International Civil Aviation Organization

Eighth Meeting of Aeronautical Communication Service Implementation Co-ordination Group of APANPIRG (ACSICG/8)

Video Tele-Conference, 21 – 23 June 2021

Agenda Item 5: Review and update the AMHS/ATN Implementation Status

IMPLICATIONS OF CYBERSECURITY AND ASSOCIATED REQUIREMENTS FOR CRV OPERATIONS

(Presented by United States / FAA)

SUMMARY

This flimsy reviews the current and envisioned future environments for CRV operations to provide a framework for discussion of requirements for Cyber Security and SWIM.

1. INTRODUCTION

1.1 This flimsy addresses the implications for existing services and the Asia Pacific Common AeRonautical Virtual Private Network (CRV) resulting from the recent Cybersecurity Webinar[1] and future support of SWIM and other proposed services for the Region.

2. DISCUSSION

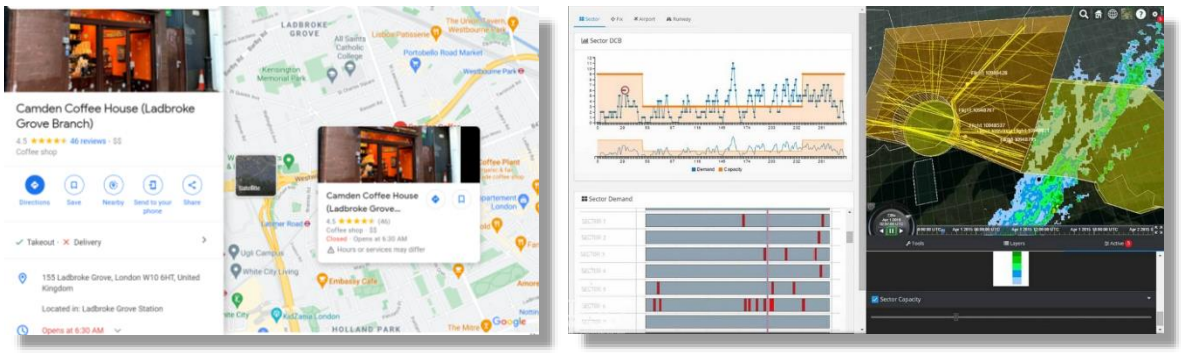
2.1 The Aeronautical Fixed Service (AFS), as specified in ICAO Annex 10, has traditionally provided voice and data connections over point-to-point telecommunications. With the migration towards IP-based Air Traffic Services Message Handling System (AMHS) and Voice over Internet Protocol (VoIP), as specified on ICAO Docs 9880 and 9896, respectively, these services can now be carried over the more flexible CRV yet still remain as limited point-to-point connections.

2.2 These point-to-point connections, and associated information flows result from, and are enforced by, functionally dedicated systems: flight processing, weather, NOTAMs etc.. System Wide Information Management (SWIM) "*shifts the ATM information architecture paradigm from point-to-point data exchanges to system-wide interoperability*."[2]

---

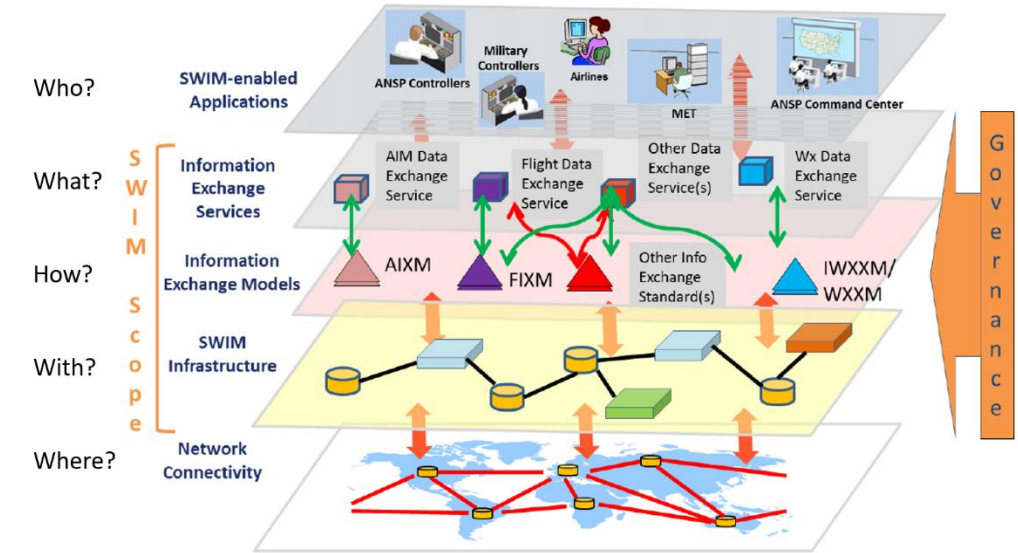
[1] Asia/Pacific Regional Cyber Security Webinar: *"Cyber Security Management Framework for CNS/ATM Systems"*, 14 June 2021

[2] Manual on System Wide Information Management (SWIM) Concept, ICAO Doc 10039.



We are familiar with Google maps "mash-ups" that combine information from multiple sources to provide convenience to the user. SWIM, likewise, aims to support applications that combine useful information in the ATM environment. The ATM Operational Concept envisages that, "*information management solutions will be defined at the overall system level, rather than individually at each major subsystem (programme/ project/ process/ function) and interface level*."[3]

2.3 SWIM has a five-layer architecture to support this change of paradigm. The lowest layer is the network that simply provides connections to request/reply or publish/subscribe functions of the SWIM infrastructure that allow access to multiple data exchange services.



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.

2.4 Broadening access in an IP environment beyond limited point-to-point connections can increase exposure to malicious infiltration. Central to mitigating this threat is verifying the legitimacy of "who" is accessing the infrastructure and "what" information they are entitled to. The recent Cyber Security Webinar presented the International Aviation Trust Framework (IATF) initiative composed of *Digital Identity* and *Network Information Security* elements.

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

2.5 *Digital Identity* says who or what you are, provides a credential to that effect and asserts that credential to a given level of assurance. Work on Digital Identity is focused on Digital Certificates that use Public/Private key encryption to support a hierarchy of certificate verification.

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

A trusted Root Certificate Authority (CA) provides a self-signed certificate and verifies the identity and signs a certificate for an Intermediate CA. The latter includes that signed credential when issuing a signed certificate for a verified User. The User can then present this certificate when requesting access. The target must be able to verify all the signatures in this presented certificate credential and so must have access to data about these CAs and any revocations (invalidated certificates). Challenges remain in expanding this concept to a global environment where there may be multiple roots of trust. Note that China has proposed[4] an interesting solution to root trust using block-chains.

2.6 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.

2.7 Today's AMHS systems uses simple authentication credentials when connecting across the CRV. This could be replaced by Digital Identity certificates. VoIP can be secured similarly.

2.8 ICAO has stated that SWIM connections require Digital Identity. Identity verification is a function of the SWIM infrastructure layer which is also responsible for data integrity using information signing. Management of Digital Identities is the responsibility of each User and may be in the network layer in each User's environment; it is not expected to be a function of CRV. The latter may need to provide transport for Digital Identity verification.

2.9 *Network Information Security* requirements were presented as: IPv6 (dedicated ICAO block); Domain Name System (DNS); information security; network management ; and network contingency plans.

2.10 IPv6 support directly affects the CRV implementation and requires implementation planning.

---

[4] SP/203 – "A method of building global mutual trust infrastructure based on blockchain", Asia/Pacific Regional Cybersecurity webinar: *"Management Framework/or CNSIATM Systems"*, 14 June 2021

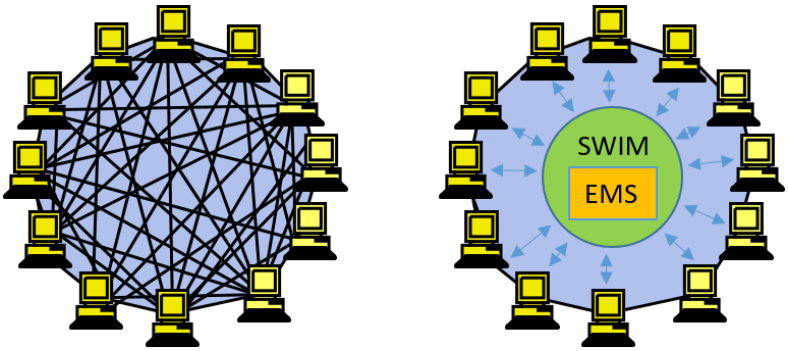
2.11 DNS will be used to translate names of connection targets into IP addresses and support common naming. The CRV needs to support transport and distribution of DNS. Non-ANSP access may be required. Users may have to provide local DNS support.

2.12 Information security addresses the requirements for information confidentiality, integrity and availability. In general, these are expected to be requirements for the Users of CRV, rather than the existing network. Naturally, when transiting across the Internet or other Public domain, encrypted tunnels may have to be used to prevent intrusion.

2.13 Network management and network contingencies suggests monitoring and intelligent use of the User's networking ecosystem including access across CRV if a shared service is being used. It does not suggest additional monitoring by the existing CRV service provider.

2.14 The SWIM concept has two separable concepts: information provision through a set of clearly defined services, subject to governance, in a service-orient architecture (SOA); and consolidation of information from multiple sources.

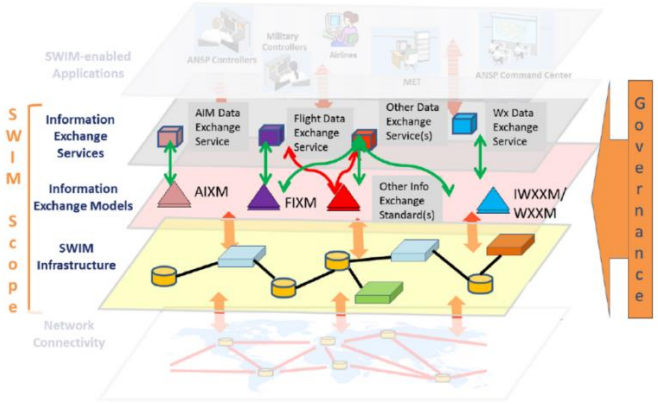
2.14.1 With well-defined SWIM services (documented in a registry), a User's information can be provided to many requesters. Similarly, the User can obtain information from multiple sources. This results in many to many connections.



2.14.2 Rather than each User have many connections, Users can supply their information to a centralized SWIM Enterprise Management System (EMS) which re-supplies recipients with combined information in a consolidated delivery. This minimizes the connections and bandwidth usage of the network. The EMS acts as an information switch. Additional mediation services or even applications can be built on such a platform.

2.15 An Information Paper[5] to the SWIM Task Force by PCCW (the CRV service provider) offered SWIM as a service (SWIM Infrastructure and Information Exchange Services accessible over the network) for Users not wishing to invest in a local SWIM implementation.

[5] Information Paper (IP/07) of the Asia Pacific Fourth Meeting of System Wide Information Management Task Force (SWIM TF/4), November 2020.



A User's client applications would access the hosted SWIM Information Exchange Services over the CRV. The hosted SWIM environment would interact with other SWIM deployments and information sources and could provide information consolidation and mediation services, e.g. translation from Traditional Alphanumeric Code (TAC) to ICAO Weather Information Exchange Model (IWXXM).

3. SUGGESTED IMPLICATIONS

3.1 The meeting is invited to comment and discuss these suggested implications:

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 DNS

c) ICAO needs to provide the Trust Framework for Digital Identities

3.1.2 CRV Network Requirements

d) CRV needs to plan to implement IPV6

e) CRV needs to provide transport for DNS access and distribution

f) CRV needs to provide transport for Digital Identity access and verification

3.1.3 Service Provider Options

g) Service Providers may offer optional SWIM services, or applications built on SWIM services, to Users.

3.1.4 CRV User Requirements

h) CRV Users need to implement network security

i) CRV Users need to plan to implement IPv6

j) CRV Users need to plan to implement DNS

k) CRV Users need to plan to adopt Digital Identities, as prescribed by ICAO, and use them in connections with SWIM services

l) CRV Users may implement SWIM, may access SWIM as a service, or may adopt some hybrid of the two.

m) CRV Users may implement data integrity by digital signing

– – – – – – – – – – – – –