Aviation Identification & Authorisation System

Whitepaper Version 1
August 2015

Non-Confidential

Introductory Note

This whitepaper, published by IATA on its website, is a testimony to the decided and relentless pursuit for action towards enabling the future of Paperless Aircraft Operations. The continuous innovation motive on which the aviation community evolves creates both the opportunity and the obligation for IATA and its constituency to be active in defining and building this paperless future instead of passively submitting to a non-participative and outside imposed reality.

This document captures the expert perspectives of members of the aviation community, including airlines, airplane manufacturers, and information technology and security experts. Moreover, and of pervasive importance, the ideas and proposals summarized in this whitepaper reflect the firsthand experience and search for solutions driving the quest of the relevant expert aviation community.

The publication of this whitepaper should be perceived as the IATA recognition and acknowledgement of an area that must be efficiently addressed by airlines and all aviation stakeholders in a way consistent with the evolution of information technology and supporting security mechanisms.

By publishing this whitepaper IATA is re-affirming its strong belief in the paperless future of the airline operations as well as its firm engagement in supporting all approaches that could bring such a future to fruition. It is from this perspective that IATA assumes a stakeholder role of the present whitepaper published to stimulate the unrestricted and more dynamic participation of all concerned parties.

In commending all contributors for their input, IATA would like to welcome the public review of this whitepaper and is committed to play a prominent role in the development and implementation of an Aviation Identification and Authorisation System that would answer the needs of the aviation community in general and those of the airline segment in particular.

Let us invite you to consider this whitepaper and share your conclusions and proposals via e-mails addressed to AIAS@iata.org.

Contents

1. Intent of this document ... 4
2. Executive Summary ... 4
3. Problem Statement: The industry need ... 5
4. Proposed solution ... 6
4.1 Evolution and future proofing of the solution ... 7
5. The benefits ... 7
5.1. Interoperability benefit explained ... 7
6. The need for a roadmap ... 7
7. Example supported use case ... 8
8. Industry Action / Next Steps ... 9
9. Conclusion ... 10

Appendix: Background & Additional Details

A-1. Paper based policy & previous implementation ... 11
A-2. Electronic Signature policy & previous implementations ... 11
A-3. Background: Standards making efforts ... 12
A-4. Background: Today's infrastructure & environment ... 13
A-5. Solution requirements & desired characteristics ... 13
A-6. Proposed infrastructure details ... 14
A-6.1. Aviation trust network and associated infrastructure ... 15
A-6.2. The Certificate Authorities (CAs) ... 16
A-6.2.1. The Bridge CA's and federation ... 17
A-6.2.2. Bridge outside the federated CA's structure ... 17
A-6.2.3. Aviation industry policy ... 18
A-6.3. The PIV-AV smartcard ... 18
A-6.3.1. The basis PIV-I ... 19
A-6.3.2. Building a standard with use of PIV-AV ... 19
A-6.4. PIV-AV scope of use ... 19
A-6.4.1. Visual identification ... 19
A-6.4.2. Access control ... 20
A-6.4.3. Device and/or application access ... 20
A-6.4.4. Electronic Signing & Data Integrity ... 21
A-6.4.5. Data security ... 21
A-6.4.6. Authorisation ... 21
A-7. Glossary ... 22
A-8. References ... 23

List of Figures

Figure 1: Aviation Identity & Authorisation System high level diagram ... 6
Figure 2: Aviation Identity & Authorisation System high level diagram (with flagged items) ... 15
Figure 3: Single bridge with connected aviation Certificate Authorities (CA) ... 16
Figure 4: Connected Bridges joining several trust groups ... 17
Figure 5: Industry Root connecting multiple Bridge CAs ... 17
Figure 6: Industry Policy Cloud ... 18

1. Intent of this document

A common framework for Identity Management and Electronic Signatures is needed for the aviation industry to gain the most from a transition to paperless aircraft operations and mobile application platforms. This document intends to make the case for a common interoperable Aviation Identification & Authorisation System (AIAS) and the supporting policies & procedures for use in the aviation flight and maintenance operations environments. A target framework and its characteristics are described here. A future revision to this document will add a detailed industry roadmap for steps to be taken toward achieving the proposed interoperable framework.

2. Executive Summary

The commercial aviation industry is striving to improve efficiency of all aspects of aircraft operation processes by making them paperless and electronically enabled. Although there are several initiatives underway at various airlines, these have been started so far without the benefit of an accepted "standard" interoperable solution for identity management & authentication. Due to the lack of a common approach, these customized projects are generally not suitable for cross organizational use and therefore not beneficial for the industry in general.

The transition to paperless aircraft operation has not yet been fully achieved. The example of the Aircraft Logbook, which has been seen throughout the industry as a desirable function to go paperless, illustrates well this idea. More than 10 years after the earliest trial implementations the industry is just now beginning a more widespread deployment of electronic logbook applications. This is in part due to the lack of a clear business case driven by uncertainty in how to design and implement a supporting identity and authorisation management system for an application which has users across many organizations (direct airline employees, contract personnel, third party MRO providers, etc.).

In addition to individual airline projects, several industry groups are working toward standards and recommended practices which enable paperless operations:

- ATA DSWG, Digital Security Working Group (ATA Spec 42)
- ATA ELPT, Electronic Logbook Project Team (ATA Spec 2000, Ch. 17)
- ATA RDIG, Regulatory Documentation Interest Group (ATA Spec 2000, Ch. 16)
- ATA Configuration Management / Traceability Interest Group (ATA Spec 2000, Ch. 9)
- IATA ALAG, Aircraft Leasing Advisory Group
- IATA Paperless Aircraft Operations initiative

More details of the above group activities can be found in Section A-3. One thing in common between all of the groups is their identification of the need for Electronic Signature universal acceptance and standardization (providing both individual Identification & Authorisation). The lack of such "standard" way of identifying users and securing data has slowed the transition to a more efficient, electronic and paperless environment. A common AIAS could be seen as a strong incentive to initiate (and financially justify) many of these paperless projects.

Several electronic application areas which could benefit from an AIAS are:

- Aircraft Technical Logbook applications (discrepancy logs, fuel records, cabin logs)
- Flight Folder applications (dispatch instructions, flight plan & loadsheet, journey logs, weather information, NOTAMS)
- Airworthiness compliance systems (configuration control & maintenance program)
- Maintenance recordkeeping systems
- Aircraft ownership and lease transfers
- Regulatory documents (XML FAA 8130 / EASA Form 1 / TCCA Form 1)

This whitepaper proposes a framework which will enable several of the above recordkeeping & signature processes to be supported in an accepted common way for the purposes of user identification, authorisation, creation and validation of electronic signature information. This framework will include the capability to use credentials issued by a variety of aviation organizations, which can be trusted and verified by another organization, both to authorise access to applications and to accept electronically signed data.

3. Problem Statement: The industry need

Airlines currently considering adopting electronic replacements to paper processes most often encounter the requirement to provide and manage assurance of user identity, to perform an authorisation check and/or to record a signature. In addition, these requirements often cross organizational boundaries where, for example, a transaction attempted by personnel of one organization (e.g. an MRO provider) would first require identity and authorisation verification performed by a second organization (e.g. an aircraft operator). With a wide variety of methods currently in existence to perform these functions electronically, but without an industry defined or recommended standard, the likelihood that development programs build toward an interoperable framework is not assured.

