SWIM Profiles - Final

Document information	
Project Title	SWIM Design
Project Number	14.01.03
Project Manager	INDRA
Deliverable Name	SWIM Profiles - Final
Deliverable ID	D39
Edition	00.01.01
Template Version	03.00.00
Task contributors	
ENAV - EUROCONTROL – FREQUENTIS– INDRA – NORACON - THALES.	

Abstract

This technical note provides background information on the motivations for defining SWIM Profiles, structuring and design related to SWIM Profile.

Authoring & Approval

Prepared By - *Authors of the document.*		
[redacted] INDRA	[redacted]	15/04/2016
[redacted] FREQUENTIS		09/06/2016

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] INDRA	[redacted]	20/05/2016
[redacted] INDRA		07/06/2016

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted] SELEX	[redacted]	20/05/2016

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
[redacted] INDRA	[redacted]	10/06/2016
[redacted] ENAV		10/06/2016
[redacted] EUROCONTROL		10/06/2016
[redacted] NORACON		10/06/2016
[redacted] FREQUENTIS		10/06/2016
[redacted] THALES		10/06/2016

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	15/04/2016	Draft	[redacted]	First evolution from D38 to D39
00.00.02	23/05/2016	Draft		First comments incorporated
00.00.03	25/05/2016	Draft		Minor updates according to discussed comments.
00.00.04	31/05/2016	Draft		Final Draft for partners review
00.01.00	09/06/2016	Final version for approval		Editorial updates according to review comments.
00.01.01	21/07/2016	Final		Updates after SJU assessment.

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

List of tables

List of figures

Executive summary

As commonly agreed by all P14.1.2 partners, in the context of reference [5]:

a SWIM profile is a coherent, appropriately-sized grouping of middleware functions/services for a given set of technical constraints/requirements that permit a set of stakeholders to realize Information sharing. It will also define the mandated open standards and technologies required to realize this coherent grouping of middleware functions/services.

The aim of the present document is – based on the WP14 SWIM Step 1 activities - to provide answers to the following questions:

- Why are SWIM profiles needed?
- What are the constraints to comply with, when defining SWIM profiles?

1 Introduction

1.1 Purpose of the document

The P14.01.03 Gate Review (September 2011) raised an action for SWIM Profiles to be clarified and justified. Furthermore it was commonly agreed with all P14.1.3 partners, that the task shall be taken over in the “Iteration 2.0 of the SWIM Profiles definition” task for Step 2. The aim of this technical note is to provide the required clarifications.

The project P14.01.02, as part of deliverable D03 (SWIM Context), produced early on in the SESAR Programme the following draft material:

- An initial and bottom up definition of SWIM Profile;
- An initial list of SWIM Profile instances for Step2;
- A process for defining the SWIM profiles;

The SWIM Profile White Paper v2.0 proposed a top-down structured rationale for the SWIM Profile as well as initial specifications of process elements for the management of the lifecycle of SWIM Profiles.

The objectives of this deliverable are to bring more clarity and more maturity to the process elements for the management of the lifecycle of SWIM Profiles, to ensure alignment with SWIM-TI TAD and SWIM-TI TS and to make the document accessible to stakeholders outside WP14.

As services developed by WP8 are iterative works, it is anticipated that further review and SWIM Profiles definition work will take place after the formal delivery of this document resulting in an update of this document (maintenance task).

In order to improve the usability and the accessibility of the deliverables related to SWIM Profiles in Iteration 3.0:

- The contents of this document in Iteration 3.0 is focused on foundation material related to the concept of SWIM Profile
- The SWIM Profile Descriptor (SPD) for Iteration 3.0 is no longer an embedded document in this document but is provided through a separate document.
- This document in Iteration 3.0 no longer contains any of the constituent elements of the SWIM Profile Instantiations (SPI), hence significantly reducing the scattering and fragmentation of constituent elements of the SPI:
    - The Views on the SPIs for Iteration 3.0 are no longer embedded documents in this document but are provided through a separate Excel spreadsheet, which allows an interactive approach through various filtering options and provide as well a complete view on the requirements.
    - The attributes that defined the classification of the requirements in the Views on the SPIs for Iterations 2.0 and 2.1, were maintained in a separate and invisible repository that was linked with previous versions of this document. They have been explicitised directly in each of the requirements. This significantly enhances manageability and maintainability of the View on the SPIs.

In SWIM Profiles for Iteration 3.1, three updates were required:

- A changed requirement from the Airspace Users, leading to bridging between SWIM Profiles to become an option
- Inclusion of the result of the impact analysis of the ISRM 1.4
- Reflect the updated structure of Functional Blocks

1.2 Intended readership

This document is intended to be reviewed and approved by WP B, 8, 9, 14 and the SWIM Architect Group (SACG). More specifically this document shall be of interest for the following projects:

- P14.1.3: as it is a deliverable for task 38.
- P14.1.4, P14.2.3 and P14.2.9: as it is an input to the system design work.
- P8.3.X, PB4.3: in order to coordinate the good adequation between services and allocated profiles. Also to define a common non-functional requirements list and taxonomy.
- P9.19 in order to learn about the SWIM-TI Purple profile.
- P10.2.5: in order to learn about the SWIM-TI Blue profile.
- 13.2.2, in order to learn about the SWIM-TI Yellow profile and prepare the design of new operational scenario for the AIM Workflow.
- P14.4 in order to provide ATM prototyping projects part of System WPs, with information about the SWIM prototypes they have to integrate.

Additionally this document together with SPD v3.10, and references [24] and [28], shall be made available to manufacturers making technical products that would need to conform to a SWIM Profile.

1.3 Inputs from other projects

1.4 Glossary of terms

The table below is the terminology shared with the Architectural Definition [24] and with the Technical Specification [28].

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.

Term	Definition
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.
Alliance	ITU-T IdM X.1252 define 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. These services are defined by WP8 and are part of the ISRM.
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.

Term	Definition
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 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.
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. Note: These services breakdown is described in §2 and it has been defined according to P14.01.04 SWIM-TI Use Case UML model **Error! Reference source not found.**.
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 as defined by SWP8.1, SWP8.3 and P14.01.04. The conformance conditions are expressed in form of well-defined policy assertions assigned to the SWIM service definition.
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.
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.

Term	Definition
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".
Federation	ITU-T IdM X.1252 defines this term as an association of users, service providers, and identity service providers.
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 define 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 define 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 business and security applications.
Identity Provider (IdP)	ITU-T IdM X.1252 define 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 Tokens 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.

Term	Definition
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. This 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 define 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.
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 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 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.

Term	Definition
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.
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)
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 define 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 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 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.
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.
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.

Term	Definition
(Security) Policy	An agreement upon which entities (e.g. Systems) can collaborate. A typical example of this is Authorization Policy and Audit Policy.
(Security) Policy Life Cycle Management	The Policies lifecycle management is a key aspects enabling the appropriate confidentiality policy enforcement.
Security Token	Security tokens are used to prove one's identity electronically. The token is used in addition to or in place of a password to prove that a given actor is who they claim to be. The token acts like an electronic key to access something. Besides the information needed to authenticate an identity, a token can provide additional information related to an identity that can be used for instance to support the authorization. Security tokens imply trust of a third party that issues the security tokens.
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 Virtualisation (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
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 defined by WP8 and the appropriate SWIM-TI defined by WP14.
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 or SWIM-TI Node	SWIM-TI Node provides a collection of SWIM-TI Functional Blocks, compliant with one or more SWIM profiles, allowing a given ATM application to use the SWIM-TI. 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).

Term	Definition
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 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.
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 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.
XML Encryption	XML Encryption is a specification (by W3C recommendation) that defines how to encrypt the contents of an XML element. *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.
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.

1.5 Acronyms and Terminology

Term	Definition
A/G	Air-Ground
ABAC	Attribute Based Access Control
ADD	Architecture Description Document
AIM	Aeronautical Information Management
AIRM	Aeronautical Information Reference Model
AIXM	Aeronautical Information eXchange Model
AMHS	Aeronautical Message Handling System

Term	Definition
AMQP	Advanced Message Queuing Protocol
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
B2B	Business to Business
BCA	Bridge Certification Authority
BP	Blue Profile
CA	Certification Authority
CAP	Consistency - Availability - Partition tolerance
CONOPS	Concept of Operations
COTS	Commercial Of The Shelf
CSP	Certificate Service ¨Provider
DDS	Data Distribution Service
EAD	European Aeronautical Database
EC	European Commission
EN	Enabler
FB	Functional Block
FDD	Flight Data Distribution
FO	Flight Object
GUID	Globally Unique Identifier
HA	High Availability
HTTPS	HyperText Transfer Protocol Secure
ICAO	International Civil Aviation Organization
IdM	Identity Management
IM	Information Management
INTEROP	Interoperability Requirements
IS	Industrial Support

Term	Definition
ISO	International Organization for Standardization
ISRM	Information Service Reference Model
IT	Information Technology
KVP	Key Value Pair
MEP	Message Exchange Pattern
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NFR	Non-Functional Requirement
NM	Network Management (CFMU)
NOP	Network OPerations or Network Operations Portal
NSOV	NAF Service-Oriented View
OGC	Open Geospatial Consortium
OMG	Object Management Group
OS	Operating System
PENS	Pan-European Network Service
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
PP	Purple Profile
QoS	Quality of Service
REC or REC FB	Recording Functional Block or SWIM-TI Recording FB
REG or REG FB	Registry Functional Block or SWIM-TI Registry FB
SAML	Security Assertion Markup Language
SEC FB or SEC	Security Functional Block or SWIM-TI Security Functional Block
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)

Term	Definition
SJU Work Programme	The programme which addresses all activities of the SESAR Joint Undertaking Agency
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 or SPV FB	Supervision Functional Block or SWIM-TI Supervision FB
SSL	Secure Socket Layer
STI	Security Token Infrastructure
SW	SoftWare
SWIM	System Wide Information Management
SWIM-TI	SWIM Technical Infrastructure
TAD	Technical Architecture Description
TLS	Transport Layer Security
TS	Technical Specification
UML	Unified Modeling Language ™
UUID	Universally Unique Identifier
WA	Work Activity (within a project)
WP	Work Package
WS	Web Services
WSDL	Web Services Description Language
WXXM	Weather Information Exchange Model
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Term	Definition
YP	Yellow Profile

Table 1 Acronyms and Terminology

2 Motivations

2.1 The key issues

2.1.1 Introduction

The following statement represents the starting point of this white paper ref. [5].

> *Given the breadth of SWIM, across all systems, data domains, and flight (planning, execution, post-execution) phases, it is not expected that one solution1 and certainly not one technology will suit all. Different stakeholders, based on their business needs, may not have the same requirements for SWIM.*

The high-level architecture of SWIM in the SoS is based on the SOA architectural style. The structuring of the services themselves is based on a layered architectural style.

This layered architecture[2] can be schematised as in Figure 1.

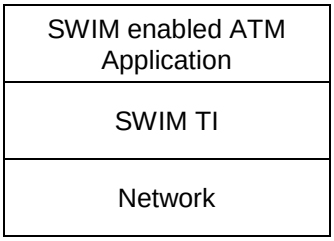

Figure 1 Layered architecture

The SWIM TI provides functions/services for the higher level layer ATM Application and relies itself on the lower level layer Network.

Technology interoperability[3] is the essential purpose of the SWIM TI. In an ideal world, from a conceptual point of view, this interoperability is provided through an agreed minimal set of standards for the entire SoS.

In the real world though, it is not possible to impose a single middleware stack providing all the needed technology interoperability to all actors, mainly because of constraints, competing requirements and risks.

> Constraints, competing requirements and risks are key issues that contribute to a large extent to the shaping of the application architecture including that of the SWIM TI.

[1] The word “solution” covers technology choices; architectural patterns; designs.
[2] This schema has no other purpose than providing a view on the place taken by the SWIM TI in the architectural structure.
[3] Interoperability as defined in ISO/IEC 25010. Technology including but not limited to messaging, security, supervision and shared functional blocks.
The term "Technology" is used to avoid confusion re. different interpretations of the term "Technical": the ETSI and the LCIM interoperability frameworks separate syntactical interoperability from technical interoperability while the EIF (European Interoperability Framework) does not make this distinction. The interpretation given to "Technology Interoperability" in this document conforms to the ETSI and LCIM interpretation in the sense that it does not include the syntactical interoperability re. data exchange models (e.g. AIXM, WXXM) but it does include format aspects (e.g. XML, KVP) of syntactical interoperability.

Each of these key issues will be developed more in detail in the following.

2.1.2 Constraints

2.1.2.1 The stakeholders

Any organisation acting in the context of European aviation is considered as a stakeholder.

Examples of areas of constraints:

- Not all stakeholders are able/willing to make the same financial means available
- Not all stakeholders have the same organisational capabilities such as
    - skilled staff to perform monitoring, troubleshooting, updates, support
    - establishment and management of internal and external support contracts
- There is a wide variety of stakeholders
    - many stakeholders are involved in multiple distinct roles thus being both consumer as well as provider of services and/or equipment

In these roles each stakeholder targets business models that are most appropriate to support its own interests.

2.1.2.2 The business activities

Examples of areas of constraints that apply to the business activities in the European aviation:

- Regulation

  Several authorities issue regulation applicable to the business activities in the European aviation (e.g. ICAO, ECAC, European Union and National Authorities). Specific business activities are subjected and constrained by specific regulation.

  Examples:
  - Commission Regulation 1032/2006 - Exchange of Flight Data Between ATC Units
  - Commission Regulation 29/2009 - Data link services for the Single European Sky
  - Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

- Certification

  Competent authorities issue certificates to confirm compliance with specific requirements

  Examples of such specific requirements are ISO standards and ICAO specifications.

2.1.2.3 The systems

Examples of areas of constraints:

- Future systems for which choices are imposed or for which domain specific constraints apply.
    - Systems based on the ED-133 standard
    - A/G
      The limited available bandwidth of the underlying network is constraining the options at the level of SWIM TI for instance regarding verbosity of the protocols

- Legacy systems. IT infrastructure that is already deployed and operational and that needs to be reused

  - NM B2B and EAD B2B as 2 examples among many to be considered
  - Some stakeholders have already invested into a SWIM kind of infrastructure which will remain used for a while

- The market has not converged to a single technology that provides interoperability in an SOA architectural style.

  - ranges of communication technology already exist and more, new options will emerge.
    - there is a varying degree of overlap between these technologies
    - none of the technologies excels in all areas but each of them targets particular use cases

The mandatory use of an SOA architectural style within the SoS does not prohibit using communication protocols that are open and standardised but incompatible.

2.1.3 Competing requirements

The identification of competing requirements takes both functional and non-functional requirements into consideration.

Such competing requirements typically emerge between following characteristics but they are not limited to these characteristics:

- Security
- Performance
- Cost
- Reliability

Examples of competing requirements:

- Security versus performance

  Increasing levels of security, for instance through use of asymmetrical encryption algorithms and longer keys, require more performance and thus increase the response time and/or reduce throughput on the same infrastructure.

- Reliability versus cost

  Increasing levels of availability require a need for deployment of additional architectural devices at infrastructure level, for instance redundant hardware and software clustering, as well as deployment of organisational means, such as management and maintenance processes and Human Resources, to ensure the required availability. At higher levels of availability the relationship with cost is not linear, as small increases of availability tend to provoke dramatic cost increases.

- Reliability versus pace of change

  When a high pace of change is required to provide a high level of flexibility, the time available to go through the change process will be shortened, leading to more undetected errors and faults at various levels – from concept to implementation -, thus increasing the risk of failures to occur and reducing the reliability of the system.

- Consistency versus Availability versus Partition tolerance (CAP)

Brewer's theorem states that it is impossible to have Consistency and Availability and Partition tolerance guaranteed at the same time in a distributed system.

2.1.4 Risks

Significant risks that can be identified in the context of the SWIM TI in the SoS:

- Wrong standards and implementations thereof
    - the standards do not become mainstream
        - a standardised technology is not an absolute guarantee for the success and the longevity of a technology
        - when a standardised technology does not get sufficient market momentum, suppliers abandon and the standard is considered dead
        - a standardised technology that is not widely implemented, can create a binding to one or only few suppliers. In such case maturity and interoperability of implementations are uncertain.
    - the standards and implementations thereof remain immature
        - a standardised technology is not an absolute guarantee for successful interoperability because it may be interpreted differently for instance because of incompleteness or ambiguity
        - the standardisation process typically goes through a phase whereby interoperability between implementations from different suppliers is unstable, hardly works or does not work at all
        - only a subset of a standard is implemented possibly combined with proprietary extensions
        - if there is no market incentive, the available implementations may remain in an immature status even though the standard is adapted/corrected/clarified
    - the implementations of the standards do not scale
    - the implementations of the standards prove to be unstable
    - the implementations of the standards do not meet the current and/or future needs
- Infrastructure complexity.
    - Excess complexity can lead to too long time to develop (for the SWIM TI such development is applicable to specific cases and specific service consumers only) and/or configure the middleware, delivery of unstable middleware or ultimately non-delivery of the middleware.
    - Excess complexity can lead to inability to understand, correctly use and maintain the operational middleware.
- Infrastructure co-existence.

Excess reuse or resource sharing can lead to applications disturbing other applications[4].

