographic message signature is used to verify the integrity of a message. This requirement ensures that the integrity of a signed message is verified before performing any processing or transformation on the message that could alter said integrity. Related NIST SP 800-53 rev4 Security Control: SC-8.
<b>Verification</b>	Test, Demonstration

### Message Protocol Validation

<b>Identifier</b>	SWIM-TIYP-0070
<b>Title</b>	Message Protocol Validation
<b>Statement</b>	The SWIM-TI <b>shall</b> ensure messages are valid against the protocol standards applicable to its Service Interface Bindings.
<b>Clarification</b>	This requirement ensures information passed through the SWIM-TI is validated against the different protocol standards composing the Interface Bindings. Related NIST SP 800-53 rev4 Security Control: SI-10.
<b>Verification</b>	Test, Demonstration, Analysis

### Message Payload Validation

<b>Identifier</b>	SWIM-TIYP-0071
<b>Title</b>	Message Payload Validation
<b>Statement</b>	The SWIM-TI <b>should</b> validate messages against the applicable message definitions of its Service Interface Bindings.
<b>Clarification</b>	This requirement ensures information passed through the SWIM-TI is validated against the message definitions required in the Service Interface Bindings. E.g. Validation against XML Schemas. Related NIST SP 800-53 rev4 Security Control: SI-10.

<b>Verification</b>	Test, Demonstration
---------------------	---------------------

### Retrieval of X.509 Certificates

<b>Identifier</b>	SWIM-TIYP-0093
<b>Title</b>	Retrieval of X.509 Certificates
<b>Statement</b>	The SWIM-TI <b>shall</b> retrieve X.509 certificates from a trusted Certificate Authority.
<b>Clarification</b>	The SWIM-TI relies on public key cryptographic certificates for several of its security capabilities. This requirement ensures that X.509 certificates are retrieved from a trusted Certificate Authority. Related NIST SP 800-53 rev4 Security Control: SC-12, IA-5 (2), SC-17.
<b>Verification</b>	Test, Configuration Inspection

### Validation of X.509 Certificates

<b>Identifier</b>	SWIM-TIYP-0094
<b>Title</b>	Validation of X.509 Certificates
<b>Statement</b>	The SWIM-TI <b>shall</b> validate X.509 certificates using a trusted Certificate Authority part.
<b>Clarification</b>	The SWIM-TI relies on public key cryptographic certificates for several of its security capabilities. This requirement ensures that X.509 certificates are validated (e.g. they have not been revoked) using a trusted Certificate Authority. Related NIST SP 800-53 rev4 Security Control: SC-12, IA-5 (2), SC-17.
<b>Verification</b>	Test, Configuration Inspection

### ECRYPT Algorithms

<b>Identifier</b>	SWIM-TIYP-0099
<b>Title</b>	ECRYPT Algorithms
<b>Statement</b>	The SWIM-TI <b>shall</b> select cryptographic algorithms according to ECRYPT-CSA D5.2.



<b>Clarification</b>	<p>Selection of secure cryptographic algorithms is necessary to ensure the security attributes (confidentiality, integrity, authenticity...) of the data are not violated. ECRYPT-CSA D5.2 provides recommendations of algorithms suitable for current, future and legacy use as well as algorithms that must be avoided.</p> <p>ECRYPT-CSA D5.2 Algorithms, Key Size and Protocols Report:  <a href="http://www.ecrypt.eu.org/csa/documents/D5.2-AlgKeySizeProt-1.0.pdf">http://www.ecrypt.eu.org/csa/documents/D5.2-AlgKeySizeProt-1.0.pdf</a>          Related NIST SP 800-53 rev4 Security Control: IA-5 c, SC-13.</p>
<b>Verification</b>	Test, Configuration Inspection

### Strong Passwords

<b>Identifier</b>	SWIM-TIYP-0104
<b>Title</b>	Strong Passwords
<b>Statement</b>	The SWIM-TI <b>shall</b> enforce strong passwords selection when using username/password authentication for its consumer credentials.
<b>Clarification</b>	<p>The SWIM-TI can be used with Service Bindings that support Username/Password authentication. This requirement ensures that service consumers use passwords with a minimum strength which helps prevent unauthorized access to the provided services.</p> <p>The following are recommended practices that will ensure strong passwords are selected:</p> <ul style="list-style-type: none"> <li>+ Require a minimum length of 8 characters or an equivalent minimum entropy</li> <li>+ Allow (as a minimum) any ASCII character as part of the password character space</li> <li>+ Check passwords against dictionary of known common or weak passwords.</li> </ul> <p>The following are recommendations to avoid in the password ruleset as they typically result in weaker selection of passwords:</p> <ul style="list-style-type: none"> <li>+ Enforce character set combination rules</li> <li>+ Routine password expiration</li> <li>+ Knowledge-Based Authentication or password hinting.</li> </ul> <p>References: NIST Special Publication 800-63B "Digital Identity Guidelines, Authentication and Lifecycle Management" - <a href="https://pages.nist.gov/800-63-3/sp800-63b.html">https://pages.nist.gov/800-63-3/sp800-63b.html</a>          Related NIST SP 800-53 rev4 Security Control: IA-5(4).</p>
<b>Verification</b>	Demonstration

