Aviation Security Trust Framework

Enhancing aviation security through open Verifiable Credential Standards

White Paper

January 2025

With appreciation to Savita Farooqui, Lucy Yang, and Kaliya Young, consultants from Identity Woman in Business, who worked with the IATA team to develop the white paper.

Contents

1. Introduction 5
2. Background 6
2.1. NCASP, AOSP and SSP 6
2.1.1 Contents of documents 6
2.1.2 Letters of Approval / Acknowledgement 7
2.1.3 Document dependencies and version control 7
2.1.4 AOSP and SSP language support 8
2.2. Roles and responsibilities 8
2.2.1 Aircraft operator's responsibilities 8
2.2.2 Aircraft operator's Chief Security Officer (CSO) responsibilities 8
2.2.3 State of the Operator responsibilities 10
2.2.4 State of operations responsibilities 10
2.3. Current business processes 11
2.3.1 AOSP 11
2.3.2 SSP 13
2.4. Current challenges and opportunity 15
2.4.1 Challenges in AOSP and SSP creation and management 15
2.5. Opportunity to a more coordinated, scalable digital future 16
3. IATA's vision 17
4. Key concepts and technologies in digital trust 18
4.1. Key aspects of digital trust 18
4.2. Evolution of digital trust 18
4.2.1 Peer-to-peer trust 18
4.2.2 Centralized trust 19
4.2.3 Federated trust 19
4.2.4 Decentralized trust 19
4.3. Cryptographic techniques 20
4.3.1 Hashing 20
4.3.2 Message Authentication Codes (MACs) 20
4.3.3 Digital signatures and certificates 20
4.3.4 Encryption 21
5. Decentralized trust standards and technologies 22
5.1. Decentralized Identifiers (DID) 22
5.2. Verifiable Credentials (VC) 23
5.3. Distributed ledgers 25
6. Enhancing aviation security with decentralized trust technologies 26
6.1. Aviation Security Trust Ecosystem 26
6.2. Entities and roles 27
6.2.1 Issuer: CAA (A) 27
6.2.2 Holder: Aircraft Operator (A) 27
6.2.3 Verifier: NSA (A) 27

6.3. Key enabling components 27
6.3.1 Verifiable Data Registry - technical trust 27
6.3.2 Trust Registry - human trust 28
6.3.3 Digital Wallets 28
6.4. Chain of trust 29
6.4.1 From trusted organizations to authorized personnel 30
6.4.2 Binding security documents to VCs 31
7. Aviation Security Trust Framework (ASTF) 32
7.1. Initial trust establishment 33
7.1.1 Roles, responsibilities, and requirements 33
7.1.2 Onboarding participants to the Ecosystem 34
7.1.3 Facilitating recognition and trust among participants 34
7.2. Levels of Assurance (LoA) 34
7.3. Standardization and interoperability 35
7.3.1 Data structures and semantics 35
7.3.2 Credential profiles and cryptographic techniques 35
7.3.3 Data security and exchange protocols 35
7.3.4 Digital Wallet and Trust Registry requirements 36
7.4. Credential lifecycle management 36
7.5. Security and privacy 36
7.5.1 Technology infrastructure and operations 36
7.5.2 User authentication and authorization 37
7.5.3 Document security and versioning 37
7.5.4 Personal information and privacy 37
7.6. Compliance and risk management 37
7.6.1 Legal and regulatory compliance 37
7.6.2 Conformance profile and trust audits 37
7.6.3 Threat modeling and risk mitigation 38
7.7. Ecosystem governance 38
8. Potential IATA roles and service offerings 39
8.1. Developing and operationalizing ASTF 39
8.1.1 Developing the ASTF 39
8.1.2 Operationalizing the ASTF 39
8.2. Potential IATA service offerings 40
8.2.1 Trust Registry and notary services 40
8.2.2 Verification APIs and services 41
8.2.3 Fully managed trust services 41
9. Conclusion 42

1. Introduction

In the evolving landscape of global aviation security, new regulations introduced as of November 18, 2022, mark a significant step forward in safeguarding international air travel. These regulations are part of a broader initiative to ensure that commercial aircraft operators adhere to the stringent security standards outlined by National Civil Aviation Security Programs (NCASP).

Compliance with these regulations demands that aircraft operators establish an Aircraft Operator Security Program (AOSP) aligned with the security requirements of their home country (defined in the NCASPs) while also creating and maintaining Supplementary Station Procedures (SSP) to address specific security needs in other countries where they operate. The growing complexity of aviation operations calls for transformation of existing systems, which still heavily rely on paper and emails, to keep up to date with the evolving regulatory requirements and protect critical security documents and exchanges against advanced cyber threats. Such transformation necessitates collaboration between humans and organizations in both the physical and digital spheres across organizational and jurisdictional boundaries.

The aviation industry has historically been collaborative in defining standards and best practices, thanks to the coordination and facilitation led by organizations such as the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA). This strong foundation of trust and collaboration paves the way for trust building in an increasingly digitized world. It is important that IATA builds on what the organization has established and continues to be an enabler and connective tissue in bridging trust across boundaries and among aviation stakeholders in the digital world.

Fortunately, the advancement of modern cryptography and the emergence of global standards in digital trust, such as Verifiable Credentials (VC) and Decentralized Identifiers (DID) defined by the World Wide Web Consortium (W3C), inspire IATA to see a promising path to improving and securing digital processes for aviation security. This path is well aligned with what the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) has defined for simple, transparent, and effective processes for global commerce in its White Paper on eDATA Verifiable Credentials for Cross Border Trade. These emerging standards have been chosen to underpin critical digital infrastructures, such as the European Union Digital Identity Wallet, U.S. Digital Immigration Credentials, the United Nations Transparency Protocol for supply chain traceability, California mobile driver's license, and Bhutan's National Digital Identity.

The increasing adoption of emerging standards speaks to the individual, organizational, and jurisdictional needs for autonomy and control of their own digital presence and interactions, as well as improved security of the data associated with their digital activities. However, this doesn't invalidate their needs for convenience and interoperability with stakeholders. In the context of aviation security, it means enabling airlines and aviation stakeholders to share critical security information interoperably with each other with enhanced security and efficiency, while recognizing that they need agency over their own systems and processes.

As indicated in the ICAO Annex 15, trust and security in aviation extends beyond just verifying the identities and authorizations of organizations and their assigned personnel. It also involves ensuring that critical documents are genuine, unaltered, and originate from a reliable source by implementing appropriate cryptographic technologies such as encryption and digital certificates. By doing so, stakeholders can trust that the information contained within these documents is accurate, up-to-date, and has not been tampered with.

This white paper, by dissecting the current regulatory requirements, business processes, and roles and responsibilities in aviation security, proposes the creation of an **Aviation Security Trust Framework** to enable trusted interactions among aviation stakeholders in today's complex digital environment. It elaborates on how to build the framework on the existing collaborative foundation of aviation stakeholders and by leveraging emerging digital trust standards and infrastructures. It also explores the potentials roles and service offerings for IATA in facilitating and enabling trust across boundaries in aviation security.

2. Background

As of November 18, 2022, new aviation security regulations have been introduced, requiring airlines to develop, implement, and maintain Aircraft Operator Security Programs (AOSP) and Supplementary Station Procedures (SSP). These updates are part of broader efforts to enhance aviation security globally, ensuring that commercial aircraft operators meet the security standards outlined by National Civil Aviation Security Programs (NCASP) developed by Civil Aviation Authorities (CAA) of nation states.

To comply with these regulations, an aircraft operator must establish an Aircraft Operator Security Program (AOSP) that aligns with the security requirements of the country where they are based (State of the Operator[1]). Additionally, the aircraft operator needs to create and maintain Supplementary Station Procedures (SSP), which are supplementary procedures attached to the AOSP, to address any specific security requirements of other countries where they operate (States of operations) that are not covered in the original AOSP. The interdependency of these documents can be seen in the Figure 1 below:

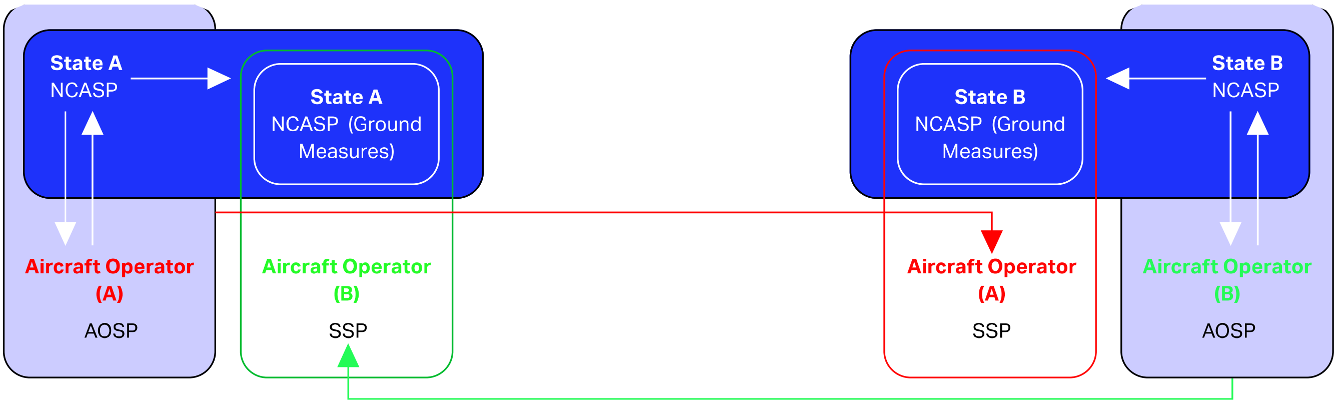


Figure 1 - Interdependency of aviation security documents

In addition to the development and implementation of AOSPs and SSPs, there is a growing emphasis on digitally transforming the creation, use, and ongoing updates of critical aviation security documents as well as how they are shared, exchanged, and verified across organizational, jurisdictional, and sectoral boundaries.

2.1. NCASP, AOSP and SSP

2.1.1 Contents of documents

A NCASP, developed by a Civil Aviation Authority (CAA), outlines a state's approach to ensuring aviation security and includes the following in the NCASP documents and guidelines for aircraft operators:

- The regulatory framework for stakeholders in aviation security and their roles and responsibilities.
- Security measures and procedures for threat prevention, detection, and response.
- Guidelines for training, oversight, and crisis management.
- Coordination mechanisms between entities for compliance with global aviation security standards.

[1] An airline may lease aircrafts from an aircraft operator based outside the airline's home country. In such case, the home country of the aircraft operator is called the 'State of Registry'. For simplicity of the use case discussion, the white paper doesn't address this situation.

Aircraft operators create AOSP documents that include key elements to ensure compliance with the requirements outlined in their home country (State of the Operator)'s NCASP. Specifically, an aircraft operator's AOSP, directly or by reference, includes:

- Security measures and procedures specific to the aircraft operator, ensuring compliance with the NCASP of their State of the Operator.
- Protocols for safeguarding passengers, crew, aircraft, and cargo against unlawful interference.
- Guidelines for implementing and maintaining security practices, both domestic and international.
- Procedures for coordination with relevant national and international security authorities.
- Documentation and reporting processes for security incidents and regular audits.

Aircraft operators also create SSP documents based on the requirements outlined in the NCASPs of any foreign countries where they operate (States of operations). The SSPs include:

- Additional security procedures that supplement the AOSP for specific airports or stations.
- Tailored security measures to address unique requirements or risks at specific locations.
- Coordination protocols with local authorities and airport operators to ensure alignment with the NCASPs of the States of operations.
- Procedures for adapting and updating security practices to meet local regulations and conditions.
- Documentation and reporting processes for compliance and incident management at each airport.

States and CAAs may provide model AOSPs, templates, and guidelines to assist aircraft operators in developing their AOSP and SSP documents that follow the guidance provided in the ICAO Aviation Security Manual (Doc 8973), particularly its Appendix 24 on AOSP and SSP. These resources can help reduce the administrative burden on aircraft operators, streamline the document approval process, and enhance the transparency and alignment of aviation security measures with NCASPs. As recommended by ICAO, these models should also be open to contributions and adaptations to meet specific needs.

2.1.2 Letters of Approval / Acknowledgement

After aircraft operators create their AOSP and SSP documents, they submit them to the relevant national and/or international authorities for review and approval. The authorities may provide feedback and request revisions. Once authorities approve the documents, an AOSP and/or SSP Letter(s) of Approval will be issued. These certificates (Letters of Approval), along with the approved documents, should also be versioned, so that each certificate is clearly associated with the version of the documents that are approved for the certificate.

Currently, the issuance of these certificates, though asked for in the ICAO guidance material, is not consistently practiced, making verifications of these certificates and documents hard to manage.

2.1.3 Document dependencies and version control

Keeping track of NCASP, AOSP, and SSP document versions is crucial for maintaining alignment with evolving threats and regulations in aviation security. These documents are interconnected, so changes in one often require updates to the others, as illustrated below (see Figure 2). Effective versioning along with linking the right versions of dependent documents is necessary to ensure consistency, compliance, and a reliable audit trail.

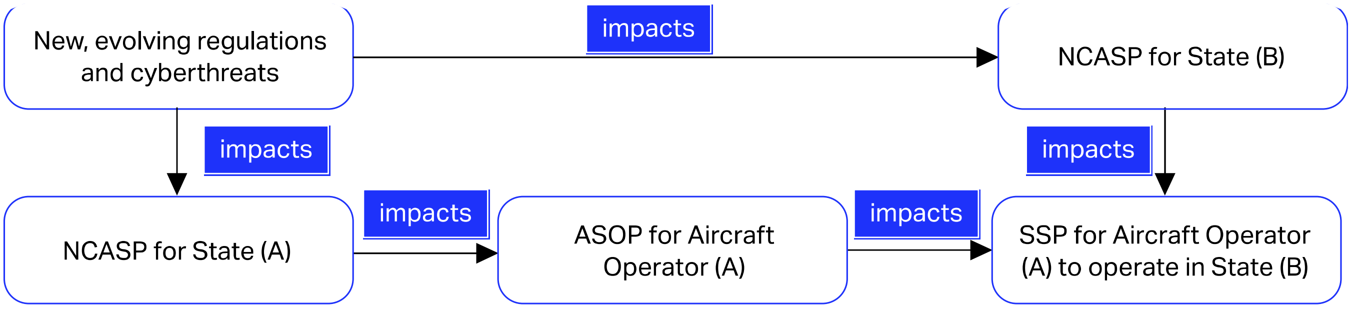

New, evolving regulations and cyberthreats
impacts
NCASP for State (B)
impacts
impacts
NCASP for State (A)
impacts
ASOP for Aircraft Operator (A)
impacts
SSP for Aircraft Operator (A) to operate in State (B)

Figure 2 - Impact of evolving regulations and cyber threats on aviation security documents

2.1.4 AOSP and SSP language support

An AOSP is usually developed in the language of the State of the Operator. It also needs to be provided in English for understanding and recognition by states other than the State of the Operator, as well as for regional and international security audits and inspections. SSPs are usually developed in the languages of both the State of the Operator and the States of operations. SSPs may also be made available in English.

