SWIM-TI Identity Management Technical Specification

Document information	
Project Title	Interface specifications and Services Technical requirements
Project Number	14.01.04
Project Manager	Leonardo-Finmeccanica
Deliverable Name	SWIM-TI Identity Management Technical Specification
Deliverable ID	D44-002
Edition	00.01.00
Template Version	03.00.00
Task contributors	
LEONARDO-FINMECCANICA, THALES, INDRA, FREQUENTIS, AIRBUS, HONEYWELL, EUROCONTROL	

Please complete the advanced properties of the document

Abstract

This document is the final SESAR 1 SWIM-TI Technical Specification including functional, non-functional and interfaces requirements applicable to the SWIM-TI Identity Management.

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
[redacted] LEONARDO-FINMECCANICA	[redacted]	04/07/2016
[redacted] EUROCONTROL		14/12/2015
[redacted] THALES		14/12/2015
[redacted] BOEING		14/12/2015
[redacted] THALES		14/12/2015

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] INDRA	[redacted]	08/04/2016
[redacted] FREQUENTIS		10/12/2015
[redacted] THALES		10/12/2015

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted] THALES	[redacted]	18/07/2013
[redacted] NATMIG		18/07/2013
[redacted] NATMIG		18/07/2013
[redacted] THALES		18/07/2013
[redacted] INDRA		18/07/2013
[redacted] THALES		18/07/2013
[redacted] ENAV		17/12/2013

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
[redacted] LEONARDO-FINMECCANICA	[redacted]	04/07/2016
[redacted] INDRA		04/07/2016
[redacted] EUROCONTROL		04/07/2016
[redacted] FREQUENTIS		04/07/2016
[redacted] THALES		04/07/2016
[redacted] HONEYWELL		04/07/2016
[redacted] AIRBUS		04/07/2016

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	02/05/2016	Revised Draft	[redacted]	Revised draft based on SJU approved previous version (D43-002). Implemented sub-set of SJU comments. Implemented sub-set of comments from project members. Integrated relevant comments from project members. Implemented additional minor updates.
00.00.02	13/05/2016	Revised Draft		Integrated and partially implemented additional comments from the partners.
00.00.03	17/06/2016	Revised Draft		Updated §1, §2 and introduction text in §3 sections. Updated/added several requirements.
00.00.04	24/06/2016	Revised Draft		Implemented open comments from previous edition. Implemented received comments on the previous edition.
00.00.05	30/06/2016	Candidate Final Version		Implemented remaining open comments. Final Version ready for approval.
00.00.06	01/07/2016	Candidate Final Version		Implemented minor changes in §1. Implemented Requirements attributes syntactical check. Final Version ready for approval.
00.01.00	04/07/2016	Final Version		Final Version.

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

None.

Executive summary

This deliverable is the final SESAR 1 SWIM-TI technical specification for the SWIM-TI Identity Management as described in the TAD. SWIM-TI TS 3.1 requirements (14.01.04.D43-002 [8]) have been analysed and improved according to maintenance activities agreed by P14.01.03 and P14.01.04 in collaboration with SJU.

1 Introduction

This document represents the TS (Technical specification) covering functional, non-functional and interface requirements identified for SWIM-Technical Infrastructure and applicable to the SWIM-TI Identity Management. In particular it includes the specifications for the SWIM-TI Public Key Infrastructure (PKI) and Security Token Infrastructure (STI) part of information security technical view as described in SWIM-TI TAD [12].

1.1 Purpose of the document

This specification provides functional, non-functional, applicable standards and interface requirements for the SWIM-TI Identity Management including PKI and STI.

1.2 Intended readership

The intended audience of this document is:

- SJU/IS in order to manage the SWIM Technical Infrastructure TS.
- SWP14.2 projects in order to review this TS and to implement and verify the requirements.
- B.4.3 in order to review this TS according to its relationship with architectural aspects.
- 08.03.10 in order to review this TS according to its relationship with service instances provisioning and consumption.
- Any other SESAR projects interested in the SWIM Technical Infrastructure TSs.

1.3 Inputs from other projects

This document is based on the following inputs:

- SWIM-TI TAD [12]
- SWIM Profiles [13]
- SWIM-TI Verification Reports [9][10].
- ISRM 2.0 [7].

1.4 Structure of the document

This document is organized as follows:

Chapter 1: Purpose and scope, requirements guidelines, SWIM-TI Identity Management high level overview.

Chapter 2: General SWIM-TI Identity Management description including context description.

Chapter 3: SWIM-TI Identity Management functional, non-functional, applicable standards and interface requirements.

Chapter 4: Assumptions.

Chapter 5: Referenced documents;

1.5 Requirements Definitions – General Guidance

14.01.04 requirements guidelines include programme level guidelines [2] which have been extended with project level guidelines [14] concerning requirement identifiers coding schema, requirements writing rules, project specific requirements attributes and links.

In particular, a number of P14.01.04 specific requirements attributes have been defined and specified. Each of the attributes can be considered as a dimension on which filtering can be applied. Combined filtering on multiple distinct attributes is meant to be meaningful. Conformance statements provided in this technical specification are possible examples of filtering criteria.

Requirements provided in this Technical Specification have been exported to a spreadsheet allowing specification "user" to apply simple and more complex/structured filtering criteria. References to this file are included in the P14.01.04 Technical Specifications Catalogue [14].

Due to tools used to manage this Technical Specification, it could happen that text and/or requirements tables are formatted as hidden text. Please make sure that Microsoft Word is configured to show hidden text (¶).

1.6 Functional block Purpose

According with SWIM-TI TAD [12], the SWIM-TI Identity Management provides primary activities concerning digital identities used in authenticated ATM information exchanges among SWIM participants. After evaluating different options offered by the current technological landscape, two main technical solutions have been identified in the TAD to support access control, transport and message level security at SWIM-TI layer. The first one relies on the Public Key Infrastructure (PKI) responsible for signing, emitting and maintaining X.509 certificates and revocation lists. The second one consists in the adoption of a Security Token Infrastructure (STI) providing capabilities to manage security tokens and Identity Store. It shall be clear that these solutions are not used in a mutually exclusive fashion, but rather they can cooperate to realise a comprehensive security strategy.

1.7 Functional block Overview

SWIM-TI PKI and STI overview is provided in §2.

1.8 Glossary of terms

Term	Definition
Access Control	ITU-T IdM X.1252 defines this term as a procedure used to determine if 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
Address	ITU-T IdM X.1252 defines this term as an identifier for a specific termination point that is used for routing
Agent	ITU-T IdM X.1252 defines this term as an entity that acts on behalf of another entity.
Alarm	An indication of an error or an abnormal and/or undesirable condition for a resource. An example of an alarm would be for a “connection down” in a data communications channel, or a non-booting processor in a hardware platform. Alarms originate with the hardware, software, and data communications infrastructure, and the infrastructure provides an indication to the Supervision when an alarm is raised or cleared. The Supervision notifies the local owner or authorized requester when an alarm is raised or cleared for a monitored resource.

Term	Definition
Alliance	ITU-T IdM X.1252 defines this term as an agreement between two or more independent entities that defines how they relate to each other and how they jointly conduct activities.
Archive	Information storage that is used for by the automation for long-term retention of information produced and/or used at the local SWIM Node. An archive may be offline with respect to the SWIM Node, meaning that it is not directly accessible to processes and services running on the SWIM Node; or it may be online with respect to the SWIM Node, meaning that the archive is directly accessible to processes and services running on the SWIM Node. Information that is logged by the SWIM Supervision is retained online for a configurable time period, after which it is archived and is then no longer guaranteed to be available in the same manner as information that has not reached its retention time limit. Each SWIM Node will have local processes and procedures for storing, maintaining, and accessing archived information. Archived information will be available to the reporting capability; however, the response time for accessing archived information will vary according to the storage approach used by the node.
Assertion	ITU-T IdM X.1252 defines this term as a statement made by an entity without accompanying evidence of its validity.
ATM Service or SWIM ATM Service	A service representing the exchange of well-defined ATM information.
Attribute	ITU-T IdM X.1252 defines this term as information bound to an entity that specifies a characteristic of the entity.
Attribute Based Access Control (ABAC)	In attribute-based access control (ABAC), access is based on attributes of the user. The user has to prove these attributes to the access control engine. An attribute-based access control policy specifies which attributes need to be satisfied in order to grant access to an object.
Attribute Value	ITU-T IdM X.1252 defines this term as a particular instance of the class of information indicated by an attribute type.
(Entity) Authentication	ITU-T IdM X.1252 defines this term as a process used to achieve sufficient confidence in the binding between the entity and the presented identity.
Authorization	ITU-T IdM X.1252 defines this term as the granting of rights and, based on these rights, the granting of access.
Authorized requester	A human user or automated process, at the local SWIM Node or at a remote SWIM Node, that has been authenticated and is authorized per security requirements to make a service request.
Binding	ITU-T IdM X.1252 defines this term as an explicit established association, bonding, or tie.
Bridge Certificate Authority (BCA)	The Bridge Certification Authority (BCA) architecture addresses the shortcomings of the two basic PKI architectures, and to link PKIs that implement different architectures. The BCA does not issue certificates directly to users. The BCA is not intended to be used as a trust point by the users of the PKI, unlike the “root” CA in a hierarchy. The BCA establishes peer-to-peer

Term	Definition
	trust relationships with the different user communities, which allows the users to keep their natural trust points. These relationships are combined to form a "bridge of trust" enabling users from the different user communities to interact with each other through the BCA with a specified level of trust.
Certificate	ITU-T IdM X.1252 defines this term as a set of security-relevant data issued by a security authority or a trusted third party, that, together with security information, is used to provide the integrity and data origin authentication services for the data.
Certificate Service Provider (CSP)	It is anticipated that security of the European SWIM-TI neither be handled by a single certification authority nor even by a single hierarchy of certification authorities. The main reason is that a few organizations (e.g. CFMU and some Airlines) have already deployed a PKI with an associated third party CA (or Certificate Service Provider (CSP)). The objective is not to replace the existing CAs by a single new one but rather to build a SWIM-TI capable of federating existing CAs and the SWIM-TI dedicated CA
Channel Protection	Channel Protection or transport level security, provides point-to-point protection of the communication. The protection will not go beyond intermediaries. This may be acceptable or not depending on the context. The Transport Layer Security TLS (cryptographic protocol) is a well-known and widely used protocol to provide transport level security. TLS encrypts the data using asymmetric cryptography for key exchange, symmetric encryption for confidentiality and Message Authentication Codes for message integrity.
Claim	ITU-T IdM X.1252 defines this term as to state as being the case, without being able to give proof.
Confidentiality Ensuring	Confidentiality Ensuring aims at providing the ability to ensure "non-disclosure" of information. This service relies on the policy enforcement features and to the cryptographic mechanisms provided by the Cryptography security enabler to ensure information confidentiality at message level.
Credential	ITU-T IdM X.1252 defines this term as a set of data presented as evidence of a claimed identity and/or entitlements.
Data Origin Authentication	Equivalent expression for Information Origin Authentication
Data Validation	Data validation allows checking for conformance to message/data type descriptions. The conformance conditions are expressed in form of well-defined policy assertions assigned to the SWIM service definition.
Dead letter queue	In message queuing, in the dead letter queue are stored messages that meet one or more of the following criteria : message that is sent to a queue that does not exist.; queue length limit exceeded; message length limit exceed; message is rejected by another queue exchange.
Delegation	ITU-T IdM X.1252 defines this term as an action that assigns authority, responsibility, or a function to another entity.
Digital Identity	ITU-T IdM X.1252 defines this term as a digital representation of the information known about a specific individual, group or organization.

Term	Definition
Digital Signature (algorithm)	Digital Signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that a known sender created the message, and that it was not altered in transit. Unlike a Message Authentication Code, a Digital Signature also provides support for non-repudiation.
Enabling Service	A service provided by the SWIM-TI.
Entity	ITU-T IdM X.1252 defines this term as something that has separate and distinct existence and that can be identified in context. 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.
European Network of Excellence in Cryptology (ECRYPT)	ECRYPT (European Network of Excellence for Cryptology) is a 4-year European research initiative launched on 1 February 2004. The stated objective is to, "intensify the collaboration of European researchers in information security and more in particular in cryptology and digital watermarking".
Failure Transparency	Failure transparency masks from an object the failure and possible recovery of other objects (or itself) to enable fault tolerance. When this transparency is provided, the designer can work in an idealized world in which the corresponding class of failures does not occur.
Federation	ITU-T IdM X.1252 defines this term as an association of users, service providers, and identity service providers.
Functional Status	Indicates the ability of the SWIM Node or an element of the SWIM Node to provide the services.
Identification	ITU-T IdM X.1252 defines this term as the process of recognizing an entity by contextual characteristics.
Identifier	ITU-T IdM X.1252 defines this term as one or more attributes used to identify an entity within a context.
Identity	ITU-T IdM X.1252 defines this term as a representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.
Identity Management (IdM)	ITU-T IdM X.1252 defines this term as a set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting

Term	Definition
	business and security applications.
Identity Provider (IdP)	ITU-T IdM X.1252 defines this term as an entity that verifies, maintains, manages, and may create and assign identity information of other entities. Depending on the type of digital identity, an Identity Provider may be Public Key Infrastructure (PKI) or Security Token Infrastructure (STI). IdP is also named Identity Service Provider (IdSP).
Information Origin Authentication	SWIM-TI service to authenticate the originator entity of a message by several techniques at message level and transport level.
Interface Control Document (ICD)	An interface control document (ICD) in systems engineering and software engineering, describes the interface or interfaces between subsystems or to a system or subsystem.
IOP Status	Indicates the ability of the SWIM Node to provide Shared Object services.
Messaging FB or SWIM-TI Messaging FB	Messaging Functional Block provides a decoupled, interoperable and effective communications between information producer and the information consumers. It supports different message exchange patterns (e.g. publish/subscribe, request/response, push, etc.), different subscription styles (e.g. durable, non-durable) and different set of QoS (e.g. best-effort and reliable delivery).
Mutual Authentication	ITU-T IdM X.1252 defines this term as a process by which two entities (e.g., a client and a server) authenticate each other such that each is assured of the other's identity.
Non-Repudiation	ITU-T IdM X.1252 defines this term as the ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.
Pan-European Network Service (PENS)	A joint EUROCONTROL-ANSPs led initiative to provide a common IP based network service across the European region covering voice and data communication and providing efficient support to existing services and new requirements that are emerging from future Air Traffic Management (ATM) concepts.
Persistent	ITU-T IdM X.1252 defines this term as existing and able to be used in services outside the direct control of the issuing assigner, without a stated time-limit.
Policy (Security)	An agreement upon which entities (e.g. Systems) can collaborate. A typical example of this is Authorization Policy and Audit Policy.
Policy Life Cycle Management (Security)	The Policies lifecycle management is a key concept enabling (security) policies management and proper (security) policies enforcement.
Public Key Cryptography	Public Key Cryptography refers to a cryptographic technique in which one key is secret private and a corresponding key one is public. Information are is encrypted using the public key and can only be decrypted by the corresponding secret/private key or vice-versa, information is encrypted using the private key and can only be decrypted by the corresponding public key.. Public Key Cryptography can also be used for Digital Signatures; in this case the private key is used for signing, and the corresponding public key for

Term	Definition
	verifying.
Public Key Infrastructure	A Public Key Infrastructure (PKI) is a system, which may include hardware, software, human in the loop, policies and procedures, needed to create, manage, distribute, use, store and revoke digital identities in X.509 certificates based IdM. PKIs represent the instantiation of the ITU-T X.1252 IdP when the X.509 certificates based security is adopted.
Recording Functional Block or SWIM-TI Recording FB	Recording FB includes the ability to collect, store and to retrieve on demand of information related to communication being performed via the SWIM Interfaces and supervision actions and events.
Registry Functional Block or SWIM-TI Registry FB	Registry FB includes two main groups of functions: - Information Management enabling the management several kinds of ATM-specific service meta-data allowing to discover, to subscribe and to publish/update these information. - Policy Management enabling the definition, validation and distribution of several kinds of policies including security. It covers policy administration (including creation, maintenance, change and deletion) and policy distribution and transformation and policy auditing.
Replication Transparency	Replication transparency masks the use of a group of mutually behaviorally compatible objects to support an interface. Replication is often used to enhance performance and availability.
Revocation	ITU-T IdM X.1252 defines this term as the annulment by someone having the authority, of something previously done.
SAML Token	Security Assertion Markup Language (Token)
Schematron	In markup languages, Schematron is a rule-based validation language for making assertions about the presence or absence of patterns in XML trees. It is a structural schema language expressed in XML using a small number of elements and XPath.
Security Attribute	An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.
Security Domain	ITU-T IdM X.1252 defines this term as a set of elements, a security policy, a security authority, and a set of security-relevant activities in which the elements are managed in accordance with the security policy.
Security Functional Block or SWIM-TI Security FB	Security Functional Block provides confidentiality, integrity, access control, accountability and non-repudiation functionalities, allowing data exchanged through the SWIM-TI to be protected
Security Token	Security tokens are used to prove one's identity electronically. The token acts like an electronic key to access something. Besides the information needed to authenticate an identity, a token can provide additional information (identity attributes) that are used for (e.g.) authorization purposes. Security tokens

Term	Definition
	imply trust of a third party that issues the security tokens.
Security Token Infrastructure (STI)	A Security Tokens Infrastructure (STI) is a system, which may include hardware, software, human in the loop, policies and procedures, needed to create, manage, distribute, use, store and revoke digital identities in security token based IdM. STIs represent the instantiation of the ITU-T X.1252 IdP when the security tokens based security is adopted.
Security Token Service (STS)	A Security Token Service (STS) is a software based identity provider responsible for issuing and verifying security tokens as part of a claims-based identity management.
Service	When used without further qualification, Service indicates either a SWIM Service or a SWIM Enabling Service that is to be managed by SWIM Supervision at the local SWIM Node.
Service Agent SOA Design Pattern	Service agents can be designed to automatically respond to predefined conditions without invocation via a published contract. Refer to SOA Patterns http://www.soapatterns.org/service_agent.php
Service Virtualization (Through Service Agent SOA design pattern)	Service Virtualization helps insulate service infrastructure details such as service endpoint location, service inter-connectivity, policy enforcement, service versioning and dynamic service management information from service consumers. Refer to: http://www.soapatterns.org/service_virtualization.php
Shared Object Functional Block or SWIM-TI Shared Object FB	Shared Object FB is a special category that holds a pattern used to share data across multiple SWIM Nodes according to specific roles and rules.
Supervision Functional Block or SWIM-TI Supervision FB	Monitoring and Control FB includes control, fault management and performance monitoring at SWIM Node level (local supervision).
SWIM Enabled System/Application	A SWIM Enabled System/Application is a system/application exchanging information with other ATM actors according to the SWIM ATM Services and the appropriate SWIM-TI.
SWIM Message Exchange Pattern (MEP)	SWIM Exchange Pattern is a definition to provide data exchanges of a SWIM profile. The message exchange patterns can be defined in terms of a set of technical attributes including interaction pattern, security, quality of service, network infrastructure, middleware functional needs and mandated standards.
SWIM Node Application	A SWIM Node Application represents an application or a software system that supports a particular business function and that can be managed as an independent unit. A SWIM Node Application can be local to a SWIM Node Computer or distributed over multiple SWIM Node Computers. A SWIM Node Application can be composed of other application elements (processes, software components) and other SWIM Node Applications (sub-applications).
SWIM Node Computer	SWIM Node Computer is a special collection of SWIM TI managed entities that provides computing capabilities (such as processor, memory and file

Term	Definition
	systems) for running SWIM TI applications and software components. A SWIM Node Computer is uniquely named and independently managed in a SWM Node.
SWIM Node or SWIM-TI Node	A SWIM-TI Node is an autonomous point of presence in the Distributed System (of Systems) that interacts with other SWIM-TI Nodes in the Distributed System (of Systems).
SWIM Profile Assertion (SPA)	Declaration of the existence of a SWIM Profile combined with precisions on scope and motivation and with design considerations.
SWIM Service	A service that is managed by the SWIM Supervision capability at a local SWIM Node. SWIM Supervision is responsible for the data, process control, event-reporting, and statistics for these services.
SWIM Supervision Service	A service whose functionality is part of the SWIM Supervision capability. SWIM Supervision Services are a subset of SWIM Services.
SWIM Technical Infrastructure (SWIM-TI)	The SWIM Technical Infrastructure (SWIM-TI) contributes to the services' solution, aspects providing means supporting effective and secure ATM-specific service provision and consumption among SWIM-enabled ATM systems.
SWIM-TI Administrative Console	Any application allowing authorized users to manage or control one or more SWIM Functions. Technical details of such consoles depend on implementation choices (e.g. CLI or graphical interfaces) but each console shall guarantee a certain level of security and compliance with current regulations.
SWIM-TI Solution	Software and Hardware representing the implementation of (applicable) SWIM-TI Technical Specifications.
Symmetric Key Cryptography (algorithms)	A Symmetric Key algorithm uses the same cryptographic key (shared secret key) for both encryption of plaintext and decryption of cipher text.
System Instance	A System Instance (SI) is a stakeholder system in the SoS which provides and consumes data in an ATC context e.g. CFMU, Airports.
System of systems (SoS)	System of systems (SoS) is the viewing of multiple, dispersed, independent systems in context as part of a larger, more complex system. A system is a group of interacting, interrelated and interdependent components that form a complex and unified whole.
Technical Status	Indicates whether the SWIM Node or an element of the SWIM Node is working.
X.509 certificates	In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
XML Encryption	XML Encryption is a specification (by W3C recommendation) that defines how to encrypt the contents of an XML element.

