EUROCONTROL Specification for SWIM Technical Infrastructure (TI) Yellow Profile

Edition: 1.1
Edition date: 05 July 2020
Reference nr: EUROCONTROL-SPEC 170

SUPPORTING EUROPEAN AVIATION

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

EUROCONTROL

EUROCONTROL Specification for SWIM Technical Infrastructure (TI) Yellow Profile

DOCUMENT IDENTIFIER : EUROCONTROL-SPEC-170

Edition Number	**:**	**1.1**
Edition Date	**:**	**05/07/2020**
Status	**:**	**Released Issue**
Intended for	**:**	**General Public**
Category	**:**	**EUROCONTROL Specification**

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Specification for SWIM Technical Infrastructure (TI) Yellow Profile		
	Publication Reference:	SPEC-170
	ISBN Number:	978-2-87497-096-2
Document Identifier	**Edition Number:**	1.1
EUROCONTROL-SPEC-170	**Edition Date:**	05/07/2020

Abstract

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.

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	☐	General Public	☑	Intranet	☐
Draft	☐	EUROCONTROL	☐	Extranet	☐
Proposed Issue	☐	Restricted	☐	Internet (www.eurocontrol.int)	☑
Released Issue	☑				

DOCUMENT APPROVAL

AUTHORITY	NAME AND SIGNATURE	DATE
Director General	Eamonn BRENNAN	5th July 2020

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
1.0	01 December 2017	Released Issue	All
1.1	05 July 2020	Minor update following Community of Interest review and proposals	All

CONTENTS

DOCUMENT CHARACTERISTICS 2

DOCUMENT APPROVAL 3

DOCUMENT CHANGE RECORD 4

CONTENTS 5

LIST OF FIGURES 7

LIST OF TABLES 8

EXECUTIVE SUMMARY 9

1. Introduction 10
   - 1.1 Purpose 10
   - 1.2 Scope 10
   - 1.3 Applicability 10
   - 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

2. Conformance 20
   - 2.1 Interface Binding Conformance 20
   - 2.2 Infrastructure Capabilities Conformance 21

3. Interface Binding Specifications 22
   - 3.1 Interface Bindings Catalogue 22
     - 3.1.1 Service Interface Bindings 22
       - 3.1.1.1 WS Light 24
       - 3.1.1.2 WS SOAP 24
       - 3.1.1.3 WS SOAP with Basic Message Security 25
       - 3.1.1.4 WS SOAP with Message Security 25
       - 3.1.1.5 WS SOAP with Federated Security 26
       - 3.1.1.6 WS-N SOAP 27
       - 3.1.1.7 WS-N SOAP with Basic Message Security 28
       - 3.1.1.8 WS-N SOAP with Message Security 28
       - 3.1.1.9 WS-N SOAP with Federated Security 29
       - 3.1.1.10 AMQP Messaging 30
     - 3.1.2 Network Interface Bindings 30
       - 3.1.2.1 IPv4 Unicast 31
       - 3.1.2.2 IPv4 Secure Unicast 31

3.1.2.3 IPv6 Unicast 31
3.1.2.4 IPv6 Secure Unicast 32
3.2 Interface Binding Requirements 33

4. Infrastructure Capabilities Specification 50
4.1 Security 50
4.2 Messaging 66
4.3 Monitoring 68
4.4 Reliability 70

ANNEX A – Conformity Checklist 72
A.1 Conformity with Interface Bindings 72
A.2 Conformity with Infrastructure Capabilities 73

ANNEX B – List of Contributors 75

ANNEX C – Specification Update Procedures 76

LIST OF FIGURES

Figure 1 – Interface Binding Conformance Overview..... 20

LIST OF TABLES

Table 1 – Requirement structure 12
Table 2 – List of abbreviations 14
Table 3 – List of terms with definition 17
Table 4 – Service Interface Bindings Overview 23
Table 5 – WS Light Service Interface Binding 24
Table 6 – WS SOAP Service Interface Binding 24
Table 7 – WS SOAP with Basic Message Security Service Interface Binding 25
Table 8 – WS SOAP with Message Security Service Interface Binding 26
Table 9 – WS SOAP with Federated Security Service Interface Binding 27
Table 10 – WS-N SOAP Service Interface Binding 27
Table 11 – WS-N SOAP with Basic Message Security Service Interface Binding 28
Table 12 – WS-N SOAP with Message Security Service Interface Binding 29
Table 13 – WS-N SOAP with Federated Security Service Interface Binding 30
Table 14 – AMQP Messaging Service Interface Binding 30
Table 15 – Network Interface Bindings Overview 30
Table 16 – IPv4 Unicast Network Interface Binding 31
Table 17 – IPv4 Secure Unicast Network Interface Binding 31
Table 18 – IPv6 Unicast Network Interface Binding 31
Table 19 – IPv6 Secure Unicast Network Interface Binding 32
Table 20 – Level of implementation 72
Table 21 – Conformity checklist 74
Table 22 – List of subject matter experts 75

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 Interface Binding Specifications; and
- 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 Infrastructure Capabilities 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[1])
    - 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; and
    - Recording: Ensuring that security-related events are recorded for real-time or deferred analysis;
3. Monitoring (of infrastructure components and services); and
4. 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)[2], and Service Registry[3].

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:

[1] Security requirements are traced to NIST SP 800-53 rev4 that enables traceability to ISO/IEC 27001:2013. NIST SP 800-53 has been chosen as the main reference in this specification as it provides a system-oriented point of view for security controls.

[2] PKI and STI were addressed in SESAR as part of the SWIM TI Identity Management Technical Specifications.

[3] The Runtime Service Registry (a specialised service registry that interfaces with systems) was initially addressed in SESAR and the definition work continued in SESAR 2020.

1. aeronautical information exchange;
2. meteorological information exchange;
3. cooperative network information exchange; and
4. 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 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[4].

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; or
- 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. This audience includes:
  - business experts procuring systems and services; and
  - technical experts designing and implementing systems and services.
- oversight authorities.

1.5 Conventions

The following conventions are used in this EUROCONTROL specification:

- '**shall**'- indicates a requirement that must be implemented to provide conformity with this specification;
- '**should**' - indicates a requirement that is recommended to achieve the best possible implementation of this specification; and
- '**may**' - indicates an option.

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

Identifier	Unique identifier of the requirement.
Title	Title of the requirement, used as a short name for the requirement for mnemonic and readability purposes.
Statement	Statement expressing the requirement.
Clarification	Additional information providing the rationale, a particular interpretation of the requirement, a reference to similar requirements,

[4] 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.

	as well as an example or any other description that facilitates understanding of the requirement.
Verification	Providing an indication of the methods that can be used to verify the proper satisfaction of the requirement. The following verification methods are used: 1) Document Inspection (information describing the infrastructure is analysed to assess proper compliance with a requirement) 2) Configuration Inspection (information used by the infrastructure to specify its behaviour or characteristics of its components is analysed to assess proper compliance with a requirement) 3) Demonstration (using the infrastructure as intended, confirming that the results are aligned with the requirement) 4) Test (functional, measurable characteristics, operability, supportability, or performance capability is quantitatively verified when subjected to controlled conditions that are real or simulated) 5) Analysis (based on analytical evidence obtained without any intervention on the infrastructure using mathematical or probabilistic calculation, logical reasoning, modelling and/or simulation under defined conditions to show theoretical compliance)

Table 1 – Requirement structure

1.6 Abbreviations

Abbreviation	Term
ABAC	Attribute Based Access Control
AIRM	ATM Information Reference Model
AMQP	Advanced Message Queuing Protocol
ATC	Air Traffic Control
ATM	Air Traffic Management
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CTR	Common Time Reference
DoS	Denial of Service
DDoS	Distributed Denial of Service
ERAF	EUROCONTROL Advisory Framework

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

Abbreviation	Term
WSDL	Web Services Description Language
XML	Extensible Markup Language
YP	Yellow Profile

Table 2 – List of abbreviations

1.7 Definitions

Term	Definition	Source
access control	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]
accountability	The degree to which the actions of an entity can be traced uniquely to the entity.	ISO/IEC 25010:2011 [RD 5]
analysis (verification method)	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]
authentication	Process used to achieve sufficient confidence in the binding between the entity and the presented identity.	ITU X.1252:2010 [RD 4]
authenticity	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]
authorization	The granting of rights and, based on these rights, the granting of access.	ITU X.1252:2010 [RD 4]
availability	The degree to which a system, product or component is operational and accessible when required for use.	ISO/IEC 25010:2011 [RD 5]
capability	A functional or non-functional ability for performing a particular task.	–
confidentiality	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]
configuration inspection (verification method)	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.	–
demonstration (verification method)	Verification method for a product or system that consists in using it as intended, confirming that the results are as planned or expected.	–
digital identity	A digital representation of the information known about an entity (individual, group or organization).	ITU X.1252:2010 [RD 4]
document inspection (verification	Verification method for a product or system whereby information describing the product or system is analysed to	–

Term	Definition	Source
method)	assess proper compliance with a requirement.	
entity	Something that has separate and distinct existence and that can be identified in context. *Note: An entity can be a physical person, an animal, a juridical person, an organization, an active or passive 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.*	ITU X.1252:2010 [RD 4]
identity	A representation of an entity in the form of one or more attributes that allow the entity to be sufficiently distinguished within context.	ITU X.1252:2010 [RD 4]
information service	A type of service that provides an information exchange capability.	–
integrity	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]
interface binding	Specification of the protocol and data format to be used in transmitting messages defined by the associated interface.	W3C Web Services Description Requirements: 2002, [RD 6]
interoperability	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.	–
IT infrastructure	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
message	A message is a discrete unit of communication intended by the source for consumption by a given recipient or group of recipients.	–
message exchange pattern	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]
non-repudiation	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]
performance	The performance relative to the amount of resources used	ISO/IEC

Term	Definition	Source
efficiency	under stated conditions. It includes time behaviour, resource utilization and capacity.	25010:2011 [RD 5]
protocol	A set of semantic and syntactic rules for exchanging information.	ISO/IEC 14519:2001 [RD 8]
reliability	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]
security	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]
security token	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]
service	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface.	OASIS (2006) [RD 9]
service description	The information needed in order to use, or consider using, a service.	OASIS (2006) [RD 9]
service interface	The means by which the underlying capabilities of a service are accessed. *Note: the service interface is the means for interacting with a service.*	OASIS (2006) [RD 9]
SWIM TI	A technical infrastructure conformant to one or more SWIM TI specifications (e.g. SWIM TI YP Specification).	–
SWIM TI Profile	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.	–
technical infrastructure (TI)	The software and hardware used in an organization that enables the provision of information services. *Note: Technical infrastructure is a subset of IT Infrastructure.*	–
test (verification method)	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 definition

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. 1.0, 01 December 2017

[RD 3] EUROCONTROL Specification for SWIM Service Description, Ed. 1.0, 01 December 2017

[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)

[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 (YP).

