Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS “FOR OFFICIAL USE ONLY” OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A “NEED-TO-KNOW” BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

This page left blank intentionally

Data Consolidation Point (DCP)-to-Network Access Device (NAD) Interface Control Document (ICD)
Version 1.0

U.S. Department of Homeland Security (DHS)
Science and Technology Directorate (S&T)
Cargo Security Test and Evaluation (CSTE)

Document Control CM/CS/SSC/-/REQ/R1.0/2010/1779

December 6, 2010

Point of Contact:
DHS Science and Technology Cargo Security Program Manager
Kenneth Concepcion
Kenneth.Concepcion@dhs.gov
(202) 254-5351

Container Security Test and Evaluation Team
Lawrence Livermore National Laboratory
Pacific Northwest National Laboratory
Sandia National Laboratories

United States Department of Homeland Security
Science and Technology Directorate

Cargo Security Integrated Test and Evaluation Program

Technical Document Disclaimer

This document presents scientific and technical data resulting from testing and evaluation activities performed within the Science & Technology (S&T) Borders and Maritime Cargo Security Integrated Test and Evaluation Program (CSTE). Where possible, CSTE testing is performed in accordance with national or international consensus standards. When testing is performed for federal acquisition programs, test criteria are derived from systems requirements for the acquisition program. In other cases, test criteria are based on CSTE technical expertise and the U.S. Government's anticipated future mission requirements.

System performance results presented herein reflect the best efforts of the CSTE technical staff, but they neither guarantee nor endorse the suitability of the system for untested applications or other system requirements. Federal, state, local, or tribal agencies seeking to use this report as source selection criteria in an acquisition action must evaluate this report against their specific mission requirements.

This report does not constitute a federal endorsement of any tested system. Use of this report in whole or in part for commercial vendor advertising and marketing materials is strictly forbidden, and no permission for such use will be granted.

Document Revision History

Note: Third column in the table below defines the ICD revision that used in the message header.

Date	Document Version	Message Header, ICD Revision Code. (0x00 not allowed)	Summary of Primary Changes

Table of Contents

List of Tables

List of Figures

1 Introduction

This Department of Homeland Security (DHS) Interface Control Document (ICD) provides the requirements for wireless communication between Network Access Devices (NADs) and Data Consolidation Points (DCPs). For the purposes of this ICD, a *conveyance* is an ISO 668 Dry Shipping Container, motor carrier trailer, or comparable rail enclosure.

The intent of this ICD is to enable utilization of common hardware for message exchanges between all NADs and DCPs, for both commercial messages and security-related messages. This document specifies in detail the communication protocols and network architecture needed to design the interfaces among all devices that this document is applicable to.

Network Access Devices (NADs, a.k.a. “readers”) include both fixed and handheld devices. *Data Consolidation Points* (DCPs), with which Security Devices communicate (See [3]), must interoperate with Security Device System elements defined in [3], but the structure of networks surrounding the DCPs and how these are arranged internationally is outside the scope of this document.

2 Background

The Container Security Initiative (CSI), announced in January 2002 by Customs and Border Protection (CBP), mandates that containers bound for the U.S. posing a potential risk to national security need to be examined at foreign ports. CSI consists of four key elements: (1) using intelligence and automated information to identify and target containers that pose a risk, (2) pre-screening those containers that pose a risk at the port of departure before they arrive at U.S. ports, (3) using detection technology to quickly pre-screen containers that pose a risk, and (4) using smarter, tamper-evident containers. The Department of Homeland Security (DHS) has determined that tracking and monitoring the security of intermodal container shipments are necessary to provide the required level of security information to both industry and government agencies to safeguard our borders.

The security of the global supply chain is one of DHS’s highest priorities. The ability to secure the integrity of a container/conveyance as it moves through the global supply chain is vital to our nation’s security. During the last ten years, private industry and government agencies have investigated ways to improve security in the global supply chain in an effort to protect against criminal activity and terrorist attacks. This has included development of improved mechanical and electronic container seal technology, sensor systems, and inspection agreements/processes to identify and monitor cargo movement at major ports and transit points throughout the world. In anticipation of new U.S. Government policies on enhanced security requirements for all U.S.-bound cargo, various government and industry teams have been investigating ways to adapt existing technologies and processes to provide monitoring of containers from the Point of Stuffing (PoS) to the Point of Deconsolidation (PoDC). The use of Security Device Systems in the global supply chain is one component of an improved security system.

The goal of the DHS S&T cargo security program is to provide requirements and open standards for Security Device Systems and components that will enable commercial competition and global interoperability for international container security. DHS recognizes that the security requirements must take into consideration technology, people, and procedures. Any commercial vendor developing container/conveyance security technologies must consider impacts to existing

commercial and economic global supply chain operations in considering their design choices. This document formalizes the requirements for Security Devices consistent with DHS's security needs and operations in the context of shipping operations as described in 7, [2] and [3].

3 Scope of the Document

This Interface Control Document (ICD) describes in detail the protocols necessary to satisfy the communication requirements of the Network Access Device (NAD)-to-Data Consolidation Point (DCP) interfaces. Reference [3] addresses data security, encryption, and key management in detail. This document addresses the communications requirements that are specific to the DCP.

3.1 Document Precedence and Nomenclature

Systems currently under development by the Department of Homeland Security include the Container Security Device (CSD), the Advanced Container Security Device (ACSD), the Hybrid Composite Container (HCC), Marine Asset Tag Tracking System (MATTS), and the Security Device System. Among the goals of these programs are to characterize movement and status of cargo containers and to develop technologies to detect door openings and intrusions. The ACSD, CSD, HCC and MATTS programs are managed by DHS Science and Technology (S&T) Directorate with the goal of deploying technologies to monitor all six sides (including both doors) of an ISO 688 Dry Shipping Container for intrusion while in storage and in transit. The Security Device System as envisioned further utilizes a layered security concept to provide maximum automated cargo security functions supporting container shipping from the PoS through the PoDC) in the United States.

All requirements pertaining to ACSD, CSD, HCC, MATTS and the DCP that are contained within other Security Device, MATTS or ECoC Requirements Documents are still applicable to the DCP; however, in the event of any conflicts between those documents and this one, this document has precedence with respect to the DCP communications-related capabilities, operations and functions.

3.2 System Overview

This Department of Homeland Security Interface Control Document provides the requirements for the communications interface between a Data Consolidation Point and secure and unsecure forms of Network Access Devices.

It is fully understood that, in time, multiple DCPs may exist. This document covers requirements to support a single/first DCP and its interactions with various NADs. Inter-DCP communications and multi-DCP control of single CSSCs are beyond the scope of this document. Similarly the necessary communications, interfaces, and operational concerns between DCP and the Encryption Key Management Facility (KMF) to allow for key management operations are beyond the scope of this document.

3.2.1 Data Consolidation Points (DCPs)

A DCP is a data portal for secure messaging between Security Device System elements described in [1] and [2] and essentially provides control for the entire cargo security network. The expectation is that the initial DCP designated by DHS to be the end-point for Security Device-originated messages and DCP commands/responses as described in [3]. This DHS-designated DCP must be a physically and electronically secure facility able to process thousands

or millions of secure messages from various cargo security devices daily. It must also be able to securely communicate with the Key Management Facility (KMF) and other DCPs as described in 7, [2] and [4].

3.2.2 Network Access Devices (NADs)

NADs act as the communications bridge to/from on-conveyance devices whose embedded Communications Module (CM) function is the primary wireless communications interface. All of the requirements for wireless communication between the on-conveyance Communication Modules (CMs) and Network Access Devices (NADs) are provided in [3]

Devices that contain a CM function include Container Security Devices (CSDs), Advanced Container Security Devices (ACSDs), Electronic Chain of Custody (ECoC) Devices, and External Communication Modules (ECMs). Collectively, these are called Cargo Security System Components (CSSCs) and depicted in Figure 4-1.

4 Interface Description

A DCP exchanges message-based data with CSSCs via NADs in either real time or in time-deferred batch data transfers. The capabilities of NADs are fully described in [5]. Restricted Commands, as described in [3] are sent by the DCP to on-conveyance CMs via NADs. Secure Data is received by the DCP from on-conveyance CMs and NADs and are protected from unauthorized access, modification, and spoofing by the use of encryption. The DCPs have the ability to:

1. Decrypt the Secure Data from CSSCs
2. Generate Restricted Commands,
3. Transfer Encryption Keys,
4. Process Security Device Event Logs,
5. Process Status Messages from NADs, and
6. Organize and control the cargo security network via automated tools and human operators.

