SUMMARY

This information paper consists of the report produced within the AEEC concerning key management and security. Firstly the paper describes the work that AEEC have done to assess what key management specifications are required to respond to the ATNP communiqué. Second the paper shows the growing interest in work on security in AEEC. In particular the AEEC is considering application of the ATN security provisions within other AEEC applications that need security. This is seen as a positive development for ATN security since it will enable airlines and CAAs to amortize costs and ease deployment of ATN security. The working group is invited to consider the implications of this possibility of SV8.
Report:
Airlines Electronics Engineering Committee (AEEC)
Data Link Systems Subcommittee
Ad Hoc Committee Meeting

Evaluation and Implementation of
AEEC Project Initiation/Modification (APIM) 02-002
International Civil Aviation Organization (ICAO)
Communiqué:

Request for AEEC Specification Development for
Aeronautical Telecommunication Network (ATN) Security
Services
Public Key Infrastructure (PKI) Key Management and
Distribution
Evaluation of the Implementation
Of APIM 02-002
ICAO ATN Key Management and Distribution

Executive Summary

APIM Evaluation:

The Ad Hoc members reviewed the various aspects of ATN Security during the two day meeting with the goal of answering the basic question proposed by ICAO in their communiqué to AEEC. Throughout all of the discussions, Ad Hoc members reached a general consensus that considerable work is necessary to develop an AEEC standard for Public Key Infrastructure (PKI) Security mechanisms. The major concern of the Ad Hoc Committee was the proper timing since the recent FAA decision to delay implementation of ATN Controller Pilot Data Link Communications (CPDLC) in US airspace until the 2008-2010 time frame (consistent with activation of the VHF Mode 3 Next Generation Communication (NEXCOM) and the En-route Automation Modernization (ERAM) program. The only active ATN CPDLC program remaining is the Eurocontrol Link 2000+ program. However, according to Eurocontrol representatives at the June AEEC Data Link Users Forum (DLUF) in Brussels, Belgium, Eurocontrol is developing the European ATN CPDLC network for the near future in accordance with ATN Baseline 1 communications identified in ICAO Document 9705, Edition 2. ATN Security Service is new requirement identified in the recently released ICAO Document 9705, Edition 3.

a. Other aircraft systems: As the committee further investigated the capabilities and flexibility of ATN PKI Security Service, the committee began identifying other emerging aircraft systems that would benefit from standardized information security architecture. Electronic flight bag (EFB), aircraft data network (ADN)/aircraft network and file server (ANFS), and Gatelink were immediately identified as three near term aircraft systems that are either beginning to enter service or will enter service in the next few years.

b. Basic aircraft systems security requirements to be satisfied: If the ATN PKI security mechanism can be adapted for other aircraft systems, the following questions and industry concerns must be answered:

(1) Airlines want data security: The airlines and aircraft operators already support data security on the terrestrial host networks as well as applications such as web reservation systems. A large number of airlines are already using proprietary encryption systems provided for them by avionics manufacturers for their data link (ACARS/VDL Mode 2) systems. It is a given fact that airlines or aircraft operators do not want the consequences of malicious interference (a.k.a. “hacking”) of their data processing systems.

(2) Airline Information Technology (IT) Applications: As airline IT systems expand to the aircraft environment, airline IT managers will logically try to expand their existing PKI systems to the aircraft subsystems. Where terrestrial based PKI systems are employed on relatively high bandwidth networks or lower bandwidth telephone networks, application to wireless mobile networks propose a significant challenge as evidenced by the current problems to mobile phone data networks.

Information Security Impacts: Information security will impact many different aircraft systems in the near term. To maximize cost efficiency and minimize deployment of multiple independent security mechanisms, and airline or aircraft operator IT security group should address the following concerns:

(a) A common methodology among all vendors for interoperability, not only within an airline or aircraft operator’s fleet, but also across all airlines or aircraft operators.

(b) Historically, piecemeal or customized solutions are ultimately more expensive than a standardized solution.

(c) A security mechanism that is a common solution for all avionics, yet allows individual airlines or aircraft operators to retain their individual protection.

(d) A common methodology that supports current aircraft data link technology with low bandwidth communications – not simple extension of wired “IT” security.

(e) A PKI security mechanism that is adaptable, scaleable, and flexible and allows for variations in key longevity to accommodate differences in airline security policy. So as aircraft communications network change and/or grow, the need to “reinvent the wheel” is mitigated. A good standardized key management system would be airline security policy-tolerant with respect to the number of keys required and key longevity.

(f) Putting more data across the aircraft-ground boundary through public networks. Airlines or aircraft operators will need to address the following issues:
Evaluation of the Implementation
Of APIM 02-002
ICAO ATN Key Management and Distribution

1. Integrity concerns – information is not changed as it transmit through a network.
2. Privacy concerns – company information is only read by the entities authorized to receive it, not read and reproduced on the Internet for the world to see.
3. Delivered to right place – the message is sent to the intended recipient, and if received by someone else, the sender is alerted that the message did not go to the proper recipient.
4. Authenticated source – the sender is who he or she says they are, and not someone else.

Benefits:
The benefits of a common PKI scheme for all aircraft systems will lead to a lower total cost of ownership. Each entity such as airline/operators, avionics vendors, airframe manufacturers, civil aviation authorities (CAA)/air traffic service providers (ATSPs) and data link service providers have a vested interest in developing a common PKI scheme. Effective elimination of redundant or multiple arbitrary and/or proprietary designs means significant cost savings. Effective use of a common PKI scheme that can be retrofitted into existing aircraft systems and migrate to future systems as they become available will minimize the cost of aircraft upgrade programs requiring data and data link security.

Scope of Effort:
Developing a standard PKI security mechanism for airline and aircraft operators is not a trivial task. Airlines and/or aircraft operators will have to evaluate their IT and operational activities with respect to current and future data link architectures. The work required by AEEC to develop the necessary security standards and/or characteristics will most likely entail the creation of a standing subcommittee or working group as the workload of current AEEC subcommittees or standing working groups preclude the amount of time necessary to develop a common standard. Fortunately, this new subcommittee or working group will be able to leverage the PKI work done by ICAO, as well as the work done by existing AEEC subcommittees.

a. Level of effort: The estimate of the effort by AEEC to develop a comprehensive PKI security standard is predicated on the time it will take to perform a detailed technical assessment. ATN Document 9705, Sub-Volume VIII specified in great detail the methodology to for coding and calculating PKI security algorithms and certificates. As stated by the original request for help in APIM 02-002, addition technical factors need to be developed to fully implement an operational PKI architecture on an aircraft and within a ground communications infrastructure.

(1) Technical Assessment: Table 1 represents the technical aspects that will need to be developed into an AEEC specification. This list is only the beginning. As items are discussed, additional technical aspects will most likely be identified.