### Audit of Failed Authentication Request

<b>Identifier</b>	SWIM-TIYP-0106
-------------------	----------------

<b>Title</b>	Audit of Failed Authentication Request
<b>Statement</b>	The SWIM-TI <b>shall</b> detect and record failed authentication attempts.
<b>Clarification</b>	Failed authentications may indicate an ongoing authentication attack against some of the user credentials in the system. Such attempts need to be detected and recorded for monitoring and security purposes. Related NIST SP 800-53 rev4 Security Control: AC-7 a, AU-2 a, SI-4a.2, SI-4b.
<b>Verification</b>	Demonstration, Test

### Access Control Restriction

<b>Identifier</b>	SWIM-TIYP-0107
<b>Title</b>	Access Control Restriction
<b>Statement</b>	The SWIM-TI <b>shall</b> restrict access to entities that surpass a configurable number of failed authentication attempts.
<b>Clarification</b>	Consecutive failed authentication attempts can be symptomatic of an ongoing attack to the system or its user's accounts, this requirement ensures that the SWIM-TI provides protection against these threats. Access restriction can take different forms depending on the severity and security context (e.g. delays next login prompt, locks user account for certain period or until manual release, indefinite ban of user credentials...). Related NIST SP 800-53 rev4 Security Control: AC-7.
<b>Verification</b>	Test, Demonstration, Configuration Inspection

### Satisfactory Authorization

<b>Identifier</b>	SWIM-TIYP-0108
<b>Title</b>	Satisfactory Authorization
<b>Statement</b>	The SWIM-TI <b>shall</b> allow a requesting entity to consume a service if and only if its authorization is successful.
<b>Clarification</b>	This requirement ensures that the SWIM Technical Infrastructure allows service consumption when (and only when) the requesting entity is authorized to consume it. It is assumed that access control to a public resource will not require an explicit authorization. Related NIST SP 800-53 rev4 Security Control: AC-3, AC-24.
<b>Verification</b>	Test, Demonstration, Configuration Inspection

**Mandatory Access Control**

<b>Identifier</b>	SWIM-TIYP-0110
<b>Title</b>	Mandatory Access Control
<b>Statement</b>	The SWIM-TI <b>shall</b> enforce access control to all of its resources.
<b>Clarification</b>	<p>The SWIM-TI Yellow Profile takes a proactive approach to access control where access control to any resource is enforced by default. This approach prevents unintended access to its resources.</p> <p>This requirement does not restrict in any way the existence of publicly accessible resources.</p> <p>Related NIST SP 800-53 rev4 Security Control: AC-3 (3).</p>
<b>Verification</b>	Test, Configuration Inspection

**Inactive Session Termination**

<b>Identifier</b>	SWIM-TIYP-0111
<b>Title</b>	Inactive Session Termination
<b>Statement</b>	The SWIM-TI <b>shall</b> terminate inactive sessions after a configurable amount of time.
<b>Clarification</b>	<p>This requirement addresses the termination of user-initiated logical sessions. A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organisational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.</p> <p>Related NIST SP 800-53 rev4 Security Control: AC-12.</p>
<b>Verification</b>	Test, Configuration Inspection

**Audit Data Access Control**

<b>Identifier</b>	SWIM-TIYP-0112
<b>Title</b>	Audit Data Access Control
<b>Statement</b>	The SWIM-TI <b>shall</b> restrict user access to audit data based on the principle of least privilege.
<b>Clarification</b>	<p>Audit data needs to be protected from unauthorized access.</p> <p>Related NIST SP 800-53 rev4 Security Control: AU-9</p>
<b>Verification</b>	Configuration Inspection

### Audit Data Reporting

<b>Identifier</b>	SWIM-TIYP-0114
<b>Title</b>	Audit Data Reporting
<b>Statement</b>	The SWIM-TI <b>shall</b> provide the means to analyse and produce reports of the collected audit data.
<b>Clarification</b>	It is important to monitor any incidents that may have an impact on security, to that effect the SWIM-TI has to provide the means to access recorded audit events to analyse them and produce appropriate reporting. Related NIST SP 800-53 rev4 Security Control: AU-7.
<b>Verification</b>	Demonstration

### Cryptography Key Sizes

<b>Identifier</b>	SWIM-TIYP-0120
<b>Title</b>	Cryptography Key Sizes
<b>Statement</b>	The SWIM-TI <b>should</b> select key sizes for the cryptographic algorithms used according to ECRYPT-CSA D5.2.
<b>Clarification</b>	Implementers of the SWIM-TI are recommended to adhere to ECRYPT-CSA D5.2 report for the key size selection on the cryptographic algorithms used. ECRYPT-CSA D5.2 Algorithms, Key Size and Protocols Report: <a href="http://www.ecrypt.eu.org/csa/documents/D5.2-AlgKeySizeProt-1.0.pdf">http://www.ecrypt.eu.org/csa/documents/D5.2-AlgKeySizeProt-1.0.pdf</a>
<b>Verification</b>	Test, Demonstration

### Cryptographic Key Life-cycle Management

<b>Identifier</b>	SWIM-TIYP-0121
<b>Title</b>	Cryptographic Key Life-cycle Management
<b>Statement</b>	The SWIM-TI <b>shall</b> manage the life-cycle of its cryptographic keys in accordance to NIST SP 800-57.
<b>Clarification</b>	Proper management of cryptographic keys during the entirety of their life-cycle is necessary to ensure the expected security levels of a cryptographic system. NIST Special Publication 800-57 rev. 4 Part 1 "Recommendation for Key Management Part 1: General": <a href="http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf">http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf</a> Related NIST SP 800-53 rev4 Security Control: SC-12.

