International Civil Aviation Organization

The Fifth Meeting of System Wide Information Management Task Force (SWIM TF/5)

Video Tele-conference, 9 – 11 August 2021

Agenda Item 6: Updates on the assigned tasks by task leads/contributors, including progress report and issues

b) SWIM Infrastructure
f) Validation & Demontration

SWIM INFRASTRUCTURE TO ACHIEVE MESSAGE LEVEL SECURITY

(Presented by Japan, Thailand, and USA)

SUMMARY

To assure a trusted information exchange, the security capability is required as part of SWIM Technical Infrastructure (SWIM TI) as mentioned in the Manual on SWIM (Doc 10039). Moreover, to develop a globally harmonized International Aviation Trust Framework (IATF), ICAO established the Trust Framework Study Group (TFSG) to work on it. In order to validate the concept of IATF on SWIM, a test platform has been developed by the team of Multi-Regional Trajectory Based Operation (MR TBO) Demonstration. This paper presents the technical implementation of security service on SWIM through a scenario-based validation and discusses some concerns and challenges to achieve end-to-end security through a SWIM-based trust framework.

1. INTRODUCTION

1.1 As an enabler of digital transformation in aviation, SWIM not only ensures seamless integration among geographically distributed systems in the air transportation field but also enables seamless information sharing among the multiple stakeholders in the ATM domain. 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 become available after applying SWIM. These properties brought by SWIM have presented a number of challenges in terms of information security and operation safety.

1.2 Cyber threats become more and more concerned, as aviation continues its digitization journey. To protect the safety of flight operations from these threats and ensure business continuity, all stakeholders agree that trusted information should be exchanged between trusted identities through trusted communication paths on a global basis. This means that in a digital environment, communication parties should be able to identify themselves mutually and the information exchanged should not be able to be modified by unauthorized parties.

1.3 To speed the development of SWIM required capabilities, the use of Commercial Off-The-Shelf (COTS) technologies is expected. However, the separated solution or protection of high-assurance applications using COTS technologies will be required if these threats cannot be mitigated at the architecture or framework level. Therefore, a global implementation from a holistic point of view that is flexible to protect against known threats and adapt to future threats should be focused on. Along to this, ICAO has formed a study group to address a trust framework for aviation. Digital identity and network resiliency are key focus areas of this group. Above all, States should ensure that their national regulations are aligned with global concepts and standards to allow for effective implementation of cybersecurity practices.

1.4 Security is a critical aspect of SWIM since related security failures may affect the aviation safety domain. More information is being shared by stakeholders that are increasingly interconnected when using SWIM as an enabler to modernize ATM. As a result, cybersecurity becomes an aspect of critical importance for SWIM implementation. In this paper, the technical implementation of security service on SWIM through a scenario-based validation is presented. In addition, some concerns and challenges to achieve end-to-end security through a SWIM-based trust framework are discussed.

2. DISCUSSION

2.1 The SWIM Technical Infrastructure (TI) enables the implementation of interfaces between systems, providing technical capabilities for secure, high performing and reliable information exchange. The SWIM TI functional capabilities include message capabilities, security capabilities and TI management capabilities. As supporting messaging functions, the SWIM TI security capabilities are of high importance as they enable a trusted information exchange. These capabilities are Identity Management, Authentication, Authorization, Cryptography, Key Management, Audit, Security Monitoring, Policy Enforcement, and Boundary Protection. Furthermore, the Manual on SWIM (Doc 10039) provides a series of security non-functional qualities that include Confidentiality, Integrity, Non-repudiation, Accountability and Authenticity.

2.2 In order to validate the Public Key Infrastructure (PKI) based trust framework concept and the implementation of SWIM TI security capabilities, the test platform has been developed by the team of Multi-Regional Trajectory Based Operation (MR TBO) demonstration led by Federal Aviation Administration (FAA). The FAA's MR TBO project expands the previous exercises on Flight and Flow Information for a Collaborative Environment (FF-ICE) to the demonstration of key TBO capabilities through the cooperation between international partners and industry partners.

