U//FOUO
U//FOUO
U.S. ARMY CERDEC POET
(U) General Dynamics Requirements Description Paper
NOTE: All material contained within this report should be considered U//FOUO. Individual paragraphs have not been individually marked.

UNCLASSIFIED//FOR OFFICIAL USE ONLY
CM-001-03
PROOF OF CONCEPT STUDY FOR AN ADVANCED HIGH SPEED EMBEDDABLE CRYPTOGRAPHIC CHIPSET OR MODULE REQUIREMENTS DESCRIPTION PAPER
22 November 2005
Revision 2.0
Prepared for:
Lear Siegler Services, Inc.
595 Shrewsbury Avenue
Shrewsbury, NJ 07702
and
Cryptographic Modernization Office
RDECOM, CERDEC, S&TCD CSC
Fort Monmouth, NJ 07703
Prepared by:
General Dynamics C4 Systems
8220 E. Roosevelt Street
Scottsdale, AZ 85257
Contract Number: DAAB07-03-D-B010
Delivery Order: LSI Task Order 094
Subcontract Number: 1.06.20.026
Delivery Order: GDC4S Task Order 002
UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE iNLY
CM-001-03
This Page Is Intentionally Blank
UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY
CM-001-03
Document Revision History

Revision
Date
Description
1.0
16 September 2005
Initial Release
2.0
22 November 2005
Update per CERDEC comments
THIS TABLE IS UNCLASSIFIED//FOR OFFICIAL USE ONLY

This Page Is Intentionally Blank

Table of Contents

List Of Figures

List Of Tables

This Page Is Intentionally Blank

1. SCOPE
This document is a requirements description paper for a Cryptographic chipset that can be embedded into High Capacity Communications Capability (HC3) communications

terminals or be used to develop a compatible Cryptographic module.
This requirements paper addresses the Army's HC3 application and therefore is limited to its environment and terminal platforms. The content of this requirements paper is derived from General Dynamics C4 Systems' (GDC4S) analysis and practical extensions of the information provided by the government, available in public literature, and related requirements of other current programs. The requirements herein appear to be achievable within the practical constraints of today's industrial parts and technology.
There are additional requirements that should be defined to provide some assurance that a Cryptographic Module/Cryptographic Chipset (CM) is developed that meets the intended usage. These derived requirements are identified in this document by To Be Determined (fBD), To Be
k i isik), and
.
1'o Be Specified (TBS) tags. TBR tags identify those
requirements where some information to justify an initial value or capability is available, but the justification may be weak. System design trade offs or implementation trades may result in changes to these values. Those requirements where sufficient supporting information is just not available are tagged with TBDs or TBSs. TBSs are requirements that should be defined and TBDs are requirements that may or may not be defined depending on the platform architecture and the Government procurement philosophy.
The CM is a set of hardware and software that provides cryptographic services to HC3 terminals. It supports both TRANSEC and COMSEC functions and is capable of changing crypto algorithms and keys in a tactical environment. This allows the CM to be configured to interoperate with different waveforms such as Common Data Link (CDL), Low Data Rate (LDR), Medium Data Rate (MDR), Extended Data Rate ()CDR), and Extremely High Frequency (EHF) High Data Rate ()CDR+) on a platform-by-platform and mission-by-mission basis.
The HC3 communication system is used for ground tactical and sea-based networks that form part of the Global Information Grid (GIG). HC3 supports circuit and packet switched connectivity to terrestrial, airborne, surface/subsurface and satellite communications nodes for network centric operations. A suite of modular hardware and software components can be chosen to tailor an HC3 system to meet tactical missions requiring high-capacity communications.
HC3 connects tactical users across the services using military and commercial satellite communications as well as ground-to-ground and ground-to-air Line-of-Sight (LOS) communications links. HC3 operates with the military and commercial satellites envisioned for 2010 and beyond using X, Ku, Ka, and Q waveforms. Military satellites include the Wideband Gapfiller Satellite (WGS), Advanced Extremely High Frequency (AEHF), and Transformational Satellite (TSAT). Commercial satellite support includes Ku and Ka systems. LOS enables high data rate communications from an HC3 to an
1

airborne platform as well as LOS communications capabilities on the ground-either directly or using an airborne relay.
The number of simultaneous waveforms hosted and operated depends on the communications capabilities required to perform a mission and the capabilities of the platform on which the specific HC3 resides (e.g., aboard a Ship, in a highly mobile armored vehicle, on a Heavy High Mobility Multipurpose Wheeled Vehicle (HHMMWV), etc.).
HC3 capabilities are assigned to the following categories. This set of categories is referred to throughout HC3 documents to describe HC3 variants.
â€¢ Communication on the move (COTM): The ability to establish and maintain communication while a vehicle is in motion.
â€¢ Communication at the quick halt (COTQH): The ability to establish and maintain reliable tactical communications within 5 minutes after vehicle is at rest.
â€¢ Communication on the halt (COTH): The ability to provide reliable tactical communications with a setup time of 30 minutes after coming to a full stop.
â€¢ Transit case: The ability to provide tactical communication with a minimum number of transit storage cases with a setup time of 30 minutes.
â€¢ Ship: The ability to provide reliable communications in installations distributed throughout a seagoing vessel.
â€¢ Navy Shore: The ability to provide reliable tactical communications from a shore fixed-site facility.
â€¢ Submarine: The ability to provide communications in installations distributed throu
g
hout a submarine.
2. **INFORMATION SOURCES**
The information used to derive the requirements contained in this paper consist of the Performance Work Statement (PWS), specifications, and trade study results supplied by the Government listed below.
â€¢ Performance Work Statement (PWS) Dated 05Apr05
â€¢ HAIPISv3 Specification Version 3.0.0. Dated 31 Mar 05
â€¢ LEF_ SPEC. NSA 03-OIA, Version 2.0, Dated 30 Sep 04
â€¢ IAD lntenm Procedure NO. 01-02, Dated 21 Jan 03
â€¢ High Capacity Communications Capability (HC3) Specification, Draft Dated 10 May 05
â€¢
JAoA brief Minus Funding, Dated 07 Apr 05

â€¢ Raytheon Study Documents:
o Multi-Band Operations Report, July 2004
o Network Interoperability Report, July 2004

o Modular Architecture Report, July2004
o Security Architecture Report, CDRL A005-002, 29 Mar 2005
o Raytheon HC3 Study Statement Of Work (SOW), 26 Oct 04
â€¢ Boeing Study Documents:
o HC3 Modular Architecture Description Document, CDRL A001-01 Dated
1 Oct 04
o Boeing HC3 Study Statement Of Work (SOW), 16 Mar 05
o HC3 Security Architecture Draft presentation 16 Jan 05 (proprietary
marking removed)
o TIM 4 slides, 1 i-18 May 05
o Security Architecture Report CDRL A005 Interim Draft Dated 1 Aug 05
o TIM 5 slides, 1-2 June 2005
â€¢ Algorithm Table update received 15 July 2005
The following documents are referenced by the above source material and provide additional detail from which the CM requirements were derived.
â€¢ Joint Tactical Radio System (JTRS-5000), Software Communications Architecture Specification, SCA V3.0, August 27, 2004
â€¢ JTRS-5000 SEC, Security Supplement to the Software Communications Architecture Specification, V3.0, August 27, 2004.
â€¢ JTRS-5000 SP, Specialized Hardware Supplement to the Software Communications Architecture (SCA)` Specification, V3.0, August 27, 2004.
â€¢ Electronic Key Management System (EKMS 217), EKMS Benign Techniques Specification, Revision G, 21 December 2001.
â€¢ EKMS 308, EKMS Data Tagging and Delivery Standard, Revision D, 09 September 2003.
â€¢ EKMS 317, EKMS FIREFLY Specification, 15 April 2002.
â€¢ EKMS 322, Generic Fill Format Specification, 26 August 1998.
â€¢ KG-TG-002-96 Standard for Signing and Obtaining a Hash word for a Software Package to Support INFOSEC Applications (for Signature Verification Only).
â€¢
HAIPE Legacy Encryption Implementation Guide, 31 Mar 2005

---

3. CAPABILITY OVERVIEW

Future communication terminal architectures will require enhanced high-speed cryptographic capabilities in order to support the higher data rates and increased security demands imposed by modem waveforms and ever-increasing security regulations. These future terminals are envisioned to be a family of multi-band, multi-mode, transportable, modular, flexible, Software Communications Architecture (SCA) compliant, satellite and Line of Sight (LOS) systems supporting simultaneous communications between ground, airborne and surface/subsurface units for a range of missions across all services in tactical operational environments.

