International Civil Aviation Organization

The Tenth Meeting of System Wide Information Management Task Force (SWIM TF/10)

Bangkok, Thailand, 20 – 23 May 2025

Agenda Item 5: Updates on the assigned tasks by task leads/contributors, including progress report and issues
b) SWIM Infrastructure – Task 3: Security Services

PRE-REQUISTES TO TRUST FRAMEWORK INSTANCE PARTICIPATION

(Presented by Singapore)

SUMMARY

This flimsy presents an update to the SWIM Task Force on the pre-requisites to the participation of any Trust Framework Instance and how SWIM Task Force Members can prepare for the eventuality of a SWIM Trust Framework Instance within the APAC region.

1. INTRODUCTION

1.1 Japan presented a paper, WP/15 Requirements for Implementing Aviation Information Security Framework at the APAC Region at the 10th meeting of ICAO APAC SWIM Task Force.

1.2 The paper described the requirements in implementing an aviation security framework. It references the work done by the ICAO Trust Framework Panel (TFP), ICAO Doc 10169: Aviation Common Certificate Policy (ACCP), and ICAO Doc 1024: Manual for Aviation Information Security (MAIS).

1.3 The paper also proposed the following:

- Considerations for PKI implementation within the APAC region;
- A working group or task force to looking into the development of a regional federated Public Key Infrastructure architecture; and
- A technical community to support the implementation of Trust Framework Instances (TFI), in which SWIM is just one of many potential use cases.

2. DISCUSSION

2.1 The TFP is in the midst of drafting a third document, known as the Trust Framework Manual (TFM). The purpose of the TFM, as drafted today, is to provide a guide in establishing, implementing and managing a TFI within the global aviation sector.

2.2 The TFM also serves to tie the two other materials produced by the TFP, ICAO Doc 10169 ACCP and ICAO Doc 10204 MAIS. The two documents serve as the pre-requisites to the usage of the TFM, and hence pre-requisites to the formation or participation of any TFI.

2.3 The ACCP helps establish assurance levels for the aviation sector, promoting interoperability across Certificate Authorities (CAs) and other PKI domains

2.4 The MAIS provides guidance to information system owners to implement information security objectives as defined in the MAIS.

2.5 As part of the requirements of any participation in any TFI, 2 major pieces of information from every organisation that wants to be part of any TFI are required:

- An organisation's Certificate Policy (CP). This is a set of rules that defines the issuance and management of digital certificates within a PKI, governing the trust relationships between entities.
- An organisation's Information Security Management System (ISMS). This is a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability through security controls and procedures.

2.6 The organisation's CP will be used to map against the ACCP. This is done to establish a baseline to check against for compliance in any TFI.

2.7 The organisation's ISMS will be used to map against the MAIS. This mapping is done to establish a baseline which provides insights as to whether an organisation's current security measures are sufficient for the organisation to be part of any TFI.

2.8 The current proposed standards in the TFM draft, which are still subjected to changes, for an organisation's CP are as follows:

- RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile
- ISO/IEC 9594-8 / ITU-T X.509 – Standard for defining certificates and public key infrastructure.
- ISO/IEC 27002 – Code of Practice for Information Security Controls
- NIST SP 800-57 - Recommendation for Key Management

2.9 The current proposed standards in the TFM draft, which are still subjected to changes, for an organisation's ISMS are as follows:

- ISO/IEC 27001 - Information Security Management Systems (ISMS) - Requirements
- ISO/IEC 27002 – Code of Practice for Information Security Controls
- ISO/IEC 27005 - Information security risk management
- ISO/IEC 27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 - Protection of personal data in the cloud

2.10 When an organisation completes the two mappings, they serve as the basis to determine if an organisation is able to be participate in any TFI.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) consider the status of their own organisation's Certificate Policy, and Information Security Management System;

c) discuss any relevant matter as appropriate

– – – – – – – – – – – – – – –