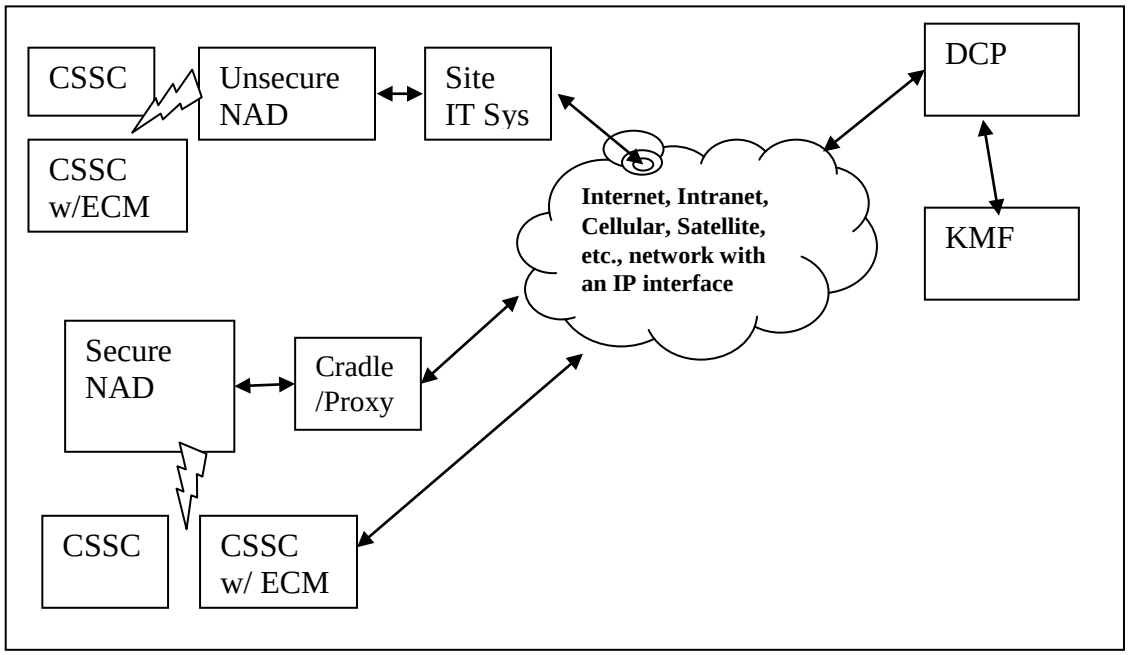

Figure 4-1, Top Level System View

The terminology in Figure 1 is as follows:

1. Data Consolidation Point – The system end-point that communicates bi-directionally with designated NADs per [3], with the KMF, and/or a higher-level organization by means not defined in this document.
2. Non-secure NAD – A device installed at facilities such as intermodal terminals, ports or manufacturers' loading docks. These devices are generally assumed to be unattended and are not given the credentials to decrypt CSSC encrypted data.
3. Secure NAD – A device that supports a subset of DCP functionality from the on-conveyance devices' perspective. Secure NADs are generally assumed to be in the

possession of a DHS-designated Trusted Agent. As such they may be given the credentials to encrypt/decrypt. Connectivity with the DCP is assumed to be intermittent.

4. Advanced Container Security Device (ACSD) - A device that is a form of CSSC. ACSDs are internally mounted and detect door openings, removals and container breaches. ACSDs communicate with NADs, and may communicate via an ECM (see below).
5. Container Security Device (CSD) - A device that is a form of CSSC. CSDs are internally mounted and detect door openings and removals. CSDs communicate with unsecure NADs similar to ACSD and may communicate via an ECM (below).
6. External Communications Module (ECM) - A device that is a form of CSSC. ECMs are functionally similar to non-secure NADs, but are battery powered and installed externally on conveyances. An ECM has two independent roles: (1) As an optional “relay” repeater between an NAD and a CCSC inside the container, as a range extension method; (2) As a device that securely reports status to a DCP via various wireless means using the messaging defined in [3]for security-related tracking information. An ECM may perform both logical functions simultaneously.
7. Electronic Chain of Custody Device (ECoC) - A device that is a form of CSSC. ECoCs are mounted external to a conveyance and may communicate with devices inside the conveyance, as does an ECM. An ECoC may communicate with a variety of wireless means using the messaging defined in [3]and [5]for security-related information.

4.1 Overall Data Flow

The bi-directional data flow of the Security Device Network is as follows**:**

1. The DCP communicates securely with CSSCs via non-secure NADs in real-time, provided connectivity is available.
2. The DCP communicates securely with secure NADs in batch/non-real time or in real time as defined by the particular device. CSSCs are given the security credentials to communicate with the DCP.
3. Secure NADs are given the security credentials to communicate with CSSCs designated by the DCP.
4. Non-secure NADs, unattended, have no security credentials and may act as transparent relays.
5. DCP may communicate with managing organizations (not shown/defined herein).
6. CSSCs communicate per the secure wireless methods in defined in [3].

4.2 Network Overview

4.2.1 DCP Operation

The purpose of the DCP is to present human operators with the information they need to determine if various CSSC devices are functioning properly and securely. The information presented should allow operators to make judgments about the security posture of the cargo network from a global perspective, down to specific trade lanes, and even down to specific conveyances.

The requirements discussed in this document are not intended to specify a preferred implementation or configuration for the DCP from an operational sense. There are no

requirements that specify a particular data management system, hardware or user interface. The full set of operational requirements of the DCP and processes to support these requirements are beyond the scope of this document.

The following is a short list of functions that have to be performed from an operational perspective. It is assumed that the DCP will:

1. Have a policy to protect data stored or retransmitted after receipt by the methods defined in this document.
2. Securely communicate with NADs per the protocols and formats defined in this document.
3. Securely communicate with the KMF.
4. Maintain and present to operators the connectivity status and history for all communications interfaces defined in this document. This includes both real time connectivity and scheduled connectivity with NADs.
5. Accept from all NADs status and log history information produced by on-conveyance devices and retain such data in a database, indexed by device UID.
6. Form data packages for NADs to execute Arm and Deactivate commands and related actions, allocating tasks to specific secure NADs via secure data packets.
7. Provide secure NAD-specific encryption information to the correct NAD at or before required time, via the methods defined in this document.
8. Be able to aggregate the information received to present a useful security picture of targeted aspects of the cargo security network to the DCP operators.

4.2.2 Types of NADs and Interfaces

The DCP must support communication with the various forms of NADs over the various available interfaces. These interfaces include wired interfaces connecting DCPs to Fixed NADs (FNADs) and (HNAD) cradles over IP, as well as Embedded Wide Area Network (WAN) interfaces acting as Embedded NADs. These WAN interfaces can provide cellular or satellite data services. It is envisioned that future products and services will define other types of NADs. For the purposes of this document, there are two categories of NADs: Non-secure NADs and secure NADs.

4.2.3 Non-secure NADs

Non-secure NADs act as functionally transparent wireless-to-IP bridges that cannot encrypt or decrypt security-purposed application layer messages passing between DCP and CSSCs. Non-secure NADs must do the following:

1. Pass messages to-and-from a DCP without data payload modification.
2. Use various public/private WANs to connect to the DCP.
3. Are elements of an untrusted network, of the same security role of switches and routers in such WANs
4. Generally are installed in locations that do not assume the presence or physical access control by, a DHS-designated Trusted Agent.

The non-secure NAD may have other security features associated with the network its backend is

tied into. Nothing in this document would preclude such functionality. For instance a non-secure NAD may or may not use IPSec as part of the networking protocols with which it delivers data.

4.2.4 Secure NADs

At the other functional extreme are secure NADs that possess authorizing credentials (Encryption Keys) that allow them to issue restricted commands and access encrypted messages and log files in the same fashion as a DCP. These devices are intended to always be in a fully secure area or in possession and complete control of a DHS-designated Trusted Agent. In the latter case, secure NADs are most likely to be portable. All forms of secure NADs must do the following:

1. Securely communicate with a DCP
2. Authenticate to DCP for download of Encryption Keys
3. Provide user the capability to view the secure Data from CSSCs per [3] and [5].
4. Aggregate and package sensitive in order to ship securely to DCP
5. Aggregate and package data secured by the CSSC devices as bound to the DCP

Secure and non-secure NADs as defined in [5] provide the capabilities to support to both ends of the security and functional spectrum. As other types of NADs become available they may have differing levels of access to security data provided by CSSCs and different levels of control in the cargo security network.