These terminals are envisioned to be capable of operating with the military and commercial satellites envisioned to be operational in the 2010 and beyond timeframe, utilizing X, Ka, and Q-band frequencies. These systems included the Wideband Gapfiller System (WGS), Advanced Extremely High Frequency (AEHF), and Transformational Communications MILSATCOM (TCM) constellations. Commercial satellite support will include both Ku and Ka-band systems. The terminals will also provide high-capacity line-of-sight (LOS) communications utilizing Common Data Link (CDL)/Networked Common Data Link (NCDL) links.

Because the family of systems will operate with many legacy waveforms currently used by military and civilian agencies, and incorporate new waveforms as they are developed, the cryptographic components of the system will need to be programmable and scaleable to meet specific user operational needs. The desire is that the system provides flexibility through an open system architecture that enables technology insertion (via re-programmability or other means). The terminal system will be capable of high data throughput rates per channel; incremental channel expansion; high levels of reliability, availability, and maintainability; technological enhancement; and commercial support service compatibility.

3.1 Architecture

The CM is intended to be a subsystem of an INFOSEC module within a HC3 terminal. All RED processing within the terminal is done within the INFOSEC module. The CM provides cryptographic services and isolates the RED processing from the rest of the terminal. A modified version of the INFOSEC module block diagram of the one in the Raytheon HC3 Security Architecture Report (SAR) showing the CM is given in Figure 3.1-1. The diagram has been annotated to show General Dynamic C4 Systems' (GDC4S) recommendation that the CM boundary should be extended to include all RED/BLACK signaling (bypass/control).

Figure 3.1-1. Annotated INFOSEC card from Raytheon HC3 SAR

The major functions provided by the CM include cryptographic key management, High Assurance

-

Internet.

Protocol

Encryptor (HAIPE) management COMSEC, TRANSEC for

up to four channels, bypass processing, non-user data COMSEC and RED data for storage. The CM interfaces to other functions of the INFOSEC module and terminal. A top-level view of the CM functional allocation and their context is shown in Figure 3.1-2.

CM-001-03
Real
Time
Clock
Power
(prime
and
battery)
CIK
(User/
Tamper
Recovery)
(.
FILL

RED High Speed
processing
Waveform
TRANSEC
and
COMSEC
ZEROIZE
TAMPER
BLACK High Speed
tâ–º
Suite
(
'T
y
p
e - - -
A/B
Interfaces to Modems
---
or
Commercial)
Terminal
Applications
RED Processing
Low Speed
modem
Interface
HAIPE or
Commercial
RED

IP formatting
and protocols
Low **Speed**
modem
Interface
HAIPE or
Commercial
BLACK IP
formatting
MILS Key
MGMT and
wrapping
(
Typ
e 1
Suite A/B or
Commercial)
MILS COMSEC
(HAIPE Type 1
Suite A/B or
Commercial)
Bypass Processing
Cryptographic Module
BLACK Processing
Figure 3.1-2. CM Requirements Context Diagram

3.2 Interim Information Assurance Directorate (IAD) Procedure

The CM design shall meet the information assurance requirements described in the following sections and must satisfy the security and certifiability of the cryptographic application by the National Security Agency (NSA). The principal sections of Interim Information Assurance Directorate (IAD) Procedure No. 01-02 that must be addressed during the design include:

14.a(4) Proper Classification
14.b Development Requirements-Buildin
g
Assurance Levels 1, 2, and 3
14.b(1)(a) Cleared Personnel
14.b(1)(b) Cleared Facilities
14.b(1)(c) Established Development Methodology and Standards
14.b(2) High Level System Requirements Review
14.b(8)(c)(1) Informal Review-Requirements
6

14.b(8)(c)(3) Informal Review-Code Review
The CM shall be designed such that follow-on product delivery is capable of achieving Type 1 certification by NSA. Certification is a process involving meeting the security requirements provided by NSA as well as evolution of the technology and policy requirements as defined by the process documented in the User Partnership Agreement (UPA) between the Army and NSA. This process defines both the policy, technical capability, and testing needed for certification for a particular use.

3.3 Initialization

The CM shall utilize a boot function contained within the CM boundary. The CM boot function shall be independent of the terminal application initialization.
The CM shall provide services to decrypt, install, and execute its run-time application.
The CM shall perform diagnostic tests during the power-up sequence. Power-up diagnostic testing will include internal health tests, memory tests, and other tests determined to be necessary to satisfy the system security -: .ysts. Upon request, the CM shall provide the results of the diagnostic tests, in addition to the overall CM version identifier.
Upon request, the CM shall perform additional diagnostics during the HC3 terminal initialization sequence. These diagnostics will include known answer tests (to verify the encrypt/decrypt path) and tests that verify the correct operation of the cryptographic bypass.

3.4 Multi-band, Multi-mode

The CM supports platforms that are multi-band and multi-mode, with the capability to run various modes/waveforms simultaneously with varying security level and data requirements for each.
The CM shall provide the waveform cryptography for at least four separate, independent, and simultaneous Radio Frequency (RF) channels. Waveform cryptography includes the generation of key streams required by the terminal TRANSEC modulation and cover functions as well as performing waveform COMSEC encryption and decryption where required.
The CM shall support both continuous and request-reply interface concepts.
The CM shall generate waveform cryptography key streams to support at least 500 Megabits per second (Mbps) bandwidth on each channel and the aggregate bandwidth of 2 Gigabits per second (Gbps) (threshold requirement).
The term Security Association (SA) is used in this requirements description paper to identify/describe a relationship between a key with the data source and/or destination. A unique key will require a unique SA, however a unique seed (e.g. Time of Day (TOD) or Net ID) does not. The CM shall support up to an aggregate of 28 simultaneous waveform SAs (4 channels, 7 SAs each). This is in addition to the SA support required for waveform COMSEC and remote managers.

CM-001-03
The CM shall provide the capability to accept seed and/or time-of-day (TOD)

information from a channel Modulator Demodulator (MODEM) and reply with the corresponding TRANSEC bits required by the MODEM to perform its TRANSEC functions.
The CM shall provide the TRANSEC bits to the channel interface within To Be Specified (TBS) msec of receiving the request (defined as the time between the last request bit is received and the last response bit is sent).

3.5 Waveform Cryptography and Management COMSEC

The CM provides both waveform cryptography and remote management COMSEC capabilities. It shall be configurable to perform either or both functions.
All user data entering the terminal will already be COMSEC encrypted (i.e. "black").
A relationship that defines a key with the source and/or destination is identified as a Security Association (SA) in this requirements description paper. A unique COMSEC key will require a unique SA.

3.6 Scalable Throughput and Power

Some platforms are not required to provide high or multi-channel throughput capability but low power consumption is critical. Reasonable means to conserve power shall be employed, including reducing CM power consumption when high performance is not needed.
The CM shall be configurable for different levels of aggregate throughput from 100 Kbps to 2 Gbps (threshold). An aggregate throughput of 10 Gbps is a desired objective capability. Derivative implementations for higher or lower throughput should implement a common control and management scheme and should implement a common design when feasible to reduce development/certification/maintenance costs.
The CM shall be configurable for the number of independent channels supported from one to four.
The CM shall scale its power requirements in relation to the configured throughput and channels supported, lower throughput using less power.

