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

REQUIREMENTS FOR IMPLEMENTING TRUST FRAMEWORK INSTANCES IN THE APAC REGION

(Presented by JAPAN/ENRI)

SUMMARY

This report details the required procedures for establishing and maintaining Trust Framework Instances across the Asia-Pacific region (APAC) in accordance with current Manual on Trust Framework.

1. INTRODUCTION

1.1 Trust Framework Panel (TFP) established three Working Groups – Identity Management (WG-IdM), Information Security (WG-IS), and Trust Framework Considerations (WG-TFC). WG-IdM compiled the Aviation Common Certificate Policy (ACCP, Doc 10169) based on the results of the discussion. WG-IS compiled the Manual on Aviation Information Security (MAIS, Doc 10204), and WG-TFC is discussing for Manual on Trust Framework and operational use cases. Manual on Trust Framework describes procedures for building and maintaining Trust Framework Instances (TFIs), to keep secure information exchange.

1.2 This paper reports requirements to implement Trust Framework Instance in the APAC region in accordance with the draft version of Manual on Trust Framework. Hereafter, we will refer the draft version of the manual as the "Manual on Trust Framework," or "the manual."

2. DISCUSSION

2.1 Establishing and maintaining a Trust Framework Instance (TFI) is essential for securely exchanging data using Public Key Infrastructure (PKI). Manual on Trust Framework describes what the TFI is, and how to establish and maintain the TFI.

2.2 Figure 1 illustrates an overview of the proposed lifecycle model to establish and maintain a single TFI with multiple participants. This model consists of four phases: Understand and Commit, Align and Build, Verify and Assess, and Sustain and Evolve. Activities associated with each phase are described below the corresponding phase. Please note that Figure 1 is still under discussion and may change.

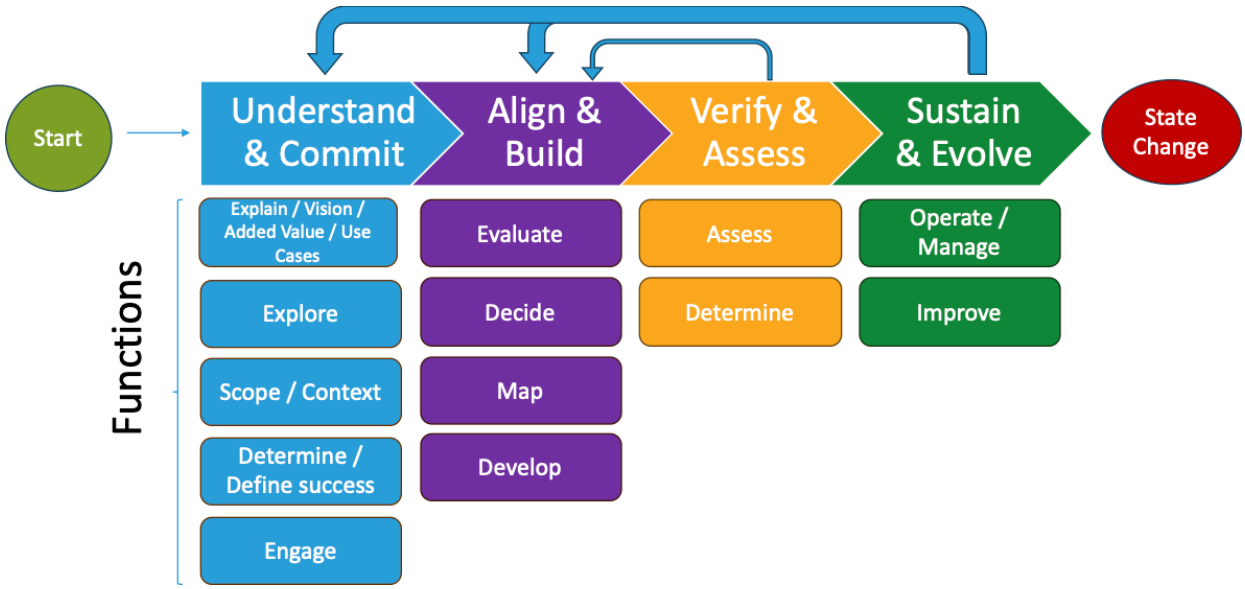

Figure 1: Proposed Trust Framework Instance Lifecycle Model

2.3 We categorized the 23 steps described in chapter 2 of the manual into items requiring attention at the national, regional, and global levels. The results are presented in Table 1. Table 1 assumes a three-level TFI structure (National-Regional-Global), similar to the European approach. However, a two-level TFI structure (National and International) may be more appropriate in some use case. For further detailed information, please refer to the manual.

Table 1: Steps and Requirements for a TFI

	Steps	National (Participants)	Regional	Global
1	Scope the TFI business use case and exchange Letter of Intent	Define the use cases and identify risks	Exchange Letter of Intent	
2	Map the ISMS to MAIS	List and evaluate MAIS requirements	Document and share findings	Develop MAIS
3	Map the Certificate Policy (CP) to the ACCP	Identity requirements and evaluate CP compliance	Document and share findings	Develop ACCP
4	Perform safety and security assessments	Conduct safety and information security risk assessments		
5	Identify TFI-Specific Requirements	Identify minimum requirements of PKI and information security		
6	Negotiate Protection Levels for exchanged information		Coordinate and agree baseline requirements	

7	Negotiate the draft TFI Agreement		Document TFI agreement	
8	Assign or elect Trust Governance Authority members and elect Chair		Assign or elect Trust Governance Authority members and elect Chair	
9	Nominate Identity and Security Working Group (IWG&SWG) Members		Nominate Identity and Security Working Group (IWG&SWG) Members	
10	Submit CP mapping to the IWG	Submit CP detailing how they meet the minimum requirements	IWG reviews, provides feedback, and validates the CP TGA approve the CP	
11	Submit ISMS mapping to the SWG	Submit ISMS detailing how they meet the minimum requirements of MAIS	SWG reviews, provides feedback, and validates the ISMS TGA approve the ISMS	
12 & 13	External or internal PKI assessment	Submit PKI assessment attestation	IWG reviews and approve	
14	Request IWG assessment (if needed)		TGA may request to submit different assessment to IWG	
15 & 16	External or internal ISMS assessment	Submit ISMS assessment attestation	SWG reviews and approve	
17	Request SWG assessment (if needed)		TGA may request to submit different assessment to SWG	
18	Signing multilateral agreement	Sign agreement		
19	Propose Trust Validation Anchor (TVA) implementation	Propose TVA implementation and establish TVA after TGA approval	IWG and SWG validate TVA TGA approves TVA	
20	Provide Trust Anchor	Provide trust anchor such as root and intermediate certificates, and certificate chains	IWG and SWG make trust information list	

		Publish the trust anchor after TGA approval	TGA reviews and approves trust list	
21	Provide level of protection for information	Set protection level for information	IWG and SWG validate the trust information list TGA reviews and approves the trust information list	
22	Propose cross-certificate policy mapping	Propose cross-certificate policy Establish Bridge CA and issue cross-certification after TGA approval	IWG and SWG review the cross-certification policy TGA evaluates and approves the cross-certification policy	
23	Designate interoperability lab(s)		Designate interoperability lab(s)	

2.4 The manual is still under discussion, and inconsistencies between Figure 1 and Table 1 remain. The APAC regional considerations for improving the procedure, as well as practical experiences to support implementation, are therefore expected.

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 such as governance or policy of TFIs in the APAC region

– – – – – – – – – – – – –