Term	Definition
	Note: W3C (World Wide Web Consortium) is the main standards organization for the world wide web.
XML Signature	XML Signature is the XML syntax for digital signatures.

1.9 Acronyms and Terminology

Term	Definition
A/C	Aircraft
A/G	Air/Ground
ABAC	Attribute Based Access Control
ACC	Air Traffic Control Centre
ACCS	Air Command and Control System (NATO terminology)
ADD	Architecture Description Document
AFF-MEP	Asynchronous Fire & Forget Message Exchange Pattern
AIM	Aeronautical Information Management
AIRM	Aeronautical Information Reference Model
AIS	Aeronautical Information Services
AIXM	Aeronautical Information eXchange Model
AMHS	Aeronautical Message Handling System
AMQP	Advanced Message Queuing Protocol
AOC	Airline Operations Centre
ARR-MEP	Asynchronous Request/Reply Message Exchange Pattern
ASM	Any-Source Multicast
ATC	Air Traffic Control
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATN/IPS	ATN using Internet Protocol Suite technologies

Term	Definition
B2B	Business to Business
BCA	Bridge Certification Authority
BP	Blue Profile
BPMN	Business Process Model and Notation
CA	Certification Authority (in the context of PKI)
CBA	Cost Benefit Analysis
CC	Capability Configuration
CDM	Collaborative Decision Making
CDP	CRLs Distribution Point
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CRL	(X.509) Certificate Revocation List
CRUD	Create, Read, Update and Delete (operations)
CSP	Certificate Service Provider
DDS	Data Distribution Service
DM	Dense Mode
DSP	Data-link Service Provider
EAD	European AIS Database
ECRYPT	European Network of Excellence in Cryptology
EFB	Electronic Flight Bag
EN	Enabler
ESB	Enterprise Service Bus
FAA	Federal Aviation Administration
FB	Functional Block
FR	Functional Requirement
FDRR-MEP	Fully Decoupled Request/Reply Message Exchange Pattern
FHA	Fault Hazard Analysis

Term	Definition
FMS	Flight Management System
FO	Flight Object
G/G	Ground/Ground
GAT	General Air Traffic
HA	High Availability
HMI	Human-machine interface
HTTP(S)	HyperText Transfer Protocol (Secure)
IATA	International Air Transport Association
ICD	Interface Control Document
ICOG	Interoperability Consultancy Group
IdM	Identity Management
IdP	Identity Provider
IdSP	Identity Service Provider
IFE	In-Flight Entertainment
IGMP	Internet Group Management Protocol
IM	Information Management
INTEROP	Interoperability Requirements
IP	Internet Protocol
IPR	Intellectual Property Rights
IS	Industrial Support
ISRM	Information Service Reference Model
iSWIM	Initial SWIM (AF5 in the context of PCP)
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MEP	Message Exchange Pattern
MET	Meteo or Meteorological

Term	Definition
MEX	Metadata EXchange
MLD	Multicast Listener Discovery
MSG or MSG FB	SWIM-TI Messaging FB or briefly Messaging FB
MQbRR	Message Queuing based Request-Response
MQbPS	Message Queuing based Publish-Subscribe
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NFR	Non-Functional Requirement
NM	Network Management (CFMU)
NOP	Network OPerations or Network Operations Portal
NOTAM	NOTice To AirMen
NOV	NAF Operational View
NSOV	NAF Service-Oriented View
NSV	NAF System View
NTV	NAF Technical View
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OFA	Operational Focus Area
OMG	Object Management Group
OPULL-MEP	Observer Pull Message Exchange Pattern
OPUSH-MEP	Observer Push Message Exchange Pattern
OS	Operating System
OSED	Operational Service and Environment Definition
OSI	Open Systems Interconnection
OTS	Off The Shelf
PAP	Policy Administration Point
PCP	EUR Pilot Common Project.

Term	Definition
PDP	Policy Decision Point
PDR	Preliminary Design Review
PENS	Pan-European Network Service
PEP	Policy Enforcement Point
PIM	Protocol Independent Multicast
PIM-SM	PIM Sparse Mode
PIM-SSM	PIM Source-Specific Multicast
PIP	Policy Information Point
PIR	Project Initiation Report
PKI	Public Key Infrastructure
PP	Purple Profile
PSM	Platform Specific Model
PSPULL-MEP	Publish/Subscribe Pull Message Exchange Pattern
PSPUSH-MEP	Publish/Subscribe Push Message Exchange Pattern
QoS	Quality of Service
RA	Registration Authority (in the context of PKI)
RBAC	Role Based Access Control
RCP	Required Telecommunication Performance
REC or REC FB	Recording Functional Block or SWIM-TI Recording FB
REG or REG FB	Registry Functional Block or SWIM-TI Registry FB
REST	REpresentation State Transfer
RFC	Request For Comments (Internet Engineering Task Force terminology)
RPO	Recovery Point Objective
RSA	Rivest Shamir Adleman
RST	Request Security Token
RSTR	Request Security Token Response
RTD	Research and Technological Development

Term	Definition
SAML	Security Assertion Markup Language
SAR	System Acceptance Review
SCVP	Server-Based Certificate Validation Protocol
SEC FB or SEC	Security Functional Block or SWIM-TI Security Functional Block
SEMP	System Engineering Management Plan
SESAR	Single European Sky ATM Research Programme
SESAR Programme	The programme which defines the Research and Development activities and Projects for the SJU.
SI	System Instance
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency
SLA	Service Level Agreement
SM	Sparse Mode
SMTP	Simple Mail Transfer Protocol
SO	Shared Object
SO or SO FB	Shared Object Functional Block or SWIM-TI Shared Object FB
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SoS	System of Systems
SPA	SWIM Profile Assertion
SPD	SWIM Profile Descriptor
SPI	SWIM Profile Instantiation
SPR	Safety, Performance Requirements
SPV	SuPerVision
SPV or SPV FB	Supervision Functional Block or SWIM-TI Supervision FB
SRR-MEP	Synchronous Request/Reply Message Exchange Pattern
SSDD	System/Segment Design Document

Term	Definition
SSL	Secure Socket Layer
SSM	Source-Specific Multicast
SSO	Single Sign-On
STI	Security Token Infrastructure
STS	Secure Token Service
SW	SoftWare
SWIM	System Wide Information Management
SWIM-TI	SWIM Technical Infrastructure
TAD	Technical Architecture Description
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRR	Test Readiness Review
TS	Technical Specification
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language TM
UTC	Coordinated Universal Time [International Telecommunication Union (ITU)]
VA	Validation Authority (in the context of PKI)
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WIMP	What-if Manager Publisher (in the context of Flight Object concept/Blue Profile FDD Profile Part)
WP	Work Package
WS	Web Services
WSDL	Web Services Description Language
WSS	Web Services Security

Term	Definition
XACML	eXtensible Access Control Markup Language
YP	Yellow Profile

2 General Functional block Description

2.1 Context

SWIM-TI Technical Specifications deal with the “how” aspect of the SWIM-TI. More precisely, the Technical Specifications provide normative requirements concerning the SWIM-TI technical view [12].

As described in the SWIM-TI TAD [12], *the key component that can provide/realize/deploy the functions of the Functional decomposition view of the SWIM-TI is the SWIM-TI Node. A SWIM-TI Node is an autonomous point of presence in the Distributed System (of Systems) that interacts with other SWIM-TI Nodes in the Distributed System (of Systems).*

The point of presence makes a set of functionality via one SWIM-TI Node available to any SWIM-TI Node or allows use of the functionality that is made available by a SWIM-TI Node via one or more SWIM-TI Nodes.

The SWIM-TI Node is a generic element that could be specialised in categories. At the time of writing, there are two categories of specifications:

- The first category of specifications that are captured and grouped under the notions of SWIM Profile, Profile Part, Role and Self-standing set.
- The second category of specifications consists of those captured and grouped under the notions of shareable functions.

This Technical Specification applies to the second category and in particular it provides specifications for the information security technical views based on PKI (based on X.509 certificates) and/or STI (based on security tokens).

2.2 Functional block Modes and States

N/A.

2.3 Major Functional block Capabilities

Identity Management deals with digital identities as a set of characteristics asserted by one digital subject about itself in a digital realm to support authentication and authorization processes in such security domain. In SWIM-TI each ATM participant shall be request a valid digital identity in order to either expose a service (ATM SWIM Enabled Service Provider) or consume services (ATM SWIM Enabled Service Consumer).

For what concern SWIM-TI suitable digital identity options, the following taxonomy has been identified into TAD [12]:

A. X.509 Certificates (related to a Public Key Infrastructure, PKI)

B. Security Tokens (related to a Security Token Infrastructure, STI)

   B1. User Name / Password

   B2. SAML tokens

   B3. X.509 token

Option A leverages directly on the PKI to associate entities to their digital identities in the form of X.509 certificates while options B involve the adoption of the Identity Provider to manage identities lifecycle.

For what concerns technical solutions based on X.509 certificates, according to SWIM-TI TAD [12] the PKI covers the following capabilities:

- Entities registration
- Digital Certificates Management including emitting, signing, maintaining, revoking and storing,
- Revocation Lists Management
- Capability to cooperate with other PKIs, including Cross-Certification and Policy Mapping
- Key lifecycle management, including archive, update and restore keys

These capabilities are detailed in the SWIM-TI TAD [12] and briefly introduced hereafter in the document.

A PKI is composed by three core functional subsystems:

- The Certificate Authority (CA), an entity which issues certificates. One or more in-house servers, or a trusted third party (such as VeriSign), can provide the CA function.
- The repository for keys, certificates and Certificate Revocation Lists (CRLs), which is usually based on an Lightweight Directory Access Protocol (LDAP)-enabled directory service
- A management function, typically implemented via a management console.

A widespread solution is to delegate certain functions of the CA to some other optional subsystems within the PKI, i.e.:

- Registration Authority (RA) which is the administrative function in charge of registration of entities in the Public Key Infrastructure (PKI),
- Validation Authority (VA) which is the function in charge of validation of the certificates.
- CRL Issuer which is an optional component that a CA can delegate to publish CRLs.

According to SWIM-TI TAD [12] another important PKI capability is the BCA that provides the support for interconnecting trust domains by creating and revoking pair of cross-signed certificates with each of the different PKI's principal CA. By cross-signing the principal CAs on each PKI with the BCA, it's possible to create trust paths between physical or virtual machines, applications or users all over the SWIM-TI whatever are their respective PKI. It is important to consider that the BCA is not issuing and managing digital certificates and that it is only needed when different SWIM stakeholders use certificates signed by CAs that do not trust each other.

In case digital identities technical solution based on security tokens (option B) the Identity Management functions are provided by the STI and the authentication process in enabled by a trust relationships and secure interactions between STI, consumer side SWIM-TI and provider side SWIM-TI. This solution does not obviate the utilization of the PKI either in case that security tokens are digitally signed by issuing STI or that X.509 tokens are used; in both cases an interaction between the STI and the PKI is required. Moreover, transport level security controls could be applied to the interaction between the STI and its consumer. This relies mostly on TLS protocol which is enabled throughX.509 certificates.

2.4 User Characteristics

According to SWIM-TI TAD [12] several SWIM nodes (or in general SWIM-TI solutions implementing one or more SWIM profiles for which security controls based on X.509 certificates have been specified) could use one or more PKIs. General speaking cross security domains exchanges may be required. In order to manage such cross domains security interaction, the SWIM-TI TAD [12] provides several deployment options (e.g. BCA).

Similar considerations and specific deployment options are also provided for the federation of STIs. Refer to the SWIM-TI TAD [12] for further details.

2.5 Operational Scenarios

The use of the PKIs and STIs in the SWIM-TI context has been already introduced above. P14.01.04 Technical Specifications are driven by user and technical Use Cases detailed in collaboration with 14.01.03.

Furthermore, in the table here below the SESAR Enablers relevant for the SWIM-TI Identity Management are provided. The current analysis is based on the latest Data Set available in the SESAR Programme (https://www.atmmasterplan.eu/data/enablers), namely version "Data Set 15".

Enablers (Data Set 15) belonging to the SWIM Operational Focus Area (ENB02.01.01) have been analysed to evaluate their relationships (if any) with the SWIM-TI and especially with the SWIM-TI Technical Specifications. In accordance with this analysis, all the requirements have been linked to one or more applicable Enablers. The semantic of this relationship is that the realization of the traced

enabler includes the implementation of the concerning SWIM-TI requirements. It has to be noted that in many cases, the scope of the enabler is not fully covered by the SWIM-TI layer. In such cases, the full scope of the enable is covered by both the application and infrastructure layers.

Table 2-1: SESAR Enablers Relevant for SWIM-TI Identity Management TS

Enabler Code	Brief Description	Applicable SWIM Profiles / SWIM-TI Functions
GGSWIM-59c	SWIM Technical infrastructure to support transport and message level security, identity management (local and federated) to provide authentication and authorization. Also includes use of public key cryptography (PKI).	**SWIM-TI Yellow Profile (YP), Blue Profile (BP), and Purple Profile (PP) Information Security functions** **SWIM-TI Identity Management (tokens services and PKIs)**
SWIM-SUPT-03b	SWIM Technical infrastructure to support transport and message level security, identity management (local and federated) to provide authentication and authorization. Also includes use of public key cryptography (PKI). (As GGSWIM-59c but for Step 2)	**SWIM-TI Yellow Profile (YP), Blue Profile (BP), and Purple Profile (PP) Information Security functions** **SWIM-TI Identity Management (tokens services and PKIs)**
SWIM-SUPT-03a	Provision, by specific stakeholder(s) of functionality to support the use of Security Keys for use by the other stakeholders where they have need of their use to provide additional security for their provision/consumption of SWIM Service with other stakeholders.	**SWIM-TI Identity Management (tokens services and PKIs)**

2.6 Functional

2.6.1 Functional decomposition

According to the SWIM-TI TAD, the SWIM-TI PKI and SWIM-TI STI provide functionalities that are briefly summarized here below (for an exhaustive list of functionalities and corresponding descriptions refer to SWIM-TI TAD [12]).

2.6.1.1 Public Key Infrastructure

2.6.1.1.1 Entities Registration

Registration is the first step in the entity enrolment process to the CA: this is usually characterized as the process whereby an entity first makes itself known to a CA. During this step the PKI shall be able to verify the entity's identity. The rigor or "level of assurance" associated with the registration process will vary based on the associated policies. As noted above, the process of registration could be accomplished directly with the CA or through an intermediate RA. This process may also be accomplished on-line or off-line (or a combination of the two).

After registration, the PKI shall associate the entity with its key pair: key pair generation can occur in advance of the End Entity enrolment process or it can take place in response to it. Key pairs can be generated by the End Entity client system, RA, CA or some other component such as a hardware security module: more details about key lifecycle management are provided hereafter in this section.

2.6.1.1.2 Digital Certificates Management

The PKI X.509 certificates management functionalities include:

- Certificate emitting,
- Certificate signing,
- Certificate distribution,
- Certificate renewal,

- Certificate revocation,
- Certificate suspension,
- Certificate verification,
- Certificate storing.

2.6.1.1.3 Revocation List Management

The CA that issues a given set of certificates is also responsible for issuing revocation information associated with those certificates: it must revoke a certificate under certain conditions, such as compromise of a certificate's encryption keys or change in status of an encryption peer, which holds this certificate.

In order to ascertain the validity status of digital certificates presented by encryption peers, SWIM PKI accommodates this requirement by implementing two mechanisms: Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP).

OCSP (Online Certificate Status Protocol) is a real-time alternative method to Certificate Revocation Lists (CRLs) for obtaining the revocation status of an individual certificate. An end host can query the OCSP server when a cert is presented to find out if the certificate has been revoked: in order to know the status of certificate, the OCSP server can interface directly with Certificate Repository of the PKI. Alternatively the server can maintain CRLs of federated CA, raising the querying entities from the need to maintain themselves the CRLs.

2.6.1.1.4 Key Lifecycle Management

The PKI performs some functions, such as issuing a certificate and listing a certificate on a CRL, in response to a current request. In contrast, key lifecycle functions, such as updating, backing up, and archiving keys, are performed routinely. Each entity is likely to have a number of keys that require lifecycle management. Key lifecycle Management includes:

- Creation of key pairs
- Updating keys
- Archiving keys
- Backup and recovery

2.6.1.2 Security Token Infrastructure

2.6.1.2.1 Security Token Lifecycle

The SWIM-TI STI consists in a technical solution for Identity Management based on the adoption of Security Tokens (i.e. plain text username/password, X.509 certificate-based token and SAML token) as means to provide Digital Identity of parties involved in SWIM-TI authenticated information exchange. The main responsibilities for STI is to manage lifecycle of Security Token in terms of:

a. Issuing
b. Validation
c. Renewal
d. Cancellation

2.6.1.2.2 Identity Store

Data and metadata associated to Digital Identities are maintained in the Identity Store (a.k.a. Identity Repository) consisting of a system which provides persistence of identity information and CRUD operations. The Identity Store represents also the abstraction layer to access identity entries in the Identity Management function. In order to enable fine grained access control mechanisms (e.g. ABAC or RBAC), the STI shall allow to associate different attributes to a digital identity and to classify identities into groups, roles and organization.

2.6.1.2.3 Blacklisting Mechanism

The STI provides and manages a blacklisting security mechanism, in case that e digital identities were compromised by a cyber-attack or because some entity undertakes a malicious behaviour. In case that an identity is placed in blacklist, this event should be distributed within the federated STI. Moreover, mechanisms to remove a digital identity from the blacklist shall be provided.

2.6.2 Functional analysis

Refer to SWIM-TI TAD [12].

2.7 Service View

N/A.

3 Functional and non-Functional Requirements

In this chapter functional, non-functional and interface requirements are provided. The chapter is organized in several sub-chapters. The first level of decomposition is between requirements that apply to both PKI and STI (§3.1) – or in general to the SWIM Node at a whole - and those that are specific of a PKI (§3.2) or STI (§3.3).

The second level of decomposition is between functional, non-functional and interface requirements. Sub-chapters §3.2 and §3.3 are structured as follows:

- Functional requirements (§3.X.1).
- Non-functional requirements, which include the following NFRs:
  - Adaptability (§3.X.2), which contains requirements related to growth and expandability.
  - Performance Characteristics (§3.X.3), which contains requirements concerning capacity, accuracy, timing performances, software resource usage, etc..
  - Safety and Security (§3.X.4), which contains security and privacy requirements, including access limitations, data protection and recovery methods; it also includes safety requirements(according to the safety analysis based on respective standards – when available).
  - Maintainability (§3.X.5), which contains quantitative maintainability requirements.
  - Reliability (§3.X.6) which contains requirements concerning the robustness to abnormal operating conditions.
  - Internal Data Requirements (§3.X.7).
  - Design and Construction Constraints (§3.X.8).
- Interface requirements (§3.X.9), which contains the specification of the interfaces (including external, internal and network bindings).

If in one or more sub-sections of §3.2 and §3.3, no requirements concerning a given category (e.g. Design and Construction Constraints) are provided, all those (if any) included in the concerning §3.1 section (e.g. §3.1.2) are applicable. This approach has been adopted to avoid the duplication of (similar) requirements.

The third level of decomposition concerns the NFRs: all the sections have been organized according to NFR characteristics and sub-characteristics defined in the ISO/IEC 25010:2011. For instance, §3.X.3 (Performance Characteristics) has been traced to ISO/IEC 25010:2011 “Performance efficiency” NFR characteristic. According to that, §3.X.3 has been decomposed by providing a section for each ISO/IEC 25010:2011 “Performance efficiency” sub-characteristics (i.e. time behaviour, resource utilization and capacity requirements). The adoption of ISO/IEC 25010:2011 as reference is coherent and consistent with the SWIM Profiles definition [13].

The interface requirements sections section (§3.X.9) has been decomposed according to interface binding kinds described in the TAD [12]. In particular, when applicable, following decomposition is adopted:

- Internal Service Interface bindings, which contains the specifications concerning the “Internal Service Binding”. This kind of binding is internal to the SWIM-TI only and related to any such internal service (e.g. PKI services).

- Network Interface bindings, which contains the specifications concerning the “Network Binding”. This kind of binding is external to the SWIM-TI and related to the Network only.
- External Service Interface bindings, which contains the specifications concerning the “External Service Binding”. This kind of binding is external to the SWIM-TI and not a <Service binding> or a <Network binding> (e.g. Time Service).

A given binding of type “Internal Service Binding” or “External Service Binding” relies on one specific “Network Binding” (traced in the concerning REQ Trace table).

For additional details about SWIM-TI TSs requirements guidelines and the mapping between ISO/IEC 25010:2011 characteristics and TS table of content, refer to [14].

3.1 General Interoperability Requirements

In this section interoperability requirements applicable to both PKIs and STIs are provided.

3.1.1 Common Time

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0010
Requirement	The SWIM-TI shall use a Common Time Reference (CTR) for non-functional (e.g. Time performances) and functional characteristics where a common time reference is needed locally by SWIM-TI and by federated Security Domains.
Title	SWIM-TI Time Service
Status	<Validated>
Rationale	For the SWIM environment, each SWIM-TI function that uses time information must be synchronised to a time reference that satisfies precision requirements. For instance, security and identity tokens are checked for freshness in order to ensure that they are still within their valid lifetimes. This requires time synchronization between federated security domains. Another security related example where time synchronization is needed is exchanging of audit information. The time synchronization is important across a distributed environment and not only for security purpose. In fact this is also required for the information gathered and exchanged by the SWIM-TI Recording. According to this, Time Service can be seen as a SWIM-TI service used by several Functions and not only by Security. The time synchronization also plays an important role in WS-ReliableMessaging and in DDS. This requirement covers NIST security control AU-8.
Category	<Design><Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>

<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

3.1.2 Standards

This section introduces, in the scope of both PKI and STI, the standards that are applicable to Interfaces through which interoperability is provided or required with and for participants that are external to the SWIM-TI as well as participants that are internal to the SWIM-TI.