2.2. Roles and responsibilities

2.2.1 Aircraft operator's responsibilities

To fulfill aviation security obligations under the ICAO Annex 17, NCASPs, and associated regulations, a commercial aircraft operator should carry out the following responsibilities[2]:

- Establish, implement, and maintain an AOSP that meets the requirements of the NCASP of the State of the Operator. In the AOSP, the aircraft operator should develop its own security requirements, procedures, and instructions, and ensure that their security programs and operations manuals are consistent with the laws and regulations of the State of the Operator.
- Develop, implement, and maintain SSPs that meet the requirements of the NCASPs of the States of operations. The aircraft operator should develop SSPs addressing requirements in their States of operations' NCASPs that are not addressed in the AOSP.
- Share their AOSP, upon request, with the State of the Operator and States of operations in accordance with relevant requirements pertaining to the distribution of sensitive aviation security information. As restrictions in the sharing of such documents may apply, the aircraft operator remains obligated to protect sensitive information from any unauthorized disclosure.
- Appoint a security manager with a professional security background and familiar with commercial air transport operations as Chief Security Officer or Head of Security. The security manager should be a senior executive or an individual with direct access to the top management. The person should be afforded sufficient authority to ensure the full implementation and enforcement of the AOSP and SSPs and will serve as the primary point of contact to receive NCASP documents. The person or their accountable manager works with CAAs to understand and follow the required administrative processes and create and seek approval of AOSP and SSP documents.

2.2.2 Aircraft operator's Chief Security Officer (CSO) responsibilities

The position of **Chief Security Officer** (CSO) or **Head of Security** has been established in the IATA Operational Safety Audit (IOSA) Standards Manual (ISM) since its inception in 2003. The CSO shall be responsible for the development, implementation, and maintenance of the Security Program (SEC 1.2 in ISM/1).

[2] **Reference: Doc 8973_AOSP+SSP_PUBLIC.pdf from AOSP and SSP (icao.int).**

With the introduction of the concept of Security Management System (SeMS) in the second edition of ISM (2007), the responsibilities of the CSO were developed such as:

- Formulate an overall security policy for senior management acceptance.
- Develop and promulgate security standards and practices to provide guideline.
- Establish a clear order of command in the security structure.
- Ensure effectiveness of security programs by regular evaluation and inspection.
- Liaise with governments, authorities, and law enforcement agencies.
- Ensure an effective risk analysis, threat assessment, and response capability.
- Initiate special security measures during periods/instances of increased threat.
- Provide specialized advice to senior and line management in all security functions.

IMS Edition 17 (January 2025) indicates that a Head of Security shall be responsible for ensuring:

- Implementation and maintenance of the AOSP (and its associated SSPs).
- Operations are conducted in accordance with conditions and restrictions of the AOSP and in compliance with applicable regulations and standards of the State of the Operator.

On the ICAO side, the position of CSO was introduced in the 7th Edition of the Aviation Security Manual (Doc 8973) and remained until the 12th Edition (2020). In the last Edition (13th in 2022), the position was renamed "**security manager**" with a direct communication with and/or report to an aircraft operator's Chief Executive Officer, Chief Operating Officer, and senior operations officers. The public ICAO guidance on AOSP and SSP develops on aircraft operator security managers' responsibilities:

- Develop and maintain an aircraft operator's overall security policy for approval by senior management.
- Develop and promulgate company-wide security standards and practices.
- Conduct security threat and risk assessments and management for all operations, which should be based on available information, including direct information collected by the operator, and appropriate threat and risk information received from the relevant authorities of the State of the Operator, the States of operations, as well as from other aircraft operators and relevant aviation security service providers.
- Develop or modify the AOSP and SSPs to correct deficiencies as necessary, and to comply with national laws and regulations of the States of operations.
- Ensure the AOSP and SSPs are current and have been endorsed by the accountable executive and submitted to the appropriate authority for verification and approval.
- Ensure the continuing effectiveness of the AOSP and SSPs through regular evaluations and inspections, and by encouraging internal security audit processes (internal quality control functions).
- Establish and maintain effective liaison with all relevant authorities and stakeholders to contribute to the industry's development of security systems and to comply with statutory requirements, taking into consideration the responsibilities of other relevant authorities with security functions.
- Maintain effective liaison with other departments of the aircraft operator, and especially senior management, to facilitate the implementation of effective security measures throughout the company.
- Advise on and managing all security systems in use by the aircraft operator and advise senior management on all aspects of security.
- Promote security awareness, culture, and vigilance.
- Ensure an effective response by the aircraft operator to any threat or security incident.
- Initiate special security measures during periods of increased risk and/or for critical flights and routes.
- Maintain familiarity with applicable aviation security-related legislation and regulations in the states served by the aircraft operator.
- Maintain a record of all unauthorized weapons or suspect explosive devices detected on the aircraft operator's aircraft or on the property used by the aircraft operator.

- Report all actual or suspected security occurrences (which may include security incidents or acts of unlawful interference) with aircraft operations to the appropriate authority[3].

2.2.3 State of the Operator responsibilities

This section describes the responsibilities of a State of the Operator to fulfill obligations under the Annex 17[4]:

- Share with aircraft operators based in its territory the NCASP and/or relevant information to enable them to meet the national requirements of their appropriate authorities. The State of the Operator should also share, in a practical and timely manner, any relevant information that could impact the risk assessments relating to an aircraft operator's operations.
- Ensure that aircraft operators' AOSPs meet the requirements of the NCASP. To achieve this, the State of the Operator, under its national legislation and/or policy, may consider the need to formally approve AOSPs and/or subject them to appropriate review or verification processes based on established procedures. The State of the Operator should ensure that aircraft operators are aware of the policy and applicable processes for AOSPs.
- Establish a means to confirm their approval, review, or verification of AOSPs and provide such acknowledgement to aircraft operators, e.g. issuance of Letters of Approval. The State of the Operator, when providing acknowledgment, should consider including information such as aircraft operator accountable manager, reference # of the AOSP, date of approval of the AOSP, validity if applicable, accountable official from the State of the Operator, reference of the NCASP used for compliance, and a confirmation that national requirements are met.
- May develop a model AOSP (including templates, guidelines) to be used by aircraft operators as their AOSP and/or SSPs. Such models may help reduce the bureaucracy of the document approval process and contribute to the transparency of aviation security measures. These models, as recommended by ICAO, should be opened for contributions and adaptations.

2.2.4 State of operations responsibilities

This section describes the responsibilities of a State of the operations to fulfill obligations under the Annex 17[5]:

- Share with aircraft operators operating in its territory, in advance of their commencement of operations, the appropriate parts of the NCASP and/or relevant information to enable them to meet the NCASP requirements. The State of the operations should also share, in a practical and timely manner, any relevant information that could impact the risk assessments relating to an aircraft operator's operations.
- Request foreign aircraft operators to establish, implement, and maintain written SSPs that meet the NCASP requirements of the State of the operations.
- Either formally approve, review, or verify SSPs, or provide such acknowledgment to aircraft operators once the verification process is complete, e.g. Letters of Approval / Acknowledgement.
- May request, in lieu of requesting SSPs, the acknowledgement that an aircraft operator's AOSP has been approved, reviewed, or verified by their State of the Operator.
- May develop model programs to be used by aircraft operators as their SSPs. Such models may help reduce the bureaucracy of the document approval process and contribute to the transparency of aviation security measures. These models, as recommended by ICAO, should be opened for contributions and adaptations.

[3] More information can be found from ICAO's Incident Reporting Guidance and Taxonomy.
[4] Reference: Doc 8973_AOSP+SSP_PUBLIC.pdf from AOSP and SSP (icao.int).
[5] Reference: Doc 8973_AOSP+SSP_PUBLIC.pdf from AOSP and SSP (icao.int).

2.3. Current business processes

2.3.1 AOSP

This section describes the current process for the creation and updates of AOSPs (see Figure 3). The CAA (A) is responsible for creating the NCASP (A) in compliance with the State (A)'s laws, regulations, and policies and providing templates and guidance for aircraft operators based in the State (A), such as Aircraft Operator (A), to create compliant AOSPs to be reviewed and checked by National Security Authority (A). The CAA (A) also verifies AOSPs and approves them.

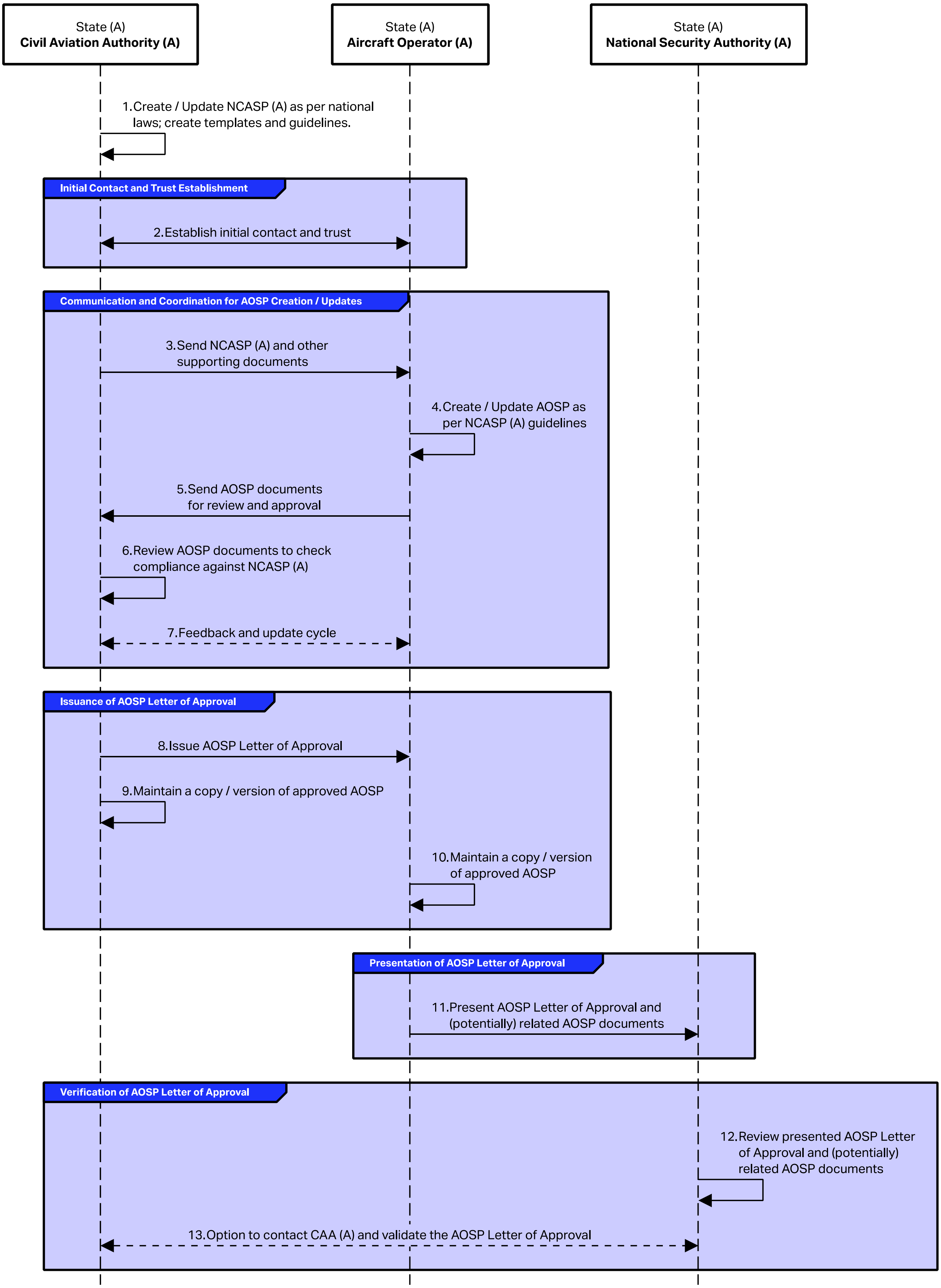

State (A)
Civil Aviation Authority (A)
State (A)
Aircraft Operator (A)
State (A)
National Security Authority (A)
1. Create / Update NCASP (A) as per national laws; create templates and guidelines.
Initial Contact and Trust Establishment
2. Establish initial contact and trust
Communication and Coordination for AOSP Creation / Updates
3. Send NCASP (A) and other supporting documents
4. Create / Update AOSP as per NCASP (A) guidelines
5. Send AOSP documents for review and approval
6. Review AOSP documents to check compliance against NCASP (A)
7. Feedback and update cycle
Issuance of AOSP Letter of Approval
8. Issue AOSP Letter of Approval
9. Maintain a copy / version of approved AOSP
10. Maintain a copy / version of approved AOSP
Presentation of AOSP Letter of Approval
11. Present AOSP Letter of Approval and (potentially) related AOSP documents
Verification of AOSP Letter of Approval
12. Review presented AOSP Letter of Approval and (potentially) related AOSP documents
13. Option to contact CAA (A) and validate the AOSP Letter of Approval

Figure 3 - Current ASOP business process

At a high level, the process involves the following steps:

1. The CAA (A) creates, maintains, and updates the NCASP (A) in accordance with national laws, regulations, and policies. The CAA (A) also establishes the AOSP requirements, and in some cases, provides templates and guidance for aircraft operators to ensure their AOSPs comply with the NCASP (A).
2. Before providing the appropriate parts of its NCASP (A) to Aircraft Operator (A), the CAA (A) establishes a basic trust relationship with the Aircraft Operator (A). This may involve conducting checks and verifications to confirm the legitimacy of the Aircraft Operator (A), ensuring that they have appointed a CSO who possesses the necessary security clearances and sufficient authority to create, update, and implement an AOSP.
3. The CAA (A) designated officer sends the NCASP (A) to the Aircraft Operator (A)'s CSO.
4. The Aircraft Operator (A)'s CSO leads the creation or updates for the AOSP as per the NCASP (A) guidelines.
5. The (updated) AOSP is sent to the CAA (A) for review, verification, and/or approval.
6. The CAA (A) reviews the AOSP for compliance against the NCASP (A) and other documents provided by the CAA (A).
7. The CAA (A) may send feedback to the Aircraft Operator (A)'s CSO, who will update the AOSP to address the feedback, leading to a newer version of the AOSP. This iterative review and feedback process may continue until the CAA (A) approves the AOSP or confirms its compliance with the NCASP (A) requirements.
8. Once the CAA (A) validates that the AOSP meets the NCASP (A) requirements, the CAA (A) issues a Letter of Approval to the Aircraft Operator (A) as an endorsement of the approved AOSP. This process is not standardized across states, and not all states issue Letters of Approval for approved AOSPs.
9. The CAA (A) may maintain different versions of Aircraft Operator (A)'s AOSP documents.
10. The Aircraft Operator (A) may maintain different versions of the AOSP documents themselves.
11. The Aircraft Operator (A) holds the AOSP Letter of Approval in its possession and presents it to the National Security Authority (A) when required. The Aircraft Operator (A) may be asked to present both the AOSP Letter of Approval and the associated AOSP documents for review and verification by the National Security Authority (A).
12. The National Security Authority (A) review the AOSP Letter of Approval (and the associated documents) presented by the Aircraft Operator (A).
13. The National Security Authority (A) may contact the CAA (A) to make sure that Aircraft Operator (A) presents the AOSP documents approved by the CAA (A). The process for verifying the validity of the ASOP Letter of Approval and/or associated documents is not currently standardized across states.

2.3.2 SSP

This section outlines the current process for creating and updating SSPs (see Figure 4). The CAA (B) oversees civil aviation security and related administrative processes in State (B). For aircraft operators not based in but working within State (B)'s territory, such as Aircraft Operator (A), CAA (B) is responsible for providing them relevant parts of their NCASP and any other necessary information or guidelines. This ensures that aircraft operators can meet the national requirements of State (B) and can satisfy the review and verification of the National Security Authority (B). The information must be shared with the aircraft operators before they begin their operations in State (B).

The Aircraft Operator (A) is required to submit its AOSP to CAA (B). They must also assess any gaps between their AOSP and NCASP (B). Based on this assessment, the Aircraft Operator (A) needs to develop SSP for State (B).

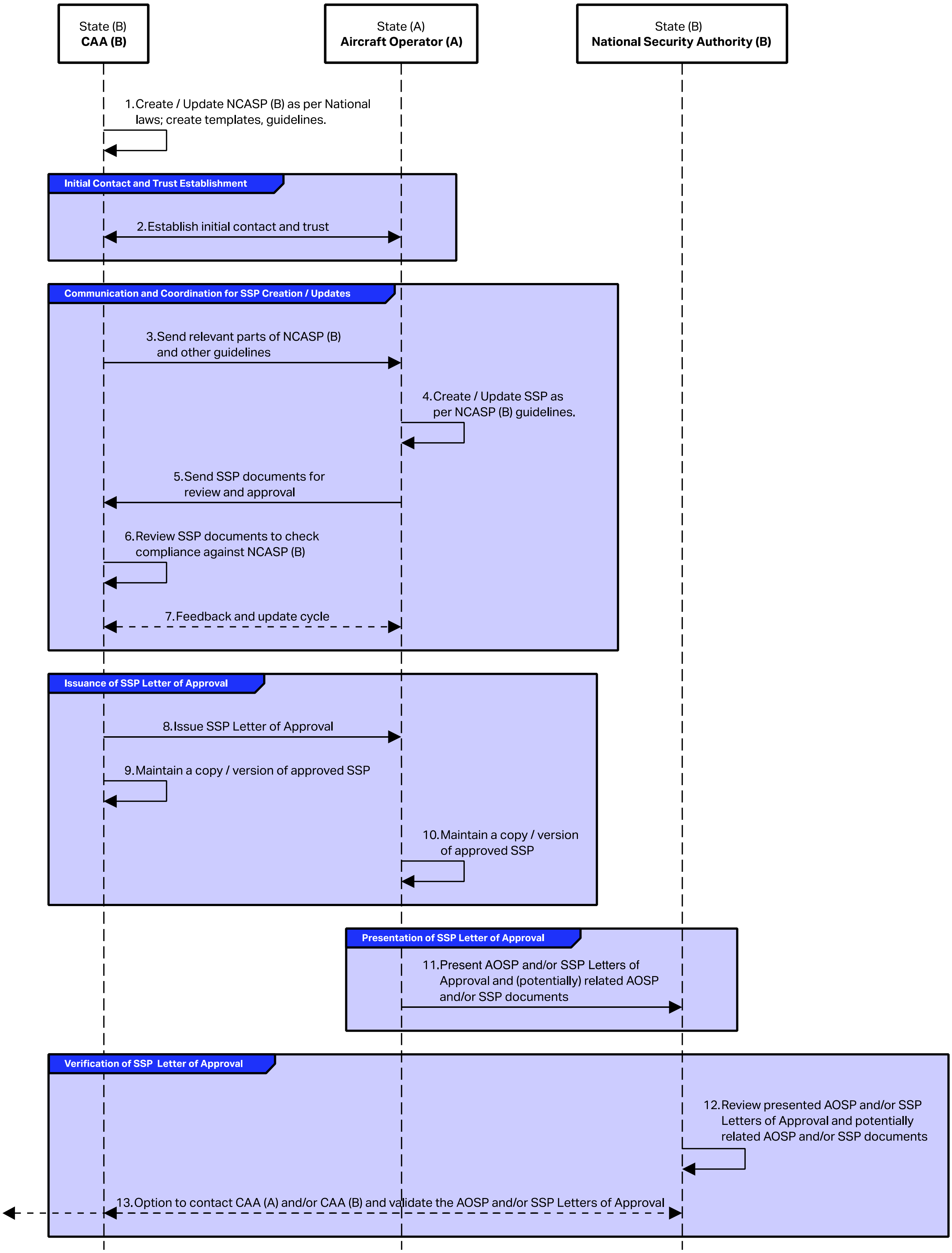

State (B)
CAA (B)
State (A)
Aircraft Operator (A)
State (B)
National Security Authority (B)
1. Create / Update NCASP (B) as per National laws; create templates, guidelines.
Initial Contact and Trust Establishment
2. Establish initial contact and trust
Communication and Coordination for SSP Creation / Updates
3. Send relevant parts of NCASP (B) and other guidelines
4. Create / Update SSP as per NCASP (B) guidelines.
5. Send SSP documents for review and approval
6. Review SSP documents to check compliance against NCASP (B)
7. Feedback and update cycle
Issuance of SSP Letter of Approval
8. Issue SSP Letter of Approval
9. Maintain a copy / version of approved SSP
10. Maintain a copy / version of approved SSP
Presentation of SSP Letter of Approval
11. Present AOSP and/or SSP Letters of Approval and (potentially) related AOSP and/or SSP documents
Verification of SSP Letter of Approval
12. Review presented AOSP and/or SSP Letters of Approval and potentially related AOSP and/or SSP documents
13. Option to contact CAA (A) and/or CAA (B) and validate the AOSP and/or SSP Letters of Approval

Figure 4 - Current SSP business process

The overall process involves the following steps:

1. The CAA (B) creates and maintains the NCASP (B) in accordance with national laws, regulations, and policies.
2. For a foreign Aircraft Operator (A) operating in State (B), the CAA (B) establishes basic trust with the Aircraft Operator (A). This may include conducting checks to verify the Aircraft Operator (A)'s legitimacy and ensuring they meet essential requirements, such as appointing a CSO. The CAA (B) will request and verify that the Aircraft Operator (A) has approved AOSP from its State of the Operator. In some cases, an existing friendly and trusted diplomatic relationship between State (A) and State (B) may need to be in place for a foreign Aircraft Operator (A) to operate in State (B).
3. The CAA (B) designated officer sends the relevant parts of the NCASP (B) to the Aircraft Operator (A)'s CSO and provides guidance for creating and/or updating the SSP. The SSP can either be an amendment to the AOSP or a separate document (or set of documents), while still preserving references to the relevant AOSP/NCASP documents.
4. The Aircraft Operator (A)'s CSO leads the creation or updates of the SSP as per the NCASP (B) guidelines.
5. The (updated) SSP is sent to the CAA (B) for review and approval.
6. The CAA (B) reviews the SSP for compliance against the NCASP (B) and other related documents.
7. The CAA (B) may send feedback to the Aircraft Operator (A)'s CSO, who will update the SSP to address the feedback, leading to a newer version of the SSP. This iterative review and feedback process may continue until the CAA (B) approves or validates the SSP for the Aircraft Operator (A).
8. Once the CAA (B) validates that the SSP meets the NCASP (B) requirements, the CAA (B) issues a SSP Letter of Approval to the Aircraft Operator (A) as an endorsement of the approved SSP. This process is not standardized across states, and not all states issue Letters of Approval for approved SSPs.
9. The CAA (B) may maintain different versions of Aircraft Operator (A)'s SSP documents.
10. The Aircraft Operator (A) may maintain different versions of the SSP documents themselves.
11. The Aircraft Operator (A) holds the SSP Letter of Approval and presents it to National Security Authority (B) when required. The Aircraft Operator (B) may be asked to present both the AOSP and SSP Letters of Approval and the associated AOSP and SSP for verification by the National Security Authority (B).
12. The National Security Authority (B) verify the Letters of Approval (and associated AOSP and SSP source documents) presented by the Aircraft Operator (A).
13. The National Security Authority (B) may contact the CAA (A) and/or CAA (B) to make sure that the Letters of Approval and AOSP and/or SSP documents presented by Aircraft Operator (A) were approved by the CAA (A) and CAA (B). The process for verifying the validity of the Letters of Approvals and/or associated documents, particularly cross-border verifications, is not standardized across states.

2.4. Current challenges and opportunity

Although the new aviation security regulations were intended to enhance global aviation security, they entail new challenges in the creation and management of these documents. These challenges, if not properly addressed, may undermine the intended outcomes of the new regulations.

2.4.1 Challenges in AOSP and SSP creation and management

2.4.1.1 Regulatory challenges

- **Regulatory compliance and consistency**: Ensuring that AOSP and SSP documents align with diverse national and international regulations can be complex and time-consuming, especially when different countries have varying security requirements.
- **Regulatory oversight and fraud risk**: Airport and aircraft operators are subject to mandatory oversight by regulators and/or other industry bodies. These audit and inspection processes involve extensive manual verification of documentation and are prone to document fraud.

2.4.1.2 Financial challenges

- **Resource and cost constraints:** Smaller aircraft operators and countries with limited resources may struggle with the administrative burdens, resources, and costs involved to develop and maintain comprehensive NCASPs, AOSPs, and SSPs and associated documents, particularly to keep the documents updated and aligned with the latest security standards.

2.4.1.3 Operational challenges

- **Complexity of customization:** While AOSPs provide a general framework, SSPs need to be tailored to specific locations and operations. Customizing these procedures without compromising overall consistency is challenging.
- **Cumbersome version maintenance:** The security landscape constantly evolves, necessitating frequent updates to AOSP and SSP documents. Keeping these documents current, maintaining versions, and ensuring all stakeholders are aware of and implementing the latest procedures is a continuous challenge.
- **Coordination among stakeholders:** Effective creation and implementation of AOSPs and SSPs requires close coordination among various stakeholders, including aircraft operators, national authorities, airport operators, and security agencies. Ensuring seamless communication and collaboration, particularly across countries and regions with diverse regulations, can be challenging.
- **Time consuming and error-prone manual processes:** The absence of a standardized, streamlined way to create and maintain aviation security documents and verify validity of the documents can be time consuming and error-prone. This leads to longer approval timelines for these documents and burdensome verification processes across organizations and borders.

2.5. Opportunity to a more coordinated, scalable digital future

To address some of the above-mentioned challenges, national authorities and aircraft operators have started implementing digital solutions to support the evolution of aviation security operations. However, these solutions are often developed independently without following a common set of requirements, standards, processes, and/or criteria, resulting in siloed systems that fall short in facilitating the critical cross-organization, cross-border processes. As more stakeholders join along the digital transformation journey, these siloed systems without a common ground will make it hard for trust to be established or digital processes to scale.

In a multi-stakeholder environment, the lack of a unified approach to digitization can lead to significant inefficiencies, reinforce distrust between government and industry, and create potential security gaps. While most aviation security stakeholders are just starting the process of digital transformation, it is time for the aviation security industry to come together and align on a common path that defines:

- **Common structures and standards for critical security documents** to allow these documents to be exchanged and verified interoperably and efficiently across systems and borders regardless of what system each stakeholder is using, similarly to how people can use different email programs to write and receive emails today.
- **Common security policies and protocols to share and exchange security documents,** giving aviation security stakeholders comfort and confidence that their critical security documents are being handled securely in the digital realm when they are out of their hands, and they are getting genuine, valid and untampered documents from others.
- **Common processes and criteria to establish trusted connections among stakeholders** so that they can always be assured of the legitimacy and authority of the organizations and relevant personnel they are dealing with and that the documents they are sending to or receiving from are from who they say they are and who have the authority to deal with the documents.

These common standards, policies, protocols, processes, and rules are often described in a “Trust Framework” for entities to build, scale trust in the digital world.

3. IATA's vision

While the aviation regulations provide the framework for security programs, IATA has been playing a crucial role in supporting airlines to meet their obligations. Through its Security Management System (SeMS) framework, IATA helps airlines implement risk-based and data-driven security measures. IATA also provides guidance, organizes workshops, and offers resources that assist airlines in navigating and complying with both international and national aviation security regulations.

