U. S. Department of Transportation

Federal Aviation Administration

Interface Control Document

NAS-IC-22030001-01

Rev C

9 September 2016

Tower Data Link Services (TDLS)
to
Communications Service Provider (CSP)

INTERFACE CONTROL DOCUMENT

APPROVAL SIGNATURE PAGE

Approval Signatures

Name	Organization	Signature	Date Signed
TDLS Program	AJW-17	Brian P. Peters	9/20/16
FTI Program	AJM-31	Maureen Cedro	9-19-16

NAS-IC-22030001-01 Rev C 9 September 2016			
Revision Record			
REVISION LETTER	DESCRIPTION	DATE	ENTERED BY
	Initial Submission to Configuration Control Board	7/5/2014	AJW-178
Rev A	Updates for Data Comm implementation	12/15/2014	AJW-178
Rev B	Update for compliance with FAA Order 7110.113E and other corrections	02/26/2016	AJW-178
Rev C	Update to remove information identified as SSI. Update to add Aircraft Registration # to DCL Dispatch messages and other corrections	9/9/2016	AJW-178

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

1 SCOPE

This Interface Control Document (ICD) defines the design characteristics for the TDLS Message Service (TDLS-MS) and the Transmission Control Protocol/ Internet Protocol (TCP/IP) interface between Tower Data Link Services (TDLS) and external Non-FAA users referred to as the Communications Service Providers (CSP).

In the context of this document, a CSP is defined as an entity that receives Gate Request (GREQ), Departure Clearance (DCL) Dispatch Message (DCC), Pre-Departure Clearance (PDC), Digital Automatic Terminal Information Service (D-ATIS), and other future messages from TDLS. The CSP also distributes the messages to authorized operators. For example, in the case of a commercial airline, the CSP may send messages to an Airline Operations Center (AOC). The CSP may include the authorized operator and its agents.

Since the CSP is not part of the National Airspace System (NAS), it is important that the interface between TDLS and the CSP is concise and well defined in order to avoid any possible ambiguity or loss of service.

1.1 Summary

Figure 1-1 shows a high-level logical drawing that illustrates the interface between TDLS and the CSP.

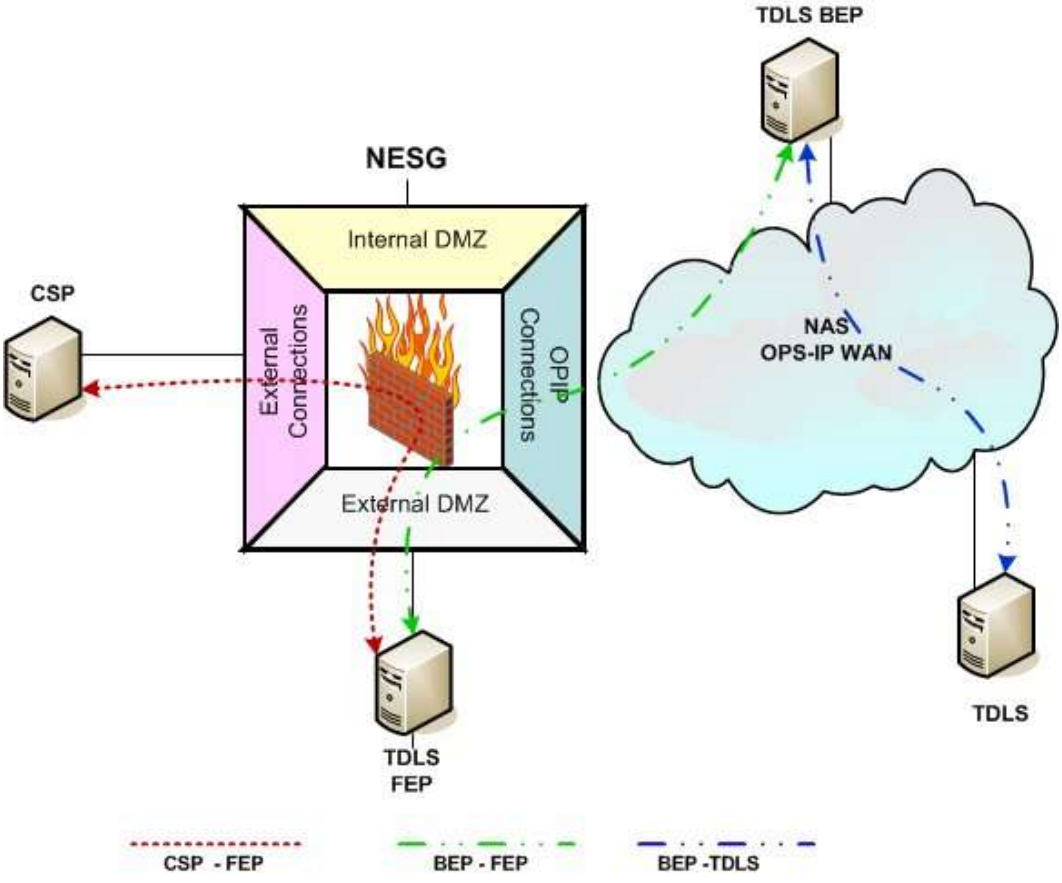

Figure 1-1. Logical View: CSP to TDLS Interface

Communication between the CSP and the TDLS Enterprise is via the NAS Operation Internet Protocol (OPS-IP) network, with the CSP connecting through a NAS Enterprise Security Gateway (NESG).

The TDLS Front End Processor (TDLS_FEP) serves as the proxy (FEP_PROXY) between the CSP and the TDLS Back End Processor (TDLS_BEP). The primary purpose of the TDLS_FEP is to isolate the CSP subsystem from the NAS OPS-IP network. Redundant TDLS_FEPs are connected to the External Demilitarized Zones (DMZ) of the NESGs. The proxy also connects and routes messages to the appropriate TDLS_BEP depending upon availability. The redundant operational TDLS_BEPs are also collocated with the TDLS_FEPs and NESGs.

TDLS is a subsystem within the NAS that is directly connected to the NAS OPS-IP network. FTI will provide the networking infrastructure for TDLS-MS up to the FTI Service Delivery Point (SDP) at the NESG.

The CSP subsystems will be able to access TDLS-MS via redundant NESGs.

The CSP is responsible for the telecommunications infrastructure up to the NESG SDP. Refer to *NAS Enterprise Security Gateway Users Guide Vol II - External Users* for additional information.

This ICD was prepared in accordance with FAA-STD-025f, *Preparation of Interface Documentation.*

1.2 Subsystem Responsibility List

Interfacing systems and responsible FAA program office for each are shown in Table 1-1.

Table 1-1. Organization System Responsibility

SUBSYSTEM	Common Name	Responsible FAA Program Office
TDLS	Tower Data Link System	AJW-17
FTI	FAA Telecommunication Infrastructure	AJM-31
CSP	Communications Service Providers	N/A

2 APPLICABLE DOCUMENTS

The following documents form a part of this ICD to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this ICD, the contents of this ICD shall be the superseding design characterization.

2.1 Government Documents

2.1.1 FAA Orders

Order 1600.6e March 11, 2004	Facility Security Policy
JO 6950.22 February 1978	Maintenance of Electrical Power and Control Cables
Order 1370.114 January 4, 2012	Implementation of FTI Services and Information Security Requirements in the NAS
Order 1370.116 April 16, 2012	Boundary Protection Policy

2.1.2 FAA Specifications

FAA-G-2100H March 2005	Electronic Equipment, General Requirements
FTI July 30, 2012	NAS Enterprise Security Gateway Users Guide Vol II - External Users - Rev 3
NAS-RD-2013 August 11, 2014	National Airspace System Requirements Document
NAS-IR-22030001 Rev C, June 10 2016	Tower Data Link Services (TDLS) to Communications Service Provider (CSP) Interface Requirements Document Rev C

2.1.3 FAA Standards:

FAA-STD-019e December 22, 2005	Lightning and Surge Protection, Grounding, Bonding and Shielding Requirements for Facilities and Electronic Equipment
FAA-STD-025f November 30, 2007	Preparation of Interface Documentation
FAA-STD-039c August 14, 2003	Open System Architecture and Protocols

2.2 Non-Government Documents

ANSI X3.4 December 30, 1986	American National Standard Code for Information Interchange (ASCII)
ANSI X3.41 1974	Code Extension Techniques for Use with the 7-Bit Coded Character Set of ASCII.
IEEE 802.3	Local Area Network (LAN) Protocols

TIA/EIA-568-B.1 April 12, 2001	Commercial Building Telecommunications Cabling Standard
IETF RFC 791 September 1981	Internet Protocol DARPA Internet Program Protocol Specification
IETF RFC 792 September 1981	Internet Control Message Protocol
IETF RFC 793 September 1981	Transmission Control Protocol, updated by RFC 3168
IETF RFC 894 April 1984	A Standard for the Transmission of IP Datagrams over Ethernet Networks
IETF RFC 950 August 1984	Internet Standard Subnetting Procedure
IETF RFC 1323 May 1992	TCP Extensions for High Performance
IETF RFC 1349 July 1992	Type of Service in the Internet Protocol Suite. (Obsoleted by RFC 2474, and updated by RFC 3168)
IETF RFC 2018 October 1996	TCP Selective Acknowledgment Options
IETF RFC 2246 January 1999	Transport Layer Security Protocol (TLS), Version 1.0
IETF RFC 2581 April 1999	TCP Congestion Control
IETF RFC 3168 September 2001	The Addition of Explicit Congestion Notification (ECN) to IP

3 INTERFACE DESIGN CHARACTERISTICS

This section provides the general functional and physical design characteristics for the TCP/IP interface between the TDLS-MS and CSP subsystems.

3.1 General Characteristics

This section provides the general functional design characteristics of the TDLS-MS, which utilizes Simple Message Handling Protocol (SMHP) to exchange GREQ, DCC, PDC and D-ATIS messages with CSP subsystems via TCP/IP. Other than the acknowledgement of messages to the application level, this ICD imposes no requirements on the processing of GREQ, DCC, PDC or D-ATIS messages at the application-level.

3.1.1 Security Characteristics

In accordance with FAA Order 1370.116, Boundary Protection Policy, as amended, the connection between TDLS and external CSP systems is implemented via ATO Authorizing Official (AO) approved secure gateways (NESG). The security controls provided by these gateways are defined in the FTI's Certification and Accreditation (C&A) Package.

External CSP systems must access the TDLS-MS through one or more of the NESGs, in accordance with the *NAS Enterprise Security Gateway Users Guide Vol II - External Users*. The FAA has deployed four of these NESGs.

The Interfacility Communications Engineering Team (IFCET) recommends that if any CSP system deems that access to the TDLS-MS is critical to meet their business needs, then the primary connection should be some form of Dedicated Telecommunications Service (DTS) to one of the two NEMC locations. The IFCET requires that all external CSP systems have the ability to access the TDLS-MS through a minimum of two of the NESGs, such that in the event that the primary connection cannot be established, a connection to the alternate NESG can be used. Note that external CSP systems have the flexibility to mix and match access connection methods, such as:

Two DTS connections

One DTS Connection and One (or two Internet Connections)

Two Internet Connections

Regardless whether access to a NESG is over a DTS or over the public Internet, a Virtual Private Network (VPN) IPSec tunnel must be configured and established to authenticate the external CSP at the network level, in accordance with the requirements specified in the *NAS Enterprise Security Gateway Users Guide Vol II - External Users*.

The TDLS-MS is supported by two TDLS FEPs deployed within the External DMZ of the NESGs. These TDLS_FEPs are the Service Access Points (SAP) for external CSP systems.

Note however, that the locations of the SAPs are de-coupled from the NESGs used by the external CSP systems. External CSPs can connect to any one of the four NESGs and will be able to access both of the TDLS_FEPs.

The CSP is responsible for establishing and maintaining redundant connections to the TDLS-MS via redundant TDLS_FEPs which serve as the SAPs for the CSP.

External CSP systems that utilize the TDLS-MS offering are required to successfully register with the IFCET via the TDLS-MS Request for Service (RFS) process before TDLS-MS messages can be exchanged.

The IFCET uses the RFS process to identify the external CSP system, issue client/server certificates for authentication, and document the external CSP connection to the NAS in the following documents:

Memorandum of Agreement (MOA) between the FAA and the CSP

Interconnection Security Agreement (ISA) for TDLS-MS

FTI IP Supplemental Form (IPSF)

All external CSP systems are required to meet the requirements of the TDLS-MS in accordance with NAS-IR-22030001 Rev C *TDLS to CSP Interface Requirements Document (IRD)* and this ICD.

All external CSP systems must be tested for service compliance by the IFCET as part of the RFS process. This is accomplished by the external CSP utilizing the TDLS Test Bed services hosted on the FTI National Test Bed (FNTB), which can be accessed by the external CSP systems through the NESG connected to the FNTB.

All equipment and cabling to support TDLS-MS fault-tolerant connections to the NESG point of demarcation are subject to FAA physical security policies. The FAA is responsible for the security of the originating equipment and transmission equipment up to the points of demarcation of the interface. This ICD does not specify security capabilities outside of TDLS-MS. Refer to *NAS Enterprise Security Gateway Users Guide Vol II - External Users* for security requirements pertaining to the external CSP connections to the NESGs.

The NESGs provides TDLS-MS with all of the necessary functional security measures (such as firewalls, DMZ, authentication, proxy services, packet inspection, etc.) required to support and protect the TCP/IP interface to the NAS OPS-IP network.