2.3 With the support of FAA, the PKI-based security service including message signing service and message validation service has been applied on the test system of MR TBO. As a part of technical exercises of MR TBO, an FF-ICE message exchange demonstration with security service was conducted between Aeronautical Radio of Thailand Ltd. (AEROTHAI) and Japan Civil Aviation Bureau (JCAB) at the ICAO APAC SWIM Workshop on July 7th, 2021.

2.4 The high-level system architecture of MR TBO is shown in Figure 1. The Global Enterprise Messaging Service (GEMS), which facilitates information sharing between a variety of partners and applications is divided into two parts, i.e. Asian GEMS and US GEMS. Each GEMS service provider provides SWIM access point to his users, and assure the interoperability of SWIM TI by cooperating with other GEMS service providers. The GEMS connectivity of JCAB to other partners is provided by NEC. The communication between SkyFusion Frontier (SFF) supported by L3Harris and NEC is based on Transport Layer Security (TLS). The site-to-site Virtual Private Network (VPN) connections have been established between NEC and JCAB and AEROTHAI. The network connection between NEC and CAAS has not been established yet. The communication standard for Pub/Sub messaging is Advanced Messaging Queuing Protocol (AMQP).

2.5 At the current stage, the security service has been installed in the SWIM-enabled local systems of FAA, AEROTHAI and JCAB. For the first step of validation, the FAA hosts a common Certificate Authority (CA) server for issuing certificates and a Server-based Certificate Validation Protocol (SCVP) server for providing the real-time certificate verification for all users. The communication between the security service and SCVP server is based on the point-to-point VPN connection. In the AEROTHAI's and JCAB's test systems, the security service has been applied to the available FF-ICE services for trusted information exchange among trusted ATM Service Providers (ASPs) and Airspace Users (AUs).

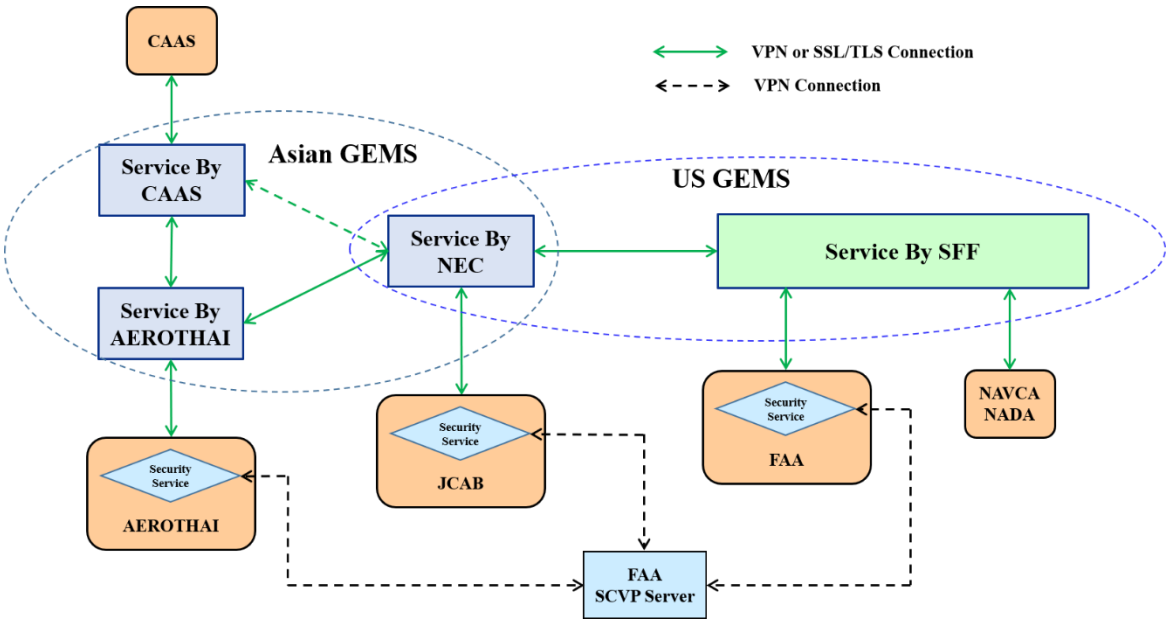

Figure 1. System Architecture of MR TBO with Security Service

2.6 The AEROTHAI's and JCAB's SWIM test beds provide a basic technical infrastructure, information services, and SWIM-enabled applications to support the SWIM concept-based development, validation and demonstration. Figure 2 shows the structure of SWIM-based trust framework and the message exchange by using security service. Each producer is required to have its own certificate for signing messages. Along with the concept of IATF, the message should be exchanged between trusted identities with trusted information through the trusted network.