Recognizing the current challenges in implementing the security standards outlined in the Annex 17, IATA has identified a window of opportunity to create an Aviation Security Trust Framework (ASTF), which will lay the critical groundwork for the aviation security industry to manage and exchange information in a secure and trusted manner across systems and borders before digital transformation gaps become too wide among stakeholders. The ASTF will establish clear standards and secure practices to offer aviation security stakeholders a path towards a more coordinated digital future without compromising their autonomy and control of their existing systems and processes.

This white paper is intended to propose the core components of the ASTF by addressing the initial use case - the creation, maintenance, approval, and verification of AOSPs and SSPs. The goal is to eventually eliminate SSPs altogether by allowing the same AOSP to be evaluated and accepted in all countries as originally created. The ASTF may expand to encompass other areas of aviation security where trust building and interoperability is required across organizations and jurisdictions, but it is considered future work and not within the scope of the white paper. Such future work may include:

- The "security status" that should be maintained throughout the cargo supply chain.
- The background checks of airline security managers that need access to different national requirements in all the States of the operations for producing SSPs.
- The technical certifications of screeners or security managers that operate in different states.

4. Key concepts and technologies in digital trust

Digital trust refers to the confidence that stakeholders (individuals and/or organizations) have in digital systems, particularly whether these systems protect their interests to the extent they should. It encompasses not just the assurance that digital processes operate correctly, but also that identities, data, and documents are handled safely and protected against misuse or fraud in the processes.

In aviation, securely managing and sharing critical security information across systems and borders, such as NCASP, AOSP, and SSP documents, plays a crucial role in building and scaling trust among stakeholders. It goes beyond verifying the identities of organizations and personnel who are managing the information; it also involves ensuring that these essential documents are genuine, unaltered, and come from a trusted source.

4.1. Key aspects of digital trust

To build a safe and secure digital environment that can nurture trust, addressing the following aspects is key:

- **Veracity:** Verifying the identities of organizations and relevant personnel involved in digital transactions, making sure all parties are properly vetted, authenticated before accessing data.
- **Non-repudiation:** Having measures in place to ensure non-repudiation, whereby parties involved cannot deny their role and/or participation in a digital transaction.
- **Data authenticity and integrity:** Ensuring that all information—whether organizational/personnel information or important documents like NCASP, AOSP, and SSP—is accurate and remains unchanged. This includes verifying that data is coming from stated sources and guaranteeing that data is not altered or tampered from creation to receipt.
- **Confidentiality and proper access:** Protecting sensitive and confidential information from unauthorized access, leakage or misuse. For aviation documents, this means ensuring they are accessible only to those who are authorized and have security measures to prevent unauthorized disclosure or misuse.

By ensuring the veracity of identities and integrity, authenticity, and confidentiality of data and documents, digital systems can provide the necessary assurances for safe and secure aviation operations.

4.2. Evolution of digital trust

Ways to establish trust have evolved significantly as our digital footprints expand. Understanding the evolution of digital trust models is important as earlier models still and will co-exist with new ones.

4.2.1 Peer-to-peer trust

Historically, trust has been established through direct peer-to-peer connections between two or a small number of parties through out-of-band methods like secure email exchanges, phone calls, manual checking of authorizations, or in-person exchanges of devices (e.g. USB drives) containing shared secrets (e.g. cryptographic keys). Such connections can also be achieved when the parties have matured technical systems and invest in building connections/integrations between systems due to the large number of transactions between them. Normally started with bilateral agreements and existing trust relationships, these peer-to-peer relationships are limited in scale and prone to inefficiencies, especially as the number of stakeholders requiring such relationships and same sets of data increases.

In this model, an aircraft operator will need to share their AOSP documents with an increasing number of CAAs and National Security Authorities (NSA) if they expand their operations internationally. A peer-to-peer trust model means the aircraft operator may need to manage different terms with different parties for the same AOSP-related matter. This process is also highly dependent on long-standing trusted relationships between known personnel and their existing communication channels or custom integrations between systems. While effective for frequent transactions at a smaller scale, as the aircraft operator scales and the complexity of relationships increases, this approach will become inefficient and less secure.

4.2.2 Centralized trust

When our digital activities expanded and grew more complex, it only became intuitive to streamline trust by relying on existing institutions, such as governments, regulatory bodies, trade organizations, and even large technology companies (e.g. Facebook, Google), to become centralized repositories for trust. The extremely large number of relationships and interactions (essentially data points) these institutions have about individuals and organizations made them natural intermediaries to speak to the trustworthiness of and/or provide 'vetted' data of one party to another. As a result, many of them have become our "identity providers".

However, the centralized model, on one hand, made a very small number of entities extremely powerful, on the other hand, turned them into big honey pots of data susceptible to breaches. It also creates single points of failure, whereby if one central system fails or is compromised, many entities and individuals' work and lives could be disrupted. Furthermore, it is also unlikely that one party has broad enough coverage to include all stakeholders when it comes to cross-border and cross-industry processes.

Imagine in a centralized model where the NCASP, AOSP, and SSP documents may be all stored and managed by a global centralized authority in a global centralized repository, and each stakeholder will get their credentials (e.g. usernames and passwords) from the authority to access the system. While the stakeholders may find convenience to begin with by having a single source of truth, as digital transformation proceeds with more activities added into this centralized system, the consequences of security breaches and system failures will become unmanageable. Also, for critical matters like aviation security, some states may also prefer more control of their own data and documents.

4.2.3 Federated trust

We have seen advancement of centralized trust in places such as higher-ed, where students from one university can use the credentials (identity tokens) provided by the university to log into other universities' systems. While at the heart of it is still centralized trust, the federation of existing centralized systems provided by each centralized authority based on some sort of standardized agreements among them provides a path to scaling trust in the centralized model. Federation could be applied to aviation security as well to enable cross-border verifications of NCASP, AOSP, and SSP documents among a sizable number of states, aircraft operators, and other stakeholders.

While federating centralized systems addresses the challenges of centralization to some extent, it still requires centralized authorities, such as universities, to exist in the first place. And if a university's system is down, there is no way that their students can continue to use their credentials to log into other universities' systems. Same idea applies to aviation security scenarios - if State (A)'s centralized system that provides centralized services to all the aviation stakeholders is down, Aircraft Operator (A) won't be able to share their security documents with State (B) even if State (A) and State (B) are already in a federation.

4.2.4 Decentralized trust

Decentralized trust emerged in the past decade or so to address a key challenge previous models fail to tackle. That is, how to enable digital trust in a fairer, securer, and most importantly, more scalable manner. This model strives to address the following main issues:

- The dependence on a small number of centralized authorities who can become 'identity providers' and issue credentials
- The dependence of relying parties (verifiers of credentials) on identity providers (issuers of credentials) for verifications of credentials.

In a decentralized trust model, any entities can issue credentials by themselves, for example, Aircraft Operator (A) to self-issue AOSP and SSP documents and CAA (A) to issue a AOSP Letter of Approval to Aircraft Operator (A) after reviewing the AOSP documents. Once Aircraft Operator (A) receives the AOSP Letter of Approval from CAA (A), it can present to anyone else, e.g. NSA (A), who needs to verify the Letter, and there is no need for any contact or integration between NSA (A) and CAA (A)'s systems. Any party that receives Aircraft Operator (A)'s AOSP Letter of Approval can verify its integrity and confirm the identity and authority of the issuer. Even when CAA (A)'s system is down, NSA (A) can still verify Aircraft Operator (A)'s AOSP Letter of Approval.

This model works well in scenarios where there are complex ecosystems of large but undefined numbers of stakeholders across organizational, jurisdictional, and sectoral boundaries.

4.3. Cryptographic techniques

Before diving into the emerging technologies that make decentralized trust possible, it is important to understand the cryptographic techniques that provide the technical foundation for digital trust across all trust models. Some of these techniques are likely used in protecting aviation security documents today. Each cryptographic method can address one or more of the above-mentioned key aspects of digital trust.

4.3.1 Hashing

Overview: Hash functions are mathematical algorithms that generate a unique, fixed-size digital fingerprint (hash) for a document or dataset. Even the smallest change to the input data will produce a completely different hash, making it a reliable method for detecting any tampering.

Application to achieve data integrity: Hash functions can play a critical role in maintaining the integrity of important NCASP, AOSP, and SSP documents. By generating a unique hash for each version of these documents, aviation security stakeholders can detect unauthorized changes or tampering, because any modification will result in a new hash. Stakeholders can compare the hash values of shared or stored documents to verify their integrity and ensure the trustworthiness of vital aviation security information. Hashes can play a crucial role in verifying the immutability of records stored in decentralized repositories, such as distributed ledgers.

4.3.2 Message Authentication Codes (MACs)

Overview: Message Authentication Codes (MACs) are cryptographic tools to ensure both the authenticity and integrity of a message. A MAC is generated by applying a secret key and a cryptographic function to a message, creating a fixed-size output. The recipient can verify the MAC using the same key, confirming that the message has not been altered and that it was sent by the stated source.

Application in secure communications: MACs are commonly used in secure communication protocols and digital payment systems to protect data in transit. In the aviation sector, MACs can be used to help ensure the integrity and authenticity of messages exchanged between stakeholders, such as CAAs and aircraft operators.

4.3.3 Digital signatures and certificates

Overview: Digital signatures use asymmetric cryptography (a public and private key pair) to verify the origin and integrity of digital documents. When a sender signs a document with their private key, anyone with the corresponding public key can check the authenticity of the signature and verify whether the document is signed by the stated sender.

Digital signatures are used by Certificate Authorities (CA) to sign and issue digital certificates to entities with known identities. CAs publish lists of the public keys belonging to these entities. This is Public Key

Infrastructure (PKI). PKI manages the lifecycle of digital certificates, ensuring secure issuance, distribution, and revocation so that known entities can participate in secure communications and provide data integrity.

Application for authenticity: Digital signatures can be applied to enhance the authenticity of documents like AOSPs and SSPs. When a document is signed by an organization on a CA list using their private key, the recipient can find and use the associated public key to confirm that the document was issued by the said organization.

Application for integrity: Digital signatures also play a crucial role in preserving document integrity. The signature is tied to both the document's content and the signer's identity, meaning any alteration to the document after signing invalidates the signature. This gives stakeholders confidence that critical documents, such as NCASPs, AOSPs, or SSPs, remain unchanged after signing.

Application for non-repudiation: Digital signatures can provide non-repudiation, meaning that the signer cannot deny having signed a document. This is because only the entity, with their public key and real-world identity on a published CA's list, have access to the corresponding private key that can be used to sign the document. Non-repudiation is particularly important when accountability and traceability is required.

4.3.4 Encryption

Overview: Encryption is a cryptographic technique that transforms plaintext data into an unreadable format (ciphertext) using specific algorithms and keys. Only those with the correct decryption keys can access original data, ensuring confidential and sensitive information doesn't end up in the hands of unintended recipients.

Application for confidentiality: Encryption is vital for protecting sensitive aviation data, such as flight plans, passenger data, and security documents. By encrypting sensitive data in storage and transmission, organizations make sure only authorized personnel with correct keys can decrypt and access the information, preventing unauthorized access or breaches.

Application in protecting data in transit: Encryption is used in MACs and secure communication protocols (such as TLS/SSL) to ensure data integrity and authenticity.

5. Decentralized trust standards and technologies

Decentralized trust represents a shift towards a more interoperable and scalable model of digital interactions. This shift becomes possible due to the emergence and evolution of critical standards and technologies. This section is going to cover a few of these core standards and technologies.

5.1. Decentralized Identifiers (DID)

Decentralized Identifiers (DID), an open standard defined at the W3C, are unique, globally resolvable identifiers, not necessarily issued by centrally managed registries, such as ICANN for domain names. DIDs are very large unique random numbers (see Figure 5) composed of three parts—scheme, method, and DID method-specific identifier, so there is effectively an unlimited supply of DIDs. A DID method defines how a DID and its associate DID document works.

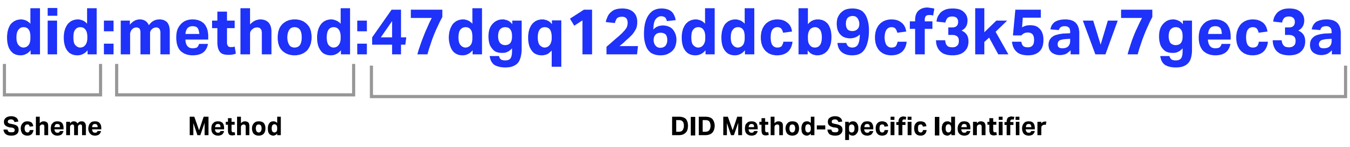

did:method:47dgq126ddcb9cf3k5av7gec3a
Scheme
Method
DID Method-Specific Identifier

Figure 5: An example of W3C Decentralized Identifiers (DID)

At the heart of DIDs is public-private key cryptography, which underpins the trust and security of these identifiers, ensuring that no entity can alter, revoke, or manage a DID without the explicit consent of the DID controller. Each DID is associated with a public-private key pair that is fully controlled by the DID controller. The controller generates their own public-private key pairs, with the public keys linked to the DID and the private keys securely controlled by themselves. This gives the controller full control over their identifiers (as well as the keys associated with the identifiers), because only the controller holds the private keys. The private keys are used to sign transactions, authenticate claims, and perform secure interactions, while others can verify the authenticity using the public keys tied to the DID.

Each DID can resolve to a DID document (see Figure 6), which contains information associated with the DID, including the public keys and other metadata of the DID, such as, the type of keys and ways to cryptographically authenticate the DID controller.

```
{
 "@context": [
  "https://www.w3.org/ns/did/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1"
 ]
 "id": "did:method:47dgq126ddcb9cf3k5av7gec3a",
 "authentication": [{
     // used to authenticate as did:...ec3a
  "id": "did:method:47dgq126ddcb9cf3k5av7gec3a#keys-1",
  "type": "Ed25519VerificationKey2020",
  "controller": "did:method:47dgq126ddcb9cf3k5av7gec3a",
  "publicKeyMultibase": "zH3C2WCvLMv6gmVNam3uVDjZpfkcJCwDwnZn6z3wXmqPV"
 }]
}
```

Figure 6: An example of a simple DID document

Unlike the traditional Certificate Authorities (CA) model—where organizations (e.g. ICANN accredited registrars) act to validate the identities of entities and bind the identifiers (often a domain name) listed in the registrar to cryptographic keys through the issuance of electronic documents known as digital certificates—DIDs have been designed to decouple identifier creation from CAs. This means any entity can create a DID (becoming the owner and sole controller of the identifier) with a public-private key pair for any reason without having to get their real-world identities validated in the first place by a CA.