Each technical configuration at the level of such Interfaces that requires adherence to one or more standards, in order to support and promote interoperability, includes these standards by referencing the standards in this section.

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0180
Requirement	IETF 5905 Proposed Standard, Network Time Protocol Version 4: Protocol and Algorithms Specification https://tools.ietf.org/html/rfc5905 shall be supported.
Title	Interoperability standard. NTP
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control AU-8.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>

<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0103
Requirement	IETF RFC 791 Internet Protocol September 1981 http://tools.ietf.org/html/rfc791 shall be supported.
Title	Interoperability standard. IPv4 RFC 791
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0104
Requirement	IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification December 1998 http://tools.ietf.org/html/rfc2460 shall be supported.
Title	Interoperability standard. IPv6 RFC 2460
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes

	interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0275
Requirement	IETF RFC 7568 Deprecating Secure Sockets Layer (SSL) Version 3.0 June 2015 https://tools.ietf.org/html/rfc7568 shall be supported.
Title	Interoperability standard. Prohibit SSL V3.0 RFC 7568
Status	<Validated>
Rationale	The SSLv3 protocol has been subject to a long series of attacks, both on its key exchange mechanism and on the encryption schemes. In SWIM-TI support of its predecessor is already prohibited according to RFC6176 (see REQ-14.01.04-TS-0811.0114). After the discovery of the Poodle Attack (https://www.openssl.org/~bodo/ssl-poodle.pdf) the use of SSL v3.0 shall be considered deprecated. At the time of writing (June 2016) the IETF RFC 7568 is a PROPOSED STANDARD.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider><Network provider>

Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0166
Requirement	IETF RFC 6434, Memo, IPv6 Node Requirements, December 2011 http://tools.ietf.org/html/rfc6434 shall be supported in the following manner: Reference to this specification is equivalent to inclusion of all protocol functions described in this document.
Title	Interoperability standard. IPv6 Node Requirements
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A

<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0169
Requirement	IETF RFC 792 Internet Standard, INTERNET CONTROL MESSAGE PROTOCOL, September 1981 http://tools.ietf.org/html/rfc792 shall be supported.
Title	Interoperability standard. ICMP
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>

<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0170
Requirement	IETF RFC 950, Internet Standard, Internet Standard Subnetting Procedure, August 1985 http://tools.ietf.org/html/rfc950 shall be supported.
Title	Interoperability standard. Internet Standard Subnetting Procedure
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0168
Requirement	IETF RFC 1122 Internet Standard, Requirements for Internet Hosts -- Communication Layers, October 1989 http://tools.ietf.org/html/rfc1122 shall be supported.

Title	Interoperability standard. Requirements for Internet Hosts -- Communication Layers
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0101
Requirement	IETF RFC 793 Transmission Control Protocol September 1981 http://tools.ietf.org/html/rfc793 shall be supported.
Title	Interoperability standard TCP RFC 793
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>

Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0111
Requirement	IETF RFC 2246 The TLS Protocol Version 1.0 January 1999 http://tools.ietf.org/html/rfc2246 shall be supported.
Title	Interoperability standard. TLS1.0 RFC 2246
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A

<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0115
Requirement	IETF 2616 Hypertext Transfer Protocol -- HTTP/1.1 June 1999 http://tools.ietf.org/html/rfc2616 shall be supported.
Title	Interoperability standard. HTTP 1.1 RFC 2616
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Messaging Bridging>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0112
Requirement	IETF RFC 4346 The Transport Layer Security (TLS) Protocol Version 1.1 April 2006 http://tools.ietf.org/html/rfc4346 shall be supported.
Title	Interoperability standard. TLS1.1 RFC 4346
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-13
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0113
Requirement	IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2 August 2008 http://tools.ietf.org/html/rfc5246 shall be supported.
Title	Interoperability standard. TLS1.2 RFC 5246
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-13
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Core>

Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0114
Requirement	IETF RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0 March 2011 http://tools.ietf.org/html/rfc6176 shall be supported.
Title	Interoperability standard. Prohibit SSL V2.0 RFC 6176
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-13
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Core><BP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A

<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0116
Requirement	IETF informational RFC 2818 HTTP Over TLS May 2000 http://tools.ietf.org/html/rfc2818 shall be supported.
Title	Interoperability standard. HTTP over TLS
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Messaging Bridging>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0230
Requirement	IETF RFC 4033 Domain Name System Security Extensions (DNSSEC) March 2005 https://tools.ietf.org/html/rfc4033 shall be supported.
Title	Interoperability standard DNSSec
Status	<In Progress>
Rationale	DNSSec is a well-known and widely used standard allowing to perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. Support for this standard promotes interoperability. This requirement complies with REQ-14.02.02-TS-ACCO.0061 in 14.2.2.D26. This requirement covers NIST security control SC-21.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0811.0240
Requirement	IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework November 2003 https://www.ietf.org/rfc/rfc3647.txt shall be supported.
Title	Interoperability standard. RFC 3647

Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. RFC 3647 provides a standardized outline and explanatory text for defining certificate policies (CP) and certificate practice statements (CPS).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<ICD><Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0250
Requirement	Security Requirements for Cryptographic Modules US Federal Information Processing Standard (FIPS 140-2) May 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf shall be supported.
Title	Interoperability standard. FIPS 140-2
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. FIPS 140-2 provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of cryptographic modules.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Analysis>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A

<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

3.1.3 Safety & Security

This section includes safety and security requirements applicable to both STI and PKI.

[IREQ]

Identifier	REQ-14.01.04-TS-0411.0040
Requirement	The SWIM-TI Administrative Consoles remote connections shall be established using only encrypted VPN connections.
Title	Remote connection for administration console
Status	<In Progress>
Rationale	SWIM-TI provides different functions that need to be managed and tuned by human users. For this reason administrative console can be attached to SWIM-TI to control one or more SWIM Functions. Technical details of such consoles depend on implementation choices (e.g. shell or graphical interfaces) but each console shall guarantee a certain level of security and compliance with current regulations. This requirement ensures that SWIM-TI Administration Console communicating through external networks (e.g., the Internet) enhances confidentiality and integrity over remote connections using encrypted virtual private networks (VPNs). This requirement covers NIST Security Control 800.53, AC-17 and SC-11.
Category	<Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><BP FDD>
Domain of interest	<SLA><Governance>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance

<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	SWIM-TI	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0612
Requirement	The SWIM-TI Audit shall allow to audit encryption and decryption attempts according to the specific Audit policy.
Title	Policy Based Encryption and Decryption attempts auditing
Status	<In Progress>
Rationale	Encryption and decryption attempts (successfully or not performed) can be audited or not according to a specific Audit policy. This requirement covers NIST security control AU-2 a.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><BP Core><PP Core>
Domain of interest	<Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0641
Requirement	The SWIM-TI Audit shall audit message signature and signature validation attempts according to the specific audit policy.
Title	Policy Based Message signature generation and validation attempts auditing
Status	<Validated>
Rationale	Data signature generation and validation attempts (successfully or not performed) have to be audited. The need for audit or not of the message signature and attempts (successful or not) can be determined according to an Audit Policy. This requirement covers NIST security controls AC-6 (9) and AU-2 a.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><BP Core><PP Core>
Domain of interest	<Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0780
Requirement	The SWIM-TI Security shall record events with all additional data specified in the applicable service-specific Audit Policy.
Title	Audit's service-level specific logging

Status	<Validated>
Rationale	The existence of service-specific Audit policies may supplement/override the Global (default) Audit policy. This requirement ensures that any additional data required by these Policies gets logged. This requirement covers NIST security controls AU-12 and AU-3 (1).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><BP Core><PP Core>
Domain of interest	<Governance><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0900
Requirement	The SWIM-TI Audit Policy shall at least include the following information: - The information which need to be recorded, - The user roles that must be provided with audit records, - The frequency of reporting or event type triggering the audit.
Title	Audit Policy Minimal Content
Status	<In Progress>
Rationale	To enable the auditing process every security related event needs to be logged with all the additional information specified by the applicable Audit Policy. This requirement covers the following NIST security controls: SI-4e, SI-4 g.
Category	<Design><Functional><Security>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<Governance>

Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0512
Requirement	The Audit Policy shall be enforced after a Demand of Identity and Authentication Information Assertion.
Title	Authenticate Identity's Audit Policy Enforcement
Status	<Validated>
Rationale	To enable the auditing process every security related event needs to be logged with all the additional information specified by the applicable Audit Policy. This requirement ensures that the Audit Policy is enforced after a Demand of Identity and Authentication Information Assertion. This requirement covers NIST security controls AC-17 (1), AU-2 a , SI-4 g.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><BP Core>
Domain of interest	<Governance>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0411.0090
Requirement	Access control to SWIM-TI management functionalities shall be granted leveraging on RBAC mechanisms.
Title	Partitioning of functionalities
Status	<In Progress>
Rationale	Management functionalities include, for example, functions necessary to administer databases, network components, workstations, or servers typically require privileged user access. In order to allow access only to authorized users, SWIM-TI shall use an RBAC model to gain access to management functionalities. This requirement covers NIST security control SC-2
Category	<Security><Design>
Validation Method	
Verification Method	<Review of Design><Analysis>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD><Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	SWIM-TI	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>

<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0411.0100
Requirement	Access control to SWIM-TI security functionalities shall be implemented according to least privilege principle and leveraging on RBAC mechanisms.
Title	Security function isolation
Status	<In Progress>
Rationale	This requirement is necessary to protect the integrity of security related functionalities of SWIM-TI. Security functionalities include, for example, functions necessary to configure PKI services, administer Identity Store and define and enforce Security Policies. These functionalities typically require privileged user access. This requirement covers NIST Security Control SC-3.
Category	<Security><Design>
Validation Method	
Verification Method	<Review of Design><Analysis>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD><Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	SWIM-TI	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0411.0110
Requirement	Network connections associated with a communications session shall be

	terminated at the end of the session or after a policy defined amount of time, to prevent unauthorized access to the system.
Title	Network connection Shutdown
Status	<In Progress>
Rationale	Unneeded network connections are potential security breaches as they may be used by unauthorized bystanders. Terminations of such connections minimizes this risk, e.g. when maintenance operations are on-going. This requirement covers NIST security control SC-1.
Category	<Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer><Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	SWIM-TI	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0930
Requirement	The SWIM-TI Security shall provide tamper-proof storage of sensitive information by applying encryption and digital signature.
Title	Supporting tamper-proof information storage
Status	<In Progress>
Rationale	Certain types of information used in aviation must be secured so as to be tamper-proof. This can include certain logs for example. Tamper-proofing means that the information will be available and uncompromised for a long period of time – at least 50 years. Tamper-proof information storage is a vital aspect of non-repudiation in aviation and is achieved applying cryptographic techniques such as digital signature. This requirement complies with REQ-14.02.02-TS-SGOV.0110 and REQ-

	14.02.02-TS-ACCO.0020 and ensures coverage of NIST SP 800 53 security control SC-28.
Category	<Design><Functional><Security>
Validation Method	
Verification Method	<Review of Design><Analysis>
Profile Part	<YP Advanced><BP Core>
Domain of interest	<Governance><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0940
Requirement	The SWIM-TI Security shall allow to maintain sensitive information in an uncompromised condition for a configurable number of days to be defined either by policy or application level configuration.
Title	Sensitive information preservation
Status	<In Progress>
Rationale	Certain types of information used in aviation must be secured so as to be tamper-proof. This can include certain logs for example. Tamper-proofing means that the information will be available and uncompromised for a long period of time – at least 50 years. Tamper-proof information storage is a vital aspect of non-repudiation in aviation and is achieved applying cryptographic techniques such as digital signature. This requirement complies with REQ-14.02.02-TS-SGOV.0110 and REQ-14.02.02-TS-ACCO.0020 and ensures coverage of NIST SP 800 53 security control SC-28.
Category	<Design><Functional><Security>
Validation Method	
Verification Method	<Review of Design><Analysis>
Profile Part	<YP Advanced><BP Core>
Domain of interest	<Governance><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity

	Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0402.0030
Requirement	SWIM-TI audit logs shall be stored in a secure storage.
Title	Safe storage for audit logs
Status	<In Progress>
Rationale	Audit logs includes all information needed to successfully audit information system activity, therefore audit logs and audit tools shall 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 Security Policies to grant access to audit logs, while physical protection is addressed by media protection controls and physical and environmental protection controls. This requirement covers NIST security control AU-9.
Category	<Security>
Validation Method	
Verification Method	<Review of Design><Analysis>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<SLA><Governance>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	SWIM-TI	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>

<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0402.0040
Requirement	SWIM-TI audit data shall be stored in a storage location remote and independent from the system generating the audit data.
Title	Remote and independent storage for audit logs
Status	<In Progress>
Rationale	Audit logs need to be stored in an independent and remote system. This requirement helps to ensure that a compromise of a system being part of SWIM-TI does not also result in a compromise of the corresponding audit records. This requirement covers NIST security control AU-9 (2).
Category	<Security>
Validation Method	
Verification Method	<Review of Design><Analysis>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<SLA><Governance>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	SWIM-TI	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>

<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0802.0020
Requirement	The SWIM-TI cryptographic modules shall be developed in accordance with Level 3 of Security Requirements for Cryptographic Modules US Federal Information Processing Standard (FIPS 140-2).
Title	Conformance to Level 3 of US FIPS 140-2.
Status	<In Progress>
Rationale	The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. Given the nature of the air traffic services environment development should be to the equivalent of US Federal Information Processing Standard (FIPS) 140 Level 3.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Analysis>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Applicable but not testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-12	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ 029	<Full>
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0250	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<ALLOCATED TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0020
Requirement	The SWIM-TI Identity Management deployment options and configurations shall be in accordance with standardized PKI and STS profiles.
Title	Standardized PKI and STS Profiles
Status	<In Progress>
Rationale	PKI and STS technologies allow for many options and configurations and include provisions for extensibility. The induced technical flexibility, as well as the multiple possible ways of using these technologies (defined by regional/State regulations, laws, policies) might lead to interoperability issues. This variability can be reduced by mandating the definition of, and the compliance of PKI/STS implementations to standardized profiles. States/Regions must contribute to the definition of these Profiles under the ICAO coordination.
Category	<Design><Security><Interoperability>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0414.0010
Requirement	The SWIM-TI Identity Management shall be protected against overload resulting from Denial of Service attack or services utilisation above maximum levels.
Title	SWIM-TI Identity Management overload protection
Status	<In Progress>
Rationale	This requirement aims at ensuring that the SWIM Identity Management is protected against overload due to attacks or to legitimate, but above thresholds, use of services; for instance number of concurrent accesses could be limited. This requirement covers NIST Security Control 800.53 AC-10.This requirement covers NIST security controls SC-5 (2), SC-5 (3) and AC-10.
Category	<Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>

Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.1.4 Interface Requirements

This section includes interface requirements applicable to both PKI and STI.

3.1.4.1 External Service Interface Bindings

[IREQ]

Identifier	REQ-14.01.04-TS-0901.0324
Requirement	SNTP shall be instantiated over UDP using the following binding. + MEPs: as defined by standard + Fault handling: as defined by standard + Encoding. - as defined per standard + Security: - Confidentiality: none - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: - formalism of contract description: as defined by standard - minimum: not applicable - reference: as defined by standard + Interoperability: none
Title	Interface binding. SNTP over UDP.
Status	<In Progress>
Rationale	SNTP supports a system for provision of a common time reference. While the level of accuracy and reliability provided through SNTP can be very high (e.g. precision of a few milliseconds can be demonstrated), depending on the context this cannot always be guaranteed.
Category	<Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<External service binding>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0102	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0180	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0010	<Full>

<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

3.1.4.2 Internal Service Interface Bindings

There are no internal interfaced applicable to both PKI and STI.

3.1.4.3 Network Interface Bindings

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0201
Requirement	Network Technical Interface shall be instantiated according to the following binding + IP Unicast IPv4 + Mapping IP to IP + Security: - Confidentiality: none - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: none + Interoperability: none
Title	IP Unicast IPv4
Status	<Validated>
Rationale	Basic Unicast IPv4 binding
Category	<Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Network binding>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0103	N/A

<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0168	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0169	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0170	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0171	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0010	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0010.0090	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0100	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0302	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0303	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0801	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0317	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0318	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0800	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0802	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0803	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0324	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0325	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0327	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0328	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0050	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0332	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0020	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0807	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0806	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0805	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0804	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0040	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0020	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0160	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0170	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0202
Requirement	Network Technical Interface shall be instantiated according to the following binding: + IP Unicast IPv6 + Mapping IP to IP + Security: - Confidentiality: none

	- Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: none + Interoperability: none
Title	IP Unicast IPv6
Status	<In Progress>
Rationale	Basic Unicast IPv6 binding
Category	<Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Network binding>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0104	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0168	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0010	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0010.0090	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0100	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0302	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0303	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0801	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0317	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0318	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0800	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0802	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0803	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0324	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0325	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0327	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0328	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0050	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0332	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0020	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0710	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0720	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0807	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0806	N/A

<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0805	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0804	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0001	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0020	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0160	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0170	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0209
Requirement	Network Technical Interface shall be instantiated according to the following binding: + IP Unicast IPv4 with network security + Mapping IP to IP + Security: - Confidentiality: network - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: none + Interoperability: none
Title	IP Unicast IPv4 with network security
Status	<In Progress>
Rationale	Basic Unicast IPv4 binding with network security
Category	<Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Network binding>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0102	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0103	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0168	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0169	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0170	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0171	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0010	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0030	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0010.0090	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0100	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0302	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0303	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0801	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0317	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0318	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0324	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0327	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0328	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0050	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0332	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0020	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0040	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0020	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0060	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0160	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0170	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0210
Requirement	Network Technical Interface shall be instantiated according to the following binding: + IP Unicast IPv6 with network security + Mapping IP to IP + Security: - Confidentiality: network - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: none + Interoperability: none
Title	IP Unicast IPv6 with network security

Status	<In Progress>
Rationale	Basic Unicast IPv6 binding with network security
Category	<Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Network binding>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0102	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0104	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0168	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0010	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0030	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0010.0090	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0100	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0302	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0303	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0801	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0317	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0318	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0324	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0327	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0328	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0050	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0901.0332	N/A
<APPLIES_TO>	<ATMS Requirement>	REQ-14.01.04-TS-0914.0020	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0001	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0020	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0060	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0160	<Full>
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0910.0170	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

3.1.4.4 Network Requirements

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0001
Requirement	The Communication Network Infrastructure shall provide IPv6 support.
Title	Communication Network Infrastructure IPv6 support

Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN). Taking into account the overall context, the large number of interconnected systems, performance and Quality of Service (QoS) the adoption of IPv6 at network level is needed.
Category	<Interface>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-1	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0040
Requirement	The Communication Network Infrastructure shall provide IPv4 support.
Title	Communication Network Infrastructure IPv4 support
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN). Taking into account the overall context, the large number of interconnected systems generally belonging to several different networks adoption of IPv4 at network level is needed.
Category	<Interface>

Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-4	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0010
Requirement	The Communication Network Infrastructure shall provide IP routing.
Title	Communication Network Infrastructure IP routing support
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN). Taking into account the overall context and the large number of interconnected systems generally belonging to several different IP networks the support of IP routing at network level is needed.
Category	<Interface>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>

Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-2	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0020
Requirement	The Communication Network Infrastructure shall allow to use Transfer Control Protocol (TCP).
Title	Communication Network Infrastructure TCP support
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN). Taking into account the overall context and the large number of interconnected systems which need to exchange information in efficient and reliable manner, the support of TCP protocol at network level is needed.
Category	<Interface><Reliability>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-3	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A

<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0030
Requirement	The Communication Network Infrastructure shall provide encryption capabilities (network level security).
Title	Communication Network Infrastructure encryption support
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN). Taking into account the overall context and the sensitivity of the exchanged data for security reasons encryption and decryption techniques support at network level is needed. This requirement covers NIST security controls SC-8 (1) and SC-11.
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-12	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>

<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

3.2 PKI Functional and non-Functional Requirements

3.2.1 Capabilities

The PKI is responsible for signing, emitting and maintaining certificates and revocation lists. It is expected that each stakeholder participating in SWIM is able to provide this facility directly or indirectly. In the first case, a given stakeholder already has this facility whereas in the second case it relies (PKI provided indirectly) on a PKI provided by a third party (e.g. managed and owned at regional level). Digital certificates provided by PKI are used (when needed) for digital signature, encryption, authentication and authorization.