5 Security Architecture

The CSSC each have a unique identity code (UID), a value that uniquely defines them. This value is used in the security applications to allow authentication of data and ensure communications with intended devices are supported. Similarly the DCP must have a unique identification that the CSSCs are aware of. The DCP's UID is bound into the key derivation functions that allow CSSCs to communicate with secure NADs.

1. Every DCP is assigned a unique 64-bit (8-byte) DCP UID.
2. The DCP UID must be communicated directly to CSSC devices for secure communication.
3. All NADs must be able to communicate the UID of their parent DCP to communicate securely with the CSSCs.

To communicate secure messages to/from a CSSC, the DCP must store certain sensitive information. This includes keys obtained from the KMF and decrypted data obtained from CSSCs. The DCP's stored data obtained from the KMF or from the on-conveyance device is protected from unauthorized access or transmission on any media, in accordance with DCP security plan policy. This policy is beyond the scope of this document.

6 Communications

6.1 Communications Interface

1. The DCP Shall implement an IPv4 network interface or higher for data exchanges with non-secure NADs which bridge messages defined in [3] to/from the IEEE Standard 802.15.4-2006 wireless links to CCSCs. The DCP to/from non-secure NAD specifics are given in this document. Message security is defined in 7 and [4], and, is independent of the WAN transport service provider.
2. The DCP Shall implement an IPv4 network interface or higher for data exchanges with non-secure NADs, and CCSCs that communicate on a WAN via cellular data and satellite. The DCP also supports IPv4 interfaces to such public carrier WAN services. Message security is defined in [4] and is independent of the WAN transport service provider.
3. The DCP Shall implement an IPv4 compatible network interface or higher for data exchanges with secure NADs and utilize previously "batch" transferred data to later securely exchange data with CCSCs. The specifics of the batch transfers are given in this document. Message security is defined in [4] and is independent of the WAN transport service provider.
4. The DCP securely exchanges data with a distant or co-located KMF. Message security is defined in [4] and is independent of the WAN transport service provider.

The characteristics of the interface to the KMF database are beyond the scope of this document. This document defines methods to enable a DCP interoperable interface to each category of NAD, irrespective of the manufacturer of the NAD and independent of the specifics of varying DCPs.

6.2 DCP-to-NAD Data Connection

The DCP **Shall** accept both session-based and session-less connections from NADs or their on-site proxy. The security and transport protocols for both connection types are defined in preceding sections and are applicable for data packet exchange with the DCP at any point throughout the trip.

6.2.1 DCP-to-Non-secure NAD Data Transfer

If the CSSC is at a locale and in coverage of a non-secure NAD, the DCP **May** pass commands through the non-secure NAD using the encryption keys held by the DCP. An example is a shipping dock equipped with a non-secure FNAD(s) with IP network connectivity. The same is true for status queries, log retrieval or de-activation/de-commission by a DCP.

6.2.2 DCP-to Secure-NAD Data Transfer

The secure NAD, when in communications with the DCP, directly or via an on-site proxy, **Shall** exchange all trip information and CSSC data through encrypted batch file transfers. This can include the data needed for all of the commands of [3] and encryption credentials. This information can also used by personnel or automated processes on site to plan tasks for secure NADs. A secure NAD **Shall** obtain the encryption keys for transactions with assigned CSSC UIDs by messaging defined in this document. This done, the secure NAD is then able to undertake the tasking as directed by the DCP or DHS-designated Trusted Agent.

6.3 DCP-to/from-Secure NADs Network Protocol

All DCP IP to secure NAD data traffic **Shall** be compatible with IPv4 or higher standards. DCP to secure NAD data transfers can be accomplished per the following in an unattended manner when the devices are not in use by personnel. This condition provides secure NADs with IP connectivity with DCP(s) directly (cradle) or indirectly via an on-site proxy. In the case of a proxy or terminal server, the data flow from proxy to NAD shall conform to DCP Information Assurance (IA) policy.

6.4 DCP-to-Secure NAD Retrieval of CSSC Encryption Keys

The secure NAD or its proxy **Shall** obtain the encryption keys for CSSCs to which the operator/NAD is tasked. The messaging varies, but the means to obtain keys given here applies to all. The DCP has the option to securely Commission/ARM CSSCs via a direct connection through an on-site non-secure FNAD if available. This section, however, applies to the use of a secure NAD. Encryption keys are transferred from the DCP to a secure NAD as follows:

1. A secure NAD, having received a list of CSSC UIDs and related data and instructions must now obtain the Encryption Key to conduct secure data transactions for each CSSC. This is needed to authenticate and autonomously communicate with the CSSC per [4].
2. The DCP accepts secure File Transfer Protocol (FTP) connections from the secure NAD. The DCP authenticates by username/password and logs all connections. The username and password strength is governed by local IA policies.
3. The DCP provides a data file on the FTP server for the particular secure NAD or its proxy that has connected. This is the only file in the login directory. The content of this file is a list of UID- Encryption Key pairs matching the assignments made by the user in the preceding paragraph.
4. The secure NAD or its proxy downloads this file via secure FTP connection process and is described as follows:
    - The CSSC UIDs in the file are compared to the work assigned list of CSSC UIDs previously obtained by the secure NAD.
    - The FTP session now terminates.
    - The DCP logs this event.
    - If the list is deemed inaccurate by the secure NAD or its proxy, an exception will be alerted to on site staff for disposition and the secure NAD will become idle until re-tasked.

With the downloaded list of UID correlated Encryption Keys, the secure NAD is able to accomplish the tasking that involves secure data and command transactions for those CSSC UIDs. The NAD Requirements Document [5] defines Encryption Key security while stored in the secure NAD, and how/when this is information is to be destroyed.

6.4.1 Communications Data Prerequisites

The following sections describe the prerequisites for communications between a NAD and a DCP.

6.4.1.1 Non-secure NAD

The non-secure NAD **Shall** be provided the DNS address of the DCP(s) it will conduct message exchanges with upon installation/commissioning.

6.4.1.2 Secure NAD

Every secure NAD and/or its on-site proxy, **Shall** be provided the following information:

1. The UID of each DCP with which the secure NAD or its proxy will perform message exchanges with
2. Public network address that corresponds to each DCP UID, this being an edge router/firewall or other IT-defined mechanism for remote access to the DCP server.
3. An IP address and server login/password/home file directory. These may be used by automation on the secure NADs (or a proxy) rather than by persons. For each secure NAD (or its proxy) supported by a given DCP-UID. That is, for each secure NAD UID, there is a login account for a specific DCP UID. (The server function may be isolated/outside of firewalls at a DCP, etc. to meet IA policy.)

6.4.2 Communications to Commission/Arm a CSSC

If a CSSC is in the coverage of anon-secure FNAD with a real-time connection to the DCP, the DCP **May** use the messages in [3] to pass trip information and commission/arm a CSSC after personnel or systematic approvals to do so. Alternatively, and the topic of this section, a policy/practice compliant procedure **May** be used by a secure NAD without real-time connection to a DCP to commission/arm a CSSC.

6.4.2.1 Commission/Arm CSSC Prerequisites

A specific CSSC on or in a conveyance that is selected by the user **Shall** be made known to the DCP. The DCP data correlates conveyance ID, Seal ID, and manifest number, needed for Commission/Arm. This combined with the secure NAD UID and the CSSC Encryption Key previously provided by the DCP, enables the Arm/Commission task to be undertaken with secure commands that require the trip data plus the security credentials.

6.4.2.2 DCP-to-Secure NAD, Start of Trip Commission/Arm Data

The following steps **Shall** be completed prior to securely communicating with a CSSC for a Commission/Arm action by a secure NAD:

1. The DCP obtains the conveyance ID, manifest ID, and seal ID (per [3]) from the user.
2. The DCP obtains a list of conveyance IDs, and associated with each, a list of one or more secure NAD UIDs that is planned to communicate with the CSSC UID in that conveyance.
3. The DCP obtains from the KMF per [4] the LTK for each CSSC UID obtained in step 2, above. There may be multiple NAD UIDs for one CSSC UID if the user needs such, e.g., first-available secure NAD does the task.

6.5 General Packet Format for Message Based Interfaces

This DCP-to-NAD messaging is bi-directional and packet-based as defined for the following interfaces:

1. Non-secure NADs
2. KMF
3. ECMs and ECoCs when using public carrier (cellular/satellite) for security purposed per 7 and [2].

Note: This packet message interface is NOT used for secure (handheld) to/from NADs. The secure HNAD to/from DCP interface is described in Section 6.2.2.

This document combined with [4] specify a means such that the DCP does not need a priori knowledge of the IP address of remote site gateways used by non-secure NADs. Each packet has a general preamble followed by content, as defined in this document. Each packet has a response for flow control and error correction. Packets are sent via either connectionless UDP or via TCP connections per the conventions in this document.

The message rates may be low and infrequent for a given NAD, thus the implementer may find at large scale (NAD counts), that UDP is more reliable as compared to the need for persistent or recurring connections if TCP is chosen. Thus, ECMs and ECoC using public carrier (cellular/satellite) may use either UDP or TCP. The use of Network Address Translations (NAT) is assumed to be the norm, i.e., public IP addresses for NADs are not required.

NOTE: In this document's communications context, data sent/received by DCPs may be via a relay. This may be the norm for commercial NADs and on-conveyance devices that communicate via WANs. Per [4], sensitive data is encrypted by the secure NAD, CSSC or DCP. For such, the relay is akin to the switches and routers in the public carrier/Internet WAN and are untrusted. Non-secure NADs also do not encrypt/decrypt in their bridging function. The security mechanism of [4] enables the message integrity and authentication of the message originator by the destination system.

Table 6-1 depicts the General Packet Preamble for all packets exchanged via the above-listed DCP interfaces.

Table 6-1, Packet Message Interfaces' General Preamble Format

General Packet Preamble Format		
Size (bytes)	**Data Content**	**Notes**
For UDP: 8 For TCP: 0	For UDP: UDP header per Request for Commands (RFC) in IPv4 For TCP: Not present See note to the right	**NOTE 1:** The operating system, if any, may remove these UDP header bytes and pass the packet size and source IP address via an API. However, as transmitted, the UDP RFC requires these 8 bytes be transmitted.
1	Packet Format Revision letter (v), as a null-terminated one-character string, as: v\0 **FOR DCP-ORIGINED MESSAGES, PER THIS DOCUMEMENT, THE REVISION LETTER SHALL BE: A**	\0 depicts an ASCII NULL byte.
3	Function Code A number, 000-999, as three one-byte ASCII numeric digits, formatted as: ddd\0 Codes 000-499 are **reserved** for exclusive use per this ICD. For codes 500-999, all bytes subsequent to this Function code are not defined by this document.	Codes by function are listed in this document's subsequent sections \0 depicts an ASCII NULL byte.
8	The numeric ID of the entity producing this message, as 16 one-byte ASCII hexadecimal digits, with leading zeros, as: ddddddddddddddd\0 Byte order: leftmost digits depict byte at lowest offset in array-bytes, as in the message header of [3]. The is number shall be inserted by the message originator	For messages sent from the DCP, the ID is the UID of the DCP. For messages to the DCP, the ID shall be the UID of the sending NAD, to include the non-secure NAD's UID (i.e., UID not used for encryption), or the UID of the sending KMF. Valid for the reserved Function Codes. \0 depicts an ASCII NULL byte.
0 or n	0 or more additional text or binary data bytes, according to the Function Code above. Formatted per the specific packet Function Code shown above. Content per function code shall be wholly contained in one standard IP packet.	The size and format of additional bytes is given in the definition of the particular added content.

6.5.1 DCP UID and IP Address

Every DCP **Shall** have one associated UID. This UID is used by non-secure NADs, to inform (included in the NADA message of [3]) the DCP's identity. Per [4], this permits the CSSC to use the proper security credentials for that UID. A CSSC may retain the credentials for multiple DCPs according to the needs due to mobility. A KMF for a given DCP has security credential information based on an unchanging UID for a DCP and for CSSCs subordinated to that and optionally other DCPs.

The UID of a DCP **Shall Not** have a fixed association with a DCP's IP address. This UID cannot change though the IP address may. For the DCP's purposes, the LAN IP address of a NAD is assumed to be a non-public address, assigned by the local IT authorities as a static, DHCP, or DHCP reservation. The DCP does not need knowledge of these LAN IP values.

Security sensitive data is encrypted at the application message level. Thus, the DCP does not require a secure transport layer. This is to avoid TLS/SSL, digital certificates, etc. when using simple non-secure NADs.

6.6 DCP to/from Non-secure NADs

The DCP **Shall** communicate with non-secure NADs via IPv4 or higher UDP or TCP with the General Packet Preamble in Table 6-1.

6.6.1 UDP Option

Each UDP-based NAD communicating with a DCP **Shall** be provided at time of installation, the following:

1. Primary DCP UID per [3],
2. IP address,
3. UDP port number and
4. WAN gateway/subnet mask

A NAD optionally has a list of alternative/back-up DCP IP addresses and port numbers. The DCP should not assume this is the case.

The DCP accepts incoming UDP packets on the designated port from a valid NAD-gateway IP address for the sites affiliated with the DCP. The DCP may block/ignore others according to the firewall configurations for multiple services.

Each packet will have the NAD's UID in the General Packet Preamble of Table 6-1. As Non-secure NADs are relay/bridges and do not encrypt or decrypt, the non-secure NAD UID may not exist in the KMF database.

The DCP sends response UDP packets on the same port number as received, and to the IP address of the corresponding incoming packet's originator. This will be the firewall/gateway servicing the NAD. The LAN/WAN gateway administrator will assure that packets on the chosen port are not blocked for incoming or outgoing packets.

For policy reasons, the remote site administrator may elect to configure the firewall/gateway to route UDP for a NAD with a static LAN address solely to/from that IP address for a chosen port number. This assures that packets on a selected port (or port range), irrespective of the packet source on the WAN, go only to NADs and not other servers on the LAN.

The DCP **May** discard incoming packets for security or system loading reasons. The protocols of [3] will detect such and retry later. Messages in this document provide means for an authenticated DCP to alter the Primary DCP interface values should the need arise to change the DCP interface port number, a single DCP's IP address, and the IP address of the local WAN gateway router/firewall.

6.6.2 TCP Option

Each TCP-based NAD communicating with a DCP **Shall** be provided the following at time of installation:

1. Primary DCP UID per [3],
2. IP address,
3. TCP port number and
4. WAN gateway/subnet mask.

A NAD **May** have a list of alternative/back-up DCP IP addresses and port numbers. The DCP should not assume this is the case.

The DCP accepts incoming TCP connections on the designated port from a valid NAD-gateway IP address for the sites affiliated with the DCP. The DCP **May** block/ignore others according to the firewall configurations for multiple services.

The TCP-based NAD is responsible for initiating the TCP connection as needed. The DCP supports concurrent TCP connections from NADs where the total is chosen by the DCP administrator. When this number is exceeded, the DCP rejects the TCP connection attempt. The DCP may forcibly terminate a TCP connection for security reasons such as abusive or unintended high connection rates. The DCP may also discard incoming packets for security or system loading reasons. The protocols of [3] will detect such and retry later.

Messages in this document provide means for an authenticated DCP to alter the Primary DCP interface values should the need arise to change the DCP interface port number, a single DCP's IP address, and the IP address of the local WAN gateway router/firewall.

Security data is encrypted at the application message level. Thus, the DCP does not require a secure transport layer. This is to avoid TLS/SSL, digital certificates, etc. within simple non-secure NADs.

6.6.3 DCP-to/from- Non-secure NAD Connect to DCP

For both TCP and UDP connections, the host DCP gets notification of an incoming packet to the address provided to the NAD during installation/commissioning. Therefore, no introductory connection message/response is required.

6.6.4 Get Time and Date Message

See Section 6.6.5.1 below.

6.6.5 DCP-to-Non-secure NAD Packet Messages

This section defines the IP packets exchanged bi-directionally by a DCP and non-secure NAD via either UDP or TCP. Each message is a single packet. A DCP **Shall** accept from-NAD packets in the formats shown below. Every packet will conform to the General Packet Preamble format defined in Section 6.5.

6.6.5.1 DCP-to-Non-secure NAD Heartbeat Request Packet

Every DCP **Shall s**end this packet to every DCP-subordinated unsecure NAD, at intervals an interval in the range of 30 to 300 seconds. Because the Heartbeat Packet contains the date/time (UTC), the receiving NAD **May** set its internal clock, and use that in NADA broadcasts on wireless, per [3]. CSSCs **May** extract date/time from the NADA message for their use per [3].

The DCP **Shall** produce the Heartbeat Packet format shown in Table 6-2.

Table 6-2, DCP-to-Non-secure NAD Heartbeat Request Packet Format

DCP-to-Non-secure NAD Heartbeat Request Packet, Function Code 000 (in packet preamble)		
Size in bytes	**To-DCP Data Content**	**Notes**
	GENERAL PACKET PREAMBLE	
3	Maintenance Code, two one-byte ASCII numeric digits followed by an ASCII NULL, is as: 00\0	00-49 – reserved 50-99 – manufacturer-specific
15	Date/Time, UTC, as one-byte ASCII characters, of the form: YYYYMMDDhhmmss\0	\0 depicts the ASCII NULL byte January = 1.

6.6.5.2 Non-secure NAD-to-DCP Heartbeat Response Packet

A non-secure NAD responds to heartbeat request message packet sent only by the designated DCP, based on both the source IP address and the preamble's DCP ID being that for which the NAD is configured. Non-secure NADs **Shall** send this packet in response to not less than 90% of received Heartbeat Request packets

A DCP **Shall** accept this packet from only NADs who's ID in the preamble is among those designated as subordinated to the particular DCP.

On receipt of a valid heartbeat response, the DCP updates health status for that NAD. On receipt of an invalid heartbeat, the DCP updates a non-secure NAD configuration error status for the reporting NAD (e.g., NAD failed to change DCP affiliation as commanded by message or locally reconfigured).

The DCP **Shall** accept the Heartbeat Response Packet format shown in Table 6-3.

Table 6-3, Non-secure NAD-to-DCP Heartbeat Response Packet

Non-secure NAD-to-DCP Heartbeat Packet Response, Function Code 000 (in packet preamble)		
Size in bytes	**To-DCP Data Content**	**Notes**
	GENERAL PACKET PREAMBLE	
3	Maintenance Code, as two one-byte ASCII numeric digits followed by an ASCII NULL, is as: 00\0	00 – Normal Condition 01 – Maintenance Attention Required 02 – 802.15.4 network hardware fault 03 – 802.15.4 network CCA failures or MAC-ACK timeouts are excessive (e.g., due to persistent interference) 04-49 – reserved 50-99 – manufacturer-specific

6.6.6 Non-secure NAD-TO-DCP: CSSC ICD Content Category 1

Here, *CSSC ICD Content* means any message defined by the ICD [3], literally and unchanged in its binary form. A non-secure NAD **Shall** produce the packet defined in Table 6-4. This content will have been created and optionally encrypted by a CSSC communicating with the non-secure NAD.

The DCP accepts such content and process the information provided per the DCP functional requirements. The DCP **Shall** provide a response to each received message, formatted per [3], and transmitted to the unsecure NAD as shown in the next section. The DCP **Shall Not** respond to messages from NADs who's ID is invalid for this DCP (not affiliated). The NAD ID is in the packet preamble.

The DCP processes valid packets of this type in accordance with [3], which defines which messages are themselves a response and which yield a response. Unsolicited messages to a DCP must have a response.

Table 6-4, NAD-to-DCP, CSSC ICD Content

Non-secure NAD-to-DCP Packet Type: CSSC ICD Message Content, Function Code 010		
Size (bytes)	**To-DCP Data Content**	**Notes**
	GENERAL PACKET PREAMBLE	
variable	Binary byte-oriented ICD data content per [3], to include message header, content, and message integrity check (MIC) bytes for restricted messages.	Size is located in the [3] ICD header content, where the header size is fixed and the message size plus variable MIC size is inclusive.

6.6.7 DCP-to-Non-secure NAD: CSSC ICD Content

Here, *CSSC ICD Content* means any message defined by 7, literally and unchanged in its binary form. The DCP **Shall** produce the packet defined in Table 6-5. The non-secure NAD **Shall** accept the packet and forward to the CSSC. This content may be encrypted by the DCP depending on message type. The DCP processes a response to this from-DCP message. A response will be sent by the CSSD via the NAD if it is a DCP's command to the CSSC, with the exception of a DCP's ACK message, as defined in [3]. The response **Shall** be formatted as in Table 6-4.

Table 6-5, DCP-to-Non-secure NAD: CSSC ICD Content

DCP-to-Non-secure NAD CSSC ICD Message Content, Function Code 011		
Size (bytes)	**To-DCP Data Content**	**Notes**
	GENERAL PACKET PREAMBLE	
variable	Binary byte-oriented ICD data content per [3], to include message header, content, and message integrity check (MIC) bytes for restricted messages.	Size is located in the [3] ICD header content, where the header size is fixed and the message size plus variable MIC size is inclusive.

6.6.8 DCP-to-Non-secure NAD, Change DCP IP Address

This function enables, with authentication, a DCP to alter the following configuration items retained by a NAD in non-volatile storage:

1. DCP IP address, protocol (TCP vs. UDP), port number
2. LAN Gateway IP address, subnet mask
3. NAD ID number. (Note: Non-secure NADs do not have a UID as used for encryption purposes. The NAD ID number in this message is for the DCP indexing of a place name database, irrespective of the non-secure NAD's private NATed IP address).

This is to reduce the need for physical access to the device for a change. The change may be caused by a shift in DCP roles or an IP address management change at a DCP. The command's success is observable by the DCP, now using the changed DCP IP address, issuing Heartbeat packets and receiving a response. The NAD ignores the packet if either (a) *Four Byte authentication code* in the DCP message depicted in Table 6-6 does not agree with that retained in the NAD's non-volatile memory; or (b) the DCP UID in the General Packet Preamble is not that for which the NAD is configured.

The NAD **Shall** ignore the packet if the *Four Byte authentication code* does not match that expected, or if the parameters are invalid. The NAD **Shall** retain the *New Four Byte authentication code*, if they differ, for future use. The DCP retains the current *Four Byte authentication code* used for some or for all NADs. The DCP assigns DCP IP addresses, protocol and port numbers in accordance with Section 6.6 of this document

Note: if the configuration change is ignored by the NAD, it may be necessary to locally access the NAD to correct the settings.

The DCP Shall produce the message format shown in Table 6-6.

Table 6-6, DCP-to-Non-secure NAD, Change DCP IP Format

DCP-to-Non-secure NAD Change DCP IP Address, Function 002		
Size (bytes)	**To-DCP Data Content**	**Notes**
9	Authentication code, as 8 hexadecimal digits in one-byte per character ASCII form, with terminating NULL byte, as: `ABC12345\0`	The NAD will ignore this function if the authentication code does not match that stored in non-volatile memory. Where \0 denotes an ASCII NULL
9	Replacement Authentication code, formatted as above If 8 zeros, replacement is not performed	The NAD will replace the value stored in non-volatile memory if the code is non-zero and differs from the current authentication code
variable	Protocol and Port selection: as a one-byte ASCII character depicting the protocol to use, followed by one or more ASCII numeric digits depicting the port number to use, followed by an ASCII NULL, as: N\0 for no change `U12345\0` for UDP `T54321\0` for TCP	Where \0 denotes an ASCII NULL
variable	New DCP IPv4 address, one-byte per character ASCII form, with terminating NULL byte, in dot form, as: `111.222.333.13\0`	Where \0 denotes an ASCII NULL **NOTE**: A non-public IP address may be used if the DCP and all NADs are in the same private network or virtual private network (VPN) (organization/corporate domain) irrespective of the carrier used for the WAN
variable	New LAN Gateway IPv4 address. Format as shown above, or if no change, place a zero in all octets.	
variable	New LAN Subnet Mask Format as shown above, or if no change, place a zero in all octets	
variable	New NAD ID	Note: Non-secure NADs do not have a UID used for encryption purposes. The ID number in this message is for indexing to a place name database.

6.6.8.1 CSSC UID Message Exchange

Examples and guidelines are shown in Table 6-7.

Table 6-7, Security Device ICD Message Exchange

Example DCP Message Exchange Descriptions		
Activity	**Data Content**	**DCP Action**
Incoming unsolicited message	Per [3] At this writing, the only *unsolicited* message received by the DCP is *Restricted Status* with the "is unsolicited" bit flag set to true. NOTE: An unsolicited message may arrive at any time due to real-time events in the on-conveyance device systems. For example, the DCP may receive an unsolicited message though the DCP last sent a command and expects an ACK. In this case, the unsolicited message takes precedence. The on-conveyance device shall ignore the DCP's messages except for ACK for the unsolicited message. That is, the DCP's time-coincident command is ignored or lost. The DCP will retry the command if still applicable, using the same transmit ascension number succeeding the DCP's ACK to the unsolicited status.	Extract originating on-conveyance device's UID from message header. Validate the ICD revision number given in the header and adjust message handling accordingly. If the Long Term Key (LTK) for the UID for this DCP is not known, use KMF messaging to obtain the LTK and proper message ascension numbers for transmit and receive. If the UID is already known, retrieve from DCP cache the LTK and ascension numbers. An incoming message to the DCP with an ascension number (originator's transmit ascension number) that is identical to that last received; the DCP will consider the message as a duplicate. If the message is a duplicate, skip to "send response ACK" below. Decrypt the message per the procedure in [3]. If failure, discard message and send no response. Optionally log locally for diagnosis. Take appropriate database add/modify actions using the decrypted data. Update the Registry data for the device UID, for all relevant Registry data record items. **Send response ACK:** Prepare an ICD ACK message with the proper transmit ascension number and encryption. Prepare a UDP or TCP packet with the UID of the destination device pre-pended as shown in this document. Transmit the message to the IP address from which the incoming UDP or TCP packet came. The originating on-conveyance device will retry n times (per [1]) if the DCP's ACK is lost or indecipherable. If retries are exhausted, the originating device will log the error. The DCP itself cannot otherwise determine if the ACK was undeliverable. The DCP will increment the DCP's transmit ascension number and expected receive ascension numbers for the UID in question after the first ACK transmission. All subsequent retransmissions due to duplicate incoming messages will use the same message as the first attempt, including the original ACK's transmit ascension number. The Registry update done by the DCP will have the ascension numbers associated with a successful message exchange, regardless of retransmissions due to duplicate incoming messages.
DCP ad-hoc Command	DCP command message per [3] Commands are restricted (encrypted)	DCP has reason to send an ad-hoc command to an on-conveyance device given its UID. DCP retrieves from the Registry the last known IP address for the subject UID. If this is unknown, the command cannot be sent and

Example DCP Message Exchange Descriptions		
Activity	**Data Content**	**DCP Action**
	or unrestricted (non-encrypted). Most are restricted. The DCP ACK message is sent as the response to a valid incoming unsolicited message. Every DCP message to an on-conveyance device has one or more specific response messages. Each incoming (to DCP) response message is of the same restricted/unrestricted type as the command. **Timing:** The response to a DCP outgoing message is delayed according to the power conservation characteristics of the target device. E.g., a response may be immediate if the device has sent a prior message within the last two seconds (per [3]). The worst-case response time is 30 seconds. Longer times indicate a device or network error condition or loss of wireless coverage.	the process or person is so notified and faults the action. Otherwise, DCP obtains the LTK and ascension numbers for the subject UID from the DCP's local cache. If that is absent in the cache, the DCP takes either of two courses: (1) The DCP faults the attempt notifying the process or person; or (2) the DCP messages the KMF to obtain a new LTK for the subject UID, performs over the air rekeying and ascension number initialization. On success, the DCP updates the Registry data record for the UID, noting the date/time and UID of the DCP doing the rekeying. With the proper LTK and ascension numbers for the target UID, the DCP composes a command message and transmits that to the IP address obtained from the DCP's cache or from the Registry. The DCP now times out the proper response from the target UID, this being defined in [1]. Most often, this is a status message marked "solicited". The timeout period is 30 seconds. On each timeout, the DCP retransmits the identical message, up to 5 times. When retries are exhausted, the DCP notifies the process or person affected and logs such for diagnostic purposes. The DCP then updates the Registry with the next in sequence transmit and receive ascension numbers, as if the message had been successful. On receipt of a response to the command message, the DCP validates that the UID in the message header is as expected and take appropriate action based on the ICD version number in the header. Next, the DCP compares the ascension number in the message header to the DCP's expected number. If the received number is less than the expected number, the message is to be ignored as a duplicate of an irrelevant prior message exchange. If the received number is greater than the expected number, the DCP logs "lost message" detection for diagnostic purpose and proceed to decrypt and process then message. The expected ascension number will be adjusted to reflect the lost message(s). If the received or adjusted (for lost messages) number is the expected number, the DCP proceeds to decrypt the message. If decryption which (includes a MIC validation) fails, the DCP retransmits the identical command and begin a new response time-out. After 5 retransmissions, the DCP notifies the process/person affected and log the error for diagnosis. The DCP compares the one-byte Message ACK No. in the solicited response to the transmitted command's ascension number's least significant byte. If these differ, the DCP takes the same action as for a decryption error. (The one-byte ascension number is in [3], for solicited status and for the first solicited event log record.)

Example DCP Message Exchange Descriptions		
Activity	**Data Content**	**DCP Action**
		On successful validation and decryption, the DCP updates the database as appropriate. The DCP then updates the relevant Registry data for the UID. The DCP, for a failed (retransmissions exhausted) or successful message increments the DCP transmit ascension number for the subject UID. The UID's expected receive ascension number, at this point, is to be one greater than the actual or expected receive ascension number. These numbers will be saved to the DCP's cache.
DCP command yielding multiple responses	At this writing, the DCP command messages that may yield more than one response message are: • Send Log • Send Unsent (portion of) Log • AoS Inventory Discovery	[1] defines how the DCP determines that the last response of the series has been received. A timeout on receipt of the "last" response constitutes a partial loss of data and the appropriate recovery will be taken by the DCP. This may be a retry of the entire message set or notification of the affected process/person, plus diagnostic logging.

6.6.9 DCP-to/from-Non-secure NAD, Error Detection and Correction

Every DCP conforms to the following protocol and parameters for error detection and correction.

Table 6-8, DCP-to/from-Non-secure NAD Error Detection and Correction

	DCP Error Condition	**DCP Action**
1	When the TCP connection option is used, rather than UDP, a connection-closed event or TCP keep-alive fault is detected at the DCP for a given NAD	None. NAD or its proxy is responsible for error recovery.
2	A DCP-transmitted message has no response	The DCP enforces a response-packet time-out of 30 seconds. DCP retransmits up to 5 times for error correction. Unsuccessful delivery shall trigger automated or manual intervention. The cause may be a transport LAN/WAN error, loss of wireless coverage, decryption error, or ascension number mismatch. Locally, log the anomaly for diagnosis purposes.
3	A DCP-received security message is invalid. This includes decryption errors, ascension number sequencing, message type versus context, and other causes	Send no response. Locally, log the anomaly for diagnosis purposes.
4	Message Ascension Number Handling (ascension numbers are unique for each on-conveyance device)	Initial value transmit and receive numbers, or after rekeying, is 1, as detailed in the message security document cited in [3]. See also the affect of re-keying on the ascension numbers.

6.7 DCP-to/from-Secure NADs Message Exchange

DCP-to-secure NADs data transfers can be accomplished per the following in an unattended manner when the devices are not in use by personnel. This condition provides secure NADs with IP connectivity with DCP(s) directly (cradle) or indirectly via an on-site proxy. In the case of a proxy or terminal server, the data flow from proxy to NAD shall conform to DCP Information Assurance (IA) policy.

6.7.1 DCP-to-Secure NAD Retrieval of CSSC Encryption Keys

The secure NAD or its proxy will obtain the encryption keys for CSSCs to which the operator/NAD is tasked. The messaging varies, but the means to obtain keys given here applies to all. The DCP has the option to securely Commission/ARM CSSCs via a direct connection through an on-site non-secure FNAD if available. This section, however, applies to the use of a secure NAD as follows:

1. A secure NAD, having received a list of CSSC UIDs and related data and instructions **Shall** obtain the Encryption Key to conduct secure data transactions for each CSSC. This is needed to authenticate and autonomously communicate with the CSSC per [4].
2. The DCP **Shall** accept secure File Transfer Protocol (FTP) connections from secure NADs. The DCP authenticates by username/password and logs all connections. The username and password strength is governed by local IA policies.
3. The DCP **Shall** provide a data file on the FTP server for the particular secure NAD or its proxy that has connected. This is the only file in the login directory. The content of this file is a list of UID- Encryption Key pairs matching the assignments made by the user in the preceding paragraph.
4. The secure NAD or its proxy **Shall** download this file via secure FTP connection process and is described as follows:
   - The CSSC UIDs in the file is compared to the work assigned list of CSSC UIDs previously obtained by the secure NAD.
   - The FTP session now terminates.
   - The DCP logs this event.
   - If the list is deemed inaccurate by the secure NAD or its proxy, an exception is alerted to on site staff for disposition and the secure NAD will become idle until re-tasked.

With the downloaded list of UID correlated Encryption Keys, the secure NAD is able to accomplish the tasking that involves secure data and command transactions for those CSSC UIDs. The NAD Requirements Document [5] defines Encryption Key security while stored in the secure NAD, and how/when this is information is to be destroyed.

6.7.2 DCP-provided Data Prerequisites

Every secure NAD and/or its on-site proxy, **Shall** be is provided the following information:

1. The UID of each DCP with which the secure NAD or its proxy will perform message exchanges.
2. Public network address that corresponds to each DCP UID, this being an edge

router/firewall or other IT-defined mechanism for remote access to the DCP server.

3. An IP address and server login/password/home file directory. These may be used by automation on the secure NADs (or a proxy) rather than by persons. For each secure NAD (or its proxy) supported by a given DCP-UID. That is, for 'n' secure NAD UIDs, there are 'n' login accounts for a specific DCP UID. (The server function may be isolated/outside of firewalls at a DCP, etc. to meet IA policy.)

6.8 Communications to Commission/Arm a CSSC

If a CSSC is in the coverage of a non-secure FNAD with a real-time connection to the DCP, the DCP **May** use the messages in [3] to pass trip information and commission/arm a CSSC after personnel or systematic approvals to do so.

Alternatively, and the topic of this section, a policy/practice compliant procedure **May** be used by a secure NAD without real-time connection to a DCP to commission/arm a CSSC. The balance of this section details the communications for the secure NAD alternative.

A specific CSSC is on or in a conveyance that is selected by the user then made known to the DCP. Therefore, the DCP data includes conveyance ID, Seal ID, and manifest number, used for Commission/Arm. This combined with the secure NAD UID and the CSSC Encryption Key previously provided by the DCP, enables the Arm/Commission task to be undertaken with secure commands by the secure NAD that require the trip data plus the security credentials.

6.8.1 DCP-to-Non-secure NAD, Start of Trip Commission/Arm Data

Since the non-secure NAD acts as a transparent bridge, the DCP **Shall** use the messaging described in [3] to conduct the CSSC Commission/Arm sequence using a non-secure NAD.

6.8.2 DCP to Secure NAD, Start of Trip Commission/Arm Data

The following steps **Shall** be completed prior to securely communicating with a CSSC for a Commission/Arm action by a secure NAD:

1. The DCP obtains the conveyance ID, manifest ID, and seal ID (per [3]) from the user.
2. The DCP obtains a list of conveyance IDs, and associated with each, a list of one or more secure NAD UIDs that is planned to communicate with the CSSC UID in that conveyance.
3. The DCP obtains from the KMF per [4] the LTK for each secure NAD UID and CSSC UID obtained in step 2, above. There may be multiple NAD UIDs for one CSSC UID if the user needs such, e.g., first-available secure NAD does the task.

6.8.3 DCP Trip Information Data File (TIF)

The DCP **Shall** use the data from steps 1-3 in Section 6.8.1 to generate one or more ***Trip Information File(s) (TIF).*** The TIF contents include the conveyance IDs and CSSC UIDs which secure NADs at a given site will utilize in a restricted time period. The length of this time period **Shall** be determined by the DCP and local site administrators.

The format of a TIF file, given below, enables one file to have the data for one secure NAD UID (SNADUID), listing all the assigned CSSCs for that secure NAD. A different secure NAD may also be given the same CSSC data so that either secure NAD may work the task. A TIF file **May**

include multiple secure NADs and their CSSCs in one file. This may be used by a proxy to retrieve all data for all secure NADs in one file and de-collate off-line. The choice of TIF file content **Shall** be a decision coordinated by the DCP and site administrators.

6.8.3.1 Trip Information File Encryption

The DCP formats all TIF file contents for compatibility with the AES-256 FIPS -197 encryption option of the WinZip file compressor software utility. The encryption key/password is referred to as the **Secure Trip Data File Passkey.** The **Secure Trip Data File Passkey** is provided and changed by the DCP administrator as needed per local or DCP policy, for use by manual and automated processes at sites where secure NADs are used. The method of this exchange is not described in this document.

6.8.3.2 Trip Information File Naming

The TIF's validity period commencement **Shall** be given by the file's name and contents on line one of the file. The file's validity expiration is within the file. The file contains information for one, many, or all secure NADs, as agreed to by DCP and secure NAD site administrators.

The file name convention **Shall** be:

XUUUUUUUUUUUUUUUU-YYYYMMDDhhmmss.zip

Where: X is the character X if the file contains XLM and T if the file contains tag-value, for the formats shown in the next section.

U's are the file-producing DCP's UID as 16 hexadecimal digits

YYYYMMDDhhmmss is the UTC date/time after which the file is valid (Jan = 01)

6.8.3.3 Trip Information File Contents

The DCP Shall produce two TIF file formats for use by one or a group of secure NADs or its/their proxy, where the information in each is the same. The secure NAD or its proxy **May** choose the file format that is most prudent based on data processing resources.

6.8.3.4 Trip Information File XML format

The unencrypted content of the TIF is textual XML, whose schema **Shall** be as follows. The secure NAD UID is always unique within one TIF file.

Where XML data elements

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name=”DCPUID” type="xs:string" />“
<xs:element name”VALIDITY">
  <xs:complexType>
  <xs:element name=”EFFECTIVEUTC” type="xs:string" />“
  <xs:element name=”EXPIRESUTC” type="xs:string" />“
</xs:complexType>
<xs:element name="SNADUID">
    <xs:complexType>
      <xs:sequence>
        <xs:element name=CSSCUID" type="xs:string" />
        <xs:element name="ConveyanceIDTypeCode" type="xs:string" />
        <xs:element name="ConveyanceID" type="xs:string" />
        <xs:element name="ManifestID" type="xs:string" />
        <xs:element name="SealID" type="xs:string" />
        <xs:element name="LTK" type="xs:string" />
        <xs:element name="RKK" type="xs:string" />
        <xs:element name="RKC" type="xs:string" />
        <xs:element name="AUX" type="xs:string" />
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

From above, the parameter `DCPUID` conveys the UID of the DCP producing this data

`EFFECTIVEUTC and EXPIRESUTC` are strings as: YYYYMMDDhhmmss in UTC date/time, Jan=01 depicting the validity time period for the file’s contents

`SNADUID` conveys 16 hexadecimal digits being the 8 byte UID of the secure NAD (SNADUID) to which this record applies

`ConveyanceIDTypeCode` conveys two hexadecimal digits being the conveyance ID code type as in [1], e.g,. ISO is 00, as in [3]

`ConveyanceID` conveys the alphanumeric conveyance ID and check characters as in [3]

`ManifestID` conveys the alphanumeric manifest ID as in [3]

`SealID` conveys the alphanumeric seal ID as in [3]

`LTK` is 16 hexadecimal digits depicting the long term key as 8 bytes given in [4]

`RKK` is 16 hexadecimal digits depicting the rekey key as 8 bytes given in [4]

`RKC` is 16 hexadecimal digits depicting the rekey count as 8 bytes given in [4]

`AUX` is zero or more alphanumeric data character strings, separated by commas

The DCP provides the encrypted TIF files to secure NADs or their on-site proxy via a means not

defined in this document, e.g., FTP, email, HTTP server, etc. On receipt, the secure NADs or their proxy decrypt, and place in secure storage, the XML or tag-value records. The secure NAD or its proxy then extracts the data and ensures that each secure NAD has the records pertinent to the secure NAD. The secure NAD will use the record data which matches both its UID and the CSSC UID in order to be able to conduct secure data and command transactions in defined in [3].

6.8.3.5 TIF File Tag-value Format

This format has the same information as the XML file, but in tag=value format, with one set of data per line. Each line shall end with ASCII CR/LF. If "=" appears in a tag's value, it shall be escaped with an ASCII backslash.

Line 1 is as follows:

```
DELIM=character, DCPUID=string, EFFECTIVEUTC=string, EXPIRESUTC=string
```

```
Where the one character to the right of DELIM is the value-tag delimiter for the file, followed by that character as the first actual delimiter. The DELIM shall be a printable ASCII character, e.g., a comma, semi-colon, etc. but shall not be a backslash. An example line 1 is:
```

```
DELIM=,, DCPUID=0x0102030405060708, EFFECTIVEUTC=20101231000000, EXPIRESUTC=20101231235900
```

Line 2 is

```
SNADUID=value
```

Line 3 is

`CSSCUID` = value, … For the tag/values in the XML format for a particular CSSCUID.

For additional CSSCUID's for the same SNADUID, line 3 is repeated.

For a different SNADUID, the content of line 2 now is given in the file, followed by one or more CSSCUID lines (Line 3) for all SNADUIDs and CSSCUIDs provided in this file.

The secure NAD Shall use the record data which matches both its UID and the CSSC UID in order to be able to conduct secure data and command transactions described in [3].

6.8.4 Secure NAD-to-DCP Data Transfer

At any point during a trip, a secure NAD may receive information from CSSCs via the protocols in [3]. This section defines how that data is communicated, non-real-time, to the DCP, when the secure NAD is in a condition to communicate with the DCP, e.g., in a cradle or Wireless LAN coverage, etc.

6.8.4.1 Secure NAD-to-DCP, CSSC ICD Data

The CSSC status and/or log data records are conveyed non-real-time to the DCP as follows. The secure NAD or its proxy **Shall** receive and store binary data messages in the format defined in [3]as received from CSSCs. The NAD Requirements Document [5]states which message types must be saved and communicated to the DCP.

All pertinent binary messages as in [3] **Shall** be concatenated with no added bytes, into one file as described in [5]. The content of each message is in decrypted/plain-text form, using the credentials for the secure NAD to CSSC keying.

This file **Shall** be encrypted by the secure NAD or its proxy, by the same file encryption method defined in 6.8.3.1 for the DCP-to-Secure NAD trip data file. The file name is the same as in 6.8.3.1, with the UTC in the file name being the UTC of the final CSSC communications.

The secure NAD or its proxy **Shall** transfer the file to the DCP using the same file transfer method, in reverse, as used in 6.8.3.1 for the DCP-to-Secure NAD trip data file. The DCP logs this incoming file and process its contents according to DCP procedure.

6.8.4.2 Secure NAD-to-DCP, NAD Activity Log Data

The secure NAD Activity Log as described in [5] **Shall** be accepted for upload by the DCP. The file content and format is tag-value textual **Shall** be as follows:

Line 1: SNADUID=UUUUUUUUUUUUUUU, UTC=YYYYMMDDhhmmss

Where U's are the secure NAD's UID and UTC is the time/date of file creation

Line 2: CSSCUID= UUUUUUUUUUUUUUU, UID=YYYYMMDDhhmmss

Where U's are the a CSSC's UID and UTC is the time/date of the last communication

Line 3: +COMPLETION=x for the CSSC UID

Where x is a textual task completion status code, with x=OK if no anomalies

Line 4: +NOTES:

Operator notes for the CSSC UID, if any

Line 5: if present, is another CSSCUID as in line 2, followed by the same line 3 and 4

This file **Shall** be encrypted by the secure NAD or its proxy, by the same file encryption method defined in 6.8.3.1 for the DCP-to-Secure NAD trip data file. The file name shall be the same as in 6.8.3.1, with the UTC in the file name being the UTC of the final CSSC communications.

The file name **Shall** be as follows:

TUUUUUUUUUUUUUUUUYYYYMMDDhhmmss.zip

Where U's are the secure NAD's UID and YYYYMMDDhhmmss is the UTC as in the file's line 1 content.

The secure NAD or its proxy **Shall** transfer the file to the DCP using the same file transfer method, in reverse, as used in 6.8.3.1 for the DCP-to-Secure NAD trip data file.

The DCP logs this incoming file and process its contents according to procedures.

6.8.5 Cellular Data Service using Embedded NAD

The DCP interface **Shall** be IPv4 compatible or higher for Cellular data service, and able to transport the UDP and/or TCP methods previously defined in this document. All messaging protocols and formats are per this document. Cell providers frequently change the IP address assigned to the mobile device as it does hand-offs between Metropolitan Service Areas (MSAs), or between regulatory domains/countries, the DCP i**s** transparent to this.

Note: when TCP is elected for use in DCP messaging: It is common for the carrier to drop the TCP connection due to such cross-domain mobility, as these are not usually tunneled for session continuity, nor may allow the use of Mobile IP (an older RFC) for IP address persistence. TCP connections can fail frequently with cellular data systems due to RF propagation conditions,

hand-off failures and hand-off rejections due to roaming agreements.

The DCP **Shall** respond to each incoming packet to the source address, though it could change mid-transaction. When UDP is used, as in this specification as an option, these TCP issues are not present. Per this document, the DCP **Shall Not** initiate outward connections for TCP. For UDP, the DCP can use the incoming packet's source IP address.

6.8.6 Satellite Data Service Using Embedded NAD

The DCP interface for Satellite communications **Shall** be IPv4 compatible or higher, and able to transport the UDP and/or TCP methods previously defined in this document. All messaging protocols and formats are per this document. The round trip delay in geosynchronous orbit satellite services may reach 0.8 seconds, however this is compatible with this document. For low earth orbit satellite services, the delay is less.

7 References

[1] *Security Device Requirements R1.0*; Department of Homeland Security, Science and Technology Directorate.

[2] *Marine Asset Tracking Tag System (MATTS) Requirements R1.0,* Department of Homeland Security, Science and Technology Directorate.

[3] *Security Device (CSD/ACSD) Communications Interface Control Document (ICD) Security Device-to-Network Access Device (NAD);* Department of Homeland Security, Science and Technology Directorate.

[4] *Cargo Security Network Communications Key Management and Data Security Report;* Department of Homeland Security, Science and Technology Directorate.

[5] *Cargo Security Network Access Device (NAD) Requirements R1.0*; Department of Homeland Security, Science and Technology Directorate.

8 Acronyms

ACK	Acknowledge
ACSD	Advanced Container Security Device
AoS	Add-on Sensors
ARM	Arm ACSD Device
CA	Set Alarm Status to no Alarm
CCA	Clear Channel Assessment
CEK	Change Encryption Key
CM	Communications Module
CoC	Chain of Custody
CSD	Container Security Device
CSSC	Cargo Security System Components
CTI	Change Trip Information
DARM	De-activate
dB	Decibel
dBi	Decibel isotropic
ECM	External Communications Module
ECoC	Electronic Chain of Custody Device
EEL	Erase Event Log
EUI	Extended Unique Identifier (per IEEE)
FFD	Full Functional Device
GTS	Guaranteed Time Slots
HMAC	Hash Message Authentication Code
ICD	Interface Control Document
ID	Identifier
IEEE	Institute of Electrical and Electronic and Engineers
ITP	Intermediate Transit Point
LLC	Link Layer Control
LSB	Least Significant Bit
MAC	Media Access Control
MCPS	MAC Common Part Sub-layer
MFR	MAC Footer
MH	Security Device Message Header
MHR	IEEE Standard 801.15.4-2006 MAC Header

MIC	Message Integrity Code
MID	Manifest Identification
MK	Message Key
MLME	MAC Sub-layer Management Entity
MPDU	MAC Protocol Data Units
MPH	Miles per Hour
MSB	Most Significant Bit
NAD	Network Access Point
OSI	Open Systems Interconnect
PAN	Personal Area Network
PHR	PHY Headers
PHY	Physical Layer
POA	Point of Arming
POD	Point of De-vanning
PPDU	PHY Protocol Data Units
PSDU	PHYS Service Data Units
RFD	Reduced Functional Device
RFID	Radio Frequency Identification
SA	Set Alarm to “Alarm”
SAP	Service Access Point
SEL	Send Event Log
SFD	Start-of-Frame Delimiter
SHA	Secure Hash Algorithm
SHR	Synchronized Header
SK	Secret Key
SSCL	Service Specific Convergence Layer
SSM	Send Status Message
STI	Set Trip Information
TTP	Trip Termination Point
UID	Unique Identifier
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

This page left blank intentionally

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY" OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.