Since there are only a limited number of CAs and the identifiers issued by these CAs have very narrow scopes (e.g. SSL certificates for websites), the separation of identifier creation from traditional CAs allows more entities (including individuals) with different trust focus to obtain identifiers that they can control and use to meet their requirements. This broadens the range of capabilities for an entity to build diverse ecosystems for conducting secure digital transactions. In the meantime, DIDs also provide the flexibility to work with the existing CA model, allowing entities to obtain their own DIDs while leveraging the established trust provided by a CA to improve the trustworthiness of their DIDs. For example, one can use a specific DID method to anchor their DID and the associated DID document to their existing web domain. This works particularly well for governments with high assurance .gov domains.

To learn more about the architecture of DID, see the Architecture Overview section of the W3C DID specification.

5.2. Verifiable Credentials (VC)

Verifiable Credentials (VC) is another open standard defined at the W3C. VCs are essentially a data model that defines how to digitally represent all the same information that a physical credential represents. Therefore, like physical credentials, VCs can be used to make claims or assertions about individuals, organizations, and/or assets.

VCs are designed to inherit a very important trait of their physical counterparts—separating verification of a credential (e.g. a mobile driver's license) by a verifier (e.g. an airline) from its issuer (e.g. the transportation authority), when proper technical architecture and cryptographic techniques, such as digital signatures, are applied. This means once a credential is issued to a credential holder, the holder can share a 'Verifiable Presentation" from the VC with a verifier without involving the issuer at all (see Figure 6).

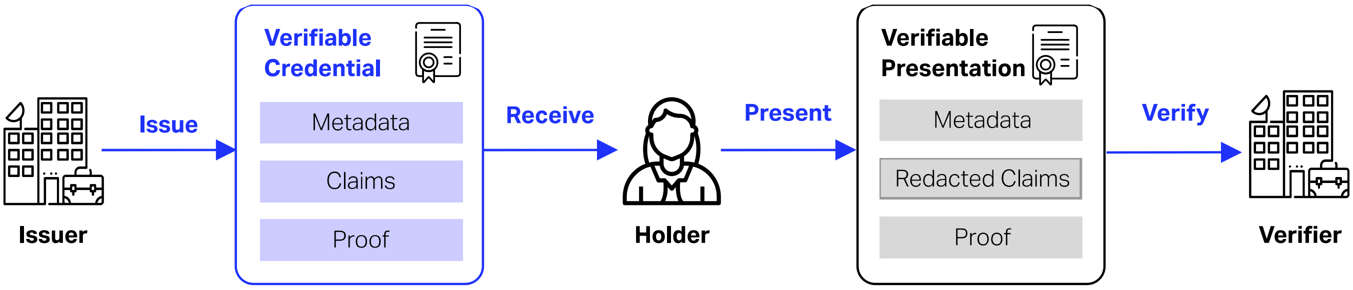


Figure 6: W3C Verifiable Credentials

The separation of verifier from the reliance on an issuer prevents mass surveillance that many are afraid of, especially when our lives are becoming more digitized. And with the use of digital signatures, VCs are more tamper-evident and trustworthy than their physical counterparts, because verifiers of VCs can find out whether the credentials are issued by entities they trust through comparing an issuer's public key in a VC with the public key made public by the said issuer.

Each VC may include one or more claims, and each claim is expressed using subject-property-value, for example (see Figure 7):

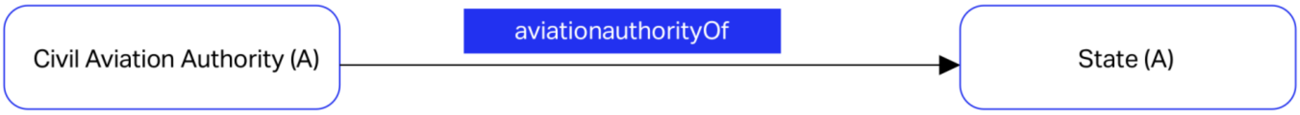


Figure 7: An example of subject-property-value

The W3C VC specification defined some must-have properties in a VC, such as credential subject, issuer, issuance date, and at least one proof mechanism (see Figure 8).

```
{
  "@context": [
    "https://www.iata.org/2024/credentials/v1",
    "https://www.iata.org/2024/credentials/examples/v1"
  ],
  "id": "http://example.caa/credentials/3732",
  "type": ["VerifiableCredential", “AviationSecurityCredential"],
  "issuer": "https://example.caa”,
  "issuanceDate": "2024-02-01T20:13:42Z",
  "credentialSubject": {
    "id": "did:method:abec7f712ebc6f1c289ae12ec21",
    “aviationsecurity”: {
      "type": "AOSP”,
      "name": “AOSP Letter of Approval"
    }
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2023-11-13T18:19:39Z",
    "verificationMethod": "https://example.caa/issuers/14#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z58DAdFfa9SkqZMDPxAPpic7ndSayn1PzZs6ZjWp1CktyAesjuSTwRdo
                WhAfGFCF5bppTESTojQCrfFPP2oumHPtz"
  }
}
```

Figure 8: An example of a VC with must-have properties

A common property in a VC is credential schema, which are used to enforce a specific structure on a given collection of data. Data schemas are often used by industries to align stakeholders on a certain way to structure data and the semantics of data in a VC, enabling data and semantic interoperability across organizational and jurisdictional boundaries. For example, TradeTrust, a technical framework developed by the Infocomm Media Development Authority of Singapore (IMDA) to promote authenticity and manage source and title ownership for trade documents, defined its own schemas for trade documents and have a version of the schema that aligns with the W3C VC Data Model.

The unique and intentional design of VCs enable the holder of credentials to have more control over their own identities and data while still allowing the verifiers to get sufficient information about the authenticity and validity of credentials and the integrity of data to conduct proper verifications. Certain types of VCs have additional features such as selective disclosure, where a holder can selectively disclose the data (e.g. 25 years old) from a VC (e.g. a mobile driver's license) in the Verifiable Presentation for a particular transaction (e.g. alcohol purchase) rather than revealing unnecessary data (e.g. address) to the verifier (e.g. a liquor store). In certain cases, it is possible to only give the verifier a derived answer (e.g. over 18) based on the credential data without revealing the real age of the holder.

To learn more about the properties and lifecycle of a VC, see the Concrete Lifecycle Example and Lifecycle Details sections in the W3C VC specification.

5.3. Distributed ledgers

Unlike traditional databases, distributed ledgers are databases without a central data store or administrator. They are digital systems for recording the same data and transactions in geographically different places at the same time, avoiding a single point-of-failure and offering a tamper-evident, transparent mechanism for record-keeping.

To keep identical copies of data at different places, distributed ledgers generally require peer-to-peer computer networks and consensus algorithms to make sure data are updated and replicated reliably across each node on a network. When an update takes place on one ledger, it will broadcast the update to the entire network and let the consensus algorithms determine which is the correct updated copy before all the nodes update themselves with the correct copy.

Distributed ledgers can take many forms, among which blockchain is the most known one. Distributed ledgers are normally used together with cryptographic keys and signatures so that only the people with right authorizations can make updates on a ledger and alterations of data/transactions are noticeable and traceable.

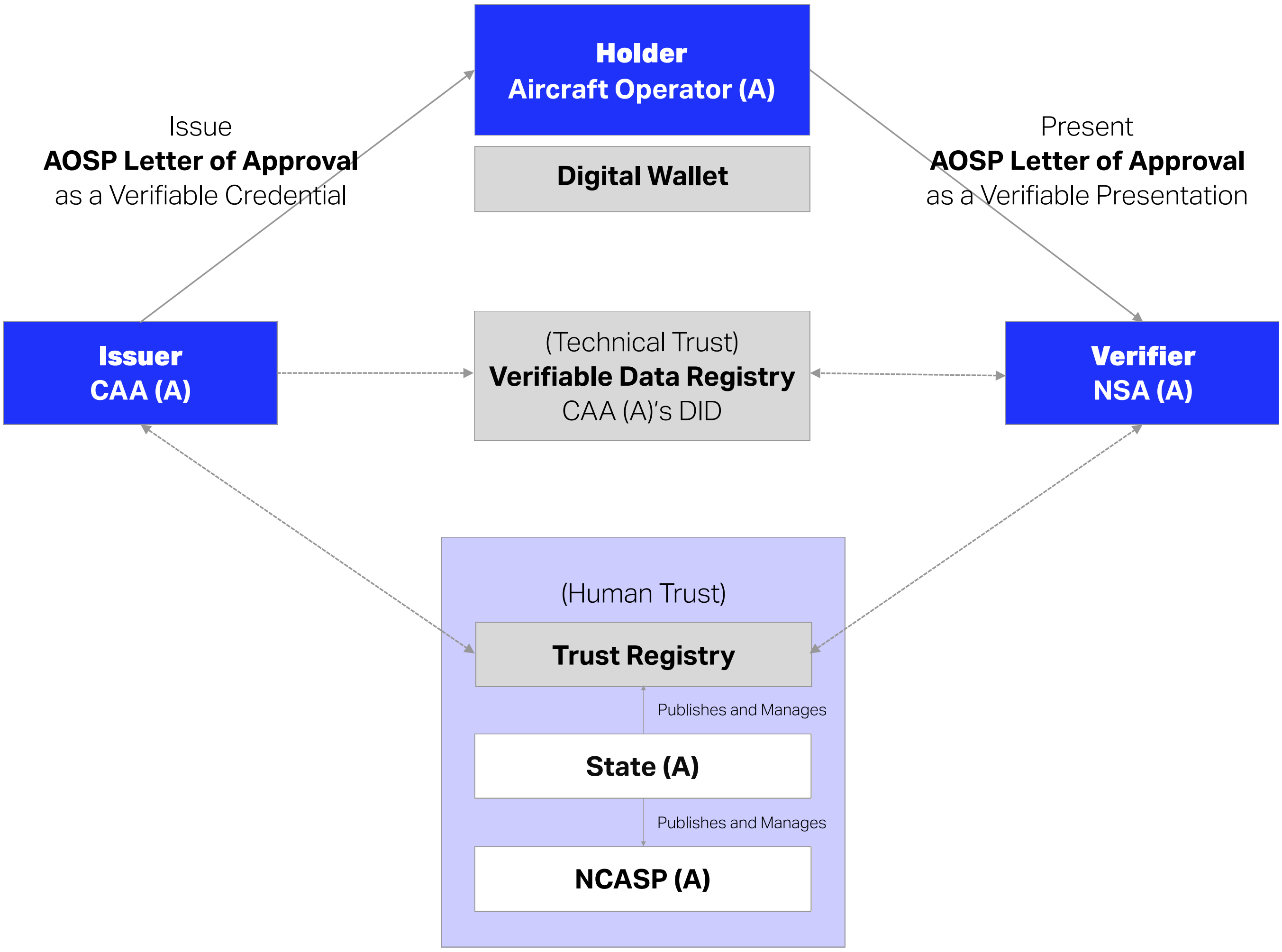
Distributed ledgers can also be applied with other cryptographic techniques such as hashing, for example, storing hashes of large-size documents on distributed ledgers as opposed to the documents themselves.

6. Enhancing aviation security with decentralized trust technologies

By decoupling identifier creation from centralized authorities and credential verifications from direct contact with issuers, decentralized trust technologies allow aviation stakeholders to create and manage critical security documents while being able to exchange and verify these documents across organizational and jurisdictional boundaries. With the many stakeholders involved in the aviation security value chain and at different paces of digital transformation, it is critical that the aviation security industry enables trust building by letting each stakeholder do their job without having to add a giant centralized hub. This section is going to provide a holistic view of how these technologies are brought together to support an **Aviation Security Trust Ecosystem**.

6.1. Aviation Security Trust Ecosystem

While W3C VCs and DIDs are essential to make aviation security scalable in the digital world, humans need to implement them properly with other enabling components. The Figure 9 below depicts the roles and key components of an Aviation Security Trust Ecosystem, modeling the simple use case scenario of inter-organizational verifications of Aircraft Operator (A)'s AOSP Letter of Approval within State (A). (See the Current Business Processes: AOSP described in an earlier section.)



Holder
Aircraft Operator (A)

Digital Wallet

Issue
AOSP Letter of Approval
as a Verifiable Credential

Present
AOSP Letter of Approval
as a Verifiable Presentation

Issuer
CAA (A)

(Technical Trust)
Verifiable Data Registry
CAA (A)'s DID

Verifier
NSA (A)

(Human Trust)

Trust Registry

Publishes and Manages

State (A)

Publishes and Manages

NCASP (A)

Figure 9 - Aviation Security Trust Ecosystem (Use case: domestic verification of AOSP Letter of Approval)

6.2. Entities and roles

6.2.1 Issuer: CAA (A)

As illustrated in the Aviation Security Trust Ecosystem diagram, after reviewing and approving Aircraft Operator (A)'s AOSP documents, the CAA (A) issues the AOSP Letter of Approval in the form of a VC. As the **Issuer**, the CAA (A) uses their private key that is associated with the public key to cryptographically sign the VC. Their public key is contained in the DID document, which is stored in a **Verifiable Data Registry**.

The CAA (A) can create their own DID relatively easily without the approval of a central authority. With a DID and its associated public-private key pairs, the CAA (A) can start to issue (sign) VCs.

6.2.2 Holder: Aircraft Operator (A)

The Aircraft Operator (A) is the **Holder** of the AOSP Letter of Approval and stores the Letter of Approval as a VC in their **Digital Wallet**. They can present the AOSP Letter of Approval from their **Digital Wallet** to the NSA (A) as needed to prove compliance in a secure manner.