2.7 The security service consists of signing service and validation service. The signing service is an application which provides a producer the ability to digitally sign a message before the message is distributed to other stakeholders through EMS. The signing service receives AMQP 1.0 messages from a message publisher, generates a detached digital signature of the message body, attaches the signature to the message and forwards the message to EMS on behalf of the producer. The validation service is an application which provides a consumer the ability to validate the message integrity and identity of the sender. The validation service subscribes to receives AMQP 1.0 messages from EMS on behalf of a consumer. The validation service validates a detached digital signature and verifies the integrity of the message as well as the identity of the signer by sending a request to the SCVP server. Then, it forwards validated messages to the consumer.

2.8 To focus on the validation of technical and operational aspects for SWIM based trust framework, a scenario involving the FF-ICE filing service and notification service for pre-departure and departure phases of flight was applied. The scenario represented a Japan Airline (JAL) flight, JAL707X, from Narita International Airport (RJAA) to Bangkok Suvarnabhumi International Airport

(VTBS). In this scenario, the AEROTHAI and JCAB were FF-ICE capable ASPs (eASPs) and the JAL was an FF-ICE capable AU (eAU). For real application, the security service and the trust framework may not be implemented by all stakeholders at one step. To consider this mixed environment, the JAL did not implement the security service in this scenario.