In lieu of a standard AIAS, business and technical rules would have to be negotiated between the parties in each application where interoperability is needed based on the use of electronic Identification & Authorisation (see below “Interoperability Benefit Explained”). To accomplish this for each data exchange between two parties is a time consuming and costly process. This makes it difficult to transfer the above mentioned areas into paperless and electronically enabled processes and, therefore, puts potential benefits on hold for the industry. The aviation industry needs a commonly accepted solution to tackle the following related challenges:

- Identification and authentication of the person
- Authorisation for the particular action
- Physical access control(which can be seen as a variation of Authorisation)

These challenges could be approached as layers identified in a roadmap fashion and allowing for growth of the solution framework.

4. Proposed solution

The proposed AIAS framework will enable recordkeeping & signature processes to be supported in a common way for the purposes of user identification, authorisation and application of electronic signature information (see Figure 1). AIAS relies on common credential issuance policies (i.e. ATA Spec 42), a standard identification card for user storage of electronic credentials (i.e. PIV-AV - see Section A-6.4.6), and a verification process which uses connected aviation user management systems (i.e. the aviation trust network) and standards for security assertion. The technical standards supporting AIAS would define the specific methods for transmitting credential information for the purpose of an authorisation check, the method of performing electronic signature creation, and the data structures used when electronic signatures are created, transmitted, validated and stored/archived.

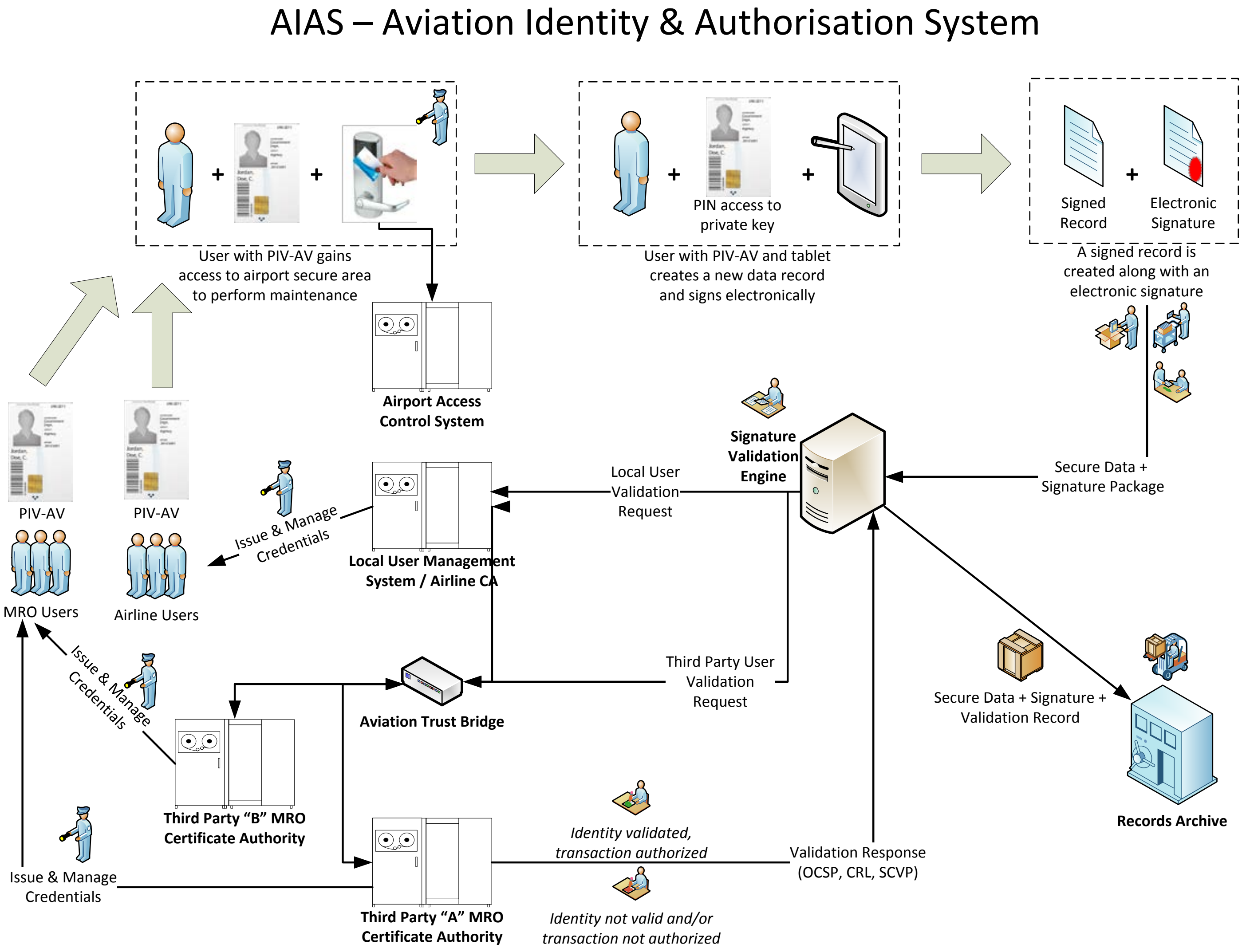

AIAS – Aviation Identity & Authorisation System
+
+
User with PIV-AV gains access to airport secure area to perform maintenance
+
PIN access to private key
+
User with PIV-AV and tablet creates a new data record and signs electronically
Signed Record
+
Electronic Signature
A signed record is created along with an electronic signature
Airport Access Control System
PIV-AV
PIV-AV
MRO Users
Airline Users
Issue & Manage Credentials
Local User Management System / Airline CA
Local User Validation Request
Signature Validation Engine
Secure Data + Signature Package
Issue & Manage Credentials
Aviation Trust Bridge
Third Party User Validation Request
Secure Data + Signature + Validation Record
Records Archive
Third Party "B" MRO Certificate Authority
Issue & Manage Credentials
Third Party "A" MRO Certificate Authority
Identity validated, transaction authorized
Identity not valid and/or transaction not authorized
Validation Response (OCSP, CRL, SCVP)

Figure 1: Aviation Identity & Authorisation System high level diagram

The AIAS depicted above provides the ability for a minimal set of technology components to provide a set of functionalities serving both access control, identity assertion and electronic signature. Components of AIAS are discussed in more detail in Section A-6.

4.1 Evolution and future proofing of the solution

While the success of the proposed AIAS framework will initially depend on the use of proven technology, the framework is living in an evolving environment. Therefore it can be foreseen that over time, the AIAS framework will adapt to emerging technologies supporting identification and authorisation. The introduction of these new technologies is anticipated to further benefit the processes and procedures of the AIAS framework and, in light of the technology evolutions, future proofing of any solution and/or its implementations is recommended.