6.2.3 Verifier: NSA (A)

As the **Verifier,** The NSA (A) is responsible for checking Aircraft Operator (A)'s compliance with aviation security standards. The NSA (A) may request the Aircraft Operator (A) to present the AOSP Letter of Approval for audits, inspections, or compliance checks. The NSA (A) can verify the authenticity, validity, and authority of the AOSP Letter of Approval by checking:

- The **Trust Registry**: Whether the CAA (A), the **Issuer**, is authorized to issue and sign the AOSP Letter of Approval.
- The **Verifiable Data Registry (VDR)**: Whether the signing public key matches with the CAA (A)'s public key in the Verifiable Data Registry to ensure the AOSP Letter of Approval is from the claimed Issuer, whether the Letter of Approval is tampered with, or whether it is superseded or revoked.

None of the two checks above involve direct contact between the NSA (A), the **Verifier**, and the CAA (A), the **Issuer**, which means there is no need for any system integrations between the two. So, even if today the CAA (A) and NSA (A) are already using their own systems to manage aviation security documents, they can still add a layer of issuance and verification capabilities on top of them without having to abandon their current systems.

6.3. Key enabling components

6.3.1 Verifiable Data Registry - technical trust

Verifiable Data Registries (VDR) play a key role in trust ecosystems by mediating the creation and verification of DIDs, cryptographic public keys, and other relevant data, such as revocation list, credential schemas, etc.

VDRs can take many forms, such as the web and DNS, government ID databases, and distributed ledgers. Often, more than one type of VDR is used in a trust ecosystem. In our Aviation Security Trust Ecosystem example, for the CAA (A) to start issuing VCs, they can leverage their existing domain (e.g. caaa.gov) as the **VDR**, especially if the CAA (A) is a known government entity with a .gov or other high assurance domain name.

The W3C VC standard leaves flexibility for the implementation of **VDRs**, but normally **VDRs** are used in the following scenarios to ensure the authenticity and validity of VCs:

- **Issuer identifiers and public keys. VDRs** store **Issuer** identifiers, such as DIDs and their associated DID documents, allowing **Verifiers** to authenticate the digital signatures on VCs. For example, when the Aircraft Operator (A) presents its AOSP Letter of Approval, the NSA (A) will check a VDR to confirm that the signature was made by the private key associated with the public key of CAA (A)'s DID listed on the **VDR**.

- **Credential status.** VDRs are also used to track the status of each VC issued using the **Issuer**'s DID, including whether it has been revoked, suspended, or has expired. This allows **Verifiers** to confirm that the AOSP Letter of Approval presented is still valid and has not been superseded or revoked due to compliance issues.
- **Credential schemas. VDRs** are a way to make credential schemas publicly discoverable. They are often used to anchor credential schemas when **Issuers** have custom credential schemas for their specific use cases that **Verifiers** need to refer to when checking whether the received credentials are created in alignment with defined schemas.

6.3.2 Trust Registry - human trust

VDRs are used to anchor DIDs and check the authenticity and integrity of VCs signed by cryptographic keys associated with the DIDs on **VDRs**. There is still the need to know whether **Issuers** with specific DIDs are authorized to issue certain VCs in the first place. This is where a **Trust Registry** is essential. It provides a list of recognized entities authorized by a trust ecosystem to issue specific credentials, like AOSP Letters of Approval, filling the gap that **VDRs** alone cannot address.

Key functions of a **Trust Registry** include:

- **Authorized issuers.** A **Trust Registry** of an ecosystem maintains a list of **authorized entities**, such as CAA (A), which are permitted to issue credentials like AOSP Letter of Approvals. Verifiers, such as NSA (A), can reference the Trust Registry to confirm that CAA (A) is authorized to issue the AOSP Letter of Approval to the Aircraft Operator (A).
- **Issuer metadata. Trust Registries** are normally where **Issuers** are asked to provide identifiable information of their entities, such as legal name, entity Identifier (e.g. Legal Entity Identifier), organizational address, website, contact information, and many others. More importantly, **Issuers** are often asked to provide 'pointers' (e.g. URLs) to their DIDs/public keys on **Trust Registries** so that **Verifiers** are assured to get the most up-to-date public keys from the **VDRs** where **Issuers** anchor their public keys for credential verifications.
- **Real-time verification of authority. Trust Registries** allow for real-time verification of an **Issuer**'s current authority. **Verifiers** can check whether an **Issuer** is still in good standing and authorized to issue certain credentials.

Trust Registries provide a list of recognized entities that are authorized to issue certain types of credentials. **Trust registries** working in combination with **VDRs** play what was traditionally a Certificate Authority (CA)'s role. How to construct the two types of registries to ensure both technical and human trust is often an implementation question and use case dependent. But some forms of both should be in place when DIDs and VCs are deployed for a trust ecosystem. There may also be **Trust Registries** for **Verifiers** and **Digital Wallets**, but they won't be discussed in depth in the paper.

6.3.3 Digital Wallets

Digital Wallets are a critical component in a trust ecosystem, serving as the secure, user-controlled storage for VCs. With a **Digital Wallet**, the Aircraft Operator (A) can securely store, manage, and present credentials, such as AOSP Letters of Approval.

Here are the core functions of **Digital Wallets**:

- **Storage of credentials**. **Digital Wallets** can securely store VCs, such as compliance certificates, using cryptographic methods. The Aircraft Operator (A)'s AOSP Letter of Approval can be stored in their digital wallet, protected from tampering and easily accessible when needed.

- **User control**. **Digital Wallets** put a **Holder** of credentials, such as the Aircraft Operator (A), in full control. The **Holders** can decide when and to whom they share their VCs. This user-centric approach enhances secure dealing of credentials and minimizes the risk of unauthorized sharing, as only the **Holder** with right access can accept VCs into the **Digital Wallet** and approve presentation of credentials from it.
- **Presentation of credentials**. When a **Verifier**, such as NSA (A), sends a verification request to a **Digital Wallet**, the **Digital Wallet** responds to the request and allows the **Holder** to present relevant VCs for verification. For example, the Aircraft Operator (A) can quickly present their AOSP Letter of Approval from their **Digital Wallet** when they receive a presentation request from the NSA (A).

Depending on use case scenarios and implementation choices, there are some other key functions to consider when building or choosing a **Digital Wallet** for a trust ecosystem.

- **VC verification. Digital Wallets** can support the verification of credentials. Before presenting a VC, a **Digital Wallet** may verify the VC status (e.g. whether it hasn't been revoked or expired) by checking against the **VDR** that the **Issuer** uses. This ensures that only valid and up-to-date credentials are shared with **Verifiers**.
- **Multi-credential support.** It's common that **Digital Wallets** can store multiple VCs from various **Issuers**. For example, the Aircraft Operator (A) may hold the SSP Letter of Approval issued by the CAA (B) from State (B) and the many other SSP Letters of Approval issued by CAAs from other countries. A **Holder** can potentially manage all aviation security related credentials in one place as the Aviation Security Trust Ecosystem use cases expand.
- **Interoperability. Digital Wallets** are normally a key component to enable interoperability across different platforms and jurisdictions. This means that the AOSP Letter of Approval issued by CAA (A) and the SSP Letter of Approval issued by CAA (B) to the Aircraft Operator (A) can be stored in the same **Digital Wallet** and presented to the NSA (B) seamlessly to facilitate cross-border trust (see Figure 10).

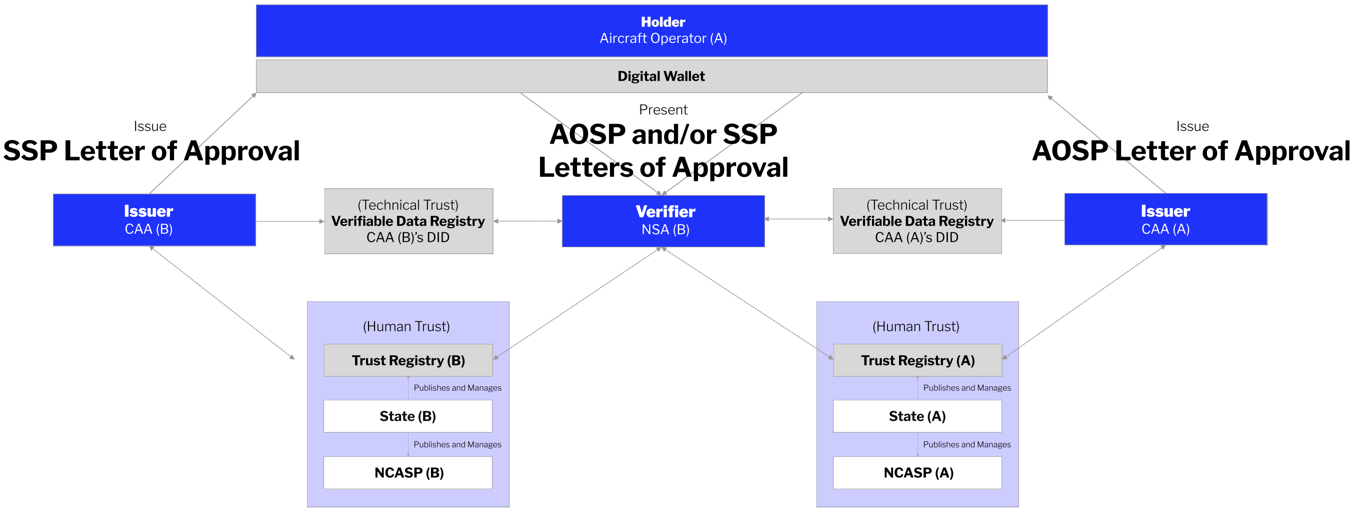


Figure 10 - Aviation Security Trust Ecosystem (Use case: cross-border verification of AOSP and SSP Letters of Approval)

Digital Wallets can be available as mobile or web apps, offering users flexibility across various devices and environments, while ensuring secure and convenient access to important credentials at any time and from any locations.

6.4. Chain of trust

Going beyond the key roles and core components of the Aviation Security Trust Ecosystem, there are some complex trust relationships that need to be further explored.

6.4.1 From trusted organizations to authorized personnel

Participants and stakeholders of the Aviation Security Trust Ecosystem will most likely take the form of organizations. However, these organizations all require real persons with appropriate authorizations to perform tasks within the Ecosystem. For example, the Aircraft Operator (A) needs to assign a CSO with appropriate authority to work on the creation, approval, and presentation of AOSP and SSP documents. The CAA (A) will also need to assign an officer to review the documents and sign/issue the Letters of Approval. This is where cryptographical techniques are needed to bind the digital representations of organizations, persons, and roles (see Figure 11).

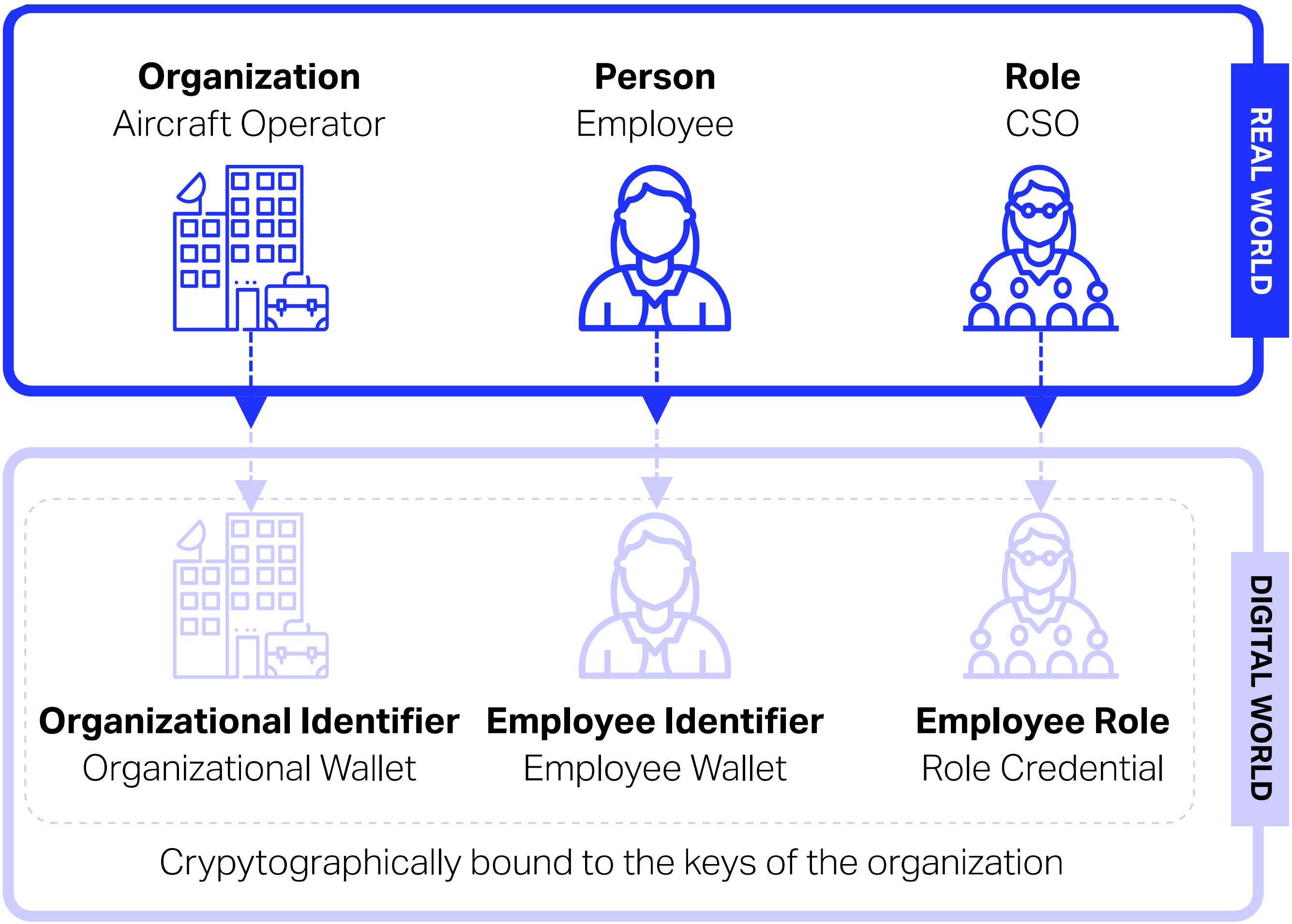


Figure 11 – Illustration of Cryptographically Binding Organizations, Persons, and Roles

Some key concepts that may be involved:

- **Organizational and employee wallets.** There may be **Digital Wallets** at different levels of the organizations. For example, the Aircraft Operator (A) can have a **Digital Wallet** that can be used to store organizational level credentials, such as AOSP Letters of Approval. Employees of the Aircraft Operator (A), e.g. a CSO, can have their own employee wallets, assigned by the Aircraft Operator (A). In this scenario, the employee wallets will be subject to the Aircraft Operator (A)'s oversight and can be suspended by the Aircraft Operator (A).
- **Authorization and role credentials.** For employees, such as a CSO, who are responsible for submitting AOSP and SSP documents to obtain Letters of Approval, they may have an authorization or role credential in their employee wallets that can speak to their authorities assigned by the Aircraft Operator (A). This could be used to prove that a person is the CSO and has the authority to submit these documents. With these authorizations and role credentials, employees may have access to their

organizational wallets and credentials in them and can use these credentials for verifications defined by their authorizations. For example, a CSO can share the AOSP Letter of Approval from an organizational wallet with a National Security Authority (NSA).