Mitigations and recommendations:

- Apply the “do not put all your eggs in one basket” principle to avoid that issues with standards cause disruptions at the level of the entire SoS.
- Acquire standards assessments by independent industry analysts on a regular base re.:
    - the level of mainstream status
    - the potential of a standard to become mainstream
    - existence and relevance of real multi-vendor interoperable implementations
    - expected longevity
    - market share
    - market value
    - market tendency
    - availability of expertise
- Use standards that have already reached the mainstream status.
- Use standards for which interoperability between different implementations is proven in operational use.
- Structure the needs and create/use an ontology for the needs. Map the standards onto this classification of needs. Ensure availability of fallback standards for each need.
- Reduce complexity by reducing the scope of the solution.
- Reduce complexity by using specific technology that is fit for purpose and thus avoiding emulation on a generic technology.
- Reduce complexity by replacing a single highly complex and/or overkill technology through a less complex right-sized composition of multiple technologies.
- Reduce complexity by replacing a highly complex and/or overkill composition of multiple technologies by single less complex technology.
- Segregate and delimit infrastructure that has high/challenging quality requirements from other infrastructure.

[4] Example: When ATM applications of different nature, written by different people with varying skills, share the same SWIM TI functional blocks the risk of harmful interference is high. Hence, a misbehaving application using the SWIM TI can provoke a crash, a hang or a depletion of required resources at the level of the SWIM TI which impacts all other applications using the SWIM TI

2.2 The solutions

2.2.1 Trade-off

One of the methods to deal with the key issues consists of finding a balance and making a trade-off.

A trade-off presents a lose-lose situation and is not always acceptable and/or necessary, i.e. a "good balance" cannot be found.

Whereas the use of the trade-off method cannot provide a single acceptable and/or necessary solution for an entire system, it can still be applicable however within a more restricted scope, i.e. subsets of an entire system.

2.2.2 Segmentation

Another method to deal with the key issues consists of the use of segmentation.

> Instead of looking for a single solution for an entire system, by segmenting the system - i.e. dividing/grouping elements of the system into subsets -, it is much easier to find a solution for each such segment that deals in a satisfactory manner with all functional, non-functional and constraints requirements and risks in scope of the segment. Each segment having an appropriate solution represents a win-win situation.
>
> The definition of a segment and the identification of the subset of an entire system that is part of it, depends on selection criteria. Finding the relevant selection criteria is the key success factor of segmentation. This subject is elaborated further in Appendix A.

Segmentation is a generic mechanism that can be applied to the SESAR SoS.

> Each layer of the architecture can be segmented using criteria that are specific for each layer. This is illustrated in Appendix B.
>
> A fundamental assumption of reference [5] work is that SWIM will indeed be segmented.

Segmentation is particularly applicable to business domains in the SoS for which the relevance and the priority of the requirements for the SWIM TI are not uniform.

> As an example, a particular business domain may require high performance (e.g. low latency) and minimal security (e.g. inside a closed network) while another business domain may require strong security (e.g. asymmetrical encryption and digital signing at message level) but has no significant performance requirements.
>
> The SWIM TI solution for the first business domain can be classified in a segment that has high performance capability and only low security capability. The SWIM TI solution for the latter business domain can be classified in another segment with high security capability.

Segmentation at the level of the SWIM TI layer can break the technology interoperability between different segments.

> The SWIM TI layer includes messaging and security as core distributed functional blocks. Using solutions for these functional blocks in different segments, that are based on different messaging and/or security protocols will break the technology interoperability between these segments.
>
> Therefore the boundaries of the segmentation are to be aligned with Communities of Interest that need to interoperate.

If such alignment were to undermine the benefits of the segmentation, more restricted boundaries can be envisaged. In such case the required technology interoperability could, for instance, be provided through a gateway or adapter between segments allowing for a controlled and possibly restricted but sufficient technology interoperability. More detailed considerations on the technology interoperability between different segments can be found in section A.3.

2.2.3 Profiling

2.2.3.1 Context

The combination of a particular segment, i.e. the selection criteria, and a prescribed solution for that segment constitutes a Profile.

2.2.3.2 Value

The first value of profiling at the level of the SWIM TI lies in cost reduction, risk mitigation and risk avoidance (risks identified in section 2.1.4) by discarding unneeded and unwanted functional blocks entirely and/or unneeded and unwanted functionalities that are specific to a functional block.

The term functional block is meant in the sense of SWIM Technical Infrastructure Functional Blocks as described in [4]. Examples of such functional blocks are Messaging, Security, Recording, Supervision or Shared Object.

Step 1 has identified that not all functional blocks are shared by all profiles: for instance Security, Interface Management, Data Validation and Shared object functional blocks are or may be required only for specific profiles.

Similarly, each of the functional blocks does not necessarily have to provide all the possible functionalities: for instance support for all the Message Exchange Patterns or QoS is not always necessary for the Messaging functional block.

A middleware stack that only provides or activates the required functional blocks and functionalities described by the profile will yield

- Reduction of infrastructure, process and organisational costs
- Avoidance of operability issues
- Mitigation of complexity

A second value of profiling at the level of the SWIM TI allows avoidance of the dependency on a monolithic multi-purpose infrastructure.

- Reduction of costs (by allowing competition and innovation)
- Mitigation of risks (by spreading)

A third value of the profiling at the level of the SWIM TI lies in establishing a common language between solution suppliers and their customers, which should facilitate significantly the process of finding an appropriate solution:

A supplier can claim conformance to a profile.

The profile provides the customer with a shorthand for his/her requirements.

Finally as a fourth value, profiling promotes interoperability.

Application of standards is often not enough to ensure interoperability.

At the level of technology interoperability, this typically materializes in standardized protocols that contain a set of mandatory specifications and also provide additional specifications and/or sets of specifications that are optional, in order to be able to meet various distinct use cases.

Equally typically, standardized protocols will provide and allow variations through choices.

Hence, interoperation between legal but distinct configurations of the same standardized protocol may be unreliable or may not be possible at all.

Profiling is a technique that is used to restrict the range of distinct configurations of a protocol, in order to significantly increase the chances of establishing successful interoperability.

3 SWIM Profile definition

3.1 SWIM-TI

As defined with more details in reference [24]:

... SWIM-TI is a set of software components distributed over a network infrastructure providing functions enabling collaboration among ATM systems.....

... SWIM-TI can be understood as an Infrastructure Capability Configuration...

The model for the Functional View of the SWIM-TI can be depicted as:

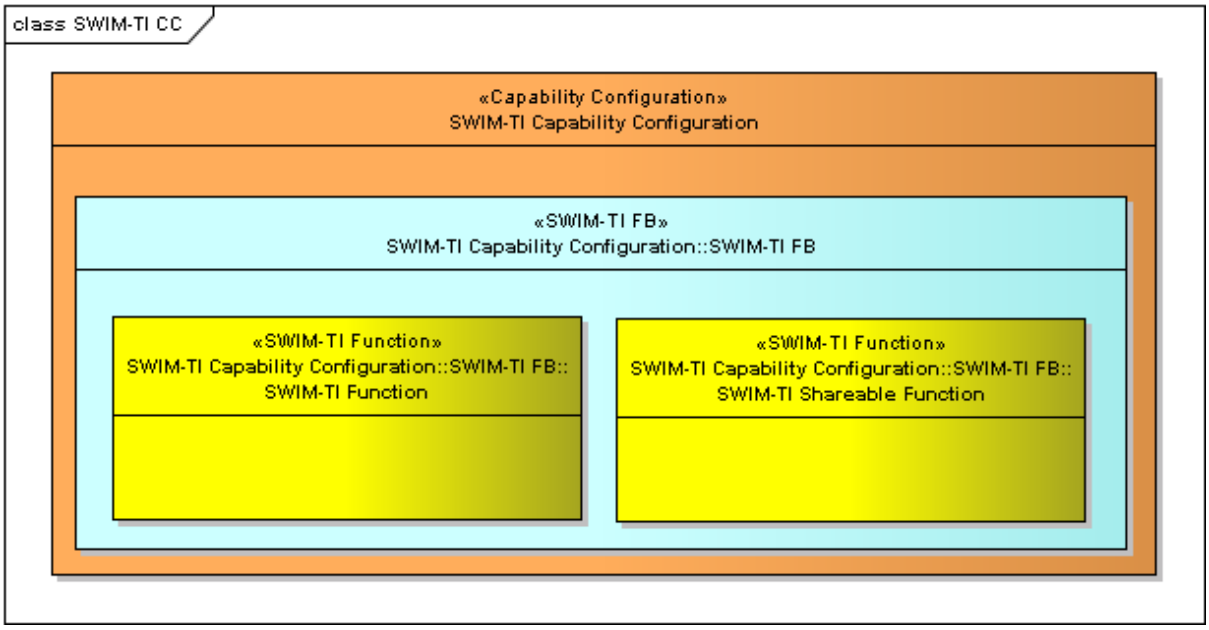

Figure 2 SWIM-TI model

3.2 SWIM-TI Functional blocks

As defined with more details in reference [24]:

*A SWIM-TI Functional Block represents a **logical aggregation** of functions within an instance of the SWIM-TI that are assembled to assist in the conducting of one or more SWIM-TI Activities.*

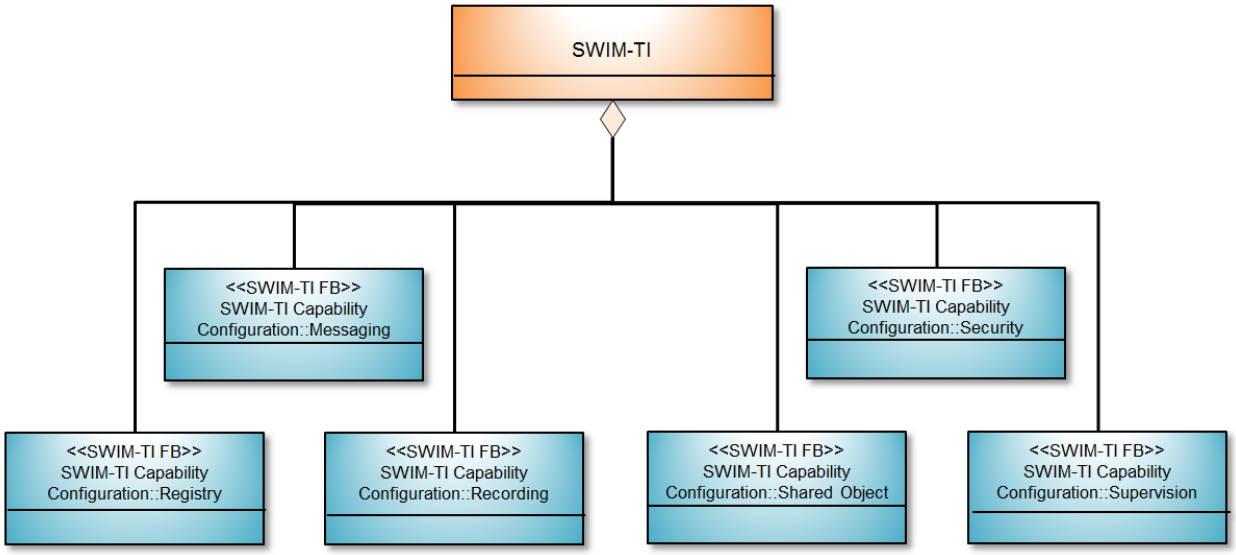

Figure 3 SWIM-TI Functional Breakdown

3.3 SWIM profile

3.3.1 Definition

The SWIM profile has been defined in reference [5] as follows:

A SWIM profile is a coherent, appropriately-sized grouping of middleware functions/services for a given set of technical constraints/requirements that permit a set of stakeholders to realize Information sharing. It will also define the mandated open standards and technologies required to realize this coherent grouping of middleware functions/services.

The profile has also been defined with more details in reference [1] [9]:

*A SWIM-TI Profile is a concrete **group of SWIM-TI Functional Blocks**. For each SWIM-TI Functional Block, a SWIM-TI Profile Instantiation derived from the SWIM-TI Profile Descriptor will define a concrete set of requirements*[5].

*Each SWIM-TI Profile Instantiation can be understood as a **specific instance** of the SWIM-TI FB decomposition.*

3.3.2 SWIM-TI Node

The SWIM profile is linked with the concept of SWIM-TI Node in reference [1] as follows:

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).

3.3.3 Overall design process

As proposed by reference [5], the SWIM-TI profiles are designed as follows:

[5] Two different SWIM-TI Profiles don't necessarily have to share the same requirements even if they are implementing both the same SWIM-TI Functional Blocks.

- WP8.3 shall provide the operational context and define a set of ATM Specific services that need to be enabled by the infrastructure. Each ATM Specific service fulfils one or more IER which in turn has a number of related NFR (including MEP) defined in the SPR (See Appendix C for details on the definition of NFR and the impact of distinct viewpoints). That is the input driving the definition of the SWIM Profiles.

- WP14 shall then map this input to architectural choices segmenting the SWIM-TI into profiles; where the concerned SWIM-TI functional blocks shall be retained.

- Finally, WP14 shall identify for each profile, the required subset of technology standards and protocol stacks for interoperability.

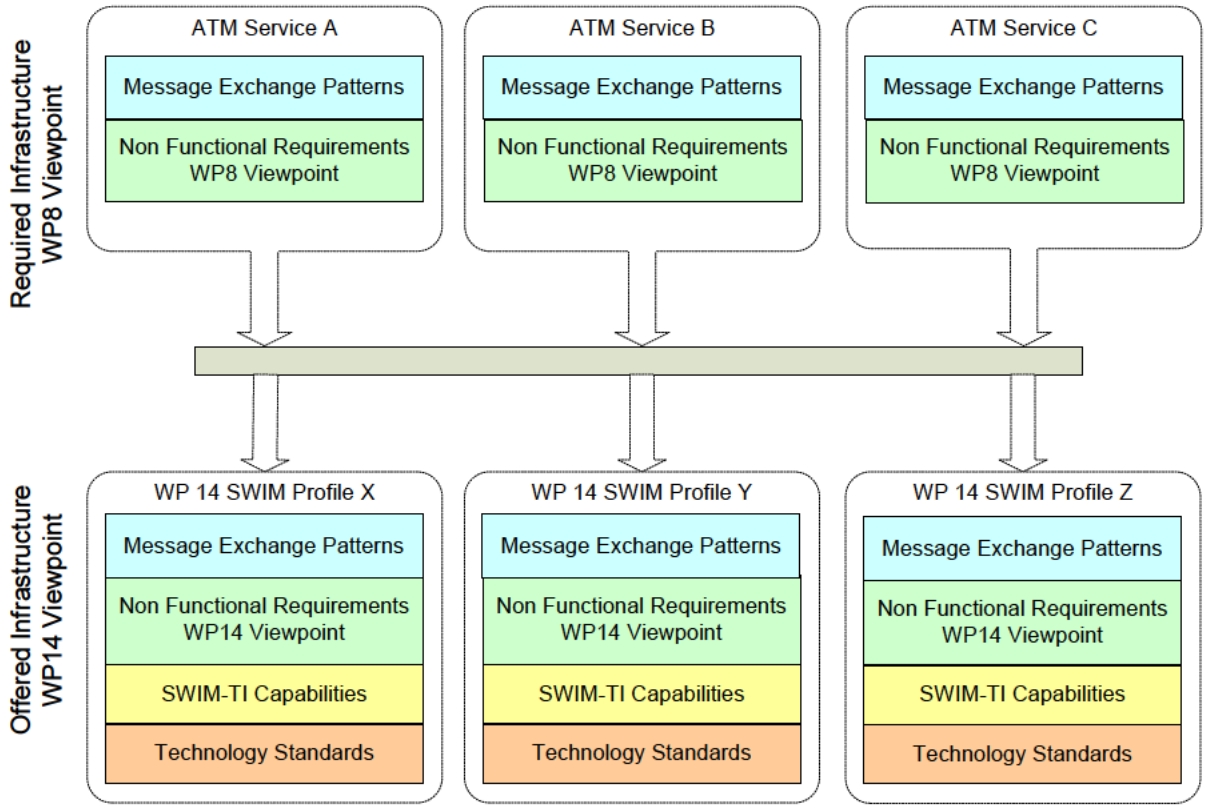

Figure 4 Relation between WP 8 and WP 14

The Profile itself may be further sub-divided down, defining the characteristics of finer-grained configurations, as shown in the following sections.

3.3.4 Asymmetrical profiles

Within a same SWIM profile, experience has shown (in Step 1) that provider and consumer attributes may differ. These are the so called asymmetrical profiles. So far, in such cases, the strategy was to always require a lightest configuration at consumer side. Both sub-profiles would obviously share the same standards/technologies for interoperability, but the service provider side would have a richer set of functional blocks. The Step-1 EAD B2B and CFMU NOP B2B profiles are the two known examples of asymmetrical profiles.

3.3.5 Varying Non-Functional Requirement attributes' values

Within a same profile, more than 1 value can be allowed for a Non-Functional Requirement.

In case there is need to be able to explicitly identify a configuration with a particular value for a Non Functional Requirement or particular values for a group of Non-Functional Requirements, the notion of Sub-Profile can be used.

For instance, within a same profile, varying levels of security may be supported.

If the varying levels are inclusive, such as https only and https + message, the profile may be divided into incremental configurations moving from 'basic' to 'full' functionality. This concept of profile is similar to that used in UML, DDS etc. Here below an example based on the Security NFR.

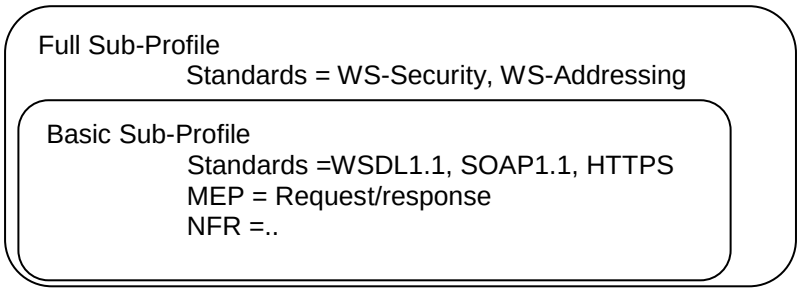

Figure 5 Basic Sub-Profile

If the varying levels are alternatives, such as https only or message only, the Basic Profile may contain alternative configurations that represent groups of choices amongst all alternatives that are supported by the profile.

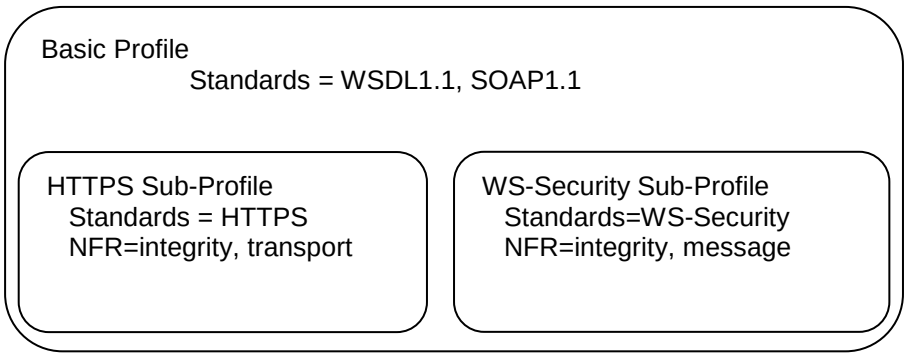

Figure 6 Encapsulated profiles

3.3.6 Number of profiles

Although the single solution shall not be the goal of the SWIM profiles study, efforts should be spent to try to limit the number of different SWIM profiles.

For instance, if it appears that a SWIM profile defined for a specific need could suit other needs, it shall be studied whether this single SWIM profile used for all those needs is not more cost effective than using different SWIM profiles.

Another case to be studied would be to assess the advantages/disadvantages when integrating different SWIM profiles into a reduced number of profiles. These "unification" or "integration" studies

shall be performed in a 2nd step after having listed and defined the different needs and the different corresponding SWIM profiles.

3.3.7 Minimum profile

The need of defining a common minimum profile that all SWIM nodes shall support will be a consequence of the identification of a minimum set of services that all SWIM nodes shall support.

Step 1 did not identify such services.

3.4 Profile versus nodes

As defined in reference [1]:

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).

As a consequence to the above statement it is envisaged that one SWIM node may implement more than one SWIM profile.

3.5 Profile versus profile

3.5.1 Up to and including D32

During the numerous SWIM Profiles discussion meetings involving P14.1.3, P14.1.4, WP8 partners and SJU representatives; the following statement was commonly agreed:

> "The interoperability between profiles was assumed so far not to exist."

The time validity of this statement includes the time of writing of the D32 document.

As a consequence the requirement REQ-14.01.03-INTEROP-SPWP.0010 was created.

Remarks:

Mitigation means for coping with profiles non-interoperability were being discussed. Basically the following methods were proposed:

1. Profiles interoperability might in future be provided by architectural concept like gateways. Gateways would allow a client SWIM node, with a specific profile consuming a service only implemented on a different profile, on a provider SWIM node. It is important to note here that such an implementation will most likely induce NFR values alterations with respect to the original WP8 service definition.

2. Implementing a same service on different profiles is also a mitigation means for coping with profiles non-interoperability.

The SWIM-TI segmentation and the interoperability between segments are two topics covered in details by section 2.2 and Appendix A.

3.5.2 D34

However the introduction of a new SWIM Profile (Purple Profile) in Iteration 2.1, has identified the need for interoperability between 2 distinct SWIM Profiles (Purple Profile and Yellow Profile).

- In A15 and 9.19 D03 [6] it is stated:

  "The first implementations of A/G SWIM are intended to support only non-critical information exchanges, more specifically, meteorological and aeronautical information exchanges."

  From above statement it is assumed that in such cases (e.g. if not directly provided by Airline using AMQP) such meteorological and aeronautical information are provided using the YP.

- This has led to a set of concrete specifications in D41 [9] for the interoperability between SWIM Profiles:

  REQ-14.01.04-TS-0001.0660

  REQ-14.01.04-TS-0901.0635

REQ-14.01.04-TS-0901.0660

- D33 [17], equally, takes the interoperability between SWIM Profiles into consideration in A.3.3, "Access Point Infrastructure System":

  "Within the analysis and further deployment options, the possibility of a Ground Capability Configuration unable to communicate via SWIM-TI with an air Capability Configuration due to the lack of common/interoperable SWIM-TI profiles in both of them was identified. To fix this eventuality, the concept of Access Point was developed. The Access Point Infrastructure System manages the switch from a SWIM-TI Profile to another. This could be extended to other SWIM-TI Profiles."

This need is further discussed in the SPA of the Purple Profile [9].

In iteration 2.1 this need has been satisfied by including in the new SWIM Profile, a protocol bridge and a subset of the other SWIM Profile. From a functional point of view, this approach aligns with first mitigation method proposed in section 3.5.1 above.

From the point of view of the Yellow Profile any interoperating participant is using the specifications of the Yellow Profile. The Yellow Profile is not concerned about the means that other SWIM Profiles may or need use to appear as an interoperating participant using the specifications of the Yellow Profile only.

In the next iteration, this approach may be reviewed by assigning the protocol switch function, the data transformation function and both SWIM Profiles to a new logical element such as the “Message Bridge”[6], which is no longer part of a SWIM Profile.

In such case a SWIM Profile would rely on the “Message Bridge” rather than include the functionality covered by the “Message Bridge”.

Hence the requirement REQ-14.01.03-INTEROP-SPWP.0010 is no longer valid.

3.5.3 D36

In Iteration 3.0, the need for interoperability between distinct SWIM Profiles has remained identical to Iteration 2.1.

The approach for the structuring of the solution for this need has remained identical to Iteration 2.1 and has not been reviewed.

The option for review of the approach remains open for a next iteration.

3.5.4 D38

In iteration 3.1, the representative of the Airspace Users has indicated that the Airspace Users, from now on, envisage to perform the bridging for their interoperability needs between the Purple Profile and the Yellow Profile at the application level rather than at the SWIM TI level.

Subsequently this bridging functionality, which was entirely included in the Purple Profile, remains in the Purple Profile but as an option.

[6] Message Bridge is a term used by www.eaipatterns.com (http://www.eaipatterns.com/MessagingBridge.html) and that reflects well the intended functionality

3.5.5 D39

In D39 (this document) the SWIM Profiles definition did not change with respect to D38 [27].

3.6 Profile versus service

In accordance with the second mitigation method proposed in section 3.5.1, it is assumed that a service as defined by WP 8, may be instantiated on more than one profile (Cf. REQ-14.01.03-INTEROP-SPWP.0010 in [18]).

Basically, different technology stacks may be able to provide a specific WP 8 service.

Consequently the physical binding of a service onto a SWIM profile will be specific to the SWIM profile in question.

Nonetheless and as expected, a service can only be supported on a profile that is able to satisfy the service's QoS.

As a consequence the requirements REQ-14.01.03-INTEROP-SPWP.0020 and REQ-14.01.03-INTEROP-SPWP.0030 specified in [18] remain valid

3.7 SWIM node set up

The physical set up of a SWIM node can be deployed in different ways:

- The physical set up of a SWIM node may not require a dedicated server.
- A SWIM node could be as simple as a software library in one of the system components.

The physical set up of a SWIM node may be performed via different business models such as:

- Installation and configuration of the open standards on the server done by service provider/consumer.
- Purchasing a fully prepared server from a system integrator.
- Leasing from or outsourcing the server to a third party.

4 SWIM Profile attributes

The unambiguous characterisation of a SWIM profile is determined by the set of values of the following attributes:

- A selection of SWIM-TI functional blocks (as defined in reference [18]).
- A selection of Message Exchange Patterns (MEP).
- A selection of infrastructure Non Functional Requirements (NFR).
- A selection of technology standards and configurations.

Remark:

Within a same SWIM Profile, experience has shown (in Step 1) that provider and consumer attributes may differ (Cf. section 3.3.4).

4.1 SWIM-TI functional blocks

4.1.1 Definition

The functional blocks discussed here are the so called SWIM-TI functional blocks, defined in reference [24] as follows:

FB Name	FB Code	Brief Description
Messaging	**MSG**	SWIM-TI Messaging FB aims at providing decoupled communication and interoperability between distributed systems including features for effective and reliable communication.
Security	**SEC**	SWIM-TI SEC FB provides technical functions enabling the Access Control (AAA - Authentication, Authorization and Audit) and Data Protection in a federation of security domains.
Supervision	**SPV**	The SWIM-TI Functional Block Supervision supports all SWIM related supervision functions collocated with the system.
Recording	**REC**	The SWIM-TI Functional Block Recording includes the ability to collect, store and on demand retrieval of information related to communication being performed via the SWIM Interfaces and related to supervision actions and events.
Shared Object	**SO**	The SWIM-TI Functional Block Shared Object function allows the sharing of data across multiple SWIM Nodes.
Registry	**REG**	The Registry is the shareable function to retrieve META Information about the Services and the ATM Information provided by them. It also generically provides discovery/subscription, publication, classification, management (including create, delete, updated, read) and deployment functions for diverse entities such as policies, standards, certifications and categories.

Table 2 SWIM-TI Functional Blocks

4.1.2 SWIM-TI functional blocks spreading over SWIM profiles

As was identified in WP 14 Step 1 activities, different profiles may implement different sets of the SWIM-TI functional blocks. The next table provides an example of SWIM-TI Functional blocks (from Step 1) spreading over different profiles.

#	SWIM Functional block	Profile 1	Profile 2	Profile 3
1	Messaging	X	X	X
2	Security		X	
4	Supervision	X		
5	Recording		X	X
8	Shared Object			X

Table 3 Example of SWIM-TI functional blocks spreading over SWIM profile

4.2 Message Exchange Patterns (MEP)

4.2.1 Definition

Distributed applications can communicate with each other through various means. One of these means is Messaging. Examples of other means are Shared Database, File transfer and Remote Procedure Invocation (sometimes called RPC). In an SOA context, Messaging is the preferred option as it specifically allows for loose coupling combined with responsiveness.

A Message Exchange Pattern (MEP) or interaction pattern describes how different parts of a message passing system connect and communicate with each other[7].

- In order to significantly enhance the degree of reuse and also as some combinations have proven to be more successful than others in a given context, recommended combinations are defined by many authors for targeted outcomes that commonly occur. Each of these combinations is called a Message Exchange Pattern.
- A MEP describes the roles of distinct participants, their individual actions, and the sequence of messages in a distributed collaborative action in order to achieve an objective in a predictable manner.
- In order to ensure interoperability, all participants need to share the same understanding of the MEP and act as prescribed by the MEP.

MEPs can exist at various levels of abstraction. The MEPs addressed here, are situated at the interface between the SWIM-TI layer and the ATM Application layer.

- In the simplest form the SWIM-TI layer can provide the ATM Application layer with a service to send a single message. This would typically take the form of an Asynchronous Fire & Forget as explained further. In such case, the ATM Application layer has to deal itself with all the complexity of any more complex MEP, such as timing and synchronization, error-handling and retries, and registration and addressing. Also, there is a high probability that many point MEP will be defined in the ATM Application layer with little or no reuse. The bonus of this approach consists of a high level of decoupling from the SWIM-TI layer.

- Conversely the SWIM-TI layer can provide services to the ATM Application layer to support complex MEPs. This will significantly reduce the complexity at the level ATM Application

[7] From http://en.wikipedia.org/wiki/Messaging_pattern the definition given in the context of software architecture

Layer and highly promote reuse of the established MEPs that profit from this support. The main disadvantage is the strong coupling of the ATM Application layer to the SWIM-TI layer for the messaging aspect.

Detailed concrete instances of MEPs have been defined that are made visible and offered by the SWIM-TI to the ATM Application. Currently this offer consists of a limited list of basic patterns that

- support both a highly-decoupled approach as well as more coupled approaches
- will be mapped inside the SWIM-TI to lower level MEPs as provided by technology.
    - Such mapping can be done through 1 or more steps
    - It is possible that technology exists that implements an MEP offered by the SWIM TI to the ATM application in a 1 to 1 manner but that is not guaranteed nor required[8]

The Non-Functional Requirements (NFRs) at the ATM service layer drive Functional Requirements (FRs) and NFRs at lower layers both of the SWIM-TI layer and of the SWIM-TI underlying network layer. The MEPs are FRs of the Messaging Functional Block. They are singled out into a separate set of attributes for the SWIM Profile, as they are the root requirements for interoperability to be specified by the ATM Application layer for the SWIM-TI layer.

The following table presents a list of possible MEP values as currently defined. These MEP are described in more detail in [1].

#	Values	Description
1	Synchronous Request/Response or Synchronous Request/Reply	A requestor[9] sends a request message to a replier system[10] which receives and processes the request, ultimately returning a message in response. It allows two applications to have a two-way conversation with one another. The requestor waits for the response or time out before doing other work or the timeout period expires. This pattern is especially common in client-server architectures.
2	Asynchronous Request/Response or Asynchronous Request/Reply	A requestor[9] sends a request message to a replier system[10] which receives and processes the request, ultimately returning a message in response. It allows two applications to have a two-way conversation with one another. The requestor does not wait for the response and the response might be returned at some unknown

[8] MEPs can occur at various levels. Any MEP can be emulated on top of another MEP. The MEPs in scope of this chapter are the MEPs as seen by the Service Consumer/Provider.
In a number of cases such MEP can be directly mapped onto a technology that provides the same MEP. In a number of cases MEP such cannot be directly mapped onto a technology that provides the same MEP but using one or more emulation layers.
Example: the MEP as seen by the Service Consumer/Provider is Synchronous Request/Reply. This can be directly mapped onto SOAP Request/Reply in a binding over HTTP as HTTP is a synchronous protocol. This cannot be directly mapped onto SOAP Request/Reply in a binding over SMTP as SMTP is an asynchronous protocol. If the use of SMTP is to be maintained, an emulation of a synchronous behaviour can be emulated by an intermediate layer
[9] The terms client and consumer are also used to address the entity with the role requestor.
[10] The terms server and provider are also used to address the entity with the role replier.

		later time.
3	Observer Push	A publisher[11] sends event data to all subscribers[12] that have manifested their interest through a subscription. The publisher knows and maintains the subscriptions. Publisher and subscriber need to be simultaneously present.
4	Observer Pull	A publisher[11] possibly sends a notification of the presence of an event (but not the event data itself) to all subscribers[12] that have manifested their interest through a subscription. Notwithstanding the sending or not of such notification, a subscriber can periodically check for any new data/update. In any case the subscriber has to fetch the event data through an interaction that is equivalent to Synchronous Request/Response. The publisher knows and maintains the subscriptions. Publisher and subscribers need to be simultaneously present.
5	Publish/Subscribe Push	A publisher[11] sends event data in the messaging service. The messaging service sends the event data to all subscribers[12] that have manifested their interest through a subscription. The publisher and subscribers do not have to know of each other. The messaging service maintains the subscriptions. Publisher and subscribers do not need to be simultaneously present.
6	Publish/Subscribe Pull	A publisher[11] sends event data in the messaging service. The messaging service possibly sends a notification of the presence of the event (but not the event data itself) to all subscribers[12] that have manifested their interest through a subscription. Notwithstanding the sending or not of such notification, a subscriber can periodically check for any new data/update. In any case the subscriber has to fetch the event data through an interaction that is equivalent to Synchronous Request/Response. The publisher and subscribers do not have to know of each other. The messaging service maintains the subscriptions. Publisher and subscribers do not need to be simultaneously present.
7	Asynchronous Fire & Forget	A requestor[9] sends a request message in the messaging service targeted at a provider system[10] which at some undetermined time receives and processes the request. The requestor is not informed on the outcome of the request. Requestor and provider system do not need to be simultaneously present.
8	Fully decoupled Request/Reply	A requestor sends a request message in the messaging service. The identity of the provider of the service is unknown by the requestor. The messaging service

[11] The term provider is sometimes used to address the publisher entity but that is a potential source of confusion.
[12] The term consumer is sometimes used to address the subscriber entity but that is a potential source of confusion.

		attempts to send the request message to a provider. When the request reaches the provider, the provider receives the message at some undetermined time and processes the request. The provider sends a reply to the messaging system which forwards it to the requestor. Both requestor and provider do not know each other nor do they know how many publishers and subscribers there are. The requestor and provider do not have to be present at the same time. The requestor and provider are not blocked waiting on each other.

Table 4 Message Exchange Patterns (MEPs)

4.3 Non Functional Requirements (NFR)

4.3.1 NFR Definition

Opposed to Functional Requirements (FR), Non Functional Requirements (NFR) are not describing the behaviour of a system. NFRs describe how a system shall be rather than what a system shall do. NFRs also describe how good a system shall do, the so called “qualities” of a system. They are used to judge the operation of a system. SWIM-TI NFRs are described in the TS documents [28].

The NFRs discussed here are not those of the possible backend systems using a SWIM node as front end. The NFRs in scope are those service NFRs required by specific WP 8 services and offered by implementations of WP 14 SWIM Profiles.

4.3.2 NFR Classification

The following list of non-functional requirement characteristics and sub-characteristics stems from the "product quality model" of ISO 25010 standard. P8.3.10 ISRM documents [15], [16], [19] [21] and [26] have not revealed the need for extension of this list.

Additionally, an analysis shall identify which NFRs from the standard are to be taken into consideration for the profiles definition. It was already identified that NFRs belonging to the "Functional suitability" and the "Usability" characteristics would not be retained. Indeed the latter are considered too contextual and subjective to be used for unambiguously characterising SWIM profiles.

Finally, ranges of "measures" ("quality measures" as defined by ISO 25010 standard) shall be proposed for each NFR.

System/Software Product Quality model (ISO/IEC FDIS 25010)

#	NFRs Characteristics	NFR sub-characteristics	Retained	Comment
-	Functional suitability	Functional completeness Functional correctness Functional appropriateness	**NO**	This NFR category was judged too contextual and subjective.

#	NFRs Characteristics	NFR sub-characteristics	Retained	Comment
1	Performance efficiency	Time behaviour Resource utilization Capacity	YES	Resource utilisation not retained: . Functional size. Explicit requirements such as the number of components and number of use cases have not been identified so far. There is no indication that there will be a need. . Resources. Explicit requirements on resources such as CPU, memory, IO and number of file or database records have not been identified so far. These requirements are implicit through other NFRs such as response time/distribution time and capacity. Explicit requirements have been found re. human resources (HR) and financial resources but only for the consumer part in asymmetrical profiles. Both HR and financial resources are categorised under efficiency in quality in use and judged too contextual and subjective
2	Compatibility	Co-existence Interoperability	YES	
-	Usability	Appropriateness recognisability Learnability Operability User error protection User interface aesthetics Accessibility	NO	This NFR category was judged too contextual and subjective.

#	NFRs Characteristics	NFR sub-characteristics	Retained	Comment
3	Reliability	Maturity Availability Fault tolerance Recoverability	YES	
4	Security	Confidentiality Integrity Non-repudiation Accountability Authenticity	YES	

#	NFRs Characteristics	NFR sub-characteristics	Retained	Comment
5	Maintainability	Modularity Reusability Analysability Modifiability Testability	YES	1. According ISO/IEC 25010 reusability is a subcharacteristic of modularity: Modularity is defined as the degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components Reusability is defined as the degree to which an asset can be used in more than one system, or in building other assets 2. The scope of the SWIM Profile definition is the technical infrastructure providing interoperability for the services offered by a SWIM enabled ATM Application. SOA aims the reusability of the services offered by a SWIM enabled ATM Application. SOA does not aim reusability of the middleware that allows interoperability with these services The SWIM Profile definition is agnostic about the way a physical implementation is performed. For instance, the deployment could be done through components that are physically separated from the SWIM enabled ATM Application as well as through components that are physically integrated in an SWIM enabled ATM Application. The reusability of the technical product itself is directly linked to this deployment and therefore not applicable.
6	Design and Construction Constraints	Adaptability Installability Replaceability	YES	

Table 5 System/Software Product Quality model (ISO/IEC FDIS 25010)

4.4 Technology standards and configurations

4.4.1 Definition

The technology standards and configurations discussed here are basically those implemented by a set of technical solutions meeting fully or partly[13] the requirements stemming from:

- the chosen Message exchange Patterns,
- the services' Non-functional Requirements
- and possibly some of the SWIM-TI functional blocks, themselves built from bottom up[14] requirements.

The following table provides a list of potential technology standards and configurations:

SWIM-TI Functional Blocks	Technology standards and configurations (examples)
Messaging	Request/Response style of MEPs: SOAP based WS, REST Style WS
	Publish/Subscribe style of MEPs: WS-N, DDS
	Queue based: AMQP, AMHS
Security	X.509 certificates, SHA-2, XACML, WS-SecurityPolicy
Supervision	
Recording	
Shared object	

Table 6 Technology standards and configurations

[13] In Step 1, more developments were sometime needed on top of the technology standards implementations of a profile.
[14] In Step 1, for the ATC-ATC profile, the bottom up requirements on which the SWIM-TI functional blocks were based, were assumptions on top down requirements captured in the ED-133 document.

5 SWIM Profile design

5.1 Overall considerations

5.1.1 Introduction

Following this introduction section a number of entities will be introduced.

The overall considerations in this section apply to all of these entities.

5.1.2 Naming and identification

Entities that are referenced require a unique and unambiguous naming structure. For the sake of this document, there are 2 kinds of referencing: technical and plain language.

In order to be able to introduce and manage the referenced entities as Configuration Items (CI), these entities need a technical naming. The technical naming structure is standardized in the SESAR programme and is applicable to all entities related to SWIM Profiles.

In order to be able to extract meaningful information from the technical name, a structured identifier is used and not an anonymous type of identifier such as a GUID/UUID.

The technical naming is however not always practically usable in a human to human communication. Hence, a notion of nickname is also introduced for some entities which can then be used for human to human communication.

Each referenced entity will have a technical name. Some referenced entities will also have a nickname.

5.1.3 Lifecycle

Every referenced entity will be subjected to a lifecycle. Any change to an entity will result in the creation of a new unique entity to ensure that the content of a referenced entity has an immutable meaning.

This principle can have a cascading effect: if the referencing entity needs to incorporate a change in the referenced entity, then a new referencing entity will have to be created including a reference to the new referenced entity and possibly excluding the original referenced entity.

5.2 SWIM Profile Assertion

5.2.1 Introduction

At any time any group of stakeholders could decide to create a set of specifications to perform information sharing.

A large number of such sets of specifications, each of them fitting extremely well another very particular need for information sharing, would pop up. This would lead to high fragmentation and thus little or no reuse as well little or no transparency.

To realize the expected values of SWIM Profiles and to ensure the “coherent and appropriately-sized grouping” aspect of the SWIM Profile, an instrument is required to manage the coming into existence

of a SWIM Profile and to ensure that an eventual definition has gone through a high level design process that supports the targeted values.

This instrument is the SWIM Profile Assertion (SPA) (see §6.4): it documents the scope, the rationale and high-level design of each SWIM Profile.

5.2.2 The scope

The scope explicitly provides the list of intended targets of the SWIM Profile as well as the list of non-targets.

The list of non-targets can be empty.

The targets are expressed as one or more criteria. The nature of the criteria can be anything that is relevant to perform the segmentation of SoS as described earlier in this document. Typically, criteria would be used from those that are provided in 2.1.

The content of the scope is meant to be readable and accessible for the reader who is not a technology expert as well as to provide sufficient guidance to the technical expert to make a detailed specification.

5.2.3 The rationale

The rationale provides some background (e.g. history, evolution, conflicts, problems, new needs) on the creation of the SWIM Profile and an overview of the reasons for the creation.

The rationale also provides an appreciation of the comparison of the scope of this SWIM Profile with any other already existing SWIM Profile and explains in case of significant overlaps, the usefulness of this SWIM Profile.

The content of the scope is meant foremost to be readable and accessible for the reader who is not a technology expert.

5.2.4 High-level design considerations

5.2.4.1 Introduction

The notion of profile is a common term and concept in the realm of standardisation organisations.

> [ISO/IEC 10000-1: Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework] defines a profile as:
>
> > “A set of one or more base standards and/or ISPs, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or ISPs necessary to accomplish a particular function.”
>
> OGC [The Specification Model — A Standard for Modular specifications, OGC 08-131r3] defines a profile as:
>
> > "specification or standard consisting of a set of references to one or more base standards and/or other profiles, and the identification of any chosen conformance test classes, conforming subsets, options and parameters of those base standards, or profiles necessary to accomplish a particular function."

The interpretation and meaning of the OGC definition is very closely aligned with that of ISO/IEC TR 10000-1.

Typically, in such context, a profile represents a restriction re. “the base”.

A superset of all requirements classes (union of all requirements classes) forms “the base” from which all possible profiles are derived through restriction.

Nevertheless, the profile is allowed to provide additional specifications that expand the specifications of the referenced standards.

SWIM Profiles are defined as being composed of 4 categories of specifications15.

- MEP(s)
- FR
- NFR
- Implementation constraints in particular for protocols, standards and configuration thereof

As the MEP(s) is(are) a particular case of FR and as the implementation constraints can be considered particular cases of NFR, from a high level a SWIM profile can be considered to be a composition of 2 categories of specifications: FR and NFR.

According to the definition of a SWIM Profile, specific sets of specifications are grouped in a SWIM Profile in a “coherent, appropriately-sized” manner.

What is a “coherent, appropriately-sized” grouping depends on the context and its appreciation.

No algorithmic approach that can provide an automatic definition of a SWIM Profile has been found.

Nevertheless, a series of high-level considerations with accompanying guidelines has been documented below. Each creation of a SWIM Profile must provide an assessment of each of these guidelines together with the scope and rationale in the SWIM Profile Assertion.

5.2.4.2 Design consideration #1. Interoperability is key.

The main objective of the SWIM-TI is to provide interoperability. Ultimately any design of SWIM Profiles needs to provide interoperability.

5.2.4.3 Design consideration #2. Reuse and size = not too many and not too few.

Too many SWIM Profiles will lead to fragmentation and lack of reuse. Too few SWIM Profiles will in many cases lead to solutions with unwanted significant overkill and with few alternatives available.

[15] The term “specification” includes the terms “requirement” as well as “recommendation”. In the context of the SWIM Profiles the term “specification” is used instead of “requirement” as some SWIM-TI Technical Specifications are expressed using “should” instead of “shall”.

5.2.4.4 Design consideration #3. Constraints, competing requirements and risks.

Due to the nature of the specifications in the scope of a SWIM Profile, the “base” from which the SWIM Profiles can be derived is very extensive and wide. It is even open-ended.

The rationale for SWIM Profiles has been developed in 2.1 The key issues. Three categories have been identified as the main drivers for SWIM Profiles: constraints, competing requirements and risks.

Each category has a significant set of possible values. Each of these values is a possible motivator for a distinct SWIM Profile and shall be taken in consideration.

The values of the categories could be combined and a SWIM Profile assigned to each combination. That would lead to a huge number of SWIM Profiles, fragmentation, little or no reuse and limited interoperability.

5.2.4.5 Design consideration #4. Modular structure.

5.2.4.5.1 The issue

The grouping of specifications into a SWIM Profile, creates a strong coupling of all the specifications in that SWIM Profile.

This coupling is only meaningful within the context of the use of that SWIM Profile. Outside the scope of that context, these specifications may be totally unrelated.

When comparing the use of a particular SWIM Profile, despite having many or most specifications in common, with other uses that require independent, possibly strong, variations of one or only very few specifications, then these variations would either require a new SWIM Profile for each such variation leading to fragmentation or require a SWIM Profile that captures many or all of the variations leading to unwanted overkill.

Also, understanding the difference between several SWIM Profiles that have many specifications in common can be difficult, error-prone and will lead to conflict opinions re. the selection of the SWIM Profileto which a service should be bound.

A method to deal with this, i.e. uses whereby a significant amount of specifications are shared, consists of using a modular structure in the SWIM Profile itself.

5.2.4.5.2 Options

5.2.4.5.2.1 Meta-model for structuring standards: ISO and OGC.

Several international standards organisations provide instruments to apply a modular structure to the definition of standards themselves.

In the case of both ISO and OGC one can find the notions of requirement class and core.

A requirements class is a grouping of specifications that are included or excluded as a whole.

A special foundational requirement class is defined that contains commonly shared requirements.

This requirement class is typically called the “core” requirements class.

The “core” requirements class is mandatory and there is only one. In some particular cases it can be empty.

All other requirement classes are optional sets of requirements.

The modular structure created by these instruments, facilitates the definition of profiles.

Although, a profile is not the same the concept as a standard, it is also a set of specifications and in case several profiles share a common set of specifications, this kind of modular structuring can be applied to these profiles.

5.2.4.5.2.2 Profile structuring standards: ISO and OGC.

The definition of the concept profile by ISO and OGC, allows a profile itself to be composed of one or more other profiles.

In the case of ISO, the “multi-part ISP” as descirbed in 8.2 of [ISO/IEC 10000-1: Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework] provides a model for dealing with common text between related profiles.

This “is essential to ensure consistency and interworking, to avoid unnecessary duplication of text, and to aid writers and reviewers of ISPs”.

Such common parts are grouped into a single-part profile or a part of a multi-part profile and are referenced from other profiles.

5.2.4.5.2.3 The legacy.

A model for structuring of SWIM Profiles had been proposed in D32 (ref. [18]) and its predecessor corresponding to some form of profiling of a profile.

This model is not easily understood, some of its terminology counterintuitive and it is also restrictive in the kind of combinations that are supported (e.g. only NFRs are taken in consideration and dependencies between sub-profiles are not mentioned) .

5.2.4.5.2.4 Profiling the SWIM Profiles.

For structuring SWIM Profiles, a profiling model can be used that is inspired by the models provided by ISO and OGC .

Typically a commonly shared foundational set of specifications is identified first. The term “core” will be used subsequently for such construct re. SWIM Profiles.

To this “core” specification, which is the mandated minimum, optional other sets of specifications can be added (building up a “level 1” specification, as it is called in the examples below) . In case such additional set of specifications does not overlap/conflict with the “core” set of specifications or any other sets of specifications, the resulting overall specification is then the union of the “core” specification with the optional sets of specifications. In case of overlap an overriding hierarchy needs to be defined.

The manner in which the additional specifications can be added to the “core” set of specifications, is essentially characterized by the dependencies amongst the sets of specifications. There are two elementary patterns: stacked and side-by-side.

In a stacked pattern, an optional set of specifications relies on the presence of one or more other sets of specifications.

In a side-by-side pattern, the presence of an optional set of specifications does not depend/conflict with the presence/absence of another optional set of specifications.

These two elementary patterns can be combined to form complex dependencies.

Any optional set of specifications always depends on the “core”.

This structuring of the SWIM Profile itself, allows for wide flexibility to cope with the current known needs as well as unknown/changed future needs.

This structuring is not applicable in all contexts where the definition of a SWIM Profile is required. In some contexts the definition of only a “core” SWIM Profile may suffice or even be imposed.

The semantics of this structuring are not generic and need to be explicitized on case by case base. Examples of different semantics:

The “core” of a SWIM Profile contains the minimum set of specifications to allow interoperability between consumer and provider but with a quality of service that is on a best effort base only. A “level 1” of the same SWIM Profile includes all of the “core” specifications and replaces some of the quality of service specifications with higher grade specifications for the provider side allowing both a client with a “core” compliant implementation as well as a client with a “level 1” compliant implementation to use the service.

The “core” of a SWIM Profile provides the specifications to allow interoperability using synchronous Request/Reply MEP. A “level 1” of the same SWIM Profile adds a Push Publish/Subscribe MEP.

The “core” of a SWIM Profile provides the specifications to allow interoperability using http 1.1 protocol without support for http compression. A “level 1” of the same SWIM Profile adds support for compression in http 1.1. both at the provider side and the consumer side.

The “core” of a SWIM Profile provides the specifications to allow interoperability providing integrity and confidentiality at transport level only using ssl v3.0, tls 1.0 and tls 1.1. A “Security Pack” of the same SWIM Profile adds support for integrity and confidentiality at message level and replaces support for ssl v3.0, tls 1.0 and tls 1.1 at transport level by tls 1.2 without fallback onto ssl v2.0.

5.2.4.6 Design consideration #5. Lifecycle of the SWIM Profile.

A SWIM Profile is a set of specifications. The specifications themselves may change and this change may impact the SWIM Profiles. Errors and specifications that need improved clarity, are examples of other triggers for change of SWIM Profiles.

Interoperability, FR and NFR in SWIM are based on strict adherence by all participants to an unambiguously identifiable set of the specifications as well as their understanding thereof. This established set of specifications for a SWIM Profile must remain unambiguously identifiable and immutable for an unlimited period.

Therefore, incorporating change in the SWIM Profile means that a new set of specifications must be defined, even if the change concerns only a single specification of the entire SWIM Profile. This new set itself must also be unambiguously identifiable and immutable for an unlimited period.

Such a new set of specifications can become a version + 1 of an existing SWIM Profile (e.g. Green Profile 1.0 exists and the new set is called Green Profile 1.1) or the name of the SWIM Profile can change altogether (e.g. Green Profile 1.0 exists and the new set is called Red Profile 1.0).

> A clear motivation and description of the purpose of a SWIM Profile, can support the decision process on the naming of a new set of specifications. If the change does not fundamentally change the motivation and purpose of the SWIM Profile, then the name of the SWIM Profile could remain, only updating the version number.
>
> Hypothetical example: the AMQP 0.9x protocol as part of a SWIM Profile is declared obsolete and superseded by AMQP 2.0. Subsequently the AMQP 0.9x protocol is no longer supported by most manufacturers/solution providers. The definition of a new SWIM Profile to mandate the AMQP 2.0 protocol instead of AMQP 0.9x protocol would not substantially change the motivation and purpose of the SWIM Profile. Hence the new SWIM Profile could keep the same name but with another version number.

As the SWIM Profile is a set of specifications of very different nature, the pace of change of some of its constituent specifications may be much higher than that of other constituent specifications. The combined effect of such changes could result in too many SWIM Profiles. The modularization of the SWIM Profile as described above can mitigate to some extent the impact of the change rate to sets of specifications only.

> In case of modularization, also each set of specifications needs its own unambiguous and immutable identification for unlimited period.
>
> Example: the rate of new versions for SSL/TLS (v2, v3.0, 1.0, 1.1 and 1.2) has been significantly higher than the rate of new versions for http (1.0 and 1.1).

Consideration must also be given to the co-existence of different versions of SWIM Profiles without any of the versions being planned to be phased out. This increases the fragmentation.

5.2.4.7 Design consideration #6. Design rules.

A SWIM Profile shall not relax the mandatory requirements of a referenced standard.

A SWIM Profile shall group mutually dependent specifications in the same set of specifications.

Distinct SWIM Profile that share common specifications should reference to these common specifications through another set of specifications.

5.2.4.8 Design consideration #7. Design criteria.

Below a series of additional potential criteria that could be used to define distinct SWIM Profiles or to perform profiling within a SWIM Profile.

- Increasing grade of functionality (e.g. GP Messaging+).
- Increasing grade of quality of service in general (e.g. GP Advanced QoS).
- Increasing grade of specific quality of service (e.g . GP Performance Pack, GP Security Pack, GP Reliability Pack, GP Evolution Pack).
- Stakeholder footprint (the core includes specifications that interest a large part of the potential stakeholders, sets of specifications for which there is a more marginal interest could be optional).

5.2.5 Naming

The content of one or more SPAs is likely to evolve in Step 3 of the SESAR Programme and beyond.

In such case human to human communication referencing a particular version of the SPA will occur. Use of the technical name may not be efficient and may lead to mistakes.

Hence a nickname structure is defined for the SPA as follows:

<Colour Name> [v<1-char SESAR step>.<1-char sequence>]

Examples:

Yellow

A generalization of all versions of the SPAs with the name Yellow

Blue v2.1

The first version of SPA Blue defined in the second step of SESAR

5.3 SWIM Profile Descriptor

5.3.1 Introduction

If there would be no guidance for defining the set of specifications that form a SWIM Profile, not a single set of specifications would look like another one in structure or they would look like one another in structure but with different semantics or subtle differences.

Such situation would make many uses of the set of specifications that form a SWIM Profile very difficult and error-prone and ultimately of no value for the stakeholders.

Areas of specifications that are not explicitly addressed in a SWIM Profile are subject to assumptions and speculation. Such assumptions and speculation will not be uniform and will lead to implementations that are not interoperable as well as to implementations that do not meet the expectations of the service bound to the implementation.

Further, even when all areas of specifications are explicitly and effectively addressed in a SWIM Profile, these specifications can still be wrong/illegal or misinterpreted making them inapt not only for interoperable implementations but for instance also for comparison in order to assess the suitability for use in a particular context.

The instrument that provides the guidance for defining the set of specifications that form a SWIM Profile is the SWIM Profile Descriptor (SPD).

The SPD is a mandatory template to use for any effective composition of specifications related to any SWIM Profile Assertion.

The SPD identifies and structures all the areas of specifications that have to be taken in consideration and, where applicable and possible, details each of these areas down to the level of provision of templates for atomic specification.

The SPD defines how the set of specifications that form a SWIM Profile must be structured and documented.

The use of the SPD creates value for distinct stakeholders.

For the creator of the SWIM Profile, the use of a mandatory template promotes both the exhaustiveness of the definition of a SWIM Profile as well as quality of the specifications.

For the governing bodies, the SPD provides a means for verification of the exhaustiveness and quality of the specifications in a SWIM Profile.

For the user of a SWIM Profile (a Communication Infrastructure provider, a SWIM-TI solution builder as well as a service binding to a SWIM-TI solution), the SPD provides standardisation, stability, consistency and transparency across SWIM Profiles.

5.3.2 Single authoritative source

Of major concern is the duplication of definition, classification and specifications (groups and/or atomic) and the management issues such duplication entails.

For each of the entities that constitute a SWIM Profile, the SPD details the elements to be taken in consideration when defining a SWIM Profile. These elements are definitions, classifications and specifications (groups and/or atomic) that exist already elsewhere in authoritative sources. The SPD does not (re)define and/or duplicate any of these elements itself but references them.

The referencing implies that each of the referenced entities has a unique and unambiguous identification.

5.3.3 Naming

The content of the SPD is likely to evolve in the iterations of the SESAR programme and beyond.

The SPD will have a lifecycle and distinct versions will exist. Each version of the SPD requires its own unambiguous unique identifier:

- In order to be manageable by the CMS.
- To be able to identify instances of relations with other elements.

Also, human to human communication referencing a particular version of the SPD will occur. Use of the technical name may not be efficient and may lead to mistakes.

Hence a nickname structure is defined for the SPD as follows:

SPD v<1-char SESAR iteration>.<1-char sequence>

The SESAR iteration and the sequence are also the attributes that make the technical name of the SPD unique. Hence, a 1-1 mapping between a technical name and a nickname is assured.

Example:

SPD v2.3

The third SPD defined in the Iteration 2.

5.3.4 Lifecycle

The content of the SPD is likely to still evolve in next iterations of the SESAR programme and beyond.

The SPD is a superstructure that encompasses through references potentially many definitions, classifications and specifications (groups and/or atomic). Each of these definitions, classifications and specifications (groups and/or atomic) have their own lifecycle. Each single change in each of these definitions, classifications and specifications (groups and/or atomic) could lead to the definition of a new SPD.

High reactivity to such changes may lead to a large amount of SPDs and low transparency. Conversely buffering and consolidating such changes in an annual or biennial definition of a new SPD may lead to inflexibility.

A trade-off between reactivity and consolidation consists of a biannual publication of a new SPD.

The appearance of a new SPD can but does not necessarily invalidate or signal the end-of-life of any preceding version. The end-of-life of an SPD will be signalled through an explicit mention in a new SPD of which SPDs it supersedes.

5.3.5 Stakeholder role

The contents of the SPD itself and thus the changes during its lifecycle will be determined by new/changed/dropped definitions, classifications and specification (groups and/or atomic). The direct sources of these changes are SWIM-TI TAD and SWIM-TI TS.

The indirect sources of SWIM-TI TAD and SWIM-TI TS that ultimately propagate into the SPD, are both Bottom-Up and Top-Down.

The maintenance of the SPD itself is currently a responsibility that is assigned to WP14.1.3.

The governance stakeholders will use the SPD to verify the exhaustiveness, usefulness and validity of the SPIs that are derived from the SPDs.

The governance stakeholders will use the SPD to verify the exhaustiveness and validity of the specifications taken into considerations compared to the contents of the SWIM-TI TAD and SWIM-TI TS.

5.4 SWIM Profile Instantiation

5.4.1 Introduction

A set of specifications that has been created according to a SPD is called a SWIM Profile Instantiation (SPI).

The SPD and the SPA are two distinct governance entities that keep the SPIs manageable.

- SPA for a reason of existence.

  Each SPI is linked with exactly one SPA (cardinality 1,1 navigable from SPI to SPA). In its nickname the SPI includes this link.

  Multiple SPIs can be linked to the same SPA.

- SPD for a standardized content.

  Each SPI is linked with exactly one SPD (cardinality 1,1 navigable from SPI to SPD). This link is not included in the nickname of the SPI.

5.4.2 Naming

The content of the SPI is likely to evolve in next iterations of the SESAR Programme and beyond.

In such case human to human communication referencing a particular version of the SPI will occur. Use of the technical name may not be efficient and may lead to mistakes.

The nickname used for SPIs revolves around the name that is given to the SPA:

Every SPI shall document the SPA that is applicable.

The applicable SPA reflects a particular scope of an SPI. When changes occur to a SPI such that its content is no longer aligned with the scope, then that will signal the need for the creation of a new SWIM Profile Assertion.

Currently the name is a colour.

Hence a nickname structure is defined for the SPI as follows:

[<profile part>]<Colour name>[{<1-char SESAR iteration><1-char sequence>}]

<Colour name>: A Swim Profile.

When used alone with none of the optional leading and/or trailing elements, it represents a generalization of all versions and all profile parts.

When used without the leading <profile part> element and including the trailing version element, then it represents all profile parts for a particular version of a SWIM Profile Instantiation.

When used with the leading <profile part> element and including the trailing version element, then it represents the specific profile part for a particular version of a SWIM Profile Instantiation.

When used with the leading <profile part> element and without the trailing version element, then it represents a generalization of all versions of the profile part.

<profile part>: A specific part of a SWIM Profile

A SWIM Profile can consist of multiple parts (in analogy with the Multi-Part technique as described in ISO/IEC TR 10000-2 for which the text is publicly available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html)

In case the part identifies an optional set of requirements then it must only be combined with the mandatory set of specifications with which they have been instantiated.

{ <1-char SESAR iteration><1-char sequence>}

The SESAR iteration and the sequence are also the attributes that make the technical name of the SPI unique. Hence, a 1-1 mapping between a technical name and a nickname is assured.

5.4.3 Lifecycle

The content of the SPI is likely to still evolve in next iterations of the SESAR Programme and beyond.

The SPI is derived from a particular SPD template. A new SPI could be derived from an existing SPD and does not necessarily have to wait for the publication of a new SPD and thus does not necessarily have to follow the schedule of publication of new SPDs.

Nevertheless, too often publication could lead to too many almost identical SPI and hence fragmentation and low transparency (i.e. it is difficult to understand the difference between SPIs and difficult to select the one that is appropriate for a particular business context). It is therefore recommended to follow the SPD schedule.

The appearance of a new SPD can but does not necessarily invalidate or signal the end-of-life of any preceding version. The end-of-life of an SPI will be signalled through an explicit mention in a new SPI of which SPIs it supersedes.

The end-of-life of an SPD signals the end-of-life of any SPI that has been created from it.

5.4.4 Presentation

The number of eligible specifications has a significant size.

The presentation of the specifications in the SPI has a high impact on the accessibility and efficiency for the user of the specifications. Providing a flat list of specifications to multiple stakeholders with different interests is counterproductive. Hence multiple views need to be provided that reflect the different interests of Stakeholders.

5.4.5 Stakeholder roles

The contents of the SPI itself and thus the changes during its lifecycle will be determined

- either dependent on the evolution SPD
    - a new SPD reflects changes to specifications that somehow should be reflected in a change at the level of the SPI.
    - In case a new SPD would not result in at least one new SPI, then this would reflect either a phoney specification or a specification that is forgotten
- or independent of the evolution of the SPD
    - a new SPI can be created from the existing SPDs that are not end-of-life in case a new/changed need (Top-Down/Bottom-Up) emerges that can be satisfied with the existing elements of one of the SPDs.
- or a combination of both

The maintenance of the SPI themselves is currently a responsibility that is assigned to WP14.1.3.

The SPIs are the instruments that are made available to the decision makers re. the binding of a service to the SWIM-TI.

The SPIs are the instruments that are made available to the solution builders to enable an autonomous built of a solution that most probably will then integrate and fit into SWIM easily.

The SPIs are the instruments that are made available to the providers of communication infrastructure builders to enable the provision of communication infrastructure that satisfies the needs of the SWIM-TI and that also allows the binding of the SWIM-TI to the communication infrastructure.

The governance stakeholders will use the SPI to verify the exhaustiveness, usefulness and validity of the SPIs that are derived from the SPDs.

The governance stakeholders will use the SPI to verify the exhaustiveness and validity of the specifications taken into considerations compared to the contents of the SWIM-TI TAD and SWIM-TI TS.

5.5 Overview

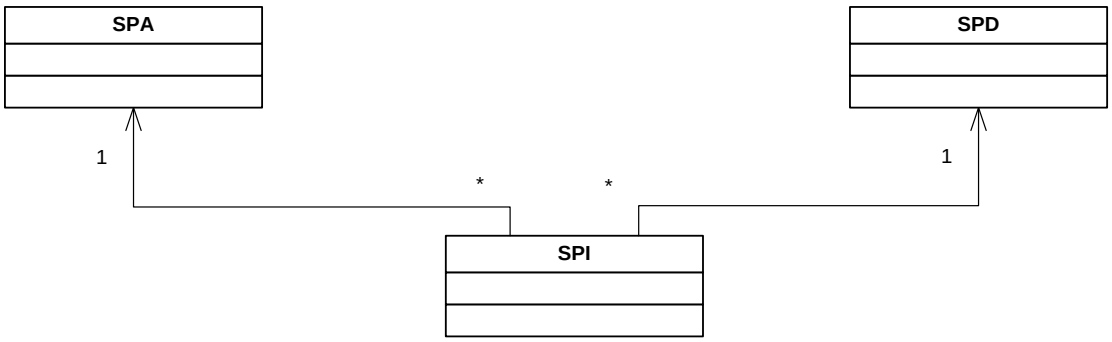

Figure 7 Relation between the SPA, SPD and SPI, class view

An SPI can only exist when there is an SPA that asserts the needs for a SWIM Profile. One or more versions of an SPI can be created that conform to the SPA.

The SPI is expressed in a form that is aligned with the guidelines provided in the SPD. Multiple SPIs can be created all aligned in a form aligned with an SPD.

5.6 Examples of links and naming

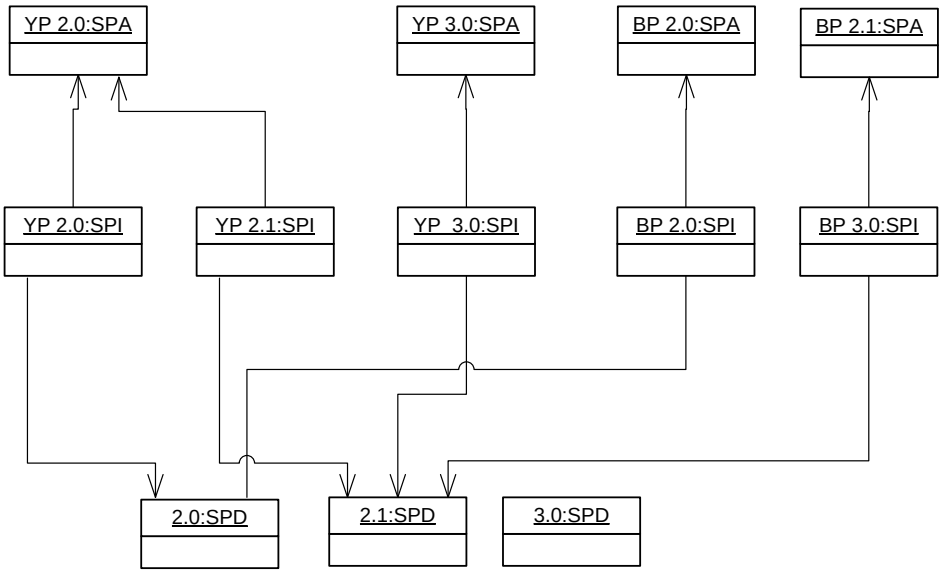

Figure 8 Relation between the SPA, SPD and SPI, object view

An SPA is declared in Iteration 2. The SPA is given nickname YP 2.0. 2 stands for Iteration 2 and 0 stands for an occurrence.

An SPA is declared in Iteration 2. The SPA is given nickname BP 2.0.

The SPA with nickname BP 2.0 requires a change in Iteration 2. The SPA is given nickname BP 2.1. 2 stands for Iteration 2 and 1 stands for an occurrence.

The SPA with nickname YP 2.0 requires a change in Iteration 3. The SPA is given nickname YP 3.0. 3 stands for Iteration 3 and 0 stands for an occurrence.

The SPD is defined Iteration 2. The version of the SPD is uniquely identified by the Iteration number and the occurrence within the iteration. The SPD is given nickname 2.0

An update of the SPD is required during Iteration 2. The updated SPD receives occurrence number 1 as occurrence number 0 is already used.

A further update of the SPD is required during Iteration 3. The version of the SPD is uniquely identified by the Iteration number 3 and occurrence number within the iteration. The updated SPD receives occurrence number 0 as it is the first definition of SPD in Iteration 3.

An SPI for the YP is defined in Iteration 2. It aligns with the scope and structure defined in SPA YP 2.0. It aligns with SPD 2.0 for its content. The SPI is given nickname YP 2.0. 2 stands for Iteration 2 and 0 stands for an occurrence.

Following the update of SPD 2.1 an update of the SPI for the YP is defined in Iteration 2. It aligns with the scope and structure defined in SPA YP 2.0. It aligns with SPD 2.1 for its content. The SPI is given nickname YP 2.1. 2 stands for Iteration 2 and 1 stands for an occurrence.

Following an update SPA 3.0 for the YP an update of the SPI for the YP is defined in Iteration 3. It aligns with the scope and structure defined in SPA YP 3.0. It aligns with SPD 2.1 for its content. The SPI is given nickname YP 3.0. 3 stands for Iteration 3 and 0 stands for an occurrence.

An SPI for the BP is defined in Iteration 2. It aligns with the scope and structure defined in SPA BP 2.0. It aligns with SPD 2.0 for its content. The SPI is given nickname BP 2.0. 2 stands for Iteration 2 and 0 stands for an occurrence.

Following the update of SPA 2.1 for the BP and an update of the SPD 2.1 an update of the SPI for the BP is defined in Iteration 3. It aligns with the scope and structure defined in SPA BP 2.1. It aligns with SPD 2.1 for its content. The SPI is given nickname BP 3.0. 3 stands for Iteration 3 and 0 stands for an occurrence.

6 SWIM Profiles

6.1 Considerations

The study in Appendix E of D32 [18], had revealed an opportunity to merge the Step 1 B2B NOP Profile and Step 1 EAD B2B Profile into a new SWIM Profile in Iteration 2. It was proposed to take this up in Iteration 2.1. This has effectively led to the definition of a new SWIM Profile: the Yellow Profile.
The Yellow Profile renders the former Step 1 EAD B2B Profile and Step 1 NOP B2B Profile obsolete.

As identified in D32 [18] the A15 deliverable, gave clear indications of the need for at least 1 additional Iteration 2 Profile related to the Air/Ground segment. Effective work on the definition of this SWIM Profile was dependent on the availability of mature specifications aligned with the WP14 formalism. The specifications have been analysed and aligned with the WP14 formalism. As the specificities of the requirements could not be fulfilled in an appropriate manner by the existing SWIM Profiles, this has led to the definition of a new SWIM Profile: the Purple Profile.
The Purple Profile does not replace or render any other SWIM Profile obsolete.

An updated version the ATC-ATC Profile in Iteration 2 was anticipated in [18] to take into account evolution of requirements..
Evolution of the requirements has effectively taken place. The updated set of requirements has been named Blue Profile.
The Blue Profile renders the former Step 1 ATC-ATC Profile obsolete.

Also, security requirements for the Blue Profile cannot be satisfied by the DDS technology in its current status. Work is on-going at OMG and its partners to enhance the DDS technology with security functionality in a standardized manner. When such security functionality will be standardized, it will be included in the updated Blue Profile.

The information of the last release of ISRM V1.0 reference [19] has not demonstrated in Iteration 2.1 the need for the creation of other additional SWIM Profiles or the need for removal of other SWIM Profiles.

The information of the last release of ISRM V1.1 reference [21] available for Iteration 3.0 at the time of writing, has not demonstrated the need for the creation of other additional SWIM Profiles or the need for removal of other SWIM Profiles. It has demonstrated however the need for support of asynchronous messaging. This has triggered the definition of a new Profile Part in the Yellow Profile: Messaging+.

The information of the last release of ISRM V1.2 reference [22] has become available too late to be taken into account in Iteration 3.0.

The assessment of the last release of ISRM 1.4 [26] has not demonstrated the need for the creation of other additional SWIM Profiles or the need for removal of existing SWIM Profiles. This assessment has not demonstrated the need to change any of the existing SWIM Profiles. However this does not mean that such needs do not exist for the defined services because:

. The ISRM 1.4 uses to a large extent a template in the "NSOV-1 Service Taxonomy" that allows to capture NFRs relevant for the SWIM TI in a structured manner. However in very few cases only such NFRs have effectively been specified.

. Also, the ontology and semantics used in the ISRM 1.4 to identify the Message Exchange Patterns were not sufficiently clear to understand the impact on the SWIM TI. This has changed with ISRM 2.0, where a slight change in the naming of the MEPs on the ISRM side makes things more clear.

The information from FT10 and Working Method on Services has revealed for Iteration 3.0 the need for additional bindings in the Yellow Profile as well as in the Blue Profile. Moreover it has identified the need to define a new Profile Part for the Blue Profile: BP FDD.

The structuring linked to interoperable implementations as defined in the TAD [1], targeting a high flexibility in deployment options has revealed the opportunity to separate the protocol bridging function in the Purple Profile. This function has been contained in a new Profile Part in the Purple Profile: PP Message Bridging.

6.2 Iterative re-evaluation

SESAR concept and supporting SWIM services and functional blocks are still under development, therefore, further work is mandatory for what concerns the SWIM Profile.

New SESAR Concepts may reveal changed/new MEP requirements, changed/new SWIM TI functional blocks and changed/new NFRs which may require a review of the SWIM Profiles. For instance, new SESAR concept may lead to:

- The creation of a new profile
- The change of an existing profile
- The removal of an existing profile
- The merge of existing profiles

The profiles will thus not necessarily remain the same but so far there is not enough substance to motivate changes.

A review of SWIM Profiles will be performed with the next release of the ISRM. This first review will enable the SWIM development teams to refine the SWIM Profile review process.

6.3 Swim Profile Assertion (SPA)

For each SWIM Profile a separate TS document exists.

The entire SPA of the SWIM Profile is located in Chapter 2.4 of each such TS document. The description at this location is the authoritative source of the SPA.

The lifecycle of the SPA follows and is synchronized with the lifecycle of the TS document.

6.4 SWIM Profile Descriptor (SPD)

The SPD is a single separate document.

6.5 SWIM Profile Maturity

A maturity assessment has been performed for the SWIM Profiles. The result of this analysis indicate that the Blue Profile as well as the Yellow Profile have both reached the maturity level V3.

7 References

7.1 Applicable Documents

[1] **PB.04.03-D95**, ADD Step 1 (2014 edition), Edition 00.02.02

[2] WPB.01 Integrated Roadmap, Dataset 00.00.16.

7.2 Reference Documents

[3] **WP 14,** Revision Framework, v00.01.00, 21/05/2012

[4] **P14.02.09-D03**, SWIM Technical Infrastructure Definition, v00.01.02, 19/09/2011

[5] **P14.01.2-D03**, SWIM Context Definition, v00.01.00, 24/11/2010

[6] **P9.19-D03**, High-Level SWIM A-G Architecture and Functional Requirement Specification, v00.02.00, 08/12/2011

[7] **P08.01.01-D42,** SWIM Conops, v00.04.05, 30/04/2014

[8] **PB4.3-D100,** SESAR Working Method on Services (edition 2014), v00.05.01, 14/04/2015

[9] **P14.01.04-D41,** SWIM-TI Technical Specification 2.1, v00.02.00

[10]EUROCAE WG59, ED-133 Flight Object interoperability specification, June 2009

[11]ISO/IEC FDIS 25012, (SQUARE) – System and Software quality models, 14/12/2010

[12] **P1447D002**, Study on SWIM Civil-Military Interoperability – D1, V1.0, 12/09/2012

[13] **P1447D003**, Study on SWIM Civil-Military Interoperability – D2, V1.0, 12/09/2012

[14] **P1447D004**, Study on SWIM Civil-Military Interoperability – D3, V1.0, 12/09/2012

[15] **P08.03.10-D06**, ISRM 0.4 Delivery Report, v00.01.00, 30/03/2012

[16] **P08.03.10-D07**, ISRM 0.5 Delivery Report, v00.01.00, 30/09/2012

[17] **P14.01.03-D33,** SWIM Architectural Definition for Iteration 2.1, v00.02.00

[18]P14.01.03-D32, SWIM Profiles for Step 2 – Iteration 2.0- 00.02.51

[19]P08.03.10-D09, ISRM 1.0. Delivery Report, Edition 00.01.00

[20] **P14.01.03-D34**, SWIM Profiles for Step 2 – Iteration 2.1- 00.02.00

[21]P08.03.10-D61, ISRM 1.1. Delivery Report, Edition 00.01.01

[22]P08.03.10-D62, ISRM 1.2. Delivery Report, Edition 00.01.00

[23]P14.01.04-D42, SWIM-TI Technical Specifications Catalogue 3.0, v00.02.00

[24]P14.01.03-D30, SWIM Architectural Definition Final, v00.01.01

[25]P14.01.04-D43, SWIM-TI Technical Specifications Catalogue 3.1, v00.01.00

[26]P08.03.10-D64, ISRM 1.4. Delivery Report, Edition 00.01.00

[27]P14.01.03-D38, SWIM Profiles for Step 3.1 – Edition 00.01.00

[28]P14.01.04-D44-001, SWIM-TI Technical Specifications Catalogue, v00.01.00

Appendix A Segmentation at the level of SWIM TI

A.1 Context

SWIM TI profiling is delimited and driven by several sources.

- The segmentation that is established at architectural layers above the layer of the SWIM TI.

  This form of segmentation is expected to be driven by higher level WPs such as WP8 and WPB.

  Compliance is mandatory.

- Constraints, requirements and risks that cross layers to the SWIM TI layer.

  The information is expected to be provided by higher level WPs.

  Compliance is with the constraints and requirements mandatory. Dealing with the risks is mandatory.

  Non-functional requirements and crosscutting concerns[16] are typical examples of requirements.

- The segmentation that is targeted at the layer of the SWIM TI itself.

From an infrastructure point of view a segmentation that tries to maximise reuse of existing infrastructure will typically be favoured.

A.2 Possible approach

A.2.1 Granularity

Segmentation can be performed at varying levels of granularity:

- Fine-grained segmentation will allow the provided solution to closely match the requirements and constraints.
  - Provides high efficiency from the local perspective of the segment
  - Creates risk of segment-sprawl and fragmentation into many distinct technologies
    - High inefficiency from a global perspective of the SoS
    - Drifting towards the problem of a large diversity of point solutions in the current system

- Coarse-grained segmentation will allow the provided solution to meet or exceed a grouped set of requirements and constraints
  - Provides reduction of the integration and interoperability issues
  - Provides increased reuse, reduction of the costs and thus high efficiency from the global perspective of the SoSCreates risk not to take into account the key issues identified above

[16] An architectural consideration of areas that are not specific to one layer aiming to implement solutions in a centralised and shared manner and/or the application of a common policy throughout. Authentication is a typical crosscutting concern and in particular the manner by which the identities cross the layers

A.2.2 Qualitative approach

The qualitative approach is based on the view of domain experts who can determine a relevant high-level structure for segmentation that suits both the current needs and the anticipated future needs.

The main value of the qualitative approach is its fast results and its low investment costs.

The main risk of the qualitative approach is missed crucial insights and the lack of a detection mechanism.

Examples of boundaries that the domain experts may use for segmentation:

- Areas of functionality
- Client/consumer types

A.2.3 Quantitative approach

The quantitative approach is based on the exhaustive collection of detailed requirements, finding commonalities in requirements and grouping them.

The main value of the quantitative approach is the exhaustiveness.

The main cost of the quantitative approach is its lengthy and resource-intensive process.

The main risk of the quantitative approach is lack of consistency and efficiency of the grouping mainly because of the following aspects

- the bottom-up nature
- the lack of holistic visibility due to the incremental availability of the detailed requirements.

A.3 Interoperability between Segments

A.3.1 Introduction

This document does not have architectural decisions re. technology interoperability between segments in its scope.

This document provides below 2 examples of a way to establish such interoperability as input to the architecture decision process.

A.3.2 Gateway

A gateway in this context is defined as a generic device – software and/or hardware – that performs protocol conversion. From a conceptual point of view, protocol conversion can take place at any layer of the ISO OSI 7-layer model.

A gateway can provide interoperability between segments that are not interoperable otherwise because of the use of distinct protocols and/or distinct configurations of the same protocols.

The use of a gateway introduces a number of non-trivial challenges. Depending on the nature of the protocols to be converted, the challenges will be solved or remain unsolved partially or entirely. Awareness of such challenges in the architectural decision process could lead to mitigation or avoidance of these challenges if taken into account.

Examples of such challenges:

- loss of functionality:

Within the same domain of functionality, the specific functionality provided by distinct protocols can be different.

Absence of a 1-1 mapping between the functionality of the involved protocols, will make mapping of some specific functionality difficult or impossible.

Mapping may also significantly increase complexity and it may impact other protocols at other layers.

An example of a challenging mapping of functionality: the relational model of the topics in the DDS protocol to another Publish/Subscribe protocol.

- loss of end-to-end visibility

  To enable protocol conversion the gateway may be required to simulate an endpoint for a protocol where in reality it is not.

  The real end-points will not be aware of each other's real and current status.

  An example of a challenging mapping of end-to-end visibility: end-to-end security in case of protocol conversion when using security over a transport layer.

- loss of QoS.

  Different protocols can provide different QoS.

  The QoS cannot necessarily be maintained during the protocol conversion.

  An example of a challenging mapping of QoS: the very low latency in case of a Publish/Subscribe protocol that supports multicast to a Publish/Subscribe protocol that only supports unicast.

Gateways can be set up in multiple configurations. Examples:

A gateway can be located anywhere between a consumer in one segment and a provider in another segment. For instance: at the consumer, at the provider or a component in the network.

Multiple gateways can coexist. Cascading of gateways will increase the difficulty of the challenges.

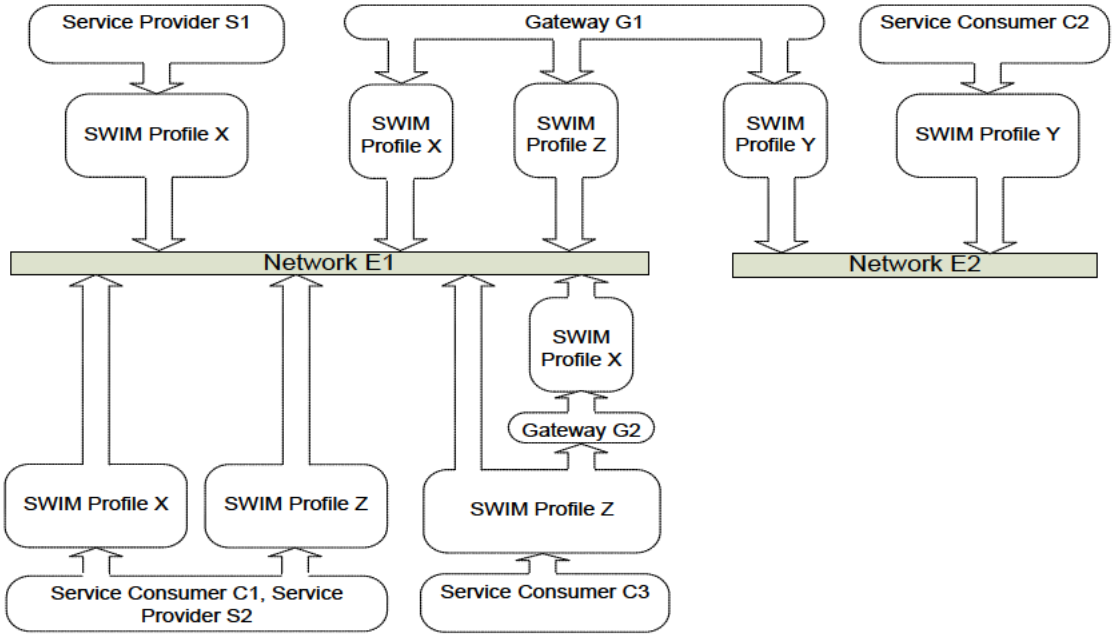

Figure 9 Interoperability provided through the use of a Gateway

A.3.3 Consumer/provider participate in more than 1 segment

Approaches that are different from the gateway but that can deal with a need to access a service in one segment from another segment, consist of for example

- instantiation of the service in multiple segments
- a consumer that participates in multiple segments

Such approach introduces its own challenges too. Examples

- undoing segmentation

  Extensive use of such technique would question the rationale of the defined segmentation

- appropriateness of QoS

  As each segment would probably have its specific set of QoS, participation as a provider or a consumer in some segments could be incompatible with the required QoS from the service perspective

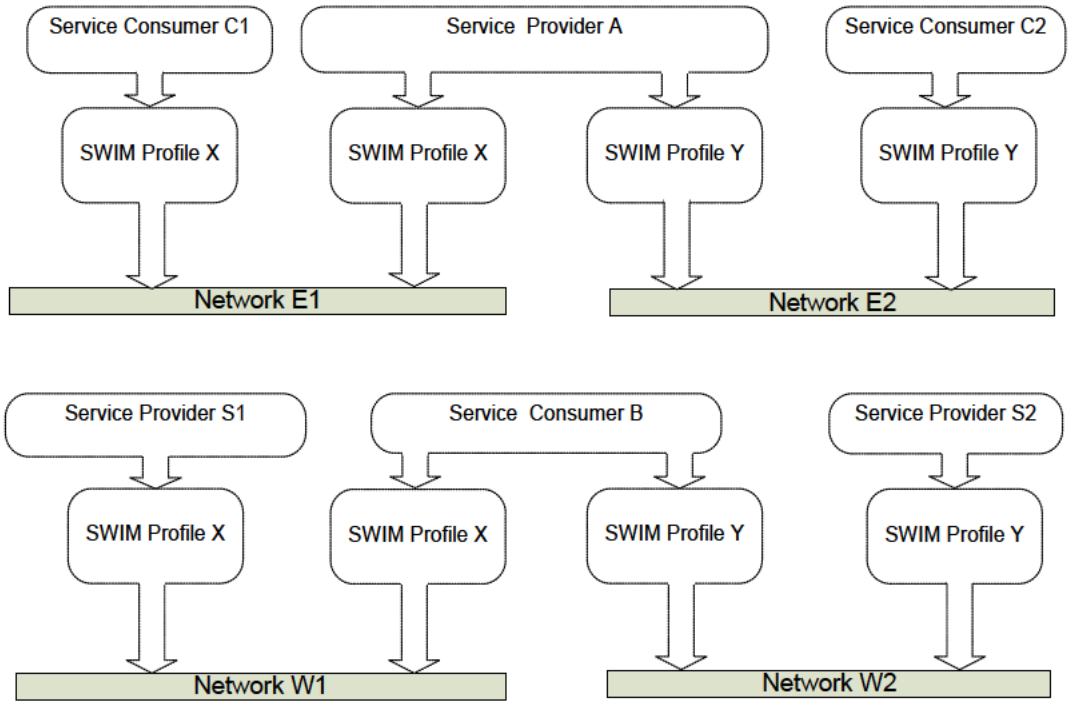

Figure 10 IOP provided through participation in multiple segments

Appendix B Segmentation across layers

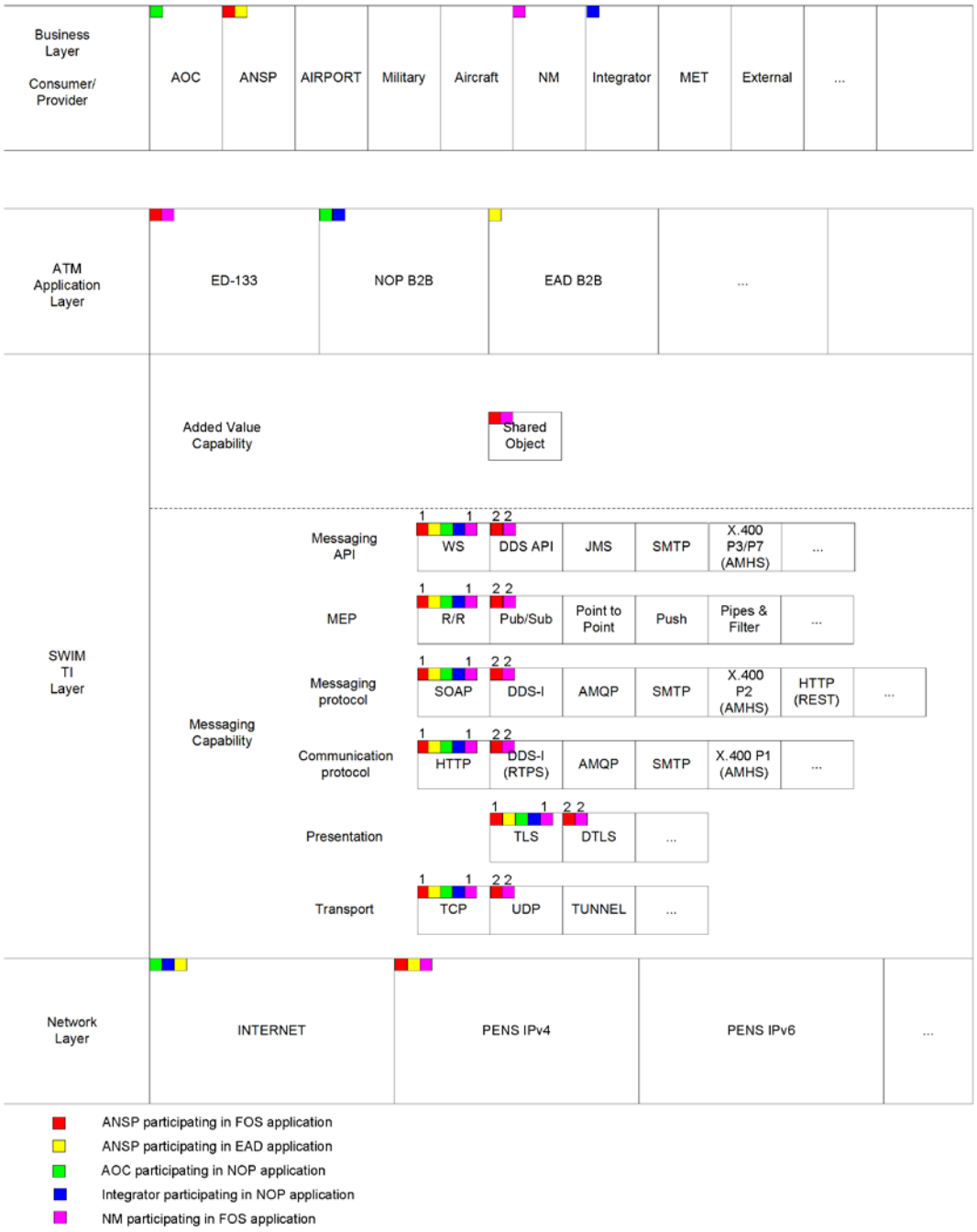

Figure 11 Segmentation at distinct layers

Figure 11 above illustrates how segmentation could be performed at distinct layers, how segments in one layer map onto segments in another layer and how segments can be reused.

This figure is by no means a reference nor complete.

The segmentation at the Business layer and the ATM application layer is a simple illustration. Many other forms of segmentation are possible at these layers but that is out of the scope of this document.

The SWIM TI layer has been detailed somewhat in the context of this white paper.

The coloured blocks identify a communication path across the layers. For instance, the red block demonstrates the communication path and the mapping of segments in case of the participation of an ANSP into the distributed FOS application:

- the ANSP uses the ED-133 compliant application
- the ED-133 compliant application uses the SWIM TI layer:
  - the Shared Object functional block
  - the path (marked with 2 in the messaging functional block) along DDS API with Pub/Sub MEP, DDS-I protocols, possibly DTLS and finally UDP
  - the path (marked with 1 in the messaging functional block) along WS with R/R MEP, SOAP, HTTP, possibly TLS and finally TCP. the 2 paths ending in the SWIM TI layer at TCP and UDP all use the PENS IPv4 network

Appendix C Clarifications on the notions FR and NFR

C.1 Authoritative requirement classification models

This document uses the terms FR (Functional Requirement) and NFR (Non-functional Requirement) to structure the requirements. The definition of these terms is based on:

- the definition provided by ISO/IEC FCD 24765.5

  non-functional requirement. 1. a software requirement that describes not what the software will do but how the software will do it. ISO/IEC 24765, Systems and Software Engineering Vocabulary. Syn: design constraints, non-functional requirement. See also: functional requirement.

  EXAMPLE software performance requirements, software external interface requirements, software design constraints, and software quality attributes.

  NOTE Non-functional requirements are sometimes difficult to test, so they are usually evaluated subjectively.

  functional requirement. 1. a statement that identifies what a product or process must accomplish to produce required behavior and/or results. IEEE 1220-2005 IEEE Standard for the Application and Management of the Systems Engineering Process. 3.1.16. 2. a requirement that specifies a function that a system or system component must be able to perform. ISO/IEC 24765, Systems and Software Engineering Vocabulary.

- complemented with information found at https://en.wikipedia.org/wiki/Non-functional_requirement

C.2 FR ontology

A number of well-known methods exist to perform the refinement and breakdown of complex systems such as functional decomposition and object oriented decomposition.

The SESAR programme has selected the functional decomposition as an overall standard and D34 fully aligns with that standard.

From the top down, the breakdown of FR for this document uses at the highest level the SWIM-TI Functional Block (FB) structure as defined in the SWIM-TI TAD. For intermediate levels below the highest level, this document uses the SWIM-TI Function as defined in the SWIM-TI TAD.

At the most granular level of the breakdown, the structure is provided by the SWIM-TI TS in the form of SWIM-TI Technical Specifications (TS).

The SWIM-TI TS adds one element to the top level defined in the SWIM-TI TAD: Overall Functional Requirements.

C.3 NFR ontology

Various models and terminology exist to refine and structure the notion of NFR. In these models there is often a strong but varying interrelationship between the terms System Qualities, Non-Functional Requirements (NFRs) and Quality of Service (QoS).

Whereas the above ISO/IEC FCD 24765.5 definition classifies “software quality attributes” as one of several subclasses of non-functional requirement, the distinction between System Qualities, NFRs and Quality of Service in itself is not clearly and authoritatively defined and these terms are often used as synonyms (http://en.wikipedia.org/wiki/Non-functional_requirement).

Further, there is a lot of confusion and a high risk of misunderstanding through the lack of consistency between the models and their terminology.

- Identical terms have different semantics (e.g. reliability) and/or different terms are used for the same semantics (e.g. flexibility, changeability, extensibility)
- The same term is used as a composition of qualities as well as an "atomic" quality that can be measured (e.g. reliability).
- In some models an "atomic" quality can be linked to more than one composition of qualities, in others they can be linked to a single composition only (e.g. availability as a sub-characteristic of both security and reliability or as a sub-characteristic of security or reliability)

At the top level, the breakdown of NFR for this document structures the notion of NFR in two groups:

- How: a group with requirements that determine how a product must do it, i.e. implementation constraints
- How good: a group with requirements that determine how good a product must do it, i.e. quality related requirements

To mitigate confusion and misunderstanding, the NFRs for the SWIM Profile should be expressed using the model and terminology of an official standard where possible.

- Implementation constraints related requirements. Relevant elements for the breakdown of the implementation constraints are already provided in the structure of the SWIM-TI TS: “Design and Construction constraints” and “Functional Block Interface Requirements”. Assuming that these are directly mapped from the ISO vocabulary (e.g. "software design constraints", "software external interface requirements"), they are considered authoritative for the implementation constraints related requirements.
- Quality related requirements. Because the context of the SWIM Profile is the SWIM TI layer, following standards are considered applicable for the quality related requirements:
    - ISO/IEC 9126-1 and ISO/IEC 25010 as software product quality oriented standards. They are applicable as the instantiation of the SWIM TI will be through a software product.
    - ISO/IEC 13236 as a more network/distributed service quality oriented standard. This is applicable as the SWIM TI will operate in a distributed environment.

C.4 ISO/IEC 25010 as baseline for model and terminology

C.4.1 ISO/IEC 25010

Recent ISO/IEC standard

- ISO/IEC means broad agreement
- Recent means that it includes corrections, enhancements and relevant current best practices and that it is state of the art

- It was derived from ISO/IEC 9126:1991 and cancels and replaces ISO/IEC 9126-1:2001

It is a part of a coherent set of standards related to software and product quality:

- SQuaRE (Software product Quality Requirements and Evaluation) aims at a consistent approach for software product quality
- It is intended to be used together with the other standards of the SQuaRE series of which following may also be applicable:
  . ISO/IEC 25012 Data Quality Model
  . ISO/IEC 2502n Measures but not yet complete: ISO/IEC 25020 and ISO/IEC 25021 already exist and seem sufficient.

Drawbacks:

- Includes perspectives that may not be relevant in the context of the SWIM Profile
- Is oriented to product quality and less to distributed applications/services

C.4.2 ISO/IEC 9126-[1-4]

- ISO/IEC 9126-1:2001 has been superseded by ISO/IEC 25010

- The elements of the ISO/IEC 9126-[2-4] standard are replaced or being replaced by standardisation in the context of SQuaRE

- Some elements of ISO/IEC 9126-[2-4] could be reused as a source for potential measures that are not or not yet proposed in the context of SQuaRE

C.4.3 ISO/IEC 13236

- Preference of ISO/IEC 25010 over ISO/IEC 13236 as baseline:
  - ISO/IEC 13236 is more than 10 years older
  - The SWIM Node implementation is a pure software product

- Elements of ISO/IEC 13236 could be reused as a source for potential qualities and measures that are not or not yet proposed in the context of SQuaRE.

C.4.4 Alignment in the SESAR programme

C.4.4.1 D41

The selection of ISO/IEC 25010:2011 as baseline for model and terminology is fully aligned with the use of the terms NFR in D41. A 1-1 mapping between D34 and D41 has been defined.

C.4.4.2 SACG

At other places in the SESAR Programme, there is work in progress re. NFR. Two main sources that are linked to each other, provide insight:

- "B4.3 Issue Description NFR Taxonomy for Information Exchanges/ Information Services" at https://extranet.sesarju.eu/WP_B/Project_B.04.03/Other%20Documentation/T2%20Architecture%20Strategy/Cycle4/Non%20Functional%20Requirements/NFR%20Taxonomy%20issue%20description%20389791.doc

- https://extranet.sesarju.eu/WP_B/Project_B.04.03/Other%20Documentation/02%20Service%20-%20SCG/Service%20Allocation/20120626%20SACG%20NFR%20List%20of%20Attributes%2040300(2).xls

These documents limit the notion of NFR to the "How good" aspect as reflected through the alignment to the ISO/IEC 25010:2011 standard.

There is no conflict between this ongoing work on NFR elsewhere in the program and D34 but the definition of NFR in D34 is an extension of that work.

C.5 Point of view

As explicitly illustrated in the citation below from the document "B4.3 Issue Description NFR Taxonomy for Information Exchanges/ Information Services", the appreciation of what is a NFR or FR not only depends on the definition and interpretation but also depends on the point of view:

"It could be said that what are NFRs at WP8 level, could later be understood as Technical Requirements at WP14 level"

Hence, what is classified as NFR from the point of view of WP8, is split into FR and NFR from the point of view of WP14.

This document is a WP14 document and therefore it uses the terms FR and NFR from the point of view of WP14.

From a WP8 point of view, these FR and NFR as used in this document can all be considered to be NFR.

To reduce possible confusion and misinterpretation, the terms FR and NFR from the WP14 point of view are prefixed with SWIM-TI.

Appendix D NFR Identification

D.1 Introduction

This appendix provides a set of tables that can serve as a checklist to support the structuring as well assessment of NFR requirements for SWIM Profiles

According the ISO 25010 classification Characteristics contain Sub-Characteristics which possibly contain measurable Properties. These Properties have been named NFR.

As some Properties are strongly linked they have been grouped and linked to a same NFR. The subsets #1, #2 and #3 each represent a measurable Property that is strongly linked with the other measurable Properties of the same NFR.

For a particular NFR there may be more than one measure. There are several ways to present this.

In order to keep all measures related to a particular NFR together for each listed NFR (one per row) in the tables below, measures have been spread over distinct columns when they each highlight a different but related aspect of the same NFR.

These columns are called Subset #1, Subset #2 and Subset #3 for reasons of traceability. There are no semantics associated with the numbering other than providing a unique identification within a row.

The numbering #1, #2 and #3 has no other meaning than to be able to identify each of these Properties in combination with the ID of the NFR.

D.2 Legend

This section provides explanations for helping understanding the NFR descriptions given from section D.3 to D.8.

D.2.1 Shared terminology

This section provides explanations on terms specific to all NFRs' descriptions.

D.2.1.1 RR, PS

RR = Request Reply

PS = Publish/Subscribe

D.2.1.2 Guaranteed | Not guaranteed

The qualification guaranteed is used for a series of NFRs. The reason is to make a distinction between measures that are targeted under normal (i.e. usual) circumstances only and measures that apply also under exceptional circumstances (e.g. machine crash, reconfiguration, upgrades, physical calamities, HR depletion). The exceptional circumstances do not include Full load.

D.2.1.3 Full load | Unknown load

The qualification “full load” is used for a series of NFRs. The reason is to make a distinction between measures that are targeted to apply under “normal load” or “unknown load” only and measures that apply also under a “full load” that has been explicitly documented.

D.2.1.4 As is

The qualification “as is” is used for a series of NFRs. This value indicates that the quality of the service as it is at the time of use will be accepted provided there is a commitment to provide a best effort.

D.2.1.5 Scalable number/size

The measure with description “scalable number” or “scalable size” is used for a series of NFRs. This value is always linked with the sub-characteristic Capacity and a “number” or “size”. The “number” or “size” measure reflects the capacity effectively required. The “scalable number” reflects the capacity that can potentially be provided by the solution without having to change the architecture or design of the solution.

D.2.1.6 Single Node | System/Distributed System

Depending on the context, measures are defined for a Single Node or for the System/Distributed System (in the naming of NFRs, System and Distributed System are used interchangeably). The measures defined for a System/Distributed System are motivated by the fact that the requirement of some NFRs is at the level of all interoperating Single Nodes rather than at a Single Node.

D.2.1.7 Multipurpose key | specific key

A single key - e.g. a private key of a public/private key pair used in the context of certificates - can be reused to perform authentication, encryption and signing at various levels. As such reuse increases the risk of the private key being compromised, in some contexts – e.g. legal – it may be desirable to use a specific key for the signing at message level that is not reused for anything else. The drawback is the increase of the number of private keys to manage.

D.2.1.8 PEP | PAP

PEP = Policy Enforcement Point

PAP = Policy Administration Point

D.2.1.9 No replay

This qualification indicates protection by a mechanism that detects replay of a captured message.

D.2.1.10 <Not available>

The qualification <Not available> indicates that the NFR measure is applicable but no value has been specified or the value is currently unknown.

This qualification is generic and can be used as a value for any measure.

D.2.1.11 <Not applicable>

The qualification <Not applicable> indicates that the NFR measure is applicable within the scope of SWIM TI but is meaningless in the current context.

This qualification is generic and can be used as a value for any measure.

D.2.1.12 <Not relevant>

The qualification <Not relevant> indicates that the NFR measure is outside the scope of SWIM TI.

This qualification is generic and can be used as a value for any measure.

D.2.1.13 <X>

The qualification <X> (“Don’t care”) indicates that the NFR measure is applicable within the scope of SWIM TI but that any value is acceptable without being limited by an external constraint.

This qualification is generic and can be used as a value for any measure.

D.2.2 Specific NFRs

This section provides explanations on terms specific to particular NFRs’ description.

D.2.2.1 WP_CPT_210

Whilst the address of the service end-point mostly needs discovery via a registry, typically a set of techniques exist to discover WSDL of an application service on the service end-point.

D.2.2.2 WP_REL_001

The depth and breadth of the testing process reflect in an essential manner the maturity of the reliability. The measurements of the testing process target to indicate:

- the degree of fault density and the extent to which the product is free from failure despite the presence of faults in the product
- the degree of effective interoperability of the product.

There are 3 subsets of measurements:

- The required presence or not of evidence for verification and validation of the end product for the intended use.
    - For verification, as in "ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes", confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
    - For validation, as in "ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes", confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

- The required presence or not of an independent verification and validation of the end product for the intended use
    - As defined in "ISO/IEC 24765 Systems and Software Engineering -- Vocabulary": V&V performed by an organization that is technically, managerially and financially independent of the development organization
- The scope of testing of the interoperability standards
    - None or Conformance and/or Interoperability

For the definition of the terms Conformance and Interoperability testing refer to http://en.wikipedia.org/wiki/Conformance_testing and http://www.itu.int/net/ITU-T/interop/default.aspx.

D.2.2.3 WP_REL_002

The first subset indicates the requirement of some form of attestation by an authority (can be self) of conformity of the product to regulatory, technical and safety requirements and/or standards.

The second subset identifies the attestation(s). Examples are a CMMI level and a SWAL level.

D.2.2.4 WP_REL_006

This measure could act as a potential abstraction to some extent for the other WP_REL_0* measures but no concrete specifications have been found for any of the Step 1 profiles.

D.2.2.5 WP_REL_102, WP_REL_103

Continuous operations reflect the extent to which the service must be maintained while performing interventions such as patching, reconfiguration and restart.

D.2.2.6 WP_REL_002

Formal certification process means that a documented process exists and it is mandatory for all stakeholders to conform to this process in order to be able to participate in the service functionality as a consumer and/or as a provider.

D.2.2.7 WP_REL_104

Content based indicates that the overload protection is differentiated on content criteria such as the identity of the requester, the type of request or specific content in the request

D.2.2.8 WP_REL_301

The relevance of this measure depends on the profile. In some profiles, little or no data is kept at the level of the TI. Conversely a data-centric middleware such as DDS logically keeps a database within the middleware.

RTO stands for Recovery Time Objective and RPO stands for Recovery Point Objective.

Specifications for WP_REL_302 have been found in the B2B EAD profile amongst the Step 1 profiles. In such case WP_REL_301 could be useful to estimate an order of magnitude for WP_REL_302.

D.2.2.9 WP_SEC_102

Hardened means that all functionality that is not strictly necessary has been explicitly removed and/or disabled.

D.2.2.10 WP_SEC_412

The identity with which the service endpoint is accessed and controlled may not be the same as the one originally presented by the consumer. In such case either the identity of a set of consumers is mapped to a single shared identity or the identity of each consumer is mapped 1-1 to another identity.

D.2.2.11 WP_SEC_413

This NFR determines which identity is propagated into the application service in case the application service needs to know an identity. The identity can come from the authentication at the level of network, transport or message. The source of the identity for the application service can also be present in the message in a manner that is different from the authentication performed at the message level protocol: it can come from the consumer or be injected by the SWIM TI. Another manner way for the application service to know about the identity is through a specific context that is fed by the SWIM TI.

D.2.2.12 WP_MNT_403 and WP_MNT_404

The NFRs describe the availability of means to perform tests and validation of evolutions from the perspective of the provider (WP_MNT_403) as well as from the perspective of the consumer (WP_MNT_404).

These means consist of a full or partial copy of the operational SWIM TI. These means exist on a permanent base or on ad-hoc base.

For an asymmetric type of profile the means for both NFRs are located at the side of the provider.

D.3 Performance efficiency

D.3.1 Network related

Performance efficiency			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_PRF_004	**Time-behaviour**	Maximum network latency	<= time | as is	[guaranteed]	[under full load]
WP_PRF_005	**Time-behaviour**	Jitter on network latency	Low | as is	[guaranteed]	[under full load]
WP_PRF_210	**Capacity**	Minimum network throughput rate	Size/time | as is	Scalable Size/time	[guaranteed], [under full load]

Table 7 Performance Efficiency NFRs (Network related)

D.3.2 SWIM TI related

Performance efficiency			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_PRF_001	**Time-behaviour**	Response[17] time RR (Application + TI + Network)	Time for percentage	[guaranteed]	[under full load]
WP_PRF_002	**Time-behaviour**	Distribution time PS (Application + TI + Network)	Time for percentage	[guaranteed]	[under full load]

[17] Here, Response time corresponds to the time measured from the consumer's request issuance to the provider's response reception.

Performance efficiency			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_PRF_003	**Time-behaviour**	Processing time in TI (if not available derived from WP_PRF_001 and WP_PRF_002)	Time for percentage	[guaranteed]	[under full load]
WP_PRF_201	**Capacity**	Maximum number of concurrent consumers per service end point	Number	Scalable Number	
WP_PRF_202	**Capacity**	Maximum number of concurrent publishers and subscribers per service end point	Number	Scalable Number	
WP_PRF_203	**Capacity**	Maximum number of concurrent publishers and subscribers in the distributed system	Number	Scalable Number	
WP_PRF_204	**Capacity**	Maximum number of sessions per service end point	Number	Scalable Number	
WP_PRF_205	**Capacity**	Maximum number of messages per second per service end point	Number per period	Scalable Number per period	
WP_PRF_206	**Capacity**	Maximum message size	Size	Scalable Size	
WP_PRF_207	**Capacity**	Maximum message volume/s in the distributed system (i.e. the SWIM network)	Size per period	Scalable Size per period	
WP_PRF_208	**Capacity**	Maximum storage for persistent messages/durable subscribers per TI	Size	Scalable Size	
WP_PRF_209	**Capacity**	Maximum storage for persistent auditing and logging per TI	Size	Scalable Size	

Table 8 Performance Efficiency NFRs (SWIM TI related)

D.4 Compatibility

Compatibility	NFR/Quality measures

ID	Compatibility Sub-characteristic	NFR Description (ISO 25010 Quality property)	Subset #1	Subset #2	Subset #3
WP_CPT_001	Co-existence	Software (e.g. OS, middleware) sharing	Allowed | Limited Allowed | Not allowed		
WP_CPT_002	Co-existence	Hardware sharing	Allowed | Limited Allowed | Not allowed		
WP_CPT_003	Co-existence	Network sharing	Allowed | Limited Allowed | Not allowed		
WP_CPT_101	Interoperability	Topology	Peer | Asymmetrical		
WP_CPT_102	Interoperability	Which service consumers for application service			
WP_CPT_103	Interoperability	Which identity providers (IP)/repositories allowed for application service	Only local | <list of directly/indirectly trusted IP>		
WP_CPT_202	Interoperability	Which PAP for authorization PEP on application service	Only local | <list of authoritative PAP >		
WP_CPT_203	Interoperability	Which service consumers for security service	Only local | <list of authorized identities>		
WP_CPT_204	Interoperability	Which identity providers (IP)/repositories allowed for security service	Only local | <list of directly/indirectly trusted IP>		
WP_CPT_205	Interoperability	Which PAP for authorization PEP on security service	Only local | <list of authoritative PAP >		
WP_CPT_206	Interoperability	Which service consumers for supervision service	Only local | <list of authorized identities>		
WP_CPT_207	Interoperability	Which identity providers/repository allowed for supervision service	Only local | <list of directly/indirectly trusted IP>		
WP_CPT_208	Interoperability	Which PAP for authorization PEP on supervision service	Only local | <list of authoritative PAP >		
WP_CPT_209	Interoperability	Application service virtualisation	Yes | No		
WP_CPT_210	Interoperabilit	Application service discovery	[registry only]		

Compatibility			NFR/Quality measures		
ID	*Compatibility Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
	y				

Table 9 Compatibility NFR

D.5 Reliability

Reliability			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_REL_001	**Maturity**	Maturity of test process	[No] Verification evidence [No] Validation evidence	[No] V&V by independent organization	None|{[Conformance] [Interoperability]}
WP_REL_002	**Maturity**	Formal certification process	Yes | No	<list>	
WP_REL_003	**Maturity**	Disturbance injection in tests	[restart OS/process]	[resource depletion]	[corruption of OS/Middleware]
WP_REL_004	**Maturity**	Stress tests	Yes | No		
WP_REL_005	**Maturity**	Penetration tests	Yes | No	Self | Certified	Frequency
WP_REL_006	**Maturity**	Mean time between failure	Model | Measure | Unknown	Number per Duration	
WP_REL_101	**Availability**	Single Node Availability	>=99,999 | >=99,99 | >=99,9 | undefined	{includes|excludes} planned outage	
WP_REL_102	**Availability**	Single Node Continuous operations	Yes | Limited | No		
WP_REL_103	**Availability**	Distributed System Continuous operations	Yes | No		
WP_REL_104	**Availability**	Overload Protection	Yes | No	[Content based]	
WP_REL_201	**Fault**	Hardware redundancy and/or Cluster	[HW redundancy]	[Cluster]	

Reliability			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
	Tolerance				
WP_REL_202	**Fault Tolerance**	Virtual service with failover rerouting	Yes | No		
WP_REL_301	**Recoverability**	Data Recovery (cross-cutting concern as not all in TI).	RTO measure of time	RPO measure of time	[guaranteed]
WP_REL_302	**Recoverability**	TI Recovery. If not provided to be derived from WP_REL_301	Measure of time		[guaranteed]
WP_REL_303	**Recoverability**	message delivery	Message loss and/or duplication | Guaranteed exactly once | Guaranteed but possible duplication	[keep order]	[known and managed]

Table 10 Reliability NFR

D.6 Security

D.6.1 Network related

Security			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_SEC_001	**Confidentiality**	RR Encryption Network layer	Yes | No	{multipurpose key|specific key}	
WP_SEC_004	**Confidentiality**	PS Encryption Network layer	Yes | No	{multipurpose key|specific key}	
WP_SEC_402	**Authenticity**	RR Authentication Network layer	Yes |	{multipurpose	[no-replay] [online

Security			NFR/Quality measures		
ID	**Sub-characteristic**	**NFR Description (ISO 25010 Quality property)**	**Subset #1**	**Subset #2**	**Subset #3**
			No	key|specific key} {unilateral|mutual}	check Identity Provider]
WP_SEC_405	**Authenticity**	PS Authentication Network layer	Yes | No	{multipurpose key|specific key} {unilateral|mutual}	[no-replay] [online check Identity Provider]

Table 11 Security NFRs (Network related)

D.6.2 SWIM TI related

Security			NFR/Quality measures		
ID	**Sub-characteristic**	**NFR Description (ISO 25010 Quality property)**	**Subset #1**	**Subset #2**	**Subset #3**
WP_SEC_002	**Confidentiality**	RR Encryption Transport layer	Yes | No	{multipurpose key|specific key}	
WP_SEC_003	**Confidentiality**	RR Encryption Message layer	Yes | No	{multipurpose key|specific key}	
WP_SEC_005	**Confidentiality**	PS Encryption Transport layer	Yes | No	{multipurpose key|specific key}	
WP_SEC_006	**Confidentiality**	PS Encryption Message layer	Yes | No	{multipurpose key|specific key}	
WP_SEC_101	**Integrity**	Internet facing	Yes | Yes with limited functionality | No		
WP_SEC_102	**Integrity**	Immunity (resistant to attack)	unknown|none|state of the art	[hardened]	[tunnel]
WP_SEC_103	**Integrity**	Checksum	Yes | No		
WP_SEC_104	**Integrity**	RR Digital Signature Transport layer			
WP_SEC_105	**Integrity**	RR Digital Signature Message layer			

Security			NFR/Quality measures		
ID	**Sub-characteristic**	**NFR Description (ISO 25010 Quality property)**	**Subset #1**	**Subset #2**	**Subset #3**
WP_SEC_106	**Integrity**	Authorization PEP in TI for application service (the service may perform authorization itself)	Yes | No		
WP_SEC_107	**Integrity**	Authorization PEP in TI for security service	Yes | No		
WP_SEC_108	**Integrity**	Authorization PEP in TI for supervision service	Yes | No		
WP_SEC_109	**Integrity**	PS Digital Signature Transport layer			
WP_SEC_110	**Integrity**	PS Digital Signature Message layer			
WP_SEC_201	**Non-repudiability**	List of actions and attributes for which proof is needed	List		
WP_SEC_202	**Non-repudiability**	Retention time of proof	Time		
WP_SEC_301	**Accountability**	Auditing PEP in TI for application service (the service may perform auditing itself)	Yes | No	[actions and attributes that need to be recorded]	
WP_SEC_302	**Accountability**	Auditing PEP in TI for security service	Yes | No	[actions and attributes that need to be recorded]	
WP_SEC_303	**Accountability**	Auditing PEP in TI for supervision service	Yes | No	[actions and attributes that need to be recorded]	
WP_SEC_401	**Authenticity**	Anonymous access to application service allowed	Yes | No		
WP_SEC_403	**Authenticity**	RR Authentication Transport layer	Yes | No	{multipurpose key|specific key} {unilateral|mutual}	[no-replay] [online check Identity Provider]
WP_SEC_404	**Authenticity**	RR Authentication Message layer	Yes | No	{multipurpose key|specific key} {unilateral|mutual}	[no-replay] [online check Identity Provider]
WP_SEC_406	**Authenticity**	PS Authentication Transport layer	Yes | No	{multipurpose key|specific key} {unilateral|mutual}	[no-replay] [online check Identity Provider]

Security			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_SEC_407	**Authenticity**	PS Authentication Message layer	Yes | No	{multipurpose key|specific key} {unilateral|mutual}	[no-replay] [online check Identity Provider]
WP_SEC_408	**Authenticity**	Authentication PEP in TI for application service (the service may perform authentication itself)	Yes | No		
WP_SEC_409	**Authenticity**	Authentication PEP in TI for security service	Yes | No		
WP_SEC_410	**Authenticity**	Authentication PEP in TI for supervision service	Yes | No		
WP_SEC_411	**Authenticity**	Application service needs to know identity	Yes | No		
WP_SEC_412	**Authenticity**	Identity mapping at application service endpoint	Mapping to shared identity | Token transformation | No		
WP_SEC_413	**Authenticity**	Identity propagation to application service	Same as {network|transport|message} service endpoint | Different from service endpoint original inside message | Different from service endpoint inject/rewrite inside message | Service has access to context | Service is unaware		

Table 12 Security NFRs (SWIM TI related)

D.7 Maintainability

Maintainability			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_MNT_201	**Analysability**	Complexity impact analysis and trouble shooting Single node	High level of specific and certified expertise | Common IT		]
WP_MNT_202	**Analysability**	Complexity impact analysis and trouble shooting Distributed System	High (many to many) | Medium (many to one | one to many) | Low (one to one)		
WP_MNT_301	**Modifiability**	Frequency of scheduled release	Number of major releases per period	Number of minor releases per period	Number of patches per period
WP_MNT_302	**Modifiability**	Decision making on changes	Centralised | Distributed		
WP_MNT_401	**Testability**	Combinatorial complexity of the distributed system	High (many to many) | Medium (many to one | one to many) | Low (one to one)		
WP_MNT_402	**Testability**	Responsibility	Centralised | Distributed		
WP_MNT_403	**Testability**	User acceptance provider	Full clone of production | subset of production	Permanent | Ad hoc	
WP_MNT_404	**Testability**	User acceptance consumer	Full clone of production | subset of production	Permanent | Ad hoc	

Table 13 Maintainability NFR

D.8 Portability

Portability			NFR/Quality measures		
ID	*Sub-characteristic*	*NFR Description (ISO 25010 Quality property)*	*Subset #1*	*Subset #2*	*Subset #3*
WP_PRT_001	**Adaptability**	Different Hardware/software environment	High level of specific and certified expertise | Common IT		]
WP_PRT_101	**Installability**	Competence level	High level of specific and certified expertise | Common IT		
WP_PRT_201	**Replaceability**	By another COTS product	Replaceable without restrictions | Replaceable with local adaptations | Replaceable with cascading effect	Standards based only | Partially proprietary | Entirely proprietary	
WP_PRT_202	**Replaceability**	1 or more FOSS (Free Open Source Software) alternatives exist	Yes | No		

Table 14 Portability

END OF DOCUMENT-