5. The benefits

Definition of an AIAS will relieve the airlines from researching and specifying an Identification & Authorisation system themselves and will instead provide a template for their development of a system compatible with the rest of the industry. AIAS will greatly help the industry in rolling out systems by providing policy, procedures, technology and information standards. Acceptance of a standard AIAS architecture will result in reduced project costs and shorter implementation times and will provide to the industry the interoperability required by many electronic recordkeeping applications.

5.1. Interoperability benefit explained

Airlines manage their operations with a multitude of IT systems & solutions covering many different operational domains (e.g. flight, maintenance, cabin service, etc.). Between one airline’s internal departments, and between an airline, its vendors & suppliers, there is a need for a common solution to the identity & authorisation requirement. Moreover, as vendors and suppliers work with more than one airline, the system should be able to avoid multiple different approaches that will create more complexity and confusion. An interoperable standard will avoid multiple point solutions that are either not common or, at worst, conflicting. In addition, government bodies and aviation regulatory agencies will need to support a common framework.

Without initially considering interoperability, the industry runs the risk that costs will increase due to implementation of various paperless/electronically enabled point solutions which IT solution providers would need to develop and support in multitude. These costs would likely outweigh the potential benefits a paperless operation can achieve.

6. The need for a roadmap

One primary basis of electronic business is electronic identification, which is needed for both internal transactions and those between companies. Establishing common methods for creating and managing electronic credentials and for authenticating identity is the logic first step toward a “Federated AIAS” framework.

Once an identity framework is established, the next step would be to find common understanding for answering the question: Is this person authorised to perform the transaction or to sign the data in question? This is a far more complicated subject than merely identifying a person because a number of business rules must typically be applied before an answer can be given. Therefore three high level approaches can be identified:

- The attestation is the individual's responsibility (e.g. a statement about authorization is included in the signature process indicating "the signer acknowledges he/she is authorized to perform the documented action".)
- The back office system performing the identity authentication also provides authorization for the transaction (e.g. based on the type of data being signed and on which type of aircraft, etc.)
- The smartcard used for the electronic Identification & Authentication holds the information for off line authorisation and what action (including access) will be allowed.

These subjects will need to be addressed in a roadmap fashion, allowing for growth of the framework.

7. Example supported use case

The example taken here is an electronic logbook implementation. In the logbook several groups document and sign for actions taken: pilots accepting the aircraft for flight or reporting defects; cabin crew reporting both service and technical defects; fueling department for a fuel uplift; engineer/mechanic releasing the aircraft or "signing off" of a repair. Even within a single airline it is a challenge to make all these people from the different departments known in an electronic logbook system and significant effort is required to maintain a user database through administration by the associated departments.

Going outside an individual airline, and extending to third party handling agents and Maintenance, Repair and Overhaul (MRO), organizations complicates identity management even further. The electronic logbook system relies on a secure identity credential from each of the users which supports creating electronically signed records. A common requirement for electronic signing is to provide credential security and identity assurance through a chain of trust where the authority to issue credentials is delegated. The airline would need a "local notary" to ensure this and a process for delegation and for identity proofing and vetting: all time consuming and expensive process steps.

A logbook system implementation using the AIAS framework would instead rely on standard user identification & authorisation methods, including standardized policy & procedures for issuing credentials. In addition, AIAS will include standard methods for relying parties to make authentication queries, for systems to respond with security assertions, and for systems to create, transmit and validate electronic signature information. Once part of the "Aviation Federation of Certifying Authorities", an airline or MRO can provide security assertions to relying parties using electronic recordkeeping & signing applications. The proposed digital credentials release each individual airline from identifying by themselves all of the potential people working on their airplanes or signing into their logbook.

8. Industry Action / Next Steps

Several specific recommendations are made to further align the interests of the aviation industry and to accelerate movement toward a common AIAS. In pursuing these recommendations, we acknowledge that three main challenges have to be always considered and addressed in a direct and realistic way:

- National regulations
- Political implications
- Cultural differences in perception of personal identification and authentication

It is important that all direct stakeholders, as well as their associated group peers, recognize and appropriately address the elements essential to a successful industry wide adoption of a common AIAS approach, including the:

- Open accessibility, free of import-export barriers or intellectual propriety imposed exclusions, to all AIAS parties using the technologies involved by the proposed solution, and
- Sustainable costs, for each one of the playing levels, in implementing the proposed solution.

The specificity of some of the recommendations should be kept open to a permanent validation and cross-reference against evolution of cybersecurity technology. While these recommendations are listed without ranking intention or timing coordination, the harmonization and synchronization of actors and their actions is essential to the successful achievement of the following:

IATA: Release of this whitepaper presenting AIAS and its benefits. Discuss the digital trust network approach in context of other IATA projects. Validate, within its airline constituency, the AIAS architecture and its federated layout with an aviation industry root or as a peer-to-peer system of trust networks. Promote the relevant aviation trust network perspective to regulators and to ICAO. Continue to develop, as applicable, the AIAS whitepaper to include roadmap of steps to take toward AIAS target. Facilitate effort coordination between entities like Smartcard Alliance, AAAE, ACI, TSA and other industry groups.

ICAO: Provide guidance to member states on the role of digital trust network in increasing security of electronic transactions in general and airplane maintenance & operations in particular.

Aviation IT Solution Providers: Build support for ATA Spec 42 eSignature data standards, PIV-AV credentials and security assertion using ATA Spec 42.

Hardware Providers: Add support for smart card readers and/or NFC into devices targeting line maintenance & flight operations environments.

Airplane Manufacturers: Build in support for PIV-AV credential and interface standards into aircraft design and in after-market services & software offerings.

Airlines: Plan for future digital credentials. Include CA & connection to trust network in short/medium term IT system planning. Work with local regulatory agency personnel to build plans to introduce electronic signatures & validation mechanism. Plan migration from local UMS validation (if employed as initial implementation) to validation using AIAS trusted network.

ATA: Continue DSWG effort to specify PIV-AV and best practices for signature data exchange, validation & archive. Add discussion of security assertion methods (e.g. SAML, ABAC, RBAC) to Spec 42. Establish recommended policy for airlines assigning staff in local active directory and/or UMS and their further issuance of digital credentials (e.g. length of validity, etc.). Continue ELPT effort to define line maintenance data exchange formats including those supporting electronic signature & validation records.

AEEC: Define standards for airplane hardware (EFBs and/or Onboard Networks) and interfaces which support the required technologies of PIV-AV, including contact or contactless card readers.

9. Conclusion

The need to constantly increase the efficiency of aircraft operations processes, motivated by financial goals, drives the need for an electronic signature solution as common as the traditional pen and paper approach. An overnight solution (a “big bang” event) where everyone has, for example, a PIV-AV card, devices that can read them plus an operational approval for an electronic recordkeeping & signature system, is unthinkable. However, the standard platform (AIAS) describing such a framework is necessary to allow for an incremental rollout of the platform which does not require the industry to wait for a “big bang” event. With a common interoperable framework goal, the industry will be enabled to develop paperless technology solutions that will increase the overall efficiency of the industry.

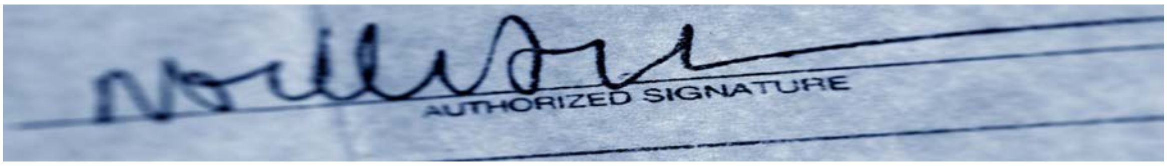
The AIAS platform is defined as a target while recognizing the implementation challenges. As a next step in updating this whitepaper, a more detailed implementation roadmap will be established to make AIAS incrementally achievable by parties in the aviation industry. The roadmap will help the industry achieve increased operational efficiency and security in moving toward the AIAS framework.

Appendix: Background & Additional Details

The following sections, which constitute the Appendix of this Whitepaper, are based on the present day validated level of technology and, as such, focus on the PKI approach. The reader should bear in mind that future evolution of identification and security technology may bring significant other approaches that should be considered.

A-1. Paper based policy & previous implementation

With the introduction of electronic signatures the pen and paper is being replaced. However, the electronic versions have one big disadvantage compared to the pen and paper: the globally accepted standard of the handwritten signature. Whether it is a signed EASA form 1, signatures in Aircraft Technical Logbooks or just signing off for receiving of a document, all over the world it is an accepted fact that the people involved place their signature on the paper document by the process depicted below.



Signature policies and legal jurisprudence on how to determine who signed a paper document are well known, and in addition, no training or special technology is required to respond to a paper form with instructions to "please sign" with a box or line for the signature. This combines with known methods used by graphologists in legal repudiation cases to form the "standard" for paper based signatures. In trying to replace the well-known pen and paper signature and validation process with an electronic solution, it is the globally accepted standard that is still missing!

A-2. Electronic Signature policy & previous implementations

Certain electronic signature approaches have been already used by various industries around the world. The simple log-on to a computer, the pin-code used in a Bank ATM transaction without a paper signed-off document of the transaction or the UPS "brick" used in package delivery transactions are essentially implementations of an electronic signature approach.

Many countries have enacted legislation defining the legality & limitations of electronic signatures replacing pen & paper signatures. Generally, these laws state that the electronic signature can be equivalent to the pen & paper one provided certain characteristics of the signature are assured (e.g. see US PL 106-229, Electronic Signatures in Global and National Commerce Act (E-Sign), June 30, 2000).

Further, in aviation, several regulatory agencies have issued advisory information of a similar flavor to national law, stating the requirements for an approvable electronic signature. FAA, EASA, Transport Canada, Singapore CAAS and other regulatory agencies have released advisory documents on the Subject. The FAA AC 120-78, being one of the first advisories, can be seen as the model for this advisory information to date. It defines the required characteristics of an electronic signature as one providing:

- Uniqueness
- Significance
- Signature Scope
- Security / data integrity
- Non-repudiation
- Traceability / identification

Other forms of aviation advisory information can be found in EASA AMC 20-25, Transport Canada AC 571-006, Singapore CAAS AC 1-2(0), etc. These recommend the same set of required characteristics and the process for seeking operational approval to use such a system.

Several implementation examples of electronic signatures exist in aviation today, notably signature solutions supporting:

- Electronic FAA Form 8130-3 & EASA Form 1 data exchange
- Electronic logbook applications
- Software part creation, distribution & loading

These solutions utilize a range of solution options, from user ID & password solutions to digital signatures based on PKI. All have taken steps to ensure adherence to the aviation advisory information, and all in use have been subject to local regulatory agency operational approval.

A-3. Background: Standards making efforts

The related standards making efforts to date have primarily focused on electronic signature data creation & data exchange between organizations. These include:

- ATA Spec 2000, Ch. 16: defines an XML format for electronic part certification documents (FAA Form 8130-3, EASA Form 1, etc.) and the signature to accompany the form data
- ATA Spec 2000, Ch. 17: defines XML format for electronic logbook data exchange including structure for electronic signatures, validation records and an overall packaging structure to include all in an XML dataset
- ATA Spec 42: defines the security principles applicable for aviation electronic data systems, and more specifically methods for using electronic credentials to sign and secure data within these systems and data for exchange with third parties. This specification currently focuses on application of PKI but is expanding to non-PKI credential requirements.

In addition to formal standards making bodies, IATA has chartered the Paperless Aircraft Operations initiative. This group is motivated to describe the vision of a paperless airline operations supply chain and aircraft maintenance processes, and to define the most relevant focal areas for improvement. The group has focused on electronic & digital signatures as a key area for improvement and one which demands a common industry approach.

The IATA group has identified several elements currently missing in the industry: a description of the minimum requirements for electronic identity & signature; a definition of a target system which meets those requirements and employs the standards; and a roadmap for taking the industry from its current state to the target. This Whitepaper is an attempt at filling some of these gaps and to provide the direction toward which future efforts in the aviation industry can be executed.

A-4. Background: Today's infrastructure & environment

Although "paperless" and "less paper" operations have been pursued in many industries in the last several decades, the line maintenance environment at most airline operators remains heavily paper oriented. Electronic access to recordkeeping systems and to reference material is provided to line mechanics, but most often the instructions coming out of maintenance planning systems are printed, and recordkeeping of line maintenance is written on the paper task cards that have to be signed off to indicate "work completion". Many efforts are underway to eliminate first the paper recordkeeping of tasks completed and to instead begin with direct entry of actions into electronic MRP systems. The next step of this is to provide a mobile platform for proving this capability at the airplane as opposed to only at a line office with a terminal computer.

The mobile devices utilized in line maintenance range from laptop computers, to more recent tablet computers and smart phones (iOS, Windows and Android devices all have been deployed in varying numbers). In certain environments, these are used in conjunction with barcode readers (most commonly used in baggage handling operations), and RFID readers (still not very common).

Typical identification devices and credentials used by line engineers for identity and access control are photo ID badges (often times one issued by the airline and a separate one issued by the airport authority), rubber stamps or chops (typically with a unique stamp number), rolling code generators, USB dongles, and client certificates loaded onto the devices mentioned above. Many airlines & airport authorities have utilized RFID in ID badges to support proximity readers for access control. A small minority have specified ID cards capable of storing certificates or biometrics (e.g. smart cards) for use in airport access control.

Several onboard systems have been installed on commercial airplanes in the last decade to assist with improving the efficiency of flight operations and line maintenance. These include older Central Maintenance Computing systems, and more recent Electronic Flight Bag and onboard server & network systems. These are typically used in conjunction with airplane provided air-ground communications capability to move data collected onboard to airline back-office systems. In addition, many newer aircraft have passenger networks (IFE systems) with similar characteristics of onboard computing & display combined with off-board connectivity.

A-5. Solution requirements & desired characteristics

The proposed solution should meet several fundamental requirements, some derived from the operating environment of airline flight operations & line maintenance, others based on business or regulatory agency requirements:

1. Suitable for use in a high stress environment with factors such as, but not limited to: noise, dirt, grease, oil, fuel, weather, time, pressure and darkness. (Combination of device & credential requirement.)
2. Compatible with: current technology deployed to airplanes or those coming online within the next two years; existing EFBs & onboard networks without card readers; current mobile devices, with some support of NFC or smartcard readers. (See Section A-4).

3. Airplane to ground data communications must be supported by current connectivity environment (where the minimum bandwidth is represented by VHF ACARS)
4. Users assigned one credential by their employing organization which can be used to provide the following functions:
    a. Access control to multiple physical locations
    b. Authorise access to one or many applications on multiple airlines hardware
    c. Store identifying and signing digital certificates
    d. Directly perform cryptographic signing computations (private key does not leave credential)
    e. Store biometric information (for optional future use)
5. Cross organizational signing & verification, to allow identification & validation of a third party MRO employee performing work for first party airline, providing improvement compared to paper signature & validation process
    a. Acceptance of e-signature validity by regulators of other stakeholders (e.g. lessors, parts pool providers)
    b. Acceptance of e-signature validity between two operators under a common regulatory agency
    c. Acceptance of e-signature validity between operators in different regulatory jurisdictions? (e.g. will an electronically approved repair be used/useable by all parts pool participants operating in different countries?)
6. Authorisation check to prevent maintenance documentation errors & regulatory compliance issues. Phase 1: disallow mechanic from completing a signed transaction after they have left their company. Phase 2: disallow mechanic from completing a signed transaction with expired qualification training or license
7. Meet guidance provided by aviation advisory information and constitute an operationally approvable system per AC 120-78, et al.

A-6. Proposed infrastructure details

The AIAS high level diagram proposed below, in Figure 2, is considering only the PKI solution which, as mentioned in the beginning of the Appendix section, is currently the leading (if not the only) available solution.

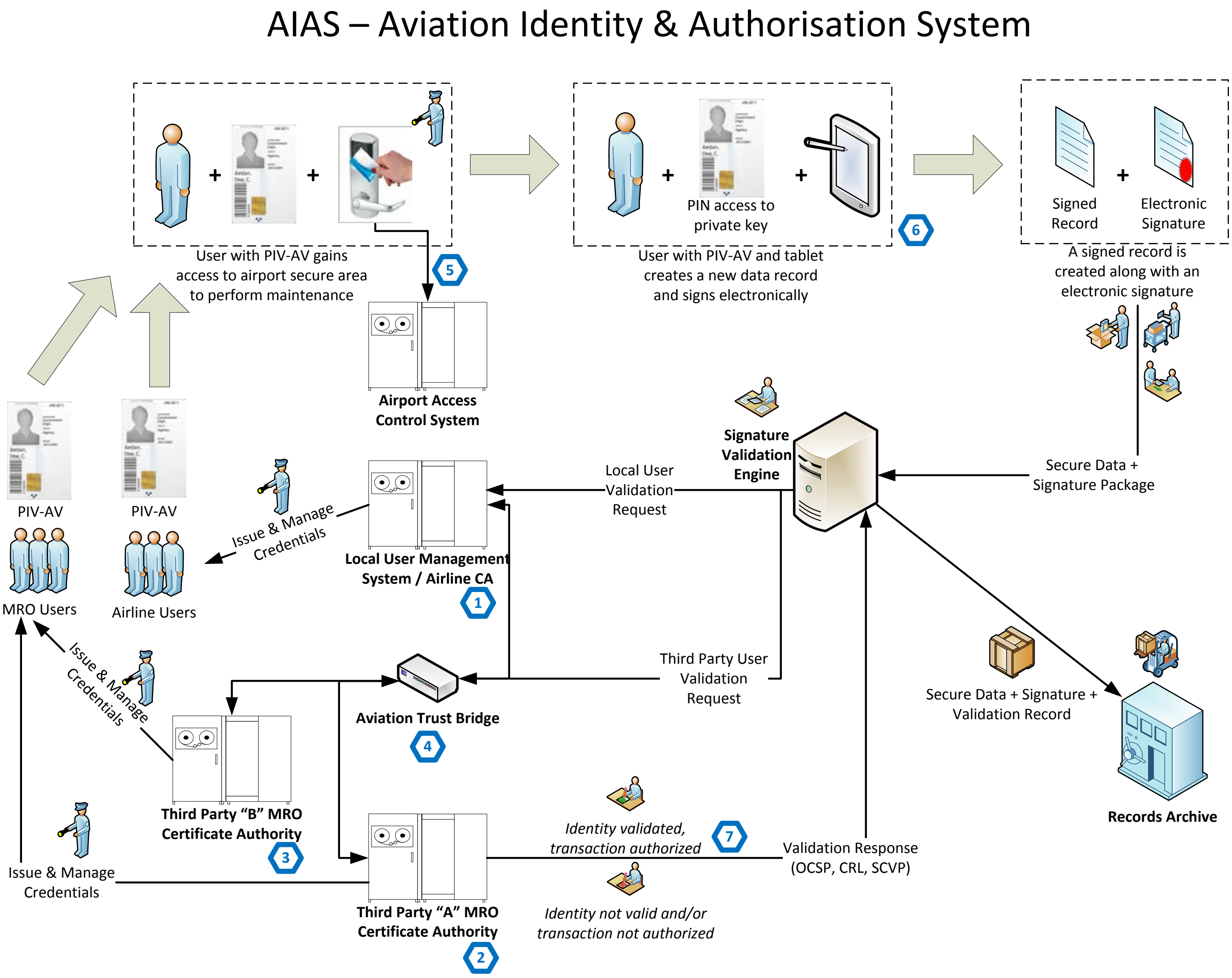

AIAS – Aviation Identity & Authorisation System
+
+
User with PIV-AV gains access to airport secure area to perform maintenance
5
+
PIN access to private key
+
User with PIV-AV and tablet creates a new data record and signs electronically
6
Signed Record
+
Electronic Signature
A signed record is created along with an electronic signature
Airport Access Control System
PIV-AV
PIV-AV
MRO Users
Airline Users
Issue & Manage Credentials
Local User Management System / Airline CA
1
Local User Validation Request
Signature Validation Engine
Secure Data + Signature Package
Issue & Manage Credentials
Aviation Trust Bridge
4
Third Party User Validation Request
Secure Data + Signature + Validation Record
Records Archive
Third Party "B" MRO Certificate Authority
3
Issue & Manage Credentials
Third Party "A" MRO Certificate Authority
2
Identity validated, transaction authorized
7
Validation Response (OCSP, CRL, SCVP)
Identity not valid and/or transaction not authorized

Figure 2: Aviation Identity & Authorisation System high level diagram (with flagged items)

A-6.1. Aviation trust network and associated infrastructure

To enable the industry to use a common, interoperable AIAS in the airline aircraft operations environments (i.e. flight, technical, ground), a trust network and supporting infrastructure needs to be set up based on standards. Such a system will allow participating Certifying Authorities to issue certificates and storage of these electronic credentials on a smartcard. The credentials can be used for many purposes within the trust network.

Setting up CA services might be a challenge for some airlines. The business case to have such services in-house needs to be made by the individual airline and the outcome will depend on volume of users and scope of use. The existence of CA service providers could nevertheless alleviate the possible "burden" associated with the entry into the trust network. There are already several such service provider entities which offer all these services so that the airline is set free of implementing the framework.

Next to the trust network and a standard smartcard, Aviation IT solution providers will need to build support for ATA Spec 42 data standards, the PIV-AV credentials, and supporting security assertion using ATA Spec 42. Also the hardware providers will need to support this smartcard technology in the form of readers and/or NFC enabled devices, targeting line maintenance & flight operations environments. For use cases on board of the aircraft, the OEM's need to support the standard in adopting the readers and/or NFC into devices as indicated above, possibly integrated with the aircraft information technology infrastructure.

The airlines using the standard will need to: associate themselves with the aviation trust network and manage the digital credentials; include CA & connection to trust network in short/medium term IT system planning; work with local regulatory agency personnel to build plans to introduce electronic signatures & validation mechanism and also plan to migrate from local user validation (if employed as an initial implementation) to validation using the AIAS trusted network.

A-6.2. The Certificate Authorities (CAs)

[Reference Figure 2: 1, 2, 3]

The general function of the aviation Certificate Authorities (CAs) would be:

- Identification of individuals within their organization, or for an outside organization, performed in accordance with policies and procedures described in ATA Spec 42.
- Issuing of credentials and digital certificates
  - In the form of a PIV-AV smartcard which binds the identity of the certificate owner to pairs (public and private) of electronic keys, stored on the card, which can be used to identify a user, to authorise access to applications or physical locations, and to sign information digitally. These electronic credentials assure that the keys actually belong to the person and organization specified. This is done in accordance with policies and procedures described in ATA Spec 42.
- Creation and maintenance of links to Bridge CAs or equivalent solution. This would be necessary to enable the federated trust network supporting interoperability between airlines, MROs, third party handling agents, regulatory agencies, etc.

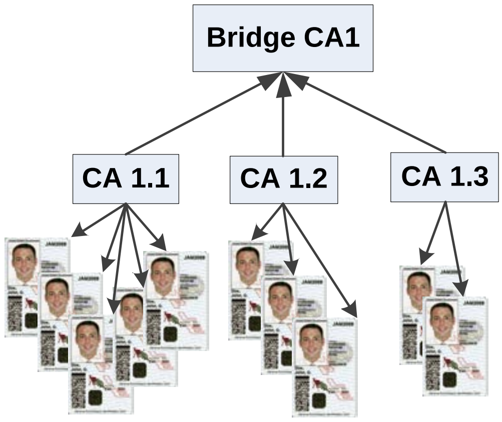


Figure 3: Single bridge with connected aviation Certificate Authorities (CA)

A-6.2.1. The Bridge CA's and federation

[Reference Figure 2: 4]
Successful cross certification to support interoperability within the AIAS, foresees that the applicant, the airline or other "entity" within the aviation industry operates in accordance with the standards, guidelines and practices of the ATA Spec 42 (or equivalent). The harmonized implementation of the standards, guidelines and practices could be supported by a Cross Certification Steering Committee type of forum for which organizations with appropriate international audience, membership and reputation may be called upon to manage (e.g. IATA). Existing CAs and bridged CA networks should be appropriately evaluated for their suitability to support AIAS. For cross-certifications within regions (e.g. internal to the US (the FAA community) or the EU (the EASA community)) the AIAS Certificate Policy would require entities to sign a cross certificate Memorandum of Agreement (MOA) formally describing the terms and conditions of the cross certification.

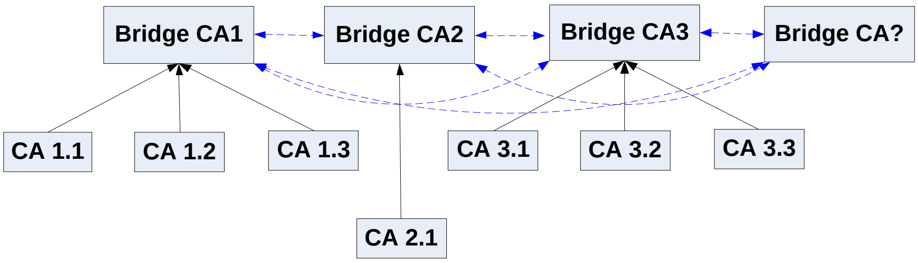


Figure 4: Connected Bridges joining several trust groups

A-6.2.2. Bridge outside the federated CA's structure

Cross certifications with non AIAS Bridge entities require the implementation of cross certification agreements between the AIAS Bridges and an envisioned common industry root certificate provider. The details of these agreements may vary based on the nature of the non Bridge entity and its relationship to the industry root.

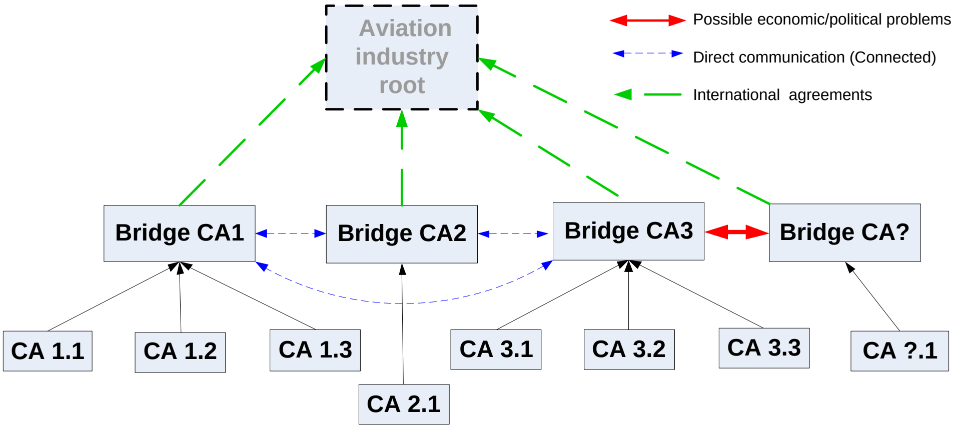


Figure 5: Industry Root connecting multiple Bridge CAs

All of the above would imply that within the trust network, standardized infrastructure and equipment should be used to ensure interoperability.

A-6.2.3. Aviation industry policy

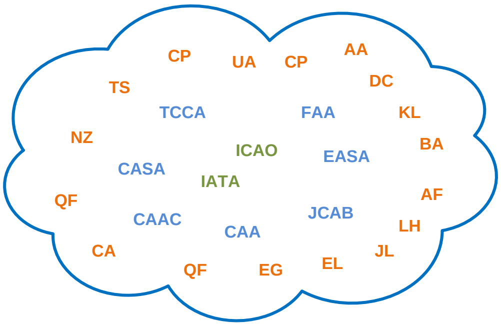


Figure 6: Industry Policy Cloud

The policies which will help govern the creation of AIAS will stem primarily from organizations such as ICAO and IATA.
ICAO in particular works with member states and their National Aviation Authorities toward common rules & regulations for licensing and security requirements which could be supplemented, as applicable, to include electronic recordkeeping provisions.
IATA serves its member airlines by helping promote and enforce standards which benefit industry efficiency (e.g. e-ticketing) and by working with ICAO and the NAAs toward clear and implementable policies & regulations.

These two groups together can work toward defining policies for establishing the trust network, and to define acceptability of relying on the federated trust network for identity and authorisation.

Although not explicitly identified in Figure 6, the suppliers and third party providers should be also involved in due time in the “Industry Policy Cloud”.

A-6.3. The PIV-AV smartcard

The PIV-AV smartcard, as the new aviation standard, has stored credentials, plus a set of extra information. From traditional ID badge credentials use to high assurance credentials, up to the PIV data model credential types with digital certificates for use in a Public Key Infrastructure or for use in cryptography, plus optional biometric information to support high assurance credentials or enhanced operational biometric identification.

The card binds the identity of the certificate owner to a pair (public and private) of electronic keys that can be used to encrypt and sign information digitally. These electronic credentials assure that the keys actually belong to the person and organization specified. Messages, data or documents can now be encrypted and/or signed with the public and private keys of the owner. The receiver can then decrypt the messages, data or documents and validate their origin with the sender’s public key available within the aviation trust network.

A-6.3.1. The basis PIV-I

In response to the US Presidential Directive HSPD 12, the Computer Security Division of the National Institute of Standards and Technology (NIST) initiated a new program to improve the identification and authentication of US Federal employees and contractors to access Federal facilities and information systems. As a result, NIST developed the standard "Personal Identity Verification (PIV) of Federal Employees and Contractors," published as Federal Information Processing Standards (FIPS) Publication 201. The US Secretary of Commerce approved this standard and it was issued on February 25, 2005.

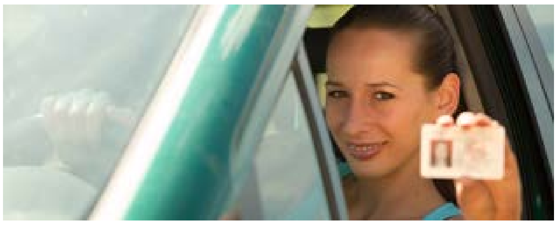
Since then, interest in applying the standard expanded to private enterprise and non-US government organizations resulting in an identity card that is interoperable or compatible with a standard identity system such as PIV. Recognizing this need, the US Federal Chief Information Officers (CIO) Council issued the "Personal Identity Verification Interoperability for Non-Federal Issuers" specification to describe PIV Interoperable (PIV-I) and PIV Compatible (PIV-C) cards

A-6.3.2. Building a standard with use of PIV-AV

Based on the PIV-I standard, the PIV-AV could be used as a multi-use credential, creating flexibility as a Secure Multi-Use Credential. It not only indicates that the cardholder has the privileges, it also could serve as the default credential for establishing that the cardholder can gain access to secure airport areas, sign records in an Electronic Logbook application, and to log on to a computer system or application. Smart card technology can support these current uses along with any additional applications that enhance maintenance convenience and/or airline service efficiency. For example, smart cards provide the unique capability to easily combine identification and authentication in both the physical and digital worlds. This capability can generate significant savings for airlines. A smart card-based Maintenance ID card could not only indicate privileges and allow physical access to services, it could also allow individuals to sign documents, request official papers (e.g., MRO status reports) online, or access secure networks. Multiple applications (with their required data elements) can be stored securely on the smart card at issuance or added after the card is issued, allowing functionality to be added over the life of the PIV-AV ID card.

A-6.4. PIV-AV scope of use

A-6.4.1. Visual identification

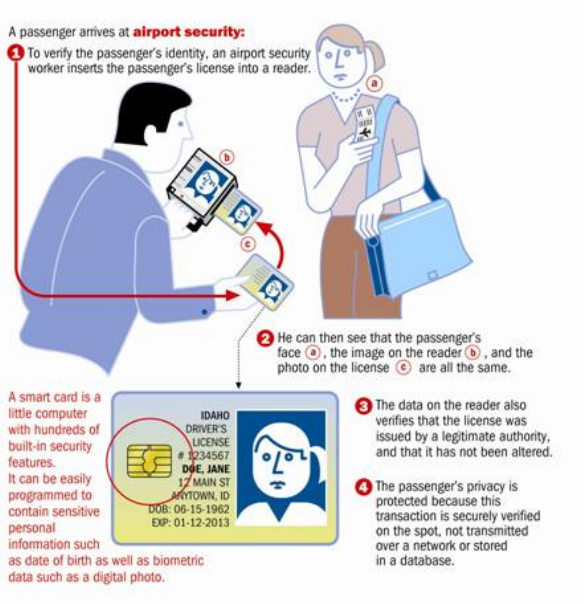


A PIV-AV smartcard can be used to visually identify the card holder based on a picture printed on the card. It also can be used in conjunction with the digital storage of the picture on the card. This use requires a security officer to visually match pictures and faces, a procedure commonly applied in existing security checks for entrance to buildings, airports and airplanes based on photo identification cards.

A-6.4.2. Access control

[Reference Figure 2: 5]

PIV-AV supports a range of additional access control mechanisms beyond simple visual identification based on the photo printed on the card (as described above). This can include automated checks on the validity of the card using the card issuer certificate and usage of biometric information (fingerprint and/or iris scan) stored on the card by electronic gate systems matching them to user biometrics.



A passenger arrives at **airport security:**

1 To verify the passenger's identity, an airport security worker inserts the passenger's license into a reader.

2 He can then see that the passenger's face (a), the image on the reader (b), and the photo on the license (c) are all the same.

3 The data on the reader also verifies that the license was issued by a legitimate authority, and that it has not been altered.

4 The passenger's privacy is protected because this transaction is securely verified on the spot, not transmitted over a network or stored in a database.

A smart card is a little computer with hundreds of built-in security features. It can be easily programmed to contain sensitive personal information such as date of birth as well as biometric data such as a digital photo.

In addition, identity information stored on the card can be used for further authorisation verification by reference to back office user management systems.

It is anticipated airport authorities will initially want to continue controlling the list of individuals with access granted and would therefore want to install their certificate on user's PIV-AV card. While PIV-AV would support an airline issued card having an airport authority certificate later installed, the initial implementations for access control may have airport authorities issuing their single function (airport access), non-interoperable PIV-AV card.

In an advanced view of distributed access control, permission to enter a secure area could be based on user type or license information contained on the PIV-AV card (see also Section A-6.4.6). PIV-AV readers used at entry points to secure flight-line areas could be programmed to grant access to certain groups of people from a variety of organizations, pilots & maintenance personnel from a number of airlines & MROs for example.

A-6.4.3. Device and/or application access

Identity certificates on the PIV-AV card can be used to provide access to hardware resources (through card-readers in the device or through RFID/NFC contactless means). Typically this access would be authorised at the organizational level, but finer control could be applied to individual users (see Section A-6.4.6). Corporate Access Authorisation Systems (e.g. SSO

using Active Directory, LDAP, SAML, etc.) will apply these finer controls based on information available in the back office systems.

A-6.4.4. Electronic Signing & Data Integrity

[Reference Figure 1, **Figure 2:** 6 **]**
For users who's job responsibilities include creating data & signing with a medium assurance or higher (Ref. ATA Spec 42), signing certificates installed on the PIV-AV card can be used to create standard, secure digital signature records. The signature data (cryptographic hash) can be used to provide identity validation with non-repudiation and data integrity (evidence that data has not been altered or tampered with).

A-6.4.5. Data security

As mentioned in the above section, the signature data (cryptographic hash) can be used to provide identity validation with non-repudiation and data integrity. Additional data security and standard means of archiving, packaging and re-signing data will be based on processes and procedures called out in ATA Spec 42, utilizing hash message authentication codes (HMAC) and cryptographic timestamps.

A-6.4.6. Authorisation

[Reference Figure 2: 7 **]**
The initial signature use cases utilizing the PIV-AV card will identify the holder of the card and bind him to signature actions to establish non-repudiation. Through this basic electronic signature process, knowledge of who "signed" a document is established, however it is not automatically established that the person was allowed or authorised to perform a documented action and/or to sign the document.

As an additional, optional step, an authorisation check could be performed by applications based on information on the PIV-AV card locally, or through a remote authorisation check. For example, a signature process in an Electronic Techlog application could employ a check based on license type whether a transaction is allowed, and a check to a back-office user management system including training & qualification data could be made before a transaction & signature are accepted.

Either of the authorisation checks illustrated above would likely be maintained as customized configuration of application business rules to a particular airline's needs. However, if agreement in the industry could be established on the standard user information and standard transaction types, and the allowed/disallowed combination of user attributes and transaction types could be recommended through industry standards, interoperable authorisation checks would be possible.

In support of standard user information, the PIV-AV card could hold generic authorisation levels, like mechanic license levels with model endorsements (e.g. B747-400 B2), pilot licenses with type endorsements (FAA Issued ATP, A320/330 endorsement), etc. Role and attribute information stored on the card would allow for granular authorisation controls at the application level and might also support offline transactions provided standards are in place to define each role and attribute meaning.

Further detailing of authorisation is a very difficult subject. To capture all types of authorisation information on one card would need very complex communication and negotiation between the several CAs, e.g. a EASA licensed 747 B1 AMT working for airline XYZ can handle the XYZ 747's once being trained by the company in their policies and procedures. In addition, the engineer needs to perform a Continuing Training Program to keep his company license valid, if not, internally, the license will be temporarily revoked until the required Continuing Training has been completed.

To further complicate the authorisation rules, if company XYZ now handles a 747 aircraft of company ABC acting as a third party MRO, the policy & procedure training for company ABC would need to be accomplished before the holder would be authorised to sign for work performed on the ABC airplane. Completion of the training would require either an update of the PIV-AV card or a back-office user management database (including training & qualification records).

The scenario above illustrates the complexity of the authorisation rules if only two companies were involved. Increasing complexity would result when considering the large number of organizations and support contracts in place in the industry. As such, it is believed that a significant effort would be required to establish standards across the industry such that a PIV-AV could be provisioned with authorisation levels and required currency rules (training & qualification) crossing these organizational boundaries.

For these reasons, it is recommended AIAS be pursued with user identification as the primary goal, and to hold authorisation checks as a secondary goal. Provisions for an eventual authorisation check can be considered at this time, including a discussion on standard user types and standard transaction types. However, due to the varied and complicated business rules around authorisation, it is believed these should be initially managed by individual organizations as part of their own policies and procedures through their own user management system, with a plan to migrate to distributed authorisation checks in the future.

A-7. Glossary

Acronym / Term	Definition
AAAE	American Association of Airport Executives
ABAC	Attribute Based Access Control
ACARS	Aircraft Communication Addressing and Reporting System
ACI	Airports Council International
AEEC	Airlines Electronic Engineering Committee
AIAS	Aviation Identity & Authorisation System

Acronym / Term	**Definition**
AMT	Aircraft Maintenance Technician (Mechanic, Ground Engineer, etc.)
ATA	Air Transport Association
ATP	Airline Transport Pilot (license)
CA	Certificate Authority
CRL	Certificate Revocation List
Digital Signature	[Reference AC 120-78 definition]
DSWG	Digital Security Working Group
EFB	Electronic Flight Bag (hardware)
ELB	Electronic Logbook (software)
Electronic Signature	[Reference AC 120-78 definition]
ELPT	Electronic Logbook Project Team
FIPS	U.S. Federal Information Processing Standard
HMAC	Hash Message Authentication Code
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
LDAP	Lightweight Directory Access Protocol
MRO	Maintenance & Repair Organization
NFC	Near Field Communications
NIST	National Institute of Standards & Technology
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PIV-AV	Personal Identity Verification – Aviation
PIV-C	Personal Identity Verification – Compatible
PIV-I	Personal Identity Verification – Interoperable
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RFID	Radio Frequency Identification
SAML	Security Assertion Markup Language
SCVP	Server-based Certificate Validation Protocol
SSO	Single Sign On
TSA	Transportation Security Administration
UMS	User Management System
XML	eXtensible Markup Language

A-8. References

1. United States Public Law 106-229, *Electronic Signatures in Global and National Commerce Act*, June 30, 2000, http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
2. Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004, http://www.dhs.gov/homeland-security-presidential-directive-12

3. Federal Information Processing Standard (FIPS) Standard 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
4. US Federal Chief Information Officers (CIO) Council, *Use of Electronic Signatures in Federal Organization Transactions*, version 2.0, January 25, 2013, https://www.idmanagement.gov/sites/default/files/documents/Use_of_ESignatures_in_Federal_Agency_Transactions_v20_20130125.pdf
5. FAA Advisory Circular 120-78, Acceptance and Use of Electronic Signatures, *Electronic Recordkeeping Systems, and Electronic Manuals*, October 29, 2002, http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_120-78_final.pdf
6. EASA AMC 20-25, Airworthiness and Operational Consideration for Electronic Flight Bags (EFBs), February 9, 2014, http://easa.europa.eu/system/files/dfu/2014-001-R-Annex%20II%20-%20AMC%2020-25.pdf
7. ATA Spec 42, *Aviation Industry Standards for Digital Information Security*, Revision 2013.1, http://www.ataebiz.org/apps/org/workgroup/ataebizspecs/download.php/3934
8. RTCA DO-230D, *Standard for Airport Security Access Control Systems,* December 18, 2013, http://www.rtca.org/store_product.asp?prodid=1129
9. Smart Card Alliance PAC-08002, *Interoperable Identity Credentials for the Air Transport Industry*, October 2008, http://www.smartcardalliance.org/resources/lib/Air_Transport_ID.pdf

Contributors:

Donald van TONGEREN	-	KLM Royal Dutch Airlines
Steven YUKAWA	-	The Boeing Company
Pascal BUCHNER	-	IATA
Dragos BUDEANU	-	IATA
Chris MARKOU	-	IATA

IATA would like to thank the airlines and industry experts who reviewed this document and provided valuable comments.