<b>Verification</b>	Test, Demonstration
---------------------	---------------------

### Non-recoverable Password Storage

<b>Identifier</b>	SWIM-TIYP-0122
<b>Title</b>	Non-recoverable Password Storage
<b>Statement</b>	The SWIM-TI <b>shall</b> store passwords in a non-recoverable manner.
<b>Clarification</b>	<p>Storing passwords in a recoverable manner is potentially insecure against malicious intrusions and various kinds of attacks including; brute force, dictionary attacks and rainbow tables.</p> <p>A simple and proven mechanism to ensure passwords are non-recoverable is to store them after:</p> <ol style="list-style-type: none"> <li>1. Appending a (pseudo)-random salt</li> <li>2. Hashing the salted password.</li> </ol> <p>For additional protection against brute force attacks key stretching mechanism can be used.</p> <p>Related NIST SP 800-53 rev4 Security Control: IA-5 h.</p>
<b>Verification</b>	Test, Demonstration

## 4.1.3 Monitoring

### Hardware Monitoring

<b>Identifier</b>	SWIM-TIYP-0101
<b>Title</b>	Hardware Monitoring
<b>Statement</b>	The SWIM-TI <b>shall</b> monitor the state of its hardware resources, including: <ul style="list-style-type: none"> <li>+ Processors</li> <li>+ Volatile and Non-Volatile memory</li> <li>+ Communication resources.</li> </ul>
<b>Clarification</b>	<p>The SWIM-TI relies on certain hardware resources to perform its operation. Monitoring of these resources ensures that their state is known and maintained up to date and that any eventual threshold violations on their use can be identified to be handled in an appropriate manner.</p> <p>Related NIST SP 800-53 rev4 Security Control: AU-2 a.</p>
<b>Verification</b>	Test, Configuration Inspection

### Monitoring Alerts

<b>Identifier</b>	SWIM-TIYP-0103
-------------------	----------------

<b>Title</b>	Monitoring Alerts
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to raise an alert when a threshold violation occurs.
<b>Clarification</b>	Threshold violations may require intervention from a supervisor or system administrators. This requirement ensures an alert mechanism is provided. Related NIST SP 800-53 rev4 Security Control: <FILL>
<b>Verification</b>	Test, Configuration Inspection

#### 4.1.4 Performance Efficiency

##### Satisfactory Throughput

<b>Identifier</b>	SWIM-TIYP-0051
<b>Title</b>	Satisfactory Throughput
<b>Statement</b>	The SWIM-TI <b>shall</b> support a maximum throughput as required by capacity management estimates.
<b>Clarification</b>	The SWIM-TI implementation has to be able to support the capacity plan of the services it provides. Implementers are required to determine the throughput and implement the SWIM TI accordingly. Throughput can be described by specifying the number of messages, or amount of data, processed/transmitted during a particular time frame, taking into account certain processing considerations (e.g. encryption, compression). For example: 100 Mbps, with no compression and no encryption.
<b>Verification</b>	Test, Analysis, Document Inspection

##### Satisfactory Transit Time

<b>Identifier</b>	SWIM-TIYP-0081
<b>Title</b>	Satisfactory Transit Time
<b>Statement</b>	The SWIM-TI <b>shall</b> support a transit time as required by capacity management estimates.
<b>Clarification</b>	The SWIM-TI implementation is required to support a transit time appropriate to the services it supports as collected in a capacity management plan. Transit time should be specific to messages traversing the TI and exclude the influence of external factors such as network. It should also exclude session set up time, or any other additional manipulations such as compression or message level encryption. It is typically expressed as the time it takes the majority of messages to transit (e.g. 95% of messages take less than 0.5 s).

<b>Verification</b>	Test, Analysis, Document Inspection
---------------------	-------------------------------------

## 4.1.5 Reliability

### Satisfactory Availability

<b>Identifier</b>	SWIM-TIYP-0066
<b>Title</b>	Satisfactory Availability
<b>Statement</b>	The SWIM-TI <b>shall</b> be available as required in documented system availability objectives.
<b>Clarification</b>	The SWIM-TI implementation has to be able to support the availability required by the services it supports. Implementers are required to determine the required availability and implement the SWIM TI accordingly. Availability can be described by specifying the percentage of time the system is available, including/excluding planned and unplanned downtime depending on the availability objectives supported.
<b>Verification</b>	Test, Analysis, Document Inspection

## 4.2 Extended Profile Part

This section contains the requirements that are included in the Extended Profile Part specification.

