

AEEC Project Initiation/Modification (APIM)

- 1.0 Name of Proposed Project** **APIM #:** [10-002A](#)
Digital Certificate Usage in the Aircraft Environment
- 1.1 Name of Originator & Organization**
Steve Arentz, United Airlines
- 2.0 Subcommittee Assignment and Project Support**
- 2.1 Suggested AEEC Group**
Network Infrastructure and Security (NIS)
Chairman: Steve Arentz, United Airlines, and Jean-Paul Moreaux, Airbus
- 2.2 Support for the Activity (as verified)**
Airlines: United Airlines, American Airlines
Airframe Manufacturers: Airbus, Boeing, **Bombardier**
Suppliers: Rockwell Collins, **GoGo**, GE Aviation, Honeywell, Panasonic, **Teledyne Controls**
Others: **Carillon Information Security**
- 2.3 Commitment for Drafting and Meeting Participation (as verified)**
Airlines: United Airlines
Airframe Manufacturers: Airbus, Boeing, **Bombardier**
Suppliers: **Rockwell Collins, GoGo, GE Aviation**, Honeywell, Panasonic, **Teledyne Controls**
Others: **Carillon Information Security**
- 2.4 Recommended Coordination with other groups**
CSS, SAI
Note: Informal coordination with ICAO and ATA
- 3.0 Project Scope**
- 3.1 Description**
There is no question that safety and security are the highest priority concerns in the air transport industry. While people typically think of physical security, there is increasing focus being placed on digital information security in the context of the airplane. This is, in part, due to the increasingly convergent nature of technologies involved (passengers want internet access, and flight systems are beginning to make use of readily available internet protocols and equipment). In addition, there is increasing pressure from:
- Regulatory agencies that want to ensure flight systems remain secure against all threats.

- Aircraft and equipment manufacturers that want to reduce design costs by using certain standard technologies when appropriate instead of specialized ones.
- Airlines that want to satisfy passenger demands, reduce maintenance costs, and take advantage of new communication networks.

Other industry standards are being developed in this area, such as Air Transport Association (ATA) Spec 42, which deals with digital identity management. It specifies standard digital certificate profiles for use across the air transport industry, as well as standard policies governing the issuance and use of these certificates, which in turn describe certain levels of assurance that may be conveyed in a digital identity.

As such, there is a consistent, high-level identity management framework that is interoperable between air transport companies and government agencies. Recognizing the need for a single, comprehensive standard across all industry projects and participants, ARINC 822 and 823, and ICAO's ATN, are among the applications that already reference (or were influenced by and are compliant with) ATA Spec 42.

Additional detail, such as an interpretation of these standards in the context of actual aircraft deployment, is needed. In Section 5.2 of ARINC 811, "Recommendations to AEEC," the third recommendation recognizes the need for AEEC to develop life-cycle key management guidance in coordination with other industry organizations such as ATA. Therefore, this APIM proposes to develop a document to provide guidance to aircraft manufacturers and operators on tasks including:

- Provide use case information.
- Define near term requirements and long term objectives.
- Determine how digital certificates can be loaded onto and used by aircraft electronic systems in all aircraft domains.
- Determine how digital certificates can be used by an aircraft in flight to validate other identities (such as on received messages).
- Identify other certificate life cycle concerns in the context of the aircraft environment.
- Describe how aircraft operators and their personnel can implement Spec 42 security policy requirements and other relevant industry standards and regulatory requirements as it relates to airline technical processes, business processes, and maintenance processes.
- Identify implications of use of digital certificates in aircraft systems for maintenance programs and procedures.
- Describe specific personnel roles that are required for compliant digital certificate operation (consistent with the fourth recommendation in Section 5.2 of ARINC 811)
- Perform further research into whether time stamping of communication, signed by an on-board authority might be required in the future.
- Coordinate between ARINC (i.e. A822, A823), ICAO 9705 and ATA documents.
- Perform further research into future FAA and Eurocontrol plans (possible requirements) of digital certificate use in NextGen and SESAR implementations (such as the requirement for a unique aircraft ID for data link logon for FAA DataCom segment 1 services starting in 2014).

- Coordinate with AMC in the areas of configuration management, procedures and transport of loadable software parts.
- Develop certificate subject naming guidance for aircraft-focused certificate-based applications. Spec 42 states only that the certificate name (CN) must be unique, but it does not provide specific guidance with respect to how names should be formed. Gatelink has suggested a naming convention such as “tailnumber.airline.com”; however, a more in-depth view at the variety of anticipated applications is needed to determine how to ensure uniqueness with a name form that makes sense.

It is the intent of this project to capture complementary elements from Spec 42 and provide additional information to a level not available in Spec 42. Specifically, the intent is to provide additional detail from an airline perspective on implementation. As the NIS and the ATA have a history of cooperation on digital security topics, the NIS will provide feedback to the ATA as appropriate so that guidance in Spec 42 may be improved to close gaps and better meet airline or implementer needs. In other situations where gaps are identified, the intent of this project will be to capture guidance complementary to, and consistent with, Spec 42, but to a greater level of detail.

The proposed document will also provide guidance to developers of other AEEC specifications, recommending that any external-entity-to-aircraft communications requiring security or message-sender authentication use existing industry standards, including this document.

Aircraft such as the A380 are already using digital certificates. Likewise, aircraft such as the B787 and the A350 will use certificates with an increasing number of applications. Standard implementation guidance for these programs, as proposed in this document, will help reduce cost of design, implementation, and operation. By ensuring a consistent approach, design work need not be repeated, and operators benefit from uniform processes, even across a heterogeneous fleet. Any guideline and implementation standard should consider all existing aircraft and retrofit capability.

3.2 **Planned usage of the envisioned specification**

New aircraft developments planned to use this specification	yes <input type="checkbox"/> no <input checked="" type="checkbox"/>
Airbus: (aircraft & date)	
Boeing: (aircraft & date)	
Other: (manufacturer, aircraft & date)	
Modification/retrofit requirement	yes <input type="checkbox"/> no <input checked="" type="checkbox"/>
Specify: (aircraft & date)	
Needed for airframe manufacturer or airline project	yes <input type="checkbox"/> no <input checked="" type="checkbox"/>
Specify: (aircraft & date)	
Mandate/regulatory requirement	yes <input type="checkbox"/> no <input checked="" type="checkbox"/>
Program and date: (program & date)	
Is the activity defining/changing an infrastructure standard?	yes <input checked="" type="checkbox"/> no <input type="checkbox"/>
Specify	
When is the ARINC standard required?	
_____ (month/year) _____	

What is driving this date? Aircraft programs that require digital certificates are becoming more and more numerous as connectivity to the aircraft increases and security requirements become more stringent. Without common standards in this area the aircraft operators will face increasing diversity and complexity in managing digital certificates.

Are 18 months (min) available for standardization work? yes no

 If NO please specify solution: _____

Are Patent(s) involved? yes no

 If YES please describe, identify patent holder: _____

3.3

Issues to be worked

Major issues to be addressed include the following:

- Define the aircraft device sponsor (airline authorized requestor) role and persons (could be IT security or aircraft engineering), and any other roles needed to support the installation, use, and maintenance of digital certificates in aircraft systems;
- Define an out-of-band process by which an issuing Certificate Authority (CA) sends its trust anchors (e.g.: its Root and the Signing CA certificates) to airline authorized requestors;
- Define a process or guidelines for ensuring safe delivery of certificate and private signing key material to the aircraft devices;
- Define recommendations for checking revocation status of certificates while in flight, or acceptable workarounds for various scenarios if real-time revocation status checking is not possible while in flight;
- Identify and define certificate profile fields that should be populated (based on ATA Spec 42, and on existing standards ARINC 628, ARINC 822 and ARINC 823).
- Determine what information is required to accomplish the aircraft device vetting process (device serial #, aircraft tail #, installation date, installation location, etc.), how it is gathered and where this information will be stored;
- Determine the aircraft device vetting process steps and which roles are involved (i.e. what actions the aircraft device sponsor will perform and how the data is compiled into a Certificate Signing Request (CSR) and sent to the CA);
- Determine binding of digital certificates to a device, which could be either an entire aircraft or an individual component;
- Determine use of digital certificates and associated services at certain phases of operation (on-ground, in-flight, after maintenance, etc.). Does this, for example, require redundancy? What are the key requirements derived from applications using the digital certificate?
- Determine handling of digital certificates on an aircraft. For example, how are digital certificates generated, loaded to an aircraft or aircraft component, and checked during operation?
- Determine handling of digital certificates on an aircraft system. For example, do Electronic Flight Bags (EFBs) and Flight Management Systems (FMS) use the same certificate or different certificates?
- Determine what logging of various transactions is needed and make recommendations as to how this should be done.

4.0 Benefits

4.1 Basic benefits

Operational enhancements yes no

For equipment standards:

a. Is this a hardware characteristic? yes no

b. Is this a software characteristic? yes no

c. Interchangeable interface definition? yes no

d. Interchangeable function definition? yes no

If not fully interchangeable, please explain: _____

Is this a software interface and protocol standard? yes no

Specify: _____

Product offered by more than one supplier yes no

Identify: _____ (company name)

4.2 Specific project benefits

4.2.1 Benefits for Airlines

Airlines will need to implement procedures to support the use and maintenance of digital certificates in order to accommodate the directions that the airframe manufacturers are taking in new aircraft, and also to comply with future regulatory requirements that may mandate message authentication by digital signature for air-to-ground communication. Standardized guidance concerning the installation, use, and life cycle maintenance of digital certificates in aircraft systems will benefit airlines by facilitating airline security procedure development and reducing the risk of insecure procedures. Furthermore, this document will ensure that consistent design practices will be used across multiple aircraft systems that may be using certificates, reducing costs for airlines and allowing uniform processes even across a heterogeneous fleet.

4.2.2 Benefits for Airframe Manufacturers

Airframe manufacturers are already implementing programs involving digital certificates on aircraft, and are providing significant push to implement more such programs. Standardized guidance concerning the contents and use of digital certificates in the aircraft environment will benefit airframe manufacturers by minimizing recurring design costs and ensuring consistent design practices across multiple aircraft systems that may be using certificates.

4.2.3 Benefits for System/Equipment Suppliers

System/equipment suppliers will need to implement digital certificate capabilities to accommodate the directions that the airframe manufacturers are taking in new aircraft system designs. Standardized guidance concerning the contents and use of digital certificates in the aircraft environment will benefit avionics suppliers by minimizing recurring design costs, as consistent design practices will ensure that requirements are similar across different aircraft systems that may be using certificates.

5.0 Documents to be Produced and Date of Expected Result

1) ARINC Project Paper 842: Guidance for Usage of Digital Certificates

Date of expected result: Mature draft is expected at the 2012 AEEC General Session with publication to follow. This initial release would include overall guidance to the industry in Sections 1-4. These sections will be considered mature and ready for publication. More detail for key management material will be developed simultaneously in the initial release. However, additional detail will be developed and included for Supplement 1.

2) Supplement 1 to ARINC 842: Guidance for Usage of Digital Certificates

Date of expected result: Mature Supplement 1 is expected at 2013 AEEC General Session. Supplement 1 will concentrate efforts in the development of detailed key management information. Sections that will be of focus include Public Key Certificate Life Cycle, Private Key Life Cycle, Certificate Revocation List (CRL) Life Cycle, and Compromise Management details.

Meetings and Expected Document Completion

The following table identifies the number of meetings and the meeting days needed to produce the documents described above.

Activity	Mtgs	Mtg-Days (Total)	Expected Start Date	Expected Completion Date
<i>Project Paper 842 Digital Certificates</i>	5	15	2010	April 2012
<i>Supplement 1 Digital Certificates</i>	3	9	2012	April 2013

The meeting days shown reflects the NIS Subcommittee schedule of three meetings per year. This will be augmented by monthly web conferences as needed.

5.1 Expiration Date for this APIM
April 2014

6.0 Comments