Attachment 1

Attachment 1

AEEC

Together "We Set the Standard."

Internet Protocol Suite (IPS) Subcommittee

June 23, 24, 29, 2020
Online Meetings
Agenda – draft RevA

1. Welcome and Introductions
2. Approval of the Agenda
3. Administrative Aspects and Schedule for 3 days
4. Status Reports - Organizations and Documents
    - ICAO Comm Panel WG-1: ICAO Annex 10, Doc 9896 ed 3, ICAO Doc 10090, ICAO Doc 10094, ICAO Doc 10095, ICAO Doc 100XX – Security Risk Assessment
    - RTCA SC-223 / EUROCAE WG-108: IPS MASPS
    - Other TBD
5. IPS Terminology - Status Report
6. **ARINC Project Paper 858:** *Internet Protocol Suite (IPS) for Aeronautical Safety Services - Technical Requirements* (focal points in red)

    1.0 Introduction
    2.0 ATN/IPS Overall Architecture
    3.0 Airborne IPS System Architecture
    4.0 Security
    5.0 Airborne Implementation Options
    6.0 Airborne Application Data Considerations
    Attachment 1 - List Of Acronyms
    Attachment 2 - Glossary
    Attachment 3 - ACARS to IPS Dialogue Service Convergence Function
    Attachment 4 - Air-Ground IPS Management Messages
    Appendix A - ATNPKT Message Format Examples
    Appendix B - IPS Protocol Build-up
    Appendix C - IPS Ground Architecture Considerations

7. Section 4.4.1, Cryptographic Key Management - Airbus
8. Appendix C, Ground IPS Architecture (Airtel, Boeing, Collins, Honeywell)
9. Roadmaps and Schedules
10. Standards Gap Analysis - Honeywell
11. Review of meeting actions and joint meeting actions
12. Any other Business
13. Next meetings (consider all IPS group plans)
    - AEEC and joint meeting plans TBD
14. Adjourn

Attachment 2

Attachment 2

AEEC

Together "We Set the Standard."

Internet Protocol Suite (IPS) for Aeronautical Safety Services Technical Requirements

ARINC Project Paper 858

Meeting Intro Slides

Luc Emberger

AIRBUS

Paul Prisaznuk

ARINC Industry Activities

Greg Saccone

BOEING

Online Meeting

June 23, 2020

Topics Covered in this AEEC Briefing

- Welcome and Introductions
- APIM 15-004A and ARINC 858: ATN/IPS Technical Requirements
- Agenda Summary
- Schedule for this Week - June 23, 24, 29
- Membership and Corporate Sponsorship
- Intellectual Property (IP) Policies

APIM 15-004A

Internet Protocol Suite (IPS) for Aeronautical Safety Services

Initiated: September 23, 2015

Updated: October 19, 2017

APIM 15-004A
IPS for Aeronautical Safety Services

- Scope - Define new Data Comm Network Infrastructure for Aviation Safety Services leveraging the Internet Protocol Suite (IPS)
  - ICAO Doc 9896 foundation
  - Support Inmarsat SBB, Iridium NEXT, AeroMACS, etc.
- Step 1: Prepare ARINC Project Paper 658: Internet Protocol Suite for Aeronautical Safety Services – Roadmap Document.
  - *ARINC Report 658 published December 18, 2017*
- Step 2: Three main tasks:
  1. Prepare ARINC Project Paper 858: Internet Protocol Suite for Aeronautical Safety Services – Technical Requirements
  2. Maintain IPS standardization roadmap (update gap analysis and standardization timing), Section 5 of ARINC 658, and Supplement 1
  3. IPS SC serves as coordination focal for all AEEC IPS-related activities
  - *Goal: Mature document end of 2020, with AEEC Adoption in May 2021 [TBC]*

ARINC Project Paper 858 - IPS Technical Requirements
Industry Editor - Mike Olive - Honeywell

ARINC Project Paper 858 - IPS Technical Requirements

- 1.0 Introduction
- 2.0 ATN/IPS Overall Architecture
- 3.0 Airborne IPS System Architecture
- 4.0 Security
- 5.0 Airborne Implementation Options
- 6.0 Airborne Application Data Considerations
- Attachment 1 - List Of Acronyms
- Attachment 2 - Glossary
- Attachment 3 - ACARS to IPS Dialogue Service Convergence Function
- Attachment 4 - Air-Ground IPS Management Messages
- Appendix A - ATNPKT Message Format Examples
- Appendix B - IPS Protocol Build-up
- Appendix C - IPS Ground Architecture Considerations

AGENDA SUMMARY
IPS Subcommittee

AGENDA - June 23, 24, 29

1. Welcome and Introductions
2. Approval of the Agenda
3. Administrative Aspects and Schedule for 3 days
4. Status Reports - Organizations and Documents
5. IPS Terminology - Status Report
6. ARINC Project Paper 858: Internet Protocol Suite (IPS) - Technical Requirements
7. Section 4.4.1, Cryptographic Key Management - Airbus
8. Appendix C, Ground IPS Architecture (Airtel, Boeing, Collins, Honeywell)
9. Roadmaps and Schedules
10. Standards Gap Analysis - Honeywell
11. Review of meeting actions
12. Any other Business
13. Next meetings
14. Adjourn

Meeting Schedule
June 23, 24, 29

Meeting Times	US Pacific	US Eastern	Central Europe	Notes
Start	0700	1000	1600	All days
Break	0900	1200	1800	All days
Re-Convene	1000	1300	1900	June 23 and 29
Adjourn	1200	1500	2100	June 23 and 29

ARINC Intellectual Property (IP) Policy

- The ARINC Patent Policy covers patented technology and copyrighted material (e.g., software) *required to comply with* an ARINC Standard.
  - This policy allows the AEEC to consider proprietary technology for inclusion in an ARINC Standard -- If it provides significant technical or economic benefit over non-proprietary technology.
- The policy has two distinct requirements:
  - A participant *must disclose* if the use of any patented, patent pending, or copyrighted technology is required to comply with an ARINC Standard being developed. This disclosure must be provided in writing to the AEEC Executive Secretary.
  - When invited to do so by the AEEC Executive Secretary, the proponent *must sign a Commitment to License* the technology under reasonable and non-discriminatory terms.
- By signing the attendance book or by submitting material for consideration at the meeting, you confirm that you understand the policies and agree to comply with them.
- The policies are available at: *www.aviation-ia.com*

Point of contact …

Paul J. Prisaznuk

Executive Secretary & Program Director
Airlines Electronic Engineering Committee (AEEC)
ARINC Industry Activities

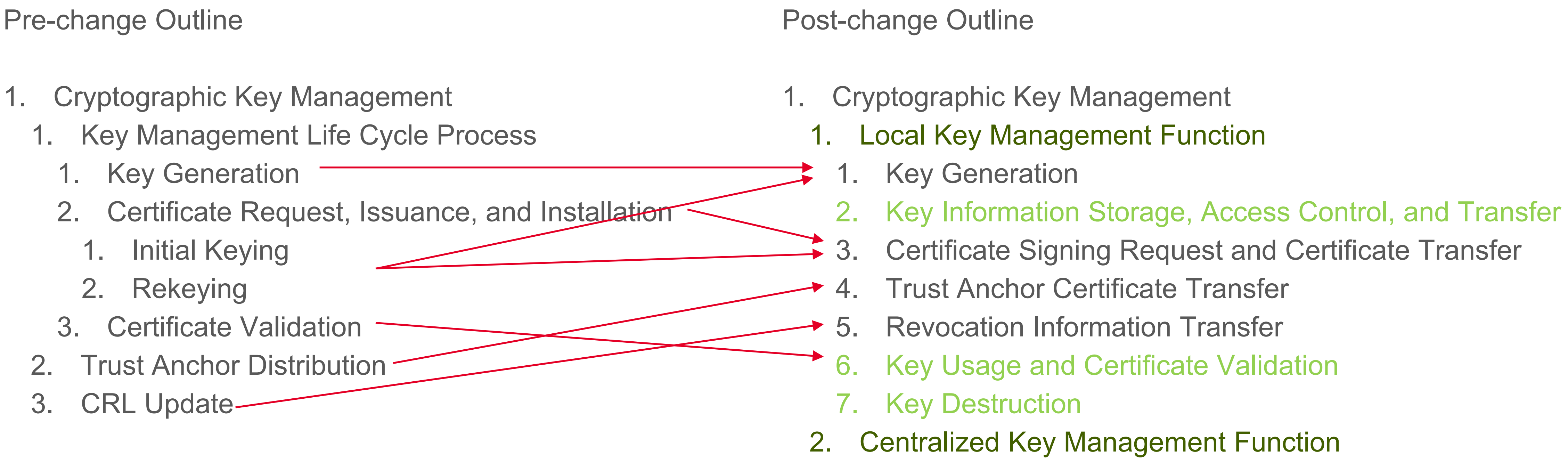
1-410-212-0913
pjp@sae-itc.org
www.aviation-ia.com/aeec

Thank You

Backup Slides

Attachment 3

Change in Structure of Section 4.4.1



Pre-change Outline

1. Cryptographic Key Management
   1. Key Management Life Cycle Process
      1. Key Generation
      2. Certificate Request, Issuance, and Installation
         1. Initial Keying
         2. Rekeying
      3. Certificate Validation
   2. Trust Anchor Distribution
   3. CRL Update

Post-change Outline

1. Cryptographic Key Management
   1. Local Key Management Function
      1. Key Generation
      2. Key Information Storage, Access Control, and Transfer
      3. Certificate Signing Request and Certificate Transfer
      4. Trust Anchor Certificate Transfer
      5. Revocation Information Transfer
      6. Key Usage and Certificate Validation
      7. Key Destruction
   2. Centralized Key Management Function

Principle Content Changes

- 4.4.1.1.1:
  - Additional considerations on automatic re-keying before certificate expiration.
  - Inhibition of re-keying during flight as configuration item

- 4.4.1.1.3:
  - Abstraction from the particular certificate management protocol, allowing to support different protocols
  - Requirement for EST protocol for certificate management

- 4.4.1.1.4:
  - Description that trust anchor distribution is implementation specific (distribution via FLS mentioned as one option)

- 4.4.1.1.6: Added „Key Usage and Certificate Validation“ content

- 4.4.1.1.7: Added „Key Destruction“ content

- *Additional explanations and commentary to provide a more comprehensive picture*
- *Additional references to ICAO DOC 10095, which will give guidance and requirements for key management.*
- *Removal of aircraft IP address consideration (not being security-related)*

Discussion Items

- 4.4.1.1.5: Shall we describe CRL provisioning in the document?
  - CRL DPs are generally HTTP-based today, which requires a TCP stack.
  - If TCP stack shall be avoided, an ATN/IPS-specific solutions needs to be found.

- 4.4.1.1.5: OCSP may allow to avoid the usage of CRLs in principle.
  - For DTLS v1.2, this seems to require RFC 6961, which is not part of the IPS profiles.
  - Which level of discussion is needed here?

- 4.4.1.1.5: Do we need an OCSP overview describing RFC-defined behavior?

- 4.4.1.1.6: Details on checks depend on DOC 10095 → dependence between the documents

- 4.4.1.1.6: Do we need a check for operator code for AOC peers?

- General question: Will the airborne system also act as DTLS server?

Attachment 4

Attachment 4

PP858 Appendix C Discussion

AEEC IPS Webex
29/06/2020

Fryderyk Wrobel
Airtel ATN

PP858 Appx. C Discussion – Airtel Feedback

- **Title** – The current title, "Ground IPS System Architecture Considerations," does not match the current scope, IPS Gateways. -> Ground IPS Gateway Air-Ground Interoperability Considerations
- **Placement** – Since PP858 specifies the Airborne IPS System, does the detailed description of IPS Gateways belong in a PP858 appendix? Possibly 'yes' depending on scope -> see next bullet. -> KEEP
- **Scope** – Consider including essential IPS ground services (e.g., name resolution, authentication/security services, mobility services, etc.) and potential deployment of these ground services, presented from the perspective of the Airborne IPS System. Then, a description of IPS Gateway functionality can follow.
  - If/when the transition period ends in the future, essential ground services will still be required even if gateways are not.
- **Content** – If IPS Gateways is the agreed scope, then need to describe the context and functions of the gateways before diving into detail, and the following concepts need to be conveyed explicitly in the text:
  - IPS Gateways provide network level translation (e.g., IPS<->OSI) and not application level translation (ATN/IPS<->FANS/ACARS).
  - An IPS Gateway must present itself as an IPS Host (i.e., a native IPS Host cannot distinguish an IPS Gateway from another native IPS Host).
  - When facing other networking technologies, an IPS Gateway acts as a transparent proxy for the applications and must distribute network reachability information in the given network domain. For example, if the gateway proxies a native IPS aircraft into the OSI domain, it must distribute the proxy NSAP for this aircraft into the OSI domain (with IDRP). Simply put, it is not enough for the gateway to pretend to be the aircraft; it must also say to the rest of the network "Hey, I am here“ so that routers know how to route traffic correctly in both directions.
  - ACTION—RTCA/EUROCAE to review this material wrt what is planned for the MASPS, and identify gaps

PP858 Appx. C Discussion

- **Proposal 1:** Keep the current title and change the content
  - Current title: “Ground IPS System Architecture Considerations”.
  - Describe the ground services essential for IPS aircraft and their possible location in the ground IPS segment.
    - name resolution
    - security management
    - mobility
    - IPS gateways
    - others?

- **Proposal 2:** Update the title and keep the current content
  - Proposed title: “Ground IPS Gateway Air-Ground Interoperability Considerations”

- **Proposal 3:** Update the title and update the content
  - Proposed title: “Ground IPS Gateway Air-Ground Interoperability Considerations”.

IPS Gateway

A system that establishes and maintains an operational correlation between two heterogeneous peer communicating systems, where one system is an IPS Node and the other is an OSI End System or an ACARS Host. Note: An IPS Gateway exchanges IPv6 packets with the IPS Node, which may be an Airborne IPS System or a Ground IPS Host.

TOC Changes – 1/2

Current outline

- Introduction
- Current Datalink Communications Environment
    - ACARS network
    - OSI network
- Ground IPS System Architecture
    - Supported datalinks
    - Ground network delivery
- IPS Gateway Functional Requirements
    - Architecture context
    - Deployment considerations
- IPS Aircraft – ACARS Host
- IPS Aircraft – ATN/OSI End System
- Legacy (ACARS, OSI) Aircraft – Ground IPS Host
- IPS Aircraft – Ground IPS Host

Proposed outline

- Introduction
- Aircraft Configurations and Datalink Applications
- IPS Gateway Overview
    - Overview
    - Main Use-Cases
    - Deployment Considerations - *???*
    - Performance and Safety Considerations - *???*
- Gateways between IPS and ACARS
- Gateways between IPS and OSI

TOC Changes – 2/2

Current outline

- Introduction
- Current Datalink Communications Environment
- Ground IPS System Architecture
- IPS Gateway Functional Requirements
- IPS Aircraft – ACARS Host
    - Message segmentation
    - Sequence number and Acknowledgement Management
    - Compression and MIC Generation/Verification
    - Example scenarios
- IPS Aircraft – ATN/OSI End System
    - Message segmentation
    - Sequence number and Acknowledgement Management
    - Compression and MIC Generation/Verification
    - Example scenarios
- Legacy (ACARS, OSI) Aircraft – Ground IPS Host
    - ATN/OSI Aircraft to Ground IPS Host Protocol Conversion
    - ACARS Aircraft to Ground IPS Host Protocol Conversion
- IPS Aircraft – Ground IPS Host
    - Message segmentation
    - Example scenarios

Proposed outline

- Introduction
- Aircraft Configurations and Datalink Applications
- IPS Gateway Overview
- Gateways between IPS and ACARS
    - Principle of operation
    - Mapping of A620 Messages to AICF Interface
    - Example scenarios
- Gateways between IPS and OSI
    - Principle of operation
    - Advertisement of Proxy Addresses
    - Application Messages Forwarding
    - Special Consideration for CM application
    - Example scenarios