### 4.2.1 Messaging

#### Content Based Routing

<b>Identifier</b>	SWIM-TIYP-0072
<b>Title</b>	Content Based Routing
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to route messages based on the content of the message.
<b>Clarification</b>	Content based routing provides the ability to determine the destination endpoint(s) of a message based on the evaluation of certain predicates against the content of a message.
<b>Verification</b>	Test, Demonstration

#### Subject Based Routing

<b>Identifier</b>	SWIM-TIYP-0073
<b>Title</b>	Subject Based Routing

<b>Statement</b>	The SWIM-TI <b>shall</b> be able to route messages based on the subject or header of the message.
<b>Clarification</b>	Subject or header based routing provides the ability to determine the destination endpoint(s) of a message based on the evaluation of certain predicates against the subject or header of a message.
<b>Verification</b>	Test, Demonstration

### Context Based Routing

<b>Identifier</b>	SWIM-TIYP-0074
<b>Title</b>	Context Based Routing
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to route messages based on the context of the message.
<b>Clarification</b>	Context based routing provides the ability to determine the destination endpoint(s) of a message based on the evaluation of certain predicates against the context of a message (e.g. delivery to alternative endpoints in case of multiple failed deliveries).
<b>Verification</b>	Test, Demonstration

### Automatic Retries

<b>Identifier</b>	SWIM-TIYP-0075
<b>Title</b>	Automatic Retries
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to perform a configurable number of automatic retries.
<b>Clarification</b>	Automatic retries provide certain resilience against deprecation of network communications and transparency during failover. Configurable aspects include the number of retries and the non-response time that triggers the next retry.
<b>Verification</b>	Test, Demonstration

### Configurable Routing

<b>Identifier</b>	SWIM-TIYP-0076
<b>Title</b>	Configurable Routing
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to select in a configurable manner the routing mechanism to be used for each message exchange.



<b>Clarification</b>	Not all information exchanges through the SWIM-TI need the same routing mechanisms. This requirement ensures that the SWIM-TI has the capability to configure the most adequate routing mechanism for service.
<b>Verification</b>	Test, Configuration Inspection

### Durable Subscriptions

<b>Identifier</b>	SWIM-TIYP-0077
<b>Title</b>	Durable Subscriptions
<b>Statement</b>	The SWIM-TI <b>shall</b> support durable subscriptions when the Publish/Subscribe MEP is used.
<b>Clarification</b>	<p>A durable subscription mechanism saves messages for an inactive subscriber and after the disconnected period, it delivers these saved messages when the subscriber is reconnected. This ensures a subscriber will not lose any messages which are published while it was disconnected. Note that this has no effect on the behaviour of the subscriber or the messaging system while the subscriber is connected, a connected subscriber acts the same whether its subscription is durable or non-durable.</p> <p>Some typical use cases for durable subscriptions include:</p> <ul style="list-style-type: none"> <li>+ restart of publisher without requiring subscribers to re-subscribe;</li> <li>+ restart of a subscriber without re-subscription to avoid multiple subscriptions.</li> </ul> <p>Subscriptions and messages have typically lifetime duration restrictions. In that case, the durable subscriptions mechanisms should take them into account.</p>
<b>Verification</b>	Test, Demonstration

### Traffic Prioritisation

<b>Identifier</b>	SWIM-TIYP-0078
<b>Title</b>	Traffic Prioritisation
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to prioritise between different types of traffic.
<b>Clarification</b>	This requirement enables the coexistence of different kinds of traffic and services with different priorities without lower priority traffic throttling.
<b>Verification</b>	Test, Demonstration

## 4.2.2 Monitoring

### Service Monitoring

<b>Identifier</b>	SWIM-TIYP-0100
<b>Title</b>	Service Monitoring
<b>Statement</b>	The SWIM-TI <b>shall</b> monitor the state of the services it supports.
<b>Clarification</b>	The SWIM-TI is used for the provision of certain services. Monitoring of these services ensures that their state is known and maintained up to date and that any eventual threshold violations on their use can be identified to be handled in an appropriate manner. Related NIST SP 800-53 rev4 Security Control: AU-2 a.
<b>Verification</b>	Test, Configuration Inspection

### Persistent Storage Recording

<b>Identifier</b>	SWIM-TIYP-0102
<b>Title</b>	Persistent Storage Recording
<b>Statement</b>	The SWIM-TI <b>shall</b> log in persistent storage threshold violations of the monitored resources and services.
<b>Clarification</b>	Collected logs can be used to provide reports, analyse system performance, analyse errors or investigate security incidents. Persistent storage is considered any kind of storage which is able to retain data after a power loss (e.g. Hard Drives, Solid State Drives, magnetic tapes...). Related NIST SP 800-53 rev4 Security Control: AU-11.
<b>Verification</b>	Test, Configuration Inspection

### Log Retention

<b>Identifier</b>	SWIM-TIYP-0119
<b>Title</b>	Log Retention
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to retain for a configurable number of days the collected logs.
<b>Clarification</b>	Collected logs can be used to provide reports, analyse system performance, analyse errors or investigate security incidents. The SWIM-TI is required to retain them for a non-specified number of days which can be configured to fit implementation needs. Related NIST SP 800-53 rev4 Security Control: AU-11.
<b>Verification</b>	Test, Configuration Inspection

### 4.2.3 Reliability

#### Replication Transparency

<b>Identifier</b>	SWIM-TIYP-0067
<b>Title</b>	Replication Transparency
<b>Statement</b>	The SWIM-TI <b>shall</b> provide replication transparency to its consumers.
<b>Clarification</b>	Replication transparency ensures that the multiple instances of the elements of a system or service that provides high availability are invisible to its consumers. Examples of elements under the scope of this specification for which replication transparency is applicable include brokers and endpoints. Related NIST SP 800-53 rev4 Security Control: SI-13 (b).
<b>Verification</b>	Test, Demonstration