3.7 **Multiple Security Levels**

The CM shall provide the capability to operate at all security levels from Sensitive, But Unclassified (SBU) to Top Secret/Sensitive Compartmented Information (TS/SCI). Simultaneous operation on up to four channels at different security levels with required domain separation shall be supported. Each channel. however, operates at a single classification level. (See the discussion in the comments section)
The CM shall provide multiple security level COMSEC support to the terminal management function. The terminal management function communicates with Multiple Network Management Servers operating at different security levels. The Network

management data/messages are expected to be classified at the level of the channel being managed and will need to be segregated for each Network Manager and channel.

3.8 Remote Management Capability

The CM shall provide COMSEC and authentication services to the remote management

function of the terminal. Note that the CM provides authentication and COMSEC services to the terminal and responds to terminal provided commands but does not interface directly with remote sites. The CM also supports "unattended" operations indirectly where an operator is not physically present at the terminal. These operational requirements will include features such as zeroization and low power consumption. Management includes cryptographic device control and status, network/system management and key management and distribution. A common management structure over all implementations is a threshold requirement with a single management view or model. A desired objective capability is that the entire community of terminals should be able to be managed from a single workstation. It is also a desired objective capability that .i.,glc ma,1agel,.:: ,t worl.o:ation also Le able to enforce terminal con .
guidelines and policies. All management shall be in accordance with current security guidelines.
The CM COMSEC shall be interoperable with High Assurance Internet Protocol Encryptor (HAIPE) compliant Inline Network Encryptor (INE) devices located at the management sites and used to encrypt and decrypt management messages.
The CM shall provide the cryptography needed by the terminal authentication function to identify and authenticate Remote Management Entities.
The CM shall provide the capability to accept restart commands and restart without an operator physically present at the terminal/crypto. The HAIPE Management Information Base (MIB) includes objects that provide the capability to restart the terminal from a management workstation.
The CM supports the terminal capability to accept Over The Air Zeroize (OTAZ) commands without an operator physically present at the terminallcrypto with its authentication and cryptographic services. The terminal interfaces with remote entities and generates the commands that select and execute the CM zeroization capabilities provided for both keys and algorithms.
The CM shall support an aggregate of at least 16 remote management SAs. This accommodates four remote managers operating at up to four security levels and is in addition to SAs that may be needed to support other terminal functions.

3.9 Interoperable

The CM shall interoperate with legacy systems and modem systems desi
g
ned to existing
standards as defined in this requirements paper.

3.10 Upgradeable

It is desirable to maximize the field upgradeability of the CM. All upgrading should be achievable from the management workstation. The device should have technology

insertion built in. This ability should allow continued operation as the current standards evolve (e.g., Link Encryptor Family (LEF) 2.0). All upgrading shall be in accordance

with security requirements.
The HAIPE Interoperability Specification (IS) includes requirements to support over-the-network field upgrade of terminal software/firmware. The terminal communicates with a manager using either the Trivial File Transfer Protocol ('1'N 1'P) or the Hypertext Transfer Protocol (HTTP) to retrieve an encrypted upgrade package. The CM shall support software and signature verification in accordance with KM-TG-002-96, "Standard for Signing and Obtaining a Hash word for a Software Package to Support INFOSEC Applications (for Signature Verification Only)." The CM shall verify the signature on a software file prior to non-volatile storage.

3.11 Algorithms

The CM shall provide the capability to generate key streams and support COMSEC functions using the following algorithms. Table 3.11-1 lists the waveform, associated algorithms and highest security level associated with each.

MEDLEY
SHILLELAGH
BATON
KEESEE
AES (Advanced Encryption Standard)
WALBURN
Commercial SATCOM
SAVILLE

The CM shall provide WEASEL cryptographic capability to the terminal for authentication services.

TABLE 3.11-1. Waveform Algorithms

THIS TABLE IS UNCLASSIFIED//FOR OFFICIAL USE ONLY

Waveform	**Modulation Algorithm(s)**	**Cover Algorithm(s)**	**COMSEC Algorithm(s)**	**Max Security Level**
AEHF LDR				
Suite A:				
MEDLEY				
SHILLELAGH				
BATON				
KEESEE				

Suite A:
MEDLEY
SHILLELAGH
BATON
KEESEE
TBS
SECRET
AEHF MDR
Suite A:
MEDLEY
SHILLELAGH
BATON
KEESEE
Suite A:
MEDLEY
SHILLELAGH
BATON
KEESEE
TBS
SECRET
A
: '
..
Suite A:
MEDLEY
SHILLELAGH
BATON
KEESEE
Suite
A:
MEDLEY
SHILLELAGH
TBS
SECT
BATON
KEESEE
TSAT XDR+
Suite A or B:
MEDLEY
SHILLELAGH
BATON
KEESEE
AES
Suite A or B:
MEDLEY
SHILLELAGH

BATON
KEESEE
AES
TBS
SECRET
WGS (MIL-188-165A) None
WALBURN
AES
SECRET
Commercial
SATCOM
TBS
TBS
TBS
UNCLASS
CDL 1
None
Suite A*
Suite A*
TOP SECRET
CDL 2
None
Suite A*
Suite A*
TOP SECRET
MILSTAR
TBS
TBS
TBS
TBS
MIL-188-EEE
AES
AES
TBS
TBS
THIS TABLE IS UNCLASSIFIED//FOR OFFICIAL USE ONLY
*-Details classified,
Required algorithms could be selected from a library of SCA compliant implementation sets.

3.12 Integratable

While the CM design demonstrated will not be a production item, the design approach is expected to meet the requirements described in this document and have the features

necessary for NSA certification to the maximum extent possible. When the design is certified by NSA and taken to production, it is envisioned that the CM would be delivered as an item(s) that could be embedded into a variety of platforms.

3.13 Standards Based Interfaces

To maximize the usability of the CM, industry standards shall be used for all external interfaces. The proper use of interface standards to allow future technology insertion and development of derivative products is a requirement. The interfaces discussed in this requirements paper are listed below in summary form. These interfaces are discussed in more detail in the corresponding capability section.

The interface list below does not mean to imply physically separate interfaces. Interfaces may be aggregated on physical media subject to meeting other requirements.

The CM shall provide four high speed aggregate TRANSEC stream interfaces (one for each channel's modulation and cover).

The CM shall provide four high speed waveform COMSEC interfaces (red and black interface for each).

The CM shall provide an identification and authentication service interface.

The CM shall provide remote management message interface(s).

The CM shall provide a recoverable zeroize key command discrete signal interface (i.e. recoverable via Over-the-air rekey (OTAR), benign, or black fill techniques).

The CM shall provide a zeroize all keys command discrete signal interface (zeroize all key command includes the key material needed to support OTAR, benign, or black fill techniques).

The CM shall provide a zeroize algorithm command discrete signal interface.

The CM shall provide a TAMPER command discrete signal interface.

The CM shall provide discrete status interfaces to indicate alarm and tamper conditions.

The CM shall provided a TBS power interface. The CM power consumption, when configured as a module, shall be less than or equal to 35 Watts.

The goal is to maintain CM operation when its stored or transported without the need for battery power. If a battery is required to maintain CM operation during storage or transport, and the CM is configured as a module, the CM shall provide an interface for a transport battery. In this case a transport battery will be attached to the CM in order to provide power when the CM is not installed in and powered by an Line Replaceable Unit (LRU), i.e., when the CM is in storage or in transit from its factory location. The transport battery will be indelibly marked with a visible, human-readable date (day, month, and year) that identifies when the battery should be replaced.

The CM shall provide a TBS interface for a remote Cryptographic Ignition Key (CIK) device.

The CM shall provide a DS-101 and EKMS 308 compatible fill interface. These standards specify, among other things, the mechanical interface (hosted by the HC3

terminal) and the physical, data link, and application layer services utilized by an End Cryptographic Unit (ECU) (i.e., the HC3 terminal, specifically the CM, in this case). These services combine to provide a method by which an EKMS 308 compliant Data Transfer Device (DTD), such as the ANICYZ-10, can load RED or BLACK key material, cryptographic algorithms, applications, and other data into the terminal.
The CM shall provide a local interface for loading data such as algorithms, programs, and configuration. There are a number of concepts that accomplish this e.g. a serial, console, or Ethernet port or use of the DS-101 fill interface.
The CM shall provide an interface(s) to accept software and configuration files from the terminal and return the encrypted or decrypted results.
The CM shall provide an interface to accept real time clock information from the terminal to be used for TRANSEC waveform sync purposed.
The CM, when configured as a module, shall be designed to be compatible with VMEbus International Trade Association (VITA) standards for packaging, connectors, and ele trical interf-
_;A;o
case the CM snail be configured as
a
15U form factor using a
maximum of 1 slot (the hardware and software required for the terminal INFOSEC processing functions not allocated to the CM are not included in the CM).
The CM weight, when configured as a module, shall be less than or equal to seven pounds.

