International Civil Aviation Organization

AVSECP/36-IP/4
6/3/25
English only

AVIATION SECURITY PANEL (AVSECP)

THIRTY-SIXTH MEETING

Hybrid meeting, 7 to 11 April 2025

Agenda Item 6: Other business

AVIATION SECURITY TRUST FRAMEWORK

(Presented by the Observer nominated by the International Air Transport Association – IATA)

INFORMATION PAPER

SUMMARY

The Aviation Security Trust Framework (ASTF) addresses new regulations requiring commercial aircraft operators to create and maintain Aircraft Operator Security Programmes (AOSPs) and Supplementary Station Procedures (SSPs). Developed by the International Air Transport Association (IATA), the ASTF leverages decentralized trust standards—like Verifiable Credentials and Digital Wallets—to streamline compliance, protect sensitive data, and unify disparate requirements across multiple jurisdictions. By issuing cryptographically verifiable approvals that can be verified without direct system integration, stakeholders can ensure document integrity during oversight activities while reducing risk and paperwork.

For more details, visit https://astf.iata.org.

Link to GASeP Global Priorities	Global Priority 4: Improve technological resources and foster innovation Global Priority 5: Improve oversight and quality assurance Global Priority 6: Increase cooperation and support

1. INTRODUCTION

1.1 New aviation security standards introduced in late 2022 require that aircraft operators develop, implement, and maintain their own Aircraft Operator Security Programmes (AOSPs) in alignment with State of Operator National Civil Aviation Security Programmes (NCASP) rules while also creating Supplementary Station Procedures (SSPs) for jurisdictions abroad, if required.

1.2 These updates are intended to strengthen global aviation security. Yet, the shift toward multiple interlinked security documents, often drafted separately and iterated over time, creates significant complexity. Tracking version control, ensuring cross-border alignment, and verifying document authenticity can quickly become impractical and vulnerable to gaps or inconsistencies in processes.

1.3 In parallel, the airline industry is embracing new paradigms of digital collaboration and data-sharing. National Civil Aviation Authorities (CAAs) and aircraft operators are exploring how to

manage security credentials efficiently and securely. Thanks to advances in cryptography, decentralized trust standards, and global initiatives such as the World Wide Web Consortium's Verifiable Credentials (VC) model, stakeholders see an opportunity to streamline these critical security processes while protecting vital, sensitive data.

1.4 Against this backdrop, the International Air Transport Association (IATA) proposes an Aviation Security Trust Framework (ASTF), a guiding structure for secure, decentralized information exchange that preserves organizational autonomy, enhances cross-jurisdictional trust, and meets the complex requirements of modern aviation security.

1.5 For more details, visit https://astf.iata.org. Which contains a white paper for review.

2. DISCUSSION

2.1 A centerpiece of the new regulations is the requirement for AOSPs and SSPs. Each aircraft operator must craft an AOSP that conforms to its State of Operator NCASP, detailing how it will prevent, detect, and respond to acts of unlawful interference. In each foreign jurisdiction, the aircraft operator's AOSP may need a localized in the form of a supplement (the SSP) to their original, one and only AOSP, if the host state's rules differ or impose additional requirements. However, these documents usually rely on paper-based or ad-hoc digital approaches, making updates and verification time-consuming and vulnerable to human error. Notwithstanding, mandatory oversight activities that could be partly completed remotely and prior to deployment in the field.

2.2 The proposed Aviation Security Trust Framework seeks to address these challenges through decentralized trust, building on open standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VC). Under this model, regulatory bodies like CAAs issue cryptographically verifiable approvals or certificates (e.g., AOSP Letters of Approval) as VCs. Once an operator receives a digitally signed AOSP Letter of Approval, it can store it in a secure "digital wallet" and present it on demand to National Security Authorities or airport authorities—no direct system integration with the issuing CAA is required. Verifiers, in turn, use trust registries and verifiable data registries to confirm that the issuer is legitimate, the credential is unaltered, and the aircraft operator still holds valid authorization.

2.3 Key enabling components include.

- **Verifiable Data Registries (VDRs)** to anchor essential cryptographic details, such as public keys and revocation lists, allowing third parties to confirm a document's authenticity and validity.
- **Trust Registries** to list which entities are authorized to issue credentials (e.g., which CAAs can issue official Letters of Approval).
- **Digital Wallets** that let holders manage and selectively share credentials with verifiers in a secure, user-controlled environment.

2.4 IATA envisions playing a central role by defining the governance, technical standards, and best practices that form the backbone of the ASTF. By weaving together decentralized trust standards with industry-specific security requirements, IATA aims to simplify compliance and bring consistency to AOSP and SSPs management across diverse jurisdictions.

2.5 Longer term, this approach could scale to other critical areas, including cargo security status, oversight auditing activities, personnel background checks, and standardization of security-related processes.

2.6 Ultimately, the ASTF aspires to create an ecosystem where stakeholders retain local autonomy while operating within a globally recognized structure that reduces fraud, inefficiency, and data management risks, even in challenging the need to produce SSPs.

— END —