#### Failure Transparency

<b>Identifier</b>	SWIM-TIYP-0068
<b>Title</b>	Failure Transparency
<b>Statement</b>	The SWIM-TI <b>shall</b> provide failure transparency to its consumers in the case of a single replicated element failure.
<b>Clarification</b>	Failure transparency ensures that a system or service is able to mask to its consumers the failure of a replicated element and that possible recoveries are invisible to its consumers. Examples of elements under the scope of this specification for which failure transparency is applicable include brokers and endpoints. Related NIST SP 800-53 rev4 Security Control: SI-13 (b).
<b>Verification</b>	Test, Demonstration

#### Durable Subscription Persistency

<b>Identifier</b>	SWIM-TIYP-0079
<b>Title</b>	Subscription Persistency
<b>Statement</b>	The SWIM-TI <b>shall</b> provide persistency across reboot and crash of the durable subscription mechanism when the Publish/Subscribe MEP is used.
<b>Clarification</b>	This requirement ensures that the durable subscription mechanism is resilient against crashes or reboots of the entity managing the subscription. Subscription persistency provides efficiency and reliability benefits. It is generally more efficient to make the entity managing the push or the entity managing the pullpoint the one responsible for the message persistence, than to have both subscriber and publisher

	maintain a complex infrastructure to detect message loss and to allow for recuperation. Related NIST SP 800-53 rev4 Security Control: SC-24.
<b>Verification</b>	Test, Demonstration

### 4.3 Security+ Profile Part

This section contains the requirements that are included in the Security+ Profile Part specification.

#### Admin Console Notifications

<b>Identifier</b>	SWIM-TIYP-0052
<b>Title</b>	Admin Console Notifications
<b>Statement</b>	The SWIM-TI <b>shall</b> have an administration console that displays: + A notification message or banner that includes privacy and security notices + Date and time of last log-on.
<b>Clarification</b>	SWIM-TI provides different functions that need to be managed and tuned by the administrators via an administration console (HMI). Technical details of such consoles depend on implementation choices (e.g. shell or graphical interfaces) but each console shall guarantee a certain level of security and compliance with current regulations. This requirement ensures that SWIM-TI Administration Console offers some necessary notification to the user logging-in into the system Related NIST SP 800-53 rev4 Security Control: AC-8, AC-9.
<b>Verification</b>	Demonstration

#### Security Patching

<b>Identifier</b>	SWIM-TIYP-0062
<b>Title</b>	Security Patching
<b>Statement</b>	The SWIM-TI <b>shall</b> be the subject of a documented vulnerability patching process that mitigates known vulnerabilities within a predefined maximum timeframe.

<b>Clarification</b>	<p>Service provision in a potentially hostile environment, such as the Internet, needs a regular update of software to apply security patches.</p> <p>The longer a known vulnerability remains unpatched, the higher the risk of exploits. For some types of information higher assurance of the integrity is required.</p> <p>Security patching should be a documented activity that is performed with a well-defined maximum delay to minimize risks on the system. The criticality of the vulnerabilities and the complexity and criticality of the system should be factors to be considered.</p> <p>Related NIST SP 800-53 rev4 Security Control: SI-2.</p>
<b>Verification</b>	Document Inspection

### Vulnerability Assessment

<b>Identifier</b>	SWIM-TIYP-0064
<b>Title</b>	Vulnerability Assessment
<b>Statement</b>	The SWIM-TI <b>shall</b> be the subject of a documented yearly vulnerability assessment which includes penetration tests.
<b>Clarification</b>	<p>Service provision in a public environment needs to be protected against possible hostile attacks. A regular check of unprotected vulnerabilities helps mitigate said risk.</p> <p>The vulnerability assessment can be performed through self-assessment or via a third party, verifiable evidence of the vulnerability assessment has to exist for consumers and regulators.</p> <p>Related NIST SP 800-53 rev4 Security Control: CA-8, RA-5.</p>
<b>Verification</b>	Document Inspection

### Documentation of Cryptographic encryption methods

<b>Identifier</b>	SWIM-TIYP-0083
<b>Title</b>	Documentation of Cryptographic encryption methods
<b>Statement</b>	The SWIM-TI <b>shall</b> have associated documentation describing the cryptographic encryption methods supported.
<b>Clarification</b>	<p>The following aspects need to be documented for a given information exchange:</p> <ul style="list-style-type: none"> <li>+ Which parts of the payload have to be encrypted.</li> <li>+ Which encryption algorithm is used</li> <li>+ Key length</li> </ul> <p>SOAP based Web Services support the use of WS-SecurityPolicy which provides a formal and standardised language to detail these aspects.</p> <p>Related NIST SP 800-53 rev4 Security Control: SC-1.</p>

<b>Verification</b>	Document Inspection
---------------------	---------------------

### Data Origin Authentication

<b>Identifier</b>	SWIM-TIYP-0085
<b>Title</b>	Data Origin Authentication
<b>Statement</b>	The SWIM-TI <b>shall</b> ensure data origin authentication using cryptographic signatures.
<b>Clarification</b>	Information Origin Authentication enables to determine the source of information. The SWIM-TI supports data origin authentication in all of its Service Interface Bindings by means of cryptographic signature at transport or message levels but does not necessarily impose it for all of them (e.g. WS Light, WS SOAP). This requirement further restricts this freedom by mandating its use. For the aforementioned examples it suffices to configure the Service Interface Bindings with TLS mutual authentication. Related NIST SP 800-53 rev4 Security Control: IA-1, IA-9.
<b>Verification</b>	Test, Configuration Inspection

### Documentation of Cryptographic signature methods

<b>Identifier</b>	SWIM-TIYP-0086
<b>Title</b>	Documentation of Cryptographic signature methods
<b>Statement</b>	The SWIM-TI <b>shall</b> have associated documentation describing the cryptographic signature methods supported.