4. TRANSMISSION SECURITY (TRANSEC)

The Type 1 crypto functions needed to support specific communication channels are described in this section and organized by channel. and waveform type. The CM shall provide Type 1 TRANSEC features sufficient to satisfy the NSA requirements allocated to the CM. The NSA will provide a document containing these requirements as part of the UPA for NSA cryptographic certification.
The functionality of the CM includes generating TRANSEC key stream(s) sent to the MODEM(s)._These control fine and course frequency_hopping for spectrum spreading and despreading.
The TRANSEC stream also contains sequences of pseudo random bits generated by a cryptographic process that may be exclusively OR-ed with the bit stream between the modem encoding and modulation functions. This process is called "cover".
The TRANSEC stream generated by the CM also contains information that controls the order used in the frequency and time permutation process.
The cryptographic function of the CM also provides waveform transmission security via encryption/decryption of link and control data as required by the channel.

4.1 AEHF Waveform

The CM shall provide the capability to generate an aggregate AEHF TRANSEC stream using Suite A uplink key.

CM-001-03
The CM shall provide the capability to generate an independent aggregate AEHF TRANSEC stream using Suite A downlink key.
The CM shall provide the capability to generate aggregate AEHF cover streams using distinct Suite A cover keys.
The CM shall provide the capability to encrypt/decrypt AEHF payload-to-terminal messages using Suite A keys.
The CM shall provide COMSEC services for the inband communications channel (XCO) as required by select AEHF platforms.

4.1.1 Low Data Rate (LDR)

LDR transmissions are protected by three uplink TRANSEC functions:
1) Frequency hopping
2) Time and frequency permutation
3) Selective C2 (Terminal-to-Payload Control Message) cover using separate high/low C2 cover keys

and three downlink TRANSEC functions:
1) C3 (Payload-to-Terminal Control Message)
2) Acquisition and
3) Report-back Order-Wire (AROW) cover

4.1.2 Medium Data Rate (MDR)

MDR transmissions are protected by four uplink TRANSEC functions:
1) Frequency hopping
2)
=
Time-and frequenc_y erm_utation_
3) MC2 (Terminal-to-Payload Control Message) cover
4) Probing slot time rotation

and three downlink TRANSEC functions:
1) MC3 (Payload-to-Terminal Control Message)
2) Acquisition and
3) Tracking Order-Wire (ATOW) cover

4.13 Extended Data Rate (XDR)

XDR transmissions are protected by four uplink TRANSEC functions:
1) Frequency hopping
2) Time and frequency permutation

CM-001-03
3) XC2 (Terminal-to-Payload Control Message) encryption using individual terminal Traffic Encryption Key (TEK)
4) Probing slot time rotation

and three downlink TRANSEC functions:
1) XC3 cover using country specific Transmission Security Key (TSK)
2) ATOW cover using country specific Transmission Security Key (TSK)
3) XC3 encryption using individual terminal-, service- or payload-specific TEK

4.2 TSAT Waveform

The CM shall provide the capability to generate an aggregate TSAT TRANSEC stream using Suite A or Suite **B** uplink key.
The CM shall provide the capability to generate an aggregate TSAT TRANSEC stream using Suite A or Suite B downlink key
The CM shall provide the capawity to decrypt TSAT satellite broadcast using Suite A or Suite B decryption key
The CM shall provide. the capability to generate aggregate TSAT cover streams using Suite A or Suite B cover key. Up to 7 (TBR) unique keys may be required for each channel.
The CM shall provide the capability to generate aggregate TSAT cover streams using distinct Suite A or Suite B cover keys. Up to 7 (TBR) unique keys may be required for each TSAT channel. Note that the use of 7 unique keys drives the support requirement for 7 SAs on TSAT waveform channels.
The CM shall provide the capability to Encrypt/decrypt
.
TSAT payload-to-terminal
messages using Suite A or Suite B keys (potential; not yet finalized).
The CM shall provide the capability to generate key streams for use by the TSAT Suite B coveLexpansioniunction..
The CM shall provide TSAT payload-to-terminal resource control Confidentiality and integrity services.

4.3 WGS Waveform

The CM shall provide the capability to generate aggregate WGS TRANSEC stream using unclassified WGS keys and algorithms
The CM shall provide the capability to encrypt/decrypt WGS positive control messages using unclassified WGS keys and algorithms

4.4 Commercial SATCOM Waveform

The CM shall provide the capability to generate aggregate commercial SATCOM TRANSEC stream using unclassified keys and algorithms.

4.5 MILSTAR Waveform

The CM shall provide the capability to generate aggregate MILSTAR SATCOM TRANSEC stream(s) (TBR). This is a placeholder here as the details are not available in provided documentation and MILSTAR was not on the original HC3 support listing. It was added as a requirement during a Technical Interchange Meeting (TIM).

4.6 MIL-188-EEE Waveform

The CM shall provide the capability to generate aggregate MIL-188-EFF, TRANSEC stream(s). MIL-188-F.F.F, is a variant of MIL-STD-165A and is the emerging standard . The MIL-188-EEE waveform uses the Advanced Encryption Standard (AES) in a Cipher Block Chaining (CBC) mode with key lengths of 256 bits.

4.7 Waveform COMSEC

Some waveforms require COMSEC processing for non-user data. The CM shall provide Type 1 COMSEC features sufficient to satisfy the NSA requirements allocated to the CM. The NSA will provide a document containing these requirements as part of the UPA for NSA cryptographic certification.

The CM shall provide the capability to support two independent data streams (i.e. SAs) per channel for an aggregate total of up to 8.

4.7.1 CDL Streams Bulk Encryption/Decryption

The CM shall provide the capability to bulk encrypt/decrypt distinct CDL streams using Suite A or Suite B keys.

4.7.2 Encryption/Decryption of Inband Terminal Control/Status (COMSEC)

The CM shall provide COMSEC services for the inband communications channels as required by some platforms. (additional detail TBD).

.

HAIPEDEVICE INTEROPERABILITY

High Assurance Internet Protocol Encryptor (HAIPE) devices front management workstations to protect HC3 terminal management messages, including information related to device control and status, network/system management information, and key management and distribution. The HAIPE Interoperability Specification (IS) captures the traffic protection, networking, management, and application level functional requirements necessary to ensure interoperability of HAIPE compliant devices.

The CM services provided to the HC3 terminal shall be compliant with the core and extension HAIPE IS Version 3.0 requirements. Compliance with both the core and extension documents ensures that the CM is interoperable with all HAIPE Version 1.3.5 and Version 3.0 devices. The requirements traceability matrix provided in Appendix B indicates the allocation of requirements to the system based on the architecture described in Section 3.

At this time, legacy compliance to HAIPE IS Version 1.3.5 is required as the roll-out of HAIPE IS Version 3.0 devices is not expected to begin until the second quarter of 2008.

If the fielding of HC3 terminals is sufficiently further into the future, compliance with the legacy algorithms and protocols may be waived.

