CNS SG/27 – **WP/29**
Agenda Item 3.2
28/08-01/09/23

International Civil Aviation Organization

Twenty Seventh Meeting of the Communications/ Navigation and Surveillance Sub-group (CNS SG/27) of APANPIRG

Bangkok, Thailand, 28 August – 01 September 2023

Agenda Item 3: Aeronautical Fixed Service (AFS)

3.2. Other AFS related matters

CHALLENGES AND REQUIREMENTS FOR IPS ENVIRONMENT

(Presented by USA / Federal Aviation Administration)

SUMMARY

This paper addresses challenges and requirements for supporting future services, including SWIM, in an Internet Protocol Suite (IPS) environment.

1. INTRODUCTION

1.1 As aviation communications (messaging, voice, air/ground) migrate towards a common transport based on the Internet Protocol Suite (IPS), the underlying infrastructure is presented with additional challenges and requirements.

1.2 This paper reviews some current ideas in order to identify planning requirements.

2 DISCUSSION

Migration to Services

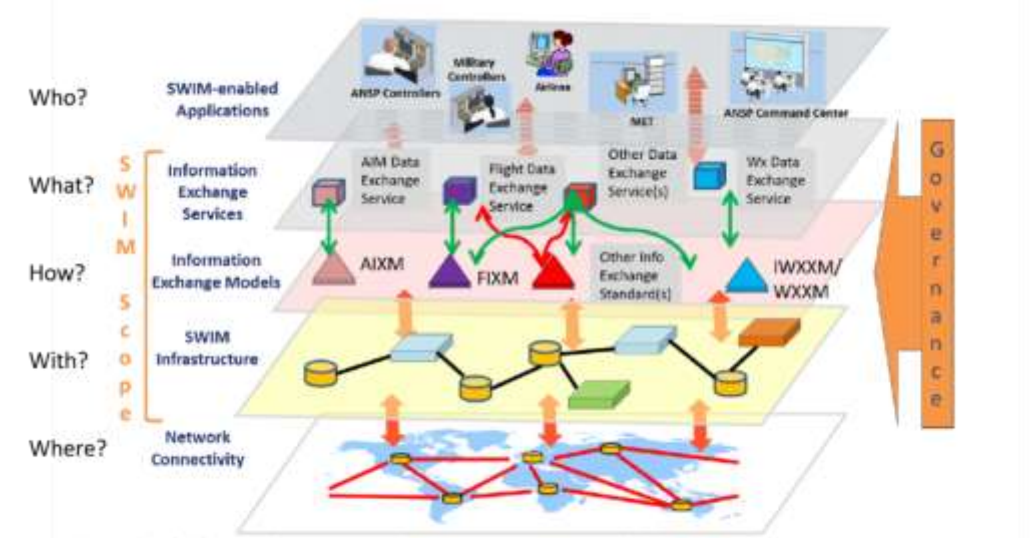
2.1 The Aeronautical Fixed Service (AFS), as specified in ICAO Annex 10, has traditionally implemented point-to-point telecommunications for voice and data connections. With IP-based Air Traffic Services Message Handling System (AMHS) and Voice over Internet Protocol (VoIP), as specified on ICAO Docs 9880 and 9896 respectively, these services can now be carried by IP transport over networks such as the Asia Pacific Common AeRonautical Virtual Private Network (CRV).

2.2 As point-to-point dataflows between ANSPs, these services can be obfuscated by GRE tunnels and constrained to identified IP addressing by firewalls at ANSP boundaries. But as the aviation environment moves to service architectures, protecting the increased number of connections presents a challenge.

System Wide Information Management (SWIM)

2.3 System Wide Information Management (SWIM) “shifts the ATM information architecture paradigm from point-to-point data exchanges to system-wide interoperability.”

2.4 The ATM Operational Concept envisages that, “information management solutions will be defined at the overall system level, rather than individually at each major subsystem (program / project/ process/ function).”[1] Rather than the subsystem defining the display, the paradigm is changed so that the desired application/display defines the information requirements from subsystems.


Who?
SWIM-enabled Applications
ANSP Controllers
Military Controllers
Airlines
MET
ANSP Command Center
What?
Information Exchange Services
AIM Data Exchange Service
Flight Data Exchange Service
Other Data Exchange Service(s)
Wx Data Exchange Service
How?
Information Exchange Models
AIXM
FIXM
Other Info Exchange Standard(s)
IWXXM/ WXXM
With?
SWIM Infrastructure
Where?
Network Connectivity
SWIM Scope
Governance

Information Exchange Services defined for each ATM information domain and for cross domain purposes, where opportune, following governance specifications and agreed upon by SWIM stakeholders. SWIM-enabled applications will use information exchange services for interaction;

Information Exchange Models using subject-specific standards for sharing information for the above Information Exchange Services. The information exchange models define the syntax and semantics of the data exchanged by applications;

SWIM Infrastructure for sharing information provides the core services such as interface management, request-reply and publish-subscribe messaging, service security, and enterprise service management.

Figure 1: SWIM Five Layer Architecture

2.5 Figure 1 shows the SWIM five-layer architecture where SWIM-enabled applications may fuse information from different information exchange services, potentially from different providers. These exchanges are supported by connections over one or more networks (both private and public).

2.6 Broadening the number of IP exchanges, between ANSPs in a SWIM environment, will increase the security challenge. There is increasing movement away from simple network boundary protection toward a ‘*Zero Trust*’ model. Zero Trust relies on authentication and authorization; verifying the legitimacy of “who” is requesting access and tightly controlling “what” resources they are entitled to. Typically implemented within an organization, this can equally be applied *between* entities using shared networking.

2.7 ICAO’s International Aviation Trust Framework (IATF) initiative is addressing Digital Identity and Network Information Security which can be elements of Zero Trust.

Digital Identity

2.8 Digital Identity declares who or what you are by providing a credential to that effect for a given level of assurance. Work on Digital Identity is focused on Digital

[1] Global Air Traffic Management Operational Concept, Doc 9854

Certificates that use Public/Private key encryption to support a hierarchy of certificate verification.

2.9 A trusted Root Certificate Authority (CA) provides a self-signed certificate and then signs a certificate for a verified Intermediate CA. The latter nest those credentials when issuing a signed certificate for a verified User.

[[[Root CA] Intermediate-CA] User]

The User can then present this ‘nested’ certificate when requesting access. The recipient must be able to verify all signatures in this presented certificate credential and so must have access to data about these CAs and any revocations (invalidated certificates). Significant challenges remain in expanding this concept to a global environment with multiple trust roots, but local solutions can be implemented in the interim.

2.10 ICAO has stated that Digital Identity is required for SWIM connections. Identity verification is a security function of the SWIM infrastructure layer, shown in Figure 3.

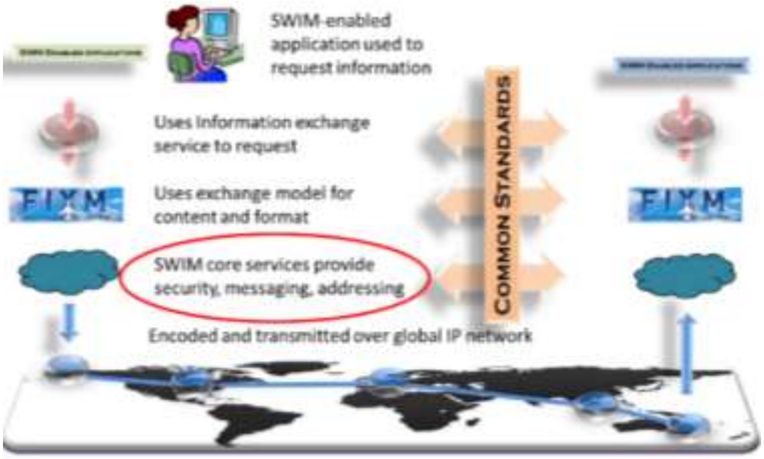

SWIM-enabled application used to request information
Uses Information exchange service to request
Uses exchange model for content and format
SWIM core services provide security, messaging, addressing
Encoded and transmitted over global IP network
COMMON STANDARDS
FIXM
FIXM

Figure 2: SWIM Layered Functionality

2.11 Management of Digital Identities and validation of those received will be the responsibility of each network user, but networking will need to provide the necessary transport for the associated information across the ‘trust network’.

Network Information Security

2.12 Network Information Security requirements include: IPv6 (dedicated ICAO block); Domain Name System (DNS); information security; network management and network contingency plans.

2.13 The expanded address range of IPv6 is deemed essential for air/ground IP access to the myriad of future airborne craft (including drones). Network access to air/ground providers must support IPv6. Ground/ground exchanges between ANSPs can be implemented prior to an ICAO block using existing IPv6 country allocations.

2.14 A common naming system must be adopted for use by all the entities that are likely to inter-communicate, e.g. authorities, ANSPs, service providers, manned and unmanned aircraft. Where needed, a Domain Name System (DNS) must translate names into IP addresses.

2.15 Information security addresses the requirements for information confidentiality, integrity and availability. In general, these are expected to be requirements for users rather than networks.

2.16 Finally, network management and network contingencies suggest increased monitoring and intelligent use of the user's networking ecosystem including access from shared networks and 'cloud services'.

SWIM Implementation

2.17 SWIM has two separable concepts: information services in a service-oriented architecture (SOA); and information consolidation from multiple sources.

2.18 With well-defined SWIM services (documented in a registry), a user's information can be provided to many requesters. Similarly, the user can obtain information from multiple sources. This results in many to many (federated) connections.

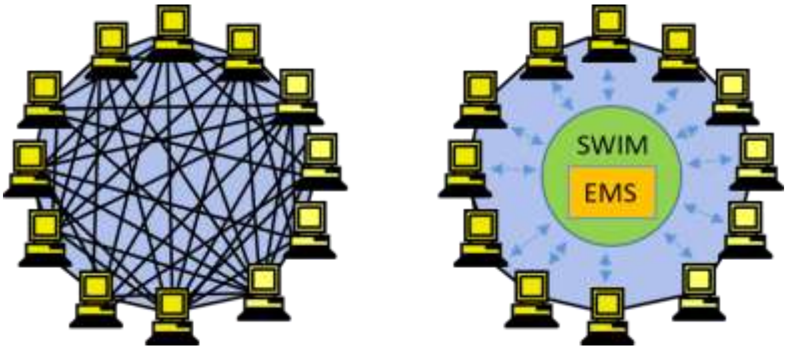


Figure 3: Federated and Centralized SWIM Architectures

2.19 Rather than each user having multiple connections, it is more efficient and beneficial to pool information in some centralized SWIM Enterprise Messaging Service (EMS). An information 'producer' can upload information messages to an EMS, and multiple information 'subscribers' can receive messages with content that match their filters. In this way, the EMS acts as an 'information switch'. The EMS can offer additional mediation services or applications taking advantage of this broader pooled dataset.

2.20 Establishing a regional EMS offers advantages to users and creates a focal point for information exchange between SWIM systems. For example, filing a flight plan in the FF-ICE environment might involve distribution of a FIXM flight to multiple FIRs in different regions along the flight route. Such distribution can be accomplished by exchanges between regional EMSs and subsequent selected distribution to the EMS participants. Figure 4 attempts to illustrate such a concept.

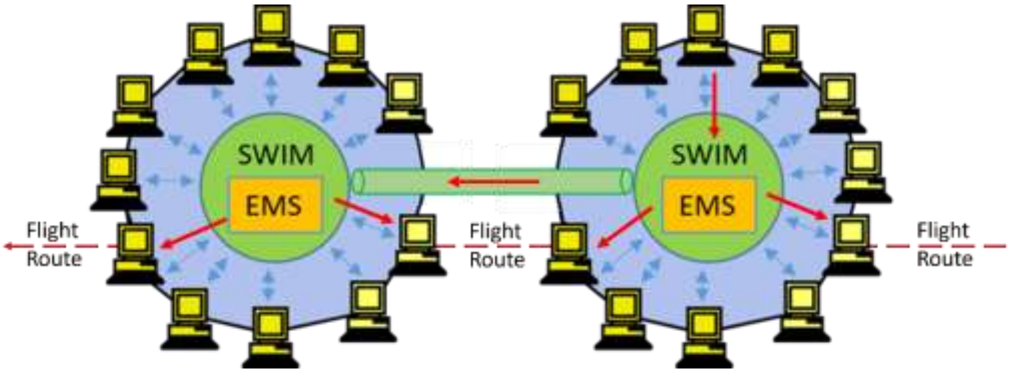


Figure 4: Regional SWIM Exchanges

3 REQUIREMENTS AND CHALLENGES

3.1 Migration toward a service environment suggests the following requirements:

3.1.1 ICAO Requirements

a) ICAO needs to provide an IPv6 dedicated address block

b) ICAO needs to propose a Name Space and field a DNS

c) ICAO needs to deliver IATF recommendations for security including a Trust Framework for Digital Identities

3.1.2 Network Requirements

d) Networks need to plan to implement IPv6

e) Networks need to provide transport for DNS access and distribution

f) Networks need to provide transport for Digital Identity information access

3.1.3 User Requirements

g) Users need to plan for IPv6 implementation

h) Users need to plan to adopt Digital Identities

i) Users need to plan to support ICAO naming and DNS

j) Users need to plan for SWIM.

3.2 Migration toward a service environment poses some challenges:

3.2.1 Which body will provide support for management of the IPv6 address space and DNS namespace? Perhaps something similar to the ATS Messaging Management Centre (AMC) is needed.

3.2.2 ANSPs will continue to work in conjunction with Service Providers (e.g. surveillance, air/ground, airline interactions). Before engaging any shared service, the Service Provider should agree to conform to any ICAO security recommendations, provide services in accordance with ICAO Standards and Recommended Practices (SARPS), and operate with an agreed Service Level Agreement (SLA). Which entities should enter into such an agreement, execute governance and oversee the service provision?

3.2.3 Shared SWIM services can lead to the exchange of information between ANSPs through an Enterprise Messaging Service (EMS). How should competing EMSs within a region be selected and authorized?

3.2.4 As part of the Aeronautical Telecommunication Network (ATN), the existing private networks (eg. CRV) transport voice and time-critical data. As time-critical information flows move to SWIM, they should also use the ATN, but SWIM also carries a much greater bandwidth of advisory information that is not time-critical. Carrying the latter over a private network may be cost-prohibitive for many ANSPs. Guidelines for sensible use of the ATN and the Internet for SWIM information is needed.

4 ACTION BY THE MEETING

4.1 The meeting is invited to:

a) Consider the suggestions presented in this paper

b) Take appropriate planning actions as required.

– – – – – – – – – – – – –