<b>Clarification</b>	<p>Information Origin Authentication enables to determine the source of information. The SWIM-TI should be flexible to use different cryptographic methods depending on the critically of information exchanged. The SWIM-TI is configurable to specify:</p> <ul style="list-style-type: none"> <li>+ If the digital signature is required</li> <li>+ Which signature scheme has to be used</li> </ul> <p>E.g. Message Authentication Code (MAC) for symmetric signing or private key digital signature for asymmetric signing based on public/private key pair (note that the symmetric signing does not fulfil non-repudiation needs because the shared secret used to sign the information is shared among several participants).</p> <ul style="list-style-type: none"> <li>+ The signing algorithm to be used</li> <li>+ Which key has to be used and in particular if it is a multipurpose or a dedicated one.</li> </ul> <p>SOAP based Web Services support the use of WS-SecurityPolicy which provides a formal and standardized language to detail these aspects.</p> <p>Related NIST SP 800-53 rev4 Security Control: SC-1.</p>
<b>Verification</b>	Document Inspection

### Identity and tokens documentation

<b>Identifier</b>	SWIM-TIYP-0088
<b>Title</b>	Identity and tokens documentation
<b>Statement</b>	The SWIM-TI <b>shall</b> have associated documentation describing the types of identities and security tokens supported for authentication.
<b>Clarification</b>	<p>Identity authentication should be documented providing information on how digital identities and security tokens are produced and the content included in these (information describing the entity or security claims). Authentication constraints should be described (e.g. maximum number of login attempts, password strength characteristics).</p> <p>SOAP based Web Services support the use of WS-SecurityPolicy which provides a formal and standardized language to detail these aspects.</p> <p>Related NIST SP 800-53 rev4 Security Control: IA-1.</p>
<b>Verification</b>	Document Inspection

### Audit of identity validity events

<b>Identifier</b>	SWIM-TIYP-0089
<b>Title</b>	Audit of identity validity events

<b>Statement</b>	The SWIM-TI <b>shall</b> detect and record identities whose access has been restricted with the relevant context information.
<b>Clarification</b>	Entities which have their access restricted to a service have to be logged for future auditing. Any additional context information that may be relevant needs to be included. Related NIST SP 800-53 rev4 Security Control: AU-2.
<b>Verification</b>	Demonstration, Test

### Protection of information at rest

<b>Identifier</b>	SWIM-TIYP-0092
<b>Title</b>	Protection of information at rest
<b>Statement</b>	The SWIM-TI <b>shall</b> cryptographically secure the stored sensitive data.
<b>Clarification</b>	The SWIM-TI may be used to exchange potentially sensitive data whose confidentiality and/or integrity needs to be protected. This data could reside in local storage where it could be accessible to eavesdroppers. This requirement ensures the SWIM-TI supports the necessary means to secure stored sensitive data. Related NIST SP 800-53 rev4 Security Control: SC-28.
<b>Verification</b>	Test, Configuration Inspection

### Protection of Audit Information

<b>Identifier</b>	SWIM-TIYP-0096
<b>Title</b>	Protection of Audit Information
<b>Statement</b>	The SWIM-TI <b>shall</b> store audit data in non-volatile secure storage.
<b>Clarification</b>	Audit logs includes all information needed to successfully audit information system activity, therefore audit logs and audit tools need to be protected from unauthorized access, modification, and deletion. This should be achieved applying both logical and physical protection of audit logs. Logical protection can be addressed by enforcing adequate access controls to audit logs, while physical protection is addressed by media protection controls and physical access control. Audit records will be store persistently until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. Related NIST SP 800-53 rev4 Security Control: AU-9, AU-11.
<b>Verification</b>	Demonstration



**Audit Data Remote Storage**

<b>Identifier</b>	SWIM-TIYP-0097
<b>Title</b>	Audit Data Remote Storage
<b>Statement</b>	The SWIM-TI <b>shall</b> replicate audit data in a different system from the system generating the audit data.
<b>Clarification</b>	This requirement helps to ensure that a compromise of the system does not also result in a compromise of the corresponding audit records. Related NIST SP 800-53 rev4 Security Control: AU-9 (2).
<b>Verification</b>	Demonstration

**Audit Data Management Reporting**

<b>Identifier</b>	SWIM-TIYP-0115
<b>Title</b>	Audit Data Management Reporting
<b>Statement</b>	The SWIM-TI <b>shall</b> provide an interface to manage audit reports.
<b>Clarification</b>	This requirement ensures that the SWIM-TI provides the functionality necessary to manage the report of auditable events. It is expected that some human interaction is needed for fulfilling these reports, the details of which are system specific and not specified by this requirement (e.g. review, analysis, annotation functionalities could be included as part of the audit interface). Related NIST SP 800-53 rev4 Security Control: AU-7
<b>Verification</b>	Demonstration

**Audit of Access Requests**

<b>Identifier</b>	SWIM-TIYP-0116
<b>Title</b>	Audit of Access Requests
<b>Statement</b>	The SWIM-TI <b>shall</b> detect and record access to its services and resources.
<b>Clarification</b>	Recording access to the SWIM-TI services and resources enables its future auditing. Related NIST SP 800-53 rev4 Security Control: AC-17 (1) and AU-2a and SI-4a.2.
<b>Verification</b>	Demonstration, Test

**Audit of Authentication Requests**

<b>Identifier</b>	SWIM-TIYP-0117
<b>Title</b>	Audit of Authentication Requests
<b>Statement</b>	The SWIM-TI <b>shall</b> detect and record authentication requests.
<b>Clarification</b>	Authentication requests are auditable events due to their impact on the security of a system. Related NIST SP 800-53 rev4 Security Control: AU-2.
<b>Verification</b>	Demonstration, Test

### Audit of Authorization Requests

<b>Identifier</b>	SWIM-TIYP-0118
<b>Title</b>	Audit of Authorization Requests
<b>Statement</b>	The SWIM-TI <b>shall</b> detect and record authorization requests.
<b>Clarification</b>	Authorization requests are auditable events due to their impact on the security of a system. Related NIST SP 800-53 rev4 Security Control: AU-2.
<b>Verification</b>	Demonstration, Test

## 4.4 Security+2 Profile Part

This section contains the requirements that are included in the Security+2 Profile Part specification.

### Safe Mode Operation

<b>Identifier</b>	SWIM-TIYP-0056
<b>Title</b>	Safe Mode Operation
<b>Statement</b>	When certain adverse conditions are met, the SWIM-TI <b>shall</b> support a safe mode of operation that prioritises mission critical functions.
<b>Clarification</b>	When mission critical and not critical services are supported by the TI, it is necessary that the TI is able to operate in a safe mode to prioritise mission critical functions during certain adverse conditions e.g. reduced communication bandwidth or limited computational resources. This requirement covers the following NIST security controls: CP-12.
<b>Verification</b>	Test, Demonstration

### Safe Mode Description

<b>Identifier</b>	SWIM-TIYP-0057
<b>Title</b>	Safe Mode Description
<b>Statement</b>	The SWIM-TI <b>shall</b> have associated documentation identifying the mission critical functions that comprise the safe mode of operation.
<b>Clarification</b>	When mission critical and not critical services are supported by the TI, it is necessary to tell them apart so that there can be a consequent allocation of resources during certain adverse conditions e.g. reduced communication bandwidth or limited computational resources. This requirement covers the following NIST security controls: CP-12.
<b>Verification</b>	Document Inspection

### Vulnerability Assessment by Third-Party

<b>Identifier</b>	SWIM-TIYP-0065
<b>Title</b>	Vulnerability Assessment by Third-Party
<b>Statement</b>	The SWIM-TI <b>shall</b> be the subject of a documented yearly vulnerability assessment including penetration tests, conducted by an independent organisation.
<b>Clarification</b>	The service provider shall perform a yearly vulnerability assessment including penetration testing. The assessment cannot be performed through a self-assessment and needs to be performed by an independent organisation. Verifiable evidence of the vulnerability assessment has to exist for consumers and regulators. Related NIST SP 800-53 rev4 Security Control: CA-8 (1), RA-5.
<b>Verification</b>	Document Inspection

### CAVP validated Cryptographic Modules

<b>Identifier</b>	SWIM-TIYP-0098
<b>Title</b>	CAVP approved Cryptographic Modules
<b>Statement</b>	The SWIM-TI <b>shall</b> use cryptographic modules approved by the Cryptographic Algorithm Validation Program (CAVP).

<b>Clarification</b>	<p>The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptographic modules including both hardware and software components. The FIPS 140 standard is subdivided into the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). The CAVP ensures cryptographic algorithm implementations are tested for the correct implementation of the selected algorithms.</p> <p>Satisfaction of this requirement is achieved using cryptographic algorithm implementations approved by the Cryptographic Algorithm Validation Program (CAVP).</p> <p>Cryptographic Algorithm Validation Program (CAVP):  <a href="http://csrc.nist.gov/groups/STM/cavp/index.html">http://csrc.nist.gov/groups/STM/cavp/index.html</a>  List of validated cryptographic algorithms:  <a href="http://csrc.nist.gov/groups/STM/cavp/validation.html">http://csrc.nist.gov/groups/STM/cavp/validation.html</a>  Related NIST SP 800-53 rev4 Security Control: SC-13.</p>
<b>Verification</b>	Configuration Inspection

### Audit of Cryptographic Events

<b>Identifier</b>	SWIM-TIYP-0084
<b>Title</b>	Audit of Cryptographic Events
<b>Statement</b>	The SWIM-TI <b>shall</b> detect and record uses of its cryptographic modules.
<b>Clarification</b>	<p>The SWIM-TI makes use of cryptographic modules for secure exchange, local storage as well as cryptographic signature and verification. Detecting and recording these events is necessary for auditing purposes.</p> <p>Related NIST SP 800-53 rev4 Security Control: AU-2.</p>
<b>Verification</b>	Demonstration, Test

### Configurable Authentication

<b>Identifier</b>	SWIM-TIYP-0087
<b>Title</b>	Configurable Authentication
<b>Statement</b>	The SWIM-TI <b>shall</b> be able to enforce different types of identity security tokens on a per service basis.

<b>Clarification</b>	Access control to services is enforced by the SWIM TI that authenticates requests. The SWIM TI has to be able to enforce the use of different identity security tokens on a per service basis according to their security needs. Related NIST SP 800-53 rev4 Security Control: IA-4.
<b>Verification</b>	Test, Configuration Inspection

### Audit of federated identity events

<b>Identifier</b>	SWIM-TIYP-0090
<b>Title</b>	Audit of federated identity events
<b>Statement</b>	When integrated with a federated identity management, the SWIM-TI <b>shall</b> detect and record updates received from external identity management systems related to restricted identities.
<b>Clarification</b>	The SWIM-TI manages updates related to the validity of identities received from external identity management systems and these are relevant for protecting the system from unauthorized access. Related NIST SP 800-53 rev4 Security Control: AU-2.
<b>Verification</b>	Demonstration, Test

### Security Assessment

<b>Identifier</b>	SWIM-TIYP-0091
<b>Title</b>	Security Assessment
<b>Statement</b>	The SWIM-TI <b>shall</b> be the subject of a security assessment that is regularly maintained
<b>Clarification</b>	A security assessment of a system is performed to identify improvements to current baseline allowing the implementation to be improved and mitigate security risks. Related NIST SP 800-53 rev4 Security Control: CA-2.
<b>Verification</b>	Document Inspection

### Denial of Service Protection

<b>Identifier</b>	SWIM-TIYP-0095
<b>Title</b>	Denial of Service Protection
<b>Statement</b>	The SWIM-TI <b>shall</b> provide defensive measures against Denial of Service attacks.

<b>Clarification</b>	<p>A variety of solutions exist to reduce the effects of Denial of Service (both DoS and DDoS).</p> <p>Examples include:</p> <ul style="list-style-type: none"> <li>+ Boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks.</li> <li>+ Increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.</li> <li>+ Content Delivery Networks.</li> </ul> <p>Related NIST SP 800-53 rev4 Security Control: SC-5.</p>
<b>Verification</b>	Test, Analysis

### Identity Validity Information Exchange

<b>Identifier</b>	SWIM-TIYP-0105
<b>Title</b>	Identity Validity Information Exchange
<b>Statement</b>	When integrated with a federated identity management, the SWIM-TI <b>shall</b> exchange information related to restricted identities.
<b>Clarification</b>	<p>Maintaining up to date the identity information and its validity is important for ensuring a properly controlled access to resources. When the management of identities is federated and external to the SWIM-TI, it should get up to date information and contribute with any information concerning the validity of an identity in the SWIM-TI domain. (E.g. blocked identities due to suspicious behaviour, certificate revocation lists).</p> <p>Related NIST SP 800-53 rev4 Security Control: IA-5(9).</p>
<b>Verification</b>	Demonstration, Test

### Attribute Based Access Control

<b>Identifier</b>	SWIM-TIYP-0109
<b>Title</b>	Attribute Based Access Control
<b>Statement</b>	The SWIM-TI <b>shall</b> support Attribute Based Access Control (ABAC).

<b>Clarification</b>	Attribute Based Access control is an access control paradigm where access to different resources is leveraged on the use of policies describing rules and conditions to access a resource based on its attributes. Implementers can rely on existing standards like XACML to benefit from a standardised and formal framework to establish their Attribute Based Access Control. Attribute Based Access Control generalises and OASIS extensible Access Control Mark-up Language 3.0: <a href="http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html">http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html</a> Related NIST SP 800-53 rev4 Security Control: AC-16.
<b>Verification</b>	Test, Configuration Inspection

### Hardware Tokens

<b>Identifier</b>	SWIM-TIYP-0113
<b>Title</b>	Hardware Tokens
<b>Statement</b>	The SWIM-TI <b>shall</b> support the use of hardware security tokens for authentication.
<b>Clarification</b>	For most critical services (e.g. services exchanging classified data) it is necessary to have a stronger authentication mechanism, hardware security tokens add additional layers of protection as they require physical access to the authenticator. Related NIST SP 800-53 rev4 Security Control: IA-5.
<b>Verification</b>	Demonstration

## ANNEX A – List of Contributors

This specification was prepared by EUROCONTROL with the assistance of the following subject matter experts:

Name	Organisation
Antonio Strano	LEONARDO
Dario Di Crescenzo	LEONARDO
Guillaume le Cam	GROUPE ADP
Harald Milchrahm	FREQUENTIS
Idalina Mendes Videira	EUROCONTROL NM
Laurent Macquet	DSNA
Luis Moreno	ENAI
Lukas Winkler	AUSTRO CONTROL
Maciej Dąbrowski	PANSA
Matteo Pace	ENAV
Mike Williamson	NATS
Oliver Schrempf	DFS
Sebastien Barbereau	EUROCONTROL NM
Yves Steyt	EUROCONTROL NM

**Table 5 – List of subject matter experts**