The following CM requirements represent a subset of those that are either explicitly stated in the HAIPE IS (and elevated to this level to highlight the necessary algorithms and capabilities) or implied by one or more of the requirements from that set:

â€¢ Key management:

o The CM shall support key fill (load) operations in accordance with EKMS

308.
o The CM shall accept FIREFLY vector sets formatted in accordance with EKMS 322.
o - Key update:
â– The CM shall perform deterministic update of a TEK used to protect MEDLEY encrypted traffic using ACCORDION 3.0 in accordance with R21
.
=
MEDLEY
Implementation Standard: An ACCORDION MEDLEY", 7 Feb 2002.
â– The CM shall perform deterministic update of a TEK used to protect BATON encrypted traffic using ACCORDION 1.3 in accordance with KM-TG-0001-87, "ACCORDION 1.3", 30 Oct 1987.
â– The CM shall perform deterministic update of a Suite B TEK using the algorithm specified in R21-TECH-02-05, "R21 Information Technical Report: A Key Update Function Based on the AES Key Wrap", 10 Jan 2005.
o Key agreement:
â– The CM shall support the FIREFLY exchange in accordance with
=
=-EKMS 322B- in order to generate-Suite A encryption keys (either for traffic or key encryption).
â– The CM shall support the Menezes-Qu-Vanstone (MQV) exchange in order to generate Suite B encryption keys.
â– The CM shall support the use of exclusion key in accordance with "Exclusion Key and it's Application to Foreign Interoperability", 7 June 2002 and "Guidance for Exclusion Key Specification", 8 Nov 2004.
â€¢ User traffic protection:
o The CM shall support the use of MEDLEY in Galois Counter Mode (GCM) to protect Suite A user traffic communication with IS Version 3.0 HAIPE devices.
17
UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY
CM-001-03
o The CM shall support the use of MEDLEY in the mode defined in "HAIPE Legacy Encryption Implementation Guide", 31 Mar 2005 to protect user traffic communication with HAIPE IS Version 1.3.5 compliant devices.
o The CM shall support the use of BATON in the mode defined in "HAIPE

Legacy Encryption Implementation Guide", 31 Mar 2005 to protect user traffic communication with HAIPE IS Version 1.3.5 compliant devices.
o The CM shall support the use of AES in Counter Mode to protect Suite B user traffic communication with HAIPE IS Version 3.0 compliant devices.
The HC3 terminal must be designed in such a way to permit HAIPE interoperability testing to be performed. The implications of this statement are solely applicable to terminal components other than the CM. For example, the RED processor must provide an RJ-45 connector through which the RED interface of the HAIPE Interoperability Tester (HIT) connects.

6. LEF DEVICE INTEROPERABILITY

Link Encryptor Family (LEF) devices may be used by interfacing payloads or platforms to provide link encryption on some channels. HC3 terminals are required to comply with the Cryptographic Interoperability Specification for LEF Equipment so it will interoperate with these payloads and platforms.
The LEF specification defines requirements for developing link encryptors to ensure interoperability with Cryptographic Modernization Initiative devices. These requirements include performance characteristics, key management requirements, and human machine interface requirements.
The CM services provided to the HC3 terminal shall be compliant with the LEF IS Version 2.0 requirements. The requirements traceability matrix provided in Appendix C indicates the allocation of requirements to the system based on the architecture described in Section 3.
-The following--CM requirements-represent a subset of those that are either explicitly --
stated in the LEF IS (and elevated to this level to highlight the necessary algorithms and capabilities) or implied by one or more of the requirements from that set:
â€¢ Key management:
o The CM shall support key fill operations in accordance with EKMS 308.
o The CM shall accept Enhanced FIREFLY vector sets formatted in accordance with EKMS 322.
o The CM shall support BLACK key fill operations in accordance with EKMS 217 (EKMS Benign Techniques Specification).
o Key update:
â€¢ The CM shall perform deterministic update of a TEK using ACCORDION 3.0.
o
Key agreement:

â– The CM shall perform Enhanced FIREFLY key calculation in accordance with EKMS 322 and the classified appendix to the LEF **IS.**

â€¢ User traffic protection:
o The CM shall support the use of MEDLEY in Counter Mode. Details in the MEDLEY Implementation Standard, NSA document 0N679197 and TBS in the classified appendix to the LEF IS.
o The CM shall support the NSA authentication algorithm in conjunction with MEDLEY. Details TBS in the classified appendix to the LEF IS.
o The CM shall support the National Institute of Standards and Technology (NIST) AES (NIPS 197) algorithm in Counter Mode. Details TBS in the classified appendix to the LEF IS.
o The CM shall support the NSA authentication algorithm in conjunction with AES. Details TBS in the classified appendix to the T.EF,IS.
o The CM shall support EKMS 322 requirements for Enhanced FIREFLY.

7. KEY MANAGEMENT INFRASTRUCTURE INTEROPERABILITY

The CM shall provide cryptographic services needed by the HC3 terminals
.
for
interoperability with EKMS, Public Key Infrastructure (PKI) and Key Management Infrastructure (KMI) infrastructures. Similar to HAIPE and T.FF interoperability, the CM provides cryptographic services to the terminal's INFOSEC function. The interchange of messages and data with the key management infrastructures are within protocols processed by the terminal red processor. The CM provides confidentiality, integrity, and authentication services to the red processor.
Note that the CM also provides a fill interface capability that is interoperable with the KMI as described in the cryptographic key management section of this document.

8. INTERNET PROTOCOL SECURITY (IPSEC)

HC3 terminals are required to use IPsec on the Transformational Satellite Mission Operations System (TMOS) and TSAT router plane interfaces. The CM provides IPsec confidentiality, integrity, and authentication services to the HC3 terminal INFOSEC function as defined in this section.
IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. These services are provided at the Internet Protocol (IP) layer, offering protection in a standard fashion for all protocols that may be carried over IP (including IP itself).

The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The IPsec, Internet Key Exchange (IKE), and IKEv2 protocols rely on security algorithms to provide privacy and authentication between the initiator and responder. The Encapsulating Security Payload (ESP) and the Authentication

Header (AH) provide two mechanisms for protecting data being sent over an IPsec Security Association (SA). IKE provides a mechanism to negotiate which algorithms should be used in any given association. Request For Comments (RFCs) and Internet-Draft documents define the current set of algorithms that are mandatory to implement, as well as algorithms that should be implemented because they may be promoted to mandatory at some future time.
There are many such algorithms available, and two IPsec systems cannot interoperate unless they are using the same algorithms. The Internet-Drafts listed below contain the latest IPsec information and proposed requirements:
INTERNET-DRAFT Cryptographic Algorithms For ESP & AH
August 2004
INTERNET-DRAFT Cryptographic Algorithms for IKE Version 2
April 2004
INTERNET-DRAFT Security Architecture for IP
March 2005
INTERNET-DRAFT Cryptographic Suites for IPsec
April 2004
INTERNET-DRAFT IP Authentication Header
March 2005
INTERNET-DRAFT Internet Key Exchange (IKEv2) Protocol
Sept 2004
INTERNET-DRAFT IP Encapsulating Security Payload (ESP)
Mar 2005
INTERNET-DRAFT Ext Seq No Addendum to IPsec DOI for ISAKMP Feb 2004

8.1 TSAT terminal-to-TMOS message Confidentiality and integrity

The CM shall provide IPSec confidentiality and integrity processing services to the terminal-to-TMOS interface function.
The CM shall support the capability to generate DoD PKI public/private key pairs for non-type 1 IPSec functions
The CM shall provide the capability to store DoD PKI private keys for non-type 1 IPSec functions

8.2 TSAT router control plane Confidentiality and integrity

The Type 1 crypto shall (TBD) support non-type 1 IPSec confidentiality and integrity processing for the terminal router.
The Type 1 crypto shall (TBD) support generation of DoD PKI public/private key pairs for non-type 1 IPSec functions.
The Type 1 crypto shall (TBD) support storage of DoD PKI private keys for non-type 1 IPSec functions.

9. CRYPTOGRAPHIC KEY MANAGEMENT

The CM shall provide the capability to accept keys from the centralized cryptographic

Key Management System (KMS) as defined in TBS.
The CM cryptography shall be capable of interfacing with DoD encryption devices to include the High Assurance IP Encryptor (HAIPE), KIV-19, and KG-194 (TBR).
The CM shall provide the capability to accept keys from KMS key distribution to include Over-the-Air Re-keying (OTAR). HC3 terminals connect to existing systems to communicate and receive OTAR messages. Rekey messages are waveform-specific and are generated by the manager of that waveform. Rekey messages may be transmitted over the air in small pieces which are assembled by the terminal processor(s) and send to the CM as a single complete message.
The CM shall provide supporting capability to the terminal subsystems to support Tactical Network management (TNM) KMS in the "dis-avowing" (i.e., "de-affiliation" or , canceling the registration, to include remote "zero-izing" of the crypto) o - lay captured or lost systems or nodes that will:
Preclude such systems from being used to access, disrupt the system's networks, or "Tie-up" network access request mechanisms in hostile "denial of service" attempts.

