International Civil Aviation Organization

THE FIRST MEETING OF THE ANS INFORMATION ASSURANCE (ANSIA) TASK FORCE (ANSIA TF/1)

(Bangkok, Thailand, 28 – 30 January 2026)

Agenda Item 6: Issues and Challenges in implementation

DISCUSSION OF APAC REGIONAL TRUST FRAMEWORK IMPLEMENTATION

(Presented by JAPAN/ENRI)

SUMMARY

This working paper analyses a phased approach and technical models for implementing a trust framework using Public Key Infrastructure (PKI), and discusses the challenges for its implementation in the APAC region.

1. INTRODUCTION

1.1 To protect the safety of flight operations from cyber threats and ensure business continuity, a trust framework is required to ensure trusted information exchange between trusted identities through trusted communication paths within the aviation community. This means that in a digital environment, communication parties must be able to mutually authenticate each other, and the exchanged information must be protected from unauthorized modifications.

1.2 The Procedures for Air Navigation Services - Information Management (PANS-IM, Doc 10199) maintains that stakeholders processing, storing, consuming or transferring information shall implement an information security framework. This framework is designed to ensure the confidentiality, integrity and availability of the information and information services. It refers to the information security framework applying to the IPS-based network, the technical infrastructure, the information, the information service and the applications that process, use or distribute information.

1.3 In order to clarify the information security management for aviation safety management, the Manual on Aviation Information Security (MAIS, Doc 10204) has been published by the Trust Framework Panel (TFP). Moreover, to implement aviation information security framework, the Aviation Common Certificate Policy (ACCP, Doc 10169) for trusted identity management, and the Manual on Trust Framework for integrating different trust framework instances (TFIs) are being drafted by TFP working groups.

1.4 However, due to the varying operational requirements and implementation levels, several challenges exist in implementing a digital trust framework in the APAC region. As the technical infrastructure, the information, and the information service are included in the SWIM scope, related issues have been discussed within the APAC SWIM Task Force. In addition, a joint practical experience aimed at achieving secure, interoperable, and consistent implementation of a regional trust framework has been conducted by the SWIM Implementation Pioneer Group (SIPG). This working paper analyses a phased

approach and technical models for implementing a trust framework using Public Key Infrastructure (PKI), and discusses the challenges for its implementation in the APAC region.

2. DISCUSSION

2.1 As described in the MAIS, compared to other approaches, the Public Key Infrastructure (PKI) standard can provide a best practice for system-to-system authentication using digital certificates, secure data exchange with digital signatures, and encrypted communication through secure protocols. The ACCP defines the minimum requirements for PKI that participants must meet.

2.2 In the APAC region, deploying a PKI based trust framework for aviation requires a technical approach to ensure security, interoperability, and regulatory compliance. Based on practical experience, the following phased approach outlining the key steps should be considered to enable an interoperable PKI framework across multiple aviation stakeholders.

- Phase 1: Planning and Stakeholder Engagement
  - Define governance model and trust framework
  - Requirements analysis and use case definition
- Phase 2: Architecture and Design
  - Design a regional PKI architecture
  - Develop PKI policies and security measures
- Phase 3: Prototype and Testing
  - Develop and deploy a regional PKI System
  - Conduct interoperability testing
- Phase 4: Deployment and Operationalization
  - Scale deployment across aviation networks
  - Monitor, audit and continuous improvement
- Phase 5: Full Integration and Compliance
  - Integrate with other regions
  - Regulatory compliance and standardization

2.3 In the APAC region, to ensure interoperability among TFIs established in different member States, an appropriate technical infrastructure and governance structure are required for implementing a regional trust framework. As each member State has its own Certificate Authority (CA) and Trust Governance Authority (TGA), the following three models are being considered for implementing a regional trust framework by interconnecting national PKIs. Table 1 shows a comparison of these three models.

- Centralized Regional Root CA: A single regional root CA (or a small set under a single authority) issues or signs subordinate CAs for each member State.
- Decentralized National CAs: Each member State operates its own root CA, and participants trust national CAs directly. Interoperability is achieved through bilateral or multilateral trust agreements.
- Federated Bridge CA: National CAs remain operational, but a bridge CA acts as a trust broker that cross-certifies with national CAs or provides a metadata/trust registry, enabling relying parties to validate certificates across domains.

Table 1. Comparison of Three Models

Aspect	Centralized Regional Root CA	Decentralized National CAs	Federated Bridge CA
Trust model simplicity	High	Low	Medium
Political acceptability	Low	High	High
Single point of failure risk	High	Low	Low
Interoperability effort for endpoints	Low	High	Low
Governance complexity	Low	High	Medium
Revocation complexity	Centralized	Many endpoints	Centralized metadata + distributed revocation
Suitability for TFIs	Good - simple & uniform	Challenging - many trust anchors	Best trade-off - scalability & interoperability
Operational burden for operator	High	Distributed	Distributed

2.4 Given the varying levels of implementation among States, the federated bridge CA model is considered an appropriate approach to meet diverse requirements and ensure interoperability during the transition period. From a technical perspective, the federated bridge CA model avoids the single point of failure inherent in a centralized model, while at the same time preventing the complex management overhead associated with a fully decentralized model. To minimize endpoint complexity while preserving national control and maintaining efficient interoperability, it is recommended to define clear federation policies and profiles for different TFI, and to require each national CA to comply with minimal assurance and security standards when implementing the federated bridge CA model.

CONCLUSION

2.5 As the implementation of trust framework impacts all information systems in aviation, it is critical to ensure seamless integration with ATM systems, ATC systems, and airborne systems. The issuance and management of digital certificates for information entities (ATM Service Providers, Airspace Users, Information Services, and relevant devices) are essential to ensure the safety of flight operations. Furthermore, the use of digital signatures for cross-border and multi-regional message exchanges enhances data integrity and communication trust. Based on the discussions at TFP WG/3, the challenges and requirements outlined in Table 2 should be addressed and clarified to achieve effective national, regional and global integration.

Table 2. Challenges and Requirements

Changes	Requirements
Harmonization of regional trust framework: Since different regional implementations may have distinct trust framework, common procedures for establishing multiple bridge interconnections, and consistent governance for achieving end-to-end	· Governance for Bridge CA based certificate validation · Technical specification for Bridge CA management

certificate validation across regional bridges are required.	
Alignment of national security policies: As States maintain varying data protection and information security policies, a unified approach for message signing and validation using digital signature should be clarified.	· Governance for Bridge CA based message exchange · Technical specification for message signing and validation
Interoperability testing: Multi-regional interoperability testing and validation across multiple bridge participants are necessary to ensure coexistence and compatibility among mixed trust models.	· Governance for Bridge CA based regional operation · Technical specification for safety and security assessments

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matter as appropriate

– – – – – – – – – – – – –