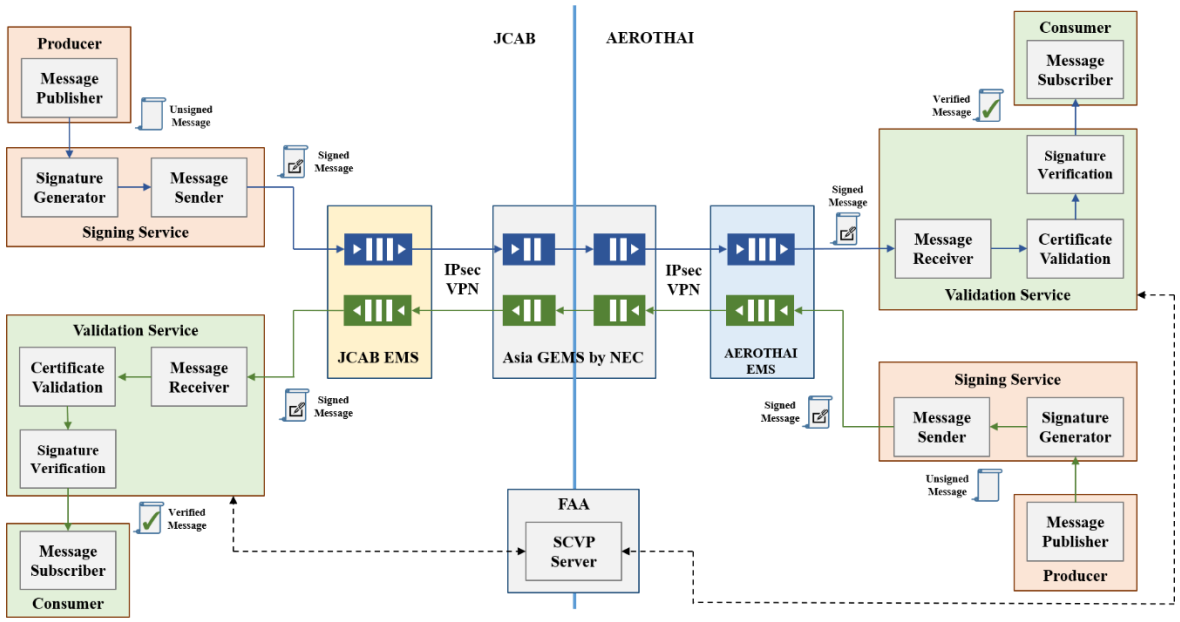

Figure 2. Message Exchange via Security Service

2.9 At first, we confirmed that the security service supports not only signed message exchange but also unsigned message exchange between different stakeholders with different capabilities. The JAL submitted a Filed Flight Plan message without signature to both eASPs. It is possible to configure the validation service to pass through the messages without signature to the consumer. As a result, the AEROTHAI's and JCAB's filing services replied Submission Response and Filing Status messages with digital signature to JAL. As a detached digital signature of the message body was attached as a message header, the JAL was able to process the original message body without any system change.

2.10 In addition, we validated that any modification during the message transition will cause the signature verification failure. In the demonstration, when the flight took off, the JCAB's notification service submitted the Flight Departure message through the signing service that signed the message with JCAB's certificate to AEROTHAI. Then, AEROTHAI received the message via the validation service that validated the JCAB's certificate and verified the signature of the message to ensure the message from the trusted producer and the integrity of the message. As the Java Messaging Service (JMS) was used by NEC for Pub/Sub messaging, the message transformation between AMQP and JMS was required. Due to the different message type, some transformation process modified the format of original message body, such as deleting the end control characters. Although this modification did not affect the content of the message, the signature verification failure would occur. In the real application, this problem should be addressed when constructing regional and global SWIM TI by connecting different EMSs provided by different parties.

2.11 It is generally agreed that the best security is a layered approach considering all participants in the system. The goal of any cybersecurity protection is to ensure the risk is reduced to an acceptable level. Based on the lessons learned from the development and demonstration of SWIM based trust framework aforementioned, the approaches to implement SWIM TI security functional capabilities and non-functional qualities are listed in Table.1.

Table 1. Approaches for SWIM TI Security Capabilities

Functional Capability	Non-functional Quality	Approach
Identity Management		· CA, SCVP
Authentication	Confidentiality, Accountability, Authenticity	· PKI
Authorization	Confidentiality	· Local EMS, GEMS
Cryptography	Integrity, Non-repudiation, Accountability	· Digital Signature · VPN, TLS
Key Management		· PKI
Audit		· Semantic Logging
Security Monitoring		· Visualization Tools
Policy Enforcement		· Local EMS, GEMS
Boundary Protection		· Firewall and EMS

2.12 Moreover, some considerations and observations for implementing SWIM TI security capabilities and SWIM based IATF are provided below:

1) To construct the PKI based IATF, it is required to define a global architecture and a common trust model between CAs of different States and regional PKI domains. Moreover, a trust principle or mechanism for certificate validation within domain and cross domain should be clarified.

2) From the concept of connected aircraft, not only the Ground/Ground SWIM security but also Air/Ground SWIM security should be considered to assure information exchanges in safety-critical applications.

3) With the advancement of wireless communications, mobile devises and cloud-oriented services, the traditional security boundaries of systems have been removed. This raises a number of challenges for protecting information exchange under such zero-trust environment. An adaptive, dynamic, multi-facet information security framework is expected.

4) During the transition period, some GEMS service providers are required to provide message validation and message transformation between different message formats and different versions of information exchange model. How to integrate these processes with the security service to avoid validation failure should be discussed.

3. CONCLUSION

3.1 Due to the fact that different States and regions have different security policies and governance, the common information security trust framework is required for all related stakeholders and organizations to be ablet to trust each other's identities. To achieve interoperability during the transition period, it requires solutions that can scale to not only achieve the security information exchange between multiple interconnected SWIM with various implementations and protocols but also protect the information exchange between legacy and SWIM-enable applications.

3.2 In next steps, the federated trust architecture between different CAs will be established to guarantee digital identities and security policies. Moreover, the solutions to integrate the security service with GEMS to assure information security between heterogeneous systems and applications will be discussed.

4. ACTION BY THE MEETING

4.1 The SWIM TF/5 is invited to:

a) Note and review the content of this working paper;

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

c) Discuss any relevant matters as appropriate.

– – – – – – – – – – – – – –