9.1 Key Management and Loading

The CM provides a service by which the fill interface can be configured to receive data. Key material received in this manner can include a seed, operational, or one-time-use FIREFLY vector set or traditional key material. Delivery may be in red form, black form (using a Transfer Key Encryption Key (TrKEK)), or utilizing benign techniques.
The CM shall provide the capability to accept key and control/status information from the DS-101 fill interface provided by the platform.
The CM shall provide the capability to send control/status information to the DS-101 fill
The CM shall be compatible with the DS-101 link/physical layer processing required by HAIPE IS v3.0.
The CM shall support accepting key loads in accordance with EKMS 308.
EKMS Benign Techniques (EKMS 217) support is required. Operations identified here as Benign Key/Fill/Rekey operations can be performed with the Local Management Device/Key Processor (LMD/KP) via the DTD.
The CM shall support EKMS Benign Techniques in accordance with EKMS 217.
The CM shall accept keys in both EKMS 317 generic fill format and DS-100-1 tagged key data formats.
The CM shall provide a interface by which information (e.g., update count, key tag, description) about one or more keys may be requested and provided.
The CM shall perform cryptographic rollover without loss of communications.

9.2 Key Handling and Storage

The CM shall protect keys stored within CM.
Red keys shall be stored in volatile memory only and only stored in red form when the terminal configuration requires them for TRANSEC or COMSEC functions.
Unused or de-assigned Red keys shall be erased from volatile memory.

9.3 Zeroization

The CM shall complete zeroization of all key material within 1 second of zeroize discrete assertion.

The CM shall complete zeroization of all TRANSEC and COMSEC keys within 1 second of recoverable zeroize discrete insertion. Key material needed for black/benign fill techniques shall be retained through a recoverable zeroize event.

The CM shall complete zeroization of all associated channel TRANSEC and COMSEC keys within 1 second of channel zeroize discrete insertion. Key material needed for black/benign fill techniques as well as non selected channels shall be retained through a channel zeroize event.

The CM shall complete zeroization of all key material within 10 seconds of zeroize command reception.

The CM shall complete zeroization of all TRANSEC and COMSEC keys within 10 seconds of recoverable zeroize command. Key material needed for black/benign fill techniques shall be retained through a recoverable zeroize event.

The CM shall complete zeroization of all associated channel TRANSEC and COMSEC keys within 10 seconds of channel zeroize command receipt. Key material needed for black/benign fill techniques as well as non selected channels shall be retained through a channel zeroize event.

9.4 AEHF Channel Key Management

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite A BLACK fill.

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite A BLACK fill during "on air" terminal operation.

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite A EKMS benign fill.

The CM shall provide the capability to Re-encrypt keys up to SECRET for unclassified terminal host storage.

The CM shall provide the capability to accept, process, and store unencrypted Suite A key material on a fill port interface to support crypto initialization.

9.5 TSAT Channel Key Management

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite A or Suite B BLACK fill.

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite A or Suite B BLACK fill during "on air" terminal operation.

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite A or Suite B KMI over-the-network keying (OTNK).

The CM shall provide the capability to accept, decrypt, and store keys up to SECRET using Suite'A or Suite B KMI OINK during "on air" terminal operation.

The CM shall provide the capability to Re-encrypt keys up to SECRET for unclassified

terminal host storage.
The CM shall provide the capability to accept, process, and store unencrypted Suite A or Suite B key material on a fill port interface to support crypto initialization.

9.6 CDL Channel Key Management

The CM shall provide the capability to accept, decrypt, and store keys up to TOP SECRET using Suite A or Suite B BLACK fill.
The CM shall provide the capability to accept, decrypt, and store keys up to TOP SECRET using Suite A or Suite B BLACK fill during "on air" terminal operation.
The CM shall provide the capability to accept, decrypt, and store keys up to TOP SECRET using Suite A or Suite B KMI OTNK.
The CM shall provide the capability to accept, decrypt, and store keys up to TOP SECRET using Suite A or Suite B KMI OTNK during "on air" terminal operation.
The CM shall provide the capability to re-encrypt keys up to TOP SECRET for unclassified terminal host storage.
_The_CM shall ..providethecapability _to accept, process, andstore_unencr_y_pted Suite A _or Suite B key material on a fill port interface to support crypto initialization.

10. CRYPTOGRAPHIC ALGORITHM MANAGEMENT

The CM provides the capability to generate key streams and support COMSEC functions using the following algorithms:
MEDLEY
SHILLELAGH
BATON
KEESEE
AES
WALBURN
Commercial SATCOM
SAVILLE

-UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASIFIED//FOR OFFICIAL USE uNLY
CM-001-03
The CM provides WEASEL cryptographic capability to the terminal to support its authentication functions.

10.1 Cryptographic Algorithm Management and Loading

The CM shall provide the capability to accept and store algorithms and assign them to TRANSEC streams, COMSEC functions, and channels.
The CM shall provide the capability to accept both encrypted (black form) and decrypted (red form) cryptographic algorithms from a local fill port. Note that JTRS-5000 SEC requires all classified cryptographic algorithms to be encrypted.
The CM shall provide the capability to load, configure, and assign algorithms to one channel without affecting the operation of other channels.
The CM shall be reprogrammable. The CM shall permit configuration of the cryptographic algorithm or algorithms as part of device configuration. The CM shall permit removal of the cryptographic algorithm or algorithms as part of device

configuration.
The CM shall provide the services to the terminal such that the terminal can authenticate the source of a request to assign a stored algorithm to a particular terminal channel waveform modulation and/or cover and/or link COMSEC independently.

10.2 Cryptographic Algorithm Handling and Storage

The CM shall provide the capability to store cryptographic algorithms in black form within the CM.
The CM shall protect cryptographic algorithms stored within CM.
The CM shall provide the capability to decrypt classified cryptographic algorithms using the JOSEKI-1 algorithm.
The CM shall only accept cryptographic algorithms signed by the NSA
Only the assigned algorithm for the current mission shall be available within the terminal in red
form during cannel configuration and operation.

10.3 Cryptographic Algorithm Zeroization

The CM shall complete zeroization of all TRANSEC and COMSEC cryptographic algorithms within 1 second of zeroize algorithm discrete assertion.
The CM shall complete zeroization of all associated channel TRANSEC and COMSEC cryptographic algorithms within 1 second of channel algorithm zeroize discrete insertion.
Cryptographic algorithms material needed for non selected channels shall be retained through a channel algorithm zeroize event.
The CM shall complete zeroization of all TRANSEC and COMSEC cryptographic algorithms material within 10 seconds of zeroize algorithm command reception.
The CM shall complete zeroization of all associated channel cryptographic algorithms within 10 seconds of channel zeroize algorithm command receipt. Cryptographic

---

algorithm material needed for non selected channels shall be retained through a channel zeroize event.

10.4 AEHF Channel Algorithm Management

The CM shall provide the capability to accept and store encrypted and unencrypted Suite A cryptographic algorithms material from a local port interface up to SECRET during "on air" and "off-air" terminal operation.
The CM shall provide the capability to accept and store Suite A cryptographic algorithms up to SECRET using over-the-network algorithm update during "on air" terminal operation.

10.5 TSAT Channel Algorithm Management

The CM shall provide the capability to accept from a local port interface and store unencrypted and encrypted Suite A or Suite B cryptographic algorithms up to SECRET during "on air" and "off-air" terminal operation.
The CM shall provide the capability to accept and store Suite A or Suite B cryptographic algorithms up to SECRET using over-the-network algorithm update during "on air"

terminal operation.