<table>
<thead>
<tr>
<th>Technical Parameter</th>
<th>Functions to be Evaluated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Physical and software security controls to limit access to authorized personnel and detect unauthorized personnel and/or activities. Procedures will need to be established for aircraft systems as to personnel authorized to load and manage the PKI Security Service keys and databases.</td>
</tr>
<tr>
<td>Airborne Context Management (CM) Database</td>
<td>Database that stores information about aircraft parameters. Physical location needs to be determined as well as how aircraft and ground host systems will access the database.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Part of access control, function to log all authorized access and communications as well as unauthorized attempts to access systems. For airborne equipment, where recording database will be stored and frequency of download by airline/aircraft operator to review database log.</td>
</tr>
<tr>
<td>Certificate Authority (CA) Key/Certificate Update</td>
<td>Physical organization that certifies airline/aircraft operator PKI certificates and distributes PKI public and private keys and X.509 certificates and certificate updates. Airlines and Aircraft Operators will need to determine who and/or where CA Key/Certificate Updates will be processed.</td>
</tr>
<tr>
<td>Technical Parameter</td>
<td>Functions to be Evaluated</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Crypto Parameter Database</td>
<td>Physical database in airborne and ground systems that store shared keys and “X” values for a given security session.</td>
</tr>
<tr>
<td>Crypto Services Implementation</td>
<td>Function that determines when security services are required and which aircraft subsystems will require security services based on information content.</td>
</tr>
<tr>
<td>Data Recording Requirements</td>
<td>Determination of how information will be recorded, before or after security service processing, and where the recording will take place. Airlines and aircraft operators will also need to determine how copies of aircraft and ground host system private keys are stored for accident investigation.</td>
</tr>
<tr>
<td>Ground Context Management Application (CMA) Database of Aircraft Root Certificates</td>
<td>Ground system database that stores all active aircraft Root Certificates in ATN for access by the CMA and other ATS/AOC applications during a secure session. The physical location of this Database needs to be developed along with the procedures and technical applications to distribute the information.</td>
</tr>
<tr>
<td>Key Generation</td>
<td>The software process to actually generate aircraft and ground system Private and Public Keys, then manage and distribute the keys to aircraft and ground system security services.</td>
</tr>
<tr>
<td>Legal Intercept</td>
<td>The process by law enforcement agencies to de-encrypt encrypted messages for use as evidence in a criminal or civil investigations. Airlines and aircraft operators will need to develop procedures and processes to provide aircraft and ground system Private and Public Keys when required by applicable law or laws to law enforcement agencies.</td>
</tr>
<tr>
<td>Loading Certificates</td>
<td>The technical procedures to electronically upload X.509 certificates into the Aircraft Avionics PKI security service application and ground systems PKI security service application. Technical analysis will be required to determine the minimum required content for certificates in order to minimize transmission times to aircraft, if required over bandwidth limited links.</td>
</tr>
<tr>
<td>Loading Keys</td>
<td>The technical procedures to electronically upload Private Keys into aircraft avionics PKI security service application and ground systems PKI security service application. Technical analysis will be required to determine the longevity of private keys, which is likely to vary by application and airline security policy.</td>
</tr>
<tr>
<td>Private Key Protection</td>
<td>The physical and electrical procedures required for protecting the installation and location of private keys in the aircraft and ground systems. Analysis will be required to develop techniques for alerting authorized personnel that a private key has been transmitted or corrupted.</td>
</tr>
<tr>
<td>Private Key Removal</td>
<td>The physical and electrical procedures required to remove private keys from aircraft avionics and ground systems so that hardware may be sent out for maintenance.</td>
</tr>
<tr>
<td>Sharing Keys and “X” value</td>
<td>The technical specifications for allowing aircraft and ground systems to establish and terminate security sessions by negotiating session key values and the Shares Key Value “X” based on X.509 certificate information.</td>
</tr>
<tr>
<td>Verify “Goodness” of implementation</td>
<td>Determining what is the most appropriate FIPS 140 procedures for analyzing PKI security schemes and requiring avionics and ground system vendors to implement FIPS 140 into test and evaluation program.</td>
</tr>
</tbody>
</table>

(2) **Schedule and resources required**: Figure 3 shows a typical timeline for developing an AEEC Characteristic or Specification. The Ad Hoc committee evaluated the timeline and determined that a two-phased approach would support the need for a common PKI Security Service in the aircraft.

(a) **Near Term Effort**: The Ad Hoc committee evaluated the requirements for work for next year. The consensus of the committee members is that the scope of the current APIM needs to be expanded in order to fully evaluate the technical requirements for a common PKI security architecture. In Figure 4, the Ad Hoc committee evaluated the time flow versus aircraft architecture roadmap of Figure 1. By beginning ground work now to develop
a technical specification or specifications, the committee believes that a common PKI security architecture can be specified in time for the near term and next generation aircraft systems. The committee estimates that it will take three regularly scheduled meetings, each meeting lasting 2 days, and a potential for two to three ad hoc meetings as necessary to formally draft a project plan. A preliminary outline for a project plan is found in Appendix B to this report.

(b) Far Term Effort: The far term effort will entail the creation of permanent Security Service Subcommittee since a common PKI Security Service will cover many aircraft subsystems. The work effort will be to develop the necessary AEEC PKI Security Service Characteristics and/or Specifications for implementation on near term avionics. This subcommittee would continue to work with Data Link Systems Subcommittee, VDL Subcommittee, Air-Ground Subcommittee and the Systems Architecture and Interface subcommittees and working groups to ensure that all of these committees and groups would reference the corresponding security documents, and not developing or incorporating other available standards. The work estimate for this phase is three scheduled meetings per year, 2-3 days per meeting with ad hoc meetings as necessary. The first draft specifications would be due in December of 2004.

b. Synergy with other AEEC committees: Synergy will be very important. As reported by SITA [4] in a presentation to September Data Link Systems Subcommittee, the ARINC 763 Working Group adopted the EAP-TLS protocol for strong authentication, yet did not identify a security protocol for integrity. The EAP-TLS authentication protocol is designed to support large-scale networks using Internet Protocol (IP) services. It is not a very efficient protocol for small message formats or bandwidth limited communications services. This is an excellent example that if a common PKI security architecture is not adopted, then a proliferation of software services can and will occur on the aircraft.

![TIME FLOW FOR SECURITY DEVELOPMENT](image-url)
Conclusions:

The following recaps the conclusions identified by the members of the Ad Hoc Committee:

a. The current APIM 02-002 work effort for ICAO is still valid, but that the aviation community will not begin operation on a fully deployed ATN until after 2010. It would be premature for the AEEC to begin developing security service specifications specifically for the ATN at this time.

b. As seen in Figure 2 above, there are several near term avionics systems being deployed on aircraft that will require security services to protect the information stored and transmitted between the aircraft and the ground.

c. The ATN Security Services specified in ICAO Document 9705, Edition 3, Sub-Volume VIII are well documented as to the way a PKI Security Service should function and could be readily adapted to other systems on the aircraft. The development of common PKI security service that will eventually support ATN security requirements is very desirable, both from a technical and operational benefit by owners, avionics vendors, aircraft integrators, CAAs, and DSPs.

d. A common PKI security mechanism will lead to a lower life-cycle cost for the aircraft and associated ground systems than the proliferation of separate proprietary security mechanisms.

Recommendations:

It is the recommendation of the Ad Hoc Committee on ATN Key Management that the AEEC adopt a work plan to develop a common PKI security architecture for aircraft. As such, the Ad Hoc Committee further recommends that the current APIM 02-002 be either broadened to include other systems, or that a separate APIM be generated to develop a project plan for common PKI security services in the aircraft.
Evaluation of the Implementation
Of APIM 02-002
ICAO ATN Key Management and Distribution

Table of Contents

Executive Summary.......................................................................................................................ii
1. APIM Evaluation: .............................................................................................................1
2. Benefits: ........................................................................................................................3
3. Scope of Effort: ...............................................................................................................6
4. Conclusions: ..................................................................................................................11
5. Recommendations: .......................................................................................................12
6. References: ...................................................................................................................12
7. Acknowledgements: .....................................................................................................13

Appendix A: Ad Hoc Meeting Attendees.................................................................................1
Appendix B: Outline ARINC Project Paper 6XX .................................................................1

Table of Figures

Figure ES-1: Time Flow for Security Development (Courtesy AEEC Staff) v
Figure ES-2: Aircraft Platforms Functions Roadmap - Security Mechanism vi
Figure 1: Aircraft Platform Functions Roadmap 1
Figure 2: Airborne Infrastructure 8
Figure 3: Time Flow for Security Development (Courtesy AEEC Staff) 11
Figure 4: Aircraft Platforms Functions Roadmap - Security Mechanism 12

List of Tables

Table ES-1: Technical Parameters and Functions to be Evaluated iii
Table 1: Technical Parameters and Functions to be Evaluated 9
1. APIM Evaluation:

The Ad Hoc members reviewed the various aspects of ATN Security during the two day meeting with the goal of answering the basic question proposed by ICAO in their communiqué to AEEC. Throughout all of the discussions, Ad Hoc members reached a general consensus that considerable work is necessary to develop an AEEC standard for Public Key Infrastructure (PKI) Security mechanisms. The major concern of the Ad Hoc Committee was the proper timing since the recent FAA decision to delay implementation of ATN Controller Pilot Data Link Communications (CPDLC) in US airspace until the 2008-2010 time frame (consistent with activation of the VHF Mode 3 Next Generation Communication (NEXCOM) and the En-route Automation Modernization (ERAM) program. The only active ATN CPDLC program remaining is the Eurocontrol Link 2000+ program. However, according to Eurocontrol representatives at the June AEEC Data Link Users Forum (DLUF) in Brussels, Belgium, Eurocontrol is developing the European ATN CPDLC network for the near future in accordance with ATN Baseline 1 communications identified in ICAO Document 9705, Edition 2. ATN Security Service is new requirement identified in the recently released ICAO Document 9705, Edition 3.

a. Other aircraft systems: As the committee further investigated the capabilities and flexibility of ATN PKI Security Service, the committee began identifying other emerging aircraft systems that would benefit from standardized information security architecture. Figure 1 identifies the timeline for the deployment of these emerging technologies. Electronic flight bag (EFB), aircraft data network (ADN)/aircraft network and file server (ANFS), and Gatelink were immediately identified as three near term aircraft systems that are either beginning to enter service or will enter service in the next few years. EFB and ADN will migrate to high bandwidth data link communications such as broadband satellite while airborne and Gatelink on the ground. Initially, the communications paths may or may not connect to the current aircraft communications management unit (CMU) onboard aircraft. Eventually, all of these systems will connect to an ATN aircraft router when ATN is available. Finally, all of these systems will contain information that is very sensitive to the individual owner airlines and will require strict security procedures to prevent unauthorized access or release of information.

![Figure 3: Aircraft Platform Functions Roadmap](image-url)
b. Basic aircraft systems security requirements to be satisfied: If the ATN PKI security mechanism can be adapted for other aircraft systems, the following questions and industry concerns must be answered:

1. **Airline want data security:** The airlines and aircraft operators already support data security on the terrestrial host networks as well as applications such as web reservation systems. A large number of airlines are already using proprietary encryption systems provided for them by avionics manufacturers for their data link (ACARS/VDL Mode 2) systems. It is a given fact that airlines or aircraft operators do not want the consequences of malicious interference (a.k.a. “hacking”) of their data processing systems. The major question is, “do airlines and aircraft operators want the same level of protection applied to their air to ground data link communications as applied to current terrestrial networks? As DSPs open up their front-end communications to Internet web-based clients in order to increase accessibility for smaller airlines or aircraft operators, the probability of someone attacking the DSP network geometrically increases with the number of new communications paths.

(a) **ATS Applications:** ARINC Characteristics 622 for Future Air Navigation Services (FANS) messaging and 623 for Air Traffic Information Services (ATIS) currently comprise the ATS applications on aircraft.

   1. **ARINC 622 (FANS):** ARINC 622 messages employ a 16-bit Cyclic Redundancy Check (CRC) value calculated to the message body information (usually referred to as the message payload). When a FANS message reaches the aircraft communications management unit (CMU) -- communications management function (CMF) in integrated avionics such as Honeywell’s Airplane Information Management System (AIMS) in the Boeing 777, or the Airbus Industries’ Air Traffic Services Unit (ATSU) – the CMU/CMF strips the ARINC 618/620 message header and routes the message payload with CRC to the aircraft flight management computer (or system) (FMC) where the message payload is evaluated. If the transmitted CRC value does not match the FMC calculated value for the message payload, the FMC ignores the “corrupted” message. If the FMC calculated value matches the transmitted CRC value, the FMC accepts and processes the message. The purpose for the CRC value is to prevent corruption of the FANS message as it is transmitted. However, CRC checks do not constitute message integrity as defined by the ATN SARPs in that integrity is defined from the message sending entity on the ground to the aircraft receiving entity (CMU/CMF) and visa versa. It is entirely possible to intercept an ARINC 622 message and alter the message payload with new instructions and provide a recalculated CRC to match the new instructions. The FMC would not differentiate the difference because the FMC would calculate the CRC based on the message payload only and compare to the CRC transmitted for message validity (i.e., a rogue entity could transmit a “valid” message as far as the FMC is concerned, but not what an Civil Aviation Authority/Air Traffic Service Provider (CAA/ATSP) originally instructed). The ATN SARPs PKI architecture goes further in that message integrity and authenticity are checked based on certified public certificates between the aircraft and CAA/ATSP (or AOC entity). In addition, the ATN SARPs require the use of counters that preclude message playback. Employing a standardized PKI service for FANS messaging would lead the way for ATN security service in the future. It would facilitate the development of the policies and practices for CAAs/ATSPs for the rollout of the ATN security services to oceanic areas.

   2. **ARINC 623:** ARINC 623 message formats such as Pre-Departure Clearance, Departure Clearance, Oceanic Clearance, et cetera support ARINC 622 CRC. Instead of the FMC being the end system on the aircraft, the CMU/CMF is designated end system that performs the same type of CRC evaluation. ARINC 623 messages also have the same failing as ARINC 622 messages. CRC are calculated based on the length of physical message payload only. An altered message can be sent as long as a new CRC is generated that properly reflects the altered message content.

(b) **Aeronautical Operational Control (AOC) Messaging:** This report is using ICAO definition of “AOC” for messages between an aircraft and the airline or aircraft operator’s terrestrial host systems. AEEC documentation uses several definitions for AOC such as Airline Operational Communications, Airline Operational Control, or Aeronautical Operational Communications (ARINC 758). Currently, AOC messaging constitutes the vast majority of data link communications between aircraft and ground host systems. AOC messaging is an integral part of an airline’s operations, yet except for a very small number of airlines employing vendor proprietary encryption schemes primarily to meet governmental laws (mostly European airlines at this time), the message content is readily accessible on the Internet by an avid community of “eavesdroppers” who intercept and publish messages. Just use any available Internet search engine and type “ACARS”. Most search engines will return over 10,000 “hits”, many of them will be for software products that can decode ACARS messages and display them on both graphical (e.g., position reports) and textual human readable formats (i.e., properly formatted). The ad hoc committee could not come to a consensus as to the value of developing a common PKI scheme for AOC messaging.
at this time. As such, the USAF will continue working with a major vendor in developing its “Secure ACARS” program. The basic question still exists for AOC messaging, does AEEC want to invest in developing a common PKI security mechanism that would or could be applied to ACARS AOC messaging in order to prevent interception and publication on the Internet?

(c) Aeronautical Administrative Communication (AAC) Messaging: AAC messaging is analogous to AOC messaging and has the same limitations to message content privacy and is just as vulnerable to intercept and unsolicited publication. The same question about the application of common PKI security mechanism to preclude interception and unsolicited publication exists.

(2) Airline Information Technology (IT) Applications: As airline IT systems expand to the aircraft environment, airline IT managers will logically try to expand their existing PKI systems to the aircraft subsystems. Where terrestrial based PKI systems are employed on relatively high bandwidth networks or lower bandwidth telephone networks, application to wireless mobile networks propose a significant challenge as evidenced by the current problems to mobile phone data networks. The airline industry will face the same “growing pains” as airline IT groups expand their information security envelope. Without development of a standardized PKI scheme for the aircraft, different aircraft communications paths could impose different security mechanisms that an airline or aircraft operator IT group would have to manage.

(3) Information Security Impacts: Information security will impact many different aircraft systems in the near term. To maximize cost efficiency and minimize deployment of multiple independent security mechanisms, and airline or aircraft operator IT security group should address the following concerns:

(a) A common methodology among all vendors for interoperability, not only within an airline or aircraft operator’s fleet, but also across all airlines or aircraft operators.

(b) Historically, piecemeal or customized solutions are ultimately more expensive than a standardized solution.

(c) A security mechanism that is a common solution for all avionics, yet allows individual airlines or aircraft operators to retain their individual protection.

(d) A common methodology that supports current aircraft data link technology with low bandwidth communications – not simple extension of wired “IT” security.

(e) A PKI security mechanism that is adaptable, scaleable, and flexible and allows for variations in key longevity to accommodate differences in airline security policy. So as aircraft communications network change and/or grow, the need to “reinvent the wheel” is mitigated. A good standardized key management system would be airline security policy-tolerant with respect to the number of keys required and key longevity.

(f) Putting more data across the aircraft-ground boundary through public networks. Airlines or aircraft operators will need to address the following issues:

1. Integrity concerns – information is not changed as it transmit through a network.

2. Privacy concerns – company information is only read by the entities authorized to receive it, not read and reproduced on the Internet for the world to see.

3. Delivered to right place – the message is sent to the intended recipient, and if received by someone else, the sender is alerted that the message did not go to the proper recipient.

4. Authenticated source – the sender is who he or she says they are, and not someone else.

2. Benefits:

The benefits of a common PKI scheme for all aircraft systems will lead to a lower total cost of ownership. Each entity such as airline/operators, avionics vendors, airframe manufacturers, civil aviation authorities (CAA)/air traffic service providers (ATSPs) and data link service providers have a vested interest in developing a common PKI scheme. Effective elimination of redundant or multiple arbitrary and/or proprietary designs means significant cost savings. Effective use of a common PKI scheme that can be retrofitted into existing aircraft systems and migrate to future systems as they become available will minimize the cost of aircraft upgrade programs requiring data and data link security. The benefits to each major organizational entity are as follows:
a. **Airlines/Operators:** Airlines and aircraft operators to include the military use various and/or multiple vendors in order to get the best price for mixed fleet of aircraft. In some cases, the airline or aircraft operator may not have a choice as to the equipment available for a particular airframe. This is particularly true today with ACARS communications management units (CMUs) today. One vendor may offer a rudimentary character substitution scheme using look-up tables while another may offer a totally different algorithm for encrypting the data. Neither scheme will be acceptable for ATN security. Neither scheme will support EFB nor ADN security requirements because of the very large binary data exchange anticipated for these systems versus the much lower data exchange requirements for existing aircraft systems such as a CPDLC FANS flight management system (100s megabytes for EFB or ADN/ANFS on average data transfers vs. 1-2 kilobytes for CPDLC FANS on average data transfers). However, a significant cost driver to airline and aircraft operators is the current propensity for vendors to develop proprietary functions for aircraft systems that require a corresponding proprietary solution for their ground host systems. If a standard PKI scheme is not applied for EFB and/or ADN/ANFS security that will eventually support ATN, then an airline or aircraft operator could potentially end up with a series of mutually exclusive security services that would entail separate installation costs as well as increased annual operating and maintenance costs. A unified PKI security mechanism for an airline’s or aircraft operator’s ground host system would lead to a single one-time set-up and installation cost with incremental modification cost as necessary as well as reduced annual operating and maintenance costs. The other significant cost reduction will be on the aircraft as a common scheme could lend to a centralized PKI installation and operation. In this case, the airline or aircraft operator would only have to perform routine PKI key maintenance on the centralized aircraft system as opposed to multiple aircraft systems.

b. **Avionics Vendors:** A standardized security key management system that is common to all aircraft systems requiring data security enables avionics vendors to offer this important security feature to their airline and aircraft owner customers at an affordable price. Consequently, affordable pricing will permit a large portion of the airline and aircraft owner community to justify investment in this important infrastructure protection technology. Also, standardizing the method of managing security keys for all aircraft systems provides avionics vendors with a larger potential market than if each vendor implements a proprietary solution. However, if proprietary solutions develop, airline and aircraft owners will be faced with the decision of: (1) potentially implementing multiple key management systems and procedures in their operations centers, one for each unique aircraft system implementation at a significantly higher cost due to duplication of functionality, (2) purchase aircraft systems from only one or a few vendors to reduce their key management system cost of ownership, or (3) forego critical data security functionality because it its too costly to implement.

With respect to the first option, it is obvious that implementing multiple proprietary key management solutions is disadvantageous for all stakeholders due to the duplicative costs for development, procurement, fielding, operation, and maintenance associated with each proprietary solution. The second option represents a significant threat to avionics vendors in terms of the size of the potential market. If an airline adopts a proprietary security key management system to support one particular aircraft system of one avionics vendor, this may lock the airline into a single-vendor solution and place other avionics vendors at a competitive disadvantage for sales of other, future aircraft systems. Other vendors will need to overcome the price advantage that the original vendor enjoys because the airline does not need to re-purchase the original vendor’s key management system where as the other vendors will need to quote the price of their key management system. This will just artificially inflate the cost of security features for all purchasers. The only parties to benefit would be the first avionics vendors to sell proprietary key management systems in significant numbers. Finally, option 3 is the worst outcome for avionics vendors and airline and aircraft owners alike since this is the case where the cost of data security functionality for aircraft systems is unaffordable. In this case all stakeholders lose and only those who seek to harm or disrupt the industry win.

Specifically, avionics vendors see that a security key management standard would enable them to lower their development costs by reusing key loading, key protection, key removal, and related security functionality across multiple product offerings. Also a security key management standard that covers multiple aircraft systems will result in an overall lower cost of developing industry standards than if subcommittees develop unique security key management standards within each industry product specification. For these reasons, avionics vendors encourage the development of an aircraft systems security key management standard.

c. **Airframe Manufacturers:** Present aircraft mostly support ACARS datalink, used for AOC/AAC operations as well as for ATC applications (ATS - ARINC 623 and FANS 1/A - ARINC 622). Requirements on security (especially confidentiality and integrity) have been expressed by a number of airlines (for AOC operations).
Evaluation of the Implementation
Of APIM 02-002
ICAO ATN Key Management and Distribution

However, no standard security solution has been defined yet for ACARS. Some proprietary solutions are under development or already available. To an airframe manufacturer, this is creates an added burden in requiring multiple part numbers for hardware and software as well as multiple documentation numbers. Costs, which are ultimately, passed on to the airlines and aircraft operators.

Another set of systems also requiring datalink is emerging, Airborne Information Systems. Main Equipment and Aircraft manufacturers already propose products to the airlines (AFIS by Airbus for example). These systems may use ACARS datalink but primarily access higher speed subnetworks, such as Gatelink (802.11), INMARSAT High Speed Data (HSD) Satellite Communications (SATCOM), or Satellite Broadband, and others, using mostly IP standards, thus benefiting from IP widespread solutions and performances, but also increasing the exposure and sensitivity of aircraft systems to security attacks. Developing appropriate security solutions for these systems is a must.

As seen in Figure 1, limited Controller Pilot Data Link Communications (CPDLC) Baseline 1 (B1)/ATN deployment takes place now – full level C deployment of CPDLC/ATN and thus probably of ATN security is not defined today.

Security concerns also were raised on other types of systems, for example Software upload. Depending on the ATN roadmap and other services availability, a single PKI infrastructure solution, several independent, or homogeneous solutions may be elected, but tackling with this issue globally will maximize commonality between PKI solutions. Having homogeneous approaches will decrease airborne equipment cost, alleviate support activities, and decrease key management activities cost.

d. CAA/ATSP: Today information security is a hot topic for CAAs and ATSPs. The focus on information security stems from increased awareness of threats and new vulnerabilities introduced by advanced aeronautical applications. Within the US, for example, this was highlighted by Presidential Decision Directive 63 [1], which promotes information security within all government departments and specifically requires the FAA to “develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks”.

The security of data link applications are of particular concern for CAAs and ATSPs because they introduce new digital data connections to ground systems which cannot be physically isolated due to their wireless nature. The Mission Need Statement for the FAA’s NEXCOM program [2], for example, cites security and prevention of so-called “phantom controllers” as one of the fundamental drivers for the program.

CAAs and ATSPs therefore have a strong interest in the introduction of ATN security. However they recognize that ATN security requires equipment in aircraft as well as in ground systems. Therefore AEEC work in this area will ease the transition to secure ATN that CAAs and ATSPs desire.

Furthermore in the current industry climate, deployment of ATN security will be to an extent dependent on economic concerns. The desire identified by the ad hoc group on key management to promote a common security architecture across applications will help to address economic considerations by amortizing the cost of security. Thus a common security architecture will benefit CAAs and ATSPs in two ways: first it will further ease the transition to secure ATN, and second it will indirectly protect CAA and ATSP ground systems from indirect attacks launched through non-ATC aircraft applications via ATC applications.

It is worth noting that developing a common security architecture will also complement ongoing efforts driven by CAAs and ATSPs in the ICAO ACP. ICAO ACP is working on the addition of confidentiality support to the ATN SARPs with the goal of facilitating the use of the ATN for ATC applications. Thus the fundamental aim of both efforts is to promote synergy between the security provisions used by ATC and AOC applications.

e. Data Link Service Providers (DSPs): Establishing standardization in the area of Key Management and Distribution for datalink would be in the best interest of DSPs. Standardization has the potential to provide benefits to DSPs in the following areas.

(1) Interoperability from DSP to DSP: Users have come to expect seamless datalink service no matter where in the world they are flying and no matter which service provider they may be using. For security services, this expectation would indeed continue. Lack of standardization for these services could result in degradation in the security services from one DSP to another or no security services capabilities being available to a user at all if a DSP supports a proprietary solution.
Evaluation of the Implementation
Of APIM 02-002
ICAO ATN Key Management and Distribution

It has been demonstrated in the past that in order to keep interoperability issues to a minimum or alleviate them entirely, standards must be established. To DSPs, standardization in this area means a more satisfied customer with less costs incurred since less engineering hours would have to be spent troubleshooting interoperability issues.

(2) Interoperability from Application to Application: Not only do users expect seamless service from DSP to DSP, they expect the same level of service from application to application. Applications services may be provided by the DSPs using products developed in-house or DSPs may use a third party for this purpose. In order to reduce costs for providing datalink security services, being able to standardize security for all application services provided is imperative.

(3) Cost Reduction: A standardized solution will reduce DSPs costs immensely. Conversely, proprietary solutions could be quite costly to the DSPs. Depending on the implementation chosen, without standardization, DSPs may have to implement proprietary software for each user depending on the users’ requirements. The cost for this would then have to be levied back to the customers.

(4) Administrative: Standardization for Key Management and Distribution would reduce the level of administrative support required from DSPs. Proprietary security solutions may levy various requirements on the DSPs from user to user. Administrative costs would be incurred for this to record and manage the various customer needs. Also, managing the information for proprietary solutions could propose a security risk in and of itself.

3. Scope of Effort:

Developing a standard PKI security mechanism for airline and aircraft operators is not a trivial task. Airlines and/or aircraft operators will have to evaluate their IT and operational activities with respect to current and future data link architectures. The work required by AEER to develop the necessary security standards and/or characteristics will most likely entail the creation of a standing subcommittee or working group as the workload of current AEER subcommittees or standing working groups preclude the amount of time necessary to develop a common standard. Fortunately, this new subcommittee or working group will be able to leverage the PKI work done by ICAO, as well as the work done by existing AEER subcommittees.

a. What is needed: As stated earlier, the ad hoc committee identified technologies that will precede the ATN. Underlying the deployment of these technologies will be need for a common security mechanism.

(1) Future aircraft systems:

(a) ADN: The ARINC 664 Aircraft Data Network (ADN) working group perspective is provided herein. This is a view from the current editor of the security component and has not been vetted by the ADN working group as a whole.

The ARINC 664 Aircraft Data Networks (ADN) working group is adapting commercially defined networking standards to an aircraft environment to provide a common interface definition at the architectural and guidance level. The commercial networking standards that are being adapted include IEEE Ethernet and IETF IP Protocols.

At a high level, four network domains have been defined onboard the aircraft: Avionics, Information Systems, In Flight Entertainment and Passenger Electronic Devices. Devices in each of these domains are connected or will be connected with off-board communications. The Avionics and potentially the Information Systems domains support both ATC and AOC communications. The Information Systems and In Flight Entertainment domains support AAC. It is desirable to have a single Security Key Management system to support any or all of ATC, AOC and AAC.

Although the impetus for a unified Security Key Management system is for the ATN, its utility includes supporting the IP-based ADN environment -- which itself supports ATN and future IP-based air-ground communications for ATC, AOC and AAC.

The ADN Network Security Architecture provides firewall and VPN components between the four major onboard network domains and within individual sub-domains as appropriate. Strong cryptographic mechanisms are used for the Virtual Private Networks (VPNs) and for the infrastructure protocols including Routing and Quality of Service. These cryptographic mechanisms can simultaneously utilize the same Security Key Management system that supports the ATN Application Layer and Routing security.
Architectural and guidance material on Security Key Management including Key/Certificate Management Lifecycle, the Certificate Request Model, and the Certificate Policy and Certificate Practice Statement should be included in or referenced by the ADN specification.

(b) **EFB**: EFB technology is being developed and deployed current generation aircraft. There are three types of EFBs. Type 1 EFBs are basically carry-on computer with no interface to the aircraft data link communications network. Information updates are performed only on the ground and any security service would be the responsibility of the airline or aircraft operator’s IT department. Type 2 EFBs and Type 3 EFBs on the other hand connect to the aircraft data link communications architecture, with difference being Type 2 EFBs are carry-on systems like Type 1 EFBs while Type 3 EFBs are permanently installed in the cockpit. Both Type 2 and Type 3 EFBs contain safety of flight and company sensitive information. While on the ground, Type 2 and Type 3 EFBs would most like communicate to the host server via Gatelink. While in the air, these systems will most likely use high bandwidth satellite services when available.

(c) **Gatelink**: Gatelink technology currently uses wireless communications networks in the 800 Mhz to 2.4 G Hz frequency range while the aircraft is on the ground to communicate with a ground host application. Depending on the vendor, the technology employs either cellular phone technology or IEEE 802.11 wireless communications protocols. For systems using 802.11 protocols, the de facto standard for link security is the Wired Equivalent Privacy (WEP) protocol. This protocol provides encryption at the physical link layer between the aircraft and the ground receiver/transmitter. The initial WEP protocol did not protect the privacy of messages very well. The next IEEE standard for wireless communication security will be 802.11i. The IEEE final 802.11i standard will incorporate Federal Information Processing Standard (FIPS) Advanced Encryption Standard (AES), a very robust and secure standard recently approved by the US Government for transmission of sensitive information [3].

(d) **HSD SATCOM and Satellite Broadband**: INMARSAT Swift64 and Connexion By Boeing Satellite Broadband are being installed on aircraft today. Currently, neither the HSD SATCOM nor Satellite Broadband systems are authorized to interface with the aircraft system avionics. However, both systems are designed to be the principal communications path for the ADN while an aircraft is flying. It is this type of multiple communications paths in the aircraft where a common PKI security mechanism needs to be developed; otherwise multiple security mechanisms could evolve over time increasing the support costs for different systems.

(2) **Future aircraft architectures**: The Security Key Management mechanism will have a significant impact on the future onboard aircraft architectures in areas including the interface to Certificate and Registration Authorities, and the centralization or distribution of private keys onboard the aircraft. Figure 2 represents the various airframe manufacturers near term plans for equipage. This paper addresses the demarcation between aircraft systems and airline or aircraft owner operations represented by the “Essential” and “Non-Essential” Network currently planned for aircraft. This paper does not address passenger In-Flight Entertainment (IFE)/Cabin Distribution or wired/wireless passenger communication service to the right of the “Open” Network. Any aircraft server would require application of security services that come under control by the airline or aircraft operator.

(3) **Develop Guidance on how to implement PKI security mechanisms**:

(a) Section 2 of this report presented the benefits of a standardized Public Key Infrastructure (PKI) that permits aircraft operators to address the security needs of both their ground-based as well as aeronautical applications. The AEEC Ad Hoc attendees recognized that guidance is necessary to enable implementation of such a PKI. Examples of areas where guidance is needed include:

1. Loading of keys and certificates into avionics in order to ensure that a single PKI can support interaction with avionics supplied by different vendors.

2. Sharing security information between avionics in order to ensure that it is possible to centralize security even in environments involving multiple aircraft systems and equipment from multiple vendors.
Uniform life-cycle key management processes that support secure key distribution to multiple aircraft systems provided by different vendors and that support interchangeability of avionics equipment across multiple platforms.

(b) Issues to be considered: Section 3.a provides a complete list of the areas where the AEEC Ad Hoc attendees felt that guidance would be beneficial.

1 The development of a standardized PKI will require the input from several perspectives and functional groups, some of which are not traditionally involved in avionics specification development. The aircraft operators’ Chief Information Officers (CIOs) and Information Technology (IT) Security Managers may be more knowledgeable about data security threats and vulnerabilities than the avionics-engineering department because of their years of experience in wired network threats and vulnerabilities. Also, with the development of higher bandwidth communications links to the aircraft, the distinction between an aircraft operator’s wired, ground-based, end systems and aircraft end systems will begin to blur. Therefore, it is important that the CIOs and IT security managers are involved with the development of aeronautical PKI standards and key management system specifications. The aircraft systems create a few unique challenges due to their limitations in processing and storage capacity, interface and certification requirements. Therefore, participation of aircraft/avionics systems engineers and aircraft operators is also essential for the development of cost-effective, implementable PKI and key management standard.

2 There are several issues that it will be necessary to take into account during develop of guidance on implementing PKI. In particular, the air/ground data links supporting aircraft essential and airline operational data will be significantly lower in bandwidth with respect to terrestrial networks for the foreseeable
future. As illustrated by the analysis conducted by ICAO when developing the ATN Security solution, these low
bandwidth links cannot easily assimilate the overhead brought by a traditional wired network security solution
without significant impact to the cost of data transmission and network message capacity. In order to address this
concern, it is recommended to use the work completed by ICAO on ATN Security as a valuable baseline for
expanding security key management into other aircraft systems. Some of the other issues to be considered in
defining a standardized key management system are include the following:

a. Can a unique or small set of options be developed across all aircraft systems for
loading keys into aircraft systems and for secure distribution of keys to all required systems?

b. Do aircraft operators operate in-house Certificate Authorities (CA) to support data
security services for their existing ground-based applications?

c. If yes, can existing PKI systems accommodate the unique requirements of aircraft
systems and ATN-like security cost-effectively?

d. Can the existing/proposed PKI and key management systems seamlessly migrate to
ATN security to support ICAO applications?

b. Level of effort: The estimate of the effort by AEEC to develop a comprehensive PKI security standard is
predicated on the time it will take to perform a detailed technical assessment. ATN Document 9705, Sub-Volume
VIII specified in great detail the methodology for coding and calculating PKI security algorithms and certificates.
As stated by the original request for help in APIM 02-002, additional technical factors need to be developed to fully
implement an operational PKI architecture on an aircraft and within a ground communications infrastructure.

(1) Technical Assessment: Table 1 represents the technical aspects that will need to be developed into an
AEEC specification. This list is only the beginning. As items are discussed, additional technical aspects will most
likely be identified.

<table>
<thead>
<tr>
<th>Technical Parameter</th>
<th>Functions to be Evaluated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Physical and software security controls to limit access to authorized personnel and detect unauthorized personnel and/or activities. Procedures will need to be established for aircraft systems as to personnel authorized to load and manage the PKI Security Service keys and databases.</td>
</tr>
<tr>
<td>Airborne Context Management (CM) Database</td>
<td>Database that stores information about aircraft parameters. Physical location needs to be determined as well as how aircraft and ground host systems will access the database.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Part of access control, function to log all authorized access and communications as well as unauthorized attempts to access systems. For airborne equipment, where recording database will be stored and frequency of download by airline/aircraft operator to review database log.</td>
</tr>
<tr>
<td>Certificate Authority (CA) Key/Certificate Update</td>
<td>Physical organization that certifies airline/aircraft operator PKI certificates and distributes PKI public and private keys and X.509 certificates and certificate updates. Airlines and Aircraft Operators will need to determine who and/or where CA Key/Certificate Updates will be processed.</td>
</tr>
<tr>
<td>Crypto Parameter Database</td>
<td>Physical database in airborne and ground systems that store shared keys and “X” values for a given security session.</td>
</tr>
<tr>
<td>Crypto Services Implementation</td>
<td>Function that determines when security services are required and which aircraft subsystems will require security services based on information content.</td>
</tr>
<tr>
<td>Data Recording Requirements</td>
<td>Determination of how information will be recorded, before or after security service processing, and where the recording will take place. Airlines and aircraft operators will also need to determine how copies of aircraft and ground host system private keys are stored for accident investigation.</td>
</tr>
</tbody>
</table>
**Evaluation of the Implementation**  
**Of APIM 02-002**  
**ICAO ATN Key Management and Distribution**

<table>
<thead>
<tr>
<th>Technical Parameter</th>
<th>Functions to be Evaluated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground Context Management Application (CMA) Database of Aircraft Root Certificates</td>
<td>Ground system database that stores all active aircraft Root Certificates in ATN for access by the CMA and other ATS/AOC applications during a secure session. The physical location of this Database needs to be developed along with the procedures and technical applications to distribute the information.</td>
</tr>
<tr>
<td>Key Generation</td>
<td>The software process to actually generate aircraft and ground system Private and Public Keys, then manage and distribute the keys to aircraft and ground system security services.</td>
</tr>
<tr>
<td>Legal Intercept</td>
<td>The process by law enforcement agencies to de-encrypt encrypted messages for use as evidence in a criminal or civil investigations. Airlines and aircraft operators will need to develop procedures and processes to provide aircraft and ground system Private and Public Keys when required by applicable law or laws to law enforcement agencies.</td>
</tr>
<tr>
<td>Loading Certificates</td>
<td>The technical procedures to electronically upload X.509 certificates into the Aircraft Avionics PKI security service application and ground systems PKI security service application. Technical analysis will be required to determine the minimum required content for certificates in order to minimize transmission times to aircraft, if required over bandwidth limited links.</td>
</tr>
<tr>
<td>Loading Keys</td>
<td>The technical procedures to electronically upload Private Keys into aircraft avionics PKI security service application and ground systems PKI security service application. Technical analysis will be required to determine the longevity of private keys, which is likely to vary by application and airline security policy.</td>
</tr>
<tr>
<td>Private Key Protection</td>
<td>The physical and electrical procedures required for protecting the installation and location of private keys in the aircraft and ground systems. Analysis will be required to develop techniques for alerting authorized personnel that a private key has been transmitted or corrupted.</td>
</tr>
<tr>
<td>Private Key Removal</td>
<td>The physical and electrical procedures required to remove private keys from aircraft avionics and ground systems so that hardware may be sent out for maintenance.</td>
</tr>
<tr>
<td>Sharing Keys and “X” value</td>
<td>The technical specifications for allowing aircraft and ground systems to establish and terminate security sessions by negotiating session key values and the Shares Key Value “X” based on X.509 certificate information.</td>
</tr>
<tr>
<td>Verify “Goodness” of implementation</td>
<td>Determining what is the most appropriate FIPS 140 procedures for analyzing PKI security schemes and requiring avionics and ground system vendors to implement FIPS 140 into test and evaluation program.</td>
</tr>
</tbody>
</table>

(2) **Schedule and resources required:** Figure 3 shows a typical timeline for developing an AEEC Characteristic or Specification. The Ad Hoc committee evaluated the timeline and determined that a two-phased approach would support the need for a common PKI Security Service in the aircraft.

(a) **Near Term Effort:** The Ad Hoc committee evaluated the requirements for work for next year. The consensus of the committee members is that the scope of the current APIM needs to be expanded in order to fully evaluate the technical requirements for a common PKI security architecture. In Figure 4, the Ad Hoc committee evaluated the time flow versus aircraft architecture roadmap of Figure 1. By beginning ground work now to develop a technical specification or specifications, the committee believes that a common PKI security architecture can be specified in time for the near term and next generation aircraft systems. The committee estimates that it will take three regularly scheduled meetings, each meeting lasting 2 days, and a potential for two to three ad hoc meetings as necessary to formally draft a project plan. A preliminary outline for a project plan is found in Appendix B to this report.

(b) **Far Term Effort:** The far term effort will entail the creation of permanent Security Service Subcommittee since a common PKI Security Service will cover many aircraft subsystems. The work effort will be to develop the necessary AEEC PKI Security Service Characteristics and/or Specifications for implementation on near term avionics. This subcommittee would continue to work with Data Link Systems Subcommittee, VDL
Subcommittee, Air-Ground Subcommittee and the Systems Architecture and Interface subcommittees and working groups to ensure that all of these committees and groups would reference the corresponding security documents, and not developing or incorporating other available standards. The work estimate for this phase is three scheduled meetings per year, 2-3 days per meeting with ad hoc meetings as necessary. The first draft specifications would be due in December of 2004.

c. Synergy with other AEEC committees: Synergy will be very important. As reported by SITA [4] in a presentation to September Data Link Systems Subcommittee, the ARINC 763 Working Group adopted the EAP-TLS protocol for strong authentication, yet did not identify a security protocol for integrity. The EAP-TLS authentication protocol is designed to support large-scale networks using Internet Protocol (IP) services. It is not a very efficient protocol for small message formats or bandwidth limited communications services. This is an excellent example that if a common PKI security architecture is not adopted, then a proliferation of software services can and will occur on the aircraft.

### TIME FLOW FOR SECURIT DEVELOPMENT

- **Five years**

  - **Near Term**
    - 36 months: Develop Top-Level Procedures
  - **Far Term**
    - 24 months: Coordinate Detail Procedures with Operators and States
  - Implement the Procedures: 12 months
  - 24 months: Design the Required Equipment
  - Install and Certify the Equipment: 18 months
  - Ready to Operate

**Figure 3: Time Flow for Security Development (Courtesy AEEC Staff)**

### 4. Conclusions:

The following recaps the conclusions identified by the members of the Ad Hoc Committee:

a. The current APIM 02-002 work effort for ICAO is still valid, but that the aviation community will not begin operation on a fully deployed ATN until after 2010. It would be premature for the AEEC to begin developing security service specifications specifically for the ATN at this time.
As seen in Figure 4 above, there are several near term avionics systems being deployed on aircraft that will require security services to protect the information stored and transmitted between the aircraft and the ground.

The ATN Security Services specified in ICAO Document 9705, Edition 3, Sub-Volume VIII are well documented as to the way a PKI Security Service should function and could be readily adapted to other systems on the aircraft. The development of common PKI security service that will eventually support ATN security requirements is very desirable, both from a technical and operational benefit by owners, avionics vendors, aircraft integrators, CAAs, and DSPs.

A common PKI security mechanism will lead to a lower life-cycle cost for the aircraft and associated ground systems than the proliferation of separate proprietary security mechanisms.

5. Recommendations:

It is the recommendation of the Ad Hoc Committee on ATN Key Management that the AEEC adopt a work plan to develop a common PKI security architecture for aircraft. As such, the Ad Hoc Committee further recommends that the current APIM 02-002 be either broadened to include other systems, or that a separate APIM be generated to develop a project plan for common PKI security services in the aircraft.

6. References:


7. Acknowledgements:

The co-chairman for this meeting wish to acknowledge the following individuals for input to this report:

a. Figure ES-1 and Figure 3: Courtesy of Mike Russo, AEEC Staff, ARINC, Annapolis, MD.

b. Figure ES-2 and Figures 1, 2, and 4: Courtesy of Arnold Oldach, Rockwell Collins, Cedar Rapids, IA.

c. Various sections of this document:
   • Simon Blake-Wilson, BCI
   • Vic Patel, FAA WHJTC
   • Mike Olive, Honeywell
   • Debbie Jacobs, ARINC
   • Eric Mehn, SITA
   • Frederic Durand, Airbus
   • Don Kauffman, Honeywell
   • Arnold Oldach, Rockwell Collins
   • Jim McMath, Titan Corp. (USAF)
   • Bob Stevens, Tectura Corp. (Boeing)
## Evaluation of the Implementation
Of APIM 02-002
ICOA ATN Key Management and Distribution

### Appendix A: Ad Hoc Meeting Attendees

<table>
<thead>
<tr>
<th>Name/Title</th>
<th>Address</th>
<th>Office #/Fax #</th>
<th>Email Address</th>
</tr>
</thead>
</table>
| Blake-Wilson, Simon  
Director, Information Security | BCI/FAA ACB-250  
96 Spadina Ave, Unit 606  
Toronto, Ontario, M5V 2J6 Canada | 416-214-5961 (office)  
416-214-5961 (fax) | sblakewilson@bcisse.com |
| Dhas, Chris  
Computer Networks & Software, Inc.  
7405 Alban Station Court, Suite B-225  
Springfield, VA 22150-2318 | 703-644-2103 (office)  
703-644-2309 (fax) | Chris.dhas@cnsi.com |
| Durand, Frederic  
Airbus Industries |  |  | Frederic.d.durand@airbus.com |
| Freeman, Mark  
Volpe |  |  | freeman@volpe.dot.gov |
| Gallagher, Alan  
Volpe Center Cyber Security Program Manager | 2001 L St NW, Suite 1000  
Washington, D.C. 20036 | 318-387-9999 (office)  
318-387-9999 (fax) | alan@netcorp.org |
| Harnett, Kevin  
Volpe Center Cyber Security Program Manager |  | 617-699-7086 (office)  
617-699-7086 (fax) | harnett@volpe.dot.gov |
| Hooper, James  
Computer Security Rep | Northrop Grumman  
12011 Sunset Hills Rd  
DC10/3354  
Reston, VA 20190 | 202-314-1270 (office)  
717-252-3784 (fax) | james.hooper@auatac.com |
| Jacobs, Debbie  
Aeronautical Radio, Inc.  
2551 Riva Road  
Annapolis, MD 21401 |  | 410-964-7343 (office)  
410-964-7343 (fax) | daic@arinc.com |
| Kauffman, Don  
Senior Principal Engineer  
Northrop Grumman | Honeywell  
7000 Columbia Gateway Drive  
Columbia, MD 21046-2119 | 410-964-7343 (office)  
410-964-7343 (fax) | Don.kaufman@honeywell.com |
| Keblawi, Feisal  
FAA |  |  | Feisal.keblawi@faa.gov |
| Madsen, 1Lt John J.  
Project Manager  
ESC/GAD | ESC/GAD  
75 Vandenberg Drive  
Hanscom AFB, MA 01731-2103 | 781-377-9162 (office)  
781-377-9319 | John.madsen@hanscom.af.mil |
| McGowan, Shirley Brewer  
Chief System Engineer  
Information System Security  
ESC/GAD (Titan Corporation)  
75 Vandenberg Drive  
Hanscom AFB, MA 01731-2103 | ASD-103  
Federal Aviation Administration  
800 Independence Avenue, S.W.  
Washington, D.C. 20591 | 202-385-7239 (office)  
202-385-7239 (fax) | Shirley.McGowan@faa.gov |
| McMath, James M.  
Senior Engineer  
ESC/GAD (Titan Corporation)  
75 Vandenberg Drive  
Hanscom AFB, MA 01731-2103 |  | 781-377-1248 (office)  
781-377-9319 (fax) | James.mcmath@hanscom.af.mil |
| Mehn, Eric  
SITA |  |  | Eric.mehn@sita.aero |
## Evaluation of the Implementation

**Of APIM 02-002**

**ICAO ATN Key Management and Distribution**

<table>
<thead>
<tr>
<th>Name/Title</th>
<th>Address</th>
<th>Office #/Fax #</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oishi, Roy T.</td>
<td>Aeronautical Radio, Inc. 2551 Riva Road Annapolis, MD 21401</td>
<td>410-266-2982 (office) 410-266-2047 (fax)</td>
<td><a href="mailto:RTO@arinc.com">RTO@arinc.com</a></td>
</tr>
<tr>
<td>Oldach, Arnold Principal Manager CNS/ATM</td>
<td>Rockwell Collins Commercial Systems M/S 124-110 400 Collins Road NE Cedar Rapids, IA 52498</td>
<td>319-295-6913 (office) 319.651.7432 (mobile) 319.295.0649 (fax)</td>
<td><a href="mailto:aoldach@rockwellcollins.com">aoldach@rockwellcollins.com</a></td>
</tr>
<tr>
<td>Olive, Michael Sr. Principal Systems Engineer</td>
<td>Honeywell 7000 Columbia Gateway Drive Columbia, MD 21046-2119</td>
<td>410-964-7342 (office) 410-964-7322 (fax)</td>
<td><a href="mailto:Mike.olyve@honeywell.com">Mike.olyve@honeywell.com</a></td>
</tr>
<tr>
<td>Patel, Vic Information Security Group Manager</td>
<td>ACB-250 William J. Hughes FAA Technical Center Atlantic City International Airport Atlantic City, NJ 08045</td>
<td>609-485-5046 (office)</td>
<td><a href="mailto:Vidyut.patel@faa.gov">Vidyut.patel@faa.gov</a></td>
</tr>
<tr>
<td>Pitts, Darlene</td>
<td>Volpe/CSC</td>
<td></td>
<td><a href="mailto:Pitt2211@bellsouth.net">Pitt2211@bellsouth.net</a></td>
</tr>
<tr>
<td>Rajcsok, Vic</td>
<td>Aeronautical Radio, Inc. 2551 Riva Road Annapolis, MD 21401</td>
<td></td>
<td><a href="mailto:var@arinc.com">var@arinc.com</a></td>
</tr>
<tr>
<td>Roy, Alok</td>
<td>AES Center of Excellence Communications &amp; Surveillance Tech Honeywell 7000 Columbia Gateway Drive Columbia, MD 21046-2119</td>
<td>410-964-7341 (office) 410-964-7322 (fax)</td>
<td><a href="mailto:Alok.roy@honeywell.com">Alok.roy@honeywell.com</a></td>
</tr>
<tr>
<td>Signore, Ted Principal Staff Center for Advanced Aviation System Development</td>
<td>The MITRE Corporation M/S N660 7517 Colshire Drive McLean, VA 22102-7508</td>
<td>703-883-7919 (office) 703-883-1367 (fax)</td>
<td><a href="mailto:signoret@mitre.org">signoret@mitre.org</a></td>
</tr>
<tr>
<td>St. John, Ed Product Marketing Manager</td>
<td>Rockwell Collins Commercial Systems M/S 124-115 400 Collins Road NE Cedar Rapids, IA 52498</td>
<td>319-295-8131 (office) 319-295-7214 (fax)</td>
<td><a href="mailto:eastjohn@rockwellcollins.com">eastjohn@rockwellcollins.com</a></td>
</tr>
<tr>
<td>Stella, Marie</td>
<td>FAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stenger, John Manager, Business Development</td>
<td>Honeywell Communication &amp; Surveillance Center of Excellence 2861 Bradley Acres Court Herndon, VA 20171</td>
<td>202-662-2683 (office)</td>
<td><a href="mailto:John.stenger@honeywell.com">John.stenger@honeywell.com</a></td>
</tr>
</tbody>
</table>
## Evaluation of the Implementation
### Of APIM 02-002
#### ICAO ATN Key Management and Distribution

<table>
<thead>
<tr>
<th>Name/Title</th>
<th>Address</th>
<th>Office #/Fax #</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stephens, Robert W.</td>
<td>Tectura Corporation&lt;br&gt;14205 SE 36th Street&lt;br&gt;Bellevue, WA 98006-1574</td>
<td>425-373-2563 (office)</td>
<td><a href="mailto:Robert.w.stephens2@boeing.com">Robert.w.stephens2@boeing.com</a></td>
</tr>
<tr>
<td>Toth, Louis</td>
<td>Honeywell&lt;br&gt;7000 Columbia Gateway Drive&lt;br&gt;Columbia, MD 21046-2119</td>
<td>410-964-7334 (office) 410-964-7322 (fax)</td>
<td><a href="mailto:Louis.toth@honeywell.com">Louis.toth@honeywell.com</a></td>
</tr>
<tr>
<td>Witulski, Robert D.</td>
<td>ARINC, MS 6-3550&lt;br&gt;2551 Riva Road&lt;br&gt;Annapolis, MD 21401-7465</td>
<td>410-266-4467 (office) 410-266-2047 (fax)</td>
<td><a href="mailto:Robert.witulski@arinc.com">Robert.witulski@arinc.com</a></td>
</tr>
</tbody>
</table>
Evaluation of the Implementation
Of APIM 02-002
ICAO ATN Key Management and Distribution

Appendix B: Outline ARINC Project Paper 6XX
Common Aircraft Public Key Infrastructure (PKI) Security Services

1. Introduction
2. General Provisions
   2.1. Public Key Management Infrastructure
   2.2. Roles And Responsibilities
       (CA Operator, CA Entity, RA Entity, Aircraft and Ground Entity, Relying Party, Certificate Repository)
   2.3. Data Recording Requirements
   2.4. Legal Intercept
   2.5. Verification and Validation
       (i.e., Verifying “Goodness” Of Implementations)
3. Aircraft and Ground Entity Identification And Authentication
   3.1. Entity Registration
   3.2. Revocation Authentication
   3.3. Re-Key Authentication
   3.4. Recovery Authentication
4. Technical Security Controls
   4.1. Certificate Authority Public/Private Key Pair Generation
       (Generation Techniques, Key Sizes, Key Usage, Cryptographic Parameters, Parameter Quality Checking)
   4.2. Certificate Authority Private Key Management And Protection
       (Escrow, Backup, Delivery, Installation, Activating, Deactivating, Archival, Destruction)
   4.3. Certificate Authority Public Key Certificate Management
       (Issuance, Validation, Re-key, Update, Suspension, Revocation, Archival)
   4.4. Certificate Authority Compromise Recovery
   4.5. Certificate Authority Cross-certification
   4.6. Aircraft and Ground Entity Public/Private Key Pair Generation
       (Techniques, Key Sizes, Key Usage, Domain Parameters, Parameter Quality Checking)
   4.7. Aircraft and Ground Entity Private Key Management And Protection
       (Escrow, Backup, Delivery, Installation, Activating, Deactivating, Archival, Destruction)
   4.8. Aircraft and Ground Entity Public Key Certificate Management
       (Issuance, Validation, Re-key, Update, Suspension, Revocation, Archival)
   4.9. Aircraft and Ground Entity Compromise Recovery
   4.10. Access Controls
   4.11. Security Accounting and Auditing
   5.1. RSA-Based Certificates And CRLs
   5.2. Elliptic Curve-Based Certificates And CRLs
6. Public Key Enabled Applications
   6.1. Cryptographic Services
       (Confidentiality, Integrity, Authentication, Key Agreement)
   6.2. Cryptographic Mechanisms
       (Digital Signature, Hash, Message Authentication Codes, Encryption, etc.)
   6.3. Cryptographic Algorithms
   6.4. Application Key Sharing
   6.5. Context/Session Management Databases
       (Airborne Entity, Ground Entity)