1.9 Document Structure

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

Chapter 2 provides Conformance statements which specify how to conform to the SWIM TI YP Specification taking into account the different integrating parts of this specification.

Chapter 3 specifies Interface Bindings, providing requirements for the implementation of service and network interfaces.

Chapter 4 specifies Infrastructure Capabilities, providing requirements for the implementation of an infrastructure that enables the reliable, secure and efficient exchange of information.

Annex A summarises the requirements to be met when assessing conformity to this specification.

Annex B lists contributing subject matter experts.

Annex C provides Specification Update Procedures.

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 (see Annex C).

2. Conformance

The SWIM TI YP provides requirements related to Interface Bindings (chapter 3) and Infrastructure Capabilities (chapter 4). Conformance with the SWIM TI YP specification requires conformance with both as explained by the conformance statements of this section.

Conformance with this specification is not expected to conflict with the conformance required by existing national or international regulations[5] that in case of conflict prevail over this specification.

When a requirement of this specification requires conformance with externally defined specifications (e.g. OASIS WS-I):

- conformance is expected in accordance to the rules of this externally defined specification
- partial conformance is acceptable if the non-conformant elements are limited to unused or not-applicable aspects; and
- conformance is expected to the referenced version; however newer versions are acceptable if they are backwards compatible with the referenced version.

2.1 Interface Binding Conformance

The SWIM TI YP specification provides different alternatives for the implementation of interfaces (i.e. interface bindings) and requires the implementer to make a selection.

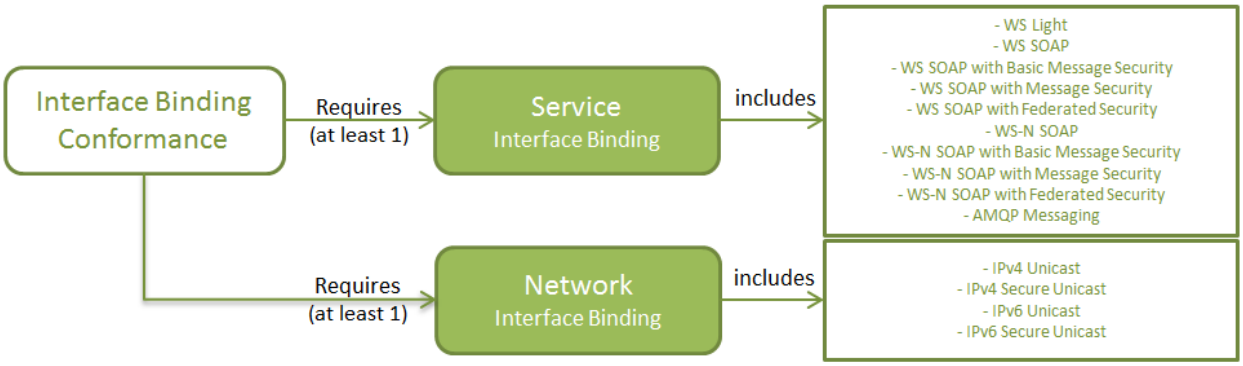

Figure 1 – Interface Binding Conformance Overview

The statements provided in this chapter describe how to conform to the SWIM TI YP specification for the implementation of interfaces:

Identifier	SWIM-TIYP-0001
Title	Conformance with Service Interface Bindings Specification
Conformance Statement	A SWIM TI YP implementation **shall** be conformant with at least one of the Service Interface Bindings included in the SWIM TI YP Specification.
Clarification	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.

[5] In case of security requirements, other requirements based on Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of network and information systems should be considered. Furthermore, additional security requirements on service providers could already exist when a provider or consumer is identified as a European critical infrastructure in the context of Council Directive 2008/114/EC or when the service provision is in scope of Commission Implementing Regulation (EU) 2017/373 or Commission Regulation (EU) 677/2011.

Verification	Analysis

Identifier	SWIM-TIYP-0002
Title	Conformance with Network Interface Bindings Specification
Conformance Statement	A SWIM TI YP implementation **shall** be conformant with at least one of the Network Interface Bindings included in the SWIM TI YP Specification.
Clarification	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.
Verification	Analysis

The conformance to an interface binding specification implies conformance to each of its integrating requirements, as indicated by the operative verbs described in section 1.5 (shall, should, may).

2.2 Infrastructure Capabilities Conformance

The SWIM TI YP specification provides requirements on infrastructure capabilities that enable a reliable, secure and efficient exchange of information, with a special focus on cost effective protective capabilities.

This chapter specifies how to conform to the SWIM TI YP specification for the implementation of infrastructure capabilities:

Identifier	SWIM-TIYP-0003
Title	Conformance with Infrastructure Capabilities
Conformance Statement	A SWIM TI YP implementation **shall** conform to the Infrastructure Capabilities Specification.
Clarification	The Infrastructure Capabilities Specification is a sub-specification of the SWIM TI YP that specifies the minimum set of requirements, the recommended set of requirements and optional requirements for the implementation of infrastructure capabilities.
Verification	Analysis

Conformance to the infrastructure capabilities section of the SWIM TI YP implies conformance to each of its integrating requirements, as indicated by the operative verbs described in section 1.5 (shall, should, may). ANNEX A – provides a table summarising the requirements and their relation to the operative verbs.

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 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. Interface Bindings are grouped into two categories:

1. Service Interface Bindings that enable services to exchange data with consuming applications;
2. Network Interface Bindings that enable the SWIM TI to exchange data with the network.

3.1.1 Service Interface Bindings

Service Interface Bindings can be differentiated from each other based on messaging and security characteristics:

- 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[6]/Specified[7] MEP describes the capability to implement (supported) 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); or
    - 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;
    - 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 table below provides an overview of all service bindings, highlighting the main differentiating characteristics.

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

Table 4 – Service Interface Bindings Overview

The following sub-sections specify the interface bindings, stating the requirements they include and their corresponding level of implementation as described in section 1.5. (Mandatory, Recommended, Optional) and Table 20 – Level of implementation. When a requirement needs to be satisfied when a condition is met, a “Conditional” suffix will be added (e.g. Mandatory Conditional).

Annex A to this specification provides the conformity checklist indicating, per requirement, the level of implementation to be achieved – see Table 20.

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

[7] “Pattern Specified” refers to message exchange patterns which are explicitly defined as part of the protocol specification.

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0042	TLS Server Authentication	M
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M Conditional
SWIM-TIYP-0010	HTTP over TLS	M
SWIM-TIYP-0009	HTTP	M
SWIM-TIYP-0008	TLS	M

Table 5 – WS Light Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0042	TLS Server Authentication	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0010	HTTP over TLS	M
SWIM-TIYP-0009	HTTP	M
SWIM-TIYP-0008	TLS	M

Table 6 – WS SOAP Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0042	TLS Server Authentication	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0030	WS Security Username Token	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0027	SOAP Message Security	M
SWIM-TIYP-0017	WS-I Security	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0010	HTTP over TLS	M
SWIM-TIYP-0009	HTTP	M
SWIM-TIYP-0008	TLS	M

Table 7 – WS SOAP with Basic Message Security Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0046	SOAP Message Encryption	O
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0023	WS Policy	O

SWIM-TIYP-0040	XML Digital Signature	M
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0031	WS Security X509	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0028	XML Message Encryption	M Conditional
SWIM-TIYP-0027	SOAP Message Security	M
SWIM-TIYP-0017	WS-I Security	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0009	HTTP	M

Table 8 – WS SOAP with Message Security Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0026	WS Addressing	M
SWIM-TIYP-0024	WS Secure Conversation	M
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0047	WS Security Token Profiles	M
SWIM-TIYP-0046	SOAP Message Encryption	O
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0034	WS Federation	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0025	WS Trust	M
SWIM-TIYP-0040	XML Digital Signature	M
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0028	XML Message Encryption	M Conditional

SWIM-TIYP-0027	SOAP Message Security	M
SWIM-TIYP-0017	WS-I Security	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0009	HTTP	M

Table 9 – WS SOAP with Federated Security Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0018	WS Notification	M
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0042	TLS Server Authentication	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0010	HTTP over TLS	M
SWIM-TIYP-0009	HTTP	M
SWIM-TIYP-0008	TLS	M

Table 10 – WS-N SOAP Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0018	WS Notification	M
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0042	TLS Server Authentication	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0030	WS Security Username Token	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0027	SOAP Message Security	M
SWIM-TIYP-0017	WS-I Security	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0010	HTTP over TLS	M
SWIM-TIYP-0009	HTTP	M
SWIM-TIYP-0008	TLS	M

Table 11 – WS-N SOAP with Basic Message Security Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0018	WS Notification	M
SWIM-TIYP-0046	SOAP Message Encryption	O
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M

SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0040	XML Digital Signature	M
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional
SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0031	WS Security X509	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0028	XML Message Encryption	M Conditional
SWIM-TIYP-0027	SOAP Message Security	M
SWIM-TIYP-0017	WS-I Security	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0009	HTTP	M

Table 12 – WS-N SOAP with Message Security Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0026	WS Addressing	M
SWIM-TIYP-0024	WS Secure Conversation	M
SWIM-TIYP-0035	WS Reliable Messaging	O
SWIM-TIYP-0018	WS Notification	M
SWIM-TIYP-0047	WS Security Token Profiles	M
SWIM-TIYP-0046	SOAP Message Encryption	O
SWIM-TIYP-0045	HTTP POST	M
SWIM-TIYP-0044	HTTP Reason Phrase Header	M
SWIM-TIYP-0043	HTTP Status Code Header	M
SWIM-TIYP-0034	WS Federation	M
SWIM-TIYP-0023	WS Policy	O
SWIM-TIYP-0025	WS Trust	M
SWIM-TIYP-0040	XML Digital Signature	M
SWIM-TIYP-0038	HTTP Compression and Content Encoding Header	M Conditional

SWIM-TIYP-0033	HTTP Content Type Header	M
SWIM-TIYP-0029	XML	M
SWIM-TIYP-0028	XML Message Encryption	M Conditional
SWIM-TIYP-0027	SOAP Message Security	M
SWIM-TIYP-0017	WS-I Security	M
SWIM-TIYP-0016	WS-I	M
SWIM-TIYP-0015	WSDL 2.0	O
SWIM-TIYP-0014	WSDL 1.1	M
SWIM-TIYP-0013	MTOM	O
SWIM-TIYP-0012	SOAP 1.2	O
SWIM-TIYP-0011	SOAP 1.1	M
SWIM-TIYP-0009	HTTP	M

Table 13 – WS-N SOAP with Federated Security Service Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0049	AMQP Content Encoding Header	O
SWIM-TIYP-0048	AMQP Content Type Header	M Conditional
SWIM-TIYP-0037	AMQP Transport Security Authentication	M
SWIM-TIYP-0051	SASL	M
SWIM-TIYP-0052	AMQP over TLS	M
SWIM-TIYP-0036	AMQP	M
SWIM-TIYP-0008	TLS	M

Table 14 – AMQP Messaging Service Interface Binding

3.1.2 Network Interface Bindings

Network Interface Bindings can be differentiated on their support of network security and the version of the IP protocol used. The following table summarizes their main characteristics:

Network Binding	Network Communication Pattern	Network Security	IP version
IPv4 Unicast	Unicast	No	4
IPv4 Secure Unicast	Unicast	Yes	4
IPv6 Unicast	Unicast	No	6
IPv6 Secure Unicast	Unicast	Yes	6

Table 15 – Network Interface Bindings Overview

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0022	RFC 950	M
SWIM-TIYP-0020	RFC 1122	M
SWIM-TIYP-0006	IPv4	M
SWIM-TIYP-0004	TCP	M

Table 16 – IPv4 Unicast Network Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0022	RFC 950	M
SWIM-TIYP-0020	RFC 1122	M
SWIM-TIYP-0006	IPv4	M
SWIM-TIYP-0005	IPsec	M
SWIM-TIYP-0004	TCP	M

Table 17 – IPv4 Secure Unicast Network Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0019	IPv6 Node Requirements	M
SWIM-TIYP-0020	RFC 1122	M
SWIM-TIYP-0007	IPv6	M
SWIM-TIYP-0004	TCP	M

Table 18 – IPv6 Unicast Network Interface Binding

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.

Identifier	Title	Level of Implementation
SWIM-TIYP-0019	IPv6 Node Requirements	M
SWIM-TIYP-0020	RFC 1122	M
SWIM-TIYP-0007	IPv6	M
SWIM-TIYP-0005	IPsec	M
SWIM-TIYP-0004	TCP	M

Table 19 – IPv6 Secure Unicast Network Interface Binding

3.2 Interface Binding Requirements

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

TCP

Identifier	SWIM-TIYP-0004
Title	TCP
Statement	The Service Interface Binding **shall** support IETF RFC 793 (Transmission Control Protocol).
Clarification	This requirement mandates the use of the Transmission Control Protocol. + IETF RFC 793 (TCP): http://tools.ietf.org/html/rfc793
Verification	Test, Demonstration, Configuration Inspection

IPsec

Identifier	SWIM-TIYP-0005
Title	IPsec
Statement	The Network Interface Binding **shall** support IPsec according to IETF RFC 5406.
Clarification	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. + IETF RFC 5406: https://www.ietf.org/rfc/rfc5406.txt The IPsec protocol itself is defined in IETF RFC 4301. + IETF RFC 4301: https://www.ietf.org/rfc/rfc4301.txt While different algorithms and configuration options are defined in IETF RFC 4302 to IETF RFC 4309. Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

IPv4

Identifier	SWIM-TIYP-0006
Title	IPv4
Statement	The Network Interface Binding **shall** support IETF RFC 791 (Internet Protocol v4).
Clarification	This requirement mandates the use of IETF RFC 791 (Internet Protocol v4). + IETF RFC 791 (Internet Protocol v4): http://tools.ietf.org/html/rfc791
Verification	Test, Demonstration, Configuration Inspection

IPv6

Identifier	SWIM-TIYP-0007
Title	IPv6
Statement	The Network Interface Binding **shall** support IETF RFC 2460 (Internet Protocol v6).
Clarification	This requirement mandates the use of IETF RFC 2460 (Internet Protocol v6). + IETF RFC 2460 (Internet Protocol v6): http://tools.ietf.org/html/rfc2460
Verification	Test, Demonstration, Configuration Inspection

TLS

Identifier	SWIM-TIYP-0008
Title	TLS
Statement	The Service Interface Binding **shall** support the following versions of the Transport Layer Security Protocol (TLS): + IETF RFC 5246 (TLS v1.2)
Clarification	TLS is a widespread protocol to secure communications at the transport layer. + IETF RFC 5246 (TLS v1.2): http://tools.ietf.org/html/rfc5246 Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

HTTP

Identifier	SWIM-TIYP-0009
Title	HTTP
Statement	The Service Interface Binding **shall** support HTTP/1.1.
Clarification	This requirement specifies the use of the HTTP/1.1 protocol. HTTP/1.1 is defined across 6 IETF RFCs spanning from RFC 7230 to RFC 7235. + IETF RFC 7230: http://tools.ietf.org/html/rfc7230 + IETF RFC 7231: http://tools.ietf.org/html/rfc7231 + IETF RFC 7232: http://tools.ietf.org/html/rfc7232 + IETF RFC 7233: http://tools.ietf.org/html/rfc7233 + IETF RFC 7234: http://tools.ietf.org/html/rfc7234 + IETF RFC 7235: http://tools.ietf.org/html/rfc7235
Verification	Test, Demonstration, Configuration Inspection

HTTP over TLS

Identifier	SWIM-TIYP-0010
Title	HTTP over TLS
Statement	The Service Interface Binding **shall** comply with IETF RFC 2818 (HTTP over TLS).
Clarification	This requirement mandates compliance with the interoperability standard for the use of HTTP over TLS (HTTPS). + IETF RFC 2818 (HTTP over TLS): http://tools.ietf.org/html/rfc2818 Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

SOAP 1.1

Identifier	SWIM-TIYP-0011
Title	SOAP 1.1
Statement	The Service Interface Binding **shall** support SOAP 1.1.
Clarification	Service Providers that use a Service Interface Binding relying on SOAP has to support version 1.1. + Simple Object Access Protocol 1.1: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
Verification	Test, Demonstration, Configuration Inspection

SOAP 1.2

Identifier	SWIM-TIYP-0012
Title	SOAP 1.2
Statement	The Service Interface Binding **may** support SOAP 1.2.
Clarification	Service Providers that use a Service Interface Binding that uses SOAP can optionally provide a SOAP 1.2 endpoint. + SOAP 1.2 Part 1: http://www.w3.org/TR/soap12-part1/ + SOAP 1.2 Part 2: http://www.w3.org/TR/2007/REC-soap12-part2-20070427/
Verification	Test, Demonstration, Configuration Inspection

MTOM

Identifier	SWIM-TIYP-0013
Title	MTOM
Statement	The Service Interface Binding **may** support MTOM encoding.
Clarification	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: http://www.w3.org/Submission/soap11mtom10/ + MTOM 1.0 Binding for SOAP 1.2 http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/
Verification	Test, Demonstration, Configuration Inspection

WSDL 1.1

Identifier	SWIM-TIYP-0014
Title	WSDL 1.1
Statement	The Service Interface Binding **shall** support the Web Services Description Language version 1.1 (WSDL 1.1).
Clarification	This requirement specifies the mandatory support of the Web Service Description Language in its versions 1.1. WSDL can be used to specify in machine-processable service description of a Web Service. + WSDL 1.1: http://www.w3.org/TR/wsdl + WSDL 1.1 SOAP 1.2 Binding: https://www.w3.org/Submission/wsdl11soap12/ Related NIST SP 800-53 rev4 Security Control: SI-10.
Verification	Test, Demonstration, Configuration Inspection

WSDL 2.0

Identifier	SWIM-TIYP-0015
Title	WSDL 2.0
Statement	The Service Interface Binding **may** support the Web Services Description Language version 2.0 (WSDL 2.0).
Clarification	This requirement provides the option to support version 2.0 of the Web Service Description Language. + WSDL 2.0 Part 1: http://www.w3.org/TR/wsdl20/ + WSDL 2.0 Part 2: http://www.w3.org/TR/2007/REC-wsdl20-adjuncts-20070626/ + WSDL 2.0 SOAP 1.1 Binding: http://www.w3.org/TR/wsdl20-soap11-binding/ Related NIST SP 800-53 rev4 Security Control: SI-10.
Verification	Test, Demonstration, Configuration Inspection

WS-I

Identifier	SWIM-TIYP-0016
Title	WS-I
Statement	The Service Interface Binding **shall** support the following versions of the OASIS WS-I Basic Profile: + OASIS WS-I Basic Profile Version 1.2 for SOAP 1.1 endpoint + OASIS WS-I Basic Profile Version 2.0 if SOAP 1.2 endpoint is used.
Clarification	WS-I 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. WS-I Basic Profile Version 1.2 targets SOAP 1.1 interoperability and WS-I Basic Profile Version 2.0 targets SOAP 1.2 interoperability. Every SOAP endpoint provided needs to comply with its respective WS-I Basic Profile version. + OASIS WS-I Basic Profile Version 1.2: http://ws-i.org/profiles/basicprofile-1.2-2010-11-09.html + OASIS WS-I Basic Profile Version 2.0: http://ws-i.org/profiles/basicprofile-2.0-2010-11-09.html
Verification	Test, Demonstration, Configuration Inspection

WS-I Security

Identifier	SWIM-TIYP-0017
Title	WS-I Security
Statement	The Service Interface Binding **shall** support the OASIS WS-I Basic Security Profile 1.1.
Clarification	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: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1 Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

WS Notification

Identifier	SWIM-TIYP-0018
Title	WS Notification
Statement	The Service Interface Binding **shall** support OASIS Web Services Notification 1.3.
Clarification	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: http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.htm + OASIS Web Services Brokered Notification 1.3: http://docs.oasis-open.org/wsn/wsn-ws_brokered_notification-1.3-spec-os.pdf + OASIS Web Services Topics 1.3: http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf Related NIST SP 800-53 rev4 Security Control: SI-10.
Verification	Test, Demonstration, Configuration Inspection

IPv6 Node Requirements

Identifier	SWIM-TIYP-0019
Title	IPv6 Node Requirements
Statement	The Network Interface Binding **shall** support IETF RFC 6434 (IPv6 Node Requirements).
Clarification	This requirement mandates the support of IETF RFC 6434 (IPv6 Node Requirements). + IETF RFC 6434 (IPv6 Node Requirements): http://tools.ietf.org/html/rfc6434
Verification	Test, Demonstration, Configuration Inspection

RFC 1122

Identifier	SWIM-TIYP-0020
Title	RFC 1122
Statement	The Network Interface Binding **shall** support IETF RFC 1122 (Internet Standard, Requirements for Internet Hosts- Communication Layers).
Clarification	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: http://tools.ietf.org/html/rfc1122
Verification	Test, Demonstration, Configuration Inspection

RFC 950

Identifier	SWIM-TIYP-0022
Title	RFC 950
Statement	The Network Interface Binding **shall** support IETF RFC 950 (Internet Standard Sub netting Procedure).
Clarification	This requirement mandates the use of IETF RFC 950 (Internet Standard Sub netting Procedure). + IETF RFC 950 (Internet Standard Sub netting Procedure): http://tools.ietf.org/html/rfc950
Verification	Test, Demonstration, Configuration Inspection

WS Policy

Identifier	SWIM-TIYP-0023
Title	WS Policy
Statement	The Service Interface Binding **may** include general service policies expressed using W3C Web Service Policy 1.5.
Clarification	Web Service Policy allows expressing, 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: https://www.w3.org/TR/2007/REC-ws-policy-20070904/ + W3C Web Services Policy 1.5 - Attachment: http://www.w3.org/TR/ws-policy-attach/
Verification	Test, Demonstration, Configuration Inspection

WS Secure Conversation

Identifier	SWIM-TIYP-0024
Title	WS Secure Conversation
Statement	The Service Interface Binding **shall** support WS-SecureConversation 1.4.
Clarification	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: http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.html Related NIST SP 800-53 rev4 Security Control: SC-23.
Verification	Test, Demonstration, Configuration Inspection

WS Trust

Identifier	SWIM-TIYP-0025
Title	WS Trust
Statement	The Service Interface Binding **shall** support WS-Trust 1.4.
Clarification	WS-Trust extends WS-Security providing a framework for requesting and issuing security tokens, and to broker trust relationships. + OASIS WS-Trust 1.4: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html Related NIST SP 800-53 rev4 Security Control: IA-4 (6).
Verification	Test, Demonstration, Configuration Inspection

WS Addressing

Identifier	SWIM-TIYP-0026
Title	WS Addressing
Statement	The Service Interface Binding **shall** support WS-Addressing 1.0.
Clarification	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: https://www.w3.org/TR/2006/REC-ws-addr-core-20060509/ + W3C Recommendation Web Services Addressing 1.0 - SOAP Binding: https://www.w3.org/TR/ws-addr-soap/
Verification	Test, Demonstration, Configuration Inspection

SOAP Message Security

Identifier	SWIM-TIYP-0027
Title	SOAP Message Security
Statement	The Service Interface Binding **shall** support OASIS Web Services Security SOAP Message Security 1.1.1.
Clarification	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. + OASIS Web Services Security: SOAP Message Security Version 1.1.1: http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html + OASIS WS-SecurityPolicy 1.3: http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

XML Message Encryption

Identifier	SWIM-TIYP-0028
Title	XML Message Encryption
Statement	The Service Interface Binding **shall** support the W3C XML Encryption Syntax and Processing 1.1 **if** message encryption is needed.
Clarification	This requirement is applicable when message encryption is used, in such case the encryption and processing is done according to W3C XML Encryption Syntax and Processing 1.1. + XML Encryption Syntax and Processing 1.1: https://www.w3.org/TR/xmlenc-core1/ Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

XML

Identifier	SWIM-TIYP-0029
Title	XML
Statement	The Service Interface Binding **shall** support the Extensible Mark-up Language (XML) 1.0.
Clarification	This requirement specifies support for XML 1.0. + Extensible Mark-up Language (XML) 1.0 (Fifth Edition): https://www.w3.org/TR/2008/REC-xml-20081126/
Verification	Test, Demonstration, Configuration Inspection

WS Security Username Token

Identifier	SWIM-TIYP-0030
Title	WS Security Username Token
Statement	The Service Interface Binding **shall** support the WS-Security Username Token Profile 1.1.
Clarification	This requirement specifies support for a username/password token to be used with WS-Security. + OASIS Web Services Security Username Token Profile 1.1: https://www.oasis-open.org/committees/download.php/13392/wss-v1.1-spec-pr-UsernameTokenProfile-01.htm Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9.
Verification	Test, Demonstration, Configuration Inspection

WS Security X509

Identifier	SWIM-TIYP-0031
Title	WS Security X509
Statement	The Service Interface Binding **shall** 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
Clarification	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: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf + WS-Security X.509 Token Profile 1.1.1: http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
Verification	Test, Demonstration, Configuration Inspection

HTTP Content Type Header

Identifier	SWIM-TIYP-0033
Title	HTTP Content Type Header
Statement	The Service Interface Binding **shall** use the HTTP *Content-Type* header to specify the Media Type of the payload **if**: + The HTTP message contains a payload body and; **+** The content-type is not statically defined in the interface definition.
Clarification	The HTTP/1.1 specification recommends the use of the content-type header when the message contains a payload body, this requirement constraints further this recommendation by requiring its use when the consumer does not know ahead of time the content-type of the payload received. This is the case when the content-type is subject to some content negotiation or when multiple types of payloads can be received through the same interface. The dynamic specification of the content-type promotes interoperability in these cases. When this is not the case implementers can fall back to HTTP/1.1 recommendations and best practices. Possible values include: + IANA registered Media Types + Protocol specific extensions + Vendor proprietary extensions. IANA registered Media Types: http://www.iana.org/assignments/media-types/media-types.xhtml Related NIST SP 800-53 rev4 Security Control: CM-6.
Verification	Test, Demonstration, Configuration Inspection

WS Federation

Identifier	SWIM-TIYP-0034
Title	WS Federation
Statement	The SWIM-TI Interface **shall** support WS-Federation 1.2
Clarification	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: http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html Related NIST SP 800-53 rev4 Security Control: IA-4 (6).
Verification	Test, Demonstration, Configuration Inspection

WS Reliable Messaging

Identifier	SWIM-TIYP-0035
Title	WS Reliable Messaging
Statement	The Service Interface Binding **may** support WS-ReliableMessaging 1.2.
Clarification	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. + OASIS Standard Web Services Reliable Messaging 1.2: https://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.2-spec-os.html + WS-ReliableMessaging Policy 1.2: http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-os.html
Verification	Test, Demonstration, Configuration Inspection

AMQP

Identifier	SWIM-TIYP-0036
Title	AMQP
Statement	The Service Interface Binding **shall** support the Advanced Message Queuing Protocol (AMQP) 1.0.
Clarification	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. + ISO/IEC 19464:2014 Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64955
Verification	Test, Demonstration, Configuration Inspection

AMQP Transport Security Authentication

Identifier	SWIM-TIYP-0037
Title	AMQP Transport Security Authentication
Statement	The Service Interface Binding **shall** support at least one of the following authentication methods: + TLS server authentication and SASL PLAIN + TLS mutual authentication and SASL ANONYMOUS + TLS mutual authentication and SASL PLAIN.
Clarification	This requirement specifies the supported authentication methods of the AMQP 1.0 Service Interface Binding. Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
Verification	Test, Demonstration, Configuration Inspection

HTTP Compression and Content Encoding Header

Identifier	SWIM-TIYP-0038
Title	HTTP Compression and Content Encoding Header
Statement	The Service Interface Binding **shall** use one of the following values of the HTTP header *Content-Encoding* **if** data compression is used: + deflate + gzip + exi
Clarification	This requirement is applicable when data compression is used, in such case it restricts the possible compression algorithms and requires the use of the HTTP Content-Encoding header. 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: https://www.ietf.org/rfc/rfc1951.txt + GZIP File Format Specification 4.3: https://tools.ietf.org/html/rfc1952 + Efficient XML Interchange (EXI) Format 1.0: http://www.w3.org/TR/2014/REC-exi-20140211/ Related NIST SP 800-53 rev4 Security Control: CM-6.
Verification	Test, Demonstration, Configuration Inspection

XML Digital Signature

Identifier	SWIM-TIYP-0040
Title	XML Digital Signature
Statement	The SWIM-TI **shall** digitally sign messages in accordance with W3C XML Signature Syntax and Processing (Second Edition).
Clarification	XML Signature Syntax and Processing provides the capability to sign XML messages, thus adding integrity and origin authentication at message level. + XML Signature Syntax and Processing (Second Edition): http://www.w3.org/TR/xmldsig-core/ Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration

TLS Server Authentication

Identifier	SWIM-TIYP-0042
Title	TLS Server Authentication
Statement	The Service Interface Binding **shall** support, at least, the following authentication mechanisms for TLS: + Server authentication with X.509 certificate.
Clarification	TLS supports three authentication modes: mutual authentication, server authentication and total anonymity. This requirement specifies that, at a minimum, server authentication with X.509 certificates must be supported. Implementers are free to select the appropriate level and mechanism required for client authentication (e.g. anonymous client authentication, X.509 client authentication, HTTP Basic client authentication, HTTP Bearer client authentication...). + IETF RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile): https://tools.ietf.org/html/rfc5280 + IETF RFC 5246 (The Transport Layer Security (TLS) Protocol Version 1.2): https://tools.ietf.org/html/rfc5246 Related NIST SP 800-53 rev4 Security Control: IA-9, SC-8, SC-17.
Verification	Test, Demonstration, Configuration Inspection

HTTP Status Code Header

Identifier	SWIM-TIYP-0043
Title	HTTP Status Code Header
Statement	The Service Interface Binding **shall** be able to use the HTTP *Status-Code* header.
Clarification	This requirement specifies the need to use the Status-Code header of HTTP. The *Status-Code* rules and semantics are defined as part of the HTTP/1.1 specification. + IETF RFC 7231 (HTTP/1.1): https://tools.ietf.org/html/rfc7231#section-6 Related NIST SP 800-53 rev4 Security Control: CM-6.
Verification	Test, Demonstration, Configuration Inspection

HTTP Reason Phrase Header

Identifier	SWIM-TIYP-0044
Title	HTTP Reason Phrase Header
Statement	The Service Interface Binding **shall** be able to use the HTTP *Reason-Phrase* header.
Clarification	This requirement specifies the need to use of the Reason-Phrase header of HTTP. The *Reason-Phrase* rules and semantics are defined as part of the HTTP/1.1 specification. + IETF RFC 7230 (HTTP/1.1): https://tools.ietf.org/html/rfc7230 Related NIST SP 800-53 rev4 Security Control: CM-6.
Verification	Test, Demonstration, Configuration Inspection

HTTP POST

Identifier	SWIM-TIYP-0045
Title	HTTP POST
Statement	The Service Interface Binding **shall** use the following HTTP methods: + POST
Clarification	SOAP Web Services rely on HTTP's POST method.
Verification	Test, Demonstration, Configuration Inspection

SOAP Message Encryption

Identifier	SWIM-TIYP-0046
Title	SOAP Message Encryption
Statement	The SWIM-TI **may** encrypt any combination of body blocks, header blocks and any of these sub-structures of a SOAP message.
Clarification	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.
Verification	Test, Demonstration

WS Security Token Profiles

Identifier	SWIM-TIYP-0047
Title	WS Security Token Profiles
Statement	The Service Interface Binding **shall** 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
Clarification	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: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf + WS-Security X.509 Token Profile 1.1.1: http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html + WS-Security SAML Token Profile 1.1.1: http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SAMLTokenProfile-v1.1.1.html Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9, SC-17.
Verification	Test

AMQP Content Type Header

Identifier	SWIM-TIYP-0048
Title	AMQP Content Type Header
Statement	The Service Interface Binding **shall** use the AMQP 1.0 *content-type* header to specify Media Type values **if:** + The body is composed of data sections and; + The content-type is not statically defined in the interface definition.
Clarification	The content-type is an optional property in the AMQP 1.0 specification, this requirement constraints further this optionality by requiring its use when the consumer does not know ahead of time the content-type of the payload received. This is the case when the content-type is subject to some content negotiation or when multiple types of payloads can be received through the same interface. The dynamic specification of the content-type promotes interoperability in these cases. Possible values include: + IANA registered Media Types + Protocol specific extensions + Vendor proprietary extensions. IANA registered Media Types: http://www.iana.org/assignments/media-types/media-types.xhtml Related NIST SP 800-53 rev4 Security Control: CM-6.
Verification	Test, Configuration Inspection

AMQP Content Encoding Header

Identifier	SWIM-TIYP-0049
Title	AMQP Content Encoding Header
Statement	The Service Interface Binding **may** use Media Type values in the AMQP 1.0 *content-encoding* header to specify additional content encodings applied to the body.
Clarification	This requirement specifies the possible use of the content-encoding header of AMQP 1.0 to detail additional encoding applied over the application-data section (e.g. compression). Possible values include: + IANA registered Content Coding Media Types IANA registered Content Coding Media Types: https://www.iana.org/assignments/http-parameters/http-parameters.xml#content-coding Related NIST SP 800-53 rev4 Security Control: CM-6.
Verification	Test, Configuration Inspection

SASL

Identifier	SWIM-TIYP-0051
Title	SASL
Statement	The Service Interface Binding **shall** support Simple Authentication and Security Layer (SASL).
Clarification	This requirement specifies the support of SASL authentication mechanism (RFC 4422) for the AMQP Service Binding. The framing of the SASL protocol inside AMQP 1.0 is defined in the AMQP 1.0 Specification (section 5). + Simple Authentication and Security Layer (SASL): https://tools.ietf.org/html/rfc4422 Related NIST SP 800-53 rev4 Security Control: IA-2, IA-8, IA-9.
Verification	Test, Demonstration, Configuration Inspection

AMQP over TLS

Identifier	SWIM-TIYP-0052
Title	AMQP over TLS
Statement	The Service Interface Binding **shall** use the AMQP over TLS (amqps) for transport security.
Clarification	This requirement mandates the establishment of a TLS session prior to the exchange of AMQP headers as defined in the AMQP 1.0 specification, section 5.2.1. This mechanism of establishing the transport secure layer is denominated amqps by IANA. + ISO/IEC 19464:2014 Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64955 Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration, Configuration Inspection

4. Infrastructure Capabilities Specification

4.1 Security

Common Time Reference

Identifier	SWIM-TIYP-0053
Title	Common Time Reference
Statement	The SWIM-TI **shall** rely on a Common Time Reference (CTR) for time synchronisation.
Clarification	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 (1).
Verification	Test, Demonstration

Overload Protection

Identifier	SWIM-TIYP-0054
Title	Overload Protection
Statement	The SWIM-TI **shall** provide overload protection mechanisms for its provided services.
Clarification	This requirement mitigates the risk of exhausting available resources resulting in service unavailability. 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 different use cases and needs. Common examples of such protection mechanisms include: + Request rate limitations on a per Service or Consumer basis + Software firewalls + Hardware solutions like routers and firewalls + Replicas, load balancers and ingress controllers + Content Delivery Networks Related NIST SP 800-53 rev4 Security Control: SC-5.
Verification	Test, Analysis, Configuration Inspection

Encrypted Connections for Remote Administrative Access

Identifier	SWIM-TIYP-0055
Title	Encrypted Connections for Remote Administrative Access
Statement	The SWIM-TI **shall** use an encrypted connection **if** remote access to its administrative functionality is needed.
Clarification	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. Related NIST SP 800-53 rev4 Security Control: AC-17, AC-17 (2).
Verification	Demonstration, Configuration Inspection

Obscure Password Typing

Identifier	SWIM-TIYP-0056
Title	Obscure Password Typing
Statement	The SWIM-TI **shall** obscure screen typing feedback of passwords **when** a password prompt is presented for authentication.
Clarification	This requirement ensures that the feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. 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. Related NIST SP 800-53 rev4 Security Control: IA-6.
Verification	Demonstration

Least Privileged Principle Access

Identifier	SWIM-TIYP-0057
Title	Least Privileged Principle Access
Statement	The SWIM-TI **shall** rely on the principle of least privilege to grant access to its resources.
Clarification	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, AU-9.
Verification	Demonstration, Analysis

Automatic Sessions termination

Identifier	SWIM-TIYP-0058
Title	Network Connection Termination
Statement	The SWIM-TI **shall** terminate network connections associated to a communication session: + At the end of the session.
Clarification	Unneeded network connections are a potential source of security breaches, termination of such connections minimizes this risk. Related NIST SP 800-53 rev4 Security Control: SC-10.
Verification	Test, Configuration Inspection

Trusted Software

Identifier	SWIM-TIYP-0059
Title	Trusted Software
Statement	The SWIM-TI **shall** be composed of software components whose origin authenticity and integrity can be verified.
Clarification	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.
Verification	Configuration Inspection, Test, Analysis

Verification of Signed Messages Integrity

Identifier	SWIM-TIYP-0060
Title	Verification of Signed Messages Integrity
Statement	The SWIM-TI **shall** verify, prior to any processing or data transformation, the integrity of messages **when** a message cryptographic signature is used.
Clarification	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 its integrity. Related NIST SP 800-53 rev4 Security Control: SC-8.
Verification	Test, Demonstration

Message Payload Validation

Identifier	SWIM-TIYP-0062
Title	Message Payload Validation
Statement	The SWIM-TI **should** validate messages against the applicable message definitions of its Service Interface Bindings.
Clarification	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, JSON Schema, IDL… Related NIST SP 800-53 rev4 Security Control: SI-10.
Verification	Test, Demonstration

Validation of X.509 Certificates

Identifier	SWIM-TIYP-0064
Title	Validation of X.509 Certificates
Statement	The SWIM-TI **shall** validate X.509 certificates by: + Constructing and verifying a trust path to an accepted trust anchor and; + Verifying the certificate status information.
Clarification	The SWIM-TI relies on public key cryptographic certificates for several of its security capabilities. Validation of the X.509 certificates used by the SWIM-TI is required to ensure they can be trusted and their security properties are satisfied. SWIM-TI implementers must be able to construct a trust path from the X.509 certificate to an accepted trust anchor (e.g. trusted Certification Authority or trust store) and verify the certificate status information by checking for freshness (i.e. not expired) and verifying it has not been revoked. Related NIST SP 800-53 rev4 Security Control: IA-5 (2), SC-17.
Verification	Test, Configuration Inspection

Cryptographic Algorithms

Identifier	SWIM-TIYP-0065
Title	Cryptographic Algorithms
Statement	The SWIM-TI **shall** select cryptographic algorithms and key sizes in accordance with: + Applicable national or international regulations on cryptographic algorithms and key sizes or; + ECRYPT-CSA recommendations.
Clarification	Selection of secure cryptographic algorithms is necessary to ensure the security attributes of cryptographically protected data are not violated. When national or international regulations on the selection of cryptographic algorithms and key sizes are available and applicable to the SWIM-TI implementation, implementers can rely directly on said recommendations. In the case said regulations are not available or applicable; implementers can rely on ECRYPT-CSA recommendations. Recommendations on cryptographic algorithms and key sizes ought to be updated

	frequently to avoid vulnerabilities. Implementers are advised to check for up-to-date recommendations. + ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018): https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf Related NIST SP 800-53 rev4 Security Control: IA-5 c, SC-13.
Verification	Test, Configuration Inspection, Analysis

Strong Passwords

Identifier	SWIM-TIYP-0066
Title	Strong Passwords
Statement	The SWIM-TI **shall** enforce strong passwords selection **when** using username/password authentication for its consumer credentials.
Clarification	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. The following are recommended practices that help ensure strong passwords are selected: + Require a minimum length of 8 characters or an equivalent minimum entropy + Allow a wide character space for the password (e.g. allow all printing ASCII characters) + Check passwords against dictionary of known, common or weak passwords. The following are recommendations to avoid in the password ruleset as they typically result in weaker selection of passwords: + Enforce character set combination rules + Routine password expiration + Knowledge-Based Authentication or password hinting. References: NIST Special Publication 800-63B "Digital Identity Guidelines, Authentication and Lifecycle Management" - https://pages.nist.gov/800-63-3/sp800-63b.html Related NIST SP 800-53 rev4 Security Control: IA-5(4).
Verification	Demonstration, Analysis

Mandatory Access Control

Identifier	SWIM-TIYP-0067
Title	Mandatory Access Control
Statement	The SWIM-TI **shall** enforce access control to all of its resources.
Clarification	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. This requirement does not restrict in any way the existence of publicly accessible resources. Related NIST SP 800-53 rev4 Security Control: AC-3 (3).
Verification	Test, Configuration Inspection, Analysis

Recording of Failed Authentication Requests

Identifier	SWIM-TIYP-0068
Title	Recording of Failed Authentication Requests
Statement	The SWIM-TI **shall** record failed authentication attempts.
Clarification	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.
Verification	Demonstration, Test

Restriction after Failed Authentication Requests

Identifier	SWIM-TIYP-0069
Title	Restriction after Failed Authentication Requests
Statement	The SWIM-TI **shall** restrict access to entities that surpass a configurable number of failed authentication attempts.
Clarification	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.
Verification	Test, Demonstration, Configuration Inspection

Satisfactory Authorization

Identifier	SWIM-TIYP-0070
Title	Satisfactory Authorization
Statement	The SWIM-TI **shall** allow a requesting entity to consume a service **if and only if** its authorization is successful.
Clarification	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.
Verification	Test, Demonstration, Configuration Inspection, Analysis

Cryptographic Key Life-cycle Management

Identifier	SWIM-TIYP-0071
Title	Cryptographic Key Life-cycle Management
Statement	The SWIM-TI **should** manage the life-cycle of its cryptographic keys in accordance to NIST SP 800-57.
Clarification	Proper management of cryptographic keys during the entirety of their life-cycle helps 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": http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf Related NIST SP 800-53 rev4 Security Control: SC-12.
Verification	Test, Demonstration, Configuration Inspection

Inactive Administrative Session Termination

Identifier	SWIM-TIYP-0072
Title	Inactive Administrative Session Termination
Statement	The SWIM-TI **shall** terminate inactive administrative sessions (including local, network and remote access) after a configurable amount of idle time.
Clarification	This requirement addresses the termination of administrative sessions, an administrative session is initiated whenever a user (or process acting on behalf of a user) accesses an organisational information system for administrative purposes. Open administrative sessions pose a security risk to the information system, this requirement introduces a mitigation to this risk. Related NIST SP 800-53 rev4 Security Control: AC-12.
Verification	Test, Configuration Inspection

Secure Password Storage

Identifier	SWIM-TIYP-0073
Title	Secure Password Storage
Statement	The SWIM-TI **shall** store passwords at rest in a form that is resistant to offline attacks.
Clarification	Password storage poses a risk in case of security breach, to mitigate this security risk passwords must be stored in a form that is resistant to offline attacks (e.g. brute forcing, dictionary attacks, rainbow tables...). Storage of consumer credentials does not require that the password is stored in a recoverable manner. In this case, passwords can be stored in a form that is resistant to offline attacks by storing them after salting and hashing them with an appropriate hash function or key-derivation function. When a password needs to be stored in a recoverable manner for later use (e.g. SWIM-TI's own credentials to be used for external services), encryption at rest provides a mechanism that is resistant to offline attacks provided strong algorithms and key sizes are selected. The selection of cryptographic algorithms, key sizes, salt sizes and iteration rounds is subject to SWIM-TIYP-0065. + NIST Special Publication 800-63B – Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html Related NIST SP 800-53 rev4 Security Control: IA-5 h, IA-5 (1)c.
Verification	Configuration Inspection

Security Patching

Identifier	SWIM-TIYP-0074
Title	Security Patching
Statement	The SWIM-TI **should** be the subject of a documented vulnerability patching process that mitigates known vulnerabilities within a predefined maximum timeframe.
Clarification	Service provision in a potentially hostile environment, such as the Internet, needs a regular update of software to apply security patches The longer a known vulnerability remains unpatched, the higher the risk of exploits. 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. Security patches need to be tested prior to their application into operational systems for effectiveness and potential side effects. Related NIST SP 800-53 rev4 Security Control: SI-2.
Verification	Document Inspection

Vulnerability Assessment

Identifier	SWIM-TIYP-0075
Title	Vulnerability Assessment
Statement	The SWIM-TI **may** be the subject of a documented yearly vulnerability assessment which includes penetration tests.
Clarification	Service provision in a public environment needs to be protected against possible hostile attacks. A regular check of unprotected vulnerabilities helps mitigate said risk. 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. The choice of framework or methodology followed is in the remit of the implementer, a number of framework and methodologies are readily available (e.g. Penetration Testing Execution Standard, NIST SP 800-115, PCI DSS guidance…). Satisfaction of this requirement is achieved through proper documentation of the vulnerability assessment and penetration testing scope and methodology followed. Related NIST SP 800-53 rev4 Security Control: CA-8, RA-5.
Verification	Document Inspection

Audit Data Reporting

Identifier	SWIM-TIYP-0076
Title	Audit Data Reporting
Statement	The SWIM-TI **may** provide the means to analyse and produce reports of the collected audit data.
Clarification	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.
Verification	Demonstration

Audit of identity validity events

Identifier	SWIM-TIYP-0077
Title	Audit of Identity Validity Events
Statement	The SWIM-TI **may** detect and record identities whose access has been restricted with the relevant context information.
Clarification	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.
Verification	Demonstration, Test

Protection of information at rest

Identifier	SWIM-TIYP-0078
Title	Protection of Information at Rest
Statement	The SWIM-TI **may** cryptographically secure data in local storage.
Clarification	The SWIM-TI could 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 might be accessible to eavesdroppers. This requirement provides the SWIM-TI the necessary means to secure stored sensitive data. Related NIST SP 800-53 rev4 Security Control: SC-28, SC-28 (1).
Verification	Test, Configuration Inspection

Protection of Audit Information

Identifier	SWIM-TIYP-0079
Title	Protection of Audit Information
Statement	The SWIM-TI **may** store audit data in non-volatile secure storage.
Clarification	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 stored 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.
Verification	Demonstration

Audit Data Remote Storage

Identifier	SWIM-TIYP-0080
Title	Audit Data Remote Storage
Statement	The SWIM-TI **may** replicate audit data in a different system from the system generating the audit data.
Clarification	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).
Verification	Demonstration

Audit Data Management Reporting

Identifier	SWIM-TIYP-0081
Title	Audit Data Management Reporting
Statement	The SWIM-TI **may** provide an interface to manage audit reports.
Clarification	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.
Verification	Demonstration

Audit of Access Requests

Identifier	SWIM-TIYP-0082
Title	Audit of Access Requests
Statement	The SWIM-TI **may** detect and record access to its services and resources.
Clarification	Recording access to the SWIM-TI services and resources enables its future auditing. Related NIST SP 800-53 rev4 Security Control: AU-2a, SI-4a.2.
Verification	Demonstration, Test

Audit of Authentication Requests

Identifier	SWIM-TIYP-0083
Title	Audit of Authentication Requests
Statement	The SWIM-TI **may** detect and record authentication requests.
Clarification	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.
Verification	Demonstration, Test

Audit of Authorization Requests

Identifier	SWIM-TIYP-0084
Title	Audit of Authorization Requests
Statement	The SWIM-TI **may** detect and record authorization requests.
Clarification	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.
Verification	Demonstration, Test

Safe Mode Operation

Identifier	SWIM-TIYP-0085
Title	Safe Mode Operation
Statement	**When** certain adverse conditions are met, the SWIM-TI **may** use a safe mode of operation that prioritises mission critical functions.
Clarification	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.
Verification	Test, Demonstration

Safe Mode Description

Identifier	SWIM-TIYP-0086
Title	Safe Mode Description
Statement	The SWIM-TI **may** have associated documentation identifying the mission critical functions that comprise the safe mode of operation.
Clarification	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.
Verification	Document Inspection

CAVP validated Cryptographic Modules

Identifier	SWIM-TIYP-0087
Title	CAVP approved Cryptographic Modules
Statement	The SWIM-TI **may** use cryptographic modules approved by the Cryptographic Algorithm Validation Program (CAVP).
Clarification	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. Satisfaction of this requirement is achieved using cryptographic algorithm implementations approved by the Cryptographic Algorithm Validation Program (CAVP). Cryptographic Algorithm Validation Program (CAVP): http://csrc.nist.gov/groups/STM/cavp/index.html List of validated cryptographic algorithms: http://csrc.nist.gov/groups/STM/cavp/validation.html Related NIST SP 800-53 rev4 Security Control: SC-13.
Verification	Configuration Inspection

Audit of Cryptographic Events

Identifier	SWIM-TIYP-0088
Title	Audit of Cryptographic Events
Statement	The SWIM-TI **may** detect and record uses of its cryptographic modules.
Clarification	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. Related NIST SP 800-53 rev4 Security Control: AU-2.
Verification	Demonstration, Test

Configurable Authentication

Identifier	SWIM-TIYP-0089
Title	Configurable Authentication
Statement	The SWIM-TI **may** enforce different types of identity security tokens on a per service basis.
Clarification	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.
Verification	Test, Configuration Inspection

Audit of federated identity events

Identifier	SWIM-TIYP-0090
Title	Audit of federated identity events
Statement	**When** integrated with a federated identity management, the SWIM-TI **may** detect and record updates received from external identity management systems related to restricted identities.
Clarification	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.
Verification	Demonstration, Test

Security Assessment

Identifier	SWIM-TIYP-0091
Title	Security Assessment
Statement	The SWIM-TI **may** be the subject of a security assessment that is regularly maintained.
Clarification	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.
Verification	Document Inspection

Denial of Service Protection

Identifier	SWIM-TIYP-0092
Title	Denial of Service Protection
Statement	The SWIM-TI **may** provide defensive measures against Denial of Service attacks.
Clarification	A variety of solutions exist to reduce the effects of Denial of Service (both DoS and DDoS). Examples include: + 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. + Increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. + Content Delivery Networks. Related NIST SP 800-53 rev4 Security Control: SC-5.
Verification	Test, Analysis

Identity Validity Information Exchange

Identifier	SWIM-TIYP-0093
Title	Identity Validity Information Exchange
Statement	**When** integrated with a federated identity management, the SWIM-TI **may** exchange information related to restricted identities.
Clarification	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). Related NIST SP 800-53 rev4 Security Control: IA-5(9).
Verification	Demonstration, Test

Role Based Access Control

Identifier	SWIM-TIYP-0094
Title	Role Based Access Control
Statement	The SWIM-TI **may** support Role Based Access Control (RBAC).
Clarification	Role based access control enables to provide access to a particular resource (e.g. service) based on the roles associated to an identity. Related NIST SP 800-53 rev4 Security Control: AC-3 (7).
Verification	Test, Configuration Inspection

Attribute Based Access Control

Identifier	SWIM-TIYP-0095
Title	Attribute Based Access Control
Statement	The SWIM-TI **may** support Attribute Based Access Control (ABAC).
Clarification	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 Role Based Access Control. OASIS extensible Access Control Mark-up Language 3.0: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html Related NIST SP 800-53 rev4 Security Control: AC-16.
Verification	Test, Configuration Inspection

Hardware Tokens

Identifier	SWIM-TIYP-0096
Title	Hardware Tokens
Statement	The SWIM-TI **may** support the use of hardware security tokens for authentication.
Clarification	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.
Verification	Demonstration

4.2 Messaging

Content Based Routing

Identifier	SWIM-TIYP-0097
Title	Content Based Routing
Statement	The SWIM-TI **may** route messages based on the content of the message.
Clarification	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.
Verification	Test, Demonstration

Subject Based Routing

Identifier	SWIM-TIYP-0098
Title	Subject Based Routing
Statement	The SWIM-TI **may** route messages based on the subject or header of the message.
Clarification	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.
Verification	Test, Demonstration

Context Based Routing

Identifier	SWIM-TIYP-0099
Title	Context Based Routing
Statement	The SWIM-TI **may** route messages based on the context of the message.
Clarification	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).
Verification	Test, Demonstration

Automatic Retries

Identifier	SWIM-TIYP-0100
Title	Automatic Retries
Statement	The SWIM-TI **may** perform a configurable number of automatic retries on failed message delivery.
Clarification	Retries on failed message delivery provide certain resilience against deprecation of network communications and transparency during failover. This requirement is restricted to application layer messages, retries at transport and network layers are handled as specified in their specific protocols. Configurable aspects include the number of retries and the non-response time that triggers the next retry.
Verification	Test, Demonstration, Configuration Inspection

Configurable Routing

Identifier	SWIM-TIYP-0101
Title	Configurable Routing
Statement	The SWIM-TI **may** select in a configurable manner the routing mechanism to be used for each message exchange.
Clarification	Not all information exchanges through the SWIM-TI need the same routing mechanisms. This requirement provides the SWIM-TI with the capability to configure the most adequate routing mechanism for each service.
Verification	Test, Configuration Inspection

Traffic Prioritisation

Identifier	SWIM-TIYP-0102
Title	Traffic Prioritisation
Statement	The SWIM-TI **may** prioritise between different types of traffic according to predefined prioritisation rules.
Clarification	This requirement enables the coexistence of different kinds of traffic and services with different priorities without lower priority traffic throttling high priority traffic.
Verification	Test, Demonstration, Configuration Inspection

4.3 Monitoring

Hardware Monitoring

Identifier	SWIM-TIYP-0103
Title	Hardware Monitoring
Statement	The SWIM-TI **may** monitor the state of its hardware resources: + Processors + Volatile and Non-Volatile memory + Communication resources.
Clarification	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.
Verification	Test, Demonstration, Configuration Inspection

Monitoring Alerts

Identifier	SWIM-TIYP-0104
Title	Monitoring Alerts
Statement	The SWIM-TI **may** raise an alert when a threshold violation occurs.
Clarification	Threshold violations may require intervention from a supervisor or system administrators. This requirement ensures an alert mechanism is provided.
Verification	Test, Demonstration

Service Monitoring

Identifier	SWIM-TIYP-0105
Title	Service Monitoring
Statement	The SWIM-TI **may** monitor the state of the services it supports.
Clarification	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.
Verification	Test, Demonstration

Persistent Storage Recording

Identifier	SWIM-TIYP-0106
Title	Persistent Storage Recording
Statement	The SWIM-TI **may** log in persistent storage threshold violations of the monitored resources and services.
Clarification	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.
Verification	Test, Demonstration

Log Retention

Identifier	SWIM-TIYP-0107
Title	Log Retention
Statement	The SWIM-TI **may** retain for a configurable number of days the collected logs.
Clarification	Collected logs can be used to provide reports, analyse system performance, analyse errors or investigate security incidents. This requirement specifies its retention 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.
Verification	Test, Demonstration, Configuration Inspection

4.4 Reliability

Replication Transparency

Identifier	SWIM-TIYP-0108
Title	Replication Transparency
Statement	The SWIM-TI **may** provide replication transparency to its consumers.
Clarification	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).
Verification	Test, Demonstration, Configuration Inspection

Failure Transparency

Identifier	SWIM-TIYP-0109
Title	Failure Transparency
Statement	The SWIM-TI **may** provide failure transparency to its consumers in the case of a single replicated element failure.
Clarification	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).
Verification	Test, Demonstration

Subscription Persistency

Identifier	SWIM-TIYP-0110
Title	Subscription Persistency
Statement	The SWIM-TI **may** provide persistency across reboot and crash of the subscription mechanism **when** a Publish/Subscribe MEP is used.
Clarification	This requirement ensures that the subscription mechanism is resilient against crashes or reboots of the entity managing the subscription. Subscription persistency provides efficiency and reliability benefits as it prevents subscribers from re-subscribing after reboot of the subscription management entity. Related NIST SP 800-53 rev4 Security Control: SC-24.
Verification	Test, Demonstration

Message Persistency

Identifier	SWIM-TIYP-0111
Title	Message Persistency
Statement	The SWIM-TI **may** provide message persistency **when** a Publish/Subscribe MEP is used.
Clarification	Message persistency ensures that messages are kept until confirmation of successful delivery is received. Restrictions to message persistence can be applied (e.g. lifetime restrictions, number of messages in persistent storage or size of total stored messages restrictions). Related NIST SP 800-53 rev4 Security Control: SC-24.
Verification	Test, Demonstration

ANNEX A – Conformity Checklist

This annex summarises the requirements to be met when assessing conformity to this specification. In accordance with the structure of this specification, this annex distinguishes between conformance with Interface Bindings and Infrastructure Capabilities.

The following table describes the operative verbs and corresponding indicated level of implementation. In some cases, the requirement is “Conditional” which means that the requirement statement contains a clause that indicates the condition under which the requirement is applicable.

Level of Implementation	Operative verb used in the requirement
M = Mandatory	**shall**
R = Recommended	**should**
O = Optional	**may**

Table 20 – Level of implementation

A.1 Conformity with Interface Bindings

Conformity with the Interface Bindings specification is achieved by implementing, at a minimum, a Service Interface Binding and a Network Interface Binding. The requirements mandated by each Interface Binding are detailed in the following tables:

Service Interface Bindings:

Table 5 – WS Light Service Interface Binding

Table 6 – WS SOAP Service Interface Binding

Table 7 – WS SOAP with Basic Message Security Service Interface Binding

Table 8 – WS SOAP with Message Security Service Interface Binding

Table 9 – WS SOAP with Federated Security Service Interface Binding

Table 10 – WS-N SOAP Service Interface Binding

Table 11 – WS-N SOAP with Basic Message Security Service Interface Binding

Table 12 – WS-N SOAP with Message Security Service Interface Binding

Table 13 – WS-N SOAP with Federated Security Service Interface Binding

Table 14 – AMQP Messaging Service Interface Binding

Network Interface Bindings:

Table 16 – IPv4 Unicast Network Interface Binding

Table 17 – IPv4 Secure Unicast Network Interface Binding

Table 18 – IPv6 Unicast Network Interface Binding

Table 19 – IPv6 Secure Unicast Network Interface Binding

A.2 Conformity with Infrastructure Capabilities

The following table lists each requirement in the infrastructure capabilities section and the corresponding level of implementation.

Identifier	Title	Level of Implementation
SWIM-TIYP-0053	Common Time Reference	M
SWIM-TIYP-0054	Overload Protection	M
SWIM-TIYP-0055	Encrypted Connections for Remote Administrative Access	M Conditional
SWIM-TIYP-0056	Obscure Password Typing	M Conditional
SWIM-TIYP-0057	Least Privileged Principle Access	M
SWIM-TIYP-0058	Automatic Sessions termination	M
SWIM-TIYP-0059	Trusted Software	M
SWIM-TIYP-0060	Verification of Signed Messages Integrity	M Conditional
SWIM-TIYP-0062	Message Payload Validation	R
SWIM-TIYP-0064	Validation of X.509 Certificates	M
SWIM-TIYP-0065	Cryptographic Algorithms	M
SWIM-TIYP-0066	Strong Passwords	M Conditional
SWIM-TIYP-0067	Mandatory Access Control	M
SWIM-TIYP-0068	Recording of Failed Authentication Requests	M
SWIM-TIYP-0069	Restriction after Failed Authentication Requests	M
SWIM-TIYP-0070	Satisfactory Authorization	M Conditional
SWIM-TIYP-0071	Cryptographic Key Life-cycle Management	R
SWIM-TIYP-0072	Inactive Administrative Session Termination	M
SWIM-TIYP-0073	Secure Password Storage	M
SWIM-TIYP-0074	Security Patching	R
SWIM-TIYP-0075	Vulnerability Assessment	O
SWIM-TIYP-0076	Audit Data Reporting	O
SWIM-TIYP-0077	Audit of Identity Validity Events	O
SWIM-TIYP-0078	Protection of Information at Rest	O
SWIM-TIYP-0079	Protection of Audit Information	O
SWIM-TIYP-0080	Audit Data Remote Storage	O
SWIM-TIYP-0081	Audit Data Management Reporting	O
SWIM-TIYP-0082	Audit of Access Requests	O
SWIM-TIYP-0083	Audit of Authentication Requests	O
SWIM-TIYP-0084	Audit of Authorization Requests	O

Identifier	Title	Level of Implementation
SWIM-TIYP-0085	Safe Mode Operation	O Conditional
SWIM-TIYP-0086	Safe Mode Description	O
SWIM-TIYP-0087	CAVP approved Cryptographic Modules	O
SWIM-TIYP-0088	Audit of Cryptographic Events	O
SWIM-TIYP-0089	Configurable Authentication	O
SWIM-TIYP-0090	Audit of federated identity events	O Conditional
SWIM-TIYP-0091	Security Assessment	O
SWIM-TIYP-0092	Denial of Service Protection	O
SWIM-TIYP-0093	Identity Validity Information Exchange	O Conditional
SWIM-TIYP-0094	Role Based Access Control	O
SWIM-TIYP-0095	Attribute Based Access Control	O
SWIM-TIYP-0096	Hardware Tokens	O
SWIM-TIYP-0097	Content Based Routing	O
SWIM-TIYP-0098	Subject Based Routing	O
SWIM-TIYP-0099	Context Based Routing	O
SWIM-TIYP-0100	Automatic Retries	O
SWIM-TIYP-0101	Configurable Routing	O
SWIM-TIYP-0102	Traffic Prioritisation	O
SWIM-TIYP-0103	Hardware Monitoring	O
SWIM-TIYP-0104	Monitoring Alerts	O
SWIM-TIYP-0105	Service Monitoring	O
SWIM-TIYP-0106	Persistent Storage Recording	O
SWIM-TIYP-0107	Log Retention	O
SWIM-TIYP-0108	Replication Transparency	O
SWIM-TIYP-0109	Failure Transparency	O
SWIM-TIYP-0110	Subscription Persistency	O Conditional
SWIM-TIYP-0111	Message Persistency	O Conditional

Table 21 – Conformity checklist

ANNEX B – List of Contributors

This specification was prepared by EUROCONTROL with the assistance of the following subject matter experts that contributed to the first version 1.0:

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	ENAIRE
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 22 – List of subject matter experts

Additional contributions have been provided by members of the SWIM TI community of interest to support the evolution of this specification.

ANNEX C – Specification Update Procedures

It is necessary to periodically check this EUROCONTROL Specification for consistency with referenced material, notably ICAO SARPS and relevant Regulations. The Specification is also expected to evolve following real project and field experience, as well as advances in technology.

The main objectives of a regular review are:

a) to improve the quality of the requirements (e.g. clarity, testability, etc.);
b) to verify that the level of detail published is adequate;
c) to ensure that design-oriented requirements, imposing unnecessary constraints to technical solutions, have been avoided;
d) to ensure that advances in technology are properly reflected;
e) to make all stakeholders, including industry, aware of the latest developments.

The update process for this EUROCONTROL Specification may be summarised as follows:

Stakeholders may provide change proposals either through existing working arrangements (e.g. established working groups) or by sending a formal Change Request (CR) to the generic email address: standardisation@eurocontrol.int

The CR needs to provide following minimum elements:
• Originator information (name, Organisation, contact details)
• Specification title, number and edition date
• Page, chapter, section (subsection) where the issue appears
• Description of the issue and reason for change
• Specific change proposal text (incl. potential alternatives, if any).

Main steps towards a revised version:

- Agency (Standardisation unit) will assess each CR in coordination with content owners, classify the urgency and establish the CR impact category (major, minor or editorial).
- Agency will then prepare resolution proposal(s) and, if needed, discuss those with the originator and/or relevant working arrangements. Note: CR will be grouped into “change packages” to consider reasonable update cycles.
- Agreed changes will be integrated into a revised version “Proposed Issue” including a summarised list of changes.
- Consultation will be performed in accordance with the CR impact category identified:
    - Major changes require full formal stakeholder consultation (PC level)
    - Minor changes need consultation at working layers (e.g. working group or Team)
    - Editorial changes may be implemented directly at any stage though grouped with change packages.

Note: Identified errors which may cause potential problems when implementing, may be corrected directly via separate “Corrigendum”.

The Agency will apply this process in an objective and impartial way and will consult stakeholders as needed and in line with the formal Standards Development Process.

EUROCONTROL

SUPPORTING EUROPEAN AVIATION

© **EUROCONTROL -**
This document is published by EUROCONTROL for information purposes. It may be copied in whole or in part, provided that EUROCONTROL is mentioned as the source and it is not used for commercial purposes (i.e. for financial gain). The information in this document may not be modified without prior written permission from EUROCONTROL.

www.eurocontrol.int