10.6 CDL Channel Algorithm Management

The CM shall provide the capability to accept from a local port interface and store unencrypted and encrypted Suite A or Suite B cryptographic algorithms up to TOP SECRET during "on air" and "off-air" terminal operation.

The CM shall provide the capability to accept and store Suite A or Suite B cryptographic algorithms up to TOP SECRET using over-the-network algorithm update during "on air" terminal operation.

11. CRYPTOGRAPHIC BYPASS

Cryptographic-bypass-is-t-he-process-of-tr-ansferrin-g-information between-the-terminal RED and BLACK domains unencrypted. The CM shall provide the only bypass function between the RED and BLACK side of the terminal.

Protocol- or waveform-specific communicator information (normally in-band with user information), such as unencrypted protocol headers or addresses, may require bypass.

The CM shall provide the capability to configure a bypass function security policy on a per-waveform basis.

Application-specific control/status information may require bypass. For example:

1) The RED processor may initiate an IKE exchange by sending a control message to the BLACK processor, which then constructs and sends the IKE message 1 (unencrypted).

---

2)The RED processor may initiate an antenna pointing change by sending antenna control commands to the antenna control system (Black Processor), which performs the configuration change.

3) The BLACK processor may provide signal level status information to the RED processor, which initiates adjustments to data rates.

The CM shall provide the capability to configure a control/status bypass function security policy on a per-application basis

The communicator information bypass function shall be distinct from the control/status information bypass function. Both the communicator information bypass function and the control/status information bypass function shall be reprogrammable.

The CM shall use a message identifier and the total message length to make bypass decisions.

12. TERMINAL SOFTWARE CONFIDENTIALITY AND INTEGRITY

The CM shall provide the capability to encrypt terminal software for data at rest storage.

The CM shall provide the capability to decrypt and integrity check terminal software taken from data at rest.

The CM shall provide the capability to decrypt and integrity check terminal software updates loaded during "on air" terminal operation using

The terminal shall be configurable to use Suite A or Suite B keys for encryption and decryption of terminal software. Potentially a security requirement may be derived that

assures only Suite A keys are used for non releasable terminal software.

13. CRYPTOGRAPHIC SOFTWARE CONFIDENTIALITY AND INTEGRITY

The CM shall provide the capability to encrypt the cryptographic software for data at rest storage.

The CM shall provide the capability to decrypt and integrity check the cryptographic software taken from data at rest storage.

The CM shall provide the capability to decrypt and integrity check the cryptographic software updates loaded during "on air" terminal operation.

The terminal shall be configurable to use Suite A or Suite B keys for encryption and decryption of cryptographic software. Potentially a security requirement may be derived that assures only Suite A keys are used for non releasable cryptographic software.

14. UNCLASSIFIED STORAGE/SHIPPING OF CM

The CM shall provide the capability to render it unclassified for storage/shipping.

15. DATA AT REST PROTECTION

The CM should support both Type 1 and non-type 1 data at rest encryption/decryption services.

---

16. CRYPTOGRAPHIC MODERNIZATION

When the CM satisfies the requirements defined in this paper, it will satisfy NSA Policy 3-9 requirements for cryptographic modernization. This policy includes: Assured security robustness, Cryptographic algorithm support, Interoperability, Releasability, Programmability, CM Management, and KMI Compatibility.

17. SCA COMPLIANCE

The HC3 terminal is required to be compliant with the Software Communications Architecture (SCA). The CM architecture shall be compliant with the applicable requirements of the Software Communications Architecture Specification, JTRS-5000, SCA V3.0, August 27, 2004. There are several methods by which SCA compliance may be provided by a particular implementation of these requirements. The choice of method is an implementation detail outside the scope of this document.

The SCA specifies an Operating Environment (OE) that includes a Core Framework (CF), a Portable Operating System

Tp

tr.*f ee (POSIX) compliant Operating System (OS),

and a Common Object Request .,faer Architecture (CORBA) middleware.

The CM shall be compliant with the applicable requirements in the Security Supplement to the Software Communications Architecture, JTRS-5000 SEC, V3.0, August 27, 2004.

The following CM requirements represent a subset of those that are either explicitly stated collection of SCA specifications (and elevated to this level to highlight the necessary algorithms and capabilities) or implied by one or more of the requirements from that set:

â€¢ Identification and authentication:

o The CM shall provide Digital Signature Standard (DSS) cryptographic processing.
o The CM shall store DSS certificates.
o The CM shall generate DSS authentication messages._
â€¢ Integrity:
o The CM shall provide Secure Hash Algorithm (SHA-1) processing.
o The CM shall generate SHA-1 based integrity checks.
â€¢ Key management:
o The CM shall develop encryption keys via FIREFLY processing.
â€¢ Algorithm management:
o The CM shall decrypt classified cryptographic algorithms using the JOSEKI-1 algorithm.
o
The CM shall only accept cryptographic algorithms signed by the NSA.

.UNCLASSIFIED//FOR OFFICIAL USE JNLY
CM-001-03
18. INFORMATION SECURITY (INFOSEC)
The CM will comply with the security and information assurance (IA) requirements provided in a document by the NSA as part of the User Partnership Agreement (UPA) for NSA cryptographic certification.
CM security and IA requirements will be developed in accordance with tailored Unified INFOSEC Criteria (UIC), and documented in a Theory of Design and Operation (TDO).
The CM shall include security mechanisms sufficient to satisfy the NSA requirements allocated to the CM. The NSA will provide a document containing these requirements as part of the UPA for NSA cryptographic certification.
The CM will demonstrate compliance with any additional security or IA requirements imposed outside of the TDO by CM Type 1 certification with the NSA.
The CM shall protect sensitive software and firmware within the CM tamper boundary.
The CM shall support Type-1 security classification up to TS/SCI for a single compartment.
The CM shall include means of enforcing the least privilege principle. The least privilege principal requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks.
The CM shall include services that allow the terminal to enforce that the system manager is authenticated before the terminal accepts its commands.
The CM shall audit security relevant events. Security relevant events will be identified in the appropriate security document.
The CM shall provide audit data to the system manager upon request.
The CM shall perform cryptographic testing in order to become operational. The CM will not transition to the operational state until the CM passes all security-relevant tests.
The operational CM shall provide the capability to automatically perform specified periodic cryptographic testing_ The CM must pass all security-relevant tests in order-to---

remain operational.

19. SYSTEM ENVIRONMENTAL REQUIREMENTS

The CM is installed in an HC3 terminal subsystem LRU that is expected to provide a protected environment.

The CM may be configured as a chipset to be integrated into HC3 terminal circuit card(s) or

a stand alone module that plugs into a terminal circuit card backplane.

19.1 Temperature

The CM is installed in an LRU that is expected to provide an environment that satisfies the CM temperature needs.

The CM shall be designed for storage within a temperature range of -40Â° C to +71Â° C.

28

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNL ASSIFIED//FOR OFFICIAL L,E ONLY

CM-001-03

The CM, when configured as a module, shall be designed to operate at rail temperatures within the range of -40Â° C to +49Â° C.

19.2 Shock

The CM, when configured as a module, shall withstand non-operating shock levels applied on each axis of: - 75g for 11 ms, 175g for 2 ms, half-sine.

The CM, when configured as a module, shall operate normally when operating shock levels are applied on each axis of: - 20g for 11 ms, 65g for 2 ms, half-sine.

The CM, when configured as a module, shall withstand bench-handling shock in accordance with MIL-STD-810F, Method 516.5, Procedure VI: 45-degree drop.

19.3 Vibration

19.3.1 Sinusoidal Vibration

The CM, when configured as a module, shall ;:_a. ; e â€žuorally when operating vibration li

mits of 5-50 Hz/6g, 50-400Hz/1.25g, 400-2000 Hz/.25g are applied in a twenty-minute logarithmic sweep, from low to high frequency, per axis.

The CM, when configured as a module, shall withstand the non-operating vibration limits .of 5-50 Hz/6g, 50-400Hz/4g, 400-2000 Hz/.5g are applied for a twenty-minute logarithmic sweep, from low to high frequency, per axis.

19.3.2 Random Vibration

The CM, when configured as a module, shall operate normally under the random vibration conditions in [MIL-STD-810D] Figure 514.3-36, 10 minutes each axis. Figure 514.3-36 indicates a level vibration energy level that is a flat .04 g2/Hz level from 20 Hz outwards to 1,000 Hz, followed by a 6 db/octave roll-off after 1,000 Hz to 2,000 Hz limit.

The CM will be tested in a simulated operational environment (no interfacing devices).

19.4 Chemical, Biological, Radiological and Nuclear (CBRN)

The platform may be required to operate during and after exposure to a CBRN warfare agent environment and decontamination process. The CM, however, is protected from CBR contaminants by the platform and HC3 enclosures, which prevents the ingress of contamination into the CM. The CM will operate during and after exposure to radiation

dose and dose rates non-lethal to humans.

19.5 Electromagnetic Radiation

The CM design, when configured as a module, shall follow good Electromagnetic Interference (EMI) design practices as guided by the Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment [MIL-STD-461E

19.6 TEMPEST

Although the platform is ultimately responsible for Telecommunications Electronic Material Protected from Emanating Spurious Transmissions (TEMPEST) protection, the CM design, when configured as a module, shall implement design practices to support the platform TEMPEST certification.

20. SYSTEM QUALITY FACTORS

20.1 Built-in-test

The CM, when configured as a module, shall provide Failure Rate Weighted Fault Coverage greater than or equal to 95% without the use of external built-in test (BIT) components.

The CM, when configured as a module, shall provide a False Alarm Rate (FAR) of less than or equal to 3%.

20.2 Reliability

The CM, when configured as a module, shall have a minimum operating life of 15,000 hours. The CM life profile definition is TBS.

The CM, when configured as a module, shall have a Mean Time Between Failure (MTBF) of greater than or equal to 20,000 hours in a ground mobile environment at a rail operating temperature of 35 C. Failure rates will be based on the Telcordia reliability prediction procedures, Issue 1, in accordance with Section 3.1.

20.3 Maintainability

All CM maintenance, when configured as a module, will be performed at depot or factory level. If an CM fails at the field level, it or its LRU will be replaced.

20.4 Design and Construction Constraints

The CM-design-will follow good workmanship practice-as guided by the-General -- Guidelines for Electronic Equipment [MIL-HDBK-454A].

The CM design will use the General Specification for Nameplates/Labels and Marking of Electronic and Electro-Mechanical Equipment [NSA-2J] for guidance with product markings. Note that this specification may contradict Army nameplate requirements but meeting NSA's marking requirements are necessary for certification.

21. COMMENTS

The documents and studies provided do not establish hard performance requirements in terms of bandwidth and latency as there are several areas that need more rigorous system design tradeoff analyses. Some topics for consideration follow.

UNCLASSIFIED//FOR OFFICIAL USG ONLY

CM-001-03

Latency:

Latency for request/reply interfacing concepts is an example. The terminal must tune to a certain frequency and at a certain time based on TRANSEC streams provided by the CM. This may involve several components, each with processing time (latency). The terminal latency contribution budget for each component is not discussed in the documentation available, although there is some mention of a specific TRANSEC stream exposure time vs. secure protection, i.e. TRANSEC bits when used within a specified time can be treated as black data and thus simplify the terminal security architecture. There are so many variables in terms of packet lengths, overhead, security assurances, impacts on the terminal INFOSEC architecture, and interface protocol that it may not be feasible to establish latency parameters without a significant systems engineering trade effort beyond the scope of this document.

Simultaneous Keys and Active SAs:

The documentation supports the

.

CM need for the capability

.::1tLacously support up

to 7 independent TRANSEC modulation/cover keys streams per channel on some waveforms, each using a different key perhaps. In addition, there may be two independent waveform COMSEC SAs per channel and 16 additional HAIPE remote management SAs. The number of SAs the CM needs to support simultaneously, therefore, appears to be 7x4 + 2x4 + 16 = 52 SAs worst case, which is well within current technology. As mentioned in the body of this paper, a net ID or COI may be treated as a unique seed variable and may not be considered a unique SA. At the TIM it was mentioned that each COI or net may use a different key. The available documentation does not quantify this requirement, however. The current technologies can support hundreds to thousands of SAs at HC3 rates.

TRANSEC Bit Rate:

The documentation we analyzed contains TRANSEC stream bit rate inconsistencies and there is an independent effort to determine what may be required or desired. The values specified-in-this requirements-description-paper-reflects-the-worst-case scenarios--found--in-the documentation provided to General Dynamics C4 Systems (GDC4S).

Multiple Security levels for one TRANSEC Channel:

Requirements are defined to provide the capability to operate at all security levels from SBU to TS/SCI with simultaneous operation on up to four channels at different security levels while providing the required domain separation. Operating each channel at a single classification level simplifies the CM design, however. Operating at multiple levels with domain separation on a single channel impacts CM assurance mechanism complexity as well as its size and power consumption by a significant factor. We have defined the requirement as a single level per channel.

Multiple security levels was mentioned in a TIM but has not been found within the

documents provided as source information to this study. Multiple TRANSEC streams based on different keys on a single channel to support waveform TRANSEC for different Communities of Interest nets, and types of data cover is clearly required. It also appears that TS/SCI is

---

required for waveform COMSEC (encryption) functions only on certain waveforms that are used for LOS type channels. If the waveform TRANSEC streams generated on a channel are limited to SECRET high, there may be some savings in assurance complexity with resulting size and power savings along with performance improvements. Protecting TS/SCI information requires a higher level of assurance built into the design than those required to protect SECRET high information.

Security Landscape:

We should also note that the Unified INFOSEC Criteria (UIC) and certification landscape has been moving toward stricter software development guidelines and stricter guidelines regarding use of COTS as well as given increased attention to least privilege concepts and signed and encrypted software protection approaches. NSA is moving toward a more conservative certification approach where the reuse of some legacy security architectures may not be acceptable.

A. ACRONYMS

AEHF
AES
AROW
ASCII
ATOW
BIT
CBRN
CDL
CF
CIK
CKL
CM
CORBA
L:O
T
1'H

COTM
COTQH
CRC
CT
DF
DoD
DSCP
DSS
DTD
ECN
ECU
EFF
EHF
EK
EKL ---
EKMS
EMI
ESN
ESP
FAR
FIPS
FSDA
Gbps
GCM
GMT
HAIPE
HC3
HIJMMWV
Advanced Extremely High Frequency
Advanced Encryption Standard
Acquisition and Report-back Order-Wire
American Standard Code for Information Interchange
Acquisition and Tracking Order-Wire
Built-in Test
Chemical, Biological, Radiological and Nuclear
Common Data Link
Core Framework
Cryptographic Ignition Key
Compromised Key List
Cryptographic Chipset/ModuleCOMSEC Communications
Security
Common Object Request Broker Architecture
Communication on The Halt
Communication on the move
Communication on The Quick Halt
Cyclic Redundancy Check

Ciphertext
Don't Fragment
Department of Defense
Differentiated Services Code Point
Digital Signature Standard
Data Transfer Device
Explicit Congestion Notification
End Cryptographic Unit
Enhanced FIREFLY
Extremely High Frequency
Exclusion Key
Exclusion Key List
Electronic Key Management System
Electromagnetic Interference
Electronic Serial Number
Encapsulated Security Protocol
False Alarm Rate
Federal Information Processing Standard
Fail Safe Design Analysis
Gigabits Per Second
Galois Counter Mode
Greenwich Mean Time
High Assurance Internet Protocol Encryptor
High Capacity Communications Capability
Heavy High Mobility Multipurpose Wheeled Vehicle

CM-001-03
HMI
Human Machine Interface
HMS
HAIPE Management Station
HTTP
Hypertext Transfer Protocol
Hz
Hertz
IAD
Information Assurance Directorate
ICMP
Internet Control Message Protocol
ICV
Integrity Check Value
IETF

Internet Engineering Task Force
IGMP
Internet Group Management Protocol
]HI
Internet Protocol Header Length
IKE
Internet Key Exchange
ISAKMