`

1.0 SECURITY

1.1 Introduction

This section should not supersede the overall ICAO security definition for IPS. Security in this standard should be for avionics implementation only.

Objective: for implementers, being able to integrate IPS security needs in their system architecture security definition.

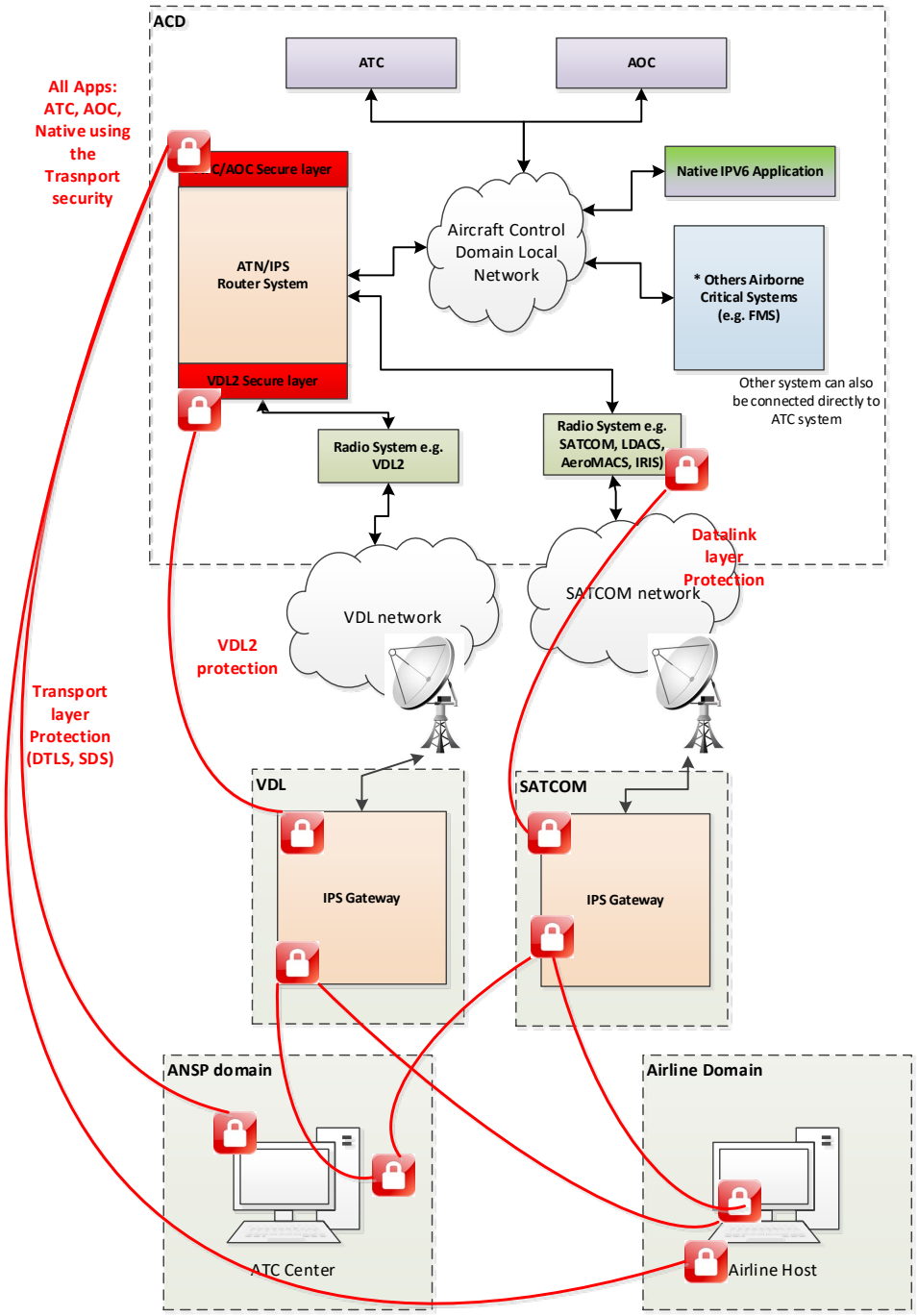
1.2 Security scope

The asset considered here is the ATN/IPS router system.

This standard describes the security measures for the Core IPS only for the avionics systems only. Other security measures hosted by the other avionics system could be given for information.

The following figure shows an overview of IPS system in a global architecture.

4.0. SECURITY



In the global architecture the IPS system is the entry point of the Aircraft. IPS System provides the data from the external origin to the Aircraft Control Domain and other sub-systems. The IPS system accesses various external entities via multiple air-ground links. Data from the various air-ground links possibly directly connected

to the IPS Systems or may flow to IPS system via intermediator system such as aircraft local network. In this case, IPS system cannot support itself for all of the security objectives.

Moreover, legacy systems like ACARS router are not considered in this standard.

1.3 Environment

The radio interfaces and the ground interfaces are considered as threat sources. In this case, attacker from these interfaces can spoof, tamper, disclose information, deny of service and elevate privileges.

The attacks from AISD domain are not considered in this secure environment as the connection with the AISD is related to the specific airframe architecture.

1.4 Security development

The IPS system shall be developed according to ED-202A/DO-326A (AIRWORTHINESS SECURITY PROCESS SPECIFICATION) document.

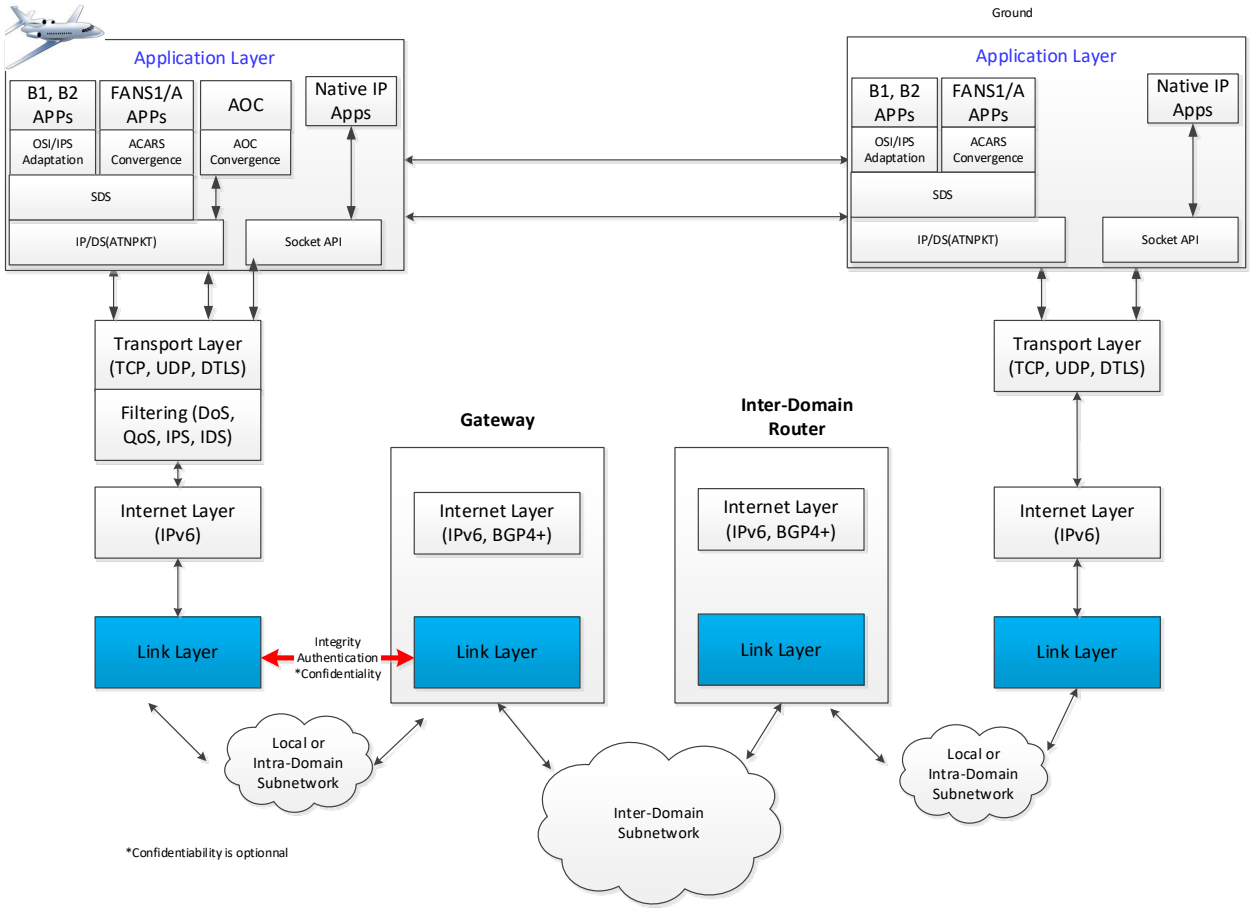
This process adds data requirements and compliance objectives, as organized by generic activities for system development and certification, to handle the threat of unauthorized interaction to system safety and is intended to be used in conjunction with other applicable guidance material, including ED-79A / SAE ARP4754A, ED-135/ SAE ARP4761, ED-12C / DO-178C, and ED-80 / DO-254 and related to the EASA and FAA certification advisory materials.

1.5 Security functions

1.5.1 Air-Ground Datalink (layer 1-2)

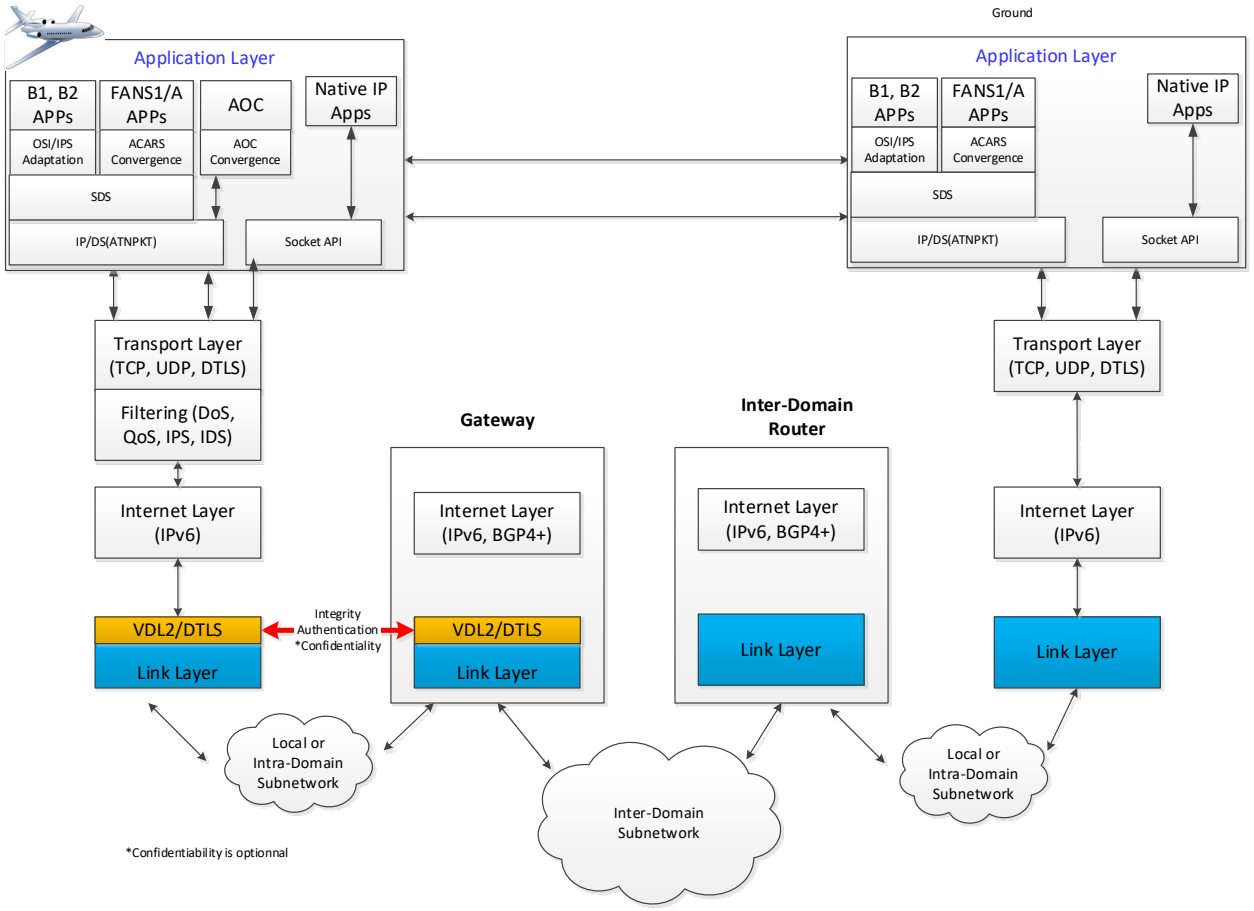
As the radio system is the entry point to the local airborne network, a secure channel between the airborne radio systems and the radio access endpoint on ground will be integrated in order to ensure the authentication and integrity of exchange at datalink level and enforce the defense in depth.

4.0. SECURITY



These security features are part of existing data link architectures. For VDL, the IPS system architecture will implement directly a DTLS security layer to secure the exchange between the airborne and ground radio system.

4.0 SECURITY



1.5.1.1 Datalink Redundancy

The IPS system shall manage multi-link in order to ensure the availability of the connection to the ground. This is done so to provide better availability and enhance the communication link quality. The IPS system will have the capabilities to switch to another link (VDL2, SATCOM, LDACS …) in case of service loss or degradation of the link. Secure communications entails both encryption of data and authentication of users to the network. The communication services must be available for legitimate aircraft to access at any time.

On the airborne, IP version 6 network will manage and utilize the multiple air-ground links to send and receive an application data. As single application data traverse via multiple links and access ground network, protecting application data from modification, deletion, and/or injection is necessary.

Adversary may able to configure via metasploit to randomly compromise the ground nodes or stations for launching a class of false data injection attack. These attacks may result in the failure of the core network infrastructure components or control and management planes data that can be misleading the essential information, such as available bandwidth information and packet routing information.

4.0. SECURITY

In the IPS system, once ground stations or any entity in networks are compromised, the adversaries could easily manipulate any sensitive information result in adverse impacts on safety and regularity of flights or compromise of airline time and mission sensitive information. To protect the transit data, IPS system should provide the mechanism to protect data. DTLS in transport layer should be utilize to provide the protection. DTLS supports peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

1.5.2 Air-Ground Transport level (layer 3-4)

In order to limit the threat exposure from an attacker on ground network that could exploit vulnerabilities of IPS system, security needs to be applied at the air-ground transport level. Moreover, security at the transport layer could will provide flexibility in several domains as:

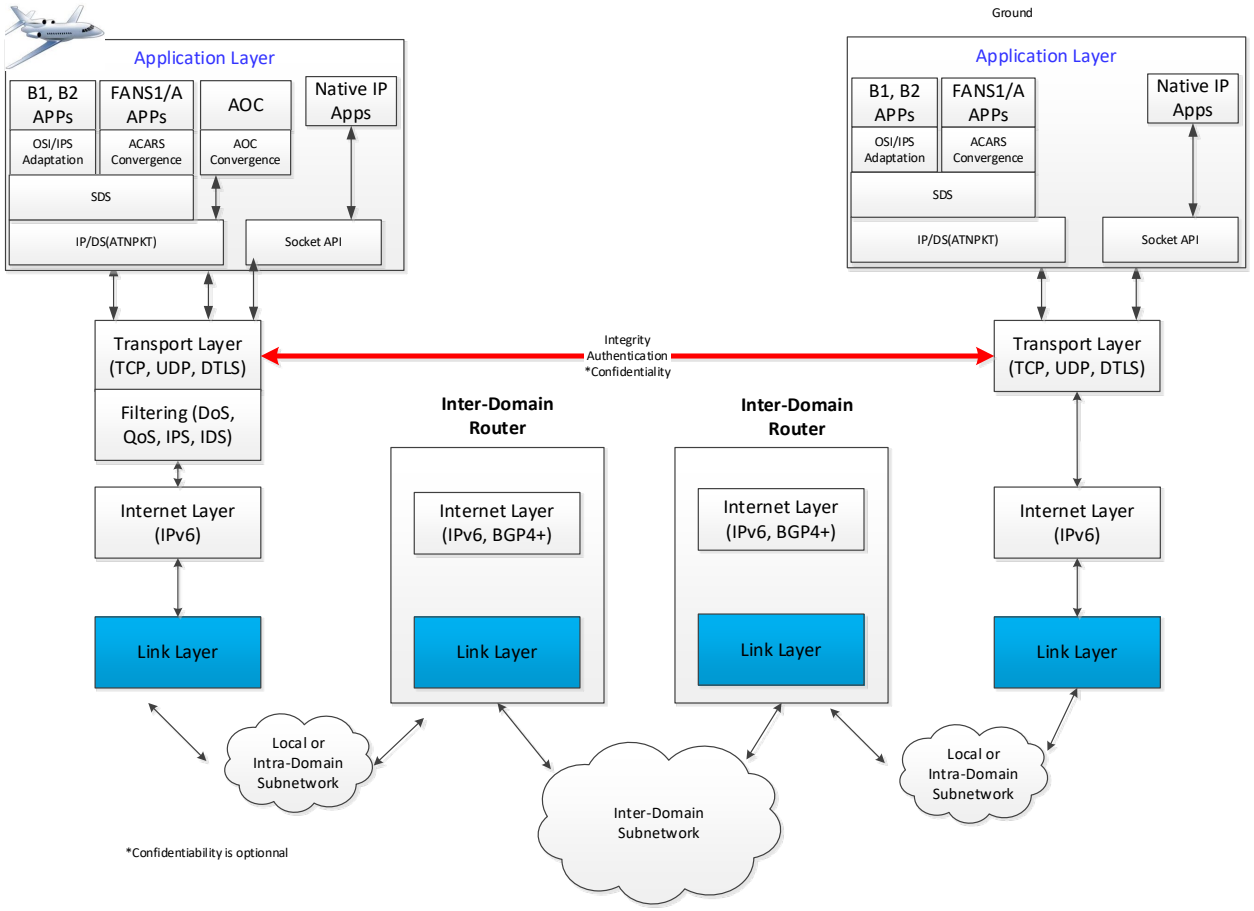
- Security layer for future native IP application.
- Security layer for cryptographic key management (Certificates, credentials … etc)
- Security layer for ATC and AOC applications
- Authentication to ground mobility service

Security provide the means and protocol establishing mutual authentication between aircraft and ground at the beginning of the session and negotiation of cryptographic keys to be used during the session. This will provide the mechanism that can be used in protecting data flows between a pair of aircraft and ground entity.

The IPS system shall authenticate traffic from Airline domain and ANSP domain using state of the art cryptographic algorithms associated to protocol at layer 3-4.

The IPS system shall ensure the integrity and confidentiality for traffic from Airline domain and ANSP domain using state of the art cryptographic algorithms associated to protocol at layer 3-4.

4.0 SECURITY



The IPS system should implement the capability to disable the payload encryption during flight. (E.g. disable encryption according to aircraft positioning)

1.5.2.1 DTLS implementation

1.5.2.1.1 Session management

There are two modes to consider for the protocol build-up as related to security:

- Session establishment message exchange
- Session management message exchange
- Application message exchange

We have to consider several kind of sessions:

- DTLS session between aircraft and peer to ensure the authentication and integrity of ATC traffic flow.
- DTLS session between aircraft and peer to ensure authentication, integrity and confidentiality of AOC traffic flow.
- DTLS session between aircraft and peer to ensure protocol convergence like ACARS to IPS …

**********TBD**********

1.5.2.1.2 Authentication

The first step for an IPS aircraft communicating with any entity is to authenticate with the IPS peer entity. Authentication is initiated by the aircraft. . DTLS will be implemented for authentication in order to protect the subnetwork that is being used.

The exchanging of PKI keys in DER format while efficient, will likely lead to multiple fragments to be transmitted across the communications media, especially when the media has a small MTU size.

1.5.2.1.2.1 IP Based Authentication

IP based communication media is assumed to have a media layer securing method. For this reason and for consistency with all other IPS traffic, DTLS will be transmitted on IP based media to secure Layer 3.

The transmission of DTLS in IP packet for authentication is illustrated in the following diagram and is detailed further in this document.

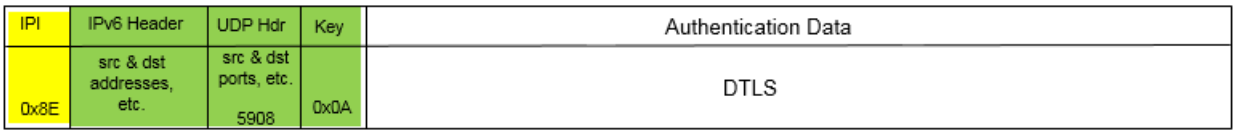


Figure 5-1 – Authentication packet on IP based media

The IPS peer entity will not have any UDP ports other than 5908 with a key tag of 0x0A available for unauthenticated aircraft over IP based media.

All messages in the authentication sequence will have UDP port 5908 and the first byte of the UDP data field will have a key tag value of 0x0A preceding the authentication data. During authentication, the IP packet carries the DTLS data in the user data. After the DTLS Logon handshaking is complete the avionics will send

a Post Authentication Message with the aircraft's IP address, tail number and Flight ID and a random sequence number. The peer gateway will respond with a random sequence number. After authentication has been completed, anything on port 5908 with a key tag of 0x0A will be TLS Alert messages.

1.5.2.1.2.2 Post Authentication Message

In order to provide IPS with enough random values to ensure data integrity and to allow IPS to ATN/OSI and ACARS translations additional pieces of information must be exchanged between the aircraft and the peer entity. This additional information is carried in the post-authentication message, the content is shown below.

Field Name	Length in Bytes	Reason for exchange
Aircraft Fixed Nomadic IP Address	16 Bytes length of an IPv6 address	Peer entity needs IPv6 address to exchange IPS information. This is especially true when logon is via AVLC.
Aircraft ATN/OSI Address	20 Bytes	Gateway needs this for ATN translation
Length in Bytes	1 Byte	Contains the Tail number length (1st nibble) and Flight ID length (2nd nibble), both can be variable. This allows for 0 to 15 characters in both
Tail Number	Variable – but must match the tail # length value in the Length in Bytes field (1st nibble)	Tail numbers are needed for ACARS conversions.
Flight ID	Variable – but must match the flight ID length value in the Length in Bytes field (2nd nibble)	Flight ID is required for ACARS Conversions.
Random Message number for downlinks	6 Bytes	Random message number for MIC generation. The value will be the sequence value for this message. Each additional transmitted message from this point will increment the value by 1. Value rolls over when necessary from 0xFF FF FF FF FF FF to 0x00 00 00 00 00 00.

1.5.2.2 DTLS Login

DTLS is an enhancement on TLS for secure UDP connections. The DTLS Protocol is recorded in RFC 6347.

There are 6 flights to a DTLS login, shown below.

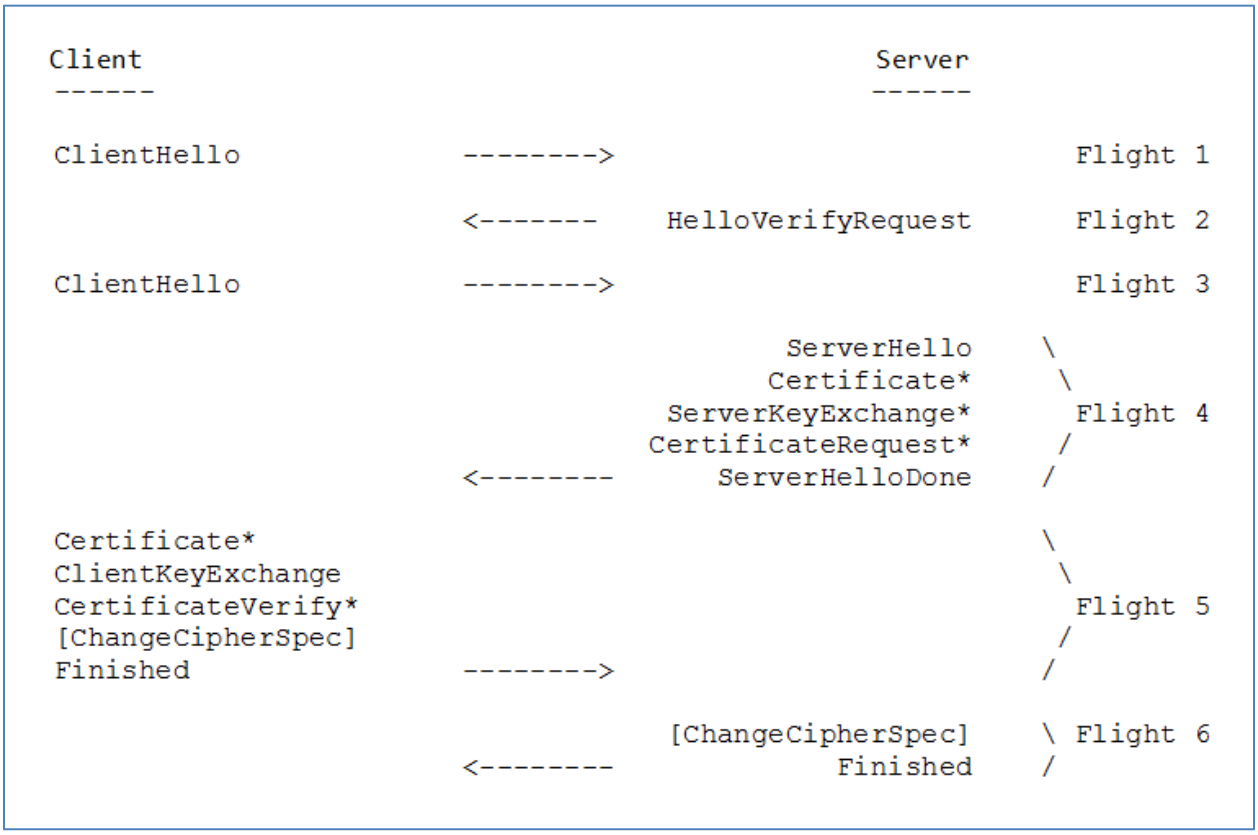


Figure 5-2 – DTLS Login Flights

During the initial rollout of IPS the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, and TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 methods will be used. SHA256 is intended for legacy systems while SHA384 will be the main requirement. To facilitate maximizing the utilization of packets, the Deflate compression option already built into DTLS will be used.

Field	Value
Keys	ECDSA
Diffie Hellman	ECDHE
Elliptic Curve	secp256r1, secp384r1
Encryption	AES 128 GCM, AES 256 GCM
Hash	SHA 256 or SHA 384
Compression	Deflate

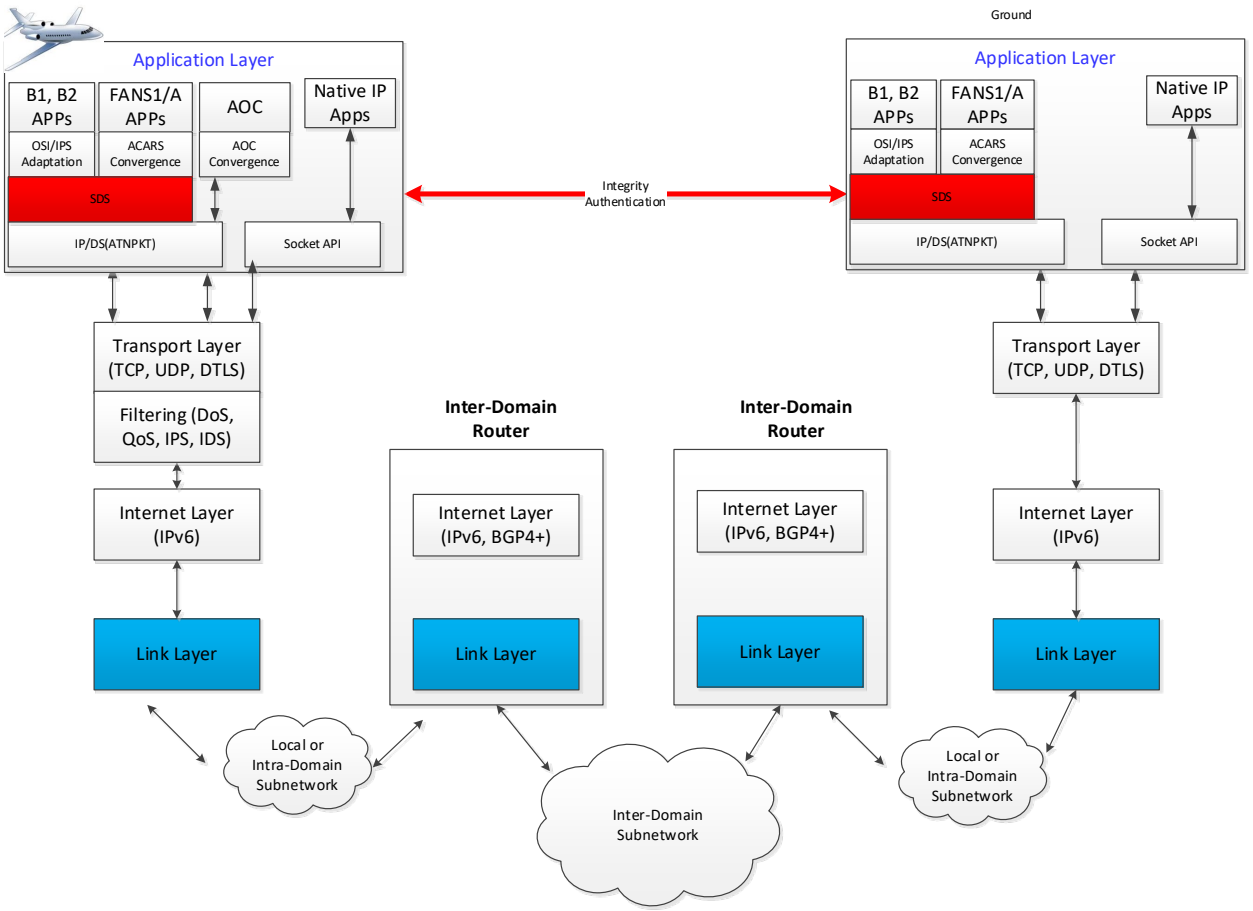
Table 5-1 – DTLS Session Parameters

1.5.2.3 Air-Ground Application Layer Security.

The IPS system shall implement security for ATC and AOC application to ensure Integrity and Confidentiality (optional) services

These security features could be provided by the following solutions:

The IPS system could implement application layer security. This security provision should supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. Multiple options are available, .

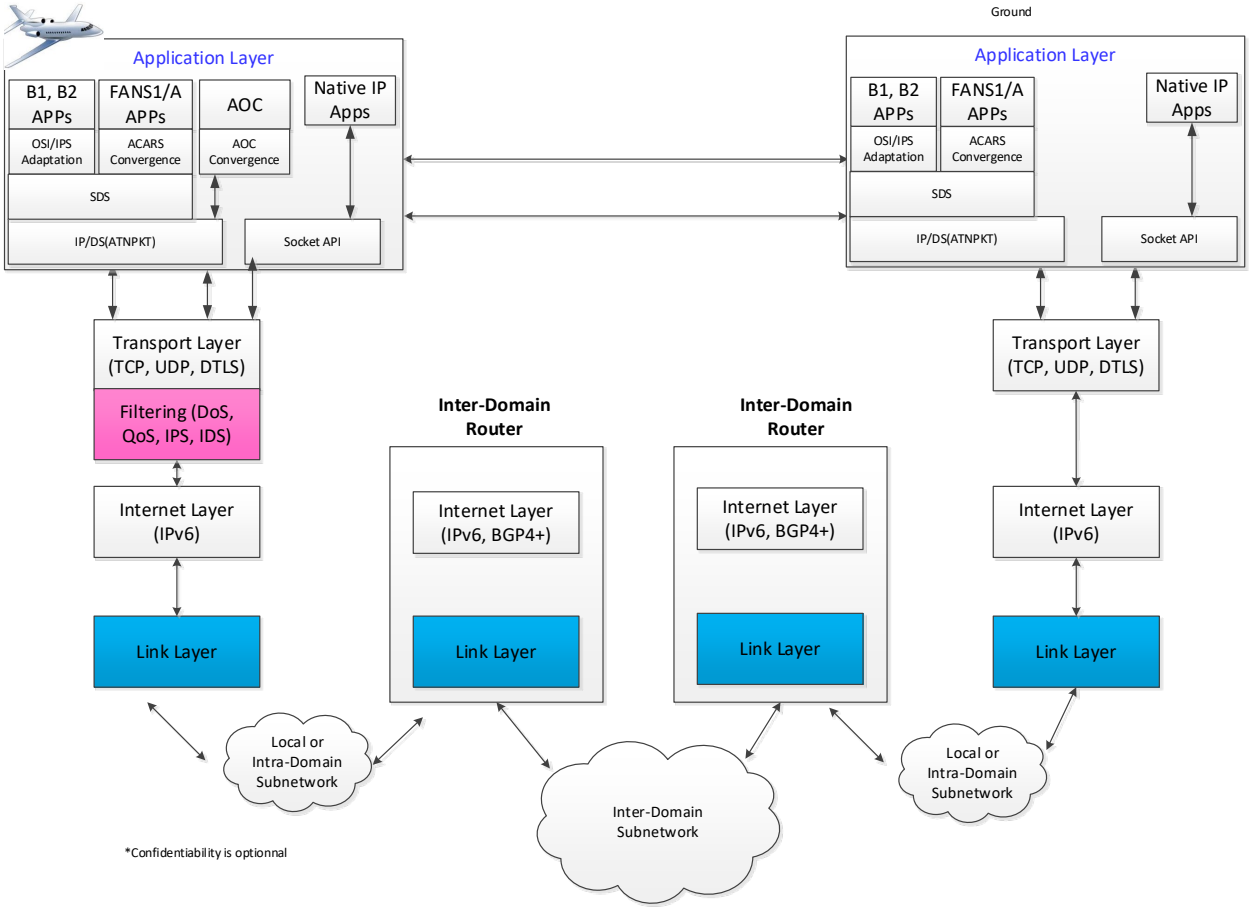


However, these features could be provided by DTLS protocol, this solution allow to implement security for both application (ATC and AOC) without AOC application

modification. The payload encryption will be enable or not in the DTLS session using null encryption service.

1.5.3 Filtering

The IPS system should allow only traffic authorized to reduce threat exposure from ground.



An anti-flooding function could be implemented in IPS system to detect and remediate flooding attack in order to maintain service for critical safety exchange like flight clearances and trajectory information.

The IPS system should implement IP-based filtering to allow only traffic from/to authorized domain.

As datalink communications are driven by standards that mandate specific application functions over specific packet format certified for operation in different safety-domain networks the IPS system should integrate advanced filtering function to inspect and authorize only datalink exchange that respect standard like:

- Aircraft Communications Addressing and Reporting System (ACARS) with ACARS core messaging is defined in ARINC 620 (ARINC, 2014) and ARINC 623 (ARINC, 2005) specifies character-oriented Messages and services such as (D-ATIS, TWIP, METAR, OCL and DCL etc..)
- Future Air Navigation System (FANS) 1/A+ services standardized by ARINC 622-4 (ARINC, 2001) also use ARINC 620 core messaging,
- Aeronautical Telecommunication Network (ATN), B1 or B2, standardized by. ICAO Doc 9880 (ICAO, 2014), ED-110b, DO-250A/ED-228A. PM-CPDLC, CM, ADS-C applications are defined in this standards.
- Some of the application defined in the SC-206 /WG-76 such FIS (D-RVR, D-VOLMAT, D-OTIS etc…) is also used the IPS and needs to include in the filtering.

1.5.4 Monitoring

The IPS system should implement monitoring function to ensure that the router continues to be secure. Security notification and security logging of event should be part of the monitoring.

In accordance with the guidance provided by AC 25.1322-1 the flight crew should be alerted by a security notification in case of security event in the IPS system cause a safety effect on the aircraft.

The IPS system shall implement logging function to generate security event in order to provide information for security incident management.

The security logging is not a preventive security measure. Security logging is only for detective electronic interaction in the frame of forensic analysis

The format of the security logs may comply with section 3 of the ARINC 852 [x] standard.

The IPS system shall securely store the logs (Access control, integrity control).

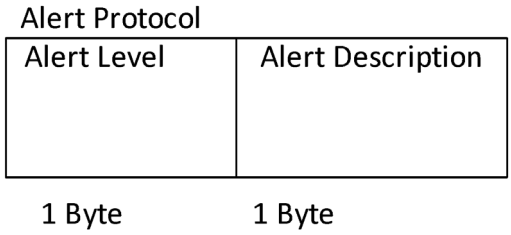
The IPS system shall integrate an export log function to transmit event on ground for live management

1.5.4.1 DTLS Error Detection

1.5.4.1.1 IPS peer entity DTLS/TLS Alert Messages (port 5908 key tag 0x0A)

The IPS peer entity will send DTLS/TLS Alert Messages to indicate warnings, and fatal errors during the authentication process (port 5098 key tag 0x0A) for IP based media. Key tag 0x0A for AVLC based media. Aircraft should be able to receive these messages without negative consequences. While it is desirable that the

aircraft use these messages to guide the authentication and connection processes, each avionics manufacturer may develop their own methodology. Alert messages will only be sent for messages that header information is intact; otherwise messages busted in RF will be ignored. The Alert Protocol Message shall be the same as recorded in RFC 5246 and takes the form:



Alert messages will take the form of Warning and Fatal errors. Warnings can be ignored however it would be useful to log or present the error to the operator. While the IPS Peer entity will be able to handle all alert types, the following alert types would be useful to the avionics.

Alert Levels can be one of:

Alert Level	Example	Meaning
Warning	0x01	This is an informational message, and should probably be logged.
Fatal	0x02	There has been an unrecoverable error with the login. Details in Description.

Table 5-2 - DTLS Alert Levels

Useful Alert Descriptions can be

Alert Description	Example	Meaning
close_notify	0x00	The aircraft or IPS Peer entity would like to close the connection. The IPS Peer entity may send this when the session has been open for 8 hours and requires renegotiation. This may also

		be sent after key management commands.
handshake_failure	0x40	A general error with the negotiation. Usually fatal and requires a new handshake.
Unsupported_certificate	0x43	The certificate presented is not authorized for use on the ground network for this provider. Fatal message.

Table 5-3 - DTLS Useful Alert Messages

The following alerts will all be Fatal, however they will never be transmitted to the aircraft. The IPS peer entity log will record the fatal message and associated certificates presented that generated the alerts, as well as any relevant information regarding the failure. Silently recording these fatal messages will prevent Denial of Service attacks against the local provider's network or the avionics.

Alert Description	Example	Meaning
Certificate_revoked	0x44	The certificate presented exists on a certificate revocation list. Fatal message.
Certificate_expired	0x45	The certificate presented validity dates are outside of the current date. (Either used before validity or after validity). Fatal message.
Unknown CA	0x48	The certificate presented is signed by a CA that is not recognized by this service provider. Fatal message.

Table 5-4 - DTLS Log only alerts

* If aircraft tries more than 3 times the revoked certificate, then the aircraft should be added to the revoked client list until human interaction can be established.

1.5.4.1.2 IPS Peer entity TLS/DTLS Message Alert Messages (non-authentication)

Some TLS Alert Messages may be generated after the authentication process. The alert protocol is the same as described above, using port 5098 key tag of 0x0A. The following are the anticipated alerts.

Alert Description	Example	Meaning
bad_record_mac	0x20	Message received did not pass the message integrity check. This is often a warning message.
decompression_failure	0x30	Message received could not be decompressed. This is often a warning message.

Table 5-5 – IPS Peer entity Alert Messages (non-authentication)

1.5.5 Cryptographic Key Management

The IPS system implements a secured automated mechanism for certificate management operability and maintainability.

The IPS system should embed crypto engine for keying generation

The IPS system should provide entropy for keying generation.

The IPS system should protect stronger the private Key (Private Key not exportable).

The IPS system should manage the request to the CA (Certificate Signing Request) it public certificate and CA public Certificate.

The IPS system should renew automatically at defining period the keying (e.g. 2 months before keys expiration)

The IPS system should manage the request to Certification Revocation List server.

1.5.5.1 Key description

1.5.5.1.1 ECDSA Keys

Each aircraft will receive public certificates and private keys. The public certificate is used for authentication with the IPS Peer entity(s) and the private key is kept secret with the aircraft. Each undoes the encryption of the other and must work in pairs to establish and maintain secured connections.

To minimize the size of the public keys, they will be encoded in X.509 certificate DER format. The private keys are never transmitted in an authentication exchange. Each key's valid dates will correspond with existing contract dates plus a grace period if applicable between the airline and the primary service provider.

In the event that an aircraft key is compromised, the aircraft will have a one-time-use back-up key that can be used for authentication. This back-up key will only be valid on the primary service provider's network to facilitate upload of replacement keys. After using a back-up certificate, if new keys are not uploaded the airline must data-load new certificates and keys. The Avionics will support a way to replace the existing public keys and certificates using both a physical media and also over the air

1.5.5.1.2 X.509 Certificate Parameters for aircraft

Each X.509 certificate has parameters that identify the valid user of the certificate. Certificates will include the aircraft's public key, a signed hash using the service provider's private key, and the following additional information.

Field	Value	Example Using Delta Airlines with tail N123456 and Rockwell Collins ARINC North America
Country Name [AU]:	2 letter country code of airline host	US
State or Province Name	Full Province or state name of airline host	Georgia
Locality Name	City of airline host	Atlanta
Organization Name	issuing airline	Delta Airlines
Organizational Unit Name	ICAO Airline Designator	DAL
Common Name	Tail Number.aircraft Type.ICAO_Code.Service	N12345.A380.DAL.IPS
Email Address []:	PKI Sponsor E-mail	PKI@delta.com
A challenge password []:		[None]
An optional company name		[None]
Issuer	Service providers information	Rockwell Collins ARINC NA
Validity	Dates and time period key is valid	[Contract specific]

Table 5-6 – X.509 Certificate Parameters for Aircraft

1.5.5.2 X.509 Certificate Parameters for non-aircraft

Maintenance devices may require certificates, which give permission for the generation of Certificate Signing Requests (CSR) for a particular airline and primary service provider. Having Certificates on the maintenance device(s) would allow that device to make CSRs for one particular airline, and service provider. Devices could then be kept secured to ensure that only authorized people and avionics receive

valid certificates thus preventing unauthorized people from installing billable certificates on unauthorized avionics. The Certificate Policy and Certificate Practice Statement will expand on this concept further.

1.5.5.3 X.509 Certificate List

It shall be the responsibility of each service provider or designate to maintain a service key directory of X.509 certificates for all aircraft for which they are the primary service provider. It also shall be the responsibility of each primary service provider to maintain a valid public CA X.509 certificate in DER encoding with all other trusted companion service providers for which a trusted relationship is established.

1.5.5.4 Service Provider Trusted Relationships

Each service provider shall have the option to enter into roaming agreements with other service providers. These trusted roaming providers shall be called trusted companion service providers. If a companion service provider has a valid trust operating agreement then an exchange of public root CA certificates between providers or the establishing of a trust bridge will allow aircraft to utilize the companion network while in transit. Certificates shall be encoded in DER format.

1.5.5.4.1 Aircraft Roaming and Keys

It is up to each airline to determine which service providers they wish to allow their aircraft to connect with if any. This is bounded by the trust relationships between service providers. If a set of trusted service providers are desired, the aircraft avionics should be loaded with server certificates for each trusted service provider. The aircraft will then be able to authenticate the IPS Peer entity and the IPS Peer entity will be able to authenticate the aircraft.

By way of example if ADCC and SITA enter into a trusted relationship: Aircraft that have ADCC as their primary service provider will have the option to roam onto the SITA network, if the aircraft is equipped with SITA's gateway server certificate. Without this trusted relationship then aircraft will not be able to roam onto the other's network even if the avionics contained the SITA certificate. In this case the SITA IPS Gateway would reject aircraft presenting a certificate signed by ADCC.

Avionics should disable IPS if they do not at a minimum have an Aircraft Public Certificate, Aircraft Private Key, Primary Service Provider's Public Server Certificate and a Primary Service Provider's CA Certificate(s). Having a Onetime Use key and certificate is highly encouraged to recover aircraft whose keys expired while out of the primary service provider's area.

Assuming the aircraft is roaming onto another service provider's network area. The following truth table depicts whether the aircraft will accept or reject the Trusted Companion service provider's server key.

Service Provider Key store / Aircraft key store	Has Trusted Companion Public Certificate	Does not Have Trusted Companion Public Certificate for Aircraft's Primary Service Provider.
Has Secondary Service Provider Server Key	Server Key accepted – Logon continues	Ground issues a DTLS Alert message and discontinues the connection.
Does not have new Service Provider's server Key	Aircraft discontinues communication with this service provider. Aircraft may issue a DTLS Alert message	Ground issues a DTLS Alert message and discontinues the connection.

Figure 5-3 - Avionics Login Results Table (Trusted Service Provider)

Service Provider Key store / Aircraft key store	Has Primary Service Provider Server Public Certificate
Has primary service provider Server Key	Server Key accepted – Logon continues
Does not have primary service provider's server key	Misconfigured Aircraft cannot authenticate with Primary Service Provider

Figure 5-4 - Truth Table Logon Results (Primary Service Provider)

1.5.5.5 Certificate Revocation List (CRL)

Each primary service provider shall maintain a certificate revocation list. Any key generated by the primary service provider that is later compromised, other than by expiration shall be listed in a certificate revocation list until the certificate expires. This list is to be shared no less than daily with all trusted companion service providers, even if no changes are recorded. It is recommended that an encrypted method be established for sharing these lists.

One time use keys may be distributed to trusted companion service providers as a Certificate Revocation list as well. See Section 5.5.3.5 on one-time use keys for more information.

Online Certificate Status protocol is recommended between trusted service companions but not required. It will be up to each service provider to setup how it wants to interact with other trusted service providers. OSCP availability does not alleviate the need to publish CRLs to trusted companion service providers. OSCP is seen as a useful resource but not impervious to outages due to network connectivity issues and server hardware failures.

1.5.5.6 Diffie-Hellman

The Elliptic Curve Diffie-Hellman Ephemeral key generation function allows for dynamic negotiation of Diffie-Hellman parameters at the time of authentication. Diffie-Hellman is a secured key generation scheme that allows each participant in a communication channel to generate the same master secret key without sending the actual key over an insecure link. This is done by exchanging a Pre-Master secret key that will guide the other participant in the communication channel to calculate a Master-Secret Key. The Elliptic Curve Diffie-Hellman Ephemeral key (ECDHE) is generated along the Elliptic curve specified during the DTLS authentication. For a more in-depth discussion on the protocol please reference RFC-4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).

1.5.5.7 Elliptic Curves

To simplify the authentication exchange and session key generation a named pre-configured elliptic curve generally accepted by the security community will be used. The curves supported will be secp256r1 (for legacy systems) and secp384r1 (the primary requirement).

1.5.5.8 Encryption

AES 256 or AES 128 both with GCM mode will be used for encrypting all message traffic on UDP port 5908 after authentication is complete and during any key or session maintenance operations. All other traffic on this and all other ports will be sent unencrypted; however a Message Integrity Code (MIC) will be generated to ensure the message was not tampered with while in transit.

1.5.5.9 Hash

Initially the hashing function shall be the same for the MIC as that used on the client's/aircraft's ECDSA Keys. The Hashing function for MIC generation will be negotiated during the authentication process. SHA 384 hashing algorithm recommended for MIC generation, with SHA 256 available for legacy aircraft. All but the last 4 Bytes will be truncated to minimize the length of the hash while maintaining the security value.

1.5.5.10 Key Management

All Crypto methods have a limited useful life time, the crypto period. It is the time from when they are derived to the point at which computing power becomes sufficient enough to brute force guess the private key in a reasonable amount of time, or a flaw is exposed in the key generation method.

In order to ensure that aircraft can initiate an IPS connection with any trusted provider, keys will need to be managed.

1.5.5.10.1 Key Management Functions

To facilitate the exchange and security of keys with an aircraft the following port 5908 key tag selectors have been defined for key management. All key tag values of 0x3X will use the encrypted connection negotiated upon DTLS logon.

Key Tag	Meaning
0x30	Upload a new Root CA Certificate
0x31	Upload a new Aircraft Private key
0x32	Upload a new Aircraft one time use Private Key
0x33	Upload a new Aircraft Certificate
0x34	Upload a new Aircraft one time use Certificate
0x35	Upload the primary service provider's certificate
0x36	Upload a secondary service provider's certificate
0x37	Change IP address to:
0x38	Reserved - Encrypted
0x39	Reserved - Encrypted
0x3A	Reserved - Encrypted
0x3B	Reserved - Encrypted
0x3C	Reserved - Encrypted
0x3D	Reserved - Encrypted
0x3E	Reserved - Encrypted
0x3F	Reserved - Encrypted

Table 5-7 - Key Management Key Tags

1.5.5.10.2 Initial Key installation

Upon manufacture completion, the avionics manufacturer will preload all root certificates for all valid service providers. The Avionics manufacturer will also upon sale load the primary service provider server certificate and work with the primary service provider to install aircraft specific certificates and keys for IPS operation.

The IP address shall also be set by the avionic provider at the direction of the primary service provider. The airline may also request the installation of other trusted companion service providers server keys to allow roaming.

Failing pre-load by the avionics manufacturer or during subsequent lease or sale of an aircraft, it is recommended that avionics have a physical way, to load certificates, IP address configs and keys for IPS. It is recommended that avionics manufactures standardize the process for physical media and configuration files. The physical loading of keys should always be available. It will allow airline to recover aircraft that have been compromised or if keys expired before returning to the primary service provider's coverage area.

The Airline can request a new set of certificates (Primary Service Provider Server, Aircraft Cert, Aircraft Private key, one time use cert, one time use private key) from the primary service provider, or a new primary service provider at any time via the processes documented in the master certificate policy and service contract. If there is a change in primary service provider the keys must be loaded manually via ground maintenance device. The airline is responsible for maintaining the security of the maintenance device(s) after issue. Compromised keys shall be reported to the primary service provider as soon as possible.

1.5.5.10.3 Subsequent Key installation

Once Avionics are initially loaded with an IP, Certificates and keys, further management can be done via the primary service provider's communication network, as long as the primary service provider remains unchanged. If a change in primary service provider is required, physical configuration of the avionics will be necessary.

1.5.5.10.3.1 Upload a new Root CA Certificate 0x30

Avionics will be expected to maintain a list of Root CA certificates (the root CA Store) to validate provider certificates. It will be the responsibility of the airline to keep this store up to date. The primary service provider can upload new Root CA certificates as provided by airline host and trusted companion service providers. The UDP port 5908 with key tag of 0x3X will use encryption negotiated upon DTLS logon.

Root CA certificates are trust anchor points. Compromise of a trust anchor has significant financial and legal implications. The service provider should not initiate a RootCA Upload for foreign root certificates without appropriate signed permission and certification that the digital certificates are authentic, genuine and that the airline wants to be able to roam onto that network. The Primary Service Provider may upload updates to its own root certificate at any time, as long as it remains the primary service provider.

Avionics upon receiving a Root CA Certificate will update the root CA store with the incoming certificate. Only one Root CA certificate will be uploaded per instance. It is expected that avionics will replace any root CA certificate previously existing in the Root CA store issued by the same authority with that received. For example a Symantec root certificate with another Symantec root certificate. The avionics should maintain its own Root CA certificate store and remove any expired Root CA Certificates periodically. Uploaded certificates will be in DER format.

Only the primary service provider will be allowed to upload new Root CA certificates over the network.

Aircraft should maintain their DTLS connection with the primary service provider after installing a new Root CA certificate. Upon any new login or refreshing of the connection the current Root CA certificate store will be used to validate any service provider's authentication certificate(s). The port 5908 key tag for uploading a new Root Certificate will be 0x30, and will be followed by certificate (upload) or one additional byte (response).

Service Provider Sends	Aircraft Sends	Meaning
Root Certificate	0x00	Certificate accepted and installed.
Root Certificate	0x01	Certificate rejected. – Already have this certificate, invalid, expired, or otherwise.

Table 5-8 - Upload new Root CA Certificate Return Codes

Only one root certificate should be maintained on the aircraft per CA. Note, it is quite possible for two different service providers to use the same CA. If a new root certificate is loaded, then any previous root certificate for that same CA should be removed and replaced with the incoming root certificate. The return code will remain the same. More information will be included in the primary service provider's Certificate Practice Statement and Certificate Policy as well as the individual customer contract.

1.5.5.10.3.2 Upload a new Aircraft Private Key 0x31

In the event that the private key expires due to crypto period lifetime or becomes compromised via other means, the service provider can upload a new Private Key via the encrypted connection, using a port 5908 key tag of 0x31. It is expected that the primary service provider or airline would change the private key, and public certificate. The IP address and Primary Service Provider's key can be changed as well if necessary.

Aircraft should maintain their DTLS connection with the service provider after installing a new private key. Upon any new login or refreshing of the connection the new private key will be used, until that time the old private key should be used. The Upload a new Aircraft Private Key will have a port 5908 key tag of 0x31, and be followed by the private key (upload) or one additional byte (response).

Service Provider Sends	Aircraft Responds	Meaning
Aircraft Private Key	0x00	New Private Key accepted and installed
Aircraft Private Key	0x01	New Private Key rejected.

Table 5-9 - Upload new Aircraft Private Key return codes

1.5.5.10.3.3 Upload a new Aircraft one time use Private Key 0x32

In the event that the onetime use key expires due to crypto period lifetime, becomes compromised via other means, or is used, the service provider can upload a new one time use private key via the encrypted connection, using port 5908 key tag 0x32. It is expected that the service provider would change the onetime use private key, and one time use public Certificate in the same DTLS session. The IP address and Primary Service Provider's key can be changed as well if necessary.

Aircraft should maintain their DTLS connection with the service provider after installing a new one time use private key. Upon any new login or refreshing of the connection the new private key (if available) will be used. The onetime use private key will expire upon the first successful logon with that key to the primary service provider; it must be changed at that time. The Upload a new Aircraft private one time use key will have a port 5908 key tag of 0x32, and be followed by the private key (upload) or one additional byte (response).

Service Provider Sends	Aircraft Responds	Meaning
Aircraft One Time Use Private Key	0x00	New One Time Use Private Key accepted and installed
Aircraft One Time Use Private Key	0x01	New One Time Use Private Key rejected.

Table 5-10 - Upload new Aircraft Private One time Use Key return codes

1.5.5.10.3.4 Upload a new Aircraft Certificate 0x33

Each Aircraft will be equipped with a digital certificate, used for authentication with the primary service provider and all trusted companion service providers. Uploaded certificates will be in DER format. The corresponding private key will be maintained by the aircraft and primary service provider.

Aircraft certificates will be signed by the primary service provider. See Section 5.3.5 ECDSA Keys for more information. The Aircraft Certificate will be transmitted over an encrypted channel negotiated at DTLS logon.

Aircraft should maintain their DTLS connection with the service provider after installing a new aircraft certificate using the old certificate if necessary. The port 5908 key tag of 0x33 will be followed by an Aircraft Certificate when sent by the service provider. The aircraft will use the same port 5908 key tag of 0x33 to send a one byte return code indicating success or failure.

Service Provider Sends	Aircraft Responds	Meaning
Aircraft Certificate	0x00	New One time use certificate is accepted and installed
Aircraft Certificate	0x01	New One time use certificate is rejected.

Table 5-11 - Install a new Aircraft Certificate return codes

1.5.5.10.3.5 Upload a new Aircraft one time use Certificate 0x34

Each Aircraft will be equipped with a one-time use certificate from its primary service provider. These certificates will be included in CRL lists provided to trusted companion providers, effectively making these certificates one time use only on the primary service provider's network. In the event that the aircraft's primary certificate fails due to expiration or CRL revocation the aircraft can use this one-time use key on the primary service provider's network. The one time use key will expire upon first use. Having a one-time use key ensures that aircraft will not require physical media in order to replace its service keys. That is as long as it is connected with the primary service provider. Uploaded one-time use certificates will be in DER format and be via the DTLS encrypted channel negotiated at logon.

Aircraft should maintain their DTLS connection with the service provider after installing a new one time use certificate using the old certificate if necessary. The UDP port 5908 key tag of 0x34 will be followed by a one-time use certificate in DER

format when sent by the Service Provider. The aircraft will use the port 5908 key tag of 0x34 and one additional byte to indicate success or failure.

Service Provider Sends	Aircraft Responds	Meaning
Aircraft One time use Certificate	0x00	New One time use certificate is accepted and installed
Aircraft One time use Certificate	0x01	New One time use certificate is rejected.

Table 5-12 - Upload a new Aircraft one-time-use Cert return codes

1.5.5.10.3.6 Upload the primary service provider's certificate 0x35

Part of the security system of the avionics is being able to recognize the primary service provider. When the aircraft is logged into the primary service provider via DTLS, then additional features will be unlocked to allow the primary service provider to maintain the keys, certificates and IP address of the aircraft. If the service provider certificate received during the DTLS logon does not match that of Primary Service Provider's, then the port 5908 key tags of 0x3X will be restricted from access. There will be only one primary service provider certificate within the avionics at any one time.

In the event that the primary service provider's server's certificate needs to change, perhaps due to nearing certificate expiration or crypto period expiry due to algorithm compromise.

Aircraft should maintain their DTLS connection with the service provider after installing a new primary service provider certificate until a re-authentication or new login is needed or requested. The port 5908 key tag of 0x35 will be followed by the Primary Service Provider's Certificate when sent by the Primary Service Provider. The aircraft will use a port 5908 key tag of 0x35 followed by one additional byte to indicate success or failure.

Service Provider Sends	Aircraft Responds	Meaning
Primary Service Provider's Certificate	0x00	New Primary Service Provider's certificate is Accepted and installed
Primary Service Provider's Certificate	0x01	New Primary Service Provider's Certificate is rejected.

Table 5-13 - Primary Service Provider Key upload return codes

1.5.5.10.3.7 Upload a secondary Service Provider's Certificate 0x36

Airlines often times contract with many service providers in order to have service if the primary service provider is not available. The primary service provider could upload via RF the secondary service provider's certificates; this is to limit who is authorized to update certificates over RF. Secondary Service provider certificate upload is limited to the customer agreement, Certificate Practice Statement and Certificate Policy, each service provider is free to develop their own policies as long as they meet or exceed the minimum standards outlined in the Master Certificate Policy.

Avionics upon receiving a secondary provider Certificate will update the secondary provider store with the incoming certificate. Only one secondary provider certificate will be uploaded per instance. It is expected that avionics will replace any secondary provider certificate previously existing in the secondary provider store issued by the same authority with that received. For example a SITA provider certificate with another SITA provider certificate. The avionics should maintain its own secondary provider certificate store and remove any expired secondary provider certificates periodically. There may be many secondary service providers' certificates in this store. Uploaded certificates will be in DER format.

Only the primary service provider will be allowed to upload new secondary provider certificates over the network. Airlines will be able to load them using on-ground avionics maintenance devices.

Aircraft should maintain their DTLS connection with the primary service provider after installing a new secondary provider certificates. Upon any new login or refreshing of the connection the current Secondary provider certificate store will be used to validate any trusted companion service provider's authentication certificate(s). The port 5908 key tag for uploading a new secondary provider certificate will be 0x36, and will be followed by certificate (upload) or one additional byte (response).

Service Provider Sends	Aircraft Sends	Meaning
Root Certificate	0x00	Certificate accepted and installed.
Root Certificate	0x01	Certificate rejected. – Already have this certificate, invalid, expired, or otherwise.

Table 5-14 - Upload new Secondary Provider Certificate Return Codes

1.5.5.10.3.8 Change the IP address 0x37

The primary service provider should assign an IP address to each aircraft under contract. This should be coordinated with IANA and be updated along with a new Aircraft Certificate, service provider key, aircraft secret key. The IP address should be changed via an encrypted connection negotiated at DTLS logon to the primary service provider.

Note: This specific command is only meant to be used infrequently due to a sale of an Aircraft or other major event.

Aircraft should maintain their DTLS connection with the service provider after installing a new IP address until a re-authentication or new login is needed or requested. The old IP address should be used until a new session is established. The port 5908 key tag of 0x37 will be followed by the new IP address when sent by the service provider. The aircraft will use a port 5908 key tag of 0x37 followed by one additional byte to indicate success or failure.

Service Provider Sends	Aircraft Responds	Meaning
New IP address	0x00	New Aircraft IP is accepted and installed.
New IP address	0x01	New Aircraft IP is rejected.

Table 5-15 - Change IP address return codes

1.5.5.10.4 Function of the One Time Private Key and Certificate

The Aircraft's One time use Key and Certificate are meant to be a failsafe mechanism to prevent aircraft from needing hands on maintenance in the event that an aircraft's key, certificate, or both become expired or compromised. It is intended that the one time use key will only be usable on the Primary Service provider's network. This will be enforced by adding the one-time use certificate to the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) shared with trusted companion service providers.

Each Primary Service Provider will need to keep two CRLs one of one-time use keys and the other of revoked certificates - other than by expiry. Primary service providers should accept logons via one-time use keys, but the detection of that key should trigger an immediate upload of a new aircraft primary key and certificate as well as one-time use Key and Certificate.

To emphasize, one-time use certificates and keys will only be usable on the primary service provider's network and then only once. They will be treated as revoked certificates on trusted companion service provider networks. Untrusted companion service providers will see them as invalid certificates.

1.5.5.10.5 Key Maintenance Operations Packet Format

Key maintenance operations are available for the primary service provider only. The DTLS Header and payload is encrypted to protect the keys and certificates while in transit. The key management packet shall look like:

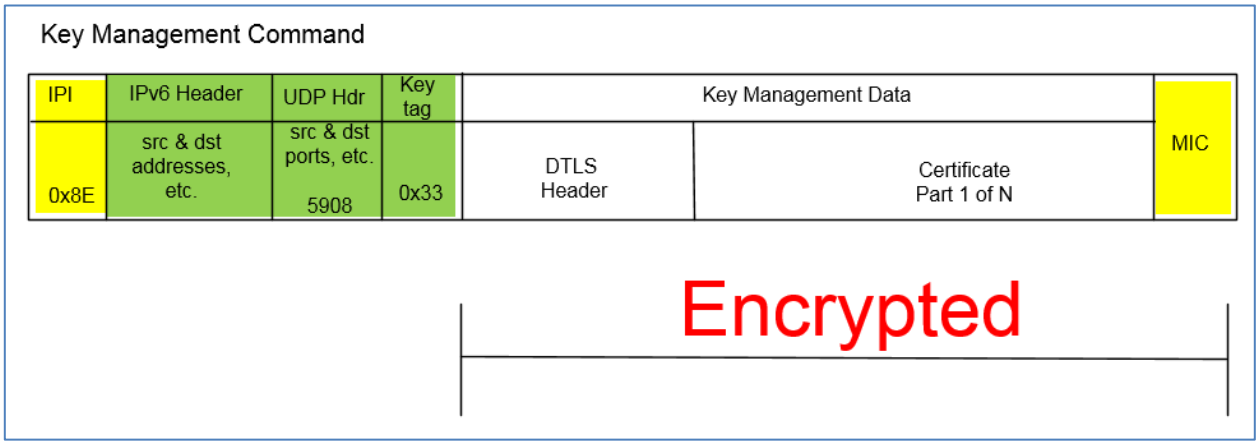


Figure 5-5 - Key Management Command format

In this example the primary service provider is sending up a new aircraft primary certificate for use on all new connections.

The response to a Key Management command shall use the DTLS Header and a response code usually 0x00 or 0x01 to indicate success or failure of the key command respectively. Please review each key management command for appropriate response codes.

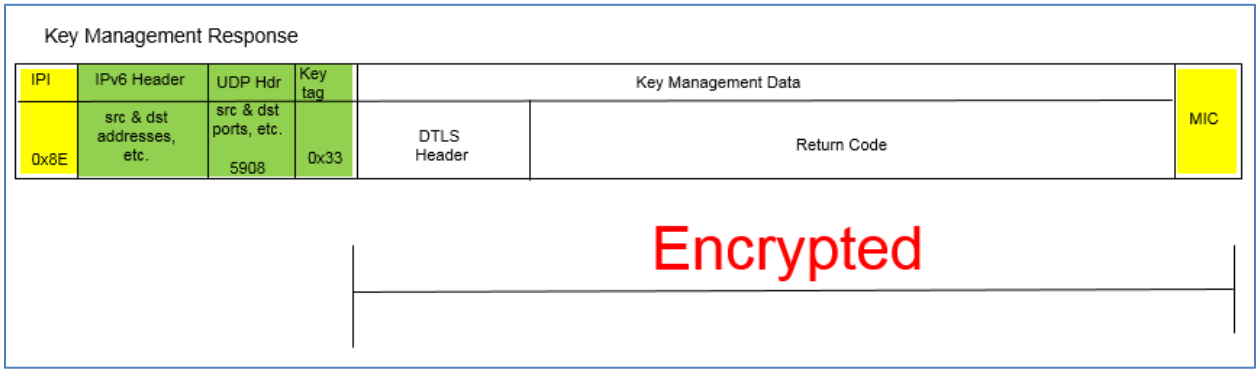


Figure 5-6 - Key Management Response format

1.5.6 IPS Mobility

To be defined

1.5.7 Maintenance

The IPS system shall be configurable and customizable. For this electronic software distribution security will implemented following the standard ARINC 835 (Guidance for Security of Loadable Software Parts Using Digital Signatures)

ATTACHMENT 1
LIST OF ACRONYMS

ATTACHMENT 1 LIST OF ACRONYMS ← *FROM 658*

4DT	Four Dimensional Trajectory
4DTRAD	Four Dimensional Trajectory Datalink
A-G or A/G	Air-to-Ground
A-ISAC	Aviation Information Sharing and Analysis Center
AC	Advisory Circular
ACARS	Aircraft Communications Addressing and Reporting System
ACD	Aircraft Control Domain
ACL	ATC Clearance
ACM	Aircraft Communications Message
ACMS	Aircraft Condition Monitoring System
ACR	Avionics Communications Router
ACSP	Air/Ground Communications Service Provider
ADS-C	Automatic Dependent Surveillance-Contract
ADS-C EPP	ADS-C Extended Projected Profile
AEEC	Airlines Electronic Engineering Committee
AeroMACS	Aeronautical Mobile Airport Communications System
AFN	ATS Facilities Notification
AIM	Aeronautical Information Management
AIREP	Aircraft Report
AIS/MET	Aeronautical Information Services/Meteorological
AISD	Aircraft Information Services Domain
ALGA	Active Low Gain Antenna
AMC	ATC Microphone Check
AMET	Airborne Meteorological
ANSP	Air Navigation Service Provider
AOA	ACARS Over AVLC
AOC	Airline Operational Control
ARAC	Aviation Rulemaking Advisory Committee
ARU	AeroMACS Radio Unit
ASBU	Aviation System Block Upgrade
ASN	Access Service Network
ASN-GW	Access Service Network Gateway
ATA	Air Transport Association
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
ATSP	Air Traffic Service Provider
ATSU	Air Traffic Services Unit

ATTACHMENT 1
LIST OF ACRONYMS

AUTOMET	Automatic Meteorological (report)
AVLC	Aviation VHF Link Control
BLOS	Beyond Line Of Sight
BS	Base Station
CA	Certificate Authority
CAA	Civil Aviation Authority
CARATS	Collaborative Actions for Renovation of Air Traffic Systems (Japan)
CDU	Control Display Unit
CDM	Collaborative Decision Making
CLNP	Connectionless Network Protocol
CM	Context Management
CMF	Communications Management Function
CMU	Communications Management Unit
CNS/ATM	Communications Navigation Surveillance/Air Traffic Management
CoS	Class of Service
COTP	Connection Oriented Transport Protocol
COTS	Commercial Off The Shelf
CP	Communications Panel (ICAO)
CP	Certificate Profile (PKI)
CPDLC	Controller Pilot Data Link Communications
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSN	Connectivity Network Service
CSP	Communication Service Provider
CSR	Certificate Signing Request
D8PSK	Differential 8-Phase Shift Keying
D-ATIS	Digital Automatic Terminal Information Service
D-OTIS	Datalink Operational Terminal Information Service
D-TAXI	Digital TAXI
DAL	Design Assurance Level
DCL	Departure Clearance
DCNS	Data Communications Network Service
DDoS	Distributed Denial of Service
DLIC	Data Link Initiation Capability
DLS-IR	Data Link Services Implementing Rule
DME	Distance Measuring Equipment
DoD	Department of Defense
DoS	Denial of Service
D-RNP	Dynamic Required Navigation Performance
DS	Dialog Service
DSI	Dialog Service Interface

ATTACHMENT 1
LIST OF ACRONYMS

DSP	Data Link Service Provider
EASA	European Aviation Safety Agency
ECAC	European Civil Aviation Conference
EFB	Electronic Flight Bag
EIPI	Extended Initial Protocol Identifier
EIRP	Equivalent Isotropically Radiated Power
ESA	European Space Agency
EU	European Union
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FCI	Future Communications Infrastructure
FDD	Frequency Division Duplex
FEP	Front End Processor
FF/ICE	Flight and Flow Information for a Collaborative Environment
FIR	Flight Information Region
FIS	Flight Information Service
FMF	Flight Management Function
FMS	Flight Management System
FY	Fiscal Year
G-G or G/G	Ground-to-Ground
GANP	Global Air Navigation Plan
GATM	Global Air Traffic Management
GES	Ground Earth Station
GHz	Gigahertz
GNSS	Global Navigation Satellite System
HDLC	High-level Data Link Control
HF	High Frequency
HFDL	High Frequency Data Link
HGA	High Gain Antenna
ICAO	International Civil Aviation Organization
ICS	Internet Communication Service
IER	Information Exchange and Reporting
IETF	Internet Engineering Task Force
IM	Information Management
IMA	Integrated Modular Avionics
IMS	Information Management Services
IOC	Initial Operational Capability
IP	Internet Protocol
IPI	Initial Protocol Identifier
IPS	Internet Protocol Suite
IPsec	Internet Protocol Security

ATTACHMENT 1
LIST OF ACRONYMS

IPv4 / IPv6	Internet Protocol Version 4 or Version 6
IS	Information Services
ISO	International Standards Organization
ISWG	Infrastructure Specific Working Group
ITP	In-Trail Procedure
ITU	International Telecommunication Union
LDACS	L Band Digital Aviation Communication System
LEO	Low Earth Orbit
LGA	Low Gain Antenna
LOS	Line of Sight
MAS	Message Assurance
MASPS	Minimum Aviation System Performance Standards
MCDU	Multi-purpose Control and Display Unit
MET	Meteorological
MHz	Megahertz
MIAM	Media Independent Aircraft Messaging
MOPS	Minimum Operational Performance Standards
MP-TCP	Multi-Path Transmission Control Protocol
MRO	Maintenance Repair and Overhaul
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
NM	Nautical Miles
NOTAM	Notice to Airmen
OCL	Oceanic Clearance
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OSWG	Operational Specific Working Group
OTIS	Operations Terminal Information System
PFIS	Passenger Flight Information Systems
PGW	Protocol Gateway
PIESD	Passenger Information Services Domain
PKI	Public Key Infrastructure
PLP	Packet Layer Protocol
PMC	Program Management Committee
POA	Plain Old ACARS
PPPoE	Point to Point Protocol over Ethernet
PR	Position Reporting
PS	Policy Statement
PT	Project Team
QAR	Quick Access Recorder
QoS	Quality of Service

ATTACHMENT 1
LIST OF ACRONYMS

RCP	Required Communication Performance
RCTP	Required Communication Technical Performance
RF	Radio Frequency
RFC	Request For Comment
RNP	Required Navigation Performance
RSP	Required Surveillance Performance
RSTP	Required Surveillance Technical Performance
SAL	Security Assurance Level
SARPS	Standards and Recommended Practices
Satcom	Satellite Communications
SBB	Swift Broadband
SBD	Short Burst Data
SCTP	Stream Control Transmission Protocol
SDO	Standards Development Organization
SDR	Software Defined Radio
sDS	Secure Dialog Service
SDU	Satellite Data Unit
SESAR	Single European Sky Air Traffic Management (ATM) Research
SIGMET	Significant Meteorological Information
SNAcP	Subnetwork Access Protocol
SPR	Safety and Performance Requirement
SWaP	Size Weight and Power
SWIM	System Wide Information Management
TAC	Technical Advisory Committee
TACAN	Tactical Air Navigation
TBD	To Be Determined
TBO	Trajectory Based Operations
TCP	Transmission Control Protocol
TDLS	Terminal Data Link System
ToR	Terms of Reference
TSO	Technical Standard Order
UDP	User Datagram Protocol
UI	Unnumbered Information
ULCS	Upper Layer Communication Services
US	United States
USB	Universal Serial Bus
V&V	Verification and Validation
VDL	VHF Data Link
VDLM2	VHF Data Link Mode 2
VHF	Very High Frequency
VOLMET	Vol (flight) Meteo (weather)

ATTACHMENT 1
LIST OF ACRONYMS

VPN	Virtual Private Network
WG	Working Group
WiMAX	Worldwide Interoperability for Microwave Access
WoW	Weight on Wheels
XID	eXchange Identification

ATTACHMENT 2 GLOSSARY ← *FROM 658*

AAC – Aeronautical Administrative Communications

Communication used by aeronautical operating agencies related to the business aspects of operating their flights and transport services. This communication is used for a variety of purposes, such as flight and ground transportation, bookings, deployment of crew and aircraft or any other logistical purposes that maintain or enhance the efficiency of over-all flight operation.

ACARS – Aircraft Communications Addressing and Reporting System

A digital datalink network providing connectivity between aircraft and ground end systems (command and control, air traffic control).

ACD – Aircraft Control Domain

It consists of systems and networks whose primary functions are to support the safe operation of the aircraft. This domain connects to high-priority Air Traffic Services (ATS) and some Airline Operational Control (AOC) communications.

ADS-C – Automatic Dependent Surveillance-Contract

ADS-C is the same as ADS-A. Automatic Dependent Surveillance-Addressed is a datalink application that provides for contracted services between ground systems and aircraft. Contracts are established such that the aircraft will automatically provide information obtained from its own on-board sensors, and pass this information to the ground system under specific circumstances dictated by the ground system (except in emergencies).

Airborne ATN/IPS System

An airborne component that supports main ATN/IPS functions.

AISD – Aircraft Information Services Domain

This domain provides general purpose routing, computing, data storage and communications services for non-essential applications. The AISD domain can be subdivided into two sub-domains;

- Administrative sub-domain, which provides operational and airline administrative information to both the flight deck and cabin,
- Passenger support sub-domain, which provides information to support the Passengers

AOA – ACARS Over Aviation VHF Link Control

AOA is an attempt at gaining some early benefits of digital technology without the full risk of ATN. It is a step between full ACARS and full ATN. The most significant near-term benefit is the reduction of VHF congestion problems by transitioning traffic to the VDLM2 air/ground network. AOA allows airborne and airline host applications to remain unchanged (character format). The airborne AOA process packages the data so that it can be routed over the digital VDLM2 network. At some point on the ground, the data is restored to its original format for processing by legacy airline host applications. VDLM2 operates at 31.5 kbps versus ACARS at 2.4 kbps.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

AOC – Airline Operational Control (Aeronautical Operational Control)

Operational messages used between aircraft and airline dispatch centers or, by extension, the DoD to support flight operations. This includes, but is not limited to, flight planning, flight following, and the distribution of information to flights and affected personnel.

APC – Aeronautical Passenger Communications

Communication relating to the non-safety voice and data services to passengers and crew members for personal communication.

Application

Functions that provide the services needed by the users. Applications are grouped into Application sets that are associated to specific network protocols. In the ACD domain the Applications sets are providing air traffic and operational control services.

ATN – Aeronautical Telecommunications Network

An internetwork architecture that allows ground/ground, air/ground, and avionic data subnetworks to interoperate by using common interface services and protocols based on the ISO OSI Reference Model.

ATN/IPS Node

An ATN/IPS node is a device that implements IPv6. There are two types of ATN/IPS nodes; 1) the ATN/IPS system that forwards Internet Protocol (IP) packets not explicitly addressed to itself and 2) ATN/IPS host, which does not have the capability to route traffic flows.

ATN/IPS

Internetwork consisting of ATN/IPS nodes and networks operating in a multinational environment in support of Air Traffic Services (ATS) as well as aeronautical industry service communication such as Aeronautical Operational Control (AOC) and Aeronautical Administrative Communications (AAC).

ATS – Air Traffic Services

A generic term meaning variously, flight information service, alerting service, air traffic advisory service, air traffic control service. The latter is a service provided for the purpose of preventing collisions, expediting and maintaining an orderly flow of traffic.

ATSU – Air Traffic Services Unit

A unit established for the purpose of receiving reports concerning air traffic services and flight plans submitted before departure. It is a generic term meaning air traffic control unit, flight information center, or air traffic service reporting office.

GLOSSARY

CM – Communication Manager

This function manages the connectivity of the aircraft with the ground system. It is decomposed into two sub-functions:

- ATN/IPS Communication Manager, which manages in the ATN/IPS system the selection of the radio bearer for a dedicated traffic flow and the associated mode of communication.
- External Communication Manager, which performs router selection and associated vertical handover decisions. This entity may be extended to include the management of multi-domain link selections.

CMU – Communication Management Unit

The CMU performs two important functions: it manages access to the various datalink sub-networks and services available to the aircraft and hosts various applications related to datalink. It also interfaces to the flight management system (FMS) and to the crew displays.

CNS/ATM – Communication, Navigation, Surveillance/Air Traffic Management

CNS/ATM is a system based on digital technologies, satellite systems, and enhanced automation to achieve a seamless global Air Traffic Management. Modern CNS systems will eliminate or reduce a variety of constraints imposed on ATM operations today.

CPDLC – Controller-Pilot Data Link Communications

The CPDLC application provides for the exchange of flight planning, clearance, and informational data between a flight crew and air traffic control. This application supplements voice communications and, in some areas, data may supersede voice.

DS – Dialog Service

The Dialog Service serves as an interface between the ATN applications and the ATN/OSI or ATN/IPS upper layer protocols via the control function.

FANS-1/A – Future Aircraft Navigation System 1/A

A set of operational capabilities centered around direct datalink communications between the flight crew and air traffic control. Operators benefit from FANS-1/A in oceanic and remote airspace around the world.

FMF – Flight Management Function

A collection of processes or applications that facilitates area navigation (RNAV) and related functions to be executed during all phases of flight. The FMF is resident in an avionics computer and automates navigational functions reducing flight crew workload particularly during instrument meteorological conditions. The Flight Management System encompasses the FMF.

FMS – Flight Management System

A computer system that uses a large database to allow routes to be preprogrammed and fed into the system by a means of a data loader. The system is constantly updated with respect to position by reference to designated sensors. The sophisticated program and its associated database insure that the most appropriate

aids are automatically selected during the information update cycle. The flight management system is interfaced/coupled to cockpit displays to provide the flight crew situational awareness and/or an autopilot.

Ground ATN/IPS Router

A ground device that is used to support ATN/IPS packet forwarding in both air/ground and ground/ground environments.

Infrastructure

This is a general term corresponding to the communication systems that support the application sets. It consists of the Network and Sub-networks functions.

LINK 2000+ – The EUROCONTROL LINK 2000+ Program

The European validation program that demonstrated controller-pilot data-link-communication (CPDLC) services into a set for implementation in the European Airspace using the ATN and VDLM2 (Aeronautical Telecommunication Network and VHF Digital Link).

MASPS – Minimum Aviation System Performance Standards

High-level documents produced by RTCA that establish minimum system performance characteristics.

MOPS – Minimum Operational Performance Standards

Standards produced by RTCA that describe typical equipment applications and operational goals and establish the basis for required performance. Definitions and assumptions essential to proper understanding are included as well as installed equipment tests and operational performance characteristics for equipment installations. MOPS are often used by the FAA as a basis for certification.

Multilink

Concept that defines the use of concurrent, existing and future communication links between air and ground (e.g., AeroMACS, LDACS and Satcom), depending on the defined criteria (performance needs).

NAS – National Airspace System

One of the most complex aviation systems in the world that enables safe and expeditious air travel in the United States and over large portions of the world’s oceans.

Network

The Network function is decomposed into two main sub-functions; a router that routes data packets from a source to a destination and the communication manager, which is responsible for the network and link selections.

Network Layer

The Network Layer is based on Internet Protocol (IP) ensuring global routing over interconnected packet-switched communication networks.

GLOSSARY

Physical and Link Layers

They are associated with the Sub-networks and handle the physical interface with the transmission medium (i.e., radio links).

PIESD – Passenger Information and Entertainment Services Domain

It is characterized by the need to provide passenger entertainment and network services. Beyond traditional IFE systems, it may also include passenger device connectivity systems, Passenger Flight Information Systems (PFIS), broadband television or connectivity systems.

SARPS – Standards and Recommended Practices

Produced by ICAO, they become the international standards for member states. As the name implies, they are only “recommended” practices. It is up to each member states to decide how/if to implement them.

Satcom – Satellite Communications

Communication service providing data, voice, and fax transmission via satellite. Allows aircraft to communicate in BLOS areas.

SESAR – Single European Sky ATM Research

European air traffic control infrastructure modernization program. SESAR aims at developing the new generation ATM system capable of ensuring the safety and fluidity of air transport worldwide over the next 30 years.

Sub-network

The sub-networks correspond to all radio systems that are used to communicate between the aircraft and the ground.

Transport Layer

The transport layer protocols are used to provide reliable or unreliable communication services over the ATN/IPS system. Those include TCP for reliable transport services and UDP that is used to provide best effort service.

VDL – VHF Data Link

Also known as VHF Digital Link, VDL is the LOS sub-network supporting data communications that are sent over VHF frequencies. The traditional VHF voice radio can be used in conjunction with a data modem to send data messages over VHF frequencies.

VDLM2 – VHF Data Link Mode 2

A datalink-only service designed to digitize VHF and improve the speed of the VHF link. VDLM2 is intended for use within the US and Europe as an interim datalink solution for enroute ATC functions. VDLM2 provides a 31.5 kbps channel rate.

Vertical Handover

GLOSSARY

APPENDIX A ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS (RC IMS)

A-1 Potential Ground Architectures

A-1.1 Full End-to-End

A-1.2 Multiple “Segment Correlations”

A-2 Gateway Architectures

A-2.1 Dual-Stack (OSI / IPS)

A-2.2 Dual-Stack (ACARS / IPS)

A-2.3 Triple-Stack (ACARS / OSI / IPS)

A-3 Gateway Functional Requirements (BOEING)

A-4 Security Gateway implementation (DTLS)

1.6 Security Characteristics

There are two modes to consider for the protocol build-up as related to security:

- Session establishment message exchange
- Session management message exchange
- Application message exchange

The Initial Protocol Identifier (IPI) is used to identify the presence of IPS data and the UDP port number is used to describe the type of IPS data. Additionally data on the authentication port (5908) has a key tag to further identify the type of message.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Note: There is an ICAO requirement to provide ATC services by default. How this requirement is addressed by IPS is a policy issue. From the viewpoint of the IPS gateway, this could be handled such that if an aircraft has a valid key then the message can be delivered.

If the aircraft does not have a valid key or no key then it may be allowed IPS ATC only communication and messages may be marked as suspect since they cannot be authenticated. Each service provider will determine their own policy on delivery of unauthenticated messages.

The specifics of the individual components of the protocol build-up are detailed further on in the document.

1.6.1 Session Establishment

The protocol build-up for session establishment (authentication) is shown for IP-based ***don't know if we want to specify IP-based since we are not showing the non-IP layer 2 session establishment*** communications (example of this is shown in Figure 5-2). IP Based session establishment shall utilize UDP port 5908. Port 5908 is reserved for specific messages (authentication, post authentication message, key management, IPS information, and IP lookup); with the type of message being defined by the first byte (key tag) of the UDP data field. For authentication, the key tag field value must be 0x0A. Prior to authentication, UDP port 5908 will be the only available port. Note that a message integrity check (MIC) field [see section 5.4 for details] is not present during authentication because the session key has not been established. No other key tags will be accepted by the gateway prior to authentication.

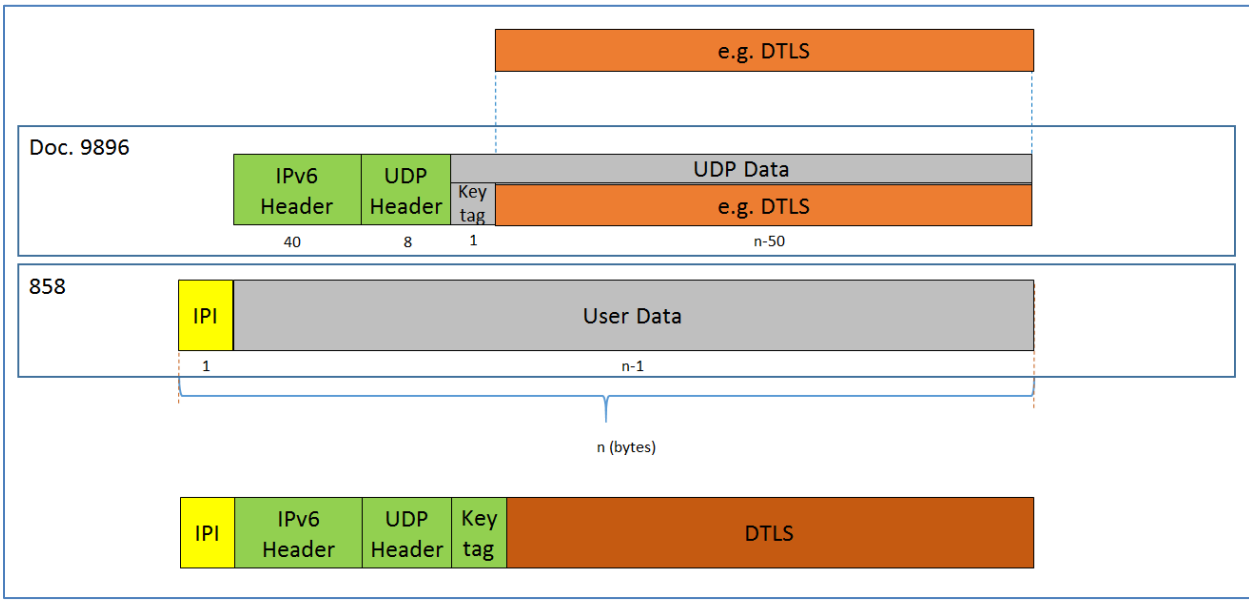


Figure 5-7 – IP-based Datalink (e.g. SATCOM) Session Establishment

1.6.2 Session Management

This message exchange covers all other messages sent over UDP port 5908. All of these messages are DTLS encapsulated messages, with the specific type of message being identified by the key tag. The format is the same as session establishment except that it includes a MIC field since authentication has been completed.

It should be noted that all messages on UDP Port 5908 use the DTLS header. Furthermore all messages that use a DTLS header, post authentication, will be encrypted. Responses to simple IP lookups and post authentication messages will also be encrypted.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

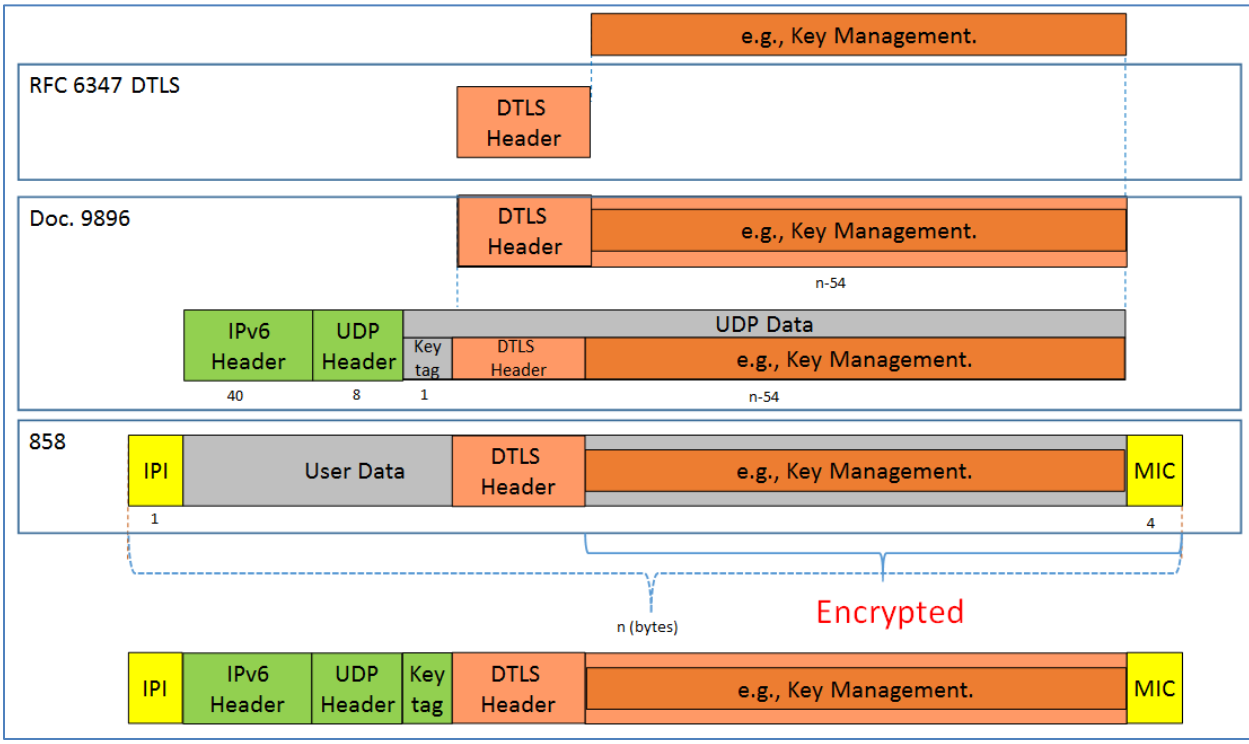


Figure 5-8 – IP-based Datalink (e.g. SATCOM) Session Management

1.6.3 Post Authentication Message

After the DTLS session is established, the avionics will use the standard IP IPS format found in Section 5.2.3 Session Management, to send an additional DTLS application packet. This application packet will use UDP port 5908 with key tag 0x0A. The DTLS header will indicate this is application traffic. The Post Authentication Message will contain the aircraft's fixed nomadic IP address, ATN address, tail number, Flight ID and a random start message number for downlinks. The server will respond with another random start message number for uplinks. After the post authentication message exchange has been completed, anything on port 5908 with a key tag of 0x0A will be a TLS Alert message and/or connection maintenance traffic. All connection maintenance and TLS alert messages will use the same format recorded in section 5.2.3 above. The purpose of the Post Authentication message is to allow IPS conversions to ATN/OSI or ACARS as necessary and to setup a random sequence number for MIC generation. See Figure 5-5 for the protocol buildup for Post Authentication Messages. Tail and flight ID lengths are in Bytes.

Aircraft Fixed Nomadic IP Address 16 Bytes	Aircraft ATN/OSI Address 20 Bytes	Tail # Length (1 nibble) / Flight ID Length (1 nibble) Length 1 Byte	Tail Number	Flight ID	Random Message Number Length for MIC generation 6 Bytes

Figure 5-9 - Post Authentication Aircraft to Gateway Message Format

Random Message Number Length for MIC generation 6 Bytes

Figure 5-10 - Post Authentication Gateway to Aircraft Message Format

1.6.4 Aircraft Information and IP lookup Message

The IPS enabled avionics will periodically report information to the local gateway to maintain the DTLS connection using UDP port 5908 Key Tag 0x0B. The avionics can also query the gateway for end system information using a simplified IP lookup message using UDP port 5908 Key tag 0x0C. See Sections 5.6 IPS Information Message and Section 5.7 IP Lookup Message for more information. All messages on UDP port 5908 will use the encryption method negotiated during DTLS logon.

1.6.5 Application Messages

The application messages are sent on specific UDP ports other than port 5908. These messages do not require the key tag used for port 5908 messages. Application messages will not be encrypted, but will have a calculated MIC to ensure message integrity while in transit. Examples of the protocol build-up are shown below for IP-based.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

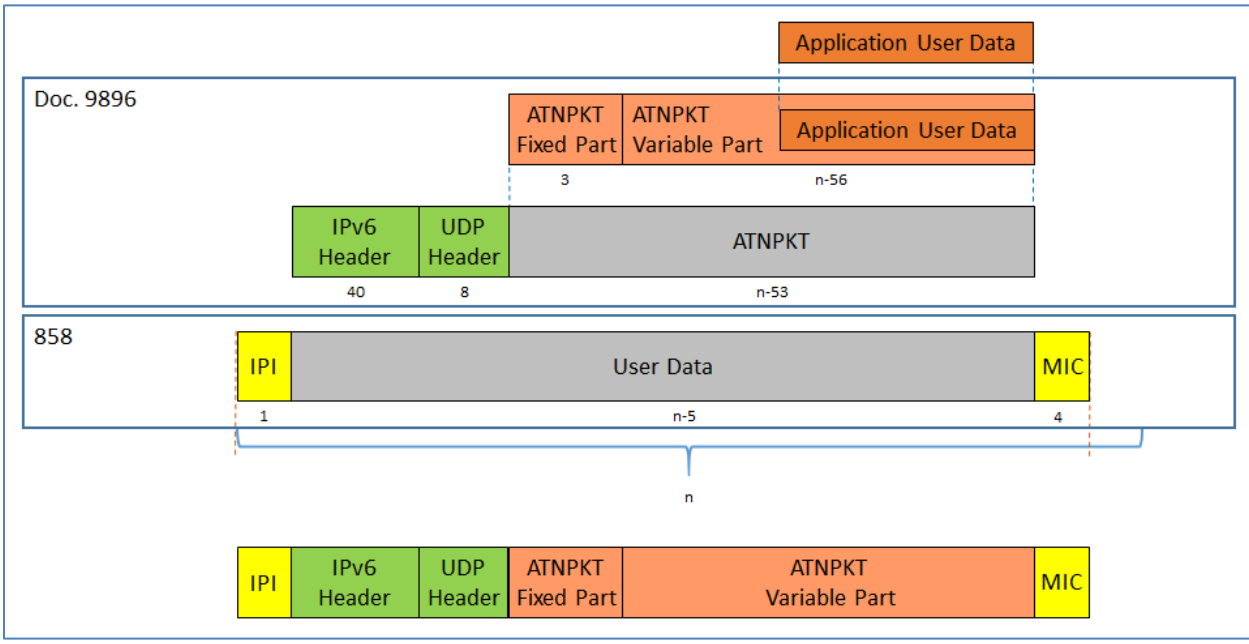


Figure 5-11 - Application Message

1.6.6 Initial Protocol Identifier

The Initial Protocol Identifier (IPI) is a 1 byte field used to identify the presence of IPv6 data. IPI 0x8E value is identified for IPv6 per ISO/IEC TR 9577 1999 edition appendix C. The ground adds the IPI before the IPv6 header for all uplink messages.

For downlink messages, the ground station (VHF or Satcom) examines the IPI and routes IPv6 messages to the IPS Gateway. The IPI will be included as a part of the message in transmission to the IPS Gateway.

1.6.7 Port 5908 Key Tag Values

The port 5908 specific messages are defined by the first byte (the port 5908 key tag field) of the data field. The following are the messages and their codes:

	Message
	Authentication

GLOSSARY

	IPS Information
	IP Lookup
	Key Management

Table 5-16 - Port 5908 Key Tag Values

The messages are defined in the respective sections.

1.7 Message Integrity Check

The message integrity check (MIC) is computed for each IPv6 packet in order to provide data integrity and authentication. For non-IP networks the MIC may also be computed for each subnetwork packet transmitted in order to secure the subnetwork (this is the case for VDL Mode 2, other subnetworks may be different).

The MIC is computed after the aircraft authentication sequence has been completed.

1.7.1 MIC for IP Packet

The MIC is computed for each IPv6 packet. A fragmented application message, consisting of a number of IPv6 packets, will have a MIC on each IP packet. The MIC is computed after compression over the entire IPv6 packet, the scope of the MIC computation is shown in Figure 5-18. The last 4 bytes from the MIC computation are used to populate the MIC field, which is added at the end of the IPv6 packet by the IPS Gateway for uplink messages.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

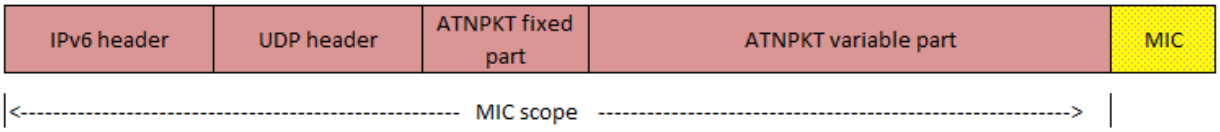


Figure 5-12 – MIC Scope for IP Packet

For downlink messages, the IPS Gateway computes the MIC the same way and compares the last 4 bytes against the value in the MIC field received in the downlink message. If the values do not match, the message is logged with the status of invalid MIC and a DTLS alert message (bad_record_mac) is generated in response. See Section 5.11 Error Detection for more information.

1.7.2 MIC for Subnetwork Packet (AVLC based media)

The MIC is computed for each subnetwork packet, this is illustrated by looking at the VDL Mode 2 network.

Note: MIC computation at the AVLC layer (sub-network layer) is not specifically IPS functionality, however it is included in the document since VDL Mode2 is not secured like other IPS media and the addition of securing VDL Mode2 is specifically for the support of IPS.

The VDL Mode 2 subnetwork utilizes the ‘orange’ protocol to provide segmentation of messages that exceed the AVLC frame size. The ‘orange’ protocol receives the IPv6 packet (maximum size of 1280 bytes) and segments it as needed to fit within the AVLC frame size (251). Each of these segments will be in an AVLC frame with the IPS IPI and the ‘orange protocol header and the computed MIC at the end of AVLC information field. This segmentation is illustrated in Figure 5-19.

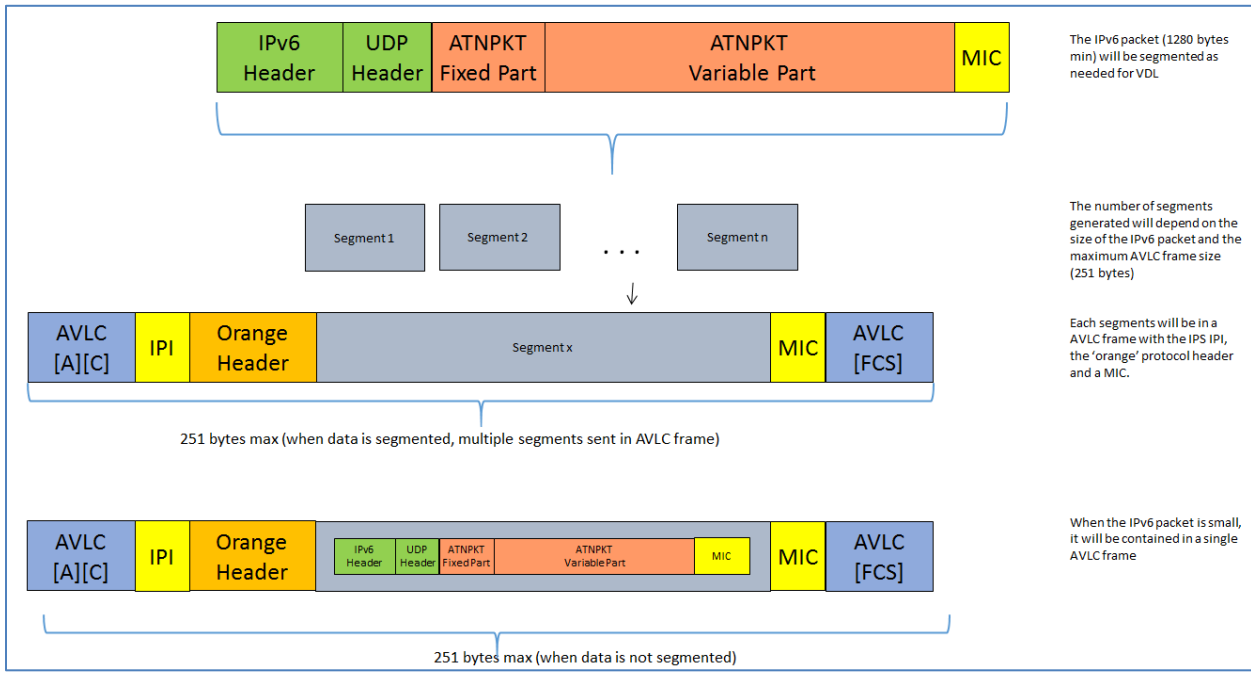


Figure 5-13 - VDL Mode 2 link layer segmentation for IPS

The MIC is computed over the AVLC header and the entire AVLC information field excluding the last 4 bytes which are reserved for the last 4 bytes of the MIC field. This is illustrated in Figure 5-20.

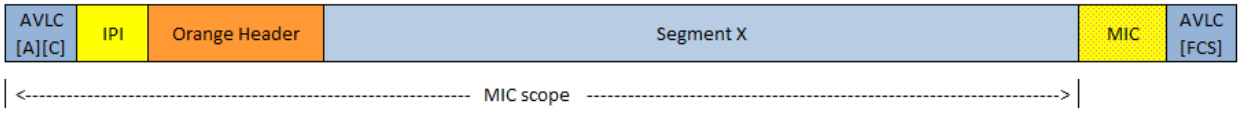


Figure 5-14 - MIC Scope for non-IP-based Datalink (e.g., VDL Mode 2)

1.7.3 MIC Generation Function for IPS IP packet

DTLS uses the following function to generate the message integrity code:

$$MIC = Truncate(4, PRF(App\ Data + Msg\# + Data\ Length\ with\ Msg\#, + Session\ Key + \ Key\ Length))$$

"+" denotes concatenation.

The MIC is generated before any encryption is applied. If encryption is applied it includes the MIC.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Variable Name	Explanation
Truncate	A Truncate function that reduces the size of the operator to a number of bytes. In this case the last 4 bytes of the message hash function will be used as a message integrity check.
PRF	Psudo Random Function: This is the hashing function negotiated during the initial DTLS handshake.
App Data	The application layer of data to be miced. For example in an http request the entire http request would be the app data.
Msg # (6 Bytes)	The random message number sent in the last message after authentication added with the total transmissions since that time. This Msg# is unique for downlinks and uplinks and starts with a random number sent after successful DTLS logon. For example the downlink message number could be 568 and the uplink message number could be 123. After one downlink the new downlink message number will be 569. The Message number rolls over to zero if it reaches it max. This message number is not to be confused with the Orange sequence number, if any.
Data Length with Msg# (6 Bytes)	The total length of the Application Data added to the current message number. If the results is greater than max value. Subtract max value. This is effectively a check on the data integrity.
Session Key (32 Bytes)	This is the lower 32 bytes of the session key derived as per RFC 5246 Section 6.3. Both the gateway (server) and aircraft (Client) have a session or master key and compute the counter parties' key using the procedure recorded in the RFC. This value is never transmitted making the PRF function difficult to duplicate by third parties.
Key Length	The total session key length in bytes.

	(4 Bytes)	

1.7.4 MIC Generation Function for AVLC.

DTLS uses the following function to generate the message integrity code:

$$MIC = Truncate(4, PRF(App\ Data + Msg\# + Data\ Length\ with\ Msg\#, + Session\ Key + \ Key\ Length))$$

"+" denotes concatenation.

Note: The session key is shared between the segment (AVLC layer) and the message (IPS Layer). The computations of MIC are different resulting in a code that is difficult to fake at both layers.

The MIC is generated before any encryption is applied. If encryption is applied it includes the MIC.

Variable Name	Explanation
Truncate	A Truncate function that reduces the size of the operator to a number of bytes. In this case the last 4 bytes of the message hash function will be used as a message integrity check.
PRF	Psudo Random Function: This shall be negotiated at DTLS logon
App Data	The information frame to be miced. For everything between the AVLC header and footer
Msg #	The Message number shall start a 1 for the first downlink/uplink and be increased for each successive

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

	(6 Bytes)	AVLC transmission. This Msg# is unique for downlinks and uplinks. For example the downlink message number could be 902 and the uplink message number could be 321. After one successful downlink the new downlink message number will be 903. The Message number rolls over to zero if it reaches it max. This message number is not to be confused with the Orange sequence number, if any.
	Data Length with Msg# (6 Bytes)	The total length of the Information Frame Data added to the current message number. If the results is greater than max value. Subtract max value. This is effectively a check on the data integrity.
	Session Key (32 Bytes)	This is the lower 32 bytes of the session key derived as per RFC 5246 Section 6.3. Both the gateway (server) and aircraft (Client) have a session or master key and compute the counter parties' key using the procedure recorded in the RFC. This value is never transmitted making the PRF function difficult to duplicate by third parties.
	Key Length (4 Bytes)	The total session key length in bytes.

1.8 Session Management

DTLS sessions to a service provider may extend to 8 hours in length or upon avionics shutdown which ever happens first. It may occur that an aircraft arrives at the gate, loads a new set of passengers and/or cargo while now powering down and is still within its 8 hour window for DTLS session. In that event the aircraft may either terminate its session and reestablish with a new Flight ID (if necessary) or alternatively may send commands to the IPS Gateway to indicate that it has changed a parameter of the flight.

1.8.1 Session Management Functions:

To facilitate max length DTLS Sessions the following commands can be initiated by the aircraft to the IPS Gateway.

Key Tag	Meaning

0x20	Change Flight ID
0x21	Reserved - Encrypted
0x22	Reserved - Encrypted
0x23	Reserved - Encrypted
0x24	Reserved - Encrypted
0x25	Reserved - Encrypted
0x26	Reserved - Encrypted
0x27	Reserved - Encrypted
0x28	Reserved - Encrypted
0x29	Reserved - Encrypted
0x2A	Reserved - Encrypted
0x2B	Reserved - Encrypted
0x2C	Reserved - Encrypted
0x2D	Reserved - Encrypted
0x2E	Reserved - Encrypted
0x2F	Reserved - Encrypted

1.8.2 Change Flight ID 0x20

Avionics will be expected to notify the gateway of any change to its flight ID information. The flight ID could change due to the completion of a flight leg or as a result of a flight amendment. The Aircraft Avionics shall initiate the change of flight ID command and the IPS Gateway will respond with an acknowledgement accepting or rejecting the change.

The protocol build-up of a session management message shall conform to section 3.3.4 Session Management - All Media. The flight ID may not exceed 15 characters including Airline code.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Aircraft Sends	Service Provider Responds	Meaning
Flight ID including Airline code Example: XA1234	0x00	New Flight ID Accepted
Flight ID including Airline code Example: XA1234	0x01	New Flight ID not accepted • length did not match actual length, • Flight ID does not match certificate ownership, such as an XA certificate when flight ID is $$1234 • Any other reason

Table 3-17 Change Flight ID Return Codes

A change in flight ID will not change the session key, session token or any other aspect of the DTLS logon. The Flight ID is used for ACARS conversions if necessary.

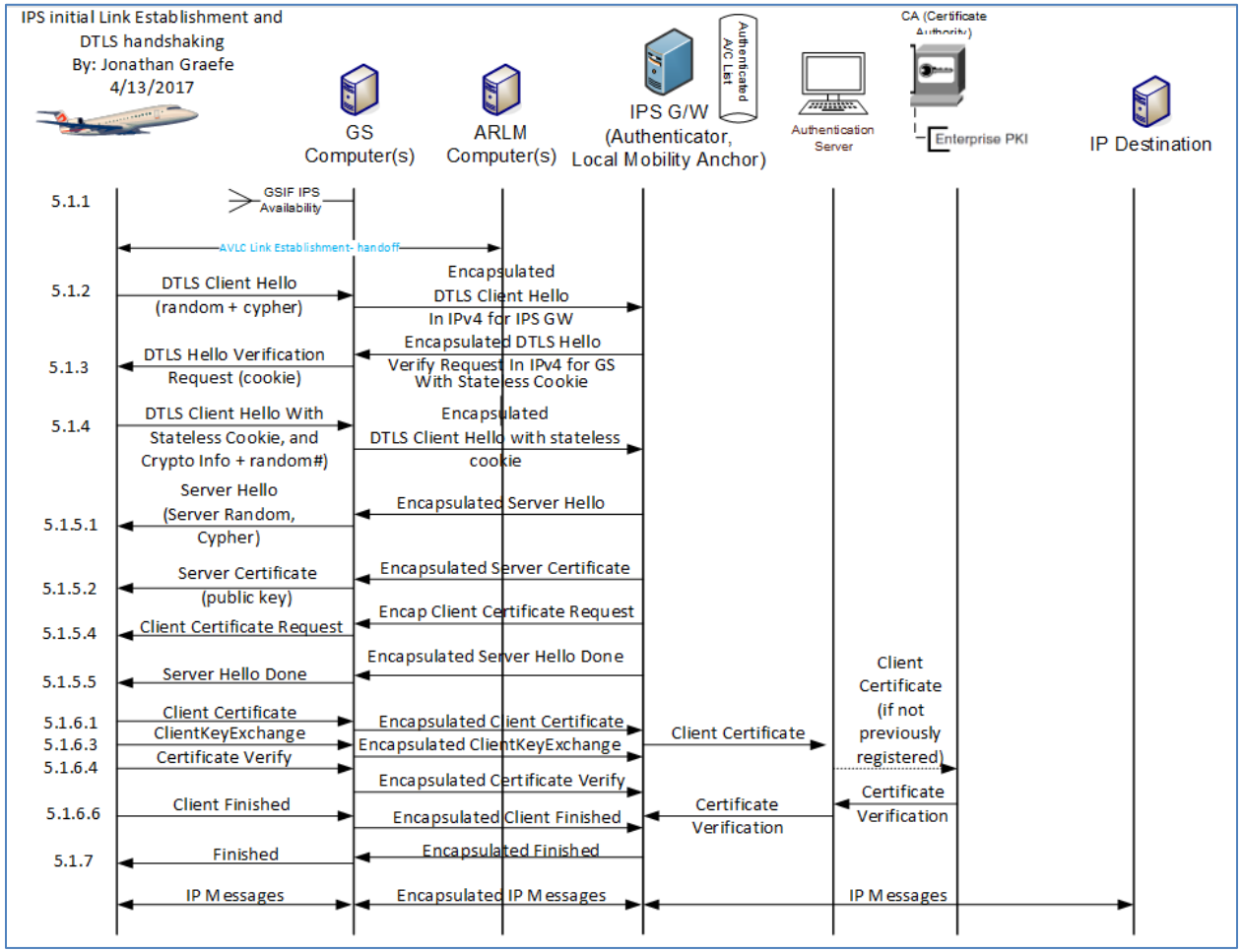
APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

1.9 Authentication Detail

Authentication is initiated by the IPS Aircraft to the current services provider's IPS Gateway. Authentication messages are not forwarded to any companion service area's IPS Ground System.

Authentication will be performed through many steps called DTLS Flights (shown in Figure 6-1) where security parameters will be exchanged and a secured communication path will be established. The IPS Aircraft and the IPS Gateway shall use Deflate compression on all the messages including all the authentication handshake process messages. Message Integrity code (MIC) checks are not included until after the authentication process is complete.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS



APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

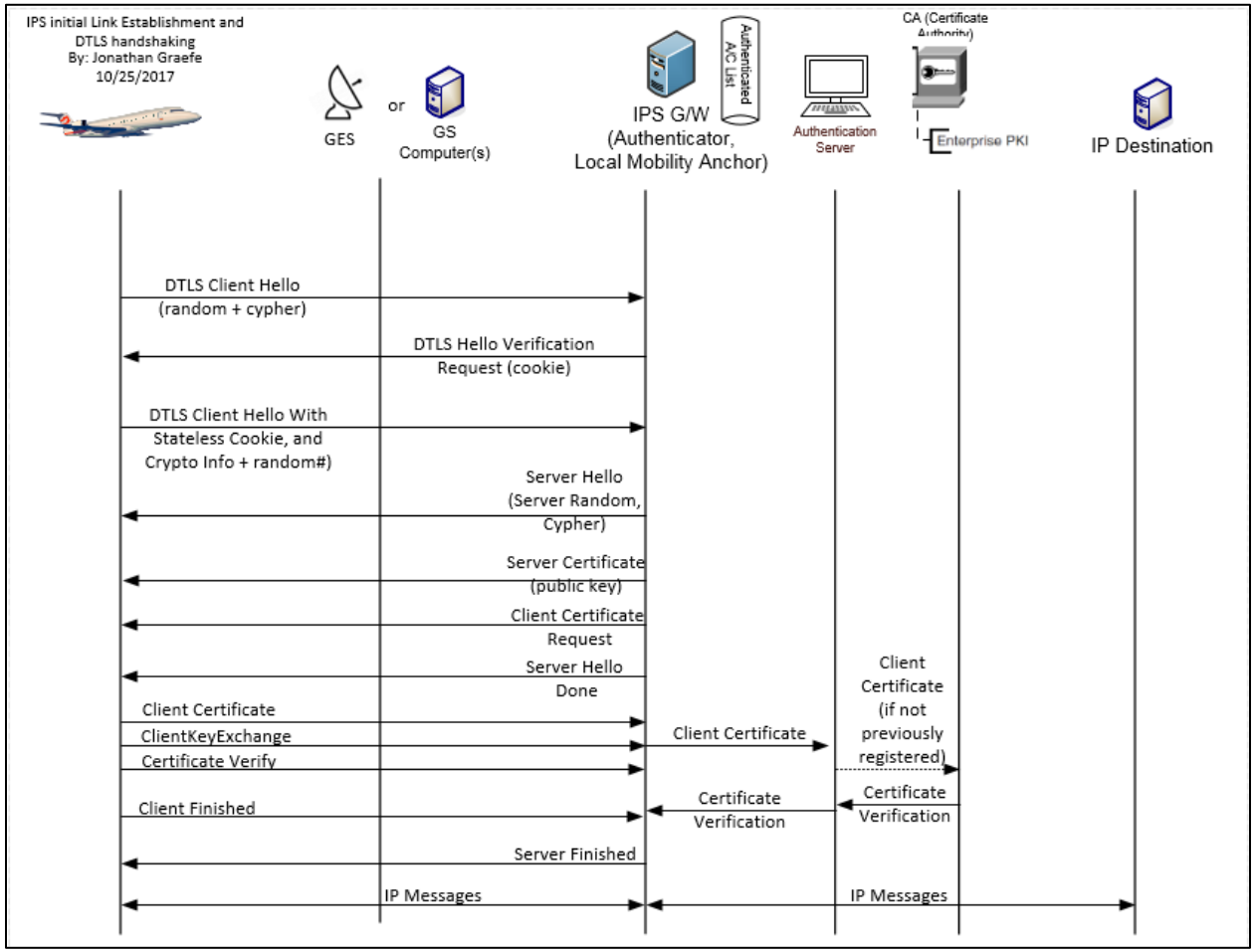


Figure 6-15 – IPS/DTLS authentication flights

General order of operation for a new connection:

1) Aircraft detects IPS availability (either GSIF advertising or route solicitation)
2) Aircraft sends a DTLS Client Hello Message leaving the opaque cookie blank.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

3) The IPS Gateway responds with a HelloVerifyRequest providing an opaque cookie.
4) Aircraft resends the DTLS Client Hello Message but inserts the opaque cookie into the message.
5) Gateway sends a series of server authentication messages including:
    a. A Server Hello with the parameters of this session
        i. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        ii. Curve is secp384r1
    b. The IPS Gateway sends a x.509 DER encoded public certificate to the aircraft
    c. ServerKeyExchange: The elliptic curve parameters including the ECDHE key are sent
    d. A request for the aircraft's certificate specifying the curve it expects
    e. A message stating that the Gateway has completed its side of the authentication
6) Aircraft sends a burst of messages including:
    a. The aircrafts public x.509 DER encoded certificate is sent to the gateway
    b. ClientKeyExchange: an ECDH Ephemeral key
    c. A certificate verify message passing a signed hash of all messages up to this point. Proves the aircraft has the private key.
    d. Message to begin applying the negotiated DTLS parameters
    e. an encrypted, MICed and compressed message indicating the client is finished with the authentication
7) The Server completes the authentication process by applying the negotiated parameters
    a. Server issues a Session Ticket
    b. Server sends a changeCipherSpec in the clear
    c. An encrypted, MICed and compressed message indicating that the server is finished with the authentication and the DTLS session is now fully established.
8) The Aircraft send via the MICed authentication channel:
    a. Aircraft sends IPv6 address, Tail ID and Flight ID to the gateway

1.9.1 Aircraft Detects IPS Availability

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

VDL enabled ground stations will advertise the availability of services periodically via a Ground Station Information Frame (GSIF). Upon hearing a GSIF that advertises IPS availability the aircraft may initiate a DTLS connection with the IPS Gateway. The ground stations that do not support IPS will ignore any request for IPS service(s). For Satcom after establishment of the Satcom link, availability of IPS service is determined by the avionics through a route solicitation message.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

1.9.2 Initial Client Hello

Upon hearing a GSIF that advertises IPS availability the aircraft can immediately initiate an IPS/DTLS logon when the frequency is clear. The initial client hello (shown in Table 6-3) will be missing an opaque cookie later provided by the IPS Gateway. The cookie is used to detect denial of service attacks against the service provider. It is intended that the initial Cipher Suite for IPS will be TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and all IPS messages including authentication messages will be compressed using the Deflate compression method. It is expected that the supported cipher list will expand in time as new methods are invented and legacy methods retired.

The Client Hello Message informs the server about the capabilities of the client.

DTLS Header Fields DTLS Handshake messages and their Meaning:

Field Name	Example Value	Meaning
Content Type	0x16 [1 Byte]	The following message is a DTLS Handshake Protocol Message – these are primarily used for authentication and session management.
Protocol Version	0xFE 0xFD [2 Bytes]	The aircraft supports DTLS Version 1.2 and below.
Epoch Cypher #	0x00 0x0	This message is using the first cipher method negotiated. In this case the default, no encryption

	0 [2 Bytes]	or Message integrity code, but compressed using deflate.
Message Seq#	0x00 0x00 0x00 0x00 0x00 0x00 [6 Bytes]	Message Sequence Number. Number represents the number of messages sent starting at 0x00. Both the server and client have their own unique counter and increment them for messages sent by each respective side.
Length	0x00 0x65 [2 Bytes]	The Total length of the data payload of the message. In this case starting from the Handshake Protocol header

Table 6-18 - DTLS Header Fields for DTLS Handshake Messages

Handshake Protocol Header fields for Initial Client Hello and their Meaning:

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Field Name	Example Value	Meaning
Handshake Type	0x01 [1 Byte]	This is a Client Hello message
Length	0x000x000x59 [3 Bytes]	The total length of the Client Hello header
Message Seq	0x000x00 [2 Bytes]	Message Sequence Number. Similar to the Message sequence number of the DTLS header, but counts the steps of the authentication handshake. This sequence number does not necessarily need to be the same as the DTLS header message sequence number but it could be.
Fragment offset	0x000x00	The first byte of this fragment position in the entire message. For instance this may be a fragment in the middle of the message, in that case this field is the position of the first byte of this packet in the assembled message.

	0x00 [3 Bytes]	
Fragment Length	0x00 0x00 0x59 [3 Bytes]	The length of this fragment. If this fragment contains the full message then the length field and this field will match.

Table 6-19 - Handshake Protocol Header for initial Client Hello

Client Hello Header fields and their Meaning:

Field Name	Example Value	Meaning
Protocol Version	0xFE 0xFD [2 Bytes]	Represents the aircraft supports the DTLS 1.2 protocol and below for handshakes.
Random	Varies	A two part random number. The first 4 Bytes is the number of seconds since January 1, 1970. The

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

		[4 Bytes + 28 Bytes]	Last 28 Bytes are a random number generated by the client.
Session ID		Varies [2 Bytes + Variable Bytes]	The first 2 Bytes represent the length of data to follow for this field. The remaining bytes are the session ID issued by the server (IPS Gateway), that this aircraft would like to resume. It is acceptable that the aircraft initiates a new connection for each authentication.
Opaque Cookie		0x00 [1 Byte + Variable]	The opaque cookie is a server based denial of service detection method. Initially this will be a 1 Byte length field of 0x00 and a variable part of 0 Bytes.
Cipher Suite		0x00 0x04 0xCO 0x2C	This is the field where the client informs the server all the cipher suites that it can support the server later will choose one. The list is presented in order of preference. The first 2 Bytes is the length in Bytes of the list

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

	0x00 0xFF	The second 2 Bytes represent TLS_ECDHE_ECDSA_WITH_AES_GCM_SHA384 The third 2 Bytes represent TLS_EMPTY_RENEGOTIATION_INFO_SCSV
Compression	0x02 0x01 0x00	Represents the compression methods that the client can support. The list is presented in order of preference. The first Byte is the length in Bytes of the list The second Bytes represents DEFLATE compression The third Byte represents none compression

Table 6-20 – Initial Client Hello Message

1.1.1.1 Client Hello Extensions Format

Client Hello Extensions are used to convey additional information or request a modification to the behavior of standard DTLS connections. IANA maintains a list of currently accepted Extension Types which can be found in the Applicable documents section.

The DTLS/TLS extension header consists of a single length field representing the total length of all extensions summed together.

Each DTLS/TLS extension has the following format:

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

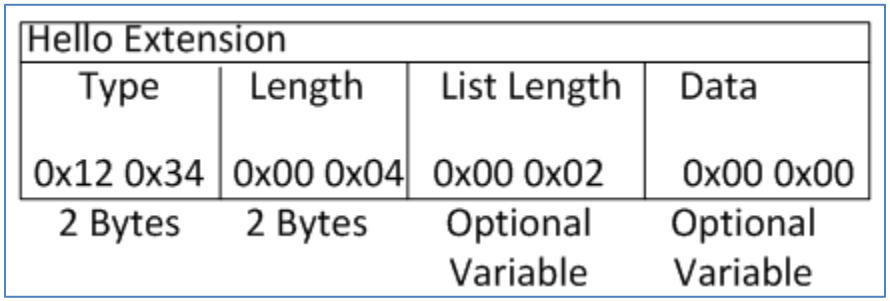


Figure 6-16 – DTLS Hello Extension Format

Field Name	Example Value	Meaning
Type	0x12 0x34 [2 Bytes]	Identifies the Extension name that is being modified or feature being requested.
Length	0x00 0x04 [2 Bytes]	The length of the List Length and Data field in bytes.

List Length	0x0 0 0x0 2 [0 or 2 Byt es]	This field may or may not be present. If it is present, it is two bytes. This field is present every time there is the possibility of a list of items; it represents the number of bytes of the list and is two less than the length field.
Data	0x0 0 0x0 0 [Va ria ble 0 – 65 53 5 Byt es]	The actual requested method for this extension type. This could be blank in the client hello to represent that the client supports this service.

Table 6-21 – Extended Hello Format

1.1.1.2 Client Hello

For purposes of IPS it is recommended that the client maintain at least the following extension capabilities however support for all extensions is recommended. Servers are expected to support most extensions including those listed below.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

1. Elliptic Curve Point Format – Defined in RFC 4492. This extension informs the Gateway that the aircraft can support custom elliptic curves where the points are transmitted in a certain format. This field is recommended when elliptic curve cryptography is used, even when using named curve.
2. Supported Groups – Defined in RFC 4492. This extension informs the Gateway that the aircraft supports named elliptic curves. This field includes a list of all curves supported.
3. Session Ticket TLS – Defined in RFC 5077. This extension informs the Gateway that the aircraft supports session tickets. Tickets can be used to resume sessions with gateways that are load balanced and have a large number of supported aircraft.
4. Signature Algorithms – Defined in RFC 5246 this extension informs the Gateway of all the signature and hashing algorithms that the aircraft supports.
5. Extended Master Secret – Defined in RFC 7627. The Aircraft supports man in the middle attack detection and will generate a master secret that is resistant to man in the middle style of attack.

Field Name		Length Example	List Length (if applicable)	Data Example and meaning
Elliptic Curve		0x	0x00 0x03	0x00 Uncompressed

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Point Format		0 0 0 x 0 5		0x01 Compressed Prime 0x02 Compressed Char2
Supported Groups (AKA Elliptic Curves)		0 x 0 0 0 x 0 4	0x00 0x02	0x00 0x18 secp384r1
Session Ticket TLS		0 x 0 0 0 x 0 0	(--)	-- Supported
Signature Algorithms		0 x 0 0 0 x 0 4	0x00 0x02	0x05 0x03 SHA384 with ECDSA

Extended Master Secret		0 x 0 0 0 x 0 0	(--)	-- Supported

Table 6-22 – Client Hello

The DTLS heartbeats will be handled via the IPS Information messages the aircraft will send periodically. See section 5.6 for more information.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

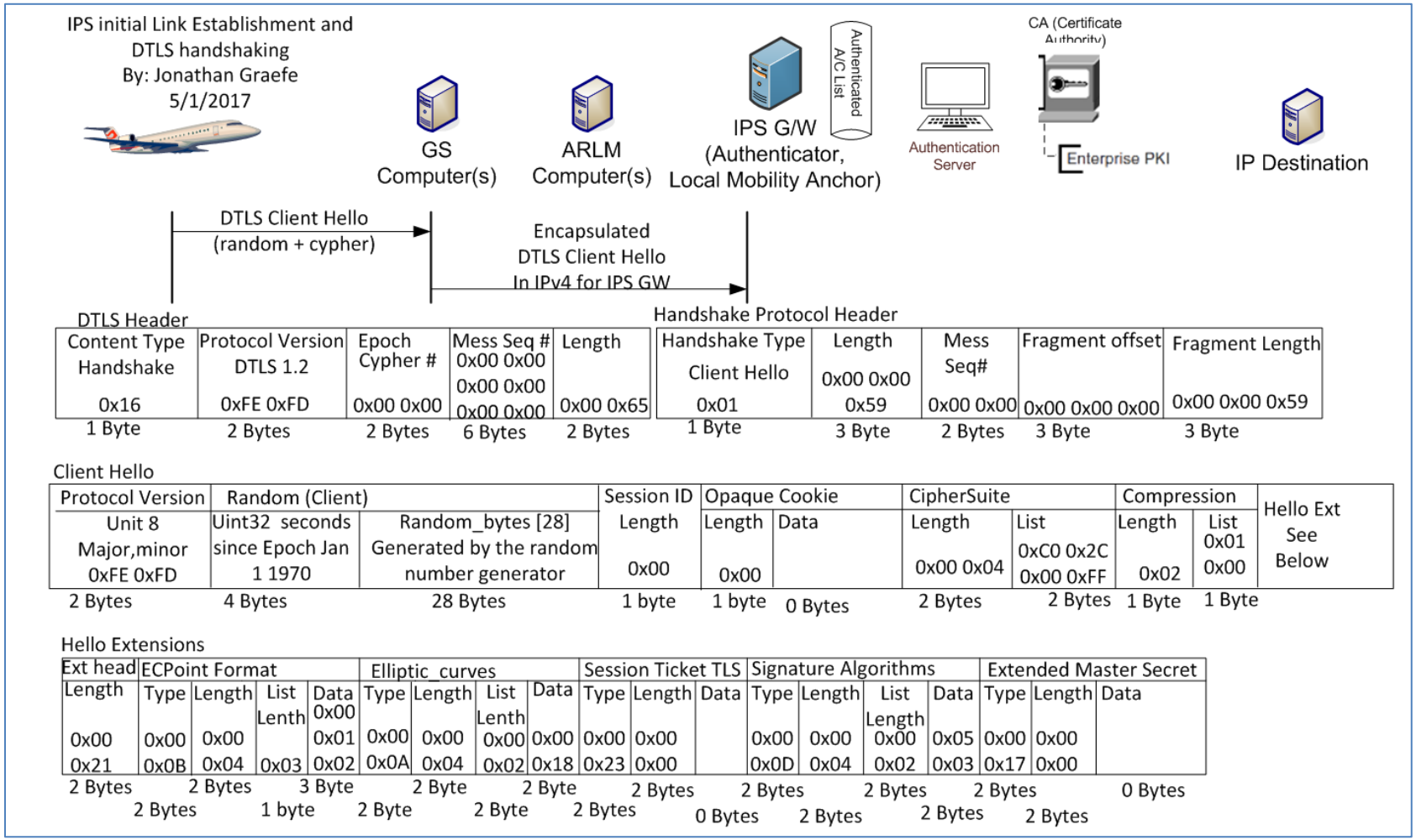


Figure 6-17 – Initial Client Hello

1.9.3 Hello Verify Request

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

In order to detect denial of service (DOS) attacks and also detect replay attacks, the IPS Gateway generates a random opaque cookie and sends it to the aircraft. The aircraft proves that it can receive messages from the IPS Gateway by including the opaque cookie in its follow up client hello message. The opaque cookie is random and shall not be the same as any previous resumable session. The Hello Verify Request is the message that contains the opaque cookie and is detailed below.

The DTLS header fields descriptions are the same as recorded in section 6.1.2 (Initial Client Hello). The Handshake Protocol header is similar to the Initial Client Hello with the exception that the Handshake Type is: 0x03 Hello Verify Req.

The Hello Verify Request Message has the following fields:

Field Name	Example Value	Meaning
Protocol Version	0xFE 0xFD [2 Bytes]	Represents that the Gateway supports the DTLS 1.2 protocol and below. DTLS 1.2 will be used for this handshake.
Length	0x14 [1 Byte]	The Length of the opaque cookie
Opaque Cookie	Varies	This is the cookie the IPS Gateway directs the aircraft to use.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

	[0-255 Bytes]	

Table 6-23 – Hello Verify Request

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

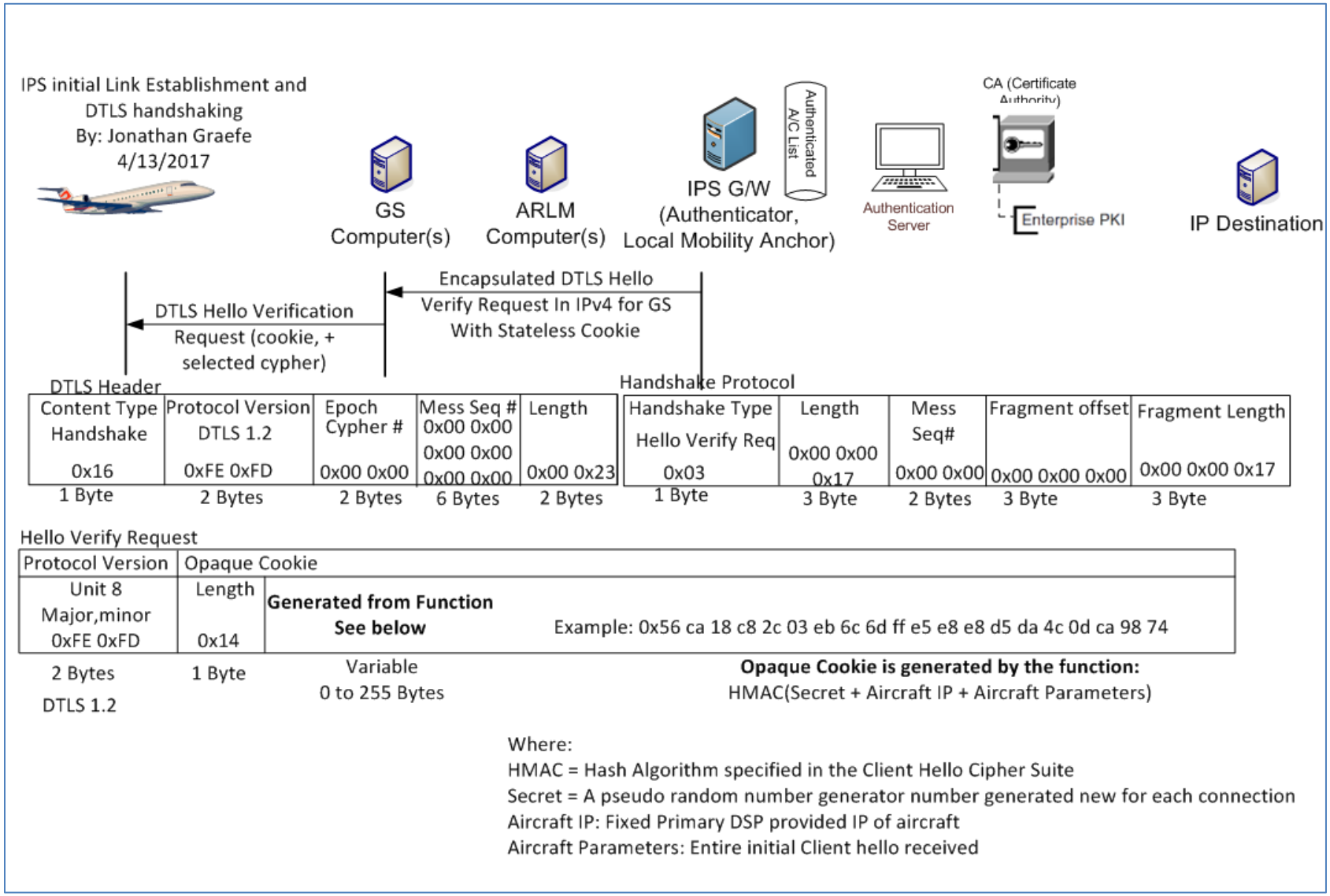


Figure 6-18 – Hello Verify Request

1.9.4 Second Hello Request

The aircraft upon successfully hearing a Hello Verification request from the IPS gateway shall extract the Opaque Cookie and insert it into the Client Hello Message. Transmission of the second Client Hello message will guarantee that the server can successfully send messages to the Aircraft and the aircraft can successfully transmit to the IPS Gateway. The Gateway expects the client hello to remain the same except for a few fields. Any other changes will result in a failed handshake.

The only fields that have changes from the initial client hello are:

Field	Explanation
DTLS Header Message Sequence Number	The Message Sequence number increments for every message sent. Since this is the 2nd message sent by the aircraft it is assigned sequence number 1.
DTLS Header Length	With the addition of the opaque cookie, the length of the packet has increased. Length captures the new length.
Handshake Protocol Header Length	With the addition of the opaque cookie, the length of the packet has increased. Length captures the new length.
Handshake Protocol Header Message Sequence Number	The Message Sequence number increments for every message sent during this handshake the IPS Gateway uses this number to determine that this is the second client hello and it should expect to find an opaque cookie matching what it sent previously.
Handshake Protocol Header Fragment Length	Assuming the message does not require fragmentation this Length would equal the Handshake Protocol Header Length

Client Hello Opaque Cookie Length	Length will change from 0x00 to the length of the opaque cookie.
Client Hello Opaque Cookie Data	This opaque cookie received in the Hello Verify Request will be placed here.

Table 6-24 – Second Hello Request

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

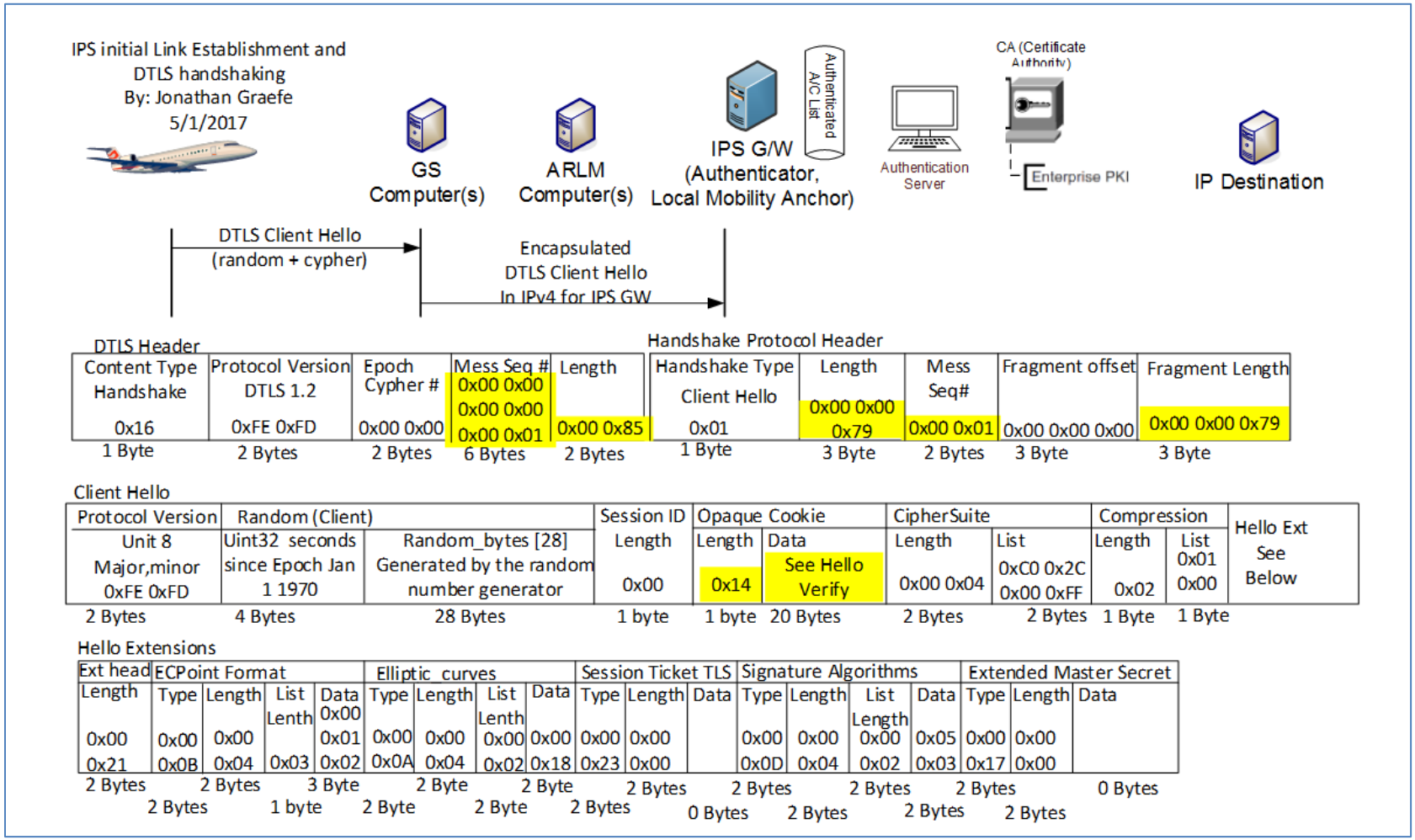


Figure 6-19 – Second DTLS Client Hello

1.9.5 IPS Gateway Authentication Messages

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

The IPS Gateway sends a burst of messages to authenticate itself to the aircraft. These messages include a Server Hello, Server Certificate message, a Server ECDHE Key exchange, a client certificate request and a server finished message.

1.1.1.3 Server Hello

The IPS Gateway initiates a server hello message to the client, specifying the maximum DTLS version number it supports, the cipher it has chosen for this session, compression method and a random integer. These choices are based upon the capabilities presented during the client hello message(s) received from the aircraft earlier. The client is expected to use the server hello message information to build a secured communication method to the IPS Gateway. The Sever Hello Message may take the suggested form detailed below.

The DTLS Header field descriptions are the same as recorded in 6.1.2 (Initial Client Hello); the only difference is in this case the server (IPS Gateway) is sending a message to the client (Aircraft). The Handshake Protocol Header is similar to the Initial Client Hello with the exception that the Handshake Type is 0x02 Server Hello. The details are provided below:

Handshake Protocol Header

Field Name	Example Value	Meaning
Handshake Type	0x02 (1 Byte)	This is a Server Hello Message

Server Hello Message

Field Name	Example Value	Meaning
Protocol Version	0xFE 0xFD [2 Bytes]	The server supports DTLS Version 1.2 and lower

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Random	Varies [4 Bytes + 28 Bytes]	A two part random number that is unique from the client random. The first 4 Bytes represent the seconds since Epoch – January 1, 1970. The Last 28 Bytes are a random number generated by the server. This 28 Bytes should be different from the client random; otherwise a man in the middle attack is possible.
Session ID	Varies [2 Bytes + Variable Bytes]	The first 2 Bytes represent the length of data to follow for this field. The remaining bytes are the session ID issued by the server (IPS Gateway). This number is unique for every active connection. The server may choose to not include a session ID if sessions are not resumable, or if the session resumption is handled via a different method.
CipherSuite	0xC0 0x2C [2 Bytes]	This is the cipher suite chosen by the server (IPS Gateway). The server has chosen from the list presented by the client. It considers the CipherSuite

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

		list in order of client preference. The 2 Bytes represent TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Compression	0x01	Represents the compression method chosen by the server from the list presented by the client. In this case the server has chosen DEFLATE compression.

Table 6-25 – Server Hello Message

Server Hello Extensions

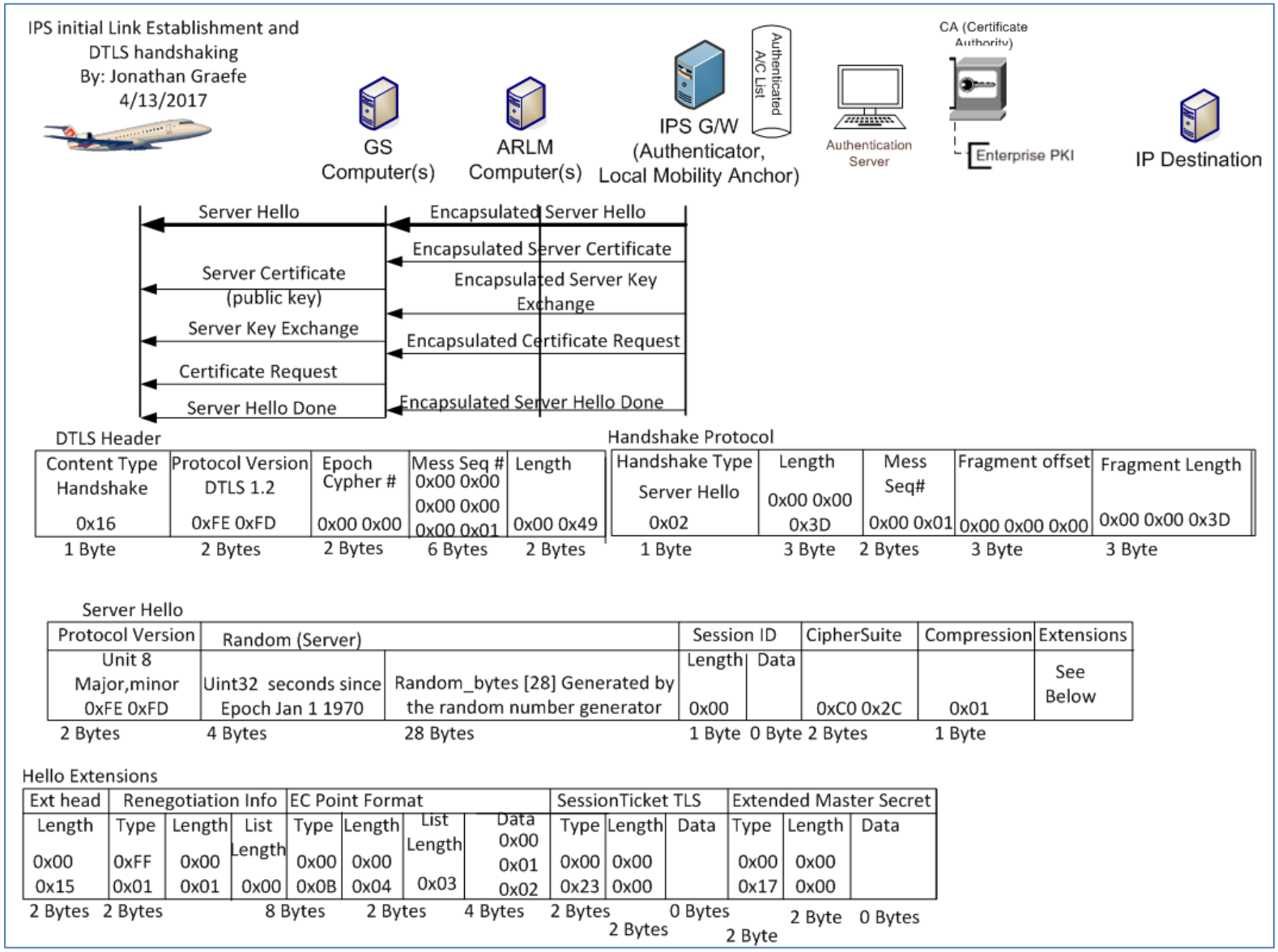
Field Name	Type Value Assigned	Length Example	List Length (if applicable)	Data Example and Meaning
Renegotiation Info	0xFF 0x01	0x00 0x01	0x00	-- Renegotiation Info Supported

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

EC Point Format	0x00 0x0B	0x00 0x04	0x03	0x00 Uncompressed 0x01 Compressed Prime 0x02 Compressed Char2
Session Ticket TLS	0x00 0x23	0x00 0x00	--	-- Session Ticket TLS Supported
Extended Master Secret	0x00 0x17	0x00 0x00	--	-- Extended Master Secret Supported

Table 6-26 – Server Hello Extensions

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS



DTLS Header

Content Type	Protocol Version	Epoch	Mess Seq #	Length
Handshake	DTLS 1.2	Cypher #	0x00 0x00	
			0x00 0x00	
0x16	0xFE 0xFD	0x00 0x00	0x00 0x01	0x00 0x49
1 Byte	2 Bytes	2 Bytes	6 Bytes	2 Bytes

Handshake Protocol

Handshake Type	Length	Mess Seq#	Fragment offset	Fragment Length
Server Hello	0x00 0x00			
0x02	0x3D	0x00 0x01	0x00 0x00 0x00	0x00 0x00 0x3D
1 Byte	3 Byte	2 Bytes	3 Byte	3 Byte

Server Hello

Protocol Version	Random (Server)		Session ID		CipherSuite	Compression	Extensions
Unit 8			Length	Data			
Major,minor	Uint32 seconds since	Random_bytes [28] Generated by					See
0xFE 0xFD	Epoch Jan 1 1970	the random number generator	0x00		0xC0 0x2C	0x01	Below
2 Bytes	4 Bytes	28 Bytes	1 Byte	0 Byte	2 Bytes	1 Byte	

Hello Extensions

Ext head	Renegotiation Info			EC Point Format				SessionTicket TLS			Extended Master Secret		
Length	Type	Length	List Length	Type	Length	List Length	Data	Type	Length	Data	Type	Length	Data
0x00	0xFF	0x00		0x00	0x00		0x00	0x00	0x00		0x00	0x00	
0x15	0x01	0x01	0x00	0x0B	0x04	0x03	0x01	0x23	0x00		0x17	0x00	
							0x02						
2 Bytes	2 Bytes		8 Bytes		2 Bytes		4 Bytes	2 Bytes		0 Bytes		2 Byte	0 Bytes
									2 Bytes		2 Byte		

Figure 6-20 – Server Hello

1.1.1.4 Server Certificate

The IPS Gateway will send its own public x.509 certificate, to the IPS Aircraft. The IPS Gateway may also send a root CA certificate to validate the IPS Gateway's server certificate. It is recommended that the first communication of the day with a service provider be a full x.509 certificate handshake. If any keys need to be updated it can be done via this daily full x.509 handshake. The IPS Gateway's public key will be used if as required to encrypt messages from the IPS Gateway with key tag of 0x0A and 0x30 to 0x3F. The RootCA Certificate is used to validate both the IPS Gateway's server key, and if it is the primary service provider, the aircrafts own key. The aircraft will compare the public key with its directory of service provider's keys to validate that the service provider's key is valid. Aircraft are expected to re-authenticate every 8 hours or at the beginning of each flight whichever comes sooner.

1.1.1.4.1 Server Authentication Methods

There are two types of acceptable authentication.

1) Full X.509 certificate exchange. The x.509 certificate and that of the signing root CAs will be exchanged with the aircraft. The aircraft can then perform a decision tree on whether to accept or not the authenticity of the presented certificate. For purposes of this tree the directory certificate is the last known good certificate stored in the aircraft's CMU. It is expected that all aircraft will support full x.509 certificate exchanges.
2) Modified X.509 certificate exchange. The gateway's X.509 Certificate only will be sent to the aircraft. The aircraft can then perform a decision tree on whether to accept or not the authenticity of the presented certificate. The aircraft should have the gateway's certificate preloaded into either the Primary Service Provider's certificate store or one of the Trusted Companion Certificate slots. If not then abort the connection. If so set the appropriate level of permissions (primary vs trusted companion) and continue the authentication process. The aircraft may send its Certificate only or the entire certificate chain. This type of exchange only works if both the aircraft and gateway certificates clearly indicate their signing authority trust anchor (CA Certificate).

1.1.1.4.2 Decision Tree for X.509 key exchanges

Decision Tree for x.509 key exchanges:

1) Directory IPS Gateway certificate and received IPS Gateway certificate match and are not expired. Then proceed with authentication.
2) Directory IPS Gateway certificate and received certificate match but both are expired. Proceed with authentication. The server will likely follow up with a new certificate to be installed.
3) Directory IPS Gateway certificate and received certificate do not match. Abort the connection.
4) RootCA Certificate is expired, but the directory IPS Gateway certificate and the installed certificate match, both are likely expired. Abort Authentication.
5) RootCA Certificate is expired; directory IPS Gateway certificate and installed certificate do not match. Abort the connection, there may be an imposter IPS Gateway.
6) Directory does not contain a certificate and/or rootCA Certificate for this provider. Switch Providers/media.

1.1.1.4.3 Example Certificate Exchange

The certificate exchange is likely to be fragmented over many packets. This example shows the message as one packet.

Certificate Packet

Field Name	Example Value	Meaning
Certificates Length	0x00 0x02 0x7C [3 Bytes]	Represents the total number of bytes that follow in this message, including all keys and key length headers.
Length of this Key (one for each key)	0x00 0x00 0x3E [3 Bytes]	The length of the key to immediately follow this message. There is one ‘Length of this key’ field for each certificate presented.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

RootCA Certificate	Varies [0 – 24 Bytes]	The Key information for the rootCA key.
Length of this Key	0x00 0x00 0x3B [3 Bytes]	The length of the key to immediately follow this message. There is one 'Length of this key' field for each certificate presented.
IPS Gateway Certificate	Varies [0 – 24 Bytes]	The IPS Gateway certificate key information.

Table 6-27 – Certificate Packet

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

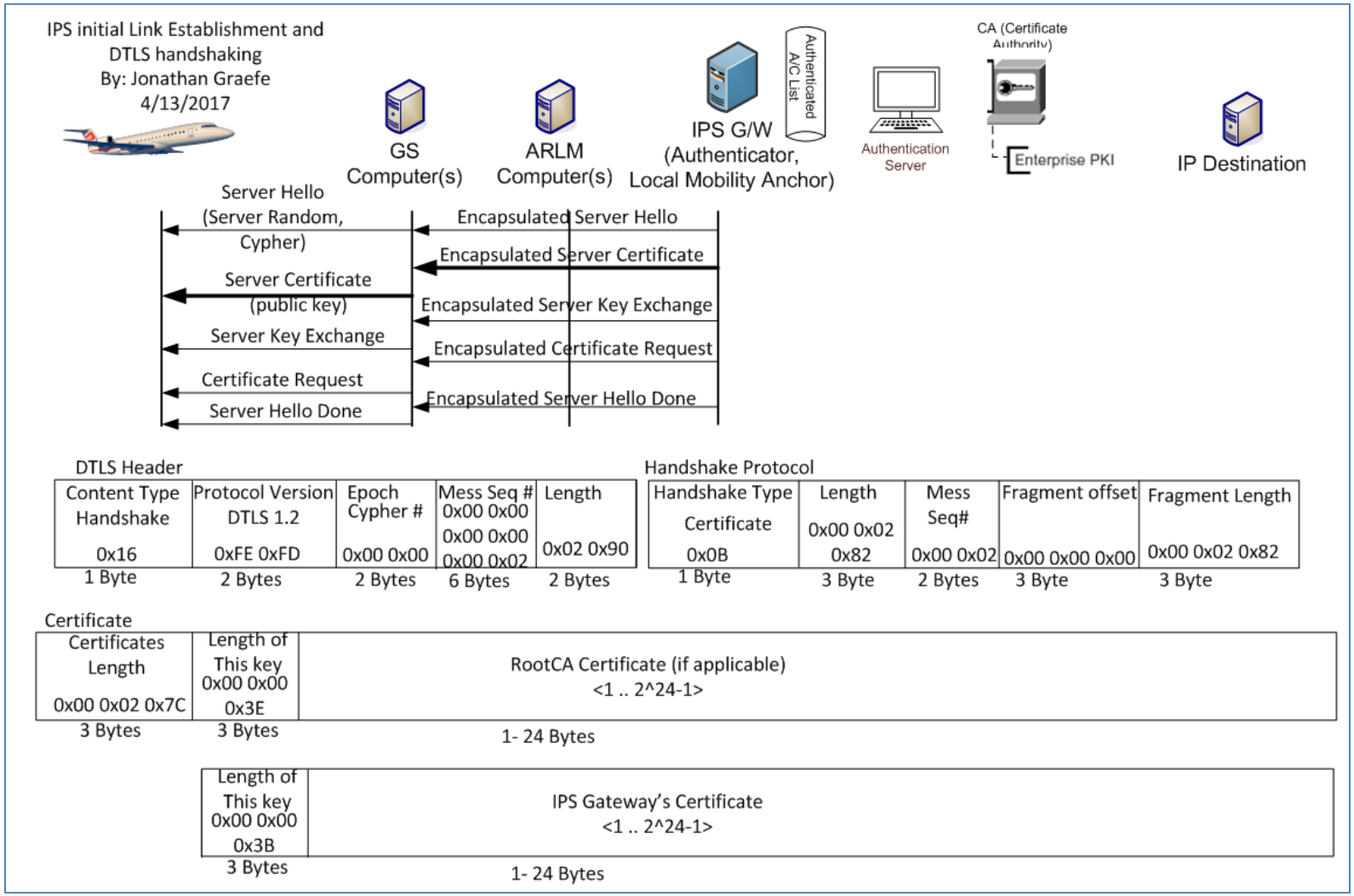


Figure 6-21 – Server Certificate Exchange

1.1.1.5 Server Key Exchange

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

After the IPS Gateway identifies itself using a public key certificate, an Elliptic Curve Diffie-Hellman ephemeral (ECDHE) key is devised for this session only. The ECDHE key is the pre-master secret negotiated key that will later be used to generate the session key. The DTLS Header field descriptions are the same as recorded in (Initial Client Hello); the only difference is in this case the server (IPS Gateway) is sending a message to the client (Aircraft). The Handshake Protocol Header is similar to the Initial Client Hello with the exception that the Handshake Type is 0x0C Key Exchange.

Field	Example	Meaning
Server EC Params – Curve Type	0x03 [1 Byte]	The ECDHE will use a named Curve to generate the public key
Server EC Params – Named Curve	0x00 0x18 [2 Bytes]	The named Curve will be secp384r1
Key Length	0x65	The Length of the Ephemeral ECDH key that will follow in the next field.
Ephemeral ECDH Public Key	Varies [0-255 Bytes]	This is the public ECDHE key, also called the pre-master secret that the IPS Gateway and Aircraft will use to generate the Master Secret.
Signature Hash	0x02 [1 Byte]	SHA384 will be used for Signature hashes
Signature Algorithm	0x03 [1 Byte]	ECDSA will be used to sign hashes

Signature Length	0x00 0x67 [2 Bytes]	The length of the signed hash of this message
Signature	Varies [1 – 65535 Bytes]	The ECDSA Signed SHA 384 hash of the current (This) message, to ensure authenticity in transit.

Table 6-28 – Server Key Exchange

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

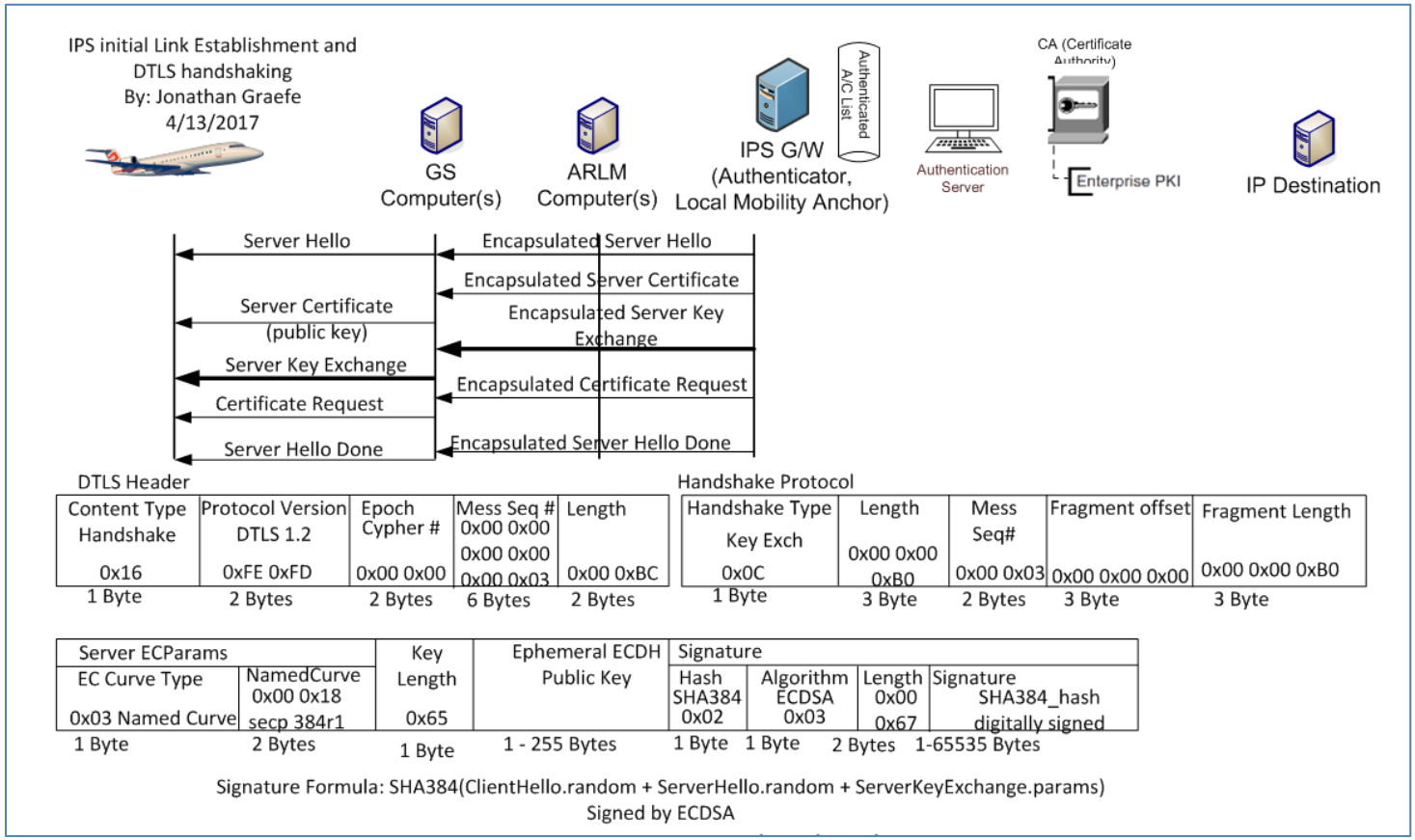


Figure 6-22 - Server Key Exchange (ECDHE)

1.1.1.6 Certificate Request

After sending a Pre-master secret ECDHE key the IPS Gateway begins the process of identifying the aircraft. This message instructs the aircraft what types of authentication keys the IPS Gateway will accept, and the key issuing authorities that are recognized. Similar

to previous sections the DTLS Header remains the same, the Handshake Protocol header's only difference is that the Handshake Type is 0x0D Certificate Request.

Field	Example	Meaning
Client Certificate Type(s)	0x01 0x40 [1-256 Bytes]	This is a list of all supported Certificate Types. The first Byte is the length of the list. Each additional Byte represents a different Certificate Type in this case the length is 1 Byte and the accepted Keys are ECDSA.
Signature and Hash Algorithm	0x01 0x05 0x03 [3 – 256 Bytes]	This is a list of all supported Signature and Hash algorithm pairs. The first Byte is the list length in Bytes. The next Byte represents SHA384 hashing and the third Byte represents ECDSA Key signatures.
Distinguished Names (CA's) List Length	0x00 0xEE [2 Bytes]	This is the length in Bytes of all CA Distinguished names that are accepted as authorized key signers for this IPS Gateway.
X.501 DN Length	0x00 0x75	The length of the CA Distinguished Name (DN) to follow. This field only

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

		represents the very next DN not the entire packet.
CA DN	Id-at-organizationName==ARINC	The name of a CA who's authority is accepted by this IPS Gateway.

Table 6-29 – Client Certificate Request

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

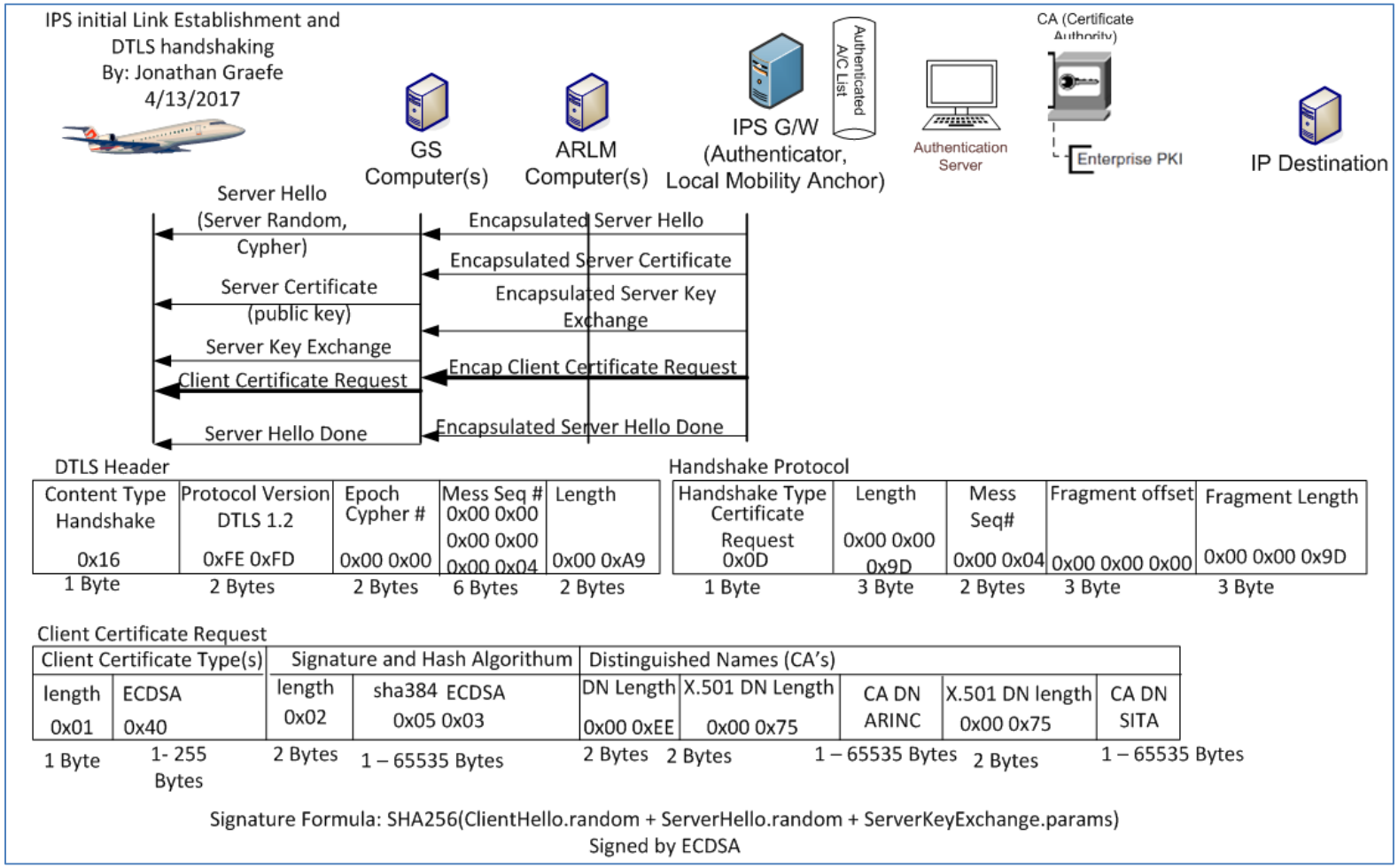


Figure 6-23 – Client Certificate Request

1.1.1.7 Server Hello Done

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

The IPS Gateway indicates at this point that it has finished transmitting identifying information and the Pre-Master Secret to the client. At this point it waits for the client's identifying information.

The only difference between fields explained in previous sections and this message is the Handshake Protocol header – Handshake Type. The Server Hello Done is 0x0E.

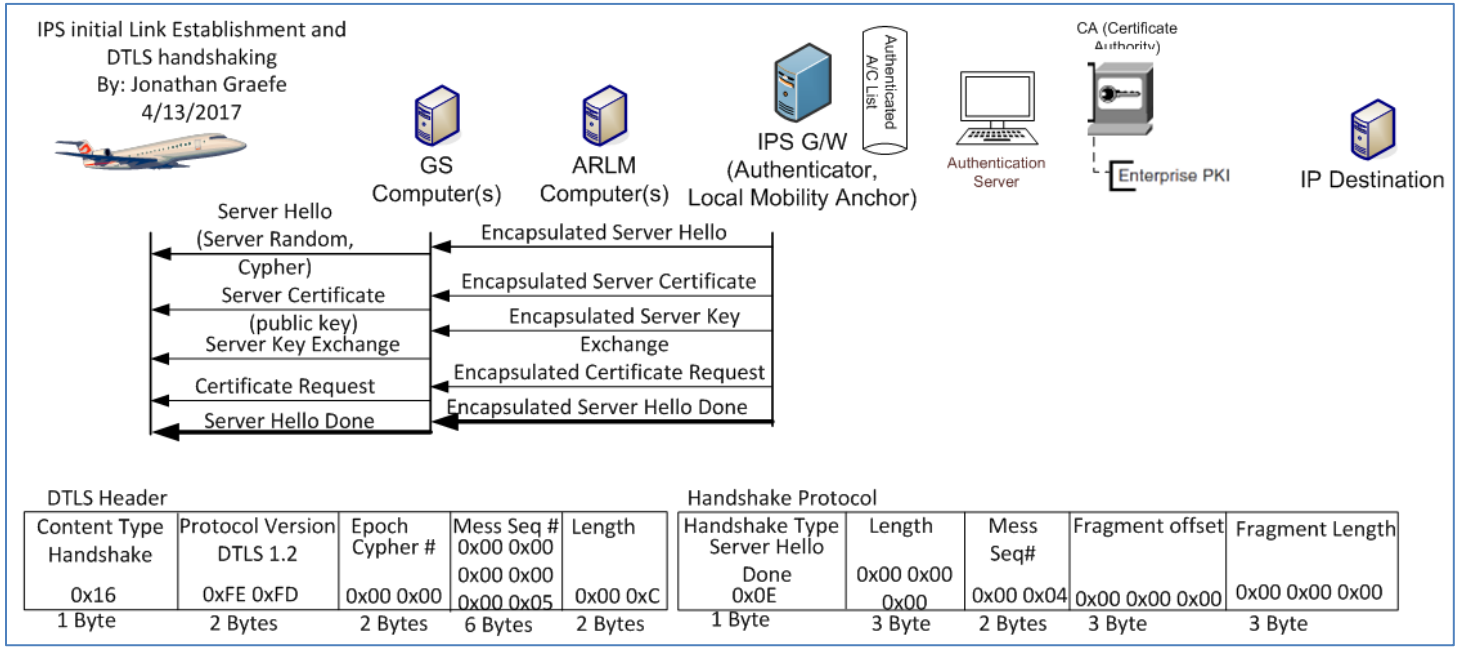


Figure 6-24 – Server Hello Done

1.9.6 Aircraft Authentication Messages

After the server completes identifying itself, sends an ECDHE key and the parameters for authentication types it will accept. It is the client's turn to authenticate itself to the server. This is done by sending an acceptable certificate that matches one of the parameter types accepted by the server and an ECDHE key pre-master secret that the aircraft will use and then starting the encrypted channel process.

1.1.1.8 Client Certificate

The Aircraft will select a certificate that is acceptable to the server. In section 6.1.5.4 it was stated that the Certificate Request that the aircraft received from the server, the server only accepts ECDSA Keys hashed with SHA384 and signed by either ARINC or SITA's private key.. If the aircraft does not have a certificate that matches the requested parameters then the handshake should be aborted. There may not be a roaming agreement in place to support this aircraft. If the aircraft does contain a certificate that matches the parameters the IPS Gateway sent then it can authenticate using that certificate.

The Aircraft can authenticate using a valid public x.509 certificate. It is recommended that the first communication of the day with a service provider be a full x.509 certificate handshake. If any keys need to be updated on the IPS Gateway it can be done via this daily full x.509 handshake. The Aircraft's public key will be used if required to encrypt messages to the IPS Gateway with key tag of 0x0A and 0x30 to 0x3F. The aircraft is expected to re-authenticate every 8 hours or at the beginning of each flight whichever comes sooner.

1.1.1.9 Aircraft Authentication Methods

There are two types of acceptable authentication.

1) Full X.509 certificate exchange. The x.509 certificate and that of the root CA will be exchanged with the IPS Gateway. The IPS Gateway can then perform a decision tree on whether to accept or not the authenticity of the presented keys. For purposes of this tree the directory certificate is the last known good certificate stored on the IPS Gateway. It is expected that all aircraft will support full x.509 certificate exchanges.
2) Modified X.509 certificate exchange. The aircraft's X.509 Certificate only will be sent to the gateway. The gateway can then perform a decision tree on whether to accept or not the authenticity of the presented certificate. The Gateway should have each trusted companion's public certificate preloaded into either the Gateway's certificate store. If not then abort the connection. If so continue the authentication process. The gateway may send its certificate only or the entire certificate chain. This type of exchange only works if both the aircraft and gateway certificates clearly indicate their signing authority trust anchor (CA Certificate).

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

1.1.1.9.1 Decision Tree for X.509 key exchanges

Decision Tree for x.509 key exchanges:

1) Directory aircraft certificate and received aircraft certificate match and are not expired, nor do they appear in the certificate revocation list. Then proceed with authentication.
2) Aircraft Key appears in a Certificate Revocation List. Abort the connection.
3) Directory aircraft certificate and received certificate match but both are expired. Abort authentication, and send a DTLS certificate expired message. Allow the aircraft to login with its one-time use key.
4) Directory aircraft certificate and received certificate do not match. Validate the received aircraft certificate against the directory rootCA certificate for the aircraft's CA provider.
    a. If the received certificate does validate, install the new aircraft certificate in the directory, deleting the old certificate.
    b. If the received certificate does not validate against the rootCA certificate for this provider, abort the connection. This may be an imposter aircraft or service provider.
5) RootCA Certificate is expired for this aircrafts certificate, abort the connection and send a DTLS alert message indicating bad certificate.
6) RootCA Certificate is expired; directory aircraft certificate and installed certificate do not match. Abort the connection, there may be an imposter aircraft.
7) Directory does not contain a certificate for this aircraft, but does have a rootCA certificate that can authenticate the new key. Validate the key against the rootCA certificate and Certificate revocation lists. If valid install aircraft certificate in the directory and allow authentication.
8) Directory does not contain a certificate or rootCA Certificate for this provider. Abort the connection and flag for follow up.

1.1.1.9.2 Example Certificate Exchange

The certificate exchange is likely to be fragmented over many packets. This example shows the message as one packet.

Field Name	Example Value	Meaning

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Certificates Length	0x00 0x02 0x7C [3 Bytes]	Represents the total number of bytes that follow in this message, including all keys and key length headers.
Length of this Key (one for each key)	0x00 0x00 0x3B [3 Bytes]	The length of the key to immediately follow this message. There is one Length of this key field for each certificate presented.
Aircraft Certificate	Varies [0 – 24 Bytes]	Certificate for Aircraft certificate.

Table 6-30 – Certificate Packet

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

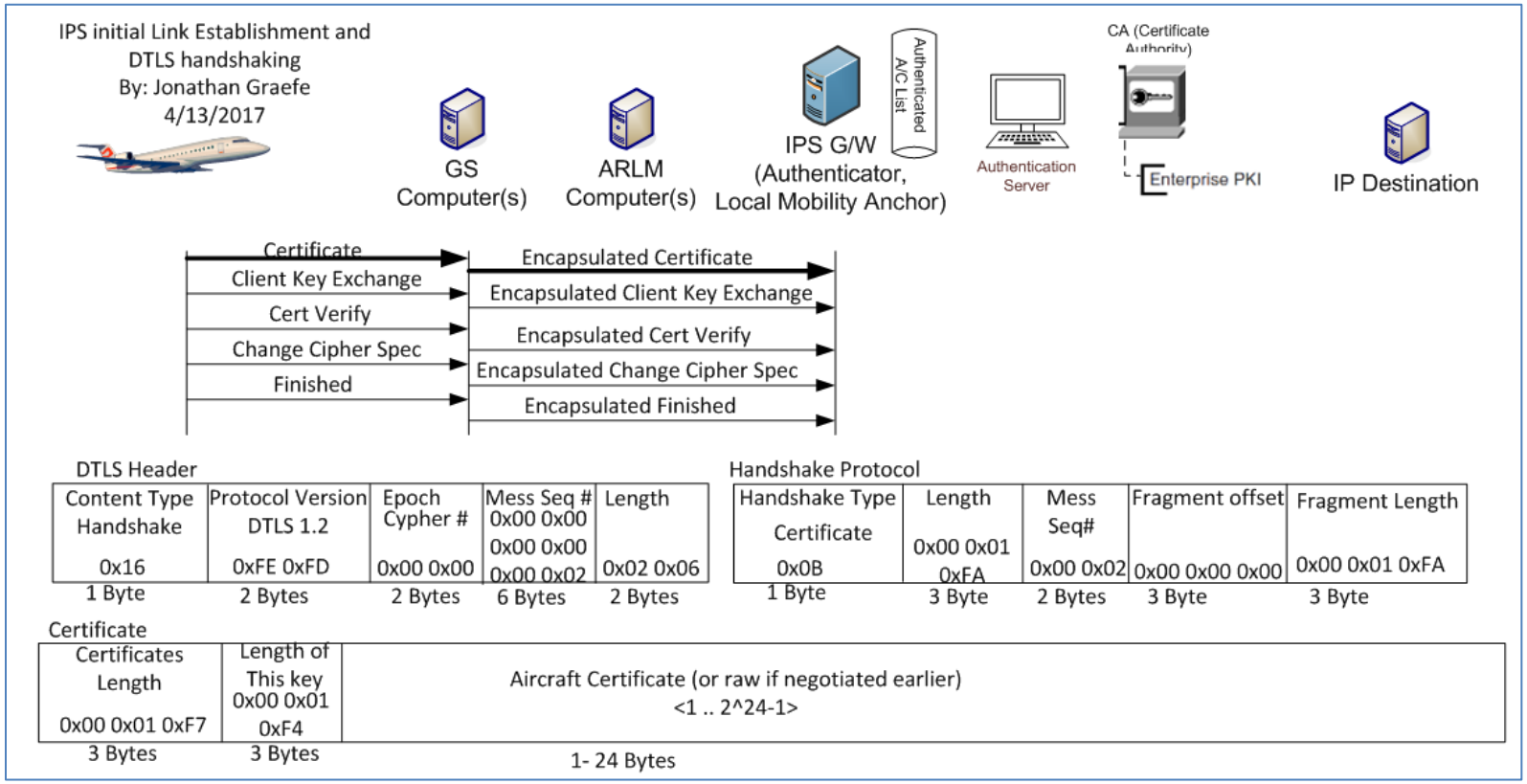


Figure 6-25 – Client Certificate

1.1.1.10 Client Key Exchange

The Aircraft after identifying itself to the server sends an ECDHE key to the IPS Gateway which is also the Pre-Master Secret key. This key with the server key represent some of the information used by both sides to generate the session secret key. The DTLS Header is similar to all other handshake messages. The Handshake protocol Type for Client Key exchange is 0x10.

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Field	Example	Meaning
EC Point Key Length	0x65 [1 Bytes]	Represents the length of the ECDHE key in Bytes to follow
ECPoint – Ephemeral ECDH Key	Varies [1-255 Bytes]	The ECDHE Key also known as the Aircraft's Pre-master Secret

Table 6-31 – Client Key Exchange

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

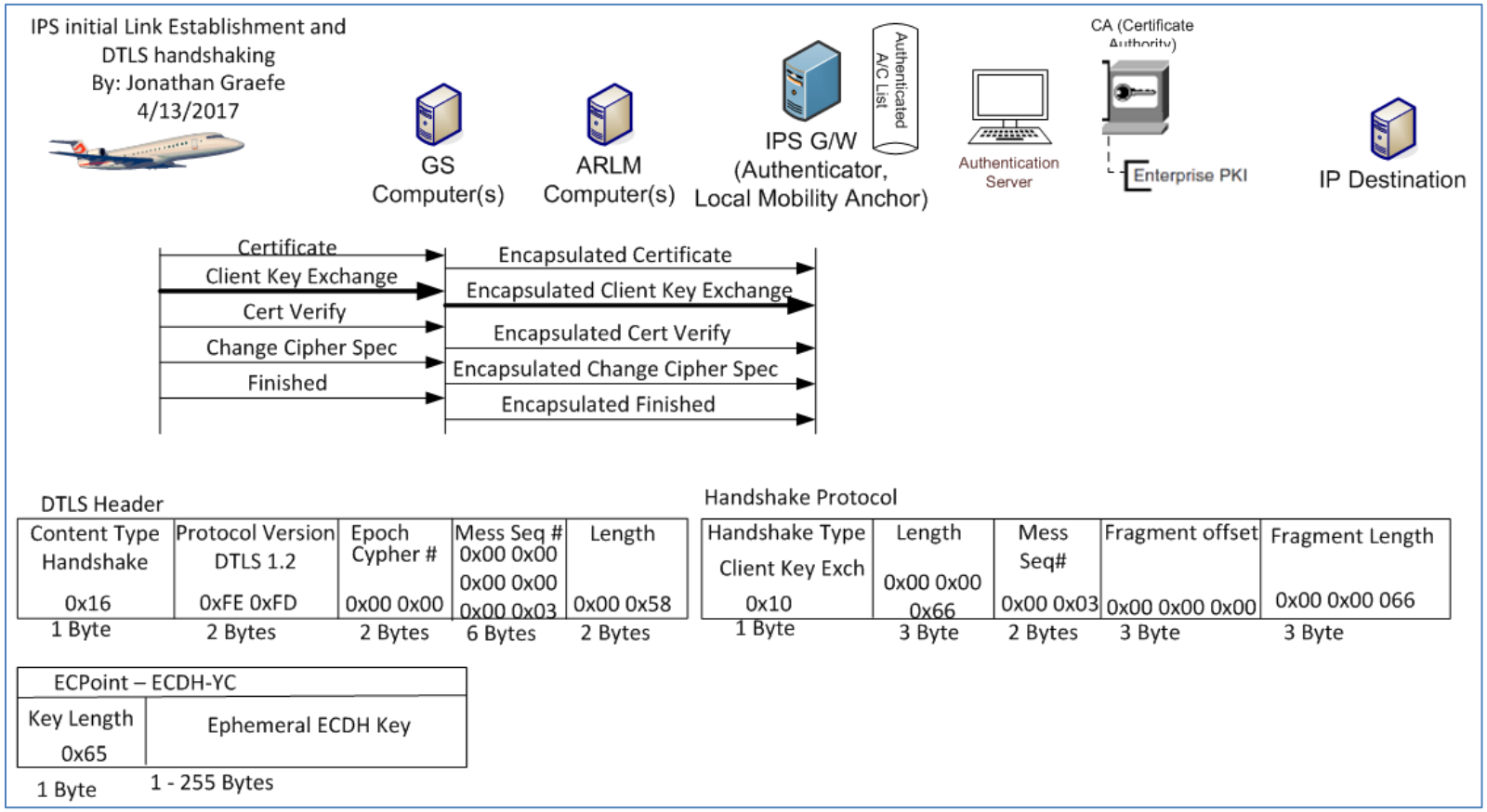


Figure 6-26 – Client Key Exchange

1.1.1.11 Client Certificate Verify

To ensure that the channel is securable, and all messages have been received from the server. The Aircraft now hashes and signs all messages sent and received during the handshake process up to this point. The IPS Gateway can then determine if all messages have been received without modification and determine if the channel is ready for encrypted. After this point both the Aircraft and the

server calculate the Session Master Secret Key which is never itself transmitted but is calculated from all messages up to this point and a seed that is well known by both sides.

Similar to all previous handshake messages the DTLS Header is similar. The Handshake Protocol header is also similar; however the Handshake Type of the client Certificate Verify is 0x0F

Field	Example	Meaning
Hash Type	0x02	The Signature field is using a SHA384 hash of all the handshake messages sent and received thus far.
Signature Type	0x03	The Signature field hash is signed with an ECDSA Private Key, the public certificate was sent earlier via the certificate exchange
Length	0x00 0x66	Represents the length in Bytes of the Signature.
Signature	Varies [1-65535] Bytes	The SHA 384 hash of all handshake messages signed by the ECDSA private key of the aircraft.

Table 6-32 - Certificate Verify Message

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

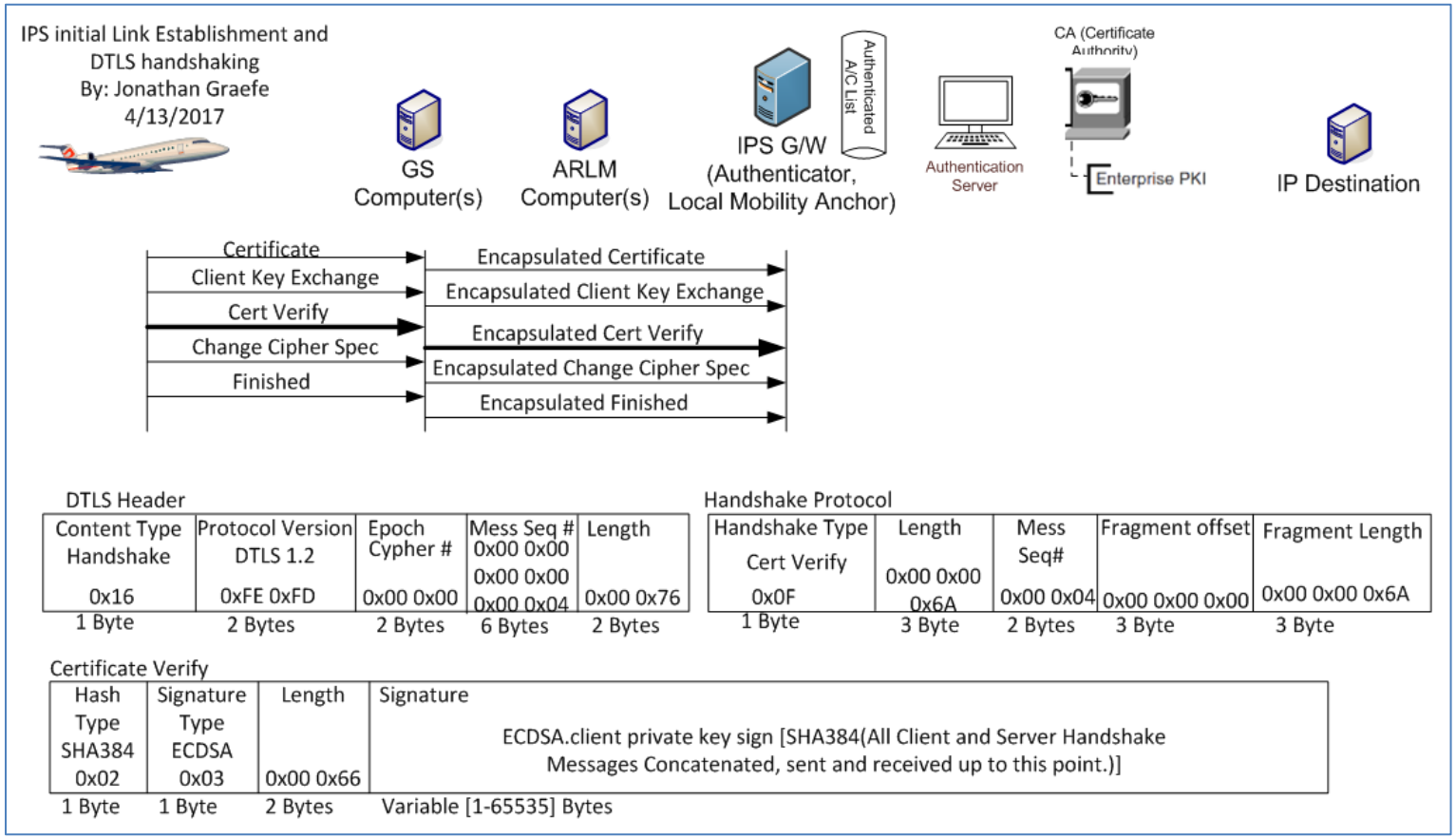


Figure 6-27 – Certificate Verify Message

1.1.1.12 Client Change Cipher Spec

This message indicates that the aircraft will now encrypt all messages sent towards the IPS Gateway using the parameters negotiated earlier. All messages from the aircraft after the change cipher spec will have SHA 384 Message integrity hashes using the

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Aircrafts Private Key for signing. In addition all Messages to the IPS Gateway UDP port 5908 with key tag of 0x0A will be encrypted using the IPS Gateway's Public Key.

The DTLS Header is different for this message. The Content type is 0x14 for Change Cipher Spec message. The Change Cipher Spec message only contains the type 0x01.

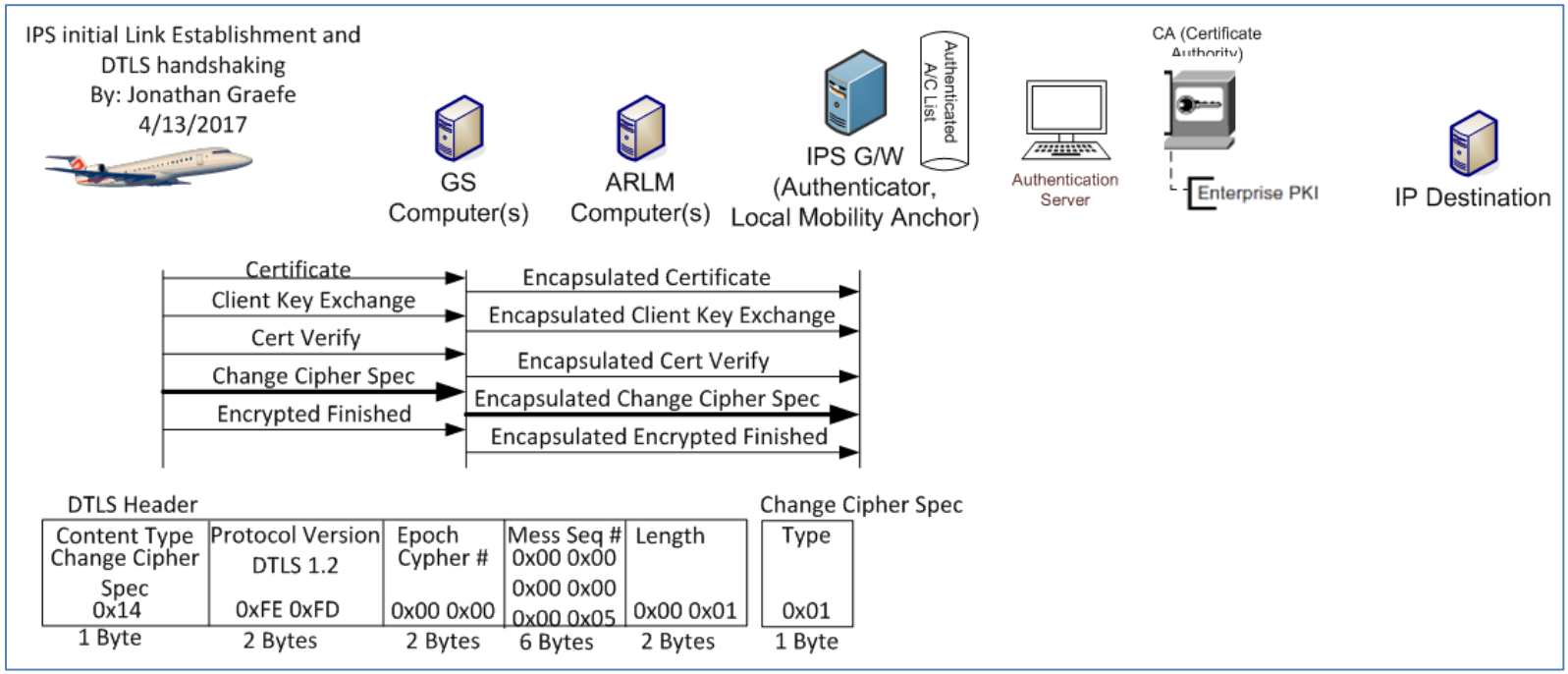


Figure 6-28 – Aircraft Change Cipher Spec

1.1.1.13 Client Finished (Encrypted)

Once the Change Cipher Spec is sent all new messages (not retries of previous messages) are encrypted with the just negotiated cipher, hash and signature methods. The aircraft is now sending a message to the IPS Gateway that it is finished identifying itself to

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

the server and is ready to begin normal traffic. The DTLS header is the standard handshake header. The Handshake Protocol header's Type is 0x14. This message is encrypted. The DTLS header is sent in the clear but the Handshake protocol header and all following materials are encrypted.

The Client Finished message is detailed below:

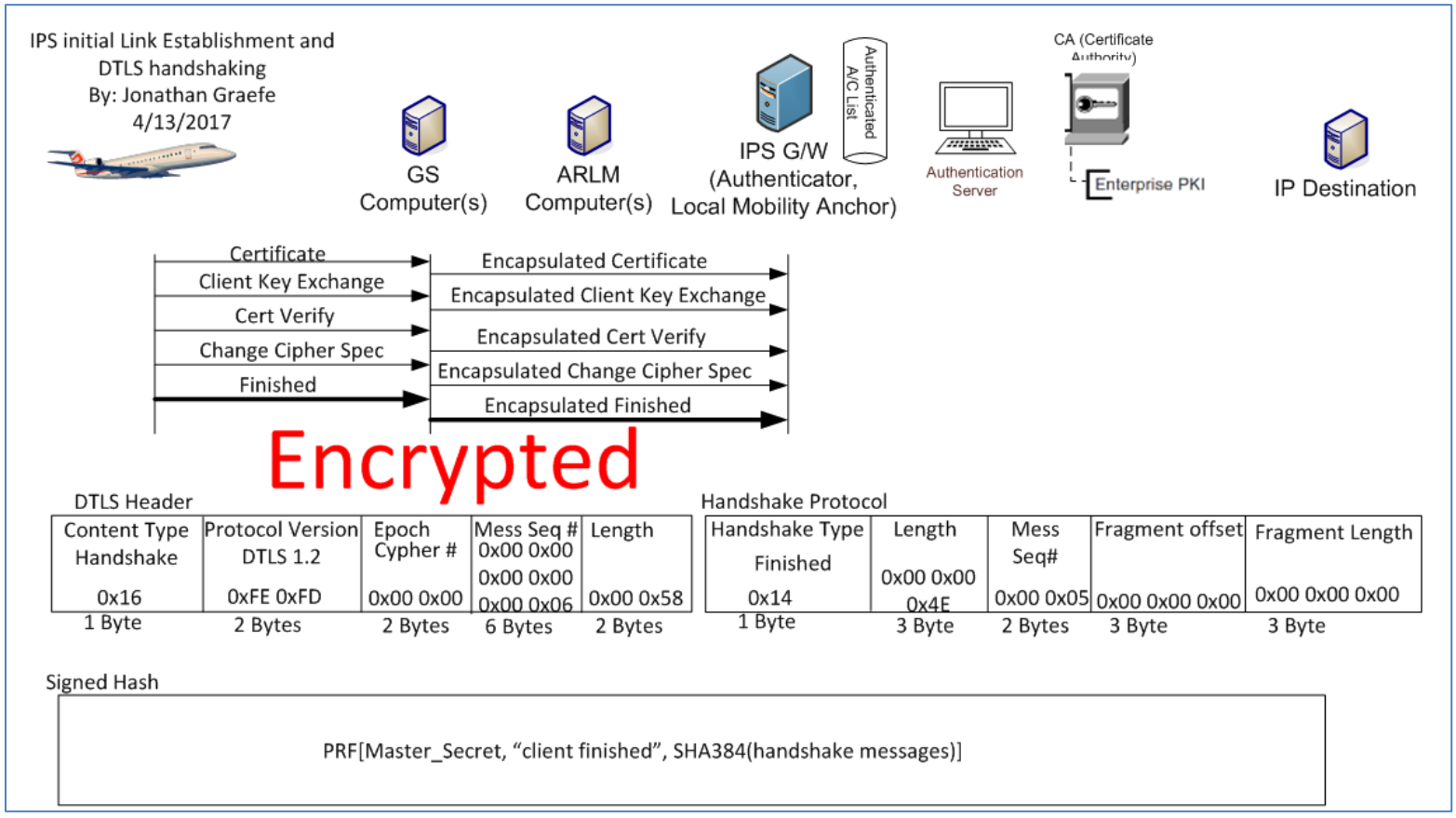


Figure 6-29 – Client Finished (Encrypted)

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

1.9.7 Server Authentication completion

The IPS Gateway completes the DTLS authentication process by providing the aircraft with a session Ticket whereby it can resume a previously lost session as long as the ticket has not yet expired. Then the server starts its side of the encrypted tunnel and finally marks the authentication process as complete.

1.1.1.14 Session Ticket Message

The IPS Gateway issues a Session Ticket so that the aircraft can resume a session as long as the ticket is still valid. Each ticket has an expiration clock that once expired invalidates the ticket. Similar to all handshake messages above the DTLS header is similar. The Handshake Protocol Handshake Type field is 0x04 for Session Ticket.

Field	Example	Meaning
Lifetime Hint	0x00 0x00 0x70 0x80 [4 Bytes]	The number of seconds that this ticket is valid from the point sent. The IPS gateway will keep the ticket and a countdown clock in memory and allow the ticket to be used as long as there is time on the clock. At the point of 0 seconds left the ticket is removed as a valid ticket. The aircraft should use a similar process.
Length	0x02 0xA0 [2 Bytes]	The total length of the session ticket
Ticket	Varies [1 – 65535 Bytes]	The Session Ticket

Table 6-33 – Session Ticket Message

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

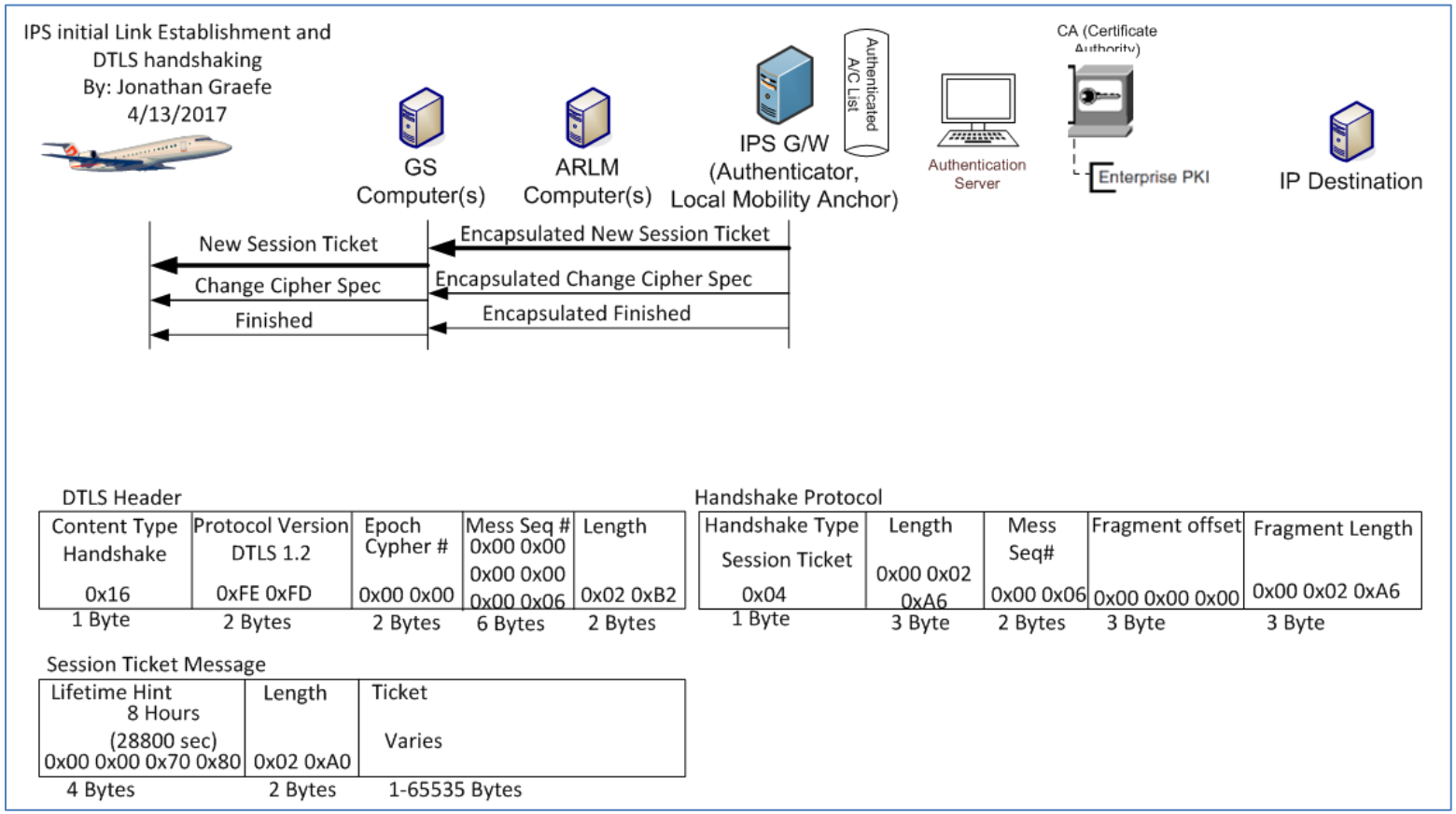


Figure 6-30 – Session Ticket

1.1.1.15 Server Change Cipher Spec

This message indicates that the IPS Gateway will now encrypt all messages sent towards the aircraft using the parameters negotiated earlier. All messages from the IPS Gateway after the change cipher spec will have SHA 384 Message integrity hashes

using the IPS Gateway's Private Key for signing. In addition all further Messages from UDP 5908 with key tag of 0x0A will be encrypted using the Aircraft's Public Key.

The DTLS Header is different for this message. The Content type is 0x14 for Change Cipher Spec message. The Change Cipher Spec message only contains the type 0x01.

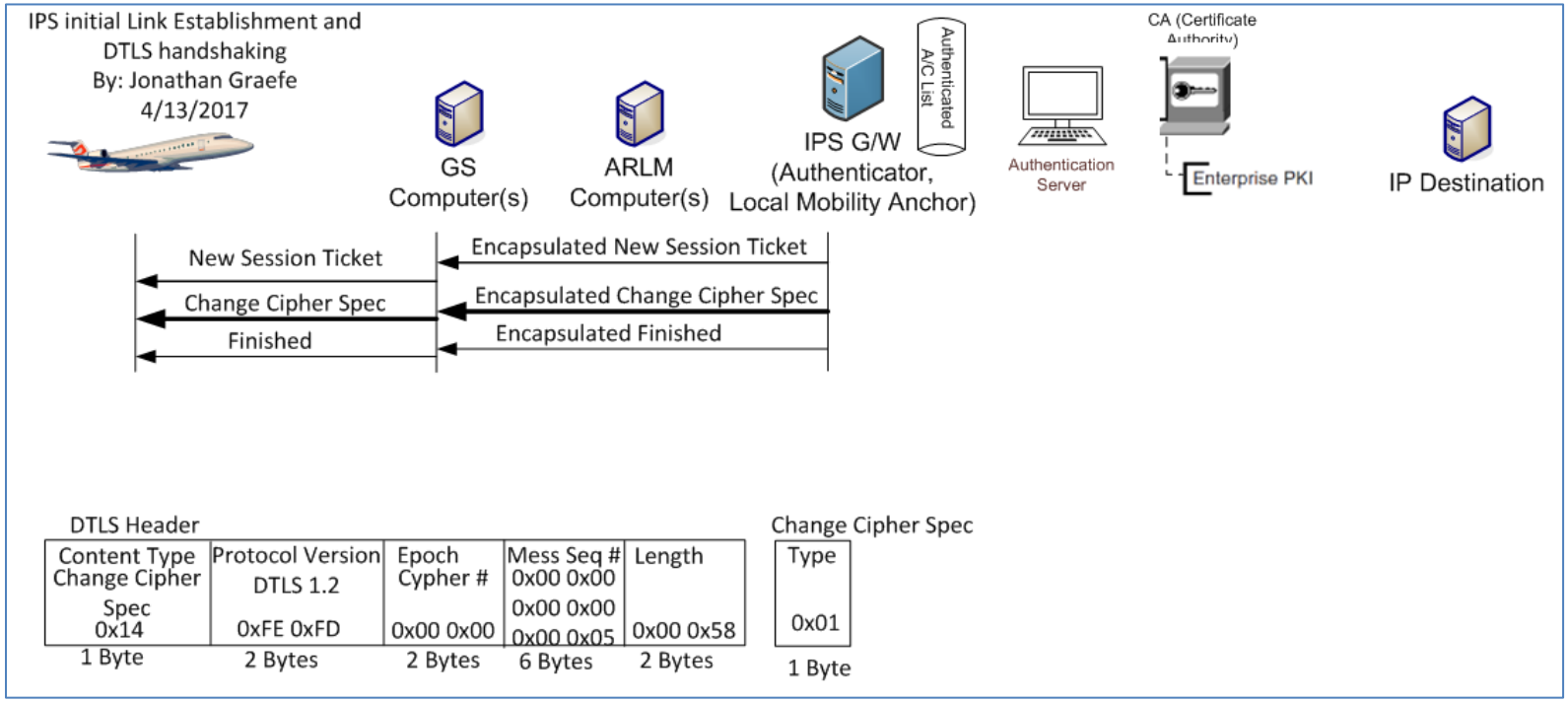


Figure 6-31 – Server Change Cipher Spec

1.1.1.16 Server Finished (Encrypted)

Once the Change Cipher Spec is sent all new messages (not retries of previous messages) are encrypted with the just negotiated cipher, hash and signature methods. The IPS Gateway is now sending a message to the aircraft that it is finished with the

identification process and is ready to begin normal traffic. The DTLS header is the standard handshake header. The Handshake Protocol header's Type is 0x14. The DTLS header is sent in the clear but the Handshake protocol header and all following materials are encrypted.

The Server Finished message is detailed below:

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

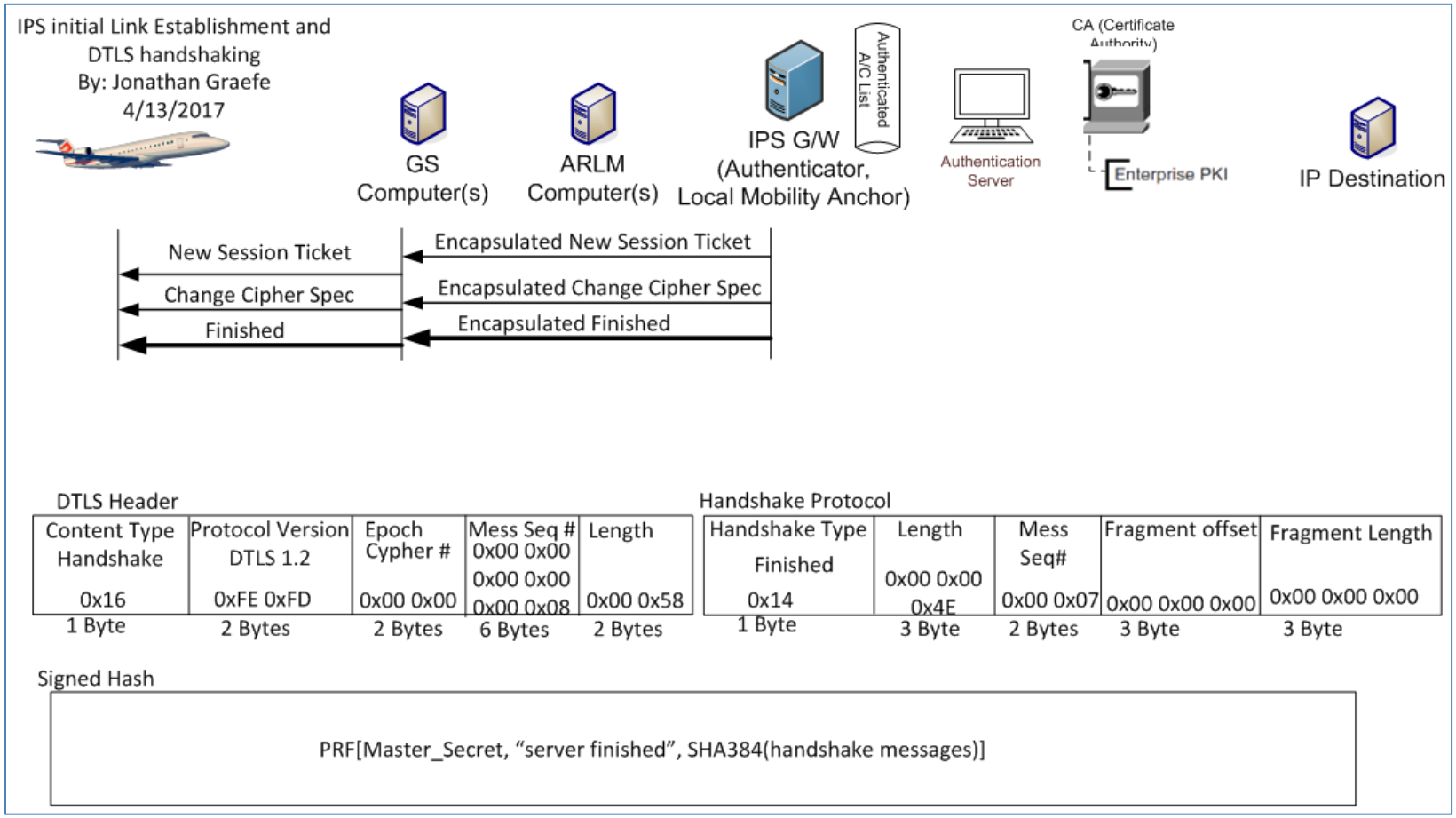


Figure 6-32 – Server Finished

1.9.8 Login information messages

Once the DTLS logon is complete, the gateway and aircraft need a few additional pieces of information to maintain the connection. These Logon Information messages will be encrypted and compressed using the methods already agreed to in the DTLS logon. It should be noted that both the gateway and aircraft will need to decrypt these messages and use their contents to determine the

correct MIC. If the MIC fails then the entire message and its contents should be discarded from memory and the DTLS session torn down.

The Aircraft to ground Login Information Message is expected by the gateway first. This way the gateway knows that the aircraft has otherwise accepted all of the servers DTLS parameters.

Aircraft to Gateway Finalized login information Message		
Field	**Value**	**Example**
Aircraft IPv6 Address	The Global Fixed Mobility address of the avionics.	00FF:0A98:2354:9222:5464:3893:2398:D4A9
Tail # Length	The total length in Bytes of the Tail Number used for ACARS translations	0x00 07
Aircraft Tail Number	The Aircraft's Tail Number used for ACARS Translations	N123456
ATN address	The Aircraft's ATN address. Used for ATN translations	0xA5F098
Random Message Number	A random number that will be the beginning message number for downlinks. This random number will be used for the MIC calculation of this very message.	0x00 00 00 00 55 16

Flight ID Length	The Total Length in Bytes of the Flight ID	0x00 06
Flight ID	The Flight ID	AB1234
MIC	The Message Integrity code generated via the function in section 5.4.3 MIC Generation Function	0x FF 87 12 85

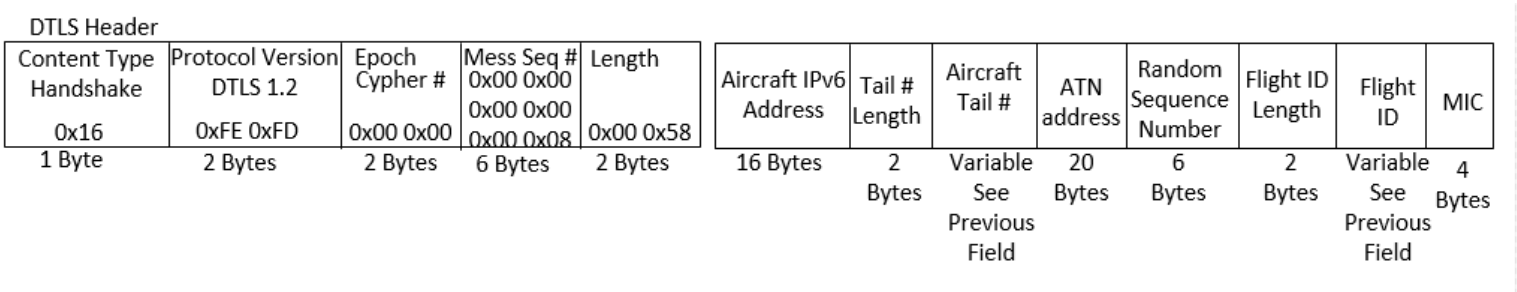


Figure 6-33 – Finalized logon Information Exchange message Aircraft to local gateway

After the login information message from the aircraft is received decoded and MIC checked the gateway will respond with its own logon information message. Informing the aircraft of the random sequence number used for uplink MIC calculations.

Gateway to Aircraft finalized logon information Message		
Field	**Value**	**Example**

APPENDIX A
ATN/IPS GROUND ARCHITECTURE CONSIDERATIONS

Random Message Number	A random number that will be the beginning message number for uplinks. This random number will be used for the MIC calculation of this very message.	0x00 00 00 88 55 16
MIC	The Message Integrity code generated via the function in section 5.4.3 MIC Generation Function	0x F0 82 13 45

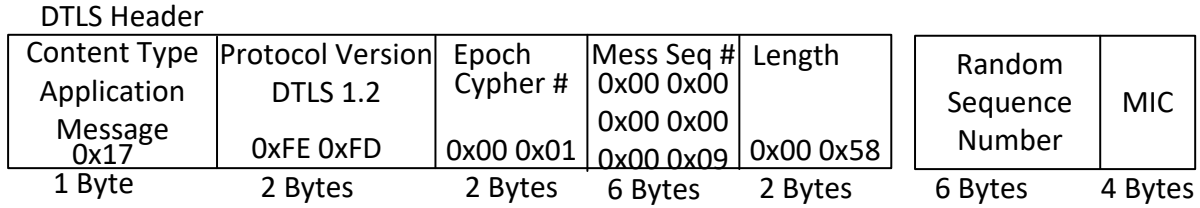


Figure 6-34 - Additional Information Message Gateway to Aircraft

APPENDIX B AIRBUS PROFILES (AIRBUS)

B-1 Federated

B-2 Modular

APPENDIX C BOEING PROFILES (BOEING)

C-1 Federated

C-2 Modular