CSP subsystems must connect to TDLS-MS through the NESG SDP and the TDLS_FEP proxy. The TDLS_FEP provides isolation between the CSP subsystem and the NAS OPS-IP network and serves as a proxy between the CSP and TDLS-MS. The TDLS_FEP is collocated with the NESG and connects directly to the External DMZ of the NESG.

Both the TDLS_FEPs and TDLS_BEPs perform validation on incoming socket connections, verifying that the peer IP address is valid for the port, with which it is attempting to establish a connection.

In addition, the CSP client application and TDLS-MS server application are required to authenticate each other using X509 certificates. All failed connection attempts will result in the socket connection being closed and a security alert message being generated.

3.1.2 Organizational System Responsibility

The IFCET, AJW-178, is responsible for the Second Level Engineering Support of the TDLS-MS system. The IFCET and the CSP will also be responsible for the testing of the software interface between the CSP and TDLS-MS on the FTI National Test Bed (FNTB) network during functional verification of the interface.

FTI provides the FAA's NAS OPS-IP network that has points of presence at FAA facilities throughout the NAS. The TDLS-MS subsystems connect directly to the NAS OPS-IP network and FTI provides the communications infrastructure services between the TDLS-MS and the NESG SDP. Access by CSP subsystems to TDLS-MS will be via NESGs.

The CSP will complete the MOA before the RFS process can be started. The CSP will be added to the Appendix A of the Air Traffic Organization (ATO) Interconnect Security Agreement (ISA), which is a security agreement between the IFCET and ATO security pertaining to TDLS-MS security when the MOA is in place.

The CSP will contact the IFCET to start the TDLS-MS RFS process. Refer to section 4.1, Responsibility for Verification, of this ICD for contact information.

During the TDLS-MS RFS process, the CSP and the IFCET will agree on the requirements stated in NAS-IR-22030001 Rev C.

The FTI program office will work with the CSP on the details of connecting to the NAS OPS-IP NESG SDPs and to the NESG attached to the FNTB network. CSPs that have a preexisting VPN connection to the NESG SDP will be able to use the existing VPN to connect to the TDLS_FEPs. This will require reconfiguration of the preexisting VPN to allow the TDLS-MS traffic. The CSP will be responsible for the communications infrastructure services leading up to the NESG SDP. For further information pertaining to the supported types of connectivity at the NESG SDP, refer to *NAS Enterprise Security Gateway Users Guide Vol II - External Users*

Before functional verification testing, the CSP will submit a digital certificate request to the IFCET. The IFCET will act as the Certification Authority (CA) and will provide the CSP with the CSP's client certificate along with the IFCET's CA certificate, which will be required to validate the CSP client and TDLS server certificates.

Once the functional verification of the TCP/IP interface between the CSP subsystem and TDLS-MS is complete, the IFCET will provide the CSP with IP address and port information for connecting to the TDLS_FEPs which are connect to the external DMZ of the NESGs.

3.1.3 Other General Characteristics

CSP General Characteristics

The NESG provides a fault-tolerant interface between the CSP subsystems and the TDLS-MS. For data path redundancy, the CSP subsystem will connect to multiple NESG SDPs to access redundant TDLS-MS SAPs. Refer to *NAS Enterprise Security Gateway Users Guide Vol II - External Users* for additional connectivity information.

The TDLS-MS interface has been designed to allow interface certification without impacting (24 hours per day, seven days per week) full-service.

The CSP client application will be designed to support the exchange of GREQ, DCC, PDC and D-ATIS messages via this TCP/IP interface.

TDLS General Characteristics

TDLS-MS is a Store-and-Forward message service that provides alternate routing, utilizing two TDLS_BEPs.

TDLS-MS supports the exchange of GREQ, DCC, PDC and D-ATIS messages between the CSP and the TDLS_BEP via the TCP/IP interface described in this ICD. The lower layers of TDLS-MS message format comply with FAA-STD-039c, Open System Architecture and Protocols.

TDLS-MS uses an application level protocol, SMHP, which provides application message acknowledgement, connection validation and client/server authentication utilizing Transport Layer Security (TLS) protocol. Refer to Appendix A for additional information on SMHP.

3.2 Functional Design Characteristics

This subsection describes the functional characteristics of the TDLS-MS TCP/IP interface. It identifies the Application Processes (AP), the information transferred between them, error handling, and correlation to the Internet Protocol Stack.

General Service Functional Requirements

The TDLS_BEP and remote TDLS subsystems connect directly to the NAS OPS-IP network and communicate with the CSP subsystem through the NESG and the TDLS_FEP.

The TDLS_FEP resides on the External DMZ of the NESG and serves as a proxy (FEP_PROXY) between the TDLS_BEP and the external CSP subsystem in accordance with NAS-RD-2013, National Airspace System (NAS) System Requirements Document.

The FEP_PROXY application has the ability to connect to either TDLS_BEP and provides automated failover and fallback services between the local and alternate TDLS_BEPs.

Once the FEP_PROXY listener accepts a connection, it spawns a child proxy process to service the incoming CSP client. This assures process isolation between CSPs when multiple CSPs connect through the same TDLS_FEP. When the child proxy process establishes a TCP/IP connection to the TDLS_BEP, it allows the host operating system to select the ephemeral local port number to bind to the address.

Figure 3-1 depicts the logical flow of the FEP_PROXY application.

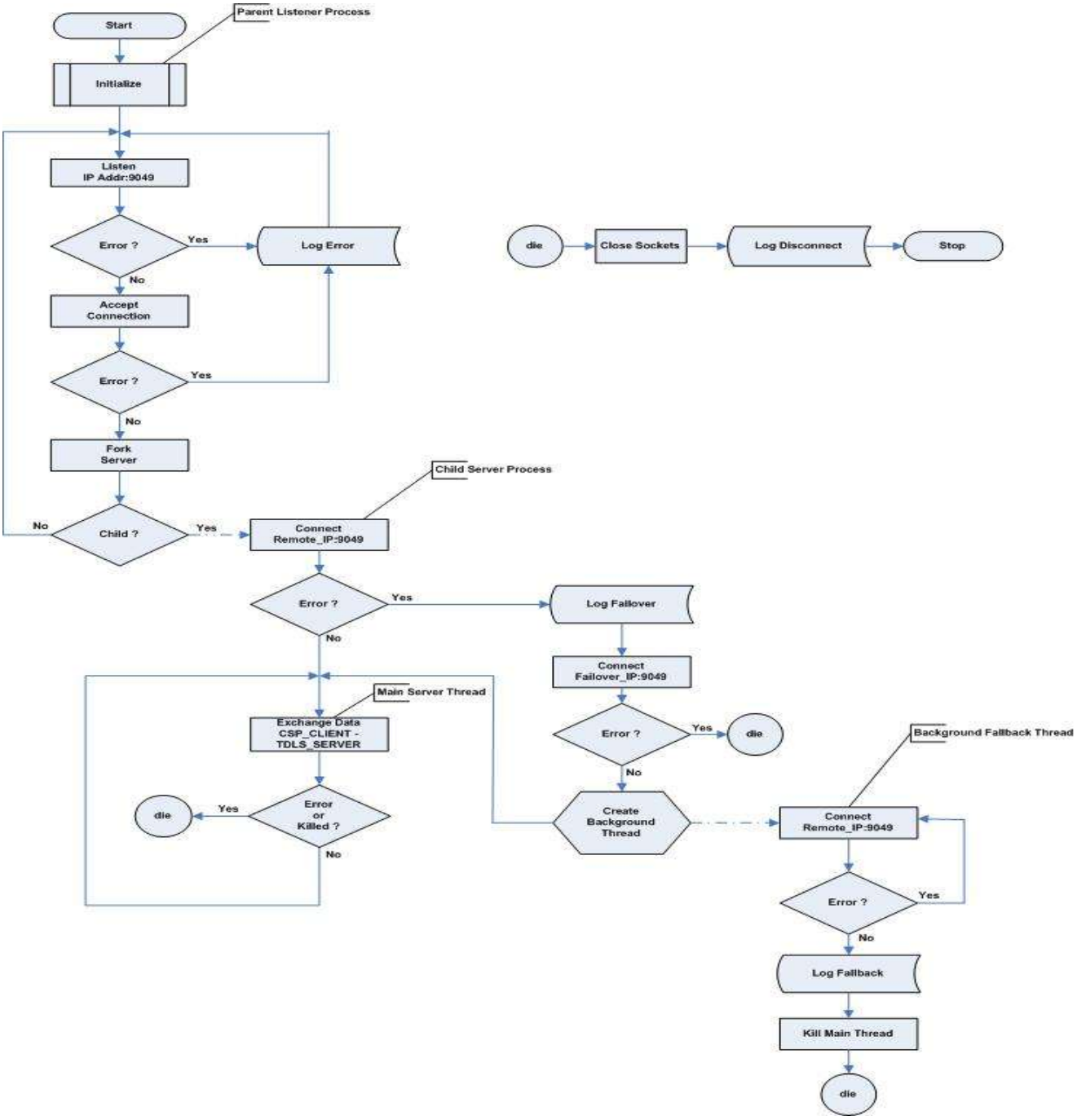

Figure 3-1. TDLS_FEP Proxy Service High Level Design

A further explanation of the FEP_PROXY application's failover and fallback mechanism will be discussed in Section 3.2.1.6, Error Handling Requirements, of this ICD.

3.2.1 Application Processes and Message Requirements

An AP is defined as an identifiable set of cooperating capabilities within a system that executes one or more information processing tasks. The following paragraphs describe the application processes that allow the TDLS-MS to send/receive GREQ, DCC, PDC and D-ATIS messages to/from the CSP subsystems.

3.2.1.1 Identification of Each Application Process

TDLS-MS uses the TDLS_BEP server application as its AP (TDLS_SERVER).

The CSP subsystem uses its client application as its AP (CSP_CLIENT).

The CSP_CLIENT connects to the TDLS_SERVER via the FEP_PROXY application.

3.2.1.2 Application Process Capability Requirements

CSP Application Process Capability Requirements

The CSP_CLIENT will initiate and maintain the TCP socket connection, i.e. the TDLS_SERVER will act as the server in the client-server paradigm. In this relationship, the CSP_CLIENT will always be responsible for establishing/reestablishing the socket connection to TDLS_FEP.

When the CSP_CLIENT establishes a TCP/IP connection to the TDLS_FEP on destination port 9049, it allows the host operating system to select the experimental local port number to bind to the address.

After establishing the virtual connection between the CSP_CLIENT and the TDLS_SERVER, the client and server applications exchange client and server certificates during the TLS handshake.

If the connection between the CSP_CLIENT and the TDLS_FEP is broken, the CSP_CLIENT should reestablish the connection within 30 seconds or less.

Figure 3-2 depicts an example high-level design of the CSP_CLIENT application.

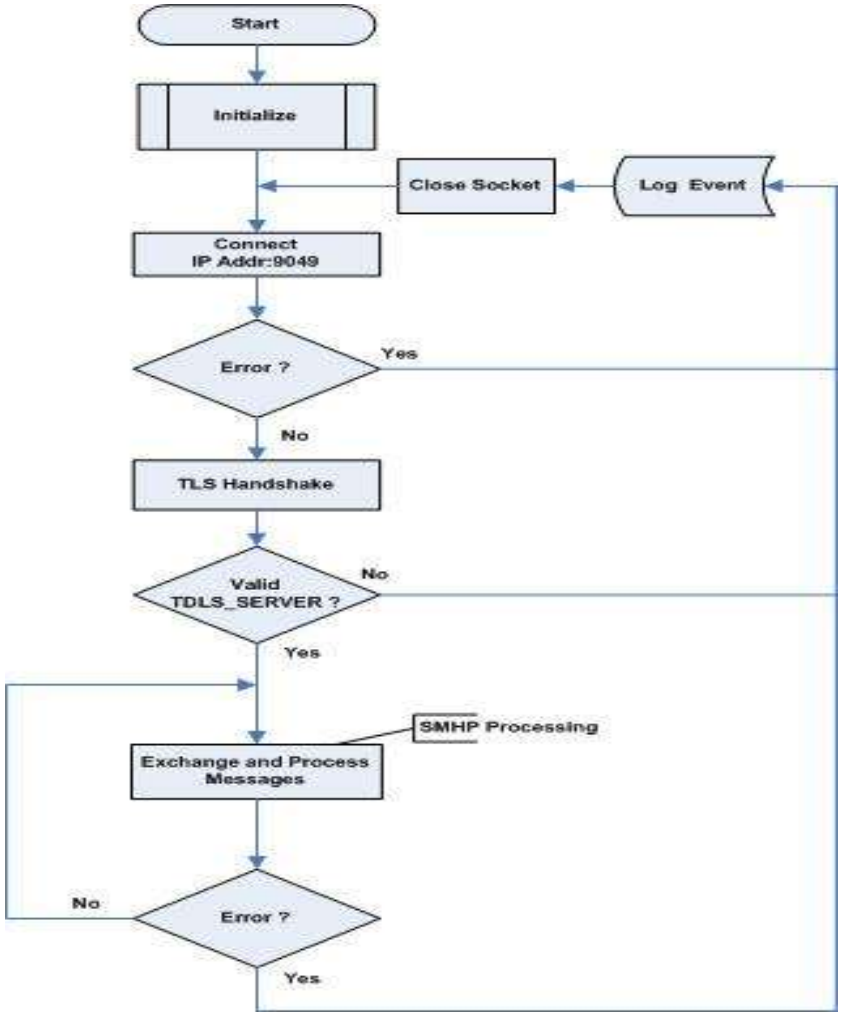

Figure 3-2. Example CSP_CLIENT High-Level Design

The CSP_CLIENT will utilize SMHP to exchange unencrypted GREQ, DCC, PDC and D-ATIS messages between the TDLS_SERVER and the CSP_CLIENT. Refer to Appendix A, *SMHP Specification* for additional information about SMHP.

SMHP provides an application-level message delivery assurance mechanism. The mechanism requires that the recipient of application data respond back to the sender to provide assurance that the message has been received and processed. In the case of TDLS-MS, the acknowledgment indicates that the message has been safe-stored.

Figure 3-4 depicts an example high-level SMHP message processing design.

TDLS Application Process Capability Requirements

The TDLS_SERVER will listen for incoming connections from the TDLS_FEP. Once a connection is established, the listener process spawns a child server process to service the CSP_CLIENT as shown in Figure 3-3. The child process provides process isolation between CSPs when multiple CSPs connect to the same TDLS_BEP. Once the child server process is spawned to service the client, the parent listener process resumes listening for incoming connections.

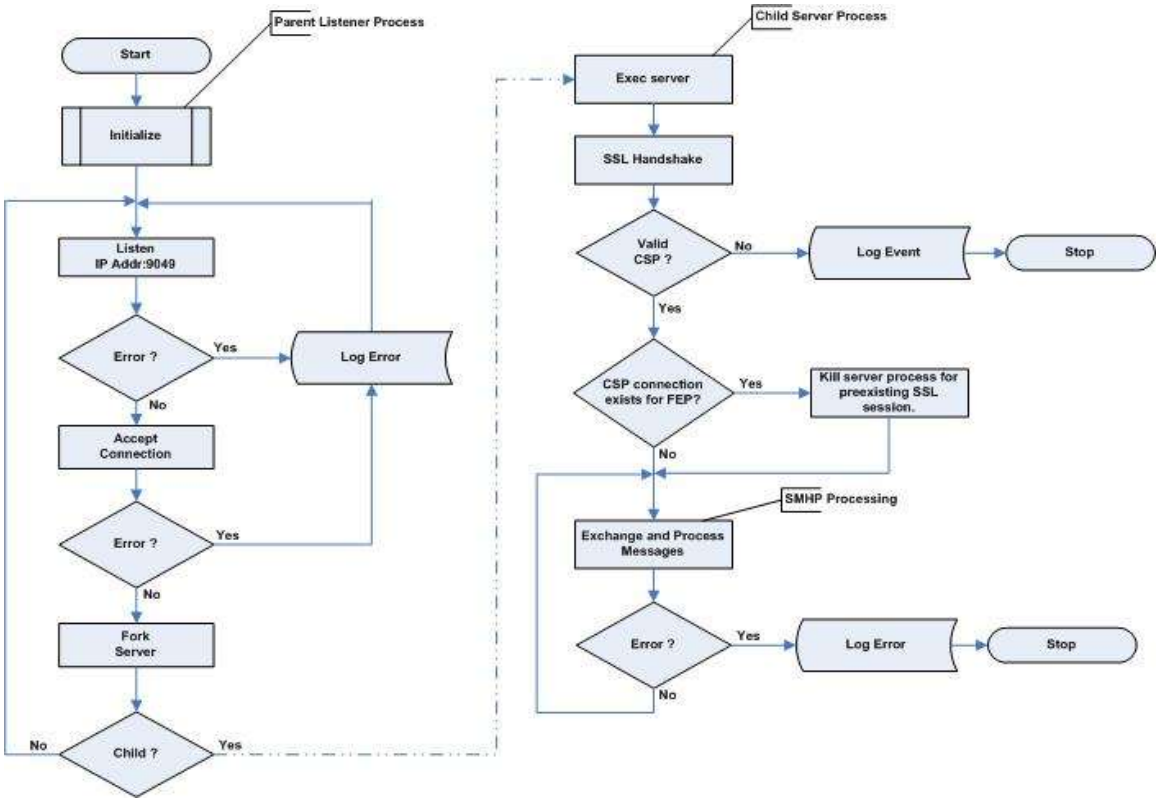

Figure 3-3. Example TDLS_SERVER High-Level Design

After establishing the virtual connection between the CSP_CLIENT and the TDLS_SERVER, the client and server applications exchange client and server certificates during the TLS handshake.

If the TDLS_SERVER receives multiple connection requests from a CSP_CLIENT originating from the same TDLS_FEP, the TDLS_SERVER will terminate the preexisting connection and accept the new connection to the CSP_CLIENT. This assures unique client/server sessions originating from the TDLS_FEP.

The TDLS_SERVER utilizes SMHP to exchange unencrypted GREQ, DCC, PDC and D-ATIS messages between the TDLS_SERVER and the CSP_CLIENT. For further information pertaining to SMHP message processing, refer to Figure 3-4, *Example High-Level SMHP Message Processing Design.*

3.2.1.3 Message Content Requirements

The application-level information units consist of SMHP data messages and management messages. The only SMHP data message types supported across this interface are those listed in Table 3-1. The actual GREQ, DCC, PDC and D-ATIS application-level data messages, in International Air Transport Association (IATA) Type B format, are contained within the payload of SMHP data messages of type GRM, GIR, CCI, CCR, CCA, CCP, PDC and TIS respectively.

Table 3-1. TDLS-MS Application-Level Data Messages

Message Type	Message Name
GRM	Gate ID Request Message
GIR	Gate ID Request Response Message
CCI	Initial Dispatch Message
CCR	Revised Dispatched Message
CCA	Dispatch Message Acknowledgement Message
CCP	Pilot Response Dispatch Message
PDC	Pre-Departure Clearance Message
TIS	Digital Automated Terminal Information Service Message

In addition to the application-level data messages, there are three application-level management messages that are transmitted across the TDLS-MS TCP/IP interface, as listed in Table 3-2. These messages are used to periodically verify the integrity of the virtual connection and to provide message delivery assurance.

Table 3-2. TDLS-MS Application-Level Management Messages

Message Type	Message Name
HART	Heartbeat Message
ACK	Acknowledgement Message
NAK	Negative Acknowledgement Message

3.2.1.3.1 Information Code

All application-level messages that cross this interface are encoded according to the American Standard Code for Information Interchange (ASCII) character set representation, which are in accordance with American National Standards Institute (ANSI) X3.4, ASCII and ANSI X3.41, Code Extension Techniques for use with the 7-Bit Coded Character Set of ASCII. All application-level messages are preceded by a 16 byte SMHP header that consists of ASCII fields only.

3.2.1.3.2 Information Structure

The only types of application-level Data Messages supported across this interface are shown in Table 3-3. See Appendix A, *Simple Message Handling Protocol*, for the format of these messages.

Table 3-3. TDLS-MS Application-Level Data Message Characteristics

Data Message	Mnemonic	Traffic Direction TDLS_SERVER | CSP_CLIENT		Transmit Frequency	Size (Bytes)
Gate ID Request	GRM	→	n/a	Unscheduled	< 100
Gate ID Request Response	GIR	n/a	←	Unscheduled	< 100
Dispatch Message for initial clearances	CCI	→	n/a	Unscheduled	< 1500
Dispatch Message for revised clearances	CCR	→	n/a	Unscheduled	< 1500
Dispatch Message ACKs	CCP	→	n/a	Unscheduled	< 1500
Dispatch Message for pilot responses	CCA	n/a	←	Unscheduled	< 1500
Pre-Departure Clearance	PDC	→	←	Unscheduled	< 400
Digital Automated Terminal Information Service	TIS	→	←	Unscheduled	< 2000

The size and frequency of the application-level Management Messages sent and received by TDLS-MS are defined in Table 3-4. See Appendix A, *Simple Message Handling Protocol*, for the format of these messages.

Table 3-4. TDLS-MS Application-Level Management Message Characteristics

Management Message	Mnemonic	Traffic Direction TDLS_SERVER | CSP_CLIENT		Transmit Frequency	Size (Bytes)
Acknowledgement	ACK	→	←	Unscheduled	16
Negative Acknowledgement	NAK	→	←	Unscheduled	32
Heartbeat	HART	→	←	Unscheduled	16

3.2.1.3.3 Information Segmentation

Messages do not need to be segmented for flow control or buffer management at the application protocol level. The total length of a message will be less than 2 KB and the TCP send buffer will be tuned to 64 KB. If the TCP output buffer is full, the process will block until it drains. There may be fragmentation of the message at the TCP level if the Maximum Segment Size (MSS) is less than the size of a message that is being sent or at the IP level if the Maximum Transmission Unit (MTU) in part of the network is less than the size of a TCP segment. However, fragmentation at the TCP or IP levels is transparent to the SMHP.

3.2.1.3.4 Direction of Flow

PDC, TIS, ACK, NAK, HART messages are bi-directional. GRM, CCI, CCR, CCP messages flow from TDLS_SERVER to CSP_CLIENT. GIR and CCA messages flow from CSP_CLIENT to TDLS_Server.

3.2.1.3.5 Frequency of Transmission

The frequency at which application-level messages are transmitted is provided in Table 3-3 and Table 3-4.

3.2.1.3.6 Responses

SMHP ACK messages are sent after the receipt of the corresponding SMHP data message.

A SMHP NAK message is sent after the receipt of a message containing an invalid SMHP header (Framing Error).

3.2.1.4 Relationship among Messages

When Air Traffic Control (ATC) at a remote TDLS site issues GREQ, DCC, PDC or D-ATIS messages, the messages are stored on the TDLS_BEP and forwarded to the CSPs that have subscribed for those messages using SMHP.

Upon successful receipt of a SMHP data message of type GRM the CSP_CLIENT will respond with a SMHP Data Message of type GIR, which is the acknowledgement at the DCL application-level. (Note: This acknowledgement comes from the airline host computer). The GIR message contains the Gate ID (surface location) that was requested in the original GRM message.

Upon successful receipt of a SMHP data message of type CCI, CCR or CCP, the CSP_CLIENT will respond with a SMHP Data Message of type CCA, which is the Dispatch Message acknowledgement at the DCL application-level.

Note: The CCA acknowledgement comes from the Airline Flight Operations Center (FOC) automation subsystem.

Upon successful receipt of a SMHP data message of type PDC, the CSP_CLIENT will respond with a SMHP Data Message of type PDC, which is the actual PDC acknowledgement at the PDC application-level.

Note: The PDC acknowledgement comes from the FOC automation subsystem.

Upon successful receipt of a SMHP data message of type TIS, the CSP_CLIENT will respond with a SMHP data message of type TIS, which is the actual D-ATIS acknowledgement at the D-ATIS application-level.

Other than acknowledging application level messages at the application level, this ICD imposes no explicit requirements on how GREQ, DCC, PDC or D-ATIS messages are processed or used.

3.2.1.5 Quality of Service Requirements

Availability: Application messages transferred over the TDLS-MS TCP/IP interface are considered NAS essential. The availability of this interface must be greater than or equal to 99.9%.

Restoration Time: Service restoration will be less than or equal to ten (10) minutes.

Message Size: The SMHP maximum message size is 9999 bytes.

Data Integrity: The CSP_CLIENT and TDLS_SERVER acknowledge a SMHP data message with a SMHP ACK message. The TDLS-MS validates network packets for accuracy completeness and validity at the network transport layer (TCP/IP) and at the application layer utilizing TLSv1.0 or greater.

Derivation Guidance: *The TIMS application CSCIs are responsible for validating the accuracy, completeness and validity of its inputs at the application layer.*

The TDLS-MS interface utilizes FTI services to protect the integrity of transmitted ground-ground information from unintended modifications.

Latency: The overall latency between the CSP_CLIENT and the TDLS_SERVER must be less than two (2) minutes.

Throughput: The network service bandwidth between the CSP_CLIENT and TDLS_SERVER must be at least 512 kbps. Under a TDLS Enterprise full Design Workload the TDLS-MS will be capable of supporting a GREQ/DCC message rate of 18 per minute between the TDLS Enterprise and a CSP.

3.2.1.6 Error Handling Requirements

Error Logging

The TDLS-MS is designed to identify errors conditions and generate error messages that provide information necessary for corrective actions without revealing, in error logs or administrative messages, sensitive information (e.g., passwords, PII) or information that could be exploited by adversaries.

The TDLS-MS logs all operational messages and enables the status of all operational messages to be monitored as they pass through the TDLS-MS interface.

The TDLS-MS also monitors the status of all TLS sessions between the TDLS FEP and the TDLS BEP and reports the up/down status to the TIMS Monitor and Control (TMC) CSCI that resides on the TIMSADM platform.

The TDLS-MS supports the monitoring of the status of all VPN connections between the CSP and FEP and reports the up/down status to the TIMS TMC CSCI.

Load Sharing:

Load balancing between TDLS_BEPs is accomplished by TDLS transmitting messages to the two TDLS_BEPs in a round-robin fashion. Database synchronization between the TDLS_BEPs is handled in the background with Oracle Streams.

Failover Mode:

The FEP_PROXY application provides the failover and fallback logic within the TDLS-MS. Once the CSP_CLIENT connects to the TDLS_FEP, the proxy listener spawns a process to service the CSP_CLIENT. The FEP_PROXY first attempts to open a connection to the local TDLS_BEP. If that attempt fails, it attempts to open a connection to the failover TDLS_BEP as shown in Figure 3-3, TDLS_FEP Proxy Service High Level Design.

When the CSP connects through multiple NESGs to the same TDLS_BEP, the TDLS_FEP collocated with the TDLS_BEP will be the primary proxy for servicing the CSP.

Fallback Mode:

Once the FEP_PROXY connects to the failover TDLS_BEP, it continually attempts to open a connection to the local TDLS_BEP in the background. Once the background process connects to the local TDLS_BEP, the FEP_PROXY closes the socket connections to both the failover TDLS_BEP and the CSP_CLIENT, triggering the CSP_CLIENT to reestablish the socket connection to the local TDLS_FEP to complete the fallback process. After reestablishing the virtual connection between the CSP_CLIENT and TDLS_SERVER, a new TLS session is established between the client and server.

Recovery Mode:

If the FEP_PROXY process fails to open a connection to the failover TDLS_BEP, the FEP_PROXY process will close the connection to the CSP_CLIENT, triggering the CSP_CLIENT to reestablish the socket connection with the TDLS_FEP. This time the FEP_PROXY will attempt to fall back to the local TDLS_BEP.

If the FEP_PROXY process loses a socket connection to either the CSP_CLIENT or the TDLS_SERVER, the FEP_PROXY process will close the socket connections to both the TDLS_SERVER and the CSP_CLIENT, triggering the CSP_CLIENT to reestablish the virtual connection to the TDLS_SERVER. Once the virtual connection is complete, the CSP_CLIENT and TDLS_SERVER establish a new TLS session.

At the application level, the CSP_CLIENT and TDLS_SERVER have a method of monitoring integrity of the virtual connection. If the CSP_CLIENT or the TDLS_SERVER have not sent any messages for 5 seconds, they will send a SMHP heartbeat (HART) message. If the CSP_CLIENT or the TDLS_SERVER have not received any messages for 20 seconds, they will close the connection trigging the CSP_CLIENT to reestablish the virtual connection between the CSP_CLIENT and TDLS_SERVER.

If the CSP_CLIENT or TDLS_SERVER receive an invalid SMHP header (framing error), it will send a SMHP NAK messages and close the virtual connection. The receipt of NAK message also results in the virtual connection being closed from the opposite end. This triggers the CSP_CLIENT to reestablish the virtual connection to the TDLS_SERVER.

If the TDLS_SERVER receives multiple connection requests from a CSP_CLIENT originating from the same TDLS_FEP, the TDLS_SERVER terminates the preexisting connection and accepts the new connection from the CSP_CLIENT. This ensures there is only a single TLS

session between the CSP_CLIENT and TDLS_SERVER associated with a particular TDLS_FEP.

3.2.1.7 Interface Summary Table

Table 3-3 and Table 3-4 summarize the application-level messages transmitted across the TDLS-MS TCP/IP interface.

Figure 3-4 depicts an example of a high-level program design to process SMHP messages. The CSP_CLIENT and TDLS_SERVER use logic similar to that in this example to process SMHP messages.

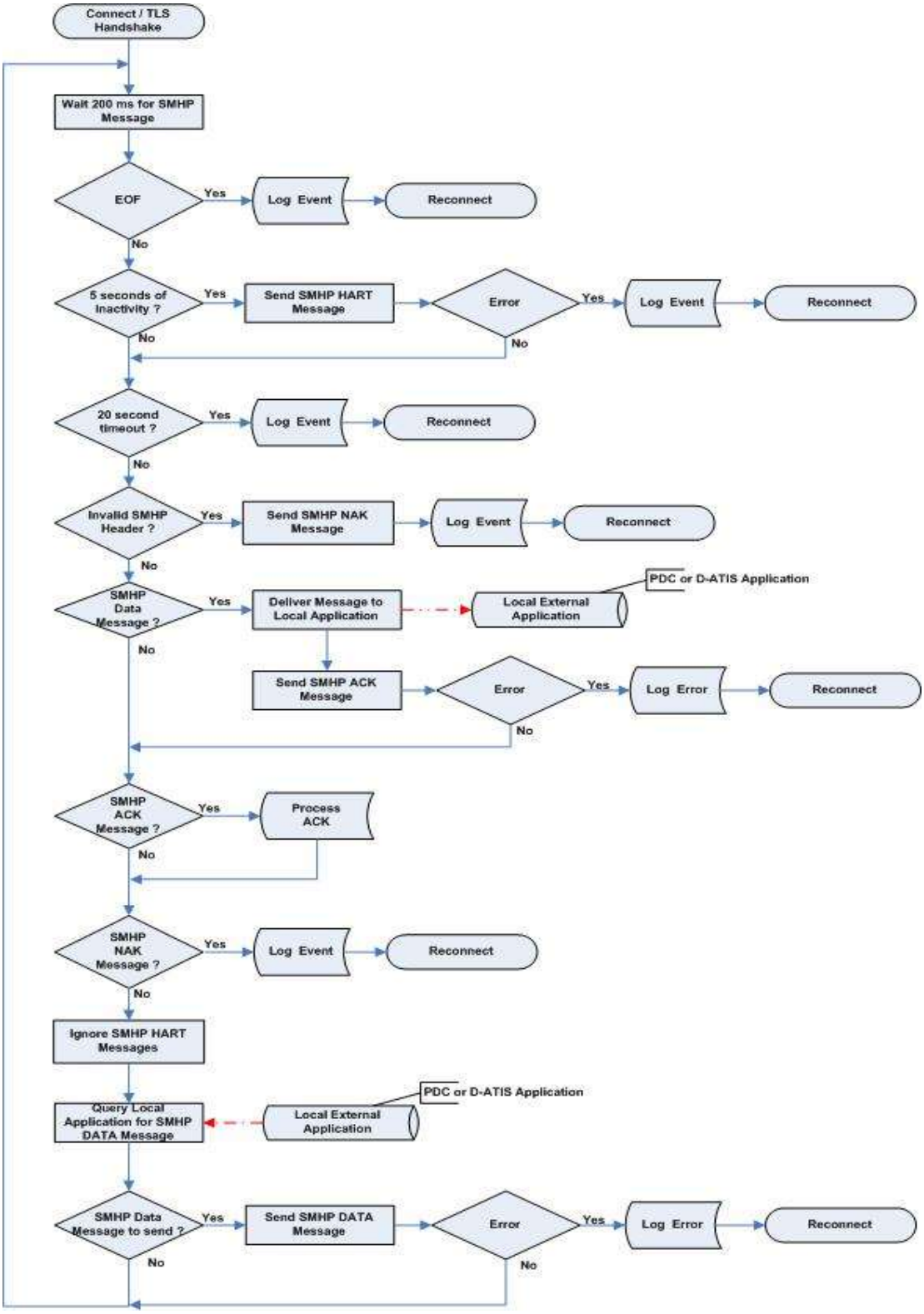

Figure 3-4. Example High-Level SMHP Message Processing Design

3.2.2 Protocol Implementation

The functional characteristics are implemented in accordance with the Internet Protocol Stack as depicted in Figure 3-5.

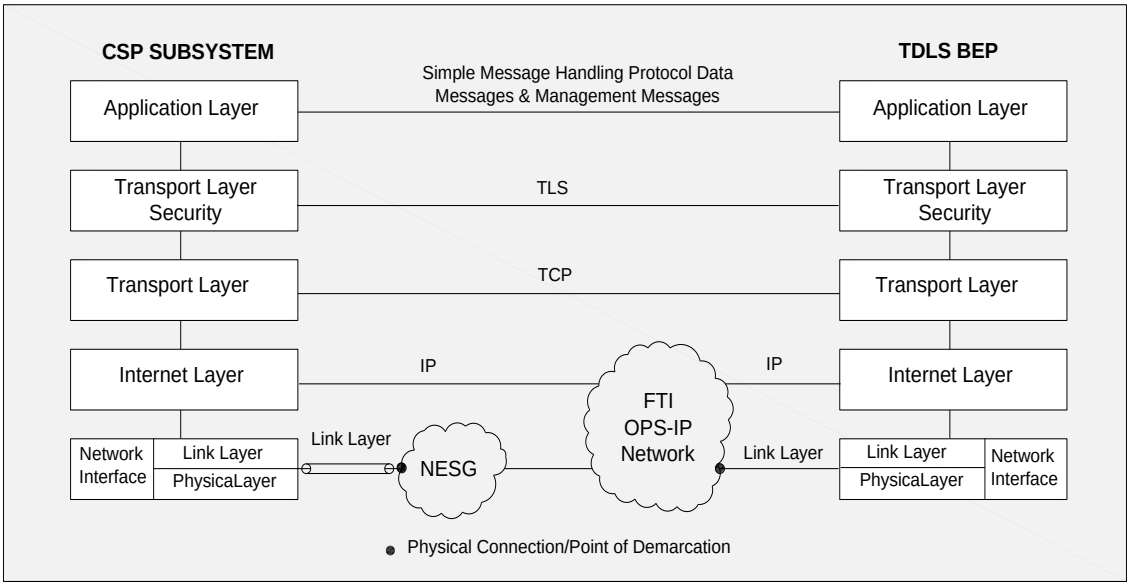

Figure 3-5. Protocol Mapping Between TDLS-MS and CSP Subsystems

Application Layer: TDLS-MS transfers SMHP messages at the application layer of the TCP/IP stack.

The Internet protocols specify a byte order convention (network byte order) for data transmitted over the network. This convention enables systems based upon differing byte-order formats (big-endian and little-endian) to communicate with each other. TDLS-MS does not require this convention since the SMHP message header consists of ASCII characters only.

Transport Layer Security: TDLS-MS utilizes Transport Layer Security (TLS) Version 1.0 as specified in RFC 2246 to provide authentication and message integrity.

Transport Layer: TDLS-MS supports TCP in accordance with RFC 793: *Transmission Control Protocol*, September 1981, updated by RFC 3168.

This ICD does not address several TCP tuning parameters. These are global variables, which may affect all TCP/IP sessions. These parameters are:

TCP-scalable window sizes. (RFC 1323)

Selective acknowledgments (SACK). (RFC 2018)

TCP fast retransmit and fast recovery. (RFC 2581)

Internet Layer: TDLS-MS implements the IP protocol at the Internet Layer in accordance with the following RFCs:

RFC 791: *Internet Protocol,* September 1981. (Updated by RFC 1349)

RFC 792: *Internet Control Message Protocol,* September 1981. (Updated by RFC 950)

RFC 894: *A Standard for the Transmission of IP Datagrams over Ethernet Networks*, April 1984.

RFC 950: *Internet Standard Sub-netting Procedure,* August 1985

RFC 1349: *Type of Service in the Internet Protocol Suite,* July 1992. (Obsoleted by RFC 2474, and updated by RFC 3168)

RFC 2474: *Definition of the Differentiated Services (DS) Field in the IPv4 and IPv6 Headers,* December 1988

RFC 3168: *The Addition of Explicit Congestion Notification (ECN) to IP*, September 2001.

The Transport Layer implements the TCP protocol as specified in RFC 793, as amended in RFC 950 and in RFC 3168 over the IP-based interfaces between TDLS-MS and its CSPs.

Network Interface: The TDLS_BEPs connect directly to the NAS OPS-IP network. The TDLS_FEP connects to the External DMZ of the NESG. CSP subsystems will not connect directly to the NAS OPS-IP network, but instead will connect through a NESG to the TDLS_FEP. The NESG provides common functions (firewalls, authentication, packet inspection, etc.) for a number of FAA Systems located at the NEMCs. The TDLS_FEP and TDLS_BEP are co-located with the NESGs.

Link Layer: For the interface to the NESG, the CSP subsystems shall utilize the Ethernet V2 framing format to implement the Data Link level in accordance with RFC 894.

Physical Layer: Each CSP subsystem will have two Category-5e (Cat5e) cables connecting it to two co-located Ethernet Switches. The CSP subsystem will implement the physical layer in accordance with IEEE 802.3 and can operate in either half or full-duplex mode.

3.2.2.1 Application Layer Services

The TDLS-MS exchanges GREQ, DCC, PDC and D-ATIS messages with the CSP subsystem utilizing SMHP.

Transport Layer Security Services

SMHP utilizes TLS Version 1.0 as specified in RFC 2246 to provide client/server authentication and message integrity.

3.2.2.2 Transport Layer Services

The transport layer service for this ICD is TCP, in accordance with the latest edition of FAA-STD-039c, Section 5.4, *Transport Sub-profile.* The TCP_NODELAY option will be set for TCP sockets so that multiple small packets can be sent before the first small packet is acknowledged at the TCP level.

3.2.2.3 Naming and Addressing

IP addressing is implemented as specified in FAA-STD-039c, Section 5.3.1, *Internet Protocol (IP).*

3.3 Physical Characteristics

The physical characteristics for the interface between TDLS-MS and the NESG are described in the following subsections and are in accordance with the FTI ICD.

3.3.1 Electrical Power and Electronic Characteristics

3.3.1.1 Connectors

For Ethernet connections, IFCET provides cables with standard RJ-45 connectors for attachment to the FTI SDPs.

All TDLS-MS network interfaces provide RJ45 female network connectors.

3.3.1.2 Wiring/Cabling

All cables located in the plenum area are plenum rated. Cabling between TDLS-MS and the FTI SDPs conforms to the specifications of the IEEE Ethernet LAN standard 802.3. Category (CAT) 5e cabling is used with the connector wiring as specified in TIA/EIA-568-B.1. These systems connect by means of metal-conductor cabling. Point-to-point cable length for 10BaseTX/100BaseTX connections is less than or equal to 100 meters. Electrical connection characteristics for the Ethernet interface between the TDLS-MS and the FTI SDP are as specified in IEEE 802.3.

For Ethernet connections, the IFCET provides cables with standard RJ-45 male connectors for attachment to FTI service SDPs. These connectors are secured by means of a tab on the connector, which mates with the jack, thereby preventing improper attachment and preventing detachment during normal movement of the unit. Connector wiring is as specified by Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA) connector wiring specification TIA/EIA-568-B.1.

3.3.1.3 Grounding

Within the electrical interfaces, grounding complies with FAA-STD-019e, Lightning and Surge Protection, Grounding, Bonding and Shielding Requirements for Facilities and Electronic Equipment.

3.3.1.4 Fasteners

TDLS-MS utilizes mechanical means of securing connectors used in the interface between directly connected subsystems or between intermediate telecommunications equipment and the respective mating jacks at the applicable demarcation point.

3.3.1.5 Electromagnetic Compatibility

The electromagnetic compatibility of all TDLS Enterprise subsystems is in accordance with FAA-G-2100H, Section 3.3.2 *Electromagnetic Compatibility*.

4 QUALITY ASSURANCE PROVISIONS

The following section specifies the process of verification for interface design characteristics.

4.1 Responsibility for Verification

The government has responsibility for developing and implementing the verification of requirements for each project. The government may delegate verification activities to other organizations, independent contractors, and/or the major prime contractor. The Test and Evaluation (T&E) process guidelines within the Acquisition Management System (AMS) will be used for the levels and methods of verification in the Verification Requirements Traceability Matrix (VRTM).

FTI provides the IP service infrastructure for the TDLS Enterprise. All CSPs requesting access to the TDLS-MS IP-based services must also connect to this (FAA) IP network. It is required that CSPs contact the IFCET, which is responsible for the RFS process that defines the roles and responsibilities for the activities that need to occur for all users connecting to the operational FTI network.

The IFCET, AJW-178, (based at the MMAC) provides all second-level support for the operational TDLS Enterprise. One of these roles is to test CSP subsystems requesting TDLS-MS TCP/IP Services. The CSP will first work with FTI on configuring the VPN connection between the external CSP subsystems and the FNTB. This phase will be where IP information is exchanged for testing. When a CSP has successfully passed FTI FNTB connectivity testing through the NESG on the FNTB, they will be handed off to the IFCET for TDLS-MS interoperability testing. The current contact information for the IFCET is:

Don Fitts
Data Communications Engineering Team Lead
(405) 945-5199
E-Mail: don.fitts@faa.gov.

The current FNTB contact is:

Joe Klapatch
FNTB Senior Engineer
(609) 485-4978
E-Mail: joe.klapatch@faa.gov

The current FTI Program Office contact is:

Mike Reamer
FTI Central Service Area Implementation Team Lead

(202) 841-5928
E-Mail: mike.reamer@faa.gov

4.2 Special Verification Requirements

Prior to the start of integration level verification, functional interoperability will be demonstrated at the William J. Hughes Technical Center (WJHTC) System Support Computer Complex on the FNTB.

4.3 Verification Requirements Traceability Matrix

Refer to NAS-IR-22030001 Rev C, Table 4-1 for the Verification Requirements Traceability Matrix (VRTM).

5 PREPARATION FOR DELIVERY

This ICD imposes no explicit preparations for delivery.

6 NOTES

6.1 Definitions

The following definitions apply to the terms used in this ICD:

Airline Operations Center: AOC is an airline capability supported by applications for flight information communication between Airline Host (ground computer) and the aircraft. AOCs also exchange flight information with FAA ground systems when flights are provided predeparture clearances.

Authorized Operators:

a. U.S. Air Carrier - An entity certificated to operate in accordance with 49 CFR Part 119, 121, 125, and 135.

b. Non-US. Aviation Entity – A non-US entity certificated to operate under 49 CFR Part 129, a Foreign-Equivalent of Airport / Port Authority/Air Carrier, a Foreign Organization providing dispatch and /or tracking functions.

Communications Service Provider (CSP): Any entity contracted to provide communications networks for delivery of Pre-Departure Clearance (PDC), Departure Clearance Services (DCL) Dispatch Messages and Gate Request Messages, and/or Digital Automatic Terminal Information Service (D-ATIS) text messages to authorized operator. CSP may include the authorized operator and its agents.

Demarcation (point of): The point of demarcation is a specific point in a chain of hardware and interconnecting circuitry where a change of responsibility for provisioning installation and operation of the hardware and circuit configuration occurs.

Digital Automatic Terminal Information Service (D-ATIS): D-ATIS are text messages sent to aircraft, operators, and other users outside the standard reception range of conventional ATIS via landline and data link communications to the cockpit. (This service also provides a computer−synthesized voice message that can be transmitted to all aircraft within range of existing transmitters, which is outside the scope of this document.)

Interface: An interface is the means of communication, including hardware and software, between two entities.

National Airspace System (NAS): The common network of U.S. airspace; air navigation facilities, equipment and services, airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material used to ensure safe and efficient use of U.S. navigable airspace. Included are system components shared jointly with the military and other governmental entities.

Tower Data Link Services (TDLS) Departure Clearance Dispatch Message: TDLS Departure Clearance Dispatch Messages provide clearance information to airline dispatchers, for each DCL clearance sent to the cockpit.

6.2 Abbreviations and Acronyms

ACK	Acknowledgement Message
AJW-178	TDLS Engineering group within the IFCET.
AMS	Acquisition Management System
ANSI	American National Standard Institute
AOC	Airline Operations Center
AP	Application Process
ARCTR	FAA Aeronautical Center
ASCII	American Standard Code for Information Interchange
ATC	Air Traffic Control
ATCT	Airport Traffic Control Tower
ATIS	Automatic Terminal Information Service
ATL	Atlanta, GA.
ATO	Air Traffic Organization
BEP	Back End Processor
BPS	Bits Per Second
CA	Certification Authority
C&A	Certification and Accreditation
CAT	Category
CSP	Communications Service Provider
CCA	SMHP message type for the Dispatch Message Acknowledgment
CCI	SMHP message type for the Initial Clearance Dispatch message
CCP	SMHP message type for the Pilot Response Dispatch message

CCR	SMHP message type for the Revised Clearance Dispatch message
CSP_CLIENT	Communications Service Provider Client
D-ATIS	Digital ATIS (Automatic Terminal Information Service)
DCC	SMHP messages that carry DCL Dispatch Messages of type CCI, CCR, CCP and CCA
DCL	Departure Clearance
DMZ	Demilitarized Zone
DOT	Department of Transportation
DTS	Data Transfer System
EIA/TIA	Electronic Industries Alliance/Telecommunications Industry Association
ETX	End of Text
FAA	Federal Aviation Administration
FEP	Front End Processor (for TDLS)
FEP_PROXY	Front End Processor (for TDLS) Proxy
FNTB	FTI National Test Bed
FOC	Airline Flight Operations Center
FTI	FAA Telecommunications Infrastructure
GIR	SMHP message type for a Gate Request Response
GREQ	SMHP messages that contain GRM and GIR messages
GRM	SMHP message type for a Gate Request
HART	SMHP heartbeat Message
IATA	International Air Transport Association
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers, Inc.
I/F	Interface
IP	Internet Protocol
IFCET	Interfacility Communications Engineering Team.
ISA	Interconnect Security Agreement
ISO	International Standards Organization
IRD	Interface Requirements Document
LAN	Local Area Network

MDL	Mason Dixon Line
MMAC	Mike Monroney Aeronautical Center
MOA	Memorandum of Agreement
MTU	Maximum Transmission Unit
MSL	TCP Message Segment Lifetime
MSS	Maximum Segment Size
NAS	National Airspace System
NAK	Non-Acknowledgement Message
NEMC	Network Enterprise Management Center
NESG	NAS Enterprise Security Gateways
NNCC	National Network Control Center
OPS	Operational
OPS-IP	NAS Operational Internet Protocol Network
OSI	Open Systems Interconnection
PDC	SMHP message type that contains Pre-Departure Clearance message
RFC	Request for Comment
RFS	Request For Service
SAP	Service Access Point (Virtual connection)
SDP	Service Delivery Point (Physical connection)
SLC	Salt Lake City, UT
SMHP	Simple Message Handling Protocol.
SOH	Start of Header
STX	Start of Text
T&E	Test and Evaluation
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
TIS	SMHP message type that contains D-ATIS message
TDLS	Tower Data Link Services
TDLS_BEP	Tower Data Link Services Back End Processor
TDLS_FEP	Tower Data Link Services Front End Processor
TDLS_SERVER	Tower Data Link Services Server

TDLS-MS	Tower Data Link Services Message Service
TLS	Transport Layer Security
TIMSADM	Administrative TDLS BEP
TIMSEST	Operational TDLS BEP
TIMSWST	Operational TDLS BEP
VPN	Virtual Private Network
VRTM	Verification Requirements Traceability Matrix
WAN	Wide Area Network
WJHTC	William J. Hughes Technical Center

Appendix A SIMPLE MESSAGE HANDLING PROTOCOL

This appendix documents the application-layer Simple Message Handling Protocol (SMHP) which is used for messaging between the Tower Data Link Services Message Service (TDLS-MS) and the Communications Service Providers (CSP). The SMHP is based on TCP/IP for transport and internetworking and uses Transport Layer Security Version 1.0 (TLSv1.0) for authentication and message integrity. The SMHP does not encrypt or compress messages at the application or TLS layer.

A.1 Protocol Formats

A.1.1 Internet Layer - IP Datagram Format

The IP datagram structure is depicted in Table A-1 below. Each datagram frame consists of a header followed by the data field, and is defined in Request for Comments (RFC) 791 (Part of the Internet Engineering Task Force (IETF STD-5). The IP header will be 20 bytes in length, as none of these systems has plans to utilize the IP Options field. The maximum length for the data field will be 1480 bytes, based upon the widely used standard of a Maximum Transmission Unit (MTU) being 1500 bytes.

Table A-1. Standard IP Datagram Structure

IP HEADER	IP DATA
20 Bytes	1 - 1480 Bytes

A.1.2 Transport Layer - TCP Segment Format

The TCP segment consists of the TCP header and TCP data fields which reside within the data field of the IP datagram as depicted in Table A-2. The definition of the individual fields within the TCP header is contained in RFC 793 (IETF STD-7). The header field is 20 bytes in length and the data field has a maximum length of 1460 bytes.

Table A-2. Standard TCP Segment Structure

IP HEADER	IP DATA	
20 Bytes	1 - 1480 Bytes	
	TCP HEADER	TCP DATA
	20 Bytes	1 - 1460 Bytes

A.1.3 TLSv1.0 Record Format

The TLSV1.0 record format (depicted in Table A-3) consists of a header, a variable length payload, and a keyed-Hash Message Authentication Code (HMAC) which provides message integrity. RFC 2246 (IETF STD-1) defines TLSv1.0. Note that there could be multiple TLSv1.0 records in one TCP segment and a TLSv1.0 record could span multiple TCP segments.

Table A-3. TLS Record Format

TLS HEADER	TLS DATA	HMAC SHA1
5 Bytes	1 – 16,383 Bytes	20 Bytes

A.1.4 SMHP Message Format

The SMHP message format consists of the SMHP header and a variable length payload, as shown in Table A-4. An SMHP message is contained within a single TLSv1 record.

Table A-4. SMHP Message Structure

TLSv1.0 Record Application Data Field	
SMHP HDR	**SMHP BODY**
16 Bytes	0 – 9999 Bytes

A.1.4.1 SMHP Header Format

The SMHP message contains a 16 byte header that contains the four fields described in Table A-5. All fields in the header will consist of only alphanumeric and space characters except for the version and pad fields.

Table A-5. SMHP Message Header Format

Field	Length	Description
Body Length	4 characters	The length of the body of the message in bytes in decimal format padded with leading '0' characters. If there is no body (such as for a heartbeat message) the body length field will be 0000.
Sequence	4 characters	The sequence number for the message being sent. The purpose of the sequence number is to facilitate the positive acknowledgement of messages. The sequence number will be padded with 0's to be exactly 4 characters in length. The sequence number will begin with 0001 and go to 9998. After 9998 it will cycle back to 0001. On restart of the connection, the sequence number will begin with 1 again. The value 9999 will be used for negative acknowledgements to report the receipt of invalid SMHP headers. In such cases the received sequence number may not be determined. Heartbeat and version messages will also use the value 9999 for the sequence number in the header. The value of 0000 for the sequence number is reserved.
Type	4 characters	The Type code for the message being sent, padded with a leading space character when needed. 'ACK': communications level positive acknowledgement (0000 length message body) 'NAK': communications level negative acknowledgement. The body will contain the header of the message being NAK'ed. ’GRM’, ‘GIR’, 'CCI', 'CCR', 'CCP’, ‘CCA', 'PDC ' or 'TIS': application data messages. 'HART': heartbeat message (0000 length message body) 'VER': first PDU sent after successful TLS handshake to advertise the desired version of SMHP

Field	Length	Description
Version	1 byte	The upper nibble contains the major version number and the lower nibble contains the minor version number of the SMHP being used. The initial version will be 0x10. The FAA will always implement newer versions of the protocol before CSPs. This will allow a CSP to advertise that it wishes to use an older version of the SMHP while working to upgrade to the latest version. If a CSP advertises a version which the FAA does not support, the connection will be denied.
Pad	3 bytes	A constant pattern 0xA5A5A5 interpreted as a sequence of bytes. This field can be checked for this value to ensure that the receiver is in sync with the writer of the data stream. Since the upper bit is set in the bytes of this pattern, this value cannot possibly be confused with any other value in the header of body of an SMHP PDU.

A.1.4.2 SMHP Body Format

The SMHP body will only contain character oriented data. This obviates the need to convert data in SMHP messages to network byte order. The data in the SMHP body will be neither compressed nor encrypted.

A.1.4.3 SMHP Message Types

SMHP messages can be divided into two groups: data messages and management messages. Management messages are used to manage the connection and will only be passed between the CSP client and TDLS-MS server processes. Data messages originate from and are consumed by applications external to the SMHP communications software.

There are eight types of SMHP data messages: GRM, GIR, CCI, CCR, CCP, CCA, PDC and TIS. The body for GRM, GIR, CCI, CCR, CCP, CCA, PDC and TIS messages will contain International Air Transport Association (IATA) Type B messages. This format includes the destination and sender IATA network addresses. Format of these messages are further described in Appendix B.

ACK, NAK, HART and Version Management messages are types of SMHP management messages. Format of these messages are further described in the following sections.

A.1.4.4 SMHP ACK Management Message

At the application level, SMHP data messages are acknowledged with a SMHP Acknowledgment (ACK) management message. The structure of a SMHP ACK management message is depicted in Table A-6. The sequence number in the header is the same as the sequence number for the SMHP data message being acknowledged.

Table A-6. SMHP ACK Message Structure

Body Length	Sequence	Type	Version	Pad	Body
0000	yyyy	ACK	0x10	0xA5A5A5	Null

A.1.4.5 SMHP NAK Management Message

At the application level, SMHP data messages can be rejected with a SMHP Negative Acknowledgment (NAK) management message. NAKs should only be sent in response to an invalid SMHP header. Table A-7 depicts the structure of a NAK message. The invalid header is returned in the body so that it can be used by the sender to help determine the reason for the NAK.

Table A-7. SMHP NAK Message Structure

Body Length	Sequence	Type	Version	Pad	Body
016	9999	NAK	0x10	0xA5A5A5	Bad Header

If an SMHP NAK message is sent or received, the connection must be torn down and reestablished.

A.1.4.6 SMHP HART Management Message

The CSP client and the TDLS-MS server shall send an SMHP heartbeat (HART) management message if nothing has been sent for 5 seconds. This message is used to monitor the health of the communications channel. If nothing has been received from the peer for more than 20 seconds, the connection must be torn down and reestablished. Table A-8 depicts the structure of a HART message.

Table A-8. SMHP HART Message Structure

Body Length	Sequence	Type	Version	Pad	Body
0000	9999	HART	0x10	0xA5A5A5	Null

A.1.4.7 SMHP Version Management Message

The first message that the CSP should send to the TDLS-MS server after a successful TLS handshake is a version message. The version field should contain the highest version number that the CSP supports. Initially, the only version will be 1.0 encoded as 0x10. In the future, the FAA may upgrade SMHP and give the CSPs the option of remaining on the previous version of SMHP for a period of time. If a CSP advertises a version that the FAA does not support, the FAA will respond with a NAK message. Otherwise, the FAA will not respond to the VER message. Table A-9 illustrates the structure of the VER message.

Table A-9. SMHP Version Message Structure

Body Length	Sequence	Type	Version	Pad	Body
0000	9999	VER	0x10	0xA5A5A5	Null

A.2 SMHP TCP Parameters

The TCP_NODELAY option should be set for TCP sockets so that multiple small packets can be sent before the first small packet is acknowledged at the TCP level. The messages that will be handled by SMHP will be small (especially the acknowledgments) and this should help ensure that the messages are received in a timely fashion.

A.3 SMHP TLSv1.0 Parameters

A.3.1 Version Compatibility

The SMHP will only use TLSv1.0 (version 3.1 in the TLSv1.0 record header). Connections which attempt to use SSLv3 or SSLv2 will be rejected.

A.3.2 Cipher Suite Selection

The SMHP client must advertise to the server in the ClientHello handshake message that it supports the TLS_RSA_WITH_NULL_SHA cipher suite. The TDLS-MS server will be programmed to use only TLS_RSA_WITH_NULL_SHA. This protocol suite uses RSA for key exchange and SHA1 for message digests. The WITH_NULL component of the cipher suite specifies that encryption will not be performed for the session.

A.3.3 Session Resumption

Session resumption will not be supported by the SMHP. There will only be a handful of connections from the CSPs and these connections should be long lived. The minute increase in performance does not justify the increased complexity in the software to support session resumption.

A.3.4 Renegotiations

The TDLS-MS server will not initiate renegotiations. However, if the CSP client initiates a renegotiation, the server will cooperate to generate a new TLS session.

A.3.5 Authentication

During the TLSv1.0 handshake the TDLS-MS server will submit an X.509v3 server certificate to the CSP client and the CSP client will submit an X.509v3 client certificate to the TDLS-MS server. The client and server certificates will be signed and verified by IFCET's root CA certificate. IFCET will insert a unique identifier for each CSP in an extension in the CSP's client certificate that will be used identify the CSP when the CSP connects.

A.3.6 Handshake Errors

If there were any errors with the TLSv1.0 handshake such as lack of TLS version compatibility, no cipher suite agreement, or an invalid client or server certificate then the connection must be torn down and the reason for the problem investigated.

A.4 SMHP Message Handling

The procedures in this section to handle SMHP message apply to both the CSP client and the TDLS-MS server. Everything in this section assumes that a successful connection from CSP client has been made and that the TLSv1.0 handshake was successful.

A.4.1 Sending Heartbeat Messages

Heartbeat messages (HART) monitor the communications channel to ensure continued connectivity between the channel endpoints. If an endpoint has had no data messages to send for at least 5 seconds, then it must send a heartbeat message to the peer. This enables the peer to distinguish between the lack of data to be transmitted with a break in the communications channel. If an endpoint has not received anything for 20 seconds, then it concludes that there is a break in the communications channel and the connection must be torn down and reestablished.

A.4.2 Sending Data Messages

The communications software at each endpoint will periodically check for messages from external applications to send to the peer. This should be done every 100 - 200 milliseconds. When a message is available to send, an SMHP data message should be constructed in a buffer large enough to hold the entire message including the header. The whole message should be sent as a single system call. The variable used to populate the header sequence number should be updated as well as the variable for the time of the last message sent.

SMHP data messages should be sent as fast as the communications channel will allow.

A.4.3 Receiving SMHP Messages

The communications software at each endpoint will periodically (every 100 – 200 milliseconds) check for messages from the peer. Typically this would be done by using the select() system call which will return as soon as the socket for the TCP/IP interface becomes readable. When the socket becomes readable the communications software will perform the following steps.

- The software will first read 16 bytes for the header.
- The header will be parsed and the fields examined.
- The time of the last message received will be updated with the current time.
- The message will be handled according to its type.

After parsing the header, the fields should be validated according the following criteria.

- The pad field must have the value 0xA5A5A5.
- The version field must be a supported value. Initially, the only supported value will be 0x10 (version 1.0).
- The body length field characters must be four ASCII digit characters (0x30 – 0x39).
- The sequence field characters must be four ASCII digit characters (0x30 – 0x39).
- The message type must be one of the values following: GRM, GIR, CCI, CCR, CCP, CCA, PDC or TIS.
- If the message is an SMHP data message, the body length has to be greater than 0.

If the header is not valid, an SMHP NAK message must be constructed and sent to the peer. The invalid header should comprise the body of the message. After the message has been sent, the connection must be torn down and reestablished.

A.4.4 Handling SMHP Heartbeat Messages

Heartbeat messages will be ignored except that they cause the time of last message received to be updated to the current time. Heartbeat messages are not acknowledged.

A.4.5 Handling SMHP Data Messages

- The communications software will read the number of bytes for the body as indicated by the header.
- The message type (GRM, GIR, CCI, CCR, CCP, CCA, PDC or TIS) will be used to dispatch the message to the appropriate external application.
- An SMHP ACK message will be constructed and sent to the peer. The sequence number in the SMHP ACK message will be set to the value of the sequence number for the SMHP data message that was received.

A.4.6 Handling SMHP ACK Messages

An SMHP ACK message informs the receiver that an SMHP data message that had been sent to the peer has been received and properly dispatched to the appropriate external application. The communications software can use this information to record the fact that the message was received by the peer and to track the performance of the communications channel. SMHP ACK messages are not acknowledged.

A.4.7 Handling SMHP NAK Messages

An SMHP NAK message indicates that the peer received an invalid header. An invalid header could mean that the receiver was out of sync with the byte stream or the header was transmitted with incorrect values such as an invalid message type. The body of the SMHP NAK message contains the invalid header. The response to an SMHP NAK is to save the invalid header for analysis and tear down the connection. SMHP NAK messages are not acknowledged.

Appendix B Application-Level Message Format

This appendix documents the format of the application-level messages transmitted between the Tower Data Link Services Message Service (TDLS-MS) and the Communications Service Providers (CSP). Application-level data messages comprise PDC and TIS messages.

B.1 PDC Message

All PDC messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z
Numeric characters 0 to 9
Characters "*", "@", ".", "-", " " (space), and "/".

PDC message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- TAB (horizontal tab)
- ETX (end of text)

B.1.1 PDC Data Message

B.1.1.1 PDC SMHP Message Format

A PDC message (depicted in Table B-1) is comprised of the SMHP header and the body which contains the PDC message.

Table B-1. SMHP PDC Message

Body Length	Sequence	Type	Version	Pad	Body
Xxxx	yyyy	PDC	0x10	0xA5A5A5	PDC MSG

The body of a SMHP message of type PDC can contain either a PDC message or a PDC ACK message. The TDLS-MS will only send PDC messages to CSPs and CSPs will only send PDC ACK messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.1.1.2 PDC Data Message Format

Table B-2 describes the format of the PDC application-level data messages. If a line contains no data, it may contain a space prior to the **CR LF** characters. Following the altitude restriction data, some lines may be omitted from or additional lines may be added to those shown in Table B-2.

Table B-2. PDC Data Message Format

Line	Format	
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU YYZAGAC
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.SLCTWXA 111149
3	**STX** [SMI] **CR LF**	PDC
4	[Sequence Number] **CR LF**	000
5	[Flight ID] **TAB** [Beacon Code] **TAB** [Depart Point] **CR LF**	DL262T 4305 KSLC
6	[Aircraft Type/Heavy Indicator] **TAB** [Depart Time] **CR LF**	A320/Q P1219
7	[Computer ID] **TAB** [Altitude] **CR LF**	038 320
8	[Route Information] **CR LF**	-LEETZ2 HOLTR MSO- or *Cleared Route if no ADR is supplied* "KSLC WEVIC2 HVE MSO KMSO"
9	[Route Information] **CR LF**	*Rest of [ADR] if longer than Line 8* or *Cleared route if ADR is supplied in Line 8* "KSLC WEVIC2 HVE MSO KMSO" or *[Rest of Cleared Route if longer than line 8]*
10	[Route Information/Remarks] **CR LF**	*[Rest of Cleared route if longer than lines 8 and 9]* or @NO STAR *(if remarks are present)* or *[blank] if no remarks and no route information*
11	[Estimated Departure Clearance Time] **CR LF**	1430

		or *[blank] if no EDCT*
12	[Revision Number/Strip Request Originator of an SR] **CR LF**	
13	[["CLEARED (DP/SID to be flown) DEPARTURE (TRANSITION to be flown) TRSN"] or [CLEARED (DP/SID to be flown) DEPARTURE] or ["NO SID" (if no SID is assigned or filed)]] CR LF	CLEARED LEETZ2 DEPARTURE HOLTR TRSN or CLEARED LEETZ2 DEPARTURE or NO SID
14	[[Associated climb-out instructions or initial heading] or [no entry]] CR LF	CANARSIE CLIMB or *[blank]*
15	[["MAINTAIN (Initial Altitude)"] or ["CLIMB VIA SID"] or ["CLB VIA SID EXC MAINT (Initial Altitude)"]] CR LF	MAINTAIN FL320 or MAINTAIN 10000FT or CLIMB VIA SID or CLB VIA SID EXC MAINT FL320 or CLB VIA SID EXC MAINT 10000FT
16	[Expected Altitude in the event of lost communications, [[DPFRQ (###.###)] or [SEE SID]] CR LF	EXP 320 10 MIN AFT DP, DPFRQ 135.500 or EXP 320 10 NM AFT DP, SEE SID
17	[[Contact Information in accordance with facility directive] or [no entry]] CR LF	CTC TOWER 118.3 NOW or *[blank if no contact info]*
18	[[Local Information in accordance with facility directive] or [no entry]] CR LF	PLAN RWY 34L FOR DEP or *[blank if no local info]*
19	**ETX**	

B.1.1.3 PDC Data Message Content

Table B-3 describes the content of the PDC application-level data messages.

Table B-3. PDC Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**PDC**".
[Sequence Number]	sequence number	Integer	3	000 to 999
[Flight ID]	flight number or tail number	Text	10	Alphanumeric characters.
[Beacon Code]	beacon code	Text	9	Alphanumeric characters.
[Depart Point]	departure airport	Text	9	Alphanumeric characters beginning with "K", "T", or "P".
[Aircraft Type/Heavy Indicator]	aircraft body type and size classification	Text	14	Slash "/" delimited strings of alphanumeric characters.

[Depart Time]	P-time	Text	5	Always "**P**" followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Computer ID]	computer identification number	Text	3	Complex combination of alphanumeric characters.
[Altitude]	initial altitude	Text	3	Complex combination of alphanumeric characters.
[Route Information]	route	Text	29	Complex combination of alphanumeric characters.
[Route Information]	route	Text	29	Complex combination of alphanumeric characters.
[Route Information/Remarks]	route and/or remarks	Text	29	Complex combination of alphanumeric characters.
[Estimated Departure Clearance Time]	Departure clearance time estimate adjusted for traffic management initiatives.	Text	5	Always "**E**" followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Revision Number/Strip Request Originator of an SR]	Revision number assigned to the flight strip associated with the clearance	Text	19	Complex combination of alphanumeric characters.
[Departure Procedure (DP) or Standard Instrument Departure (SID) to be flown]	A published, named standard instrument departure clearance procedure	Text	39	Complex combination of alphanumeric characters
[associated climb-out instructions or initial heading]	ATC instructions as to how to proceed with the flight after departure to exit	Text	39	Complex combination of alphanumeric characters.

	airport airspace into TRACON airspace.			
[initial altitude]	The altitude flight needs to maintain until further ATC Instruction	Text	39	Complex combination of alphanumeric characters.
[Expected Altitude in the event of lost communications]	Guidance as to when the aircraft is likely to climb to their requested/filed altitude	Text	39	Complex combination of alphanumeric characters.
[DPFRQ (###.###)]	Departure Control Frequency for the pilot to tune in after takeoff to contact the TRACON or standard phraseology “In accordance with facility directive”.	Text	39	Complex combination of alphanumeric characters.
[Contact Information in accordance with facility directive]	Further instructions from the facility such as direction for pilot to contact tower ground	Text	39	Complex combination of alphanumeric characters.

	control			
[Local Information in accordance with facility directive]	Further instructions from the facility such as departure runway information	Text	39	Complex combination of alphanumeric characters.

B.1.2 PDC ACK Message

B.1.2.1 PDC ACK SMHP Message Format

A PDC message (depicted in Table B-4) is comprised of the SMHP header and the body which contains the PDC ACK message.

Table B-4. SMHP PDC ACK Message

Body Length	Sequence	Type	Version	Pad	Body
Xxxx	yyyy	PDC	0x10	0xA5A5A5	PDC ACK MSG

The body of a SMHP message of type PDC can contain either a PDC message or a PDC ACK message. PDC messages to CSPs and CSPs will only send PDC ACK messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.1.2.2 PDC ACK Data Message Format

Table B-5 describes the format of the PDC application-level acknowledgment messages.

Table B-5. PDC ACK Message Format

Line	Format	
1	**SOH** (optional) **LF** (optional)	QU SLCTWXA
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.YYZAGAC 111251
3	**STX** [SMI] **CR LF**	PDC
4	[Flight ID] **SPACE** [Sequence Number] **SPACE** [Participation Code] **SPACE** [Error Code] **SPACE** [Aircraft Registration Number] **SPACE** [Proposed Depart Time] **SPACE** [Gate Location] **CR LF**	DL262T 89 Y C .N101AA P2145 G20B
5	**ETX**	

B.1.2.3 PDC ACK Message Content

Table B-6 describes the content of the PDC application-level acknowledgment messages.

Table B-6. PDC ACK Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**PDC**".
[Flight ID]	flight number or tail number	Text	10	Alphanumeric characters.
[Sequence Number]	sequence number	Integer	3	000 to 999
[Participation Code]	ACK or NAK	Text	1	"**Y**" if message is ACK. "**N**" if message is NAK.
[Error Code]	reserved for algorithm	Text	1	Always "**C**".
[Aircraft Registration Number]	aircraft registration number	Test	7	Alphanumeric characters preceded by "**.**".
[Depart Time]	proposed departure time	Text	5	Always "**P**" followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Gate Location]	gate number returned by AOC	Text	5	Alphanumeric characters.

B.2 TIS Message

All D-ATIS messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z
Numeric characters 0 to 9
Characters "*", "@", ".", "-", " " (space), and "/".

D-ATIS message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.2.1 TIS Data Message

B.2.1.1 TIS SMHP Message Format

A TIS message (depicted in Table B-7) consists of the SMHP header and the body which contains the D-ATIS message.

Table B-7. SMHP TIS Message

Body Length	Sequence	Type	Version	Pad	Body
Xxxx	yyyy	TIS	0x10	0xA5A5A5	TIS MSG

The body of a TIS message can contain a TIS message or a TIS ACK message. The TDLS-MS will only send TIS messages to CSPs and CSPs will only send TIS ACK messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.2.1.2 TIS Data Message Format

Table B-8 describes the format of the D-ATIS application-level data messages.

Table B-8. TIS Data Message Format

Line	Format	
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU ANPDAXA
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.BNAATXA 071254
3	**STX** [SMI] **CR LF**	TIS
4	[Body] **CR LF**	AD BNA /OS CR1253 - BNA ATIS INFO R 1253Z. 30004KT 10SM SCT019 BKN095 BKN130 BKN200 25/21 A3001 (THREE ZERO ZERO ONE). ILS APCHS RY 2L, RY 2C IN USE. DEPG RY 2L, RY 2C. SIMUL DEPS IN PROG. CONTACT CLEARANCE DELIVERY 126.05 FOR CLEARANCE. NOTAMS... RWY 2R CLSD, RWY 31 CLSD. . . TAXIWAY ALPHA CLOSED NORTH OF ALPHA FOUR. Bird Activity in Vicinity of Airport. NUMEROUS TAXIWAY CLOSURES ASSOCIATED WITH CLOSED RUNWAYS. BNA TACAN AZIMUTH OTS. ...ADVS you have INFO R.
5	**ETX**	

B.2.1.3 TIS Data Message Content

Table B-9 describes the content of the D-ATIS application-level data messages.

Table B-9. TIS Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**TIS**".
[Body]	D-ATIS message	Text	2000	Complex combination of alphanumeric characters describing airport conditions in effect at the message creation time.

B.2.2 TIS ACK Message

B.2.2.1 TIS ACK SMHP Message Format

A TIS message (depicted in Table B-10) consists of the SMHP header and the body which contains the D-ATIS message.

Table B-10. SMHP TIS Message

Body Length	Sequence	Type	Version	Pad	Body
Xxxx	yyyy	TIS	0x10	0xA5A5A5	TIS ACK MSG

The body of a TIS message can contain a TIS message or a TIS ACK message. The TDLS-MS will only send TIS messages to CSPs and CSPs will only send TIS ACK messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.2.2.2 TIS ACK Data Message Format

Table B-11 describes the format of the D-ATIS application-level data messages.

Table B-11. TIS ACK Message Format

Line	Format	
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU BNAATXA
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.ANPDAXA 071259
3	**STX** [SMI] **CR LF**	TIS
4	[Body] **CR LF**	AD BNA /OS CR1253
5	**ETX**	

B.2.2.3 TIS ACK Message Content

Table B-12 describes the content of the D-ATIS application-level acknowledgment messages.

Table B-12. TIS ACK Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (TDLS) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	Source (CSP/AOC) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit ordinal day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**TIS**".
[Body]	D-ATIS message	Text	2000	Complex combination of alphanumeric characters.

B.3 GRM Message

All GRM messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z

Numeric characters 0 to 9

Characters ".", "-", " " (space), and "/".

GRM message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)

- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.3.1 GRM Data Message

B.3.1.1 GRM SMHP Message Format

A GRM message (depicted in Table B-13) is comprised of the SMHP header and the body which contains the Gate ID Request message.

Table B-13. SMHP GRM Message

Body Length	Sequence	Type	Version	Pad	Body
xxxx	yyyy	GRM	0x10	0xA5A5A5	GRM MSG

The body of a SMHP message of type GRM contains a Gate ID Request message. The TDLS-MS will only send GRM messages to CSPs and CSPs will only send GIR (Gate ID Request Response) reply messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.3.1.2 GRM Data Message Format

Table B-14 describes the format of the GRM application-level data messages and example content.

Table B-14. GRM Data Message Format

Line	Format	Example
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU ANPOCWN
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.BNATWXA 062117
3	**STX** [SMI] **CR LF**	GRM
4	[Flight ID] **SPACE** [Sequence Number] **SPACE** [Registration Number] **SPACE** [Depart Point] **CR LF**	SWA2331 89 N34522 KBNA
5	**ETX**	

B.3.1.3 GRM Data Message Content

Table B-15 describes the content of the GRM application-level data messages.

Table B-15. GRM Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**GRM**".
[Sequence Number]	sequence number	Integer	3	000 to 999
[Flight ID]	flight number	Text	10	Alphanumeric characters.
[Registration Number] *optional	tail number	Text	6	Alphanumeric characters
[Depart Point]	departure airport	Text	9	Alphanumeric characters beginning with "K", "T", or "P".

B.4 GIR Message

All GIR messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z

Numeric characters 0 to 9

Characters ".", "-", " " (space), and "/".

GIR message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.4.1 GIR Data Message

B.4.1.1 GIR SMHP Message Format

A GIR (Gate ID Request Response) message (depicted in Table B-16) is comprised of the SMHP header and the body which contains the GIR message.

Table B-16. SMHP GIR Message

Body Length	Sequence	Type	Version	Pad	Body
xxxx	yyyy	GIR	0x10	0xA5A5A5	GIR MSG

B.4.1.2 GIR Data Message Format

Table B-17 describes the format of the GIR application-level data messages and example content.

Table B-17. GIR Data Message Format

Line	Format	Example
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU BNATWXA
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	. ANPOCWN 062118
3	**STX** [SMI] **CR LF**	GIR
4	[Flight ID] **SPACE** [Sequence Number] **SPACE** [Registration Number] **SPACE** [Depart Point] **SPACE** [Gate Location] **CR LF**	SWA2331 89 N34522 KBNA G48A
5	**ETX**	

B.4.1.3 GIR Data Message Content

Table B-18 describes the content of the GIR application-level data messages.

Table B-18. GIR Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**GIR**".
[Sequence Number]	sequence number	Integer	3	000 to 999
[Flight ID]	flight number	Text	10	Alphanumeric characters.
[Registration Number] *optional	tail number	Text	6	Alphanumeric characters
[Depart Point]	departure airport	Text	9	Alphanumeric characters beginning with "K", "T", or "P".
[Gate Location]	gate number returned by AOC	Text	5	Always "**G"**; followed by 4 alphanumeric characters if the gate is known or "**G**" by itself if the gate is unknown

B.5 CCI Message

All CCI messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z

Numeric characters 0 to 9

Characters ".", "-", " " (space), and "/".

CCI message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.5.1 CCI Data Message

B.5.1.1 CCI SMHP Message Format

An Initial Dispatch message (CCI) (depicted in Table B-19) is comprised of the SMHP header and the body which contains the CCI message.

Table B-19. SMHP CCI Initial Clearance Message

Body Length	Sequence	Type	Version	Pad	Body
xxxx	yyyy	CCI	0x10	0xA5A5A5	CCI MSG

The body of a SMHP message of type CCI contains a copy of the initial clearance that was transmitted to the pilot (with a few exceptions). The TDLS-MS will only send CCI messages to CSPs and CSPs will only send CCA (ACK) messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively

B.5.1.2 CCI Data Message Format

Table B-20 describes the format of the CCI application-level data messages.

Table B-20. CCI Data Message Format

Line	Format *note3	Example
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU ANPOCWN
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.OKCTWXA 081251
3	**STX** [SMI] **CR LF**	CCI
4	[Sequence Number] **SPACE** [Disclaimer Text] **CR LF**	001 CPDLC DCL DISPATCH MSG - NOT TO BE USED AS A CLEARANCE
5	[Flight ID] **SPACE** [Depart Point] SPACE [Modified Route]***note1 CR LF**	SWA999 KJFK MODIFIED RTE
6	[Aircraft Equipment Type] **SPACE** [Depart Time] **SPACE** [Delimiter] **SPACE** [Registration Number] **CR LF**	H/B744/Q P1330 /AN N34522
7	[Computer ID] **SPACE** [Altitude] **CR LF**	01D FL320
8	[Route Information] **CR LF**	KJFK.JFK1..RBV..DANNER.J60.DJB.J34.CRL.. PMM.WYNDE5.KORD
9	[Route Information] **CR LF**	BREEZY POINT CLIMB
10	[Climb via Text] **CR LF**	CLB VIA SID EXC MAINT 4000FT
11	[Estimated Departure Clearance Time] **CR LF**	EDCT 1630
12	[Departure Frequency Data] **CR LF**	DEP FREQ 135.900
13	[Contact Info], [Local Info] **CR LF**	CTC GROUND CONTROL 121.9, ADV ON INIT CTC YOU HAVE ATIS
14	[Route Information] **CR LF**	***note2**
15	**ETX**	

NOTES:
note1: The MODIFIED RTE tag is only included with certain types of CCI, see TDLS-CSP IRD
note2: The final line in a dispatch message; Full flight plan included only if the uplink is CAF or UM79; not included if uplink is a UM80.
note3: If a particular line does not have any information it will be left blank

B.5.1.3 CCI Data Message Content

Table B-21 describes the content of the CCI application-level data messages.

Table B-21. CCI Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**CCI**".
[Sequence Number]	sequence number	Integer	3	000 to 999
[Disclaimer Text]		Text	55	Alpha characters; always **CPDLC DCL DISPATCH MSG – NOT TO BE USED AS A CLEARANCE**
[Flight ID]	flight number	Text	10	Alphanumeric characters.
[Depart Point]	departure airport	Text	4	Alphanumeric characters.
[Modified Route]	Indication that the route has changed since filing	Text	13	Alpha characters; when present always **MODIFIED RTE**
[Aircraft Equipment Type]		Text	7	Alpha character, followed by Slash "/", followed by 3 alphanumeric characters, followed by Slash "/", followed by single alphanumeric character

[Depart Time]	P-time	Text	5	Always "**P**" followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Delimiter]	delimiter for registration number field	Text	3	Always "**/AN**"
[Registration Number]	tail number	Text	6	Alphanumeric characters
[Computer ID]	computer identification number	Text	3	Complex combination of alphanumeric characters.
[Altitude]	requested altitude	Text	9	Complex combination of alphanumeric characters: [FL{Expected Level}] [{Expected Altitude}FT][FL{Expected BlockAltitude}]
[Route Information 1]	route	Text	1000	Complex combination of alphanumeric characters: [CLEARED TO [{AIRPORT DESTINATION} AIRPORT {SID}.{TRANSITION FIX} [{CLIMBOUT}][{position} VIA]]{Route Information}
[Route Information 2]	route	Text	80	Complex combination of alphanumeric characters: [{SID}.{TRANSITION FIX}][AFTER {position} CLEARED TO {AIRPORT DESTINATION} ARPT][THEN][AS FILED]
[Climb Via Text]	initial altitude and climb instructions	Text	80	Complex combination of alphanumeric characters: [{climbviatext}] [MAINT [{initial altitude}FT][FL{initial level}]]
[Estimated Departure Clearance Time]	EDCT	Text	5	Always "**EDCT**", followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Departure Frequency Data]	departure frequency	Text	15	**DEP FREQ** followed by (1) three numerical characters, a period and three numerical characters (NNN.NNN); (2) or seven alpha characters (SEE SID)
[Contact Info]		Text	32	Complex combination of alphanumeric characters.
[Local Info]		Text	34	Complex combination of alphanumeric characters.
[Free Text]	full route	Text	1000	Complex combination of alphanumeric characters: [{Airport Departure}[{SID}][.{TRANSITION FIX}] {route

				info}[{ TRANSITION FIX}][.{STAR}] {AIRPORT DESTINATION}]

B.6 CCR Message

All CCR messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z
Numeric characters 0 to 9
Characters ".", "-", " " (space), and "/".

CCR message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.6.1 CCR Data Message

B.6.1.1 CCR SMHP Message Format

A Revised Dispatch message (depicted Table B-22) is comprised of the SMHP header and the body which contains the CCR message.

Table B-22. SMHP CCR Revised Clearance Message

Body Length	Sequence	Type	Version	Pad	Body
xxxx	yyyy	CCR	0x10	0xA5A5A5	CCR MSG

The body of a SMHP message of type CCR contains a copy of the revised clearance that was transmitted to the pilot (with a few exceptions). The TDLS-MS will only send CCR messages to CSPs and CSPs will only send CCA (ACK) messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.6.1.2 CCR Data Message Format

Table B-23 describes the format of the CCR application-level data messages.

Table B-23. CCR Data Message Format

Line	Format	Example
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU ANPOCWN
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.OKCTWXA 081251
3	**STX** [SMI] **CR LF**	CCR
4	[Sequence Number] **SPACE** [Disclaimer Text] **CR LF**	005 CPDLC DCL DISPATCH MSG - NOT TO BE USED AS A CLEARANCE
5	[Flight ID] **SPACE** [Depart Point] **SPACE** [Revision Text] **CR LF**	FDX9901 KMEM REVISED RTE DPP EXP ALT DEPFREQ
6	[Aircraft Equipment Type] **SPACE** [Depart Time] **SPACE** [Delimiter] **SPACE** [Registration Number] **CR LF**	D/A320/Q P1610 /AN N34522
7	[Computer ID] **SPACE** [Revised Expected Altitude] **CR LF**	555 REVISED EXP ALT FL350
8	[Revised Route] **CR LF**	REVISED RTE CLEARED TO GCK VIA EOS ICT
9	[Revised Departure Procedure] **CR LF**	REVISED DPP ZUMIT.FOXOM, AFTER GCK REST OF ROUTE UNCHANGED
10	[Revised Alt] **CR LF**	MAINT 5000FT
11	[Revised Estimated Departure Clearance Time] **CR LF**	REVISED EDCT 1630
12	[Revised Departure Frequency Data] **CR LF**	REVISED DEPFREQ 117.250
13	[Revised Contact Info] **CR LF**	REVISED CONTACT CTC GROUND CONTROL 121.9,
14	[Revised Local Info] **CR LF**	REVISED LCLINFO ADV ON INIT CTC YOU HAVE ATIS
15	[Route Information] **CR LF**	KMEM.ZUMIT.FOXOM..EOS..ICT..GCK.. KD48W..HVE..ILC..OAL.MADN5.KOAK
16	**ETX**	

B.6.1.3 CCR Data Message Content

Table B-24 describes the content of the CCR application-level data messages.

Table B-24. CCR Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (CSP/AOC) address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**CCR**".
[Sequence Number]	sequence number	Integer	3	000 to 999
[Disclaimer Text]		Text	54	Alpha characters; always **CPDLC DCL DISPATCH MSG – NOT TO BE USED AS A CLEARANCE**
[Flight ID]	flight number	Text	10	Alphanumeric characters.
[Depart Point]	departure airport	Text	4	Alphanumeric characters beginning with "K", "T", or "P".
[Revision Text]	revised field tags	Text	59	Alpha characters; **REVISED** followed by **RTE DPP ALT EXP ALT DEPFREQ EDCT CONTACT LOCALINFO** separated with a space depending on revised fields
[Aircraft Equipment Type]	aircraft type and	Text	7	Alpha character, followed by Slash "/", followed by

	equipment info			3 alphanumeric characters, followed by Slash "/", followed by single alphanumeric character
[Depart Time]	P-time	Text	5	Always "**P**" followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Delimiter]	delimiter for registration number field	Text	3	Always "/**AN**"
[Registration Number]	tail number	Text	6	Alphanumeric characters
[Computer ID]	computer identification number	Text	3	Complex combination of alphanumeric characters.
[Revised Expected Altitude]	revision to expected altitude	Text	25	Alpha characters **REVISED EXP ALT** followed by complex combination of alphanumeric characters: [FL{Expected Level}][{Expected Altitude}FT][FL{Expected BlockAltitude}]
[Revised Route]	revision to route	Text	1000	Alpha characters **REVISED RTE** followed by complex combination of alphanumeric characters: [CLEARED TO {position} VIA][AT {position} CLEARED]{ route information}
[Revised Departure Procedure]	revision to departure procedure	Text	80	Alpha characters **REVISED DPP** followed by complex combination of alphanumeric characters: {SID}[.{TRANSITION FIX},][{CLIMBOUT},]][AFTER {position} REST OF ROUTE UNCHANGED]
[Revised Altitude]	revision to initial altitude and climb instructions	Text	80	Alpha characters **REVISED ALT** followed by complex combination of alphanumeric characters: {climbviatext}][MAINT [{initial altitude}FT][FL{initial level}]
[Revised Estimated Departure Clearance Time]	revision to EDCT	Text	18	Alpha characters **REVISED EDCT** followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Revised Departure Frequency Data]	revision to departure frequency	Text	23	Alpha characters **REVISED DEPFREQ** followed by (1) three numerical characters, a period and three numerical characters (NNN.NNN) or (2) seven

				alpha characters; SEE SID
[Revised Contact Info]	revision to contact information	Text	48	Alpha characters **REVISED CONTACT** followed by complex combination of alphanumeric characters.
[Revised Local Info]	revision to local information	Text	50	Alpha characters **REVISED LCLINFO** followed by complex combination of alphanumeric characters.
[Free Text]	full route	Text	1000	Complex combination of alphanumeric characters: [{Airport Departure}[{SID}][.{TRANSITION FIX}] {route info}[{ TRANSITION FIX}][.{STAR}] {AIRPORT DESTINATION}]

B.7 CCA Message

All CCA messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z
Numeric characters 0 to 9
Characters ".", "-", " " (space), and "/".

CCA message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.7.1 CCA Data Message

B.7.1.1 CCA SMHP Message Format

A Dispatch Message Acknowledgement (depicted in Table B-25) is comprised of the SMHP header and the body which contains the CCA message.

Table B-25. SMHP CCA Dispatch Message Acknowledgement

Body Length	Sequence	Type	Version	Pad	Body
xxxx	yyyy	CCA	0x10	0xA5A5A5	CCA MSG

The TDLS-MS will only send CCR messages to CSPs and CSPs will only send CCA (ACK) messages to the TDLS-MS. Note that the <SOH>, <STX>, and <ETX> strings are printable representations of the non-printable control characters SOH (ASCII 0x01), STX (0x02), and ETX (0x03) respectively.

B.7.1.2 CCA Data Message Format

Table B-26 describes the format of the CCA application-level data messages.

Table B-26. CCA Data Message Format

Line	Format	Example
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU BNATWXA
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	. ANPOCWN 062117
3	**STX** [SMI] **CR LF**	CCA
4	[Flight ID] **SPACE** [Sequence Number] **SPACE** [Registration Number] **SPACE** [Depart Time] **SPACE** [Gate Location] **CR LF**	SWA2331 89 N34522 P2145
5	ETX	

B.7.1.3 CCA Data Message Content

Table B-27 describes the content of the CCA application-level data messages.

Table B-27. CCA Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**".
[IATA Destination ADDR]	destination (TDLS) IATA address	Text	7	Alphanumeric characters.
[IATA Source ADDR]	source (CSP)/AOC IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**".
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute.
[SMI]	System Message Identifier	Text	3	Always "**CCA**".
[Flight ID]	flight number	Text	10	Alphanumeric characters.
[Sequence Number]	sequence number	Integer	3	000 to 999
[Registration Number]	tail number	Text	6	Alphanumeric characters
[Depart Time]	P-time	Text	5	Always "**P**" followed by four numerical characters representing a valid time in 24-hour format HHMM.
[Gate Location] *optional	gate number returned by AOC	Text	4	When present always "**G**"; followed by 3 alphanumeric characters or blank **Note: This item is ignored, gate information is exchanged using GRM/GIR messages*

B.8 CCP Message

All CCP messages consist of ASCII characters with the message content limited to the following:

Uppercase alphabetic character A to Z

Numeric characters 0 to 9

Characters ".", "-", " " (space), and "/".

CCP message content delimiters include the following ASCII characters:

- CR (carriage return)
- LF (linefeed/newline)
- SOH (start of heading)
- STX (start of text)
- ETX (end of text)

B.8.1 CCP Data Message

B.8.1.1 CCP SMHP Message Format

A Pilot Response Dispatch (CCP) message (depicted in Table B-28) is comprised of the SMHP header and the body which contains the CCP message.

Table B-28. SMHP CCP Pilot Response Dispatch Message

Body Length	Sequence	Type	Version	Pad	Body
xxxx	yyyy	CCP	0x10	0xA5A5A5	CCP MSG

A Pilot Response Dispatch (CCP) message is sent when the pilot response to a particular clearance is received.

B.8.1.2 CCP Data Message Format

Table B-29 describes the format of the CCP application-level data messages.

Table B-29. CCP Data Message Format

Line	Format	Example
1	**SOH** [IATA MSG Priority] **SPACE** [IATA Destination ADDR] **CR LF**	QU ANPOCWN
2	[IATA Source ADDR] **SPACE** [Timestamp] **CR LF**	.BNATWXA 062117
3	**STX** [SMI] **CR LF**	CCP
4	[Sequence Number] **CR LF**	001
5	[Flight ID] **SPACE** [Depart Point] **SPACE** [Delimiter] **SPACE** [Registration Number] **CR LF**	FDX9901 KMEM /AN N34522
6	[Pilot Response Text] **SPACE** [Pilot Response] **CR LF**	PILOT RESPONSE - WILCO
7-18	Lines 4-15 of corresponding Dispatch Message; CCI or CCR	See Table B-20 (CCI) or B-23 (CCR)

B.8.1.3 CCP Data Message Content

Table B-30 describes the content of the CCP application-level data messages.

Table B-30. CCP Data Message Content

Data Identifier	Description	Data Type	Max Length	Permissible Values
[IATA MSG Priority]	IATA message priority	Text	2	Always "**QU**"
[IATA Destination ADDR]	destination (CSP/AOC) IATA address	Text	7	Alphanumeric characters
[IATA Source ADDR]	source (TDLS) IATA address preceded by "."	Text	8	Alphanumeric characters preceded by "**.**"
[Timestamp]	message creation time	Integer	6	Numeric characters in the format "ddhhmm" indicating a valid time where "dd" is the two-digit day of the month, "hh" is the two-digit hour in 24-hour format, and "mm" is the two-digit minute
[SMI]	System Message Identifier	Text	3	Always "**CCP**".
[Sequence Number]	sequence number	Integer	3	000 to 999
[Flight ID]	flight number	Text	10	Alphanumeric characters
[Depart Point]	departure airport	Text	4	Alphanumeric characters beginning with "K", "T", or "P"
[Delimiter]	delimiter for registration number field	Text	3	Always "**/AN**"
[Registration Number]	tail number	Text	6	Alphanumeric characters

[Pilot Response Text]	pilot response identifier	Text	17	Always "**PILOT RESPONSE –** "
[Pilot Response]	pilot response to an initial or revised clearance	Text	6	"**WILCO**", "**UNABLE**" or "**ROGER**"

This page intentionally left blank.