ATTACHMENTS

APPENDICES

1.0 INTRODUCTION

This document defines a standard implementation for strong client authentication and encryption of Wi-Fi-based client connections to onboard Wireless LAN (WLAN) networks.

WLAN networks may consist of multi-purpose inflight entertainment system networks operating in the PIES domain, dedicated aircraft cabin wireless networks or localized Aircraft Integrated Data (AID) devices operating in the Aircraft Information Services (AIS) domain.

Examples of client devices requiring connections to these networks include electronic flight bags, flight attendant mobile devices, onboard IoT devices, AID devices (acting as clients) and mobile maintenance devices.

(Add information that make it more clear that passenger device is out of scope)

1.1 Scope

This specification addresses the following characteristics of connections between mobile devices and onboard WLAN network infrastructures.

- Connections based on IEEE 802.11 wireless LAN standards.
- Onboard Remote Authentication Dial In User Service (RADIUS) authentication, authorization, and accounting (AAA) services will be required for authenticating client devices to onboard WLAN networks.
- Authentication protocol will be based on Extensible Authentication Protocol/Transport Layer Security (EAP-TLS).
- Mutual authentication will be enabled to ensure two-way trust relationships are established between clients and infrastructures.
- Encryption algorithms to be based on Advanced Encryption Standard (AES)- Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).
- The scope of this document is to create a secure connection between the infrastructure and wireless client(s).

This specification *does not* address the following characteristics of connections between mobile devices and onboard WLAN network infrastructures.

- Certificate management is outside the scope of this document but can be referenced in **ARINC Report 842:** *Guidance for Usage of Digital Certificates*.
- Client authentication policies will not require ground communication to allow a client to successfully authenticate to the WLAN network.
- Network subnet isolation and routing is outside the scope of this document.
- Client security outside of a secure wireless communication channel is outside the scope of this document.
- Wireless communication standards not included in IEEE 802.11 are outside the scope of this document.

1.2 Document Conventions

ARINC Standards are voluntary standards intended to ensure interchangeability and interoperability between equipment, independent of manufacturer or airframe.

In this standard, the following terms carry key significance:

- Shall: Identifies features required to meet the minimum level of compatibility intended by this standard.
- Must: Obligation, no other choice.
- Should: Used to recommend approaches to optimize transactions and management.
- Will/Is/Does: Used to express a statement of fact based on other requirements.
- May: Used to express an optional capability or choice.

1.3 Related Documents

ARINC standards related to this specification are listed below. When avionics systems and subsystems are designed to use the capabilities provided by this specification, they should incorporate the provisions of this specification by reference. References to this specification should assume the application of the most recent version.

ARINC Specification 628: *Cabin Equipment Interfaces, Part 1, Cabin Management and Entertainment System – Peripherals*

ARINC Specification 664: *Aircraft Data Network*

ARINC Specification 763: *Network Server System (NSS)*

ARINC Specification 763A: *Mark 2 Network Server System (NSS) Form and Fit Definition*

ARINC Specification 765: *Ethernet Switch Unit*

ARINC Report 811: *Commercial Aircraft Information Security Concepts of Operation and Process Framework*

ARINC Report 821: *Aircraft Network Server System (NSS) Functional Definition*

ARINC Specification 822A: *On-Ground Aircraft Wireless Communication*

ARINC Specification 823: *Datalink Security, Part 2, Key Management*

ARINC Report 842: *Guidance for Usage of Digital Certificates*

1.4 Relationship to Other Standards

2.0 ONBOARD SECURE WIFI NETWORK PROFILE STANDARD TERMINOLOGY

3.0 FUNCTIONAL REQUIREMENTS

3.1 Operational Assumptions

To operate a secure wireless network, the following assumptions are made to define the scope of the document and the guidance within this document.

3.1.1 General Operational Assumptions

The network shall be in an operational state, to facilitate the communications between the different nodes in the network. The different network nodes shall be able to communicate securely and in a timely manner without interference.

3.1.2 Assumptions Public Key Infrastructure

A Public Key Infrastructure (PKI) shall be in place and operational. The PKI shall be secure and trusted by the clients and the services in the infrastructure for the wireless network. The handling of the certificates must be handled in a secure manner.

3.1.3 Security Assumptions

The network, services and physical equipment on the network shall be secured against unauthorized access, both electronically and physically.

3.2 Functional/General Requirements

All authentication policies shall have the option to not require ground/external network communication. All authentication mechanics shall be present on the aircraft at all times. If any of the mechanisms fail the authentication chain shall be rendered inoperative, and thus not be able to authenticate wireless clients.

3.2.1 Network node communications

The network access point (AP) shall meet the IEEE 802.11 networking standards for the wireless communication.

All nodes should support IEEE 802.1x port-based network authentication.

3.2.2 Network services

All network services shall communicate over a secure connection for the chain of communication for the authentication process.

A remote authentication dial-in user service (RADIUS) authentication, authorization, and accounting (AAA) service must be running and connected to the Access Point (AP) for authentication.

A (S)NTP server must be running and connected to the AP to synchronize the clients, RADIUS instance and the AP in the network.

3.3 Performance Requirements

The clients that will connect to the network for authentication must support WPA2/3 Enterprise model with certificate authentication. And be able to store the certificates in a safe manner.

Performance requirements the that needs to be met are that the device needs to respond in a timely manner to the request made by both the access point and the RADIUS server. The device needs to have the right amount of system power to

handle the authentication sequence. Devices that might have issues with this are wireless IoT devices that run on SoC, SoM or similar architectures.

The RADIUS server should be assessed to measure how many clients and AP's the server can server without the loss of service.

3.4 Security Requirements

The connected networking equipment that transport any part of the authentication process from the AP to the RADIUS service shall propagate the information in a secure manner.

If the connection between the AP that the client original connected too to start the authentication process connects in anyway wireless, then that link must be encrypted via WPA2/3 and AES-CCMP, or with stronger encryption strength and mechanisms. This type of connection can be but not excluding other connection types a mesh connection topology.

3.4.1 Security Requirements for access points

All AP's in the system must comply with:

- 802.11X standard
- WPA2/3
- AES-CCMP
- Open System Authentication (OSA)
- EAPOL
- EAP
- TLS

3.4.2 Security Requirements for RADIUS Services

The RADIUS server must be able to reach the AP's in a safe manner over the network.

The server shall have a set of trusted server certificates that the client's will trust when authenticating against. These certificates should consist of a root Certificate Authority (CA) certificate and intermediate/device CA certificate. For that RADIUS server with a private key to be able to be able to authenticate locally without a ground connection to the issuing root CA.

(Should radius support Called-Station-ID, MAC addresses issue?)

3.4.3 Security Requirements for Certificates

Certificates that are used to authenticate wireless clients shall conform to the X.509 standard.

A certificate revocation list (CRL) shall be present to handle certificates that have been revoked by the organization.

The certificate should be created for each individual in the system, client and server certificates.

(? Key size for the certificates ?)

3.5 System Configuration and Logging

The logging function must be synchronized with the same Simple Network Management Protocol (SNTP) server. To ensure that the logs are kept with the same reference to time.

Logging must contain a minimum information level of:

- Date and Time of log instance
- Unit that triggered the log entry
- Category of log entry
- Source IP
- Description of the log event

4.0 FUNCTIONAL SPECIFICATION

4.1 Communication Flow Overview

The diagram in Appendix B shows the communication flow of the authentication and association from a client via the AP and accounting of a RADIUS server. This flow shall be imposed onto the client to make a successful connection to the network.

4.2 802.11 Open System Authentication

Open System Authentication (OSA) should be used to ensure that the wireless client can open a communication channel to the access point and thus further enable the EAP-TLS security protocols for securing the communication.

4.3 EAP

For key exchange between the wireless client, access point and the RADIUS server should e EAP-TLS described in RFC 5216.

4.3.1 EAP Inner Authentication

The inner authentication mechanism to be used is EAP-MSCHAPv2.

4.3.2 Transport Layer Security (TLS) *(formerly Secure Socket Layer)*

(? What version should be supported, 1.2 or 1.3 and up?)

4.3.2.1 TLS Tunnel Setup

When the tunnels are set up AES encryption with the CCMP cypher is to be used.

4.3.2.2 TLS Encryption Exchange

(? What level of Diffie Hellman should be supported, ephemeral Diffie–Hellman (TLS_DHE) or ephemeral elliptic-curve Diffie–Hellman (TLS_ECDHE)?)

4.4 WPA 2/3

The key enhance shall be handled by the enterprise model of EAP-TLS.

4.4.1 WPA 2/3 Encryption Algorithm

Advanced encryption algorithm (AES) with the counter mode cipher protocol (CCMP) cipher is the shall be used to encrypt the traffic transmitted via the Wi-Fi link.

4.5 Certificate

Certificates that are used should follow the X.509 standard.

4.5.1 Server Certificate Requirements

The server certificate must contain the following:

- Trust the organization’s root CA for client authentication.
- Not fail any of the of the checks made by the certificate store.
- The Subject line of the certificate must match the client name on the client connection.
- The Subject Alternative Name (SubjectAltName) should contain the servers fully qualified domain name (FQDN).
- Match the purposes that the certificate is intended for.
- A date range of when the certificate is valid.

4.5.2 Client Certificate Requirements

The client certificate must contain the following:

- Is issued by an CA that is trusted by the organization.
- A trust relationship with the organization root CA.
- Client Authentication purposes.
- Not fail any of the of the checks made by the certificate store.
- The Subject Alternative Name (SubjectAltName) should contain the user principal name (UPN).
- A date range of when the certificate is valid.

4.5.3 Certificate Revocation List (CRL)

The CRL should contain a reference to all certificates that have been revoked by the organization.

The CRL should update automatically if a connection to the CA has been made. If not the CRL should be update in a timely fashion.

(? What is a timely fashion, time extent needs to be determined ?)

5.0 NETWORK MANAGEMENT

Network management of a secure wireless network defines setup and monitoring of the wireless accesspoints (WAP) and the wireless networks that reside on the WAP.

5.1 WAP Management

Managing WAP's can be done in different ways to ensure that the correct setting and functions of that radio has the intended outcome.

WAP's can be managed in both direct and indirect management via a controller. When a WAP is managed directly the settings will be added to each WAP directly from an management interface. If a WAP is managed indirect via a controller the WAP gets the settings sent to it from the controller and apply them to it's radio.

When configuring a WAP there are several setting that are mandated by law by the govering area that the device is operated in that needs to be addressed prior to activateing the radio. Transmission power or Effective radiated power (EIRP) and the frequeny (channel) that the WAP is transmitting on.

When choosing the EIRP to transmit on the lowest satifacty value should be choosen to manage the distans the WAP in reachable in. The goal is to have an effective communicaton with the clients, and at the same time not broadcast the traffic futher than needed. The second importand aspect is to not pass the allowed maximum EIRP for that frequency and govering area.

Choosing a channel of the secure network relies on three aspets. The first is what the governing body of the area allow to be used per frequency and bandwith. The second aspect is to choose a channel that will give the client the intende function of the network. There is a variant of bands to choose from and dependant on the govering body the there may be more or less channels that can be used to transmit on. The thired aspect is the bandwith of the channel. These three aspects will detrmin the speed and reach of the WAP's capabilities.

In choosing these aspect the consideration should be made to keep the speed at a satisfacoty level and to minimize the reach outside of the intende area of the WAP. Choosing a setting that will transmit father that the need of the WAP will open the WAP up to more unintended interactions with wireless clients outside of the intende function of the network, adding an unessesary attack vector. If the power or quality of transmission becomes to low and traffic is dropped in an ansetifactory way. This due to channel reach due to frequency or bandwith. The experience for the network user will be degraded and unsatisfactory. This also opens up to an attack vector in that is the encrypted channel that is established between the wireless-client and the WAP is broken multiple times the handshaking procedure is done more that what is nessesary and opens up to attack on the key exhcnage and authentication process of the network accosiation.

5.2 Wireless Network Management

Wireless network management defines the networks that are assiosited with a WAP and the transmission channel that the WAP is set up to handle. The management is the handeling of the different segment in the time devision multiplexing (TDM) that the WAP offers. Eahc network will be give a slot to fill within the TDM and the functionality that reside within that slot is what defines the wireless network.

5.2.1 Security Profiles

A security profile is the set of instruction associated with a specific or multiple wireless netowrks residing on an WAP. A profile can be assoisiatd with one or more wireless networks.

A security profile will contain the information nessesary for the wirless network to establish a secure channel to the wireless client.

A security profile will contain infromaiton on what type of cryptography that will be used

5.2.2 Broadcasting

Service Set Identifier (SSID) is a identification marker that will openly identify the human readble name of the network. This marker is sent out by the radio an for a specific wireless network for clients to scan and pick up to associate with that wireless network. If the client has a stored security profile associated with the network it will then try to apply the security and get authenticated.

The option to not bradcast the SSID beacon will not break the function of the network only the direct discoverbility of the network. Indirect discoverbility will still function. Indirect discoverbility is when the client knows the channel and type of authentication method used can authenticate agins the network. When choosing the option to not broadcast a SSID the SSID packet will still be part of the transmission from the WAP, the packet will be designated as a wildcard (i.e. set to null). This means that the WAP will still be visible to a client scanning for networks with tools setup to show networks without SSID's with null values.

5.3 Management channels

When using centralized authentication methods like RADIUS that resides outside of the WAP management channeles are used to communicate that authentication information to and from the radio, as describe in appendix B. Often a secure channel is created to communicate with the authentication server that is separated from the main channel of communication the wireless network. This can be done via pysicla separated networks or with VLAN's if the same wired medium is used to transport both the main network traffic and the authentication transaction. It is recommended the the authentication ransaction resides on the sepate channel than the main tranffic resides on.

5.4 Certificate Management

Certificate management is how the certificate and ciertificate chain is setup to handle the needs of both the wireless clients and the infrastructure distribution and control of certificates.

5.4.1 Certificate Properties

A certificate contais a number of property the make up the certificate and the intended use of the sertificate. These properties give the certificate the ability preforme different functions and can pose more or less of a security risk if displaced (lost or stolen). A certificate is part of a PKI that will esure the chain of trus and the ability to authetica a client and a wireless network with an authentication server. When creating a certificate chain for authentication the chain starts with a root certificate and from the certificate the intermediate and device certificate.

A certifatce can be associated with a device or used in a generic manner. When issuing certifiacets that a generic the certificate revocation list (CRL) will not work n a granular manner.

In the list below is a typical setup for a X509v3 certifiacte with the properties is normaly used with a certificate for authentication in a wireless network enviorment.

- Certificate properties structure
  - Version Number
  - Serial Number
  - Signature Algorithm ID
  - Issuer Name
  - Validity period
    - Not Before
    - Not After
  - Subject name
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
  - Certificate Signature Algorithm
  - Certificate Signature

5.4.2 Certificate Extensions

Certificate extensions will determin the functionality that the certificate can be used in. It is there for a good practice to only use the extastion that are need for that type of a certificate for that purpose.

Certifiacte extenstion can be but not limited to.

- Digital signature
- Non-repudiation
- Key encipherment
- Data encipherment
- Key agreement
- Certificate signing
- CRL signing
- Encipher only
- Decipher only

5.4.2.1 Key Usage

- Sign (downloadable) executable code
- IPSEC End System
- IPSEC Tunnel
- IPSEC User
- Timestamping
- SSL Client
- SSL Server
- Certificate Signing
- Object Signing
- S/MIME Signing
- S/MIME Encryption

TBD, what is the recommendation.

5.4.3 CRL's

The function of the CRL is to hold a list of either revoked or valid packets, black/white listing. The CRL is compiled from the revocationlist of the certificate authority and transported out to the authenticating server.

Blacklisting is the function of adding certifiactes that are no longer valid and allowed to authenticate. Whitelisting is the oopsit of that function and list only the certificates that are valid and able to atuthenticate.

Its is recommended that the CRL is automatically updated in a timely manner.

Use of Fragmented CRL's TDB

5.5 Controls

TDB

5.5.1 Monitoring

TDB

5.5.2 Abnomoly/Threat detection

TDB

6.0 CONFIGURATION MANAGEMENT

ATTACHMENT 1 ACRONYM LIST

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AID	Aircraft Integrated Data
AIS	Aircraft Information Services
AP	Access Point
CA	Certificate Authority
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CRL	Certificate Revocation List
EAP/TLS	Extensible Authentication Protocol/Transport Layer Security
FQDN	Fully Qualified Domain Name
NSS	Network Server System
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security (formerly Secure Socket Layer
WLAN	Wireless LAN

APPENDIX B
COMMUNICATION FLOW DIAGRAM

APPENDIX A CONFIGURATION EXAMPLES

TBD (When the parameters above in function description is set)

APPENDIX A
CONFIGURATION EXAMPLES

APPENDIX B COMMUNICATION FLOW DIAGRAM