The digital relationships between the Aircraft Operator (A) and its CSO can be cryptographically bound through chained keys or credentials, so when NSA (A) and/or (B) verify Aircraft Operator (A)'s Letters of Approval, they will be able to know whether the Letters of Approval were issued by authorized personnel at CAA (A) and/or (B). Or in another way, the verifications won't be successful if unauthorized personnel issued the Letters of Approval.

6.4.2 Binding security documents to VCs

Given the potential large sizes of security documents, such as AOSPs and SSPs, it may not make sense to sign these documents directly into their Letters of Approval as VCs. However, when NSA (A) and/or (B) receive Letters of Approval from the Aircraft Operator (A) for verifications, they may also need to review some parts of the AOSP and/or SSP documents, thus requiring assurance that they are getting the right versions of the documents that are associated with the received Letters of Approval. Cryptographic techniques, such as hashing, can be used to bind these documents to a particular Letter of Approval—for example, by signing the hashes of the documents in the VC (see Figure 12).

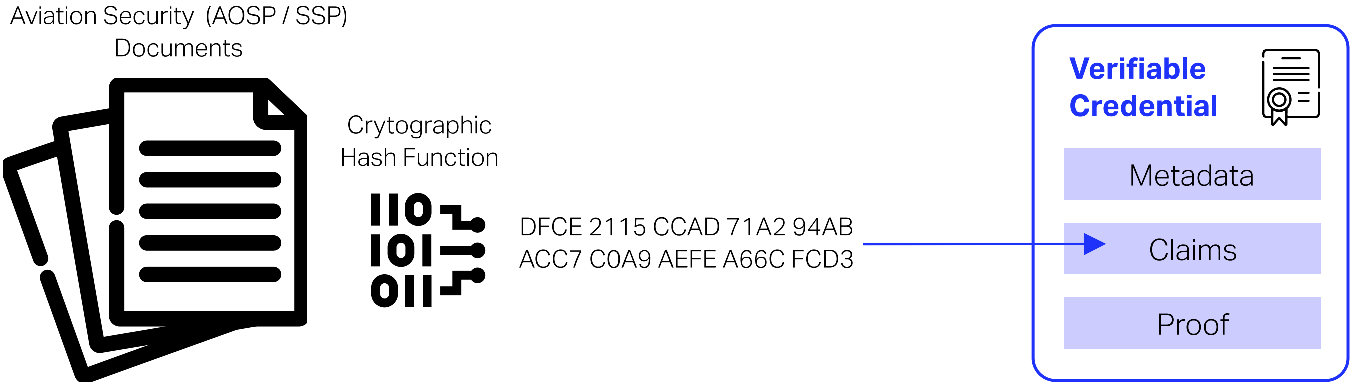


Figure 12 – Illustration of including cryptographic hashes of aviation security document in a VC

7. Aviation Security Trust Framework (ASTF)

With a holistic view of the different roles and components within the Aviation Security Trust Ecosystem that leverages decentralized trust technologies, it is time to come back to the fundamental question IATA intends to address for aviation security - how to build and scale multilateral trust in today's fragmented digital landscape.

By leveraging appropriate technologies and cryptographic techniques, the proposed Aviation Security Trust Framework (ASTF) should, on one hand, **enhance** and **standardize** existing trust building processes and activities, and on the other hand, **create** new ones to address emerging digital trust challenges.

As a result, the ASTF will provide the overarching structure that ensures all entities and enabling components within the Aviation Security Trust Ecosystem to work together in a secure, reliable, and interoperable manner.

The below table provides an overview of the key components that the ASTF should include and whether there are existing processes and practices within aviation security to build on.

Aviation Security Trust Framework Components		Enhance	Standardize	Create
Initial Trust Establishment	Roles, Responsibilities, and Requirements	x	x	x
	Onboarding Participants to the Ecosystem			x
	Facilitating Recognition and Trust among Participants		x	x
Levels of Assurance				x
Standardization and Interoperability (Technical and Data)	Data Structures and Semantics		x	x
	Credential Profiles and Cryptographic Techniques		x	x
	Data Security and Exchange Protocols		x	x
	Digital Wallet and Trust Registry Requirements			x
Credential Lifecycle Management				x
Security and Privacy	Technology Infrastructure and Operations	x	x	x
	User Authentication and Authorization	x	x	x
	Document Security and Versioning	x	x	x
	Personal Information and Privacy	x	x	x
Compliance and Risk Management	Legal and Regulatory Compliance	x	x	x
	Conformance Profile and Trust Audits	x	x	x
	Threat Modeling and Risk Mitigation	x	x	x
Ecosystem Governance				x

7.1. Initial trust establishment

To establish trust across entities, roles, responsibilities, and requirements must be clearly defined for each stakeholder within the Aviation Security Trust Ecosystem. All organizations and personnel should meet the necessary criteria before assuming their roles.

Participating in this Ecosystem also requires initializing a trust relationship between the Ecosystem and participants. This may involve signing formal agreements, memorandum of understandings or other forms of documents. Given the diversity of stakeholders, the Ecosystem should also provide a foundational mechanism that allow participants to recognize and build trust among themselves based on their own preferences.

7.1.1 Roles, responsibilities, and requirements

For the Aviation Security Trust Ecosystem to function, it requires at least two levels of roles:

- **Ecosystem leadership.** At the leadership level, two distinct functions are normally needed:
  - A governing body that defines strategic directions and decision-making processes for the Ecosystem. It will also provide the human trust factor for the Ecosystem, creating and maintaining the ASFT, and develop an ecosystem governance framework that guides the operationalization of the Ecosystem.
  - An operational body that executes the operationalization of the Ecosystem and manages the day-to-day matters based on the defined strategic directions and the ecosystem governance. The operational body may provide the technical trust for the Ecosystem by operating a VDR or public key directory.

- **Ecosystem participants.** Depending on the scope of the ASTF, ecosystem participant roles may vary. These could be Issuers, Holders, and Verifiers. The Ecosystem can also include technology and service providers that meet the defined requirements as participants. For example, the Ecosystem can have preferred Verifiable Data Registry providers that they recommend participants to use whether the Ecosystem operates a VDR or not themselves.

Each role within the Ecosystem should come along with responsibilities and qualifications that organizations and their personnel should meet to fill in these roles. For example, aircraft operators should have business licenses, Air Operator Certificates, and other relevant credentials that speak to their valid status as aircraft operators. Government agencies, such as Civil Aviation Authorities (CAA) and National Security Authorities (NSA), should also meet Issuer and Verifier requirements to assume such roles within the Ecosystem. Depending on the role(s) of each stakeholder, there may be additional technical, security, and credential requirements, which the ASTF should provide guidelines for.

For a complex ecosystem such as the Aviation Security Trust Ecosystem, there may be two sets of requirements:

- **Minimum Qualifications:** These will be the basic requirements that a participant must fulfil to join the Ecosystem. The more inclusive an ecosystem intends to be, the less these requirements are. However, without a reasonable set of minimum requirements, an ecosystem may lack credibility and trustworthiness in the first place.
- **Additional Qualifications:** These are the good-to-haves for a participant in a particular role. Meeting additional requirements may allow participants to stand out in certain ways and enjoy certain benefits that others don’t.

7.1.2 Onboarding participants to the Ecosystem

Onboarding participants to the Ecosystem may involve a multi-step process and the ASTF should define the key steps, such as:

1. **Application:** It is common for a participant to fill out an application form or go through a similar process to indicate their interest in participating in the Ecosystem.
2. **Materials Submission:** Once an application is being considered, the applicant will be asked to share their qualifications and other materials required by the Ecosystem.
3. **Due Diligence and Vetting:** The operational body of the Ecosystem will conduct due diligence and vet whether an application provides accurate and trustworthy information (e.g. identity verification) and whether they meet the minimum requirements to become a participant. This vetting process can be conducted through online and/or offline methods.
4. **Approval and Agreement:** Once vetted, the Ecosystem will approve the applicant and send an agreement or something of similar nature to officially initiate a trust relationship between the Ecosystem and the participant.
5. **Onboarding Procedures:** The participant will be provided access to the Ecosystem's platform based on their roles. They may be offered support to ensure their own system can be connected to the Ecosystem and relevant personnel is granted the right access. There may also be additional procedures to notify the Ecosystem stakeholders of a new participant.

The ASTF will provide guidelines of trust factors that need to be considered and build into the onboarding process for participants rather than define the exact steps of what an onboarding process should look like.

7.1.3 Facilitating recognition and trust among participants

For a complex trust ecosystem, becoming a participant may just be the first step to scaling digital trust. The ASTF should establish a foundational mechanism of recognition and trust building, whereby participants can develop a baseline understanding of each other and trust each other to a certain extent knowing that they are vetted by the Ecosystem based on a common set of minimum requirements.

It is critical for an ASTF to find common grounds from existing processes and activities when developing its foundational mechanism. For example,

- **Political Agreement (Air Services Agreement)**: Mutual recognition can be supported by political and legal instruments, such as Air Services Agreements, which formalize the commitments between states and establish trust of each other's aviation security standards and credentialing systems.
- **Economic Agreement**: Economic agreements between states can ensure that mutual recognition extends to the financial and commercial aspects of aviation, reducing barriers and promoting efficient cross-border operations.
- **Operational Agreement**: Operational agreements between agencies and operators can provide the groundwork for the practical implementation of mutual recognition, ensuring that security processes, standards, and credentialing methods are harmonized.

The ASTF should also define mechanisms to facilitate further trust building among participants. These mechanisms should take into consideration the diversity of participants and provide flexibility to participants based on their preferences.

7.2. Levels of Assurance (LoA)

The ASTF should define **Levels of Assurance (LoA)** based on the security needs of various credentials issued within the Ecosystem. LoAs is the certainty with which a claim to a particular organization, personnel, or asset/artifact during authentication can be trusted to be true:

- **High Assurance**: Required for critical credentials such as aircraft certifications, where any error could result in severe security risks.
- **Medium Assurance**: Applied to routine credentials that require some verification but not at the highest security level.
- **Low Assurance**: Used for credentials that carry minimal security risk, such as operational records or non-sensitive personnel certifications.

Some civil aviation authorities are already creating unencrypted PDF documents to certify certain aspects of aircraft operators and hosting those documents publicly on their '.gov' domains. Even if the .gov domains provide a rather high level of assurance that the documents hosted by them are created by the government agencies controlling the domains, the fact that anyone can access and download a document and may pretend to be the aircraft operator that is concerned in a document make the method less likely to be considered as high assurance.

Levels of Assurance (LoA) play a crucial role in aligning the security measures for different types of credentials with their associated risk profiles. All participants within the Ecosystem should follow these assurance levels when issuing, verifying, or storing credentials. Additionally, the ASTF will define the roles and responsibilities for each role, which includes specific rules and responsibilities for credential issuance, key management, and revocation processes. By ensuring that credentials are handled with the appropriate level of scrutiny, LoAs support the broader trust infrastructure established at the Ecosystem level and between organizations.

7.3. Standardization and interoperability

A robust ASTF relies heavily on standardization and interoperability among participants and stakeholders to ensure that credentials and documents can be trusted across various platforms and jurisdictions. While the W3C VC and DID standards provide a solid technical foundation, additional layers of standards and guidelines are needed to fully enable trust and interoperability within the Aviation Security Trust Ecosystem.

7.3.1 Data structures and semantics

Beyond the general data model provided by W3C VC standards, there may be need for domain-specific data schemas. In the aviation security context, standardized schemas for credentials like the AOSP and SSP Letters of Approval are essential. The ASTF should define the types of credentials that require standardized schemas and/or develop these schemas, ensuring consistent data structure and interpretation across all stakeholders.

In addition to standardizing credential schemas, following consistent document formats and content structures across different jurisdictions is also crucial for ensuring uniform interpretation of various clauses in these documents. This consistency will allow all stakeholders to understand and utilize the information effectively, regardless of the system or country involved. This standardization can be extended to the NCASP, the guidance and templates provided to aircraft operators among other documents.

7.3.2 Credential profiles and cryptographic techniques

Credential profiles define data formats, identifier types, signature types, cryptographic techniques, and other important aspects of a specific credential. To ensure consistency in the creation and verification of credentials, the ASTF should outline specific requirements for credential profiles.

7.3.3 Data security and exchange protocols

To facilitate secure exchange of credentials and related data, the ASTF should provide guidance over protocols to be used for presenting and exchanging credentials among different systems. For W3C VCs, there are several common exchange protocols, including OpenID for Verifiable Credentials (OID4VC). Beyond credential exchanges, other protocols may be used to ensure authenticity and integrity of related documents and the secure transfer of them.

7.3.4 Digital Wallet and Trust Registry requirements

The ASTF should also provide requirements for digital wallets and trust registries that can be used to ensure that participants are able to accept credentials issued to them from others within the Ecosystem and that participants can obtain and read information from others' trust registries.

7.4. Credential lifecycle management

The ASTF should provide specific guidelines to manage each stage of a credential lifecycle, tailored to the regulatory and operational requirements of the Ecosystem. The lifecycle stages may also vary based on the regulatory needs, security risks, and operational demands of aviation security.

At a high level, the ASTF should define the following stages:

1. **Issuance**: Define criteria for **Issuers**, such as national authorities (e.g. CAAs), and outline the conditions under which they may issue credentials and the required technical capabilities.
2. **Storage**: Establish secure storage guidelines for holders. **Digital Wallets** used by holders (e.g. aircraft operators) should comply with interoperability requirements of the Ecosystem to enable seamless usage of credentials across different platforms and systems.
3. **Presentation (Verification):** Define criteria for **Verifiers** (e.g. National Security Authorities, auditors) to request and verify credentials. Depending on use cases and relevant regulatory requirements, **Verifiers** may have different authorities over the type of credentials and information they can request.
4. **Update/Amendment**: Define criteria for updating or amending credentials in cases of errors or changes to ensure that the integrity and verifiability of credentials is maintained.
5. **Suspension/Revocation:** Set policies for suspending or revoking credentials, including the reasons for such actions and how **Issuers** should manage their revocation registries. This is crucial for maintaining trust and preventing the misuse of compromised or invalid credentials.
6. **Expiration:** Define expiration rules for credentials based on the type of credential and the regulatory requirements. Credentials with time sensitivity should be automatically invalidated once expire, ensuring expired credentials are no longer usable by **Holders** or verifiable by **Verifiers**.
7. **Renewal:** Establish guidelines for renewing credentials that are nearing expiration. Renewals should involve confirming that **Holders** remain eligible for the credentials. This is particularly important for credentials with a limited validity, such as security certifications, where regular re-validation ensures compliance with evolving industry standards.

7.5. Security and privacy

Implementing emerging digital trust standards and advanced cryptographic techniques alone is not enough. Additional measures are needed to ensure credentials and related documents remain secure during their entire lifecycle.

7.5.1 Technology infrastructure and operations

The ASTF should define baseline criteria for the capabilities required to operate a system that manage aviation security documents and credentials within the Ecosystem, including technology and operations related to information security management, technical security controls, risk and fraud management, information and integrity management, incident response, among others.

7.5.2 User authentication and authorization

The ASTF should promote strong authentication and authorization mechanisms to ensure that only authorized personnel with appropriate roles within a participating organization can access sensitive documents and data. Multi-factor authentication, role-based access controls, and regular identity verification processes can help prevent unauthorized access.

Recognizing that personnel changes are common within organizations, the ASTF should also define processes for how to manage any changes in roles, responsibilities, and/or access rights. In cases where roles, access, or participation need to be revoked, there should be clear policies outlining the conditions for revocation. Whether due to non-compliance, changes in role, or other reasons, the process for revocation must include steps for removing user authentication and/or authorization.

7.5.3 Document security and versioning

The ASTF should promote secure handling of documents by providing guidelines for how documents should be protected within organizations and during exchanges with others to ensure that sensitive information is consistently secured across the board. This may include encryption, regular cybersecurity assessments among others. The ASTF should also define proper version control for documents as they are updated to reflect new regulations, security measures, or changes in related documents.

7.5.4 Personal information and privacy

For the AOSP/SSP use case, little sensitive personal information is involved. As the Aviation Security Trust Ecosystem evolves, it may begin to involve use cases that deal with a larger amount of personal information. The ASTF should describe requirements for handling personal information associated with credentials within the Ecosystem and evolve as use cases expand.

7.6. Compliance and risk management

7.6.1 Legal and regulatory compliance

The ASTF should define criteria whereby stakeholders get checked on their compliance with legal and regulatory requirements to perform their roles in the Ecosystem. This includes adherence to key aviation standards, such as the ICAO Annex 17. Such mechanisms may include ways for the Ecosystem participants to raise concerns and/or red flags to the Ecosystem as they interact with each other.

Laws and regulations are not limited to the global realm of aviation security. Local and regional laws as well as data and privacy regulations, e.g. GDPR, may also become relevant depending on the roles of participants and use cases they are involved in.

7.6.2 Conformance profile and trust audits

The Ecosystem will have a set of functional (technical or operational) components that can be assessed independently. The ASTF should define clear conformance profile and criteria for these components, particularly the most critical ones.

Conformance criteria are central to the ASFT, because they specify the essential requirements agreed to by participants to ensure the integrity of the processes. The ASTF may also define testing mechanisms that can be developed to help participants stay and improve compliance. In addition, trust audits and certification programs could also be explored as potential tooling to enforce or validate conformance.

7.6.3 Threat modeling and risk mitigation

The ASTF should address the high stakes of aviation security by modeling common threats (e.g. credential forgery or key compromise) for each type of stakeholder and providing clear guidelines for identifying, mitigating, and responding to these threats. It should also establish criteria for incident response, ensuring that security breaches, credential tampering, and revocations are swiftly addressed and contained to minimize impact.

7.7. Ecosystem governance

The ASTF defines the common rules, criteria, and protocols for the Ecosystem stakeholders to build and scale trust, but it doesn't provide an operational framework or detailed operational requirements for the Ecosystem. To operationalize the Aviation Security Trust Framework, ecosystem governance needs to be in place to further define how decisions are going to be made, and specific technical, business and governance requirements are to be followed within the Ecosystem. This is normally described in an ecosystem governance framework, which will be built on the ASTF and establish mechanisms to solicit feedback on the ASTF and evolve it.

Ecosystem governance will clearly describe an operational model for the Aviation Security Trust Ecosystem. The ecosystem governance framework will also include further operational details, such as how each party should perform their responsibilities, what are the incentives for different types of stakeholders, how to implement standards and technologies, and how to manage and mitigate operational risks. If the Ecosystem is to operate Verifiable Data Registries, Trust Registries, as well as other trust services, they will also be further defined in the ecosystem governance framework. The ASTF should provide guidelines for how to develop a governance framework for the Aviation Security Trust Ecosystem.

8. Potential IATA roles and service offerings

Recognizing that the ASTF is a critical path for a better digital future for aviation security, IATA has put serious considerations into the roles our organization could play in making the ASFT a reality and in enabling aviation security stakeholders to join along and benefit from it.

8.1. Developing and operationalizing ASTF

IATA has long been creating and promoting aviation security standards and running auditing and certification programs to facilitate compliance of standards and regulations for aviation stakeholders. IATA envisions our organization to play a significant role in creating and operationalizing the ASTF.

8.1.1 Developing the ASTF

This white paper is intended to define and introduce the core components of the ASTF so that the aviation security stakeholders can further align on a collective vision for their digital future and agree to work together on developing the ASTF. Building on our experience in facilitating the development of aviation standards, IATA can lead the ASTF development in close collaboration with aviation authorities, aircraft operators, and other key stakeholders and create an ASTF that meets the needs of stakeholders to build and scale trust in today's rapidly evolving digital landscape.

IATA has proven processes for stakeholders to collaborate on industry-wide initiatives. There are also similar efforts in the digital trust space that involve broader public engagement our organization can reference; for example, the development for the private sector profile of the Pan Canadian Trust Framework by the Digital ID &. Authentication Council of Canada (DIACC).

8.1.2 Operationalizing the ASTF

8.1.2.1 Ecosystem governance and governance body

As discussed in a previous section, there needs to be an ecosystem governance framework that further defines the operational model and detailed business, technical, and governance requirements for how to meet the trust requirements in the ASTF. Depending on the level of details ASTF gets to, the structure and content of the ecosystem governance framework may vary. The ASTF will eventually become a part of the ecosystem governance framework.

A top priority for the ecosystem governance is to address how to make decisions for the Ecosystem. This is particularly important for an ecosystem of diverse stakeholders with diverse needs. Making sure that the broad stakeholder interest is represented at the decision-making level is key to the health of the Ecosystem.

With the collaborative foundation of the ASTF, IATA can continue to lead the facilitation of the development of the governance framework with the stakeholders and define the working mechanisms for the governance body, on which IATA can assume a position as well.

There are some frameworks in the digital trust space that IATA can reference, for example:

- Trust Over IP Foundation (ToIP) Ecosystem Governance Framework: The ToIP Framework is developed particularly for ecosystems that aim to implement the emerging digital trust standards, such as W3C VCs and DIDs. The Global Legal Entity Identifier Foundation (GLEIF) developed its verifiable Legal Entity Identifier (vLEI) program by building on the success of their LEI governance and leveraging the ToIP models.
- IEEE's Blockchain Governance Standards: The IEEE framework was developed for blockchain governance, but it is broadly applicable to ecosystems of a diverse group of independent stakeholders who want to achieve alignment and common practices within an ecosystem while maintaining a good control and

autonomy of their own processes. It provides a simple framework to define the roles of involved parties, the processes to be followed, the creation and implementation of policies, and a clear understanding of the incentives for all stakeholder groups.

8.1.2.2 Operational Framework and Leadership

Often included as a part of the ecosystem governance framework, an operational framework defines clear procedures for how to participate in the Ecosystem, such as terms of participation, application forms, and onboarding processes.

As a trade organization, IATA is a good candidate to become the operational body, leading the development of the operational framework and day-to-day operations of the Aviation Security Trust Ecosystem (e.g. managing applications, onboarding participants). The World Health Organization (WHO) sets a good example of operational leadership through its Global Digital Health Certification Network (GDHCN).

8.1.2.3 Technical architecture and implementations

Recognizing that aviation security stakeholders are at the different stages of digital transformation, IATA can provide more concrete guidance to stakeholders and support them in building ASTF-based trust solutions. This may include creating reference architecture and reference implementations for digital solutions using the decentralized trust technologies aligned with the ASTF.

The reference architecture will provide a structured, scalable, and interoperable technical framework that supports aviation security stakeholders in issuing, holding, and verifying credentials and associated documents interoperable within the Ecosystem. The reference implementations will include critical trust ecosystem components. They may leverage some of the existing technical components developed for or outside of the aviation industry that align with the ASTF.

8.2. Potential IATA service offerings

Once the ASTF is implementable through a governance and operational framework, IATA can assist stakeholders in operationalization through consulting and training services. IATA can also develop audit and certification programs and potentially extend them to include an interoperability test facility.

IATA has also identified additional opportunities where the organization can offer value to aviation security stakeholders and help them accelerate the digital transformation process: 1) Trust Registry and notary services; 2) Verification API and services; and 3) Fully managed trust services.

8.2.1 Trust Registry and notary services

Understanding that the implementation of key ecosystem components, such as issuance and verification infrastructures, Digital Wallets, VDRs (Verifiable Data Registries), will likely lie in the hands of aviation stakeholders themself, IATA may take on the implementation of a Trust Registry and related notary services for aviation security by building on our existing trust relationships with stakeholders.

As discussed in an earlier section, Trust Registry provides the critical human trust factor for the Ecosystem. The Trust Registry of the Ecosystem will speak to the legitimacy of a stakeholder's role within the Ecosystem, which could be the determining factor of whether a participant is trusted by the rest of the players. It also provides critical information for stakeholders to make nuanced trust decisions when needed.

This white paper has simplified the function of the Trust Registry to lists of authorized credential Issuers of the Ecosystem for the ASOP / SSP use case only, but as the Ecosystem scales, the same issuers may continue to expand their credential issuance services beyond ASOP / SSP Letters of Approval and the lists may grow to include authorized Verifiers and Digital Wallets as well.

The Trust Registry (also referred to as Trust List) and notary services will involve:

- Trust Registry of ASTF participating organizations
  - Issuing authorities for ASOP and SSP Letters of Approval
  - Participating aircraft operators that can issue their own credentials
- Metadata Services: Each participating organization will need to provide certain metadata to become a listed entity on the Trust Registry. Examples of metadata include:
  - Legal entity identity Information: Legal name, address, website, unique entity identifier, official representative/Accountable Manager, etc.
  - Aviation security information: CSO Name, CSO Contact, NCASP program (secure URL), AOSP/SSP Documents (secure URL), etc.
  - Service and technical Information: credential service (e.g. ASOP/SSP Letters of Approval), DID/public key (secure URL), revocation list (secure URL), etc.
- Vetting and Notary Services:
  - Real-world identity of participating organizations
  - Authenticity of metadata provided

Please see a conceptual Trust List example at https://astf.iata.org

8.2.2 Verification APIs and services

The Trust Registry and notary services described above serves as a directory of information that is fundamental to making trust decisions. However, to consume such information when making decisions, aviation security stakeholders will likely need additional verification services that can support them to consume Trust Registry information in a convenient manner.

Therefore, IATA could provide verification APIs to enable secure, real-time verifications:

- Issuer check: API end point(s) to check with the Trust Registry whether a credential was issued by a trusted issuer that is authorized to issue such credential.
- Public key validation: API end point(s) that can access the DID/Public Key (secure URL) provided by the issuer to verify whether the credential was issued by the said issuer.
- Status verification and revocation checks: API end point(s) that can access the revocation list (secure URL) and other relevant data/URLs to check whether the credential is active and has not been revoked.
- Authentication services: API end point(s) that can access protected participating organizations' data, such as NCASP program, AOSP/SSP Documents (secure URLs) so that only properly authenticated parties with the right authorization could access certain information.

Verifiers can use these APIs to integrate verification services into their existing platforms and applications. The combination of the notary and verification functions would create a reliable, interoperable system for verifying aviation security credentials in a way that aligns with the ASTF.

Please see a conceptual verification service example at https://astf.iata.org

8.2.3 Fully managed trust services

As requested by some, IATA also considers providing fully managed trust services that offer critical issuance, holding, and verification capacities as well as related document management services to stakeholders that need these to start their digital transformation journey and participate in the Aviation Security Trust Ecosystem.

Please see a conceptual example of the fully managed trust services at https://astf.iata.org

9. Conclusion

A better digital future for aviation security takes collective and collaborative effort of all critical stakeholders. By writing this white paper with a thought leader in the digital trust space, IATA hopes to invite these stakeholders and experts and practitioners from the digital trust space to work with us and build this future together.

IATA recognizes that many challenges lie ahead of us, especially the fast-evolving cyber threats that require us to move rapidly to deploy standards and technologies. This makes even more critical that the aviation security stakeholders align on an interoperable, scalable framework to digital trust, so the industry can evolve faster. With this foundation, the aviation security industry will be more confident in our future investments in digital transformation and our ability to combat existing and new challenges.

If this white paper resonates with your vision and thoughts, please let us know and provide feedback. IATA looks forward to engaging with many of you as our organization proceeds with this important work.