ARINC Project Initiation/Modification (APIM)

1.0 Name of Proposed Project APIM 16-004

Supplement 2 to ARINC Report 842, “Guidance for Usage of Digital Certificates”

1.1 Name of Originator and/or Organization

Network Infrastructure and Security (NIS) Subcommittee

2.0 Subcommittee Assignment and Project Support

2.1 Suggested AEEC Group and Chairman

Network Infrastructure and Security (NIS) Subcommittee
Chairman: Steve Arentz, United Airlines

2.2 Support for the activity (as verified)

Airlines: United Airlines, FedEx, Alaska, American, Delta

Airframe Manufacturers: Boeing, Airbus

Suppliers: Rockwell Collins, Honeywell, Panasonic, Teledyne, Zodiac Inflight Innovations

Others:

2.3 Commitment for Drafting and Meeting Participation (as verified)

Airlines: United Airlines, FedEx

Airframe Manufacturers: Boeing

Suppliers: Rockwell Collins, Honeywell, Panasonic, Teledyne, Zodiac Inflight Innovations

Others:

2.4 Recommended Coordination with other groups

CSS, IPS, SAI, SDL

Note: Informal coordination with ICAO and ATA

3.0 Project Scope (why and when standard is needed)

3.1 Description

ARINC Report 842 was originally published in 2012 with Supplement 1 released shortly following in 2013.

ARINC Report 842 was developed as a companion document to ATA Specification 42.

Spec 42 provides guidance on common processes, tools and practices for securely transmitting, storing and exchanging commercial aviation data.

- Considerations for protecting data from corruption or manipulation while at rest or during transmission between an airplane and back office systems.
- Methods of positively identifying a person or device electronically using digital security.

- Guidance on continuous operations from the perspective of both the airline operator and the system designer.

ARINC Report 842 provides additional information to a level not available in Spec 42. Specifically:

- Guidance detail from an airline perspective on implementation of certificate manage infrastructure
- Guidance to developers of other industry standards recommending that any external-entity-to-aircraft communications requiring security or message-sender authentication use existing industry standards.

Spec 42 has been revised twice since the last publish of ARINC Report 842. The most recent revision (2015.1) published by A4A includes:

- New guidance for non-PKI Electronic Signatures
- New guidance for selecting Certificate and Attribute Authorities
- Updated credential assurance strength recommendations
- Added typical use cases for Digital Signature in airline operations
- New guidance for use of PKI Card Management Systems
- New appendix for XML Digital Signature Profiles
- New appendices for non-PKI operational and credential provider policies
- Deprecated SHA1 in the ATA Reference Certificate Policy
- Reorganized the specification to provide more clarity, improve the flow, and better distinguish between PKI and non-PKI guidance.

In October 2015, US NIST released Special Publication (SP) 800-152, which provides general requirements/guidance for key management systems. This document expands upon the key management framework in NIST SP 800-130, which is referenced in ARINC Report 842. The general key management guidance within the new NIST document could be adapted to ARINC Report 842 with an aircraft approach.

3.2 Planned usage of the envisioned specification

Note: New airplane programs must be confirmed by manufacturer prior to completing this section.

New aircraft developments planned to use this specification yes ☐ no ☐

Airbus: (aircraft & date)

Boeing: (aircraft & date)

Other: (manufacturer, aircraft & date)

Modification/retrofit requirement yes ☐ no ☐

Specify: (aircraft & date)

Needed for airframe manufacturer or airline project yes ☐ no ☐

Specify: (aircraft & date)

Mandate/regulatory requirement yes ☐ no ☒

Program and date: (program & date)

Is the activity defining/changing an infrastructure standard? yes ☒ no ☐

Specify (e.g., ARINC 429)

When is the ARINC standard required? _____ (Feb 2018) _____

What is driving this date? _____ (state reason) _____

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

With the significant changes described above, it is necessary to update ARINC Report 842 to include:

- Updates to references to Spec 42
- Incorporate appropriate additions from Spec 42 (technology) from an airline perspective.
- Review NIST 800-152 to develop additional guidance
- Incorporate any technology/business model/business process updates
- Support IPS Subcommittee as needed
- Gather and incorporate lessons learned from new aircraft programs and experiences with key management implementation/deployment
- Review and incorporate current certificate management processes and real world application of digital certificates.

4.0 Benefits

4.1 Basic benefits

Operational enhancement 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 (Describe overall project benefits.)

4.2.1 Benefits for Airlines

Airlines have implemented 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 current and evolving 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 benefit airlines by facilitating airline security procedure development and reducing the risk of insecure procedures. Furthermore, this document ensures that consistent design practices used across multiple aircraft systems that use 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 Avionics Equipment Suppliers

System/equipment suppliers have implemented digital certificate capabilities to accommodate the directions that the airframe manufacturers are taking in 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

Supplement 2 to ARINC Report 842

5.1 Meetings and Expected Document Completion

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

Activity	Mtgs	Mtg-Days (Total)	Expected Start Date	Expected Completion Date
ARINC 842, Supp 2	6	6*	June 2016	Feb 2018

This meeting plan will be augmented by monthly web conferences.

6.0 Comments

* 6 in-person meetings with 1 day per meeting focused on ARINC 842. Should the NIS Subcommittee be tasked with the development of other standards, the actual meeting length may be extended.

6.1 Expiration Date for the APIM

April 2018

Completed forms should be submitted to the AEEC Executive Secretary.