[REQ]

Identifier	REQ-14.01.04-TS-0014.0010
Requirement	The PKI shall provide X.509 certificates management functionality that includes: - Certificate emitting. - Certificate signing. - Certificate distribution, - Certificate renewal. - Certificate revocation. - Certificate suspension. - Certificate verification. - Certificate storing.
Title	SWIM Technical Infrastructure PKI functionalities
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level. Certificates constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Digital certificates must satisfy the following requirements: - a certificate contains the public key and an ID of its owner. - a certificate is issued by a Certificate Authority (CA). The certificate is digitally signed by the CA with its own private key and a timestamp. Only a CA can issue certificates and update them. - each participant can check the validity of a certificate he has received, and properly interpret its content. To do so, a participant uses the CA public key with the proper verification algorithm (RSA, DSS) and then checks the timestamp. - a certificate can be revoked by a CA, possibly upon request of the certificate's owner. X.509 is by far the most widespread certificate format.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-6	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ_032	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0021
Requirement	The PKI shall manage and distribute certificates emitted, signed and verified by a trusted Certification Authority.
Title	SWIM Technical Infrastructure PKI Certificates and CA
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level. Certificates constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Digital certificates must satisfy the following requirements: - a certificate contains the public key and an ID of its owner. - a certificate is issued by a Certificate Authority (CA). The certificate is digitally signed by the CA with its own private key and a timestamp. Only a CA can issue certificates and update them. - each participant can check the validity of a certificate he has received, and properly interpret its content. To do so, a participant uses the CA public key with the proper verification algorithm (RSA, DSS) and then checks the timestamp. - a certificate can be revoked by a CA, possibly upon request of the certificate's owner. X.509 is by far the most widespread certificate format.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-6	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ_032	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>

<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0030
Requirement	The PKI shall provide revocation list management functionality.
Title	SWIM Technical Infrastructure PKI Revocation List Management
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level. Certificates constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Digital certificates must satisfy the following requirements: - a certificate contains the public key and an ID of its owner. - a certificate is issued by a Certificate Authority (CA). The certificate is digitally signed by the CA with its own private key and a timestamp. Only a CA can issue certificates and update them. - each participant can check the validity of a certificate he has received, and properly interpret its content. To do so, a participant uses the CA public key with the proper verification algorithm (RSA, DSS) and then checks the timestamp. - a certificate can be revoked by a CA, possibly upon request of the certificate's owner. X.509 is by far the most widespread certificate format.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-6	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ_032	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0080
Requirement	The PKI shall allow consumers to access resources using the same X.509 certificate (i.e. digital identity) within federated security domains.
Title	Federated access via PKI
Status	<In Progress>
Rationale	In the heterogeneous environment of systems and stakeholders of SWIM-TI, a federated single sign-on for authentication can greatly simplify the

	difficulties associated to a user consumption of services from a different security domain. This requirement covers NIST security controls IA-2 (10) and IA-4 (6).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0090
Requirement	The PKI shall update CRLs and notify changes to Federated PKIs if certificate for an entity of the Federated Security System is revoked.
Title	Federated blacklisted entities
Status	<In Progress>
Rationale	Authentication blacklists are to be part of auditing to prevent further authentication attempts by blacklisted entities. SWIM-TI Security System will notify a Federated Security System of a blacklisted entity. This defines some minimal requirements the Authorization Policy shall obey. This requirement is complemented by REQ-14.01.04-TS-0014.0050 (OCSP). This requirement covers NIST security controls SI-5 c and CA-3 (5).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>

<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0100
Requirement	The SWIM-TI Security shall provide a blacklisted entity in a Federated Security System with a new valid certificate according to one of the following mechanism: + Automatically after a Policy defined maximum blacklist period. + Manually.
Title	New certificate mechanisms for blacklisted entities
Status	<In Progress>
Rationale	Authentication blacklists are to be part of auditing to prevent further authentication attempts by blacklisted entities. SWIM-TI Security System needs to provide the appropriate mechanisms to release previously blacklisted entities. This requirement covers NIST security controls SI-5 c and CA-3 (5).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0110
Requirement	The PKI shall allow to establish a direct trust relationship with PKI from a different security domain by means of a shared Certification Authority
Title	SWIM Technical Infrastructure direct PKI trust relationship.
Status	<In Progress>
Rationale	Digital Certificates issued by a Certificate Authority (CA) constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. To enable secure interaction among entities belonging to different security domains, i.e. using different PKIs, a trust relationship between such PKIs can be established by sharing the same CA. The trusted CA may be also a BCA.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>

Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0120
Requirement	The PKI shall allow to establish hierarchical trust relationship with another PKI.
Title	SWIM Technical Infrastructure hierarchical PKI trust relationship.
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level. Digital Certificates issued by a Certificate Authority (CA) constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Within an enterprise, Certification Authorities are usually organized as a hierarchical tree of related CAs. Root CA issues certificates to subordinate CAs. Subordinates CAs issues certificates to CAs below them in the hierarchy, or end users.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0041
Requirement	The PKI shall use BCA to enable a trust relationship with another PKI which is not directly trusted.
Title	SWIM Technical Infrastructure PKI trust relationship through BCA

Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level. Certificates constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Digital certificates must satisfy the following requirements: - a certificate contains the public key and an ID of its owner. - a certificate is issued by a Certificate Authority (CA). The certificate is digitally signed by the CA with its own private key and a timestamp. Only a CA can issue certificates and update them. - each participant can check the validity of a certificate he has received, and properly interpret its content. To do so, a participant uses the CA public key with the proper verification algorithm (RSA, DSS) and then checks the timestamp. - a certificate can be revoked by a CA, possibly upon request of the certificate's owner. X.509 is by far the most widespread certificate format.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-6	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ_032	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0050
Requirement	The PKI shall implement an OCSP (Online Certificate Status Protocol) server to provide revocation status of X.509 certificates.
Title	SWIM Technical Infrastructure PKI OCSP support
Status	<In Progress>
Rationale	Certificates constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Digital certificates must satisfy the following requirements: - a certificate contains the public key and an ID of its owner. - a certificate is issued by a Certificate Authority (CA). The certificate is digitally signed by the CA with its own private key and a timestamp. Only a CA can issue certificates and update them. - each participant can check the validity of a certificate he has received, and

	properly interpret its content. To do so, a participant uses the CA public key with the proper verification algorithm (RSA, DSS) and then checks the timestamp. - a certificate can be revoked by a CA, possibly upon request of the certificate's owner. X.509 is by far the most widespread certificate format. OCSP (Online Certificate Status Protocol) is areal-time alternative method to Certificate Revocation Lists (CRLs) for obtaining the revocation status of an individual certificate.An end host can query the OCSP server when a certificate is presented to find out if the certificate has been revoked: in order to know the status of certificate, the OCSP server can interface directly with Certificate Repository of the PKI. Alternatively, the server it can maintain CRLs of federated CA, raising the quering entities from the need to maintain themselves the CRLs.
Category	<Functional><Interface><Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0060
Requirement	The PKI shall use an PKCS12 archive file format to bundle and distribute X.509 certificates and private keys.
Title	SWIM Technical Infrastructure PKI PKCS2 support
Status	<In Progress>
Rationale	Certificates constitute the main device utilized by entities participating in a PKI to check authenticity of received information, such as identity of a user and of its public key. Digital certificates must satisfy the following requirements: - a certificate contains the public key and an ID of its owner. - a certificate is issued by a Certificate Authority (CA). The certificate is digitally signed by the CA with its own private key and a timestamp. Only a CA can issue certificates and update them. - each participant can check the validity of a certificate he has received, and properly interpret its content. To do so, a participant uses the CA public key with the proper verification algorithm (RSA, DSS) and then checks the timestamp. - a certificate can be revoked by a CA, possibly upon request of the certificate's owner. X.509 is by far the most widespread certificate format. PKCS#12 (Personal Information Exchange Syntax Standard) specifies a portable format for storing or transporting a user's private keys, certificates

	and miscellaneous secrets under several privacy andintegrity modes. The PKI shall use this standard to bundle entities'certificates and private keys.
Category	<Functional><Interface><Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0070
Requirement	The PKI shall provide an identity store in order to store (create/update/delete) X.509 certificates and CRL.
Title	X.509 Certificates and CRL Store
Status	<In Progress>
Rationale	Identity repository/directory is used to store persistently digital identities and any relevant identity attributes. This requirement covers NIST security controls IA-4 c, IA-4 d and IA-4 e.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0015.0010
Requirement	The BCA shall be able to establish a trust path between CAs which do not trust each other.

Title	SWIM BCA purpose
Status	<In Progress>
Rationale	It is anticipated that security of the European SWIM-TI will not be handled by a single certificate authority or even by a single hierarchy of certificate authorities. Organisations (e.g. CFMU and some Airlines) already deployed a PKI with an associated third party CA (or Certificate Service Provider (CSP)).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0015.0020
Requirement	The BCA shall provide functionalities to manage the list of trusted CAs.
Title	SWIM BCA and trusted CAs
Status	<In Progress>
Rationale	It is anticipated that security of the European SWIM-TI will not be handled by a single certificate authority or even by a single hierarchy of certificate authorities. Organisations (e.g. CFMU and some Airlines) already deployed a PKI with an associated third party CA (or Certificate Service Provider (CSP)).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0014.0130
Requirement	All CAs (e.g. SWIM-TI BCA, Root CA, etc.) shall establish a Certificate Practice Statement determining mandatory and consistent practices regarding: Issuance, Publication, Archiving, Revocation, Renewal of certificates.
Title	CAs Certificate Practice Statement.
Status	<In Progress>
Rationale	A Certificate Practice Statement provides the applicable practices and rules to be followed by a Certification Authority regarding the management of Public Key Certificates.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0240	N/A

[REQ]

Identifier	REQ-14.01.04-TS-0015.0040
Requirement	The BCA shall cross-sign the Principal CA of a PKI if and only if it complies with its Certificate Practice Statement (CPS).
Title	CPS compliance for cross-certification
Status	<In Progress>
Rationale	In order to establish trust paths between different PKIs it's necessary to comply with the Bridge Certification authority CPS, to ensure an homogeneous management of certificates across heterogeneous PKIs.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.2 Adaptability

This section includes adaptability requirements as documented in ISO/IEC 25010:2011. In particular, requirements included in this section refer to adaptability sub-characteristic of portability NFRs.

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.3 Performance Characteristics

This section includes performance efficiency requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with performance efficiency NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.2.3.1) time behaviour, (§3.2.3.2) resource utilization and (§3.2.3.3) capacity.

3.2.3.1 Time behaviour Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0214.0010
Requirement	The LDAP Based X509 CRLs retrieval response time shall be as follows: + Measurements: - 90% of the requests <= 2 s - 98% of the requests <= 4 s + Measurement conditions: - Authentication (mutual), Authorization, Integrity and Confidentiality at transport level. - Full load, no overload. - Network characteristics: throughput of 100Mb/s, average latency of 200ms. - Session setup, session reuse or session creation time excluded from the measurements.
Title	LDAP Based X509 CRLs retrieval average response time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average response time in the provided conditions for LDAP based CRL Distribution Points (CDPs). CRLs fetching is periodically done in parallel with domain specific exchanges (e.g. send Flight Data, request Weather data). The on-line verification of the certificates used in such exchanges consists in checking locally stored CRLs previously (and periodically) retrieved through the LDAP CDPs (in this case). There is a complex relationship between this requirement and the CRL max size, validity period, use of Delta CRLs and CRL partitioning. This requirement is a top level one from which a number of CRLs related requirements and constraints are derived from (e.g. ranges for the validity period, the use of Delta CRLs, etc.). Measurements. Measured response time is as defined by SWIM Profile WP_PRF_01 NFR and in particular it represents a round-trip time including time spent over the network. Measurement Conditions. Provided measurements do not differentiate between the case of use of full CRLs or Delta CRLs and they do not take into account LDAP replication schema that may be used to improve performances. The presence of security controls (Authentication, Authorization, Integrity and Confidentiality at transport level) in the measurement conditions, reflects that these response times shall be met when all of these controls are active and performed during a request/response. Authentication at transport level may be part of a session setup: in such case the time spent for the Authentication at transport level will not be taken into account for targeted measurement (session reuse or session creation time excluded from the measurements). Average response time is measured relying on a network infrastructure having the provided

	characteristics (throughput of 100Mb/s and average latency of 200ms).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0214.0040
Requirement	The LDAP Based X509 CRLs retrieval request processing time shall be as follows: + Measurements: - 90% of the requests <= 20 ms - 98% of the requests <= 40 ms + Measurement conditions: - Full load, no overload.
Title	LDAP Based X509 CRLs retrieval request average processing time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average processing time in the provided conditions for LDAP based CRL Distribution Points (CDPs). There is a complex relationship between this requirement and the CRL max size, validity period, use of Delta CRLs and CRL partitioning. This requirement is a top level one from which a number of CRLs related requirements and constraints are derived from (e.g. ranges for the validity period, the use of Delta CRLs, etc.). Measurements. Processing time represents the period during which a request message is processed and related response time made available but not yet returned to the consumer. In particular it does not include time spent over the network (for both request and response messages). Measurement Conditions. Average processing time measurements do not differentiate between the case of use of full CRLs or Delta CRLs and they do not take into account LDAP replication schema that may be used to improve performances. No specific measurement conditions are provided for the security controls, network characteristics and sessions setup, because those aspects do not impact the measured NFR (see definition of processing time).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>

Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0214.0020
Requirement	The OCSP Based X509 certificate revocation status request average response time shall be as follows: + Measurements: - 90% of the requests <= 0.5 s - 98% of the requests <= 1 s + Measurement conditions: - Authentication (mutual), Authorization, Integrity and Confidentiality at transport level. - Full load, no overload. - Network characteristics: throughput of 100Mb/s, average latency of 200ms. - Session setup, session reuse or session creation time excluded from the measurements.
Title	OCSP Based X509 certificate revocation status request average response time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average response time in the provided conditions for OCSP based CRL Distribution Points (CDPs). Certificate revocation status checking is performed synchronously with domain specific exchanges (e.g. send Flight Data, request Weather data). On-line status checking of the certificates used in such exchanges consists in requesting the certificate status to an OCSP responder. It is however possible implement caching of OCSP responder responses by relying on OCSP responder responses validity period. OCSP is one of several methods that allow to check the validity of an X509 certificate. Compared to other methods, It can provide more predictable and shorter response times. Measurements. Measured response time is as defined by SWIM Profile WP_PRF_01 NFR and in particular it represents a round-trip time including time spent over the network. Measurement Conditions. Provided measurements do not differentiate between the case of use of full CRLs or Delta CRLs and they do not take into account OCSP responders replication schema that may be used to improve performances. The presence of security controls (Authentication, Authorization, Integrity and Confidentiality at transport level) in the measurement conditions, reflects that these response times shall be met when all of these controls are active and performed during a

	request/response. Authentication at transport level may be part of a session setup: in such case the time spent for the Authentication at transport level will not be taken into account for targeted measurement (session reuse or session creation time excluded from the measurements). Average response time is measured relying on a network infrastructure having the provided characteristics (throughput of 100Mb/s and average latency of 200ms).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0214.0050
Requirement	The OCSP Based X509 certificate revocation status request processing time shall be as follows: + Measurements: - 90% of the requests <= 5 ms - 98% of the requests <= 10 ms + Measurement conditions: - Full load, no overload.
Title	OCSP Based X509 certificate revocation status request average processing time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average processing time in the provided conditions for OCSP based CRL Distribution Points (CDPs). Measurements. Processing time represents the period during which a request message is processed and related response time made available but not yet returned to the consumer. In particular it does not include time spent over the network (for both request and response messages). Measurement Conditions. Average processing time measurements do not differentiate between the case of use of full CRLs or Delta CRLs and they do not take into account OCSP responders replication schema that may be used to improve performances. No specific measurement conditions are provided for the security controls, network characteristics and sessions setup, because those aspects do not impact the measured NFR (see definition of processing time).
Category	<Performance>
Validation Method	

Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0214.0030
Requirement	The SCVP Based X509 certificate verification (path discovery) request average response time shall be as follows: + Measurements: - 90% of the requests <= 3 s - 98% of the requests <= 4 s + Measurement conditions: - Authentication (mutual), Authorization, Integrity and Confidentiality at transport level. - Full load, no overload. - Network characteristics: throughput of 100Mb/s, average latency of 200ms. - Session setup, session reuse or session creation time excluded from the measurements.
Title	SCVP Based X509 certificate verification request average response time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements. This requirement provides the average response time in the provided conditions for SCVP services. SCVP allows consumer to demand certification path construction and validation to a third party. This is useful especially in cases where the certification path for a given certificate is very complex. Certificate verification is performed synchronously with domain specific exchanges (e.g. send Flight Data, request Weather data). On-line verification of certificates used in such exchanges consists in submitting an appropriate request to an SCVP server / SCVP service provider. Measurements. Measured response time is as defined by SWIM Profile WP_PRF_01 NFR and in particular it represents a round-trip time including time spent over the network. Measurement Conditions. The presence of security controls (Authentication, Authorization, Integrity and Confidentiality at transport level) in the measurement conditions, reflects that these response times shall be met when all of these controls are active and performed during a request/response. Authentication at transport level may be part of a session setup: in such case the time spent for the Authentication at transport level will not be taken into account for targeted measurement (session reuse or session creation time excluded from the measurements). Average response time is

	measured relying on a network infrastructure having the provided characteristics (throughput of 100Mb/s and average latency of 200ms).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0214.0060
Requirement	The SCVP Based X509 certificate verification (path discovery) request average processing time shall be as follows: + Measurements: - 90% of the requests <= 40 ms - 98% of the requests <= 80 ms + Measurement conditions: - Full load, no overload.
Title	SCVP Based X509 certificate verification (path discovery) request average processing time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average processing time in the provided conditions for SCVP services. Measurements. Processing time represents the period during which a request message is processed and related response time made available but not yet returned to the consumer. In particular it does not include time spent over the network (for both request and response messages). Measurement Conditions: No specific measurement conditions are provided for the security controls, network characteristics and sessions setup, because those aspects do not impact the measured NFR (see definition of processing time).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.3.2 Resource utilization Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.3.3 Capacity Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0214.0070
Requirement	The Certification Authority shall be able to manage up to 50000 digital identities for ground SWIM systems.
Title	CA capacity in terms of managed digital identities
Status	<In Progress>
Rationale	The capacity requirement is related to the whole set of CAs contributing to all the PKIs required for the European SWIM whatever is the deployment strategy. In case of centralized deployment is used the single CA shall meet the requirement. In case a federated or hierarchical deployment is preferred the capacity has to be spread over all the CAs. The number of ground systems using SWIM and being authenticated is estimated to about 5000 (40 met-providers, 1 EAD, 1 NM, 1800 Airports, 1200 Airlines, 10 centralized services) with average numbers of certificates per connected system of 10 (5000x10=50000).
Category	<Performance><Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.4 Safety & Security

This section includes security requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with security NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.2.4.1) confidentiality, (§3.2.4.2) integrity, (§3.2.4.3) non-repudiation, (§3.2.4.4) accountability and (§3.2.4.5) authenticity. Furthermore, according to SJU guidelines, a dedicated subsection (§3.2.4.6) is provided for safety requirements.

3.2.4.1 Confidentiality Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.4.2 Integrity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.4.3 Non-repudiation Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.4.4 Accountability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.4.5 Authenticity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.4.6 Safety Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.5 Maintainability

This section includes maintainability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with maintainability NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.2.5.1) modularity, (§3.2.5.2) reusability, (§3.2.5.3) analysability, (§3.2.5.4) modifiability and (§3.2.5.5) testability.

3.2.5.1 Modularity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.5.2 Reusability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.5.3 Analysability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.5.4 Modifiability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.5.5 Testability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.6 Reliability

This section includes reliability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with reliability NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.2.6.1) maturity, (§3.2.6.2) availability, (§3.2.6.3) fault tolerance and (§3.2.6.4) recoverability.

3.2.6.1 Maturity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.6.2 Availability Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0614.0040
Requirement	The LDAP CDP (CRLs Distribution Point) availability shall be as follows: + Measurement: 99,95% + Measurement conditions: - Not including planned outages, - Full load, no overload, + Observation period: 1 month
Title	LDAP CDP Availability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. LDAP CDP is an enabling/supporting service to retrieve CRLs that are used to verify revocation status of the X.509 certificates during ATM services provider and (for mutual authentication) consumer authentication (of course X.509 Security Token verification are also subject to this checking). Unavailability of LDAP CDP may impact the consumption of the ATM service in one of the following cases: (i) If CRL Pre-fetching is not implemented on ATM Service consumer/provider side, to check certificate revocation status consists in first synchronously (with the ATM interaction) download of the CRL from the CDP and then in parsing the CRL to check if the certificate under verification is included in the CRL; if the CDP is not available the certificate revocation status cannot be checked; (ii) If CRL Pre-fetching is implemented on ATM Service consumer/provider side, to check certificate revocation status consists in verifying that the certificate under verification is not included in locally available valid CRLs; if, because some problems in background tasks for refreshing CRLs, the available CRLs are expired and they cannot be used to verify revocation status; the only option in this case is to proceed as in (i) above. In all these cases the ATM Service provider/consumer cannot be authenticated and therefore the service cannot be consumed. In theory, LDAP CDP availability should be closed/equal to ATM Service(s) availability. In practice, being the LDAP CDP a supporting service and taking into account that (i) CRL Pre-fetching is typically implemented and (ii) CRLs updates downloading is a background task scheduled to spread the downloads across the CRL overlap period and (iii) CRL validity period is always greater than CRL publication period, not all the ATM service consumption requests require the involvement of the LDAP CDP and

	therefore it is reasonable to require an availability of LDAP CDP less than ATM services availability trying to establish the right trade-off between costs and needs. More demanding (in terms of availability) ATM Services may require (e.g. Security Policy) (i) CRLs with longer validity period and/or (ii) a larger CRL overlap period, to minimize the probability that the LDAP CDP is not available when required. The required availability for the LDAP CDP (99,95%) has been derived according to above considerations and it is independent of whatever deployment options and fault tolerance techniques are adopted for the LDAP CDP. Assuming 30 workdays per month, 22 working hours a day and planned outages executed in the remaining 2 hours a day, the required availability ensures a maximum down time, due to un-planned outages, of 19 minutes/month. In the declared window of availability, considering the use of CRLs Pre-fetching and CRLs overlap period techniques, the maximum down time is affordable from ATM services perspective.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0060
Requirement	The LDAP CDP Continuous unavailability shall be as follows: + Measurement: <= 2 minutes + Measurement conditions: - Not Including planned outages, - Full load, no overload, + Observation period: 1 hour
Title	LDAP CDP Continuous unavailability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. LDAP CDP is an enabling/supporting service to retrieve CRLs that are used to verify revocation status of the X.509 certificates during ATM services provider and (for mutual authentication) consumer authentication (of course X.509 Security Token verification are also subject to this checking). Unavailability of LDAP CDP may impact the consumption of the ATM service in one of the following cases: (i) If CRL Pre-fetching is not implemented on ATM Service consumer/provider side, to check certificate

	revocation status consists in first synchronously (with the ATM interaction) download of the CRL from the CDP and then in parsing the CRL to check if the certificate under verification is included in the CRL; if the CDP is not available the certificate revocation status cannot be checked; (ii) If CRL Pre-fetching is implemented on ATM Service consumer/provider side, to check certificate revocation status consists in verifying that the certificate under verification is not included in locally available valid CRLs; if, because some problems in background tasks for refreshing CRLs, the available CRLs are expired and they cannot be used to verify revocation status; the only option in this case is to proceed as in (i) above. In all these cases the ATM Service provider/consumer cannot be authenticated and therefore the service cannot be consumed. Being the LDAP CDP a supporting service and taking into account that (i) CRL Pre-fetching is typically implemented and (ii) CRLs updates downloading is a background task scheduled to spread the downloads across the CRL overlap period and (iii) CRL validity period is always greater than CRL publication period, not all the ATM service consumption requests require the involvement of the LDAP CDP and therefore it is reasonable to require an availability of LDAP CDP less than ATM services availability trying to establish the right trade-off between costs and needs. More demanding (in terms of availability) ATM Services may require (e.g. Security Policy) (i) CRLs with longer validity period and/or (ii) a larger CRL overlap period, to minimize the probability that the LDAP CDP is not available when required. Taking into account the purpose of the LDAP CDP and considerations provided in the rationale of the LDAP CDP availability requirement REQ-14.01.04-TS-0614.0040 a continuous unavailability of 2 minutes/hour is considered acceptable independently of the specific ATM service requirements and whatever deployment options and fault tolerance techniques are adopted for the LDAP CDPs.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0050
Requirement	LDAP CDP Planned Outages shall be scheduled for a time of the day when ATM activities are at their lowest and maintenance window shall never exceed 4hrs/day.
Title	LDAP CDP Planned Outages
Status	<In Progress>
Rationale	This requirement provide constrains on the scheduling of planned outages

	for the LDAP CDP. This requirement complements the LDAP CDP availability requirement REQ-14.01.04-TS-0614.0040 by ensuring that the planned outages and related maintenance window are properly scheduled in order to minimize the impact on the overall ATM activities.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0100
Requirement	The SCVP availability shall be as follows: + Measurement: 99,99% + Measurement conditions: - Not including planned outages, - Full load, no overload, + Observation period: 1 month
Title	SCVP Availability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. SCVP is an enabling/supporting service for the server-based X.509 certificates verification (path discovery) during ATM services provider and (for mutual authentication) consumer authentication (of course X.509 Security Token verification are also subject to this checking). Unavailability of SCVP service implies the ATM Service provider/consumer cannot be authenticated and therefore the service cannot be consumed. The criticality of this service is therefore highest with respect to other services such as LDAP CDP. The required availability for the SCVP service (99,99%) has been derived according to above considerations and it is independent of whatever deployment options and fault tolerance techniques are adopted for the service. Assuming 30 workdays per month, 22 working hours a day and planned outages executed in the remaining 2 hours a day, the required availability ensures a maximum down time, due to un-planned outages, of 4 minutes/month.
Category	<Reliability>
Validation Method	

Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0120
Requirement	The SCVP Continuous unavailability shall be as follows: + Measurement: <= 2 minutes + Measurement conditions: - Not Including planned outages, - Full load, no overload, + Observation period: 1 hour
Title	SCVP Continuous unavailability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. SCVP is an enabling/supporting service for the server-based X.509 certificates verification (path discovery) during ATM services provider and (for mutual authentication) consumer authentication (of course X.509 Security Token verification are also subject to this checking). Unavailability of SCVP service implies the ATM Service provider/consumer cannot be authenticated and therefore the service cannot be consumed. The criticality of this service is therefore highest with respect to other services such as LDAP CDP. Taking into account the purpose of the SCVP and the considerations provided in the rationale of the SCVP availability requirement REQ-14.01.04-TS-0614.0100 a continuous unavailability of 2 minutes/hour is considered acceptable independently of the specific ATM service requirements and whatever deployment options and fault tolerance techniques are adopted for the SCVP.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>

Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0110
Requirement	SCVP Planned Outages shall be scheduled for a time of the day when ATM activities are at their lowest and maintenance window shall never exceed 2hrs/day.
Title	SCVP Planned Outages
Status	<In Progress>
Rationale	This requirement provides constrains on the scheduling of planned outages for the SCVP. This requirement complements the SCVP availability requirement REQ-14.01.04-TS-0614.0100 by ensuring that the planned outages and related maintenance window are properly scheduled in order to minimize the impact on the overall ATM activities.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0160
Requirement	The OCSP Online Responder availability shall be as follows: + Measurement: 99,99% + Measurement conditions: - Not including planned outages, - Full load, no overload, + Observation period: 1 month
Title	OCSP Online Responder Availability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines.

	OCSP Online Responder is an enabling/supporting service for the online checking of revocation status of the X.509 certificates during ATM services provider and (for mutual authentication) consumer authentication (of course X.509 Security Token verification are also subject to this checking). Unavailability of OCSP Online Responder may impact the consumption of the ATM service in one of the following cases: (i) If OCSP responses caching is not implemented on ATM Service consumer/provider side, to check certificate revocation status consists always in synchronously (with the ATM interaction) submit the request to the OCSP Online Responder that if not available it cannot serve the request; (ii)even if OCSP responses caching is implemented on ATM Service consumer/provider side, the responses could be expired or no cached responses exist for the certificate under verification; this requires to submit the request to the OCSP Online Responder that if not available it cannot serve the request. In all these cases the ATM Service provider/consumer cannot be authenticated and therefore the service cannot be consumed. In theory, OCSP Online Responder availability should be closed/equal to ATM Service(s) availability. In practice, being the OCSP Online Responder a supporting service and taking into account that (i) OCSP responses caching is typically implemented and (ii) cached OCSP responses are typically refreshed as background tasks, not all the ATM service consumption requests require the involvement of the OCSP Online Responder and therefore it is reasonable to require an availability of OCSP Online Responder less than ATM services availability trying to establish the right trade-off between costs and needs. It is however possible that, even if OCSP responses caching is implemented, there are no cached responses for the certificate under verification. This implies that the criticality of this service is highest with respect to other services such as LDAP CDP. The required availability for the OCSP CDP (99,99%) has been derived according to above considerations and it is independent of whatever deployment options and fault tolerance techniques are adopted for the OCSP CDP. Assuming 30 workdays per month, 22 working hours a day and planned outages executed in the remaining 2 hours a day, the required availability ensures a maximum down time, due to un-planned outages, of 4 minutes/month. In the declared window of availability, even if the optional use of OCSP responses Pre-fetching technique, the maximum down time is considered affordable from ATM services perspective.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0180
Requirement	The OCSP Online Responder Continuous unavailability shall be as follows: + Measurement: <= 2 minutes + Measurement conditions: - Not Including planned outages, - Full load, no overload, + Observation period: 1 hour
Title	OCSP Online Responder Continuous unavailability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. OCSP Online Responder is an enabling/supporting service for the online checking of revocation status of the X.509 certificates during ATM services provider and (for mutual authentication) consumer authentication (of course X.509 Security Token verification are also subject to this checking). Unavailability of OCSP Online Responder may impact the consumption of the ATM service in one of the following cases: (i) If OCSP responses caching is not implemented on ATM Service consumer/provider side, to check certificate revocation status consists always in synchronously (with the ATM interaction) submit the request to the OCSP Online Responder that if not available it cannot serve the request; (ii)even if OCSP responses caching is implemented on ATM Service consumer/provider side, the responses could be expired or no cached responses exist for the certificate under verification; this requires to submit the request to the OCSP Online Responder that if not available it cannot serve the request. In all these cases the ATM Service provider/consumer cannot be authenticated and therefore the service cannot be consumed. In theory, OCSP Online Responder availability should be closed/equal to ATM Service(s) availability. In practice, being the OCSP Online Responder a supporting service and taking into account that (i) OCSP responses caching is typically implemented and (ii) cached OCSP responses are typically refreshed as background tasks, not all the ATM service consumption requests require the involvement of the OCSP Online Responder and therefore it is reasonable to require an availability of OCSP Online Responder less than ATM services availability trying to establish the right trade-off between costs and needs. It is however possible that, even if OCSP responses caching is implemented, there are no cached responses for the certificate under verification. This implies that the criticality of this service is highest with respect to other services such as LDAP CDP. Taking into account the purpose of the OCSP Online Responder and considerations provided in the rationale of the OCSP Online Responder availability requirement REQ-14.01.04-TS-0614.0160 a continuous unavailability of 2 minutes/hour is considered acceptable independently of the specific ATM service requirements and whatever deployment options and fault tolerance techniques are adopted for the OCSP Online Responder.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>

Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0170
Requirement	OCSP Online Responder Planned Outages shall be scheduled for a time of the day when ATM activities are at their lowest and maintenance window shall never exceed 4hrs/day.
Title	OCSP Online Responder Planned Outages
Status	<In Progress>
Rationale	This requirement provides constrains on the scheduling of planned outages for the OCSP Online Responder. This requirement complements the OCSP Online Responder availability requirement REQ-14.01.04-TS-0614.0160 by ensuring that the planned outages and related maintenance window are properly scheduled in order to minimize the impact on the overall ATM activities.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0220
Requirement	The publication of new CRLs shall be accessible on all CRLs Distribution Points within a timespan of: + Measurements: - 5 minutes in the nominal case. - 1 hours in case of unexpected problems. + Measurement conditions: - None relevant
Title	CRLs Distribution Points (CDPs) consistency
Status	<In Progress>
Rationale	In case multiple CDP endpoints are used to publish CRLs, there is no

	guarantee that each of those endpoints uses the CRL as reference at any moment in time. Hence, a validation based on a CRL published on one CDP endpoint could result in valid status, while the same validation based on a CRL on another CDP endpoint could result in invalid status. In the nominal case it is required that all the CDPs have a coherent state (i.e. latest CRL) within a timespan of 5 minutes. In other words, in 5 minutes whatever CDPs different relying parties will use, the returned CRLs will always be consistent. In all cases with no exception, the consistency shall be ensured within a timespan of 1h.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0230
Requirement	The publication of new CRLs shall be accessible on all OCSP Online Responder endpoints within a timespan of: + Measurements: - 5 minutes in the nominal case. - 1 hours in case of unexpected problems + Measurement conditions: - None relevant
Title	OCSP Online Responders consistency
Status	<In Progress>
Rationale	In case multiple OCSP Online Responder endpoints are used, there is no guarantee that each of those endpoints use the same CRL as reference at any moment in time. Hence, a validation request on one endpoint could result in valid status , while the same validation request on another endpoint could result in invalid status. In the nominal case it is required that all the endpoints have a coherent state (i.e. latest CRL) within a timespan of 5 minutes. In other words, in 5 minutes whatever OCSP Online Responder different relying parties will use, the returned responses will always be consistent and coherent. In all cases with no exception, the consistency shall be ensured within a timespan of 1h.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>

Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.6.3 Fault Tolerance Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0614.0070
Requirement	LDAP CDP solutions should be implemented by leveraging on replication techniques.
Title	LDAP CDP replication
Status	<In Progress>
Rationale	The adoption of replication techniques consisting in providing one or more replicas of the service and switching/routing clients' requests among all service instances, increasing both LDAP CDP performances and availability. This requirement covers NIST security controls SC-36 and SI-13b.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0080
Requirement	LDAP CDP solutions should ensure failure transparency by masking to its consumers the failure and possible recovery.
Title	LDAP CDP failure transparency
Status	<In Progress>
Rationale	The adoption of replication and in general fault tolerance (detection,

	isolation, containment, etc.) techniques allows increasing both LDAP CDP performances and availability. Failure transparency techniques mask from an object the failure and possible recovery of other objects (or itself) to enable fault tolerance. This requirement applies when an LDAP CDP consumer has already discovered an LDAP CDP endpoint which is being used to interact with the LDAP CDP. This requirement covers NIST security controls SI-13 (4).
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0090
Requirement	LDAP CDP solutions shall provide mechanisms to detect, handle and report the occurrence of failures cause by the following security incidents: + Software Failure. + Hardware Failure. + Denial of Service. + Compromised information. + Network unavailability.
Title	LDAP CDP Failure detection, handling and reporting
Status	<In Progress>
Rationale	This requirement ensures that the LDAP CDP solution provides a functionality aiming at reporting the handling of incidents that may have an impact on security. This requirement covers with NIST security control AU-2 a and AU-3.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A

<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0130
Requirement	SCVP solutions should be implemented by leveraging on replication techniques.
Title	SCVP replication
Status	<In Progress>
Rationale	The adoption of replication techniques consisting in providing one or more replicas of the service and switching/routing clients' requests among all service instances, increasing both SCVP performances and availability. This requirement covers NIST security controls SC-36 and SI-13b.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0140
Requirement	SCVP solutions should ensure failure transparency by masking to its consumers the failure and possible recovery.
Title	SCVP failure transparency
Status	<In Progress>
Rationale	The adoption of replication and in general fault tolerance (detection, isolation, containment, etc.) techniques allows increasing both SCVP performances and availability. Failure transparency techniques mask from an object the failure and possible recovery of other objects (or itself) to enable fault tolerance. This requirement applies when an SCVP consumer has already discovered an SCVP endpoint which is being used to interact with the SCVP. This requirement covers NIST security controls SI-13 (4)
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>

Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0150
Requirement	SCVP solutions shall provide mechanisms to detect, handle and report the occurrence of failures cause by the following security incidents: + Software Failure. + Hardware Failure. + Denial of Service. + Compromised information. + Network unavailability.
Title	SCVP Failure detection, handling and reporting
Status	<In Progress>
Rationale	This requirement ensures that the SCVP solution provides a functionality aiming at reporting the handling of incidents that may have an impact on security. This requirement covers with NIST security control AU-2 a and AU-3.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0190
Requirement	OCSP Online Responder solutions should be implemented by leveraging on replication techniques.
Title	OCSP Online Responder replication
Status	<In Progress>
Rationale	The adoption of replication techniques consisting in providing one or more replicas of the service and switching/routing clients' requests among all service instances, increasing both OCSP Online Responder performances and availability.

	This requirement covers NIST security controls SC-36 and SI-13b.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0200
Requirement	OCSP Online Responder solutions should ensure failure transparency by masking to its consumers the failure and possible recovery.
Title	OCSP Online Responder failure transparency
Status	<In Progress>
Rationale	The adoption of replication and in general fault tolerance (detection, isolation, containment, etc.) techniques allows increasing both OCSP Online Responder performances and availability. Failure transparency techniques mask from an object the failure and possible recovery of other objects (or itself) to enable fault tolerance. This requirement applies when an OCSP Online Responder consumer has already discovered an OCSP Online Responder endpoint which is being used to interact with the OCSP Online Responder. This requirement covers NIST security controls SI-13 (4).
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0210
Requirement	OCSP Online Responder solutions shall provide mechanisms to detect, handle and report the occurrence of failures cause by the following security incidents: + Software Failure. + Hardware Failure. + Denial of Service. + Compromised information. + Network unavailability.
Title	OCSP Online Responder Failure detection, handling and reporting
Status	<In Progress>
Rationale	This requirement ensures that the OCSP Online Responder solution provides a functionality aiming at reporting the handling of incidents that may have an impact on security. This requirement covers with NIST security control AU-2 a and AU-3.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.6.4 Recoverability Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0614.0010
Requirement	The overlap of validity periods of subsequent CRLs shall be such that 18hrs to 4 full days shall be available at any time to recover from a failed CA.
Title	Overlap of CRL validity periods
Status	<In Progress>
Rationale	CRL validity period overlapping is a technique that, irrespective to CRL validity period, can be properly used to ensure that a given time period is available to recover from a failed CA without any impact to relying parties (i.e. CRLs are still valid). This requirement provides a range for admissible minimum available time periods to recover from a failure. Depending of specific constraint the minimum value can be any value in the provided range. For instance following configurations of overlap validity period are admissible: 18hrs, 20hrs, 3 days. On the contrary, following configurations of overlap validity period are not admissible: 12hrs, 5 days.
Category	<Reliability><Design>
Validation Method	

Verification Method	<Analysis><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0020
Requirement	A Recovery Point Objective (RPO) for the OCSP Online Responder shall be at least the point in time, before the disruption event has occurred, when latest CRL is created, signed and made available by the CA.
Title	PKI OCSP Online Responder Recovery Point Objective
Status	<In Progress>
Rationale	[ISO/IEC 27031:2011] RPO is point in time to which data must be recovered after a disruption has occurred. When the OCSP Responder receives a status verification request from the client it then needs to determine the status of the certificate using the serial number presented by the client. First the OCSP Responder may determine if it has any cached responses for the same request. If it does, it can then send that response to the client. If there is no cached response, the OCSP Responder then may check to see if it has the CRL issued by the CA cached locally on the OCSP. If it does, it can check the revocation status locally, and send a response to the client stating whether the certificate is valid or revoked. If the OCSP does not have the CRL cached locally, the OCSP Responder can retrieve the CRL from the CDP locations listed in the certificate. For such reason, the loss of data by PKI OCSP Online Responder consists in the loss of cached status responses and cached CRLs; this has impacts on the performances replying the clients and consequently it also impacts performances for ATM services consumption. If data loss exceed the CRLs overlap period, then after recovery (in the general hypothesis that during the recovery the OCSP Online Responder cannot retrieve the CRLs it needs using CDPs information) the OCSP Online Responder would keep in the local storage only expired CRLs, and new valid CRLs shall be retrieved from CDPs for each different request. Conversely if the RPO doesn't exceed the CRLs overlap period, after a failure the OCSP Online Responder will still maintain at least one valid CRL (even if not the latest update) which can be used to provide fast replies to clients' requests, while background mechanism can be implemented to retrieve more updated CRLs. The required RPO has been derived according to above considerations. Furthermore, the required RPO is independent of whatever deployment options are adopted for the OCSP Online Responder. The provided RPO ensures that the recovered state is at least the latest CRL made available by CA before the disruption even has occurred. "At least" means that, if a new CRL will be available during the recovery, that one could be used to

	recover from the event. It is anticipated that required RPO is expected to be met according to business impact, threat and risk analysis documented in the business continuity planning. In case an incident occurs and it is not part of the business continuity planning, it may happen that the RPO may be not met. This requirement covers the following NIST sec. controls: CP-2 a.2.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0614.0030
Requirement	A Recovery Point Objective (RPO) for the LDAP Based CRLs Distribution Point shall be at least the point in time, before the disruption event has occurred, when latest CRL is created, signed and made available by the CA.
Title	PKI LDAP Based X509 CDP Recovery Point Objective
Status	<In Progress>
Rationale	[ISO/IEC 27031:2011] RPO is point in time to which data must be recovered after a disruption has occurred. Data loss for CDP consists in losing CRLs previously published by the CAs. If data loss exceed the CRLs overlap period, then after recovery (in the more general hypothesis that latest CRLs cannot be retrieved during the recovery phase) the CDP would keep only expired CRLs until a new valid CRLs is published. Conversely if the RPO doesn't exceed the CRLs overlap period, after a failure the CDP will still maintain at least one valid CRL (even if not the latest update) which can be provided to requesting clients without further interrupting of the service. The required RPO has been derived according to above considerations. Furthermore, the required RPO is independent of whatever deployment options are adopted for the LDAP CDP. The provided RPO ensures that the recovered state is at least the latest CRL made available by CA before the disruption even has occurred. "At least" means that, if a new CRL will be available during the recovery, that one could be used to recover from the event. It is anticipated that required RPO is expected to be met according to business impact, threat and risk analysis documented in the business continuity planning. In case an incident occurs and it is not part of the business continuity planning, it may happen that the RPO may be not met. This requirement covers the following NIST sec. controls: CP-2 a.2.
Category	<Reliability><Design>

Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.7 Internal Data Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.8 Design and Construction Constraints

This section includes compatibility and portability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with sub-characteristics of both compatibility and portability NFR described in ISO/IEC 25010:2011: (§3.2.8.1) co-existence and (§3.2.8.2) interoperability compatibility NFR sub-characteristics, (§3.2.8.3) installability and (§3.2.8.4) replaceability portability NFR sub-characteristics.

[REQ]

Identifier	REQ-14.01.04-TS-0814.0030
Requirement	The Certification Authorities shall be able to use Delta CRL policy to limit the network bandwidth consumption in periodical CRL publications.
Title	CA support of Delta CRL policy
Status	<In Progress>
Rationale	CRLs size can get potentially significantly large over the time by affecting bandwidth consumption and processing time. These effects become more relevant as the CRL publication frequency is increased. In order to meet performance requirements, CA shall use Delta CRL policy to properly manage both Delta and Base CRL size to limit network bandwidth. Delta CRLs, allow relying party to download the large CRL less frequently and the Delta more frequently. It is however anticipated that CA shall also allow relying party to use only Base CRL. Furthermore, additional policy such as "CRL partitioning" shall be provided in order to properly manage the size of Base CRL (refer to REQ-14.01.04-TS-0814.0100).
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0040
Requirement	The Certification Authority shall ensure that the use of Delta CRL does not prevent a relying party that does not support Delta CRL from using the CA functionality through Base CRL.
Title	CA support of both Delta CRL and Base CRL policies.
Status	<In Progress>
Rationale	It may happen that specific relying parties do not support Delta CRL. This requirement allows both Delta CRL capable and non-capable relying parties to use the CA. The use of additional policy such as "CRL partitioning" allows CA to properly manage the size of Base CRL and also non-capable Delta CRL relying parties will benefit of that.

Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0050
Requirement	An OCSP Online Responder should use in-memory response caching to optimize Response time, processing time and CPU consumption.
Title	In-memory OCSP Responder response caching
Status	<In Progress>
Rationale	The use of in-memory caching allows OCSP Responder to reuse cached responses (when applicable) when serving certificate revocation status requests. This will improve overall performances including response time, processing time and CPU consumption. It is anticipated that OCSP responder responses caching can be also used on OCSP consumer side by relying on OCSP responder responses validity period (similar to CRL validity period).
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0060
Requirement	The publication period of complete Base CRL shall not exceed one week.
Title	Base CRL Publication Period

Status	<In Progress>
Rationale	CRL publication period cannot exceed CRL publication overlap period. Currently, the required overlap period is such that from 18h to 4 full days is allowed for CA recovery. The provided value for the CRL publication period is considered as a reasonable trade-off between security (time when a revoked certificate is still used) and network bandwidth consumption. When supported, Delta CRL can be published more frequently. Typically 2 or 3 publications of Delta CRLs within a base-CRL publication period should be scheduled (e.g. publication period for Delta CRL is less than 2 days).
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0070
Requirement	The minimum validity of a root CA shall be 15 Years.
Title	Root CA minimum validity period
Status	<In Progress>
Rationale	The provided value for the minimum Root CA validity period is based on what is typically provided by widely used CAs (e.g. Thawte, GlobalSign, Microsoft, Verisign, etc.).
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0080
Requirement	The minimum validity of an issuing CA shall be 10 Years.
Title	Issuing CA minimum validity period
Status	<In Progress>
Rationale	The provided value for the minimum Issuing CA validity period is based on what is typically provided as root CAs (REQ-14.01.04-TS-0814.0070) by widely used CAs (e.g. Thawte, GlobalSign, Microsoft, Verisign, etc.). Typically, Issuing CA validity period should be less than root CA validity period.
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0090
Requirement	The minimum validity of an issued certificate shall be 15 Months.
Title	X.509 Certificates minimum validity period
Status	<In Progress>
Rationale	The provided value for the minimum X.509 Certificates validity period allows for renewal of a certificate every 1 year with 3 months time to obtain and install.
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0100
Requirement	The Certification Authorities shall be able to use "CRL partitioning" policy to reduce CRL size limiting the network bandwidth consumption in periodical CRL publications.
Title	CA support of CRL partitioning policy
Status	<In Progress>
Rationale	CRLs size can get potentially significantly large over the time by affecting bandwidth consumption and processing time. These effects become more relevant as the CRL publication frequency is increased. In order to meet performance requirements, CA shall use "CRL partitioning" policy allowing to properly manage CRL size through periodic renewal of the CA Key and the creation of multiple CRLs each scoping only distinct subsets of certificates. Furthermore, additional policy such as Delta CRL shall be provided in order to properly manage the size of Base CRL.
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.8.1 Co-existence Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.8.2 Interoperability Requirements

[IREQ]

Identifier	REQ-14.01.04-TS-0002.0031
Requirement	Cryptographic algorithms and key sizes shall comply with European Network of Excellence in Cryptology (ECRYPT) II recommendations.
Title	SWIM Technical Infrastructure cryptographic algorithms ECRYPTII compliance
Status	<Validated>
Rationale	ECRYPT II recommendations represent a reference that is used to analyse and to identify the most appropriate cryptographic algorithms and key sizes. For further information about ECRYPT II, please refer to

	http://www.ecrypt.eu.org.The encryption algorithms are agreed between partners but are not published for sensitivity reasons. However, taking into account that the access to these information represents a key point enabling the interoperability, the partners are expected to evaluate how to properly govern the access to these information. The ECRYPTII recommendations must be considered as a minimum set of constraints which may be further restricted in specific policies and/or governance bodies. This requirement covers NIST security controls IA-5 c and IA-7 and SC-13.
Category	<Functional><Safety><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-12	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ_029	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0802.0010
Requirement	Cryptographic algorithms and key sizes shall comply with NIST 800-131A recommendations.
Title	SWIM Technical Infrastructure cryptographic algorithms NIST 800-131A compliance
Status	<In Progress>
Rationale	NIST Special Publication 800-131A 'Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" recommendations represent a reference that is used to analyze and to

	identify the most appropriate cryptographic algorithms and key sizes. In case of differences between ECRYPT II and NIST SP 800-131A recommendations, the most stringent recommendations must be considered as applicable. Although the compliance to NIST Special Publication 800-131A (January 2011) is implicitly included by the compliance to ECRYPT II (see REQ-14.01.04-TS-0002.0031), this requirement allows to ensure that the SWIM-TI will be compliant with up-to date recommendations either from NIST or ECRYPT II. The NIST SP 800-131A recommendations must be considered as a minimum set of constraints which may be further restricted in specific policies and/or governance bodies. This requirement covers NIST security controls IA-5c, IA-7 and SC-13.
Category	<Functional><Safety><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator><Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-SEC-12	<Full>
<SATISFIES>	<ATMS Requirement>	P14.02.02-REQ_029	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0814.0010
Requirement	The EU and FAA Next Gen SWIM Certificate Policies shall be compatible.
Title	EU and FAA SWIM Certificate Policies Compatibility
Status	<In Progress>
Rationale	This requirement ensures that Certificate policies (CP) established in the context of EU SWIM will be compatible with CPs established in FAA NextGen SWIM. This will allow ATM actors to rely on compatible CPs as

	one of the building block for cross regions interoperability.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<ICD><Governance>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.8.2.1 Common Time

Requirements included in §3.1 are applicable

3.2.8.2.2 Standards

This section introduces, in the scope of the PKI, the standards that are applicable to Interfaces through which interoperability is provided or required with and for participants that are external to the SWIM-TI as well as participants that are internal to the SWIM-TI.

Each technical configuration at the level of such Interfaces that requires adherence to one or more standards to support and promote interoperability, includes these standards by referencing the standards in this section.

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0102
Requirement	IETF RFC 768 User Datagram Protocol 28 August 1980 http://tools.ietf.org/html/rfc768 shall be supported.
Title	Interoperability standard. UDP RFC 768
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>

Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0155
Requirement	IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP June 2013 http://tools.ietf.org/html/rfc6960 shall be supported.
Title	Interoperability standard. OCSP
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>

<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0156
Requirement	IETF RFC 4510 Proposed Standard, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006 http://www.rfc-editor.org/rfc/rfc4510.txt shall be supported.
Title	Interoperability standard. LDAPv3
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-4 (6).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0157
Requirement	IETF RFC 5280 Proposed Standard, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 http://www.rfc-editor.org/rfc/rfc5280.txt shall be supported.
Title	Interoperability standard. Internet PKI Certificate and CRL Profile
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0158
Requirement	IETF RFC 4523 Proposed Standard, Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates, June 2006 http://www.rfc-editor.org/rfc/rfc4523.txt shall be supported.
Title	Interoperability standard. LDAP Schema Definitions for X.509 Certificates
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-4 (6).

Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0159
Requirement	IETF RFC 4158 Internet X.509 Public Key Infrastructure: CertificationPathBuilding September 2005 http://tools.ietf.org/html/rfc4158 shall be supported.
Title	Interoperability standard. Public Key Infrastructure: Certification Path Building
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>

High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0160
Requirement	IETF RFC 5055 Proposed Standard, Server-Based Certificate Validation Protocol (SCVP), December 2007 http://www.rfc-editor.org/rfc/rfc5055.txt shall be supported.
Title	Interoperability standard. SCVP
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-5 (2.a).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A

<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0161
Requirement	IETF RFC 5816 Proposed Standard, RFC ESSCertIDv2 Update for RFC 3161, March 2010 http://www.rfc-editor.org/rfc/rfc5816.txt shall be supported.
Title	Interoperability standard. ESSCertIDv2 Update for TSA
Status	<In Progress>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control AU-8.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0162
Requirement	IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) August 2001 http://www.rfc-editor.org/rfc/rfc3161.txt shall be supported.
Title	Interoperability standard. TSA
Status	<In Progress>

Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control AU-8.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0163
Requirement	IETF RFC 5652 Internet Standard, Cryptographic Message Syntax (CMS), September 2009 http://www.rfc-editor.org/rfc/rfc5652.txt shall be supported.
Title	Interoperability standard. CMS
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-8 (1)
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A

<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0171
Requirement	IETF RFC 6918 Proposed Standard, Formally Deprecating Some ICMPv4 Message Types, April 2013 http://tools.ietf.org/html/rfc6918 shall be supported.
Title	Interoperability standard. Formally Deprecating Some ICMPv4 Message Types
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0187
Requirement	RSA Laboratories PKCS #12 v1.1: Personal Information Exchange Syntax, October 27, 2012 Standard http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm shall be supported.
Title	Interoperability standard. PKCS #12 v1.1

Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-5 (2.b).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

3.2.8.3 Installability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.8.4 Replaceability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.2.9 Interface Requirements

This section includes interface requirements applicable to the PKI.

3.2.9.1 External Service Interface Bindings

There are no specific external interfaces for the PKI. The external service interface requirements included in §3.1 are applicable.

3.2.9.2 Internal Service Interface Bindings

[REQ]

Identifier	REQ-14.01.04-TS-0914.0030
Requirement	LDAP services shall be instantiated using the following binding: + LDAPv3 over TCP + MEPs: SRR-MEP + Fault handling: as defined per LDAP standard + Encoding. - restricted encoding as defined per standard + Security: - Confidentiality: none - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: - formalism of contract description: as defined per standard - minimum: not applicable - reference: LDAPv3 + Interoperability: none
Title	Interface Binding. Unsecured LDAPv3 over TCP.
Status	<In Progress>
Rationale	A series of LDAP based operations do not necessarily need security. In particular this biding does support anonymous clients. This requirement covers NIST security control IA-5 a.
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0156	N/A

<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0157	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0158	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0159	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0914.0040
Requirement	LDAP services shall be instantiated using the following binding: + LDAPv3 over TLS over TCP. + MEPs: SRR-MEP + Fault handling: as defined per LDAP standard + Encoding. - restricted encoding as defined per standard + Security: - Confidentiality: transport - Integrity: transport - Authenticity: transport mutual or LDAP Simple or SASL - Authorization: transport or LDAP Simple or SASL - Non-repudiation: none + Contract: - formalism of contract description: as defined per standard - minimum: not applicable - reference: LDAPv3 + Interoperability: none
Title	Interface Binding. LDAPv3 over TLS over TCP.
Status	<In Progress>
Rationale	A series of LDAP based operations do at least need authentication and authorization and can take advantage of other security controls (confidentiality and integrity at transport level – i.e. TLS). This binding allows different options for authentication and authorization. The first option is to rely on authentication and authorization mechanism at transport level (i.e. TLS). The second option is to use LDAP Simple mechanism defined in the LDAP standard. The third option is to use SASL (Simply Authentication and Security Layer). A number of SASL mechanisms are currently defined. In LDAP based exchanges, External, Digest-MD5 and Kerberos V5 mechanisms are typically used. This requirement covers NIST security controls IA-4 (6) and IA-5 a.
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Core><BP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A

<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0111	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0112	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0113	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0114	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0156	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0157	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0158	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0159	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0914.0050
Requirement	OCSP services shall be instantiated using the following binding: +OCSP over HTTP(s) over TCP. + MEPs: SRR-MEP + Fault handling: the service shall be able to determine the content of the HTTP status code and HTTP reason phrase + Encoding. - restricted encoding as defined per standard + Security: - Confidentiality: optionally transport - Integrity: optionally transport - Authenticity: message level for OCSP responses or transport (optionally mutual) - Authorization: optionally transport - Non-repudiation: none + Contract: - formalism of contract description: as defined per standard - minimum: not applicable - reference: OCSP + Interoperability: none
Title	Interface Binding. OCSP over HTTP(s) over TCP.
Status	<In Progress>
Rationale	OCSP based operations do not necessarily need security. Security can be applied but can lead to significant recursive complexity. RFC 6960 requires that OSCP responses are signed. This is why the binding allows message level (OCSP layer on top of HTTP) and transport level (HTTP over TLS) as valid options to authenticate the OCSP responder. This bindings allows optionally to have mutual authentication at transport level (HTTP over TLS) in case it is required to authenticate the clients due to specific deployment options/security policies. If the OCSP server does not require some sort of authorization, an attacker can get the server to respond to arbitrary requests. Such responses may give the attacker information that may be valuable for a future attack. Furthermore, when required, the binding allows to apply the other security controls at transport level (HTTP over TLS). Authenticity at transport level has not to be confused with HTTP Basic and Digest Access Authentication that are not supported by this binding. This requirement covers NIST security control IA-5 (2.a).
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Core><BP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>

Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0115	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0155	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0901.0332
Requirement	SCVP services shall be instantiated using the following binding: + SCVP over HTTP over TCP. + MEPs: SRR-MEP + Fault handling: the service shall be able to determine the content of the HTTP status code and HTTP reason phrase + Encoding. - restricted encoding as defined per standard + Security: - Confidentiality: none - Integrity: none - Authenticity: none - Authorization: none - Non-repudiation: none + Contract: - formalism of contract description: as defined per standard - minimum: not applicable - reference: SCVP + Interoperability: none
Title	Interface Binding. SCVP over HTTP over TCP.
Status	<In Progress>
Rationale	SCVP based operations do not necessarily need security. In particular (refer to RFC 5055 §1.2) this binding should be used to interact with Untrusted SCVP for certification path construction without validation. For further security considerations refer to RFC 5055 §9. This requirement covers NIST security control IA-5 (2.a).
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0115	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0160	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0914.0020
Requirement	SCVP services shall be instantiated using the following binding + SCVP over HTTPS over TCP. + MEPs: SRR-MEP + Fault handling: the service shall be able to determine the content of the HTTP status code and HTTP reason phrase + Encoding. - restricted encoding as defined per standard + Security: - Confidentiality: transport - Integrity: transport - Authenticity: message level for SCVP responses or transport (optionally mutual) - Authorization: optionally transport - Non-repudiation: none + Contract: - formalism of contract description: as defined per standard - minimum: not applicable - reference: SCVP + Interoperability: none
Title	Interface Binding. SCVP over HTTPS over TCP.
Status	<In Progress>
Rationale	SCVP based operations can be protected. This binding should be used to interact with Trusted SCVP (refer to RFC 5055 §1.2) for certification path construction and validation. In particular (refer to RFC 5055 §9) SCVP responses to validation requests must be protected to guarantee authenticity. This is why the binding allows message level (SCVP layer on top of HTTP) and transport level (HTTP over TLS) as valid options to authenticate the SCVP server. This bindings allows optionally to have mutual authentication at transport level (HTTP over TLS) in case it is required to authenticate the clients due to specific deployment options/security policies. According to RFC 5055 §9, If the SCVP server does not require some sort of authorization, an attacker can get the server to respond to arbitrary requests. Such responses may give the attacker information that may be valuable for a future attack. Furthermore the binding requires to apply the other security controls (confidentiality and integrity) at transport level (HTTP over TLS). Authenticity at transport level has not to be confused with HTTP Basic and Digest Access Authentication that are not supported by this binding. For further security considerations refer to RFC 5055 §9. This requirement covers NIST security control IA-5 (2.a).
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+><PP Core><BP Core>

Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0111	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0112	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0113	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0114	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0115	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0116	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0160	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.2.9.3 Network Interface Bindings

There are no specific network technical interface requirements for the PKI. The network technical interface requirements included in §3.1 are applicable.

3.2.9.4 Network Requirements

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0060
Requirement	The Communication Network Infrastructure shall allow to use User Datagram Protocol (UDP).
Title	Communication Network Infrastructure UDP delivery support
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed systems interconnected at network level using a Wide Area Network (WAN). Taking into account the overall context, the large number of interconnected systems and the need in some cases (e.g. DDS technology) of transmitting information in time-sensitive manner and also to support the NTP protocol the adoption of UDP protocol is needed.
Category	<Interface><Reliability>
Validation Method	
Verification Method	<Review of Design>
Profile Part	<YP Core><BP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-6	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0160
Requirement	The Communication Network Infrastructure shall support unicast over TCP/IP.
Title	Communication Network Infrastructure TCP/IP Unicast support
Status	<In Progress>
Rationale	All the profiles currently defined use the unicast communication between two stakeholders.
Category	<Functional><Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<SATISFIES>	<ATMS Requirement>	P14.02.09-SWIM-PENS-4	<Full>
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Project>	15.02.10	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>

<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0910.0170
Requirement	The Communication Network Infrastructure shall support unicast through UDP/IP.
Title	Communication Network Infrastructure unicast support through UDP/IP
Status	<In Progress>
Rationale	The Blue Profile uses UDP/IP in OMG DDS multicast distribution as well as unicast communication. The Yellow Profile uses the unicast communication between two participants in a communication. UDP is used for instance with the NTP time protocol.
Category	<Functional><Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider><Network provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

3.3 STI Functional and non-Functional Requirements

3.3.1 Capabilities

This section includes functional requirements applicable to the STI.

[REQ]

Identifier	REQ-14.01.04-TS-0016.0010
Requirement	The STI shall provide capabilities for issuing, validation, renewal, and cancellation of Security Tokens.
Title	Digital Identities management capabilities
Status	<In Progress>
Rationale	In order to be able to authenticate and authorize to a service, the STI shall provide capabilities for issuing, validation, renewal, and cancellation of digital identities. This requirement covers NIST security controls IA-4 c, IA-4 d and IA-4 e , SC-17.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0020
Requirement	The STI shall support the following tokens:+ Username or Identification number (plain text);+ X509 certificate (binary);+ SAML (XML text document).
Title	Supported Security Tokens
Status	<In Progress>
Rationale	This requirement states the security tokens supported by the Identity Management. This requirement covers NIST security control IA-2.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>

Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0030
Requirement	The STI shall be able to support inter-system identity information exchange by:+ Secure management, storage and use of security identity information;+ Provisioning and de-provisioning identity information across trusted security domains;+ Propagation and mapping identities across trust domains.
Title	SWIM Technical Infrastructure identity management interface
Status	<In Progress>
Rationale	The SWIM Technical Infrastructure is used to enable the exchanging of several types of information among several types of geographically distributed and federated systems interconnected at network level. The concept of identity federation is that a security token issued from one federated security system should be reused (repeatedly or as reissued) for consumptions of resources “located” in distinctive (federated) security systems. Such federation describes IT systems that have made agreement to trust each other and to mutually recognize issued user identities. In order to cover these objectives, identity management functionality is needed. Taking into account that such systems already use trusted Certification Authorities (CAs), it is required to assure the integration with the SWIM-TI Identity Management. This requirement also ensures that for password-based authentication systems, SWIM-TI Identity Management stores and transmits only encrypted representations of passwords. This requirement covers NIST security controls IA-4 (6) and IA-5 (1.c).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0040
Requirement	The STI shall provide an identity store in order to store (create/update/delete) the identities and security tokens.
Title	Identity and Security Tokens Store
Status	<In Progress>
Rationale	Identity repository/directory is used to store persistently digital identities and any relevant identity attributes. This requirement covers NIST security controls IA-4 c, IA-4 d and IA-4 e.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0050
Requirement	The STI shall offer functionality for the definition of user (and associated attributes), and their classification into groups, roles, and organisations.
Title	Identity definition and classification
Status	<In Progress>
Rationale	In order to store, use and manage digital identities, it is required to have available proper functions aiming at support the creation and the classification of users and the corresponding identities. This requirement covers NIST security controls IA-4 b and IA-4 c.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.02	N/A

<ALLOCATED TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0060
Requirement	The STI shall be able to establish trusted federation with other STIs.
Title	STI trusted Federation
Status	<In Progress>
Rationale	The STI shall be able to establish trusted federation with other STIs in order to provide security token conversion, authentication and authorization for tokens issued by trusted federation members. This requirement covers NIST Security Control 800.53 SC-17.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0070
Requirement	The STI shall allow to specify mapping rules enabling different digital identity representations issued by different STIs to be assigned to the same subject.
Title	STIs Identity Mapping Configuration
Status	<In Progress>
Rationale	The STI shall be able to establish trusted federation with other STIs in order to provide security token conversion, authentication and authorization for tokens issued by trusted federation members.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0080
Requirement	The STI shall allow to establish a Trust Federation with another STI not directly trusted by mapping its digital identities on those issued by a third STIs which is trusted by each one.
Title	STIs Trust Chain
Status	<In Progress>
Rationale	The STI shall be able to establish trusted federation with other STIs in order to provide security token conversion, authentication and authorization for tokens issued by trusted federation members. This requirement covers NIST Security Control 800.53 SC-17.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0090
Requirement	The STI Federation shall leverage on the following technical standards: +WS-Federation; +SAML 2.0 and higher.
Title	Identity Federation options
Status	<In Progress>
Rationale	In order to be able to consume services which belong to distinct security realms.
Category	<Functional><Security><Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour><ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>

Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0100
Requirement	The STI Federation shall be configurable through the exchange of federation meta-data documents.
Title	STI Federation Configuration mechanism
Status	<In Progress>
Rationale	In order to be able to consume services which belong to distinct security realms, Identity Management Federation shall be configurable through the exchange of federation meta-data documents. This requirement covers NIST security controls IA-4 (6) , SC-17.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Governance><ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0110
Requirement	The STI shall allow consumers to access resources with a single sign-on and sign-off mechanism within federated security domains.
Title	Federated access via STI
Status	<In Progress>
Rationale	In the heterogeneous environment of systems and stakeholders of SWIM-TI, a federated single sign-on for authentication can greatly simplify the difficulties associated to a user consumption of services from a different security domain. This requirement covers NIST security controls IA-2 (10) and IA-4 (6).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>

Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0002.0860
Requirement	The STI shall provide the possibility for a consumer in an Identity Federation Environment to sign-in and sign-out.
Title	STI federated sign-in and sign-out
Status	<In Progress>
Rationale	Once signed-in at a local system, the consumer will be authenticated and authorized to consume services provided by federated systems as well. This requirement covers NIST security control IA-4 (6).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0120
Requirement	The STI shall notify a Federated Security System if an entity of the Federated Security System is placed in a blacklist.
Title	Federated blacklisted entities
Status	<In Progress>
Rationale	Authentication blacklists are to be part of auditing to prevent further authentication attempts by blacklisted entities. SWIM-TI Security System will notify a Federated Security System of a blacklisted entity. This defines some minimal requirements the Authorization Policy shall obey.

	This requirement covers NIST security controls SI-5 c and CA-3 (5).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0130
Requirement	The STI shall provide the following mechanisms to release a blacklisted entity in a Federated Security System:+ Automatically after a Policy defined maximum blacklist period. + Manually.
Title	Liberation mechanisms of blacklisted entities
Status	<In Progress>
Rationale	Authentication blacklists are to be part of auditing to prevent further authentication attempts by blacklisted entities. SWIM-TI Security System needs to provide the appropriate mechanisms to release previously blacklisted entities. This requirement covers NIST security controls SI-5 c and CA-3 (5).
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<ALLOCATED TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0170
Requirement	The STI shall be able to apply digital signature to issued security tokens.
Title	Security Token signature
Status	<In Progress>
Rationale	In order to assure authenticity of security token, STI shall be able to apply digital signature using asymmetric key by X.509 certificate. This requirement covers NIST Security Control 800.53 SC-17.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0002.0320
Requirement	The STI shall provide a service capable of establishing timely constrained security sessions, which authenticate conversations between Service Consumers and Service Providers.
Title	STI creates and distributes cryptographic material
Status	<In Progress>
Rationale	In order to be able to establish a time-constrained secure conversation context, the STI shall be capable to create and provide cryptographic material to service consumers and providers. This requirement covers NIST security controls AC-12, IA-11 and SC-23.
Category	<Functional><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.2 Adaptability

This section includes adaptability requirements as documented in ISO/IEC 25010:2011. In particular, requirements included in this section refer to adaptability sub-characteristic of portability NFRs.

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.3 Performance Characteristics

This section includes performance efficiency requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with performance efficiency NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.3.3.1) time behaviour, (§3.3.3.2) resource utilization and (§3.3.3.3) capacity.

3.3.3.1 Time behaviour Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0216.0010
Requirement	The STS WS-Security Token request average response time shall be as follows: + Measurements: - 90% of the requests <= 1 s - 98% of the requests <= 2 s + Measurement conditions: - Request messages types: 33% Username/Password Token requests, 33% X.509 Tokens requests, 33% SAML Token requests - STS returns signed Tokens - Authentication (mutual), Authorization, Integrity and Confidentiality at transport level. - Full load, no overload. - Network characteristics: throughput of 100Mb/s, average latency of 200ms. - Session setup, session reuse or session creation time excluded from the measurements.
Title	STS WS-Security Token request average response time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average response time in the provided conditions for WS-Security Token requests. Request messages can also be renew requests. Measurements. Measured response time is as defined by SWIM Profile WP_PRF_01 NFR and in particular it represents a round-trip time including time spent over the network. Measurement Conditions. Average response time is measured by using a request messages data set composed by 33% of Username/Password Token requests, 33% of X.509 Tokens requests and 33% of SAML Token requests. Returned tokens are signed by the STS by enabling token verification based on STS signature checking. The presence of security controls (Authentication, Authorization, Integrity and Confidentiality at transport level) in the measurement conditions, reflects that these response times shall be met when all of these controls are active and performed during a request/response. Authentication at transport level may be part of a session setup: in such case the time spent for the Authentication at transport level will not be taken into account for targeted measurement (session reuse or session creation time excluded from the measurements). Average response time is measured relying on a network infrastructure having the provided characteristics (throughput of 100Mb/s and average latency of 200ms).
Category	<Performance>
Validation Method	

Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0216.0020
Requirement	The STS WS-Security Token request average processing time shall be as follows: + Measurements: - 90% of the requests <= 20 ms - 98% of the requests <= 40 ms + Measurement conditions: - Request messages types: 33% Username/Password Token requests, 33% X.509 Tokens requests, 33% SAML Token requests - STS returns signed Tokens - Full load, no overload.
Title	STS WS-Security Token request average processing time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average processing time in the provided conditions for WS-Security Token requests. Request messages can also be renew requests. Measurements. Processing time represents the period during which a request message is processed and related response time made available but not yet returned to the consumer. In particular it does not include time spent over the network (for both request and response messages). Measurement Conditions. Average processing time is measured by using a request messages data set composed by 33% of Username/Password Token requests, 33% of X.509 Tokens requests and 33% of SAML Token requests. Returned tokens are signed by the STS by enabling token verification based on STS signature checking. No specific measurement conditions are provided for the security controls, network characteristics and sessions setup, because those aspects do not impact the measured NFR (see definition of processing time).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>

Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0216.0030
Requirement	The STS WS-Security Token verification request average response time shall be as follows: + Measurements: - 90% of the requests <= 0.5 s - 98% of the requests <= 1 s + Measurement conditions: - Request messages types: 33% Username/Password Tokens verification requests, 33% X.509 Tokens verification requests, 33% SAML Tokens verification requests. - Authentication (mutual), Authorization, Integrity and Confidentiality at transport level. - Full load, no overload. - Network characteristics: throughput of 100Mb/s, average latency of 200ms. - Session setup, session reuse or session creation time excluded from the measurements.
Title	STS WS-Security Token verification request average response time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average response time in the provided conditions for WS-Security Token verification requests. In particular the verification is not based on the (local) check of STS's signature (token being verified is not signed by the issuing STS). Measurements. Measured response time is as defined by SWIM Profile WP_PRF_01 NFR and in particular it represents a round-trip time including time spent over the network. Measurement Conditions. Average response time is measured by using a request messages data set composed by 33% of Username/Password Token verification requests, 33% of X.509 Tokens verification requests and 33% of SAML Token verification requests. The presence of security controls (Authentication, Authorization, Integrity and Confidentiality at transport level) in the measurement conditions, reflects that these response times shall be met when all of these controls are active and performed during a request/response. Authentication at transport level may be part of a session setup: in such case the time spent for the Authentication at transport level will not be taken into account for targeted measurement (session reuse or session creation time excluded from the measurements). Average response time is measured relying on a network infrastructure having the provided characteristics (throughput of 100Mb/s and average latency of 200ms).
Category	<Performance>

Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0216.0040
Requirement	The STS WS-Security Token verification request average processing time shall be as follows: + Measurements: - 90% of the requests <= 10 ms - 98% of the requests <= 20 ms + Measurement conditions: - Request messages types: 33% Username/Password Token verification requests, 33% X.509 Tokens verification requests, 33% SAML Token verification requests - STS returns signed Tokens - Full load, no overload.
Title	STS WS-Security Token verification request average processing time
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. This requirement provides the average processing time in the provided conditions for WS-Security Token verification requests. Measurements. Processing time represents the period during which a request message is processed and related response time made available but not yet returned to the consumer. In particular it does not include time spent over the network (for both request and response messages). Measurement Conditions. Average processing time is measured by using a request messages data set composed by 33% of Username/Password Token verification requests, 33% of X.509 Tokens verification requests and 33% of SAML Token verification requests. No specific measurement conditions are provided for the security controls, network characteristics and sessions setup, because those aspects do not impact the measured NFR (see definition of processing time).
Category	<Performance>
Validation Method	
Verification Method	<Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>

Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.3.2 Resource utilization Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.3.3 Capacity Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0214.0080
Requirement	The STS shall support up to 1500 password resets per months.
Title	STS capacity in terms of supported password resets/months
Status	<In Progress>
Rationale	Given the current estimated STS capacity in terms of managed digital identities (REQ-14.01.04-TS-0214.0090) for the ground systems, it is estimated that 20% of total managed tokens will Username/Password tokens (10000). About 15% of them are lost and need to be reset each month.
Category	<Performance><Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0214.0090
Requirement	The STS shall be able to manage up to 50000 digital identities for ground SWIM systems.

Title	STS capacity in terms of managed digital identities
Status	<In Progress>
Rationale	The capacity requirement is related to the whole set of STSs contributing to the European SWIM whatever is the deployment strategy. In case of centralized deployment is used the single STS shall meet the requirement. In case a federated or hierarchical deployment is preferred the capacity has to be spread over all the STSs. The number of ground systems using SWIM and being authenticated is estimated to about 5000 (40 met-providers, 1 EAD, 1 NM, 1800 Airports, 1200 Airlines, 10 centralized services) with average numbers of tokens/month per connected system of 10 (5000x10=50000).
Category	<Performance><Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.4 Safety & Security

This section includes security requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with security NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.3.4.1) confidentiality, (§3.3.4.2) integrity, (§3.3.4.3) non-repudiation, (§3.3.4.4) accountability and (§3.3.4.5) authenticity. Furthermore, according to SJU guidelines, a dedicated subsection (§3.3.4.6) is provided for safety requirements.

[REQ]

Identifier	REQ-14.01.04-TS-0402.0010
Requirement	Communication between the STI and service consumers and providers shall be secured (authentication, authorization, integrity, confidentiality).
Title	STI Security
Status	<In Progress>
Rationale	In order to establish a secure communication, communication between the STI and service consumers and providers shall be adequately secured regarding authentication, authorization, integrity, and confidentiality. This requirement covers NIST security control IA-4 (5).
Category	<Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.4.1 Confidentiality Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.4.2 Integrity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.4.3 Non-repudiation Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.4.4 Accountability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.4.5 Authenticity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.4.6 Safety Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.5 Maintainability

This section includes maintainability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with maintainability NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.3.5.1) modularity, (§3.3.5.2) reusability, (§3.3.5.3) analysability, (§3.3.5.4) modifiability and (§3.3.5.5) testability.

3.3.5.1 Modularity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.5.2 Reusability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.5.3 Analysability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.5.4 Modifiability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.5.5 Testability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.6 Reliability

This section includes reliability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with reliability NFR sub-characteristics described in ISO/IEC 25010:2011: (§3.3.6.1) maturity, (§3.3.6.2) availability, (§3.3.6.3) fault tolerance and (§3.3.6.4) recoverability.

3.3.6.1 Maturity Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.6.2 Availability Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0616.0010
Requirement	The STS availability shall be as follows: + Measurement: 99,95% + Measurement conditions: - Not Including planned outages, - Full load, no overload, + Observation period: 1 month
Title	STS Availability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. STS is an enabling/supporting service used to retrieve and verify (optionally) security tokens that are used to authenticate ATM services consumers. Unavailability of STS may impact the consumption of the ATM service in one of the following cases: (i) ATM Service consumer requests a security token to consume the ATM service but the STS is not available; (ii) Security token of the ATM Service consumer is expired, it requests security token renewal/ new security token but the STS is not available; (iii) [optional – typically it could be verified also by verifying STS signature of the token] ATM Service provider requests ATM service consumer's token verification but the STS is not available. In all these cases the ATM Service consumer cannot be authenticated and therefore the service cannot be consumed. In theory, STS availability should be closed/equal to ATM Service(s) availability. In practice, being the STS a supporting service and taking into account that (i) not all the ATM service consumption requests require the involvement of the STS because not yet expired security tokens may be reused in several ATM services consumption requests; (ii) not all the security token verification require the involvement of the STS because the verification may just consist in checking the signature of the token; (iii) some ATM service may offer the possibility (e.g. WS-SecurityPolicy) to use (e.g. degraded mode) transport level authentication as valid alterative to message level authentication (token) and (iv) the same STS may be used to support the consumption of ATM Services with very different and heterogeneous availability, it is reasonable to require an availability of STS less than ATM services availability trying to establish the right trade-off between costs and needs.

	More demanding (in terms of availability) ATM Services may require (e.g. Security Policy) (i) tokens with longer validity period to minimize the probability that the STS is not available when a new token (or renewal) is required and (ii) to use token verification based of STS signature verification (issued tokens are signed by the STS). The required availability for the STS (99,95%) has been derived according to above considerations and it is independent of whatever deployment options and fault tolerance techniques are adopted for the STS. Assuming 30 workdays per month, 22 working hours a day and planned outages executed in the remaining 2 hours a day, the required availability ensures a maximum down time, due to un-planned outages, of 19 minutes/month.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0616.0020
Requirement	The STS Continuous unavailability shall be as follows: + Measurement: <= 2 minutes + Measurement conditions: - Not Including planned outages, - Full load, no overload, + Observation period: 1 hour
Title	STS Continuous unavailability
Status	<In Progress>
Rationale	The requirement is expressed in a specific form as documented in 14.01.04 Requirements Guidelines. STS is an enabling/supporting service used to retrieve and verify (optionally) security tokens that are used to authenticate ATM services consumers. Unavailability of STS may impact the consumption of the ATM service in one of the following cases: (i) ATM Service consumer requests a security token to consume the ATM service but the STS is not available; (ii) Security token of the ATM Service consumer is expired, it requests security token renewal/ new security token but the STS is not available; (iii) [optional – typically it could be verified also by verifying STS signature of the token] ATM Service provider requests ATM service consumer's token verification but the STS is not available.

	In all these cases the ATM Service consumer cannot be authenticated and therefore the service cannot be consumed. In theory, STS continuous unavailability should be closed/equal to ATM Service(s) continuous unavailability. In practice, due to the purpose of the STS and taking into account considerations provided in the rationale of the STS availability requirement REQ-14.01.04-TS-0616.0010 a continuous unavailability of 2 minutes/hour is considered acceptable independently of the specific ATM service requirements and whatever deployment options and fault tolerance techniques are adopted for the STS. Considering current STS availability requirement REQ-14.01.04-TS-0616.0010 and assuming for the STS 30 workdays per month, 22 working hours a day and planned outages executed in the remaining 2 hours a day, the maximum total unavailability a month is of 19 minutes/month. Taking into account this requirement and the maximum of 2 minutes/hour of continuous unavailability the design of STS solutions (including fault tolerance techniques) has to make sure that this constraint on continuous unavailability/ hour is met and that, in order to meet the constraint on total unavailability/month, a maximum of 9 failures/month may occur (9 * 2 = 18 minutes = maximum unavailability a month).
Category	<Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0816.0010
Requirement	STS Planned Outages shall be scheduled for a time of the day when ATM activities are at their lowest and maintenance window shall never exceed 2hrs/day.
Title	STS Planned Outages
Status	<In Progress>
Rationale	This requirement provides constrains on the scheduling of planned outages for the STS. This requirement complements the STS availability requirement REQ-14.01.04-TS-0616.0010 by ensuring that the planned outages and related maintenance window are properly scheduled in order to minimize the impact on the overall ATM activities. Provided constrains are in relationship with Security Token validity period. Current specification constrains only the maximum validity period and the provided value is coherent with maintenance window. For what concerns Tokens with validity period less than the maintenance window, it is recommended to foreseen token renewal in such a way the impact on the activities due to planned outages is minimized.

Category	<Design><Reliability>
Validation Method	
Verification Method	<Analysis>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0616.0040
Requirement	STS endpoints shall use the latest updates of identity information within a timespan of: + Measurements: - 5 minutes in the nominal case. - 1 hours in case of unexpected problems + Measurement conditions: - None relevant
Title	STS Endpoints consistency
Status	<In Progress>
Rationale	In case multiple STS endpoints are used, depending on the underlying implementation various forms of inconsistency can occur. For example in order to provide high availability, there could be multiple master databases that replicate with each other as well as multiple service instances. As replication is not necessarily instantaneous (e.g. because not using a distributed transaction), inconsistency could occur both at the time of token request as well as at the time of validation request depending on the STS endpoint that is used. In the nominal case it is required that all the endpoints have a coherent state (latest identity information) within a timespan of 5 minutes. In other words, in 5 minutes STS endpoint different relying parties will use, the returned responses will always be consistent and coherent. In all cases with no exception, the consistency shall be ensured within a timespan of 1h.
Category	<Reliability>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance

<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.6.3 Fault Tolerance Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0816.0020
Requirement	The SWIM-TI STS solutions should be implemented by leveraging on replication techniques.
Title	STS replication
Status	<In Progress>
Rationale	Due to its roles in supporting secure interactions STS solutions should provide High Availability configurations. This can be achieved by adopting replication techniques consisting in providing one or more replicas of the service and switching/routing clients' requests among all service instances, increasing both STS performances and availability. This requirement covers NIST security controls SC-36 and SI-13b.
Category	<Design><Reliability>
Validation Method	
Verification Method	<Analysis><Review of Design>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0816.0030
Requirement	SWIM-TI STS solutions should ensure failure transparency by masking to its consumers the failure and possible recovery.
Title	STS failure transparency
Status	<In Progress>
Rationale	Due to its roles in supporting secure interactions STS solutions should provide High Availability configurations by adopting replication and in general fault tolerance (detection, isolation, containment, etc.) techniques increasing both STS performances and availability. Failure transparency techniques mask from an object the failure and possible recovery of other objects (or itself) to enable fault tolerance. This requirement applies when an STS consumer has already discovered an STS endpoint which is being

	used to interact with the STS. This requirement covers NIST security controls SI-13 (4)
Category	<Design><Reliability>
Validation Method	
Verification Method	<Analysis><Review of Design>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0816.0040
Requirement	SWIM-TI STS solutions shall provide mechanisms to detect, handle and report the occurrence of failures cause by the following security incidents: + Software Failure + Hardware Failure + Denial of Service + Compromised information + Network unavailability
Title	STS Failure detection, handling and reporting
Status	<In Progress>
Rationale	This requirement ensures that the SWIM-TI STS solution provides a functionality aiming at reporting the handling of incidents that may have an impact on security. This requirement covers with NIST security control AU-2 a and AU-3.
Category	<Design><Reliability>
Validation Method	
Verification Method	<Analysis><Review of Design>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.6.4 Recoverability Requirements

[REQ]

Identifier	REQ-14.01.04-TS-0616.0030
Requirement	A Recovery Point Objective (RPO) for the STS shall be at least the point in time, before the disruption event has occurred, when latest security token was issued by the STS.
Title	STS Recovery Point Objective
Status	<In Progress>
Rationale	[ISO/IEC 27031] RPO is point in time to which data must be recovered after a disruption has occurred. For the STS this means to analyse acceptable data loss about issued tokens. Of course the analysis may depend on the security token requests frequency but currently (due to the heterogeneous ATM services may rely on the STS) it is not possible to assume such figure. The approach adopted is to estimate the RPO according to the STS role and purpose in supporting secure ATM services consumption. In particular, what will happen if a STS does successfully issue a security token but after a recovery from a failure it loses that information (from its recovered state, that token has been never issued)? The main impacts of such events are related to the token verification on ATM service provider side. There are two valid options for security token verification: (a) ATM service provider requests STS to verify the token; (b) the ATM service provider verifies the token by verifying its signature (STS does sign the token it issues). In case (a), if the token is not known by the STS, the verification fails and the ATM service consumer has to request a new token. This will decrease overall performances of the ATM interactions. In case (b), even if the token is not known by the STS, the verification will not fail. If an accident occurs while consuming the ATM service using than token, STS logs/records may be required (e.g. non repudiation): STS will provide an inconsistent state because it could happen that the STS records include events about the issuing of that token but the recovered state was not consistent with those events. According to above considerations it is required that the RPO for the STS is next to zero minutes. The provided RPO ensures that the recovered state is at least the latest security token issued by the STS before the disruption even has occurred. "At least" means that, if a new security token will be required during the recovery, that one could be used to recover from the event. The requirement is expected to be used to properly design and implement STS solutions. In particular, the required RPO for the STS implies that synchronous or quasi-synchronous replication/backup solutions are foreseen in the technical design of the STS. The required RPO for the STS has been derived according to above considerations and it is independent of whatever deployment options are adopted for the STS. It is anticipated that required RPO is expected to be met according to business impact, threat and risk analysis documented in the business continuity planning. In case an incident occurs and it is not part of the business continuity planning, it may happen that the RPO may be not met. This requirement covers NIST security controls CP-2 a.2.
Category	<Reliability><Design>
Validation Method	
Verification Method	<Analysis><Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>

Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.7 Internal Data Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.8 Design and Construction Constraints

This section includes compatibility and portability requirements as documented in ISO/IEC 25010:2011. The structure of the section is in accordance with sub-characteristics of both compatibility and portability NFR described in ISO/IEC 25010:2011: (§3.3.8.1) co-existence and (§3.3.8.2) interoperability compatibility NFR sub-characteristics, (§3.3.8.3) installability and (§3.3.8.4) replaceability portability NFR sub-characteristics.

[REQ]

Identifier	REQ-14.01.04-TS-0814.0110
Requirement	The maximum validity period of an issued security token shall be 12 hours.
Title	STS issued Security Tokens minimum validity period
Status	<In Progress>
Rationale	The provided value for the Security Tokens validity period is a reasonable trade-off between possible security issues and network bandwidth, and more in general resources, consumption.
Category	<Design>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD><SLA>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.8.1 Co-existence Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.8.2 Interoperability Requirements

3.3.8.2.1 Common Time

Requirements included in §3.1 are applicable.

3.3.8.2.2 Standards

This section introduces, in the scope of the STI, the standards that are applicable to Interfaces through which interoperability is provided or required with and for participants that are external to the SWIM-TI as well as participants that are internal to the SWIM-TI.

Each technical configuration at the level of such Interfaces that requires adherence to one or more standards to support and promote interoperability, includes these standards by referencing the standards in this section.

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0122
Requirement	W3C Recommendation SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) 27 April 2007 http://www.w3.org/TR/soap12-part1/ shall be supported. W3C Recommendation SOAP Version 1.2 Part 2: Adjuncts (Second Edition) 27 April 2007 http://www.w3.org/TR/2007/REC-soap12-part2-20070427/ shall be supported.
Title	Interoperability standard. SOAP 1.2
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0123
Requirement	W3C Recommendation SOAP Message Transmission Optimization Mechanism 25 January 2005 http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/ shall be supported.
Title	Interoperability standard. MTOM
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.

Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Messaging Bridging><BP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0125
Requirement	W3C Note Web Services Description Language (WSDL) 1.1 15 March 2001 http://www.w3.org/TR/wsdl shall be supported.
Title	Interoperability standard. WSDL 1.1
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><BP Core><PP Messaging Bridging>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<ALLOCATED_TO>	<Functional block>	Blue Profile	N/A
<ALLOCATED_TO>	<Functional block>	Purple Profile	N/A
<SATISFIES>	<Enabler>	A/C-57	<Full>
<SATISFIES>	<Enabler>	AGSWIM-34	<Full>
<SATISFIES>	<Enabler>	AGSWIM-43	<Full>
<SATISFIES>	<Enabler>	AGSWIM-44	<Full>
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	AGSWIM-41	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-06b	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-APS-05b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-01b	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>
<SATISFIES>	<Enabler>	ER APP ATC 160	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0126
Requirement	W3C Member Submission Binding Extension for SOAP 1.2 05 April 2006 http://www.w3.org/Submission/wsdl11soap12/ shall be supported.
Title	Interoperability standard. WSDL 1.1 binding extension for SOAP 1.2
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0127
Requirement	W3C Recommendation Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language 26 June 2007 http://www.w3.org/TR/wsdl20/ shall be supported. W3C Recommendation Web Services Description Language (WSDL) Version 2.0 Part 2: Adjuncts 26 June 2007 http://www.w3.org/TR/2007/REC-wsdl20-adjuncts-20070626/ shall be supported.
Title	Interoperability standard. WSDL 2.0
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core><PP Messaging Bridging>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0130
Requirement	OASIS WSI Basic Profile Version 2.0, Final Material, 2010-11-09 http://ws-i.org/profiles/basicprofile-2.0-2010-11-09.html shall be supported in the following manner: A requirement with a reference to this WSI standard does not imply inclusion of all the standards referenced in this WSI standard. The content of this WSI standard overrides all the standards referenced in this WSI standard in so far these standards are referenced at peer level in the same requirement
Title	Interoperability standard. WSI BP 2.0
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication

	consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0136
Requirement	OASIS Standard Specification Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) 1 February 2006 https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf shall be supported.
Title	Interoperability standard. WS-Security 1.1
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-8 (1)
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0137
Requirement	OASIS Standard incorporating Approved Errata 01 WS-SecurityPolicy 1.3 25 April 2012 http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html shall be supported.
Title	Interoperability standard. WS-SecurityPolicy 1.3

Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls SC-8 (1)
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0138
Requirement	W3C Recommendation Web Services Policy 1.5 - Framework 04 September 2007 http://www.w3.org/TR/2007/REC-ws-policy-20070904/ shall be supported.
Title	Interoperability standard. Web Services Policy 1.5
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>

<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0141
Requirement	OASIS Standard WS-Trust 1.4 incorporating Approved Errata 01 25 April 2012 http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf shall be supported.
Title	Interoperability standard. WS-Trust 1.4
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-4 (6).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0142
Requirement	W3C Recommendation Web Services Addressing 1.0 - Core 9 May 2006 http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/ shall be supported.
Title	Interoperability standard. WS-Addressing 1.0
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability.
Category	<Interoperability>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0152
Requirement	OASIS Standard Web Services Security SAML Token Profile 1.1 1 February 2006 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf shall be supported.
Title	Interoperability standard; WSSE SAML Token Profile 1.1
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls IA-8 and IA-9.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0177
Requirement	OASIS Standard Web Services Federation Language (WS-Federation) Version 1.2 22, May 2009 http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf shall be supported.
Title	Interoperability standard. WS-Federation
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security control IA-4 (6).
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>

Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0186
Requirement	W3C Recommendation Web Services Policy 1.5 - Attachment 04 September 2007 http://www.w3.org/TR/ws-policy-attach/ shall be supported.
Title	Interoperability standard. WS-PolicyAttachment
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls AC-1 a.2 and IA-1 a.2.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0150
Requirement	OASIS Standard Specification Web Services Security UsernameToken Profile

	1.1 1 February 2006 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-UsernameTokenProfile.pdf shall be supported.
Title	Interoperability standard. WSSE Security UsernameToken Profile 1.1
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls IA-2, IA-8 and IA-9.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Core>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

[IREQ]

Identifier	REQ-14.01.04-TS-0811.0151
Requirement	OASIS Standard Specification Web Services Security X.509 Certificate Token Profile 1.1 1 February 2006 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf shall be supported.
Title	Interoperability standard; WSSE X.509 Certificate Token Profile 1.1
Status	<Validated>
Rationale	Compliance with well-known and widely used standard promotes interoperability. This requirement covers NIST security controls IA-2, IA-8 and IA-9.
Category	<Interoperability><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<ATM service><SWIM-TI provider>
Roles	<Service provider><Service consumer><Subscriber><Publisher><Publication consumer><Subscription handler><Publication mediator>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable><Interoperability testable>

[IREQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A

<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	MSG	N/A
<ALLOCATED_TO>	<Functional block>	Yellow Profile	N/A
<SATISFIES>	<Enabler>	GGSWIM-51c	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05a	<Full>
<SATISFIES>	<Enabler>	SWIM-INFR-05b	<Full>

3.3.8.3 Installability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.8.4 Replaceability Requirements

Requirements concerning this category have not been identified during SESAR 1 programme. This requirement category may be further investigated according to the evolution of the SWIM-TI Technical Specifications.

3.3.9 Interface Requirements

This section includes interface requirements applicable to the STI.

[REQ]

Identifier	REQ-14.01.04-TS-0902.0010
Requirement	The STI shall provide interfaces (B2B, HMI) for trust/federation configuration.
Title	Security Token Service Federation Configuration Interfaces
Status	<In Progress>
Rationale	In order to be able enter meta-data documents, the STI shall provide interfaces (B2B, HMI) for trust/federation configuration. This requirement covers NIST security control IA-4 (6).
Category	<Functional><Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0140
Requirement	The STI shall provide an interface (B2B, HMI) for administration of digital identities
Title	Identity Administration Interface
Status	<In Progress>
Rationale	When using Security Token-based digital identities, STI is in charge of managing identities lifecycle including creation, utilization and termination. In order to run such capabilities an Administration Interface shall be exposed by the STI.
Category	<Functional><Security><Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour><ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<Yes>
Testability	<Applicable but not testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0150
Requirement	The STI shall be able to interact with the PKI to retrieve a X.509 certificate.
Title	STI interaction with PKI - retrieving certificates
Status	<In Progress>
Rationale	When using X.509 tokens to perform authentication, STI shall be able to retrieve and verify X.509 certificates to the PKI in charge of managing those certificates.
Category	<Functional><Security><Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour><ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>
Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0016.0160
Requirement	The STI shall be able to interact with the PKI to verify a X.509 certificate.
Title	STI interaction with PKI - verifying certificates
Status	<In Progress>
Rationale	When using X.509 tokens to perform authentication, The STI shall be able to retrieve and verify X.509 certificates to the PKI in charge of managing those certificates.
Category	<Functional><Security><Interface>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<Not applicable>
Domain of interest	<Function/Behaviour><ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider>
Selfstanding set	<Not applicable>
Conformance	<No>
High Level	<No>

Testability	<Conformance testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.02	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.9.1 External Service Interface Bindings

There are no specific external interfaces for the STI. The external service interface requirements included in §3.1 are applicable.

3.3.9.2 Internal Service Interface Bindings

In this section, the available STI Security Token Service (STS) interface bindings are provided. This first one is based on SOAP 1.2 with all security controls at message level and the second one (still SOAP 1.2 based) but using TLS to provide confidentiality, integrity and authenticity at transport level.

[REQ]

Identifier	REQ-14.01.04-TS-0916.0010
Requirement	STS services shall be instantiated over the following interface binding. + Protocol stack: - SOAP 1.2 with WS-Security 1.1 authentication through UsernameToken 1.1, WSSE SAML Token Profile 1.1 combined and/or WSSE SAML Token Profile 1.1 with any of WS-Trust 1.4, WS-Federation 1.2 over HTTP POST over TCP. + MEPs: - SRR-MEP + Fault handling: - the service shall be able to determine the content of the HTTP status code and HTTP reason phrase + Encoding: - Text encoding + Security - Confidentiality: message level - Integrity: message level - Authenticity: message level mutual - Authorization: message level - Non-repudiation: message level + Contract: - formalism of contract description: WSDL 1.1 and optionally WSDL 2.0 both including WS-SecurityPolicy, WS-Trust 1.4, WS-Federation 1.2. - minimum: WS-Trust. - reference: OASIS. + Interoperability: WS-I Basic Profile 2.0, WSI- Basic Security Profile 1.1
Title	STS Interface Binding. SOAP 1.2 with WS-Security 1.1, WS-Trust 1.4, WS-

	Federation 1.2, and authentication through UsernameToken 1.1, WSSE X.509 Certificate Token Profile 1.1 and/or WSSE SAML Token Profile 1.1 over HTTP POST over TCP.
Status	<In Progress>
Rationale	This binding provides access to advanced security features with security controls at message level. HTTP Basic and Digest Access Authentication are transport level security techniques and they are not supported by this binding.
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0111	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0115	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0122	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0123	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0125	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0126	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0127	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0130	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0132	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0133	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0134	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0136	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0137	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0138	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0141	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0142	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0152	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0177	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0186	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0150	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0151	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0402.0010	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

[REQ]

Identifier	REQ-14.01.04-TS-0916.0020
Requirement	STS services shall be instantiated over the following interface binding. + Protocol stack:

	- SOAP 1.2 with any of WS-Trust 1.4, WS-Federation 1.2 over HTTPS POST over TCP. + MEPs: - SRR-MEP + Fault handling: - the service shall be able to determine the content of the HTTP status code and HTTP reason phrase + Encoding. - Text encoding + Security - Confidentiality: transport level - Integrity: transport level - Authenticity: transport level mutual - Authorization: transport level - Non-repudiation: transport level + Contract: - formalism of contract description: WSDL 1.1 and optionally WSDL 2.0 both including WS-SecurityPolicy, WS-Trust 1.4, WS-Federation 1.2. - minimum: WS-Trust. - reference: OASIS. + Interoperability: WS-I Basic Profile 2.0, WSI- Basic Security Profile 1.1
Title	STS Interface Binding. SOAP 1.2 with WS-Security 1.1, WS-Trust 1.4, WS-Federation 1.2, and authentication through UsernameToken 1.1, WSSE X.509 Certificate Token Profile 1.1 and/or WSSE SAML Token Profile 1.1 over HTTP POST over TCP.
Status	<In Progress>
Rationale	This binding provides access to advanced security features with security controls at transport level. Authenticity (or Authentication) at transport level has not to be confused with HTTP Basic and Digest Access Authentication that are not supported by this binding.
Category	<Interface><Security>
Validation Method	
Verification Method	<Review of Design><Test>
Profile Part	<YP Security+>
Domain of interest	<ICD>
Point of view	<SWIM-TI provider>
Roles	<Identity Management provider><Identity Management consumer>
Selfstanding set	<Internal service binding>
Conformance	<No>
High Level	<Yes>
Testability	<Conformance testable><Interoperability testable>

[REQ Trace]

Relationship	Linked Element Type	Identifier	Compliance
<APPLIES_TO>	<Operational Focus Area>	ENB02.01.01	N/A
<ALLOCATED_TO>	<Project>	14.02.09	N/A
<ALLOCATED_TO>	<Functional block>	SEC	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0101	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0111	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0115	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0122	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0123	N/A

<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0125	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0126	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0127	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0130	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0132	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0133	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0134	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0137	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0138	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0141	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0142	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0177	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0186	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0112	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0113	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0114	N/A
<INCLUDES>	<ATMS Requirement>	REQ-14.01.04-TS-0811.0116	N/A
<SATISFIES>	<ATMS Requirement>	REQ-14.01.04-TS-0402.0010	<Full>
<SATISFIES>	<Enabler>	GGSWIM-59c	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03b	<Full>
<SATISFIES>	<Enabler>	SWIM-SUPT-03a	<Full>

3.3.9.3 Network Interface Bindings

There are no network technical interface requirements specific for the STI. The network technical interface requirements included in §3.1 are applicable.

3.3.9.4 Network Requirements

There are no network requirements specific for the STI. The network requirements included in §3.1 are applicable.

4 Assumptions

None

5 References

[1] Template Toolbox 03.01.01
https://extranet.sesarju.eu/Programme%20Library/SESAR%20Template%20Toolbox.dot

[2] Requirements and V&V Guidelines 03.01.00
https://extranet.sesarju.eu/Programme%20Library/Requirements%20and%20VV%20Guidelines.doc

[3] Templates and Toolbox User Manual 03.01.00
https://extranet.sesarju.eu/Programme%20Library/Templates%20and%20Toolbox%20User%20Manual.doc

[4] EUROCONTROL ATM Lexicon
https://extranet.eurocontrol.int/http://atmlexicon.eurocontrol.int/en/index.php/SESAR

[5] SOA Service Interaction Security Patterns, http://soapatterns.org/masterlist_c.php

[6] Eurocae WG59, ED-133 Flight Object interoperability specification, June 2009

[7] 08.03.10 D65 ISRM 2.0, June 2016.

[8] 14.01.04.D43-001, SWIM-TI Technical Specifications Catalogue 3.1, Edition 00.01.00, December 2015.

[9] 14.02.09 D36-001, SWIM TI V3.0.0 Verification Report, November 2015.

[10]14.02.09 D36-002, SWIM TI V3.0.1 Verification Report, April 2016.

[11] 14.02.09 D85. WP1.3.1 Preliminary Solution Evaluations Report - V2, March 2016.

[12]14.01.03 D30, SWIM Architectural Definition Final, Edition 00.01.00, June 2016.

[13]14.01.03 D39, SWIM Profiles Final, Edition 00.01.00, June 2016.

[14]14.01.04.D44-001, SWIM-TI Technical Specifications Catalogue, Edition 00.01.00, July 2016

[15]IETF RFC 4510 Proposed Standard, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006 http://www.rfc-editor.org/rfc/rfc4510.txt

[16]IETF RFC 5280 Proposed Standard, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 http://www.rfc-editor.org/rfc/rfc5280.txt

[17]IETF RFC 4523 Proposed Standard, Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates, June 2006 http://www.rfc-editor.org/rfc/rfc4523.txt

[18]IETF RFC 5055 Proposed Standard, Server-Based Certificate Validation Protocol (SCVP), December 2007 http://www.rfc-editor.org/rfc/rfc5055.txt

[19]IETF RFC 5816 Proposed Standard, RFC ESSCertIDv2 Update for RFC 3161, March 2010 http://www.rfc-editor.org/rfc/rfc5816.txt

[20]IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) August 2001 http://www.rfc-editor.org/rfc/rfc3161.txt

[21]IETF RFC 5652 Internet Standard, Cryptographic Message Syntax (CMS), September 2009 http://www.rfc-editor.org/rfc/rfc5652.txt

[22]RSA Laboratories PKCS #12 v1.1: Personal Information Exchange Syntax, October 27, 2012 Standard http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm

[23]W3C Recommendation SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) 27 April 2007 http://www.w3.org/TR/soap12-part1/

[24]W3C Recommendation SOAP Version 1.2 Part 2: Adjuncts (Second Edition) 27 April 2007 http://www.w3.org/TR/2007/REC-soap12-part2-20070427/

[25]W3C Recommendation SOAP Message Transmission Optimization Mechanism 25 January 2005 http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/

[26]W3C Note Web Services Description Language (WSDL) 1.1 15 March 2001 http://www.w3.org/TR/wsdl

[27]W3C Member Submission Binding Extension for SOAP 1.2 05 April 2006 http://www.w3.org/Submission/wsdl11soap12/

[28]W3C Recommendation Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language 26 June 2007 http://www.w3.org/TR/wsdl20/

[29]W3C Recommendation Web Services Description Language (WSDL) Version 2.0 Part 2: Adjuncts 26 June 2007 http://www.w3.org/TR/2007/REC-wsdl20-adjuncts-20070626/

[30]OASIS Standard Specification Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) 1 February 2006 https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[31]W3C Recommendation Web Services Policy 1.5 - Framework 04 September 2007 http://www.w3.org/TR/2007/REC-ws-policy-20070904/

[32]W3C Recommendation Web Services Addressing 1.0 - Core 9 May 2006 http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/

[33]W3C Recommendation Web Services Policy 1.5 - Attachment 04 September 2007 http://www.w3.org/TR/ws-policy-attach/

[34]IETF RFC 1122 Internet Standard, Requirements for Internet Hosts -- Communication Layers, October 1989 http://tools.ietf.org/html/rfc1122

[35]IETF RFC 793 Transmission Control Protocol September 1981 http://tools.ietf.org/html/rfc793

[36]IETF RFC 2246 The TLS Protocol Version 1.0 January 1999 http://tools.ietf.org/html/rfc2246

[37]IETF 2616 Hypertext Transfer Protocol -- HTTP/1.1 June 1999 http://tools.ietf.org/html/rfc2616

[38]IETF RFC 4346 The Transport Layer Security (TLS) Protocol Version 1.1 April 2006 http://tools.ietf.org/html/rfc4346

[39]IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2 August 2008 http://tools.ietf.org/html/rfc5246

[40]IETF RFC 6176 Prohibiting Secure Sockets Layer (SSL) Version 2.0 March 2011 http://tools.ietf.org/html/rfc6176

[41]IETF informational RFC 2818 HTTP Over TLS May 2000 http://tools.ietf.org/html/rfc2818

[42]IETF RFC 768 User Datagram Protocol 28 August 1980 http://tools.ietf.org/html/rfc768

[43]IETF RFC 791 Internet Protocol September 1981 http://tools.ietf.org/html/rfc791

[44]IETF RFC 2460 Internet Protocol, Version 6 (IPv6) Specification December 1998 http://tools.ietf.org/html/rfc2460

[45]IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP June 2013 http://tools.ietf.org/html/rfc6960

[46]IETF RFC 4158 Internet X.509 Public Key Infrastructure: CertificationPathBuilding September 2005 http://tools.ietf.org/html/rfc4158

[47]IETF RFC 6434, Memo, IPv6 Node Requirements, December 2011 http://tools.ietf.org/html/rfc6434

[48]IETF RFC 792 Internet Standard, INTERNET CONTROL MESSAGE PROTOCOL, September 1981 http://tools.ietf.org/html/rfc792

[49]IETF RFC 950, Internet Standard, Internet Standard Subnetting Procedure, August 1985 http://tools.ietf.org/html/rfc950

[50]IETF RFC 6918 Proposed Standard, Formally Deprecating Some ICMPv4 Message Types, April 2013 http://tools.ietf.org/html/rfc6918

[51]IETF 5905 Proposed Standard, Network Time Protocol Version 4: Protocol and Algorithms Specification https://tools.ietf.org/html/rfc5905

[52]OASIS WSI Basic Profile Version 2.0, Final Material, 2010-11-09 http://ws-i.org/profiles/basicprofile-2.0-2010-11-09.html

[53]OASIS Standard Web Services Base Notification 1.3 (WS-BaseNotification) 1 October 2006 http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.pdf

[54]OASIS Standard Web Services Brokered Notification 1.3 (WS-BrokeredNotification), 1 October 2006 http://docs.oasis-open.org/wsn/wsn-ws_brokered_notification-1.3-spec-os.pdf

[55]OASIS Standard Web Services Topics 1.3 (WS-Topics) 1 October 2006 http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf

[56]OASIS Standard incorporating Approved Errata 01 WS-SecurityPolicy 1.3 25 April 2012 http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html

[57]OASIS Standard WS-Trust 1.4 incorporating Approved Errata 01 25 April 2012 http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf

[58]OASIS Standard Web Services Security SAML Token Profile 1.1 1 February 2006 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf

[59]OASIS Standard Web Services Federation Language (WS-Federation) Version 1.2 22, May 2009 http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

[60]OASIS Standard Specification Web Services Security UsernameToken Profile 1.1 1 February 2006 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-UsernameTokenProfile.pdf

[61]OASIS Standard Specification Web Services Security X.509 Certificate Token Profile 1.1 1 February 2006 http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf

[62]IETF RFC 4033 Domain Name System Security Extensions (DNSSEC), March 2005 https://tools.ietf.org/html/rfc4033.

[63] IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 https://www.ietf.org/rfc/rfc3647.txt.

[64] Security Requirements for Cryptographic Modules US Federal Information Processing Standard (FIPS 140-2), May 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[65] IETF RFC 7568 Deprecating Secure Sockets Layer Version 3.0,June 2015 https://tools.ietf.org/html/rfc7568.

5.1 Use of copyright / patent material /classified material

N/A.

5.1.1 Classified Material

N/A.

-END OF DOCUMENT-