International Civil Aviation Organization

The Eighth Meeting of System Wide Information Management Task Force (SWIM TF/8)

Bangkok, Thailand, 08 – 10 November 2023

Agenda Item 2: Development of Asia/Pacific Regional SWIM Implementation Guidance

Updates of APAC SWIM Technical Infrastructure Profiles

(Presented by JAPAN/ENRI)

SUMMARY

This paper presents the update of the draft version of APAC SWIM Technical Infrastructure Profiles document according to the review comments provided by other SWIM Task Force (TF) task groups and members. The paper highlights the main modifications implemented from the previous draft version presented at SWIM TF/7.

1. INTRODUCTION

1.1 As a main content of Asia/Pacific Regional SWIM Implementation Guidance, at the seventh meeting of SWIM TF (SWIM TF/7), the draft version of APAC SWIM Technical Infrastructure Profiles that contains basic requirements for the implementation of SWIM TI, optional system design models for the integration of the CRV, and common technology standards for the specification of interface bindings to eliminate technical barriers from the realization of regional SWIM was presented.

1.2 Moreover, due to the limited capabilities of CRV and varied operational requirements for information services, as an optional solution, the user-based access model to achieve technical interoperability for regional SWIM implementation during the transition period was clarified.

1.3 This working paper presents an updated version of APAC SWIM Technical Infrastructure Profiles provided as Appendix A for Asia/Pacific Regional SWIM Implementation Guidance. It highlights the main modification and added Appendixes implemented from the previous draft version.

2. DISCUSSION

2.1 According to received comments and suggestions from other members, following modifications and additions are implemented.

- As TCP/IP is the underlying protocol for all interface types, the description of TCP/IP was moved to the section of Network Bindings. Chapter 3 - STANDARDS FOR INTERFACE BINDINGS was restructured.

- Appendix A - STRUCTURE OF AMHS/SWIM GATEWAY was added to provide system structure and functional building blocks of AMHS/SWIM Gateway.

- Appendix B - ARCHITECTURE OF SDCM was added to provide high-level architecture and package diagram of Service Description Conceptual Model (SDCM).

- Appendix C - EXAPLE OF SWIM MESSAGE HEADERS was added to provide some examples of message headers for FIXM, AIXM and IWXXM messages to explain message capabilities for achieving interoperability between different SWIM TIs in separate IP network segments. Moreover, examples of message headers for surveillance data were discussed.

2.2 Further revisions and clarifications will be considered according to the requirement for the development of Asia/Pacific Regional SWIM Implementation Guidance.

3. FURTHER WORK

3.1 To support the Joint Event of SWIM over CRV Demonstration and Surveillance Data Sharing in SWIM Trial, the detailed approaches have been discussed by the SWIM Implementation Pioneer Group. Chapter 2 - SYSTEM DESIGN will be updated according to these discussions and practical implementations.

3.2 For the Structure of AMHS/SWIM Gateway, the updates will be considered according the discussion of related ICAO panels and working groups. For the Architecture of SDCM, as FAA has proposed the updated draft version of SDCM, the update is required after the revision of the new SDCM draft version.

3.3 As message exchange is a key factor to achieve interoperability, the common definition of message types and metadata for flight, aeronautical, meteorological and surveillance information sharing between different SWIM TIs is required for regional SWIM construction. The examples of message exchange for different use cases will be included based on joint demonstrations and trials.

4. ACTION BY THE MEETING

4.1 The SWIM TF/8 is invited to:

a) Review and provide feedback to the updated draft version of APAC SWIM Technical Infrastructure Profiles (Appendix A to this working paper);

b) Review and discuss the proposed modifications and additions provided in this working paper;

c) Agree to provide this document to the related Task groups under SWIM TF and other APANPIRG Working Groups/Task Forces for further deliberation; and

d) Discuss any relevant matters as appropriate.

– – – – – – – – – – – – – –

APAC SWIM Technical Infrastructure Profiles - Draft Version 0.2

November 2023

Record of Revisions

Date	Revision	Submitter
May 2023	Version 0.1 – Initial Draft for SWIM TF/7	Xiaodong Lu, JAPAN/ENRI
Nov. 2023	Version 0.2 – Revised Initial Draft for SWIM TF/8 - Restructure Chapter 3 - Add Appendix A, B and C	Xiaodong Lu, JAPAN/ENRI

Table of Contents

1. INTRODUCTION

1.1 Purpose

In order to achieve technical interoperability between different implementations, it is essential that systems use standardised interfaces and have technical infrastructure capabilities to enable reliable, secure and efficient exchange of ATM related information. It is expected that these standards enable to eliminate technical barriers from the realization of regional SWIM.

This document contains basic requirements for the implementation of SWIM Technical Infrastructure (TI), optional system design models for the integration of the Common arRonautical Virtual Private Network (CRV), and common Information and Communication Technology (ICT) standards for the specification of interface bindings to implement the regional SWIM during the transition period.

1.2 Scopes

This document focuses on the following scopes for SWIM TI implementation by considering the integration of CRV to achieve technical interoperability during the transition period in the APAC region.

- SWIM TI system design
- SWIM TI interface bindings
- SWIM TI capabilities

1.3 Prerequisite for Implementation

The main objective of SWIM is not only to enable seamless information sharing among the multiple stakeholders in the ATM domain but also to achieve interoperability and harmonization of global operation in the air transportation field. Therefore, as the backbone for ATM modernization by delivering the right information to the right decision-maker at the right time and location, the high-capacity IP-based network is required. Moreover, the implementation of SWIM has also opened the door for a variety of new, non-traditional aviation information sharing partners, seeking to introduce innovative solutions using data and information that became available after applying SWIM. Therefore, both operational interoperability and applicational flexibility should be considered for the development and implementation of regional SWIM. The required indicators for IP-based network that should be considered to construct the SWIM TI are shown in Table 1.

Table 1. SWIM TI Requirements

Indicator	SWIM TI Requirement
Performance	High-speed IP network connection with large bandwidth and low latency for various kinds and a large mass of information exchange among SWIM-enabled systems
Accessibility	Open and easy connected platform not only for traditional aviation partners but also for multiple non-aviation enterprises for the initial development of SWIM

Connectivity	Cross-border network connections not only for other SWIM-enabled systems in the APAC region but also to other SWIM platforms that have been deployed in other ICAO regions
Cost	Reduced cost for conventional message exchange, and low cost or free of cost for SWIM information exchange and sharing

1.4 Principles

The SWIM TI contributes to achieving the SWIM benefits described in the Manual on SWIM (Doc 10039), by respecting the following principles shown in Table 2.

Table 2. SWIM TI Principles

Principle	Description
Managed technical diversity	Technical diversity is managed to minimize the significant costs to maintain expertise while allowing flexibility to accommodate new technologies and select technologies that best meet ATM needs.
Standards based TI	SWIM TI implementation is based on open standards that promote technical interoperability.
Established ICT standards	SWIM TI implementation is based on widely deployed and supported ICT standards that enable economical and efficient information services implementation and operation.
Modularity	SWIM TI implementation is modular, enabling progressive deployment of SWIM TI functional capabilities and bindings, which will allow a fit for purpose, flexible and agile implementation and evolution.
Platform independent interfaces	Interfaces between systems do not create dependencies imposed by implementation platforms, such as operating system or programming language.

1.5 Structure

Chapter 1 introduces the purpose and scope of this document, the requirements and principles for regional SWIM TI implementation.

Chapter 2 provides a high-level architecture and several optional system design models to construct the SWIM TI taking into account the integration of CRV for achieving interoperability.

Chapter 3 specifies common ICT standards for Interface Bindings, providing specifications for the implementation of service, network and infrastructure interfaces.

Chapter 4 specifies SWIM TI Capabilities, providing functional and non-functional requirements for the implementation of regional SWIM TI to ensure the reliable, secure and efficient information exchange between different stakeholders.

Appendix A provides system structure and functional building blocks of AMHS/SWIM Gateway.

Appendix B provides high-level architecture and package diagram of Service Description Conceptual Model (SDCM).

Appendix C provides some examples of message headers for FIXM, AIXM and IWXXM messages to explain message capabilities for achieving interoperability between different SWIM TIs in separate IP network segments. Moreover, examples of message headers for surveillance data are discussed.

1.6 Maintenance

This document has been developed by the Task 2 group under the APAC SWIM TF. It will be updated and maintained by the APAC SWIM TF. It is accessible at SWIM Repositories of ICAO APAC SWIM Secure Portal.

1.7 References

[1] Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, ICAO Doc 9896.

[2] Manual on System Wide Information Management, ICAO Doc 10039.

[3] Procedures for Air Navigation Services – Information Management (PANS-IM), Final Draft, ICAO Doc 100xx.

[4] EUROCONTROL Specification for SWIM Technical Infrastructure, EUROCONTROL-SPEC-170.

[5] Service Description Conceptual Model (SDCM), Version 3.0.0 DRAFT, FAA, February 2023.

[6] AMHS/SWIM Gateway Specification, Version 1.0 Draft, AMHS/SWIM Gateway Study Group (SWAMWAY SG), 2022.

2. SYSTEM DESIGN

2.1 Requirements

During the transition to a global SWIM environment, legacy systems and SWIM-enabled systems will have to coexist for a longer period of time. To assure the interoperability, SWIM-enabled system is required to implement information services not only according to SWIM but also supporting the legacy systems. This is especially important during the transition period, because a legacy system may not have the capability to adapt to the new approaches introduced by SWIM. As the legacy AFTN/AMHS is used by nearly all member states, it is necessary for the SWIM TI to support the message transport between the SWIM-enabled systems and AFTN/AMHS using legacy systems.

In the APAC region, a CRV that is IP-based VPN using a private commercial network to provide service for the exchange of AMHS data and potentially other types of data has been constructed. Additionally, to facilitate the transition from AMHS to SWIM, the AMHS/SWIM Gateway Specification has been proposed and discussed by other working groups. To clarify the appropriate approach for regional SWIM implementation while considering these requirements, the joint meeting between the CRV OG and SWIM TF was held, and several optional approaches were discussed.

Due to the different levels of operational needs and limited capability of current CRV, different options can be contemplated for the transition period regarding interoperability. Some member states and third-party SWIM service providers have developed some information services on their local SWIM-enabled systems that cannot directly connect to the CRV at current stage. In addition, to support cost-effective and efficient utilization, some non-safety critical information services, such as less-sensitive meteorological information services, have been accessible on the Internet. Therefore, during the transition period, the different design models of the SWIM TI are required for the different services and implementation levels.

2.2 Service Description

From the perspective viewpoint of Service Oriented Architecture (SOA), the TI is one of SWIM services that provide the reliable, secure and efficient information exchange service to SWIM users. As the service description is integral to establishing interoperability among SOA components and critical to supporting various aspects of SOA governance, a common and consistent service description model is also required for SWIM TI. The Service Description Conceptual Model (SDCM) developed by the FAA SWIM Program is an appropriate template and can consist of the application of basic principles, common standards, methodologies, and best practices for regional SWIM TI implementation. For example, as shown in Table 3, the elements included in the profile package of SDCM should be considered for each SWIM TI service provider.

Table 3. Profile Package of SDCM Version 3.0.0

Name	Definition
Provider	An organizational entity responsible for making the service available.
Consumer	An organizational entity that uses the service.
Function	A type of activity describing the functionality of a service.
Security Mechanism	A process (or a device incorporating such a process) that is used by or within a service to prevent unauthorized or accidental access, change, destruction, or loss of data.

Policy	A statement that defines constraints on the behavior of a managed resource, a user or an organization.
Quality of Service	A parameter that specifies and measures the value of the provided service.
Geographical Extent	A specified geographic area to which the service applies.
Environmental Constraint	A characteristic of the environment or larger system within which the service operates.

2.3 Interface Bindings

The SWIM TI enables the implementation of interfaces between systems, providing technical capabilities for secure, high performing and reliable information exchange. Based on the functional position of SWIM TI, not only network bindings and service bindings but also infrastructure bindings are required to achieve interoperability between different internal and external infrastructure systems.

- Network Bindings: Specify what is expected by the SWIM TI to communicate over the IP network, including protocols from the network and transport layers;

- Service Bindings: Specify the service interface technical interoperability, including protocols to interface with the ATM applications;

- Infrastructure Bindings: Specify the interface used by a SWIM TI to communicate with other infrastructure systems, including protocols for communication with internal and external services.

2.4 Architecture

The regional SWIM will be progressively implemented by the integration of different SWIM-enabled systems and aligned with the implementation of the services it supports. Additionally, to facilitate the transition from AMHS to SWIM, the AMHS/SWIM Gateway Specification has been proposed and discussed by other working groups. To clarify the appropriate approach for regional SWIM implementation while considering these requirements, the CRV-based interoperable architecture is required for regional SWIM implementation during the transition period.

According to different sophistication and implementation levels, Figure 1 shows an interoperable architecture, which is a possible approach for CRV based regional SWIM implementation to satisfy information exchange between legacy and SWIM-enabled applications. Some stakeholders (ANSPs, ASPs, AUs or third-party partners) will have the capacity to become SWIM TI service providers by establishing common agreements and creating a collaborative environment at the regional level or between different regions. In this approach, it is important for all SWIM TI service providers to agree on using a common set of standards to ensure information exchange between different systems. The Local Router provides the function of connectivity between CRV and SWIM TI for local legacy systems and SWIM-enabled systems. SWIM TI service providers may be connected by CRV or other secure connection methods on IP-based network. As a SWIM TI service provider, it will be able to provide the reliable, secure and efficient information exchange service to SWIM-enabled ASPs and AUs.

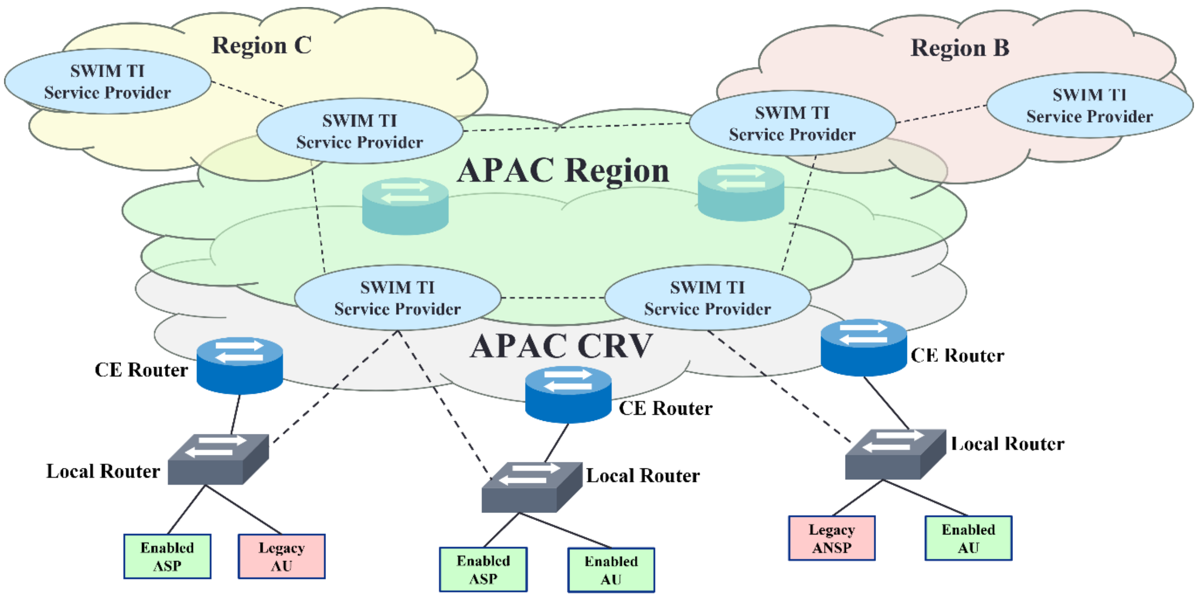

Figure 1. Interoperable Architecture

2.5 Design Models

According to the discussion of joint meetings between the CRV OG and SWIM TF, the implementation of the initial regional SWIM at the current stage can be accomplished through user-based access model and application-level integration. This approach ensures interoperability between the different SWIM-enabled systems developed by various stakeholders in different IP network segments.

Based on the availability of AMHS/SWIM Gateway and the infrastructure bindings between different systems, there are several connection ways to deal with a need of service consumers to access different services through AMHS, SWIM and the Internet. The following use cases are described for different requirements and capabilities.

2.5.1 Use Case 1

In this use case, as shown in Figure 2, due to the AMHS/SWIM Gateway and the infrastructure bindings are not available for the CRV-based SWIM TI, users must connect to each access point in separate IP network segments, such as AMHS, SWIM and the Internet using a broker or gateway. The SWIM-enabled ATM applications support users to transform messages and integrate information at the application level.

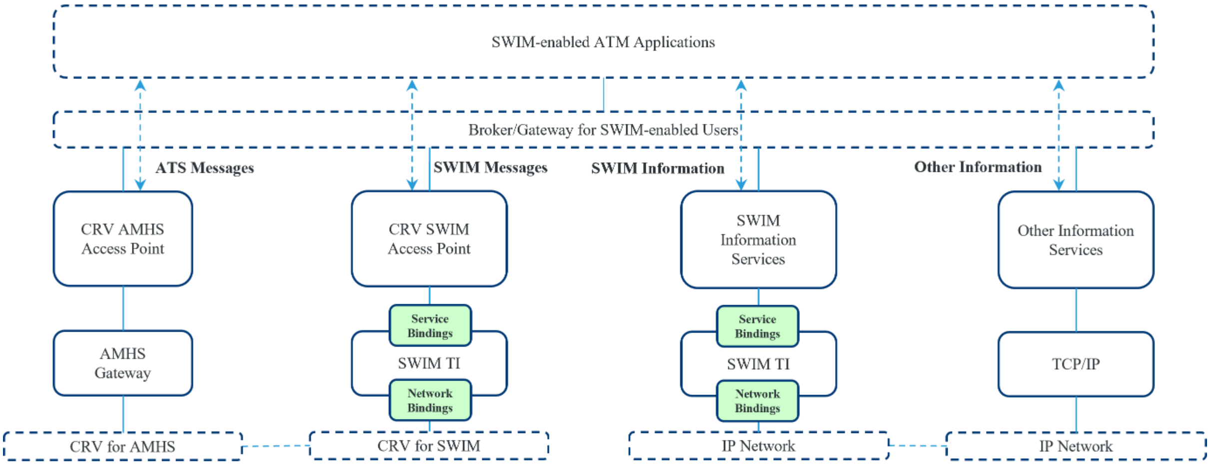

Figure 2. Use Case 1: Without AMHS/SWIM Gateway and Infrastructure Bindings

2.5.2 Use Case 2

The main difference between use case 2 (Figure 3) and use case 1 (Figure 2) is that infrastructure bindings are available between CRV-based SWIM TI and the user's local SWIM TI. This enables information exchange between different SWIM TIs in separate IP network segments when users connect to one SWIM access point. The SWIM-enabled ATM applications support users in message transformation and information integration at the application level.

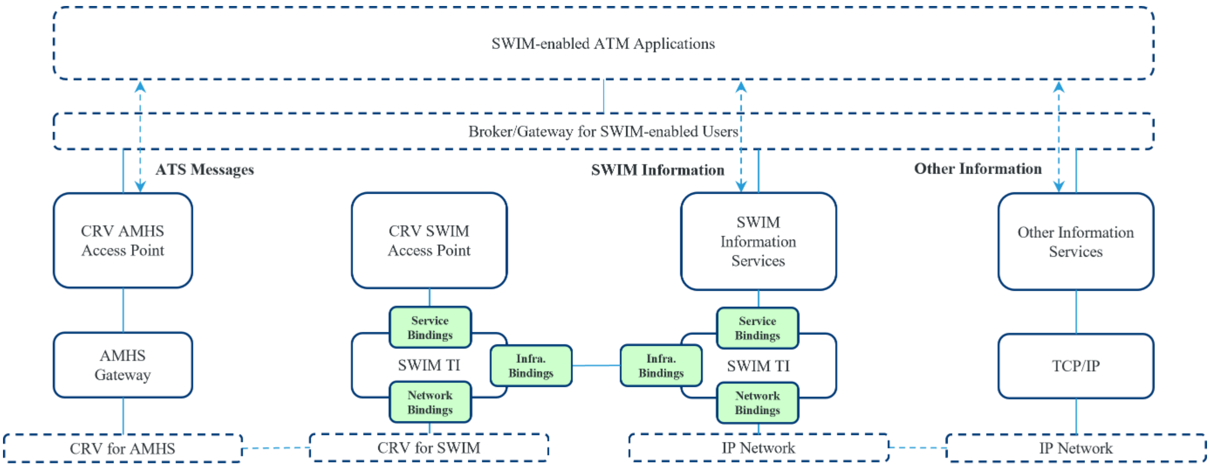

Figure 3. Use Case 2: With Infrastructure Bindings between SWIM TIs

2.5.3 Use Case 3

In this use case (Figure 4), as the AMHS/SWIM Gateway and the infrastructure bindings are available for the CRV-based SWIM TI, users would not need to connect to the CRV AMHS access point. The AMHS/SWIM Gateway will handle the exchange of information and the transformation of message between AMHS users and SWIM users. The SWIM-enabled ATM applications will be able to integrate SWIM information with other aviation-related information that is available on the Internet.

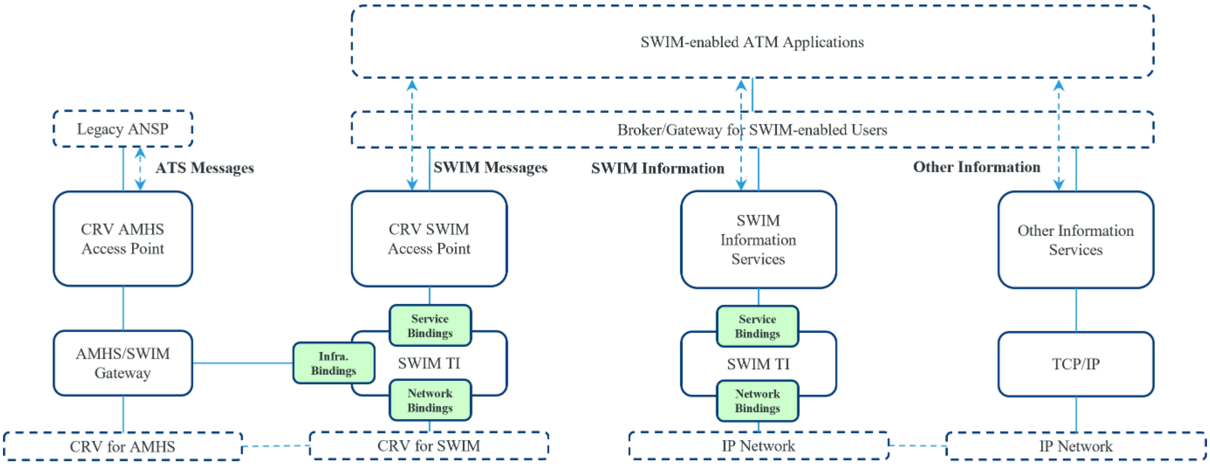

Figure 4. Use Case 3: With AMHS/SWIM Gateway and Infrastructure Bindings on CRV

2.5.4 Use Case 4

In the use case (Figure 5), as the infrastructure bindings are also available between different SWIM TIs in separate IP network segments, users only need to connect to one SWIM access point. The infrastructure bindings of SWIM TIs will cooperate with each other to achieve information exchange among SWIM users and support AMHS/SWIM Gateway to handle the massage exchange between AMHS users and SWIM users.

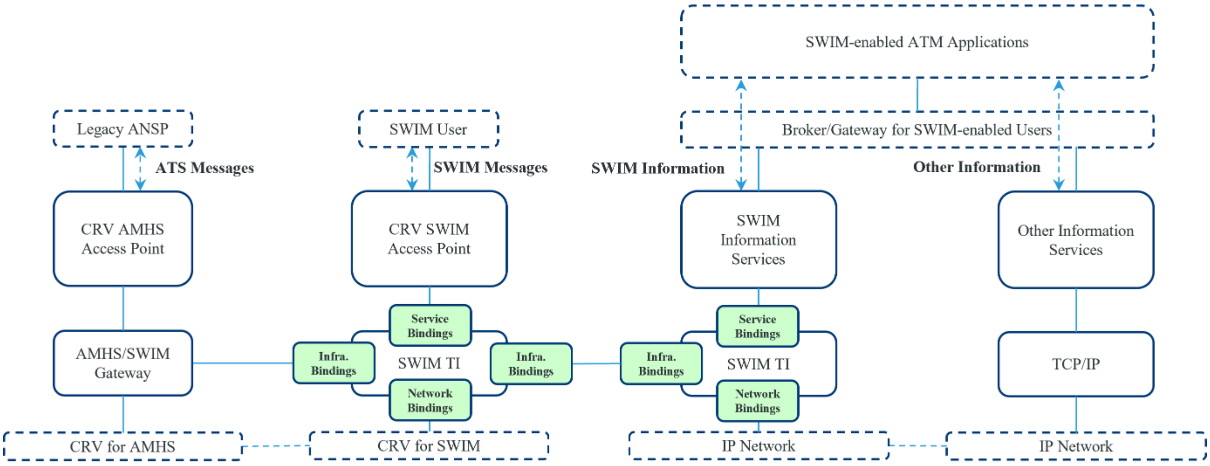

Figure 5. Use Case 4: With Infrastructure Bindings between Different Systems

To ensure interoperability, SWIM TI service providers should consider establishing common governance policies based on the trust framework discussed by ICAO TFP.

3. STANDARDS FOR INTERFACE BINDINGS

3.1 Introduction

The SWIM TI enables technical interoperability based on interface that use common ICT standards. The SWIM TI interface bindings specify the protocols for information exchange between systems. Interface bindings play a critical role in enabling technical interoperability in SWIM and are highlighted as specific TI components. This chapter specifies common technology standards for Interface Bindings, providing specifications for the implementation of service, network and infrastructure interfaces.

3.2 Network Bindings

As IP-based network connectivity is essential for SWIM TI, Table 4 makes reference to TCP/IP related technology standards required for supporting the following network bindings of SWIM TI.

- IPv4 Unicast
- IPv4 Secure Unicast
- IPv6 Unicast
- IPv6 Secure Unicast

Table 4. Standards and Specifications for TCP/IP

Standard and Specification	Description	Reference
IP (Internet Protocol)	This standard defines the format and behavior of the IPv4 protocol, which is used for transmitting packets of data over the internet.	IETF RFC 791
TCP (Transmission Control Protocol)	This standard defines the format and behavior of the TCP protocol, which is used to provide reliable, connection-oriented data transmission over the internet.	IETF RFC 793
Internet Standard Subnetting Procedure	This standard defines the procedures for subnetting IPv4 networks, which allows for more efficient use of IP addresses.	IETF RFC 950
ICMP (Internet Control Message Protocol)	This standard defines the format and behavior of the ICMP protocol, which is used for error reporting and diagnostic messages related to IPv4.	IETF RFC 792
Security Architecture for the Internet Protocol	This standard defines the overall architecture for IPsec, including the components and protocols used to provide security for IP traffic.	IETF RFC 2401
IPv6 (Internet Protocol, Version 6)	This standard defines the next generation of the IP protocol, which uses a larger address space and includes other improvements over IPv4.	IETF RFC 2460

Security Architecture for the Internet Protocol Version 6	This standard extends the IPsec security architecture to support IPv6.	IETF RFC 4301
Internet Standard, Requirements for Internet Hosts-Communication Layers	This standard describes the requirements for Internet hosts and communication protocols, such as requirements for TCP/IP protocol implementations, network interface cards, host software, and Internet applications.	IETF RFC 1122
Guidelines for Specifying the Use of IPsec Version 2	This document provides guidance to developers and administrators on how to specify the use of IPsec version 2 in different contexts, such as network architecture, service level agreements, and security policies.	IETF RFC 5406

3.3 Service and Infrastructure Bindings

Interface type is a classification of services based on the type of technological solution that they deploy. According to the requirement of service and infrastructure bindings, three interface types are defined to indicate the method by which the underlying capabilities of the service are accessed. TCP/IP is the underlying protocol for all interface types.

- Message-oriented: An interface that exposes service capabilities through creating, sending, receiving, and reading messages exchanged by distributed systems. AMQP is a common technology standard that supports this interface type.
- Resource-oriented: An interface that supports the Representational State Transfer (REST) architectural style of interactions, that is, manipulation of XML representations of Web resources using a uniform set of stateless operations, usually a set of HTTP methods.
- Method-oriented: An interface that exposes service capabilities through a set of operations. Technologies that support this interface type are Web Service framework (WS) and Open Geospatial Consortium (OGC) Web Common Services.

3.3.1 Standards for Message-oriented Interface

3.3.1.1 AMQP

The following table makes reference to AMQP related specifications required for supporting service and infrastructure bindings of SWIM TI.

Table 5. Standards and Specifications for AMQP

Standard and Specification	Description	Reference
AMQP (Advanced Message Queuing Protocol)	The latest version is AMQP 1.0, which includes a secure profile that uses TLS for message encryption and authentication. It defines the messaging protocol, message format, and message exchange patterns.	https://www.oasis-open.org/standards#amqpv1.0 ISO/IEC 19464:2014 Information technology - Advanced Message Queuing Protocol (AMQP) v1.0 specification
AMQP Management	This is a standard extension to AMQP that provides a way for administrators to manage AMQP-based messaging systems securely. It includes support for authentication, authorization, and encryption.	https://www.oasis-open.org/standards#amqpmanagementv1.0
AMQP WebSocket	This is an extension to AMQP that allows AMQP messages to be exchanged over WebSocket connections.	https://www.oasis-open.org/standards#amqpwebsocketv1.0
TLS (Transport Layer Security)	This is a security protocol that provides encryption, authentication, and integrity protection for network communications. It is commonly used as the underlying security protocol for AMQPS.	IETF RFC 5246
SASL (Simple Authentication and Security Layer)	This is a framework for authentication and authorization used in AMQP and other network protocols. It provides a standardized way for clients and servers to authenticate each other and to negotiate security parameters.	IETF RFC 4422

3.3.2 Standards for Resource-oriented Interface

3.3.2.1 RESTful API

The following table makes reference to RESTful API related standards and specifications required for supporting the service or infrastructure bindings of SWIM TI.

Table 6. Standards and Specifications for RESTful API

Standard and Specification	Description	Reference
HTTP (Hyper Text Transfer Protocol)	This is the primary protocol used for communication between clients and servers in RESTful APIs. It defines a set of request and response methods (e.g., GET, POST, PUT, DELETE), as well as rules for message framing and authentication.	IETF RFC 7230-7235
HTTPS (Hyper Text Transfer Protocol Secure)	This is a standard that provides secure communication over the internet. It is a combination of the standard HTTP protocol and the security protocol SSL/TLS (Secure Sockets Layer/Transport Layer Security).	IETF RFC 2818, RFC 5246, and RFC 7540
URI (Uniform Resource Identifier)	URIs are used to identify resources in RESTful APIs. They provide a consistent, standardized way to reference resources across different systems.	IETF RFC 3986
OAuth (Open Authorization)	This is a standard protocol for authentication and authorization, which is used to control access to resources in RESTful APIs. It defines a set of roles, grant types, and endpoints that enable third-party applications to access protected resources on behalf of resource owners.	IETF RFC 6749
JSON (JavaScript Object Notation)	It is a lightweight data format used in RESTful APIs to represent structured data. It is widely used because of its simplicity and flexibility.	IETF RFC 7159
XML (Extensible Markup Language)	It is a data format commonly used in RESTful APIs. It provides a more structured and standardized way to represent data than JSON.	https://www.w3.org/XML/
OpenAPI	This is the primary standard for defining RESTful APIs using the OpenAPI specification format. It defines a set of rules and guidelines for creating, documenting, and sharing RESTful APIs.	https://spec.openapis.org/

3.3.3 Standards for Method-oriented Interface

3.3.3.1 OGC WCS

The Open Geospatial Consortium (OGC) has developed a number of Web Common Service (WCS) standards that define services for accessing and manipulating geospatial data in a web environment, such as aeronautical information and meteorologic information. The following table makes reference to some of the key WCS standards and specifications required for supporting the service or infrastructure bindings of SWIM TI.

Table 7. Standards for OGC WCS

Standard and Specification	Description	Reference
WCS (Web Coverage Service)	This standard defines a service interface for accessing and manipulating geospatial raster data, including satellite imagery, digital elevation models, and other types of gridded data.	https://www.ogc.org/standards/wcs
WFS (Web Feature Service)	This standard defines a service interface for accessing and manipulating geospatial vector data, including points, lines, and polygons.	https://www.ogc.org/standards/wfs
WMS (Web Map Service)	This standard defines a service interface for accessing and delivering geospatial map images over the web.	https://www.ogc.org/standards/wms
WMTS (Web Map Tile Service)	This standard defines a service interface for accessing pre-rendered geospatial map tiles over the web, which are small image files that make up a larger map.	https://www.ogc.org/standards/wmts
WPS (Web Processing Service)	This standard defines a service interface for accessing and executing geospatial processing algorithms over the web.	https://www.ogc.org/standards/wps

3.3.3.2 SOAP

As most users have not applied SOAP to current web applications, this standard is not recommended for the development of SWIM services. The following table makes reference to SOAP related standards and specifications required for supporting the service bindings of SOAP applications.

Table 7. Standards and Specifications for SOAP

Standard and Specification	Description	Reference
SOAP (Simple Object Access Protocol)	This is a technology standard that defines a messaging protocol for exchanging structured data over the internet. It defines the basic structure and syntax of SOAP messages, including the use of XML to encode data and the use of HTTP/HTTPS or other protocols for message transport.	https://www.w3.org/TR/soap/
WSDL (Web Services Description Language)	This is a technology standard that is used to describe the structure and interface of a web service. It defines the types of data that can be exchanged, the methods that can be called, and the protocols and formats used for communication.	https://www.w3.org/TR/wsdl
WS-Security	This is a technology standard that provides a set of extensions to SOAP for securing web services. It defines a framework for adding digital signatures, encryption, and other security features to SOAP messages.	https://www.oasis-open.org/committees/ws-sx/ws-security-200702/
XML Signature	This standard provides a way to digitally sign an XML document.	https://www.w3.org/TR/xmldsig-core/
XML Encryption	This standard provides a way to encrypt and decrypt portions of the XML document.	https://www.w3.org/TR/xmlenc-core/

4. TI CAPABILITIES

SWIM TI capabilities are divided into functional and non-functional capabilities. While the TI functional capabilities can be conceptualized as functions that can be invoked or executed by a system and have inputs and outputs, the non-functional capabilities are derived characteristics of a system as a result of implementing functional capabilities or other contributing elements.

- SWIM TI functional capabilities are infrastructure functions (e.g., protocol transformation, encryption), not specific to a business area or information domain, that enable information exchange between systems.

- SWIM TI non-functional capabilities are SWIM TI characteristics that contribute to the quality of services (e.g., the availability of the SWIM TI has direct impact on the availability of the service it supports).

4.1 Functional Capabilities

The SWIM TI functional capabilities described in this section are common features widely supported by mainstream Commercial Off The Shelf (COTS) systems and services. Implementing a SWIM TI that supports all these capabilities is recommended. The SWIM TI functional capabilities can be grouped into three categories as follows:

Table 8. SWIM TI Functional Capabilities

Capability	Description	Related Technology
Messaging	This capability employs technologies that enable information exchange using various access methods (e.g., publish/subscribe, request/reply).	- Message brokers: such as Apache Kafka, RabbitMQ, ActiveMQ.
Security	This capability provides infrastructure security technologies that enable secured information exchange, including, but not limited to, identity access management, digital certificates, encryption.	- Trust Framework - Information Security Framework
TI Management	This capability monitors technical infrastructure for fault and performance, ensuring reliable and compliant information exchange.	- Configuration management tools - Monitoring and observability tools - Performance optimization tools - Backup and disaster recovery tools

4.1.1 Messaging

In SWIM TI, a service interface, or an infrastructure interface defines operations and related input and output messages for those operations that consumers and providers exchange to implement the functionality offered by a service. The following table presents a list of currently defined messaging capabilities of the SWIM TI.

Table 9. Message Capabilities

Capability	Description
Connectivity	This capability enables message exchange according to well-defined protocols. The transport function will instantiate interface binding specifications (set of protocols) into adaptors or connectors to exchange information with other systems.
Message Distribution	This capability enables synchronous or asynchronous message processing. It uses information exchange resources (e.g., queues, topics) to decouple TI functions involved in message processing (connectivity, validation, etc.) based on configurable distribution rules (e.g., content/context-based routing). The components that provide this kind of functionality are message brokers.
Message Validation	This capability enables message validation to ensure they are syntactically well formed.
Policy Enforcement	This capability enforces messaging policy (e.g., routing and filtering policies, reliability policy) application.
Orchestration	This capability enables coordination between SWIM TI capabilities.

4.1.2 Security

The SWIM TI security capabilities are of high importance as they enable a trusted information exchange. The following table presents a list of currently defined security capabilities of the SWIM TI.

Table 10. Security Capabilities

Capability	Description
Identity Management	This capability enables identity management (e.g., identity creation, identity validation, federated identity retrieval).
Authentication	This capability enables credential verification and validity and their correspondence with an identity.
Authorization	This capability enables permission management associated to identities and, based on these, enforcing access control to SWIM TI services and resources.
Cryptography	This capability provides secure functions for encryption, decryption and hashing.
Key Management	This capability enables cryptographic keys' secure management.
Audit	This capability records contextual information related to security events.
Security Monitoring	This capability enables security related event monitoring, event handling and reporting.
Policy Enforcement	This capability enforces security policy application.
Boundary Protection	This capability provides functions to ensure infrastructure protection against external threats (e.g., firewall, rate limit management).

As the trust framework has been discussed at the ICAO Trust Framework Panel (TFP), SWIM TI security capabilities should align with the outputs of ICAO TFP.

4.1.3 TI Management

As supporting functions to messaging, the TI management capabilities ensure reliable and performant information exchange. The following table presents a list of currently defined TI management capabilities of the SWIM TI.

Table 11. TI Management Capabilities

Capability	Description
Resource Monitoring	This capability enables TI resources (e.g., processors, memory) monitoring.
Service Monitoring	This capability enables the TI service (e.g., status, uptime, and response times) monitoring.
Alerting	This capability enables management alerts regarding infrastructure-related events (e.g., threshold management) monitoring.
Logging	This capability enables the system event recording with the relevant contextual information.
Key Management	This capability enables cryptographic keys' secure management.
Audit	This capability records contextual information related to security events.
Replication	This capability enables system and data replication management, enabling different degrees of fault tolerance and failover.
Persistence	This capability enables data persistence management in the SWIM TI.
Load Balancing /Clustering	This capability enables load distribution management across SWIM TI resources, enabling horizontal scaling and high availability.
Common Time Reference	This capability provides a common time reference for time synchronization between different systems and services.

4.2 Non-Functional Capabilities

The SWIM TI non-functional capabilities directly contribute to the quality of SWIM services that use the SWIM TI. The SWIM TI non-functional capabilities addressed in this section are a consequence of using functional capabilities. The non-functional capabilities of the SWIM TI are based on ISO 25010 and are described in the following table.

Table 12. SWIM TI Non-Functional Capabilities

Quality	Characteristic	Related Capability
Performance Efficiency Qualities	- Time behavior, including response time and latency, can be directly correlated to the functional capability execution time of the TI. - Capacity (e.g., messages per second) is directly correlated to the functional capability execution time of the TI.	- Replication - Load balancing
Reliability Qualities	- Availability enables the SWIM TI to remain operational and accessible when required for use. - Recoverability enables the SWIM TI to recover the data directly affected by an interruption or a failure and re-establish the desired system state. - Fault tolerance enables the SWIM TI to operate as intended despite the presence of hardware or software faults.	- Replication - Load balancing
Security Non-Functional Qualities	- Confidentiality ensures that data is accessible only to those authorized to have access. - Integrity prevents unauthorized access to, or modification of data. - Non-repudiation ensures actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later. - Accountability ensures actions of an entity can be traced uniquely to the entity. - Authenticity ensures the identity of a subject or resource can be verified.	- Authentication - Authorization - Cryptography - Logging - Message Validation

APPENDIX A

STRUCTURE OF AMHS/SWIM GATEWAY

The AMHS/SWIM Gateway consists of following functional building blocks (Figure A.1):

- AMHS Component: Provides the X.400 connection to AMHS agent for exchange of aeronautical information with AMHS users.
- Information Transfer and Control Unit (ITCU): Provides functions to convert and transfer information and control the flow of information.
- SWIM Component: Provides the AMQP connection to SWIM TI for exchange of aeronautical information with SWIM information providers and consumers.
- Control Position (CP): Provides the function to receive reports on issues occurred during the automated processing by the other components of the AMHS/SWIM Gateway for appropriate action.
- Directory User Agent (DUA): Provides the connection to the ATN Directory.

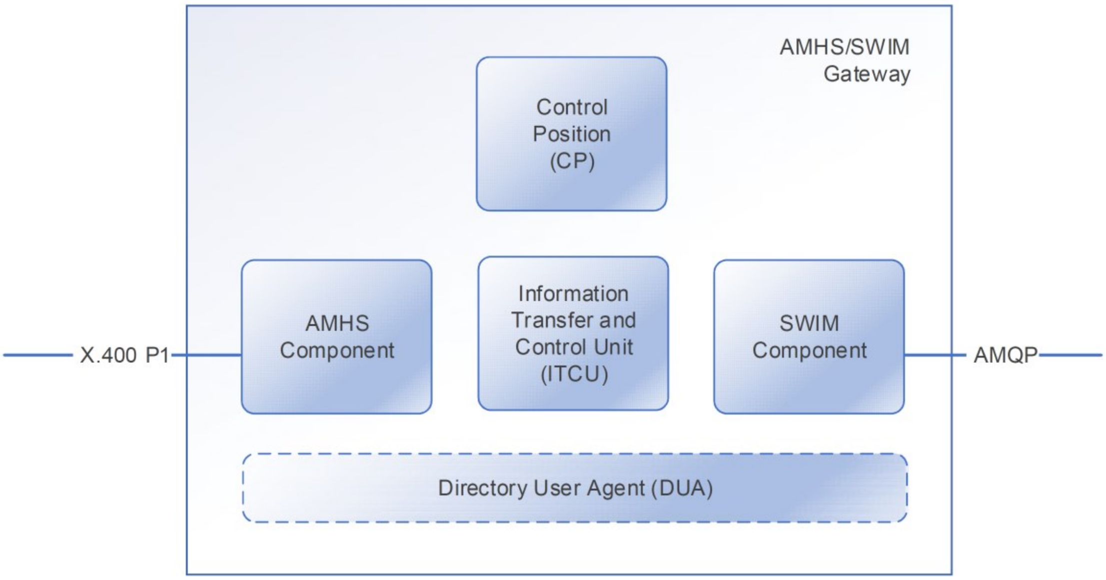

Figure A.1. Structure of AMHS/SWIM Gateway

Internally, each functional building block of the AMHS/SWIM Gateway has connections to other functional building blocks using local defined interfaces. Detailed information can be found in the "AMHS/SWIM Gateway Specification" document.

To achieve interoperability during the transition period, the function of the AMHS/SWIM Gateway can be provided by SWIM TI service providers or third-party SWIM service providers.

APPENDIX B

ARCHITECTURE OF SDCM

The Service Description Conceptual Model (SDCM) provides a graphical and lexical representation of the properties, structure, and interrelationships of all service metadata elements, collectively known as a Service Description.

The SDCM in its JSON formalization has been used to develop a SWIM Discovery Service (SDS), an international collaborative project currently supported by the FAA, the Korea Airports Corporation (KAC), the People's Republic of China's Air Traffic Management Bureau (ATMB), and Japan's Electronic Navigation Research Institute (ENRI) under the SWIM Task Force.

In the SDCM, packages and classes are two main Unified Modelling Language (UML) model elements. Packages are used to group classes into logical units, whereas classes represent specific concepts. Packages and classes are related in a variety of ways through UML-defined associations.

Figure B.1 shows the high-level architecture of the SDCM, where each part of the top, encompassing concept Service Description is shown as a package, which in its turn contains classes. The aggregation association between Service Description and Profile, Model, and Grounding indicates that these are all parts of the Service Description, and the dependency relationship between Utility and Service Description signifies that changes to Utility's classes affect classes in other packages.

- Service Description package: The information needed in order to use, or consider using, a service.

- Profile package: The part of a service description that advertises the service to potential consumers by describing the parties responsible for providing the service, what is accomplished by the service, and limitations on service applicability.

- Model package: The part of a service description that describes the service interface and its operations, including the contents of requests, message formats, data types, and how to construct an invocation message and interpret a response message.

- Grounding package: The part of a service description that describes the means by which the service is invoked, including the underlying technology protocols and network locations of the service.

- Utility package: The part of a service description that contains abstract classes for use by other classes.

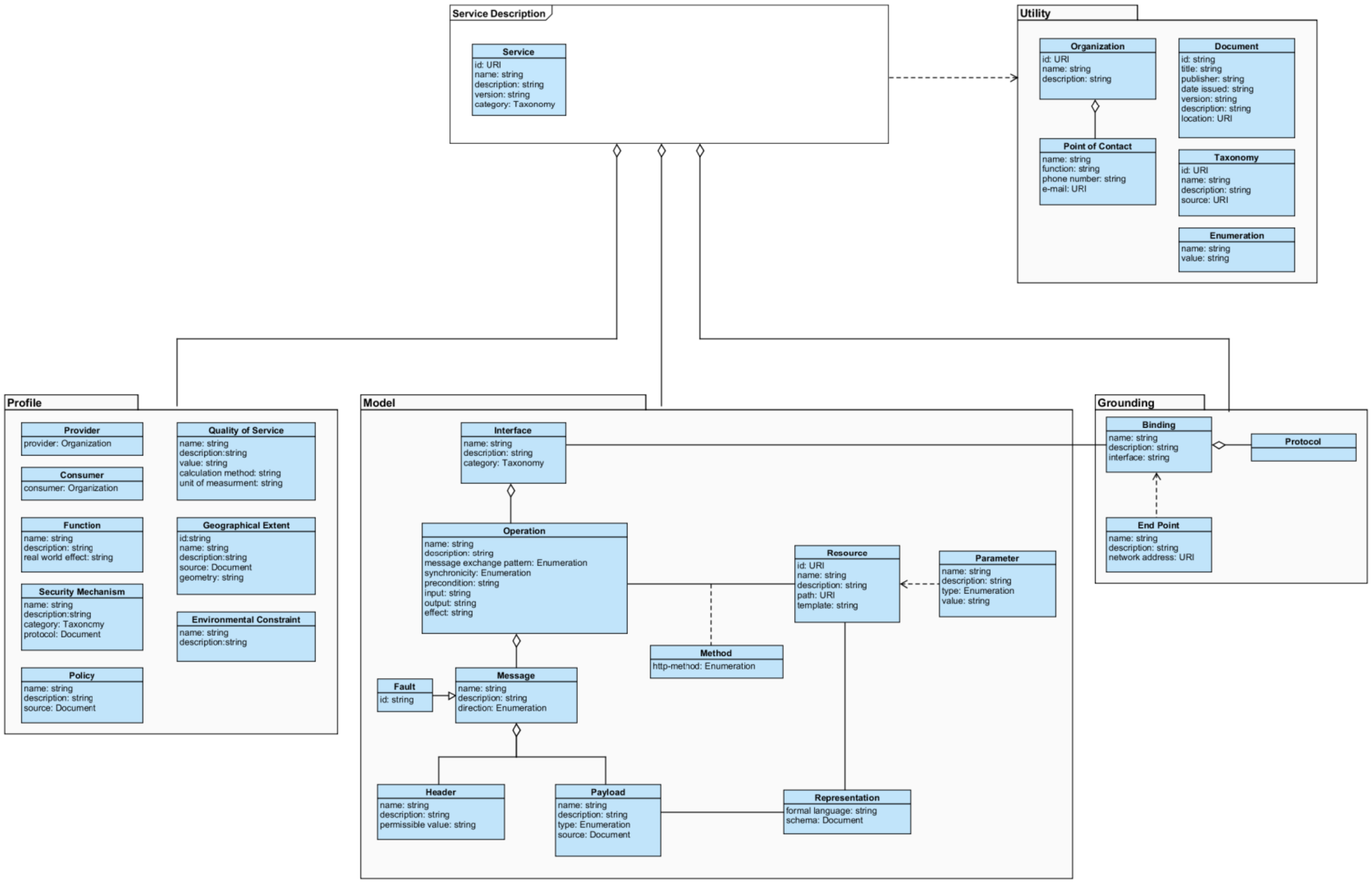

Figure B.1. Architecture of SDCM

APPENDIX C

EXAMPLE OF SWIM MESSAGE HEADERS

C.1 Message Headers for FIXM FF-ICE Messages

The following table (Table C.1) shows an example of message headers for an FF-ICE Field Flight Plan message in FIXM format.

Table C.1. Example of Message Headers for a Filed Flight Plan Message

Header Name	Values	Descriptions
SOURCE	RJ_JAL	Name of message publisher (ICAO Country Code_Organization Name)
RECIPIENT_LIST	RJ_JCAB,VT_AEROTHAI	Name list of recipients
SYSTEM	JAL	Name of system
CATEGORY	FIXM	Name of information exchange model (FIXM)
CATEGORY_VERSION	FIXM_4_2_FF_ICE	Version of information exchange model (FIXM 4.2 version for FF-ICE Messages)
MESSAGE_TYPE	FILED_FLIGHT_PLAN	Message type of information exchange model (FIXM FF-ICE message types)
FFICE_PHASE	FILED	Flight plan phase of FF-ICE (PRELIM or FILED)
DEP_AIRPORT	RJAA	Departure Airport
ARR_AIRPORT	VTBS	Arrival Airport
AIRLINE	JAL	Name of airline
ACID	JAL707X	Aircraft Identification
GUFI	0248982c-4384-49f4-bdb3-7956bd553383	Globally Unique Flight Identifier
EOBT	2023-02-01T03:00:00Z	Estimated Off-Block Time
TIMESTAMP	JAL_OUT:1675213637251	Timestamp of the message out or in the system

The following headers are mandatory for GUFI registration and validation.

- ACID
- DEP_AIRPORT
- ARR_AIRPORT
- EOBT

The following headers are required for content-based message routing between SWIM TIs.

- SOURCE
- RECIPIENT_LIST
- CATEGORY
- CATEGORY_VERSION
- MESSAGE_TYPE

The following headers are recommended for SWIM TI management.

- SYSTEM
- TIMESTAMP

C.2 Message Headers for AIXM Messages

The following table (Table C.2) shows an example of message headers for a NOTAM message in AXIM format.

Table C.2. Example of Message Headers for a NOTAM Message

Header Name	**Values**	**Descriptions**
SOURCE	RJ_JCAB	Name of message publisher
RECIPIENT_LIST	RJ_JAL,VT_AEROTHAI	Name list of recipients
SYSTEM	JCAB	Name of system
CATEGORY	AIXM	Name of information exchange model (AIXM)
CATEGORY_VERSION	AIXM_5_1	Version of information exchange model (AIXM 5.1)
MESSAGE_TYPE	NOTAM	Message type of information exchange model (NOTAM message)
TIMESTAMP	JCAB_OUT:1675213637251	Timestamp of the message out or in the system

C.3 Message Headers for IWXXM Messages

The following table (Table C.3) shows an example of message headers for a SIGMET message in IWXXM format.

Table C.3. Example of Message Headers for a SIGMET Message

Header Name	**Values**	**Descriptions**
SOURCE	RJ_JCAB	Name of message publisher
RECIPIENT_LIST	RJ_JAL,VT_AEROTHAI	Name list of recipients
SYSTEM	JCAB	Name of system
CATEGORY	IWXXM	Name of information exchange model (IWXXM)
CATEGORY_VERSION	IWXXM_3_0	Version of information exchange model (IWXXM 3.0)
MESSAGE_TYPE	SIGMET	Message type of information exchange model (SIGMET message)
TIMESTAMP	JCAB_OUT:1675213637251	Timestamp of the message out or in the system

C.4 Message Headers for Surveillance Data

Currently, two common message formats are available for surveillance data exchange in the APAC region. One is using TRACK message type defined in the FIXM APAC Extension. The other is sharing surveillance data in ASTERIX format.

The following table (Table C.4.1) shows an example of message headers for a TRACK message in FIXM APAC Extension format.

Table C.4.1. Example of Message Headers for a TRACK Message in FIXM APAC Extension

Header Name	**Values**	**Descriptions**
SOURCE	RJ_JAL	Name of message publisher
RECIPIENT_LIST	RJ_JCAB,VT_AEROTHAI	Name list of recipients
SYSTEM	JAL	Name of system
CATEGORY	FIXM	Name of information exchange model (FIXM)
CATEGORY_VERSION	FIXM_4_2_APAC	Version of information exchange model (FIXM 4.2 APAC Extension)
MESSAGE_TYPE	TRACK	Message type of information exchange model (TRACK message)
DEP_AIRPORT	RJAA	Departure Airport
ARR_AIRPORT	VTBS	Arrival Airport
AIRLINE	JAL	Name of airline
ACID	JAL707X	Aircraft Identification
GUFI	0248982c-4384-49f4-bdb3-7956bd553383	Globally Unique Flight Identifier
EOBT	2023-02-01T03:00:00Z	Estimated Off-Block Time
TIMESTAMP	JAL_OUT:1675213637251	Timestamp of the message out or in the system

For consistent operation and data governance, the following headers are mandatory for information registration and validation by using FIXM format.

- ACID
- GUFI
- DEP_AIRPORT
- ARR_AIRPORT
- EOBT

The following table (Table C.4.2) shows an example of message headers for a TRACK message in ASTERIX format.

Table C.4.2. Example of Message Headers for a TRACK Message in ASTERIX

Header Name	Values	Descriptions
SOURCE	RJ_JCAB	Name of message publisher
RECIPIENT_LIST	RJ_JAL,VT_AEROTHAI	Name list of recipients
SYSTEM	JCAB	Name of system
CATEGORY	ASTERIX	Name of information exchange model (ASTERIX)
CATEGORY_VERSION	ASTERIX _CAT021	Version of information exchange model (Data Category of ASTERIX)
MESSAGE_TYPE	TRACK	Message type of information exchange model (ADS_B TRACK message)
DEP_AIRPORT	RJAA	Departure Airport
ARR_AIRPORT	VTBS	Arrival Airport
ACID	JAL707X	Aircraft Identification
TIMESTAMP	JCAB_OUT:1675213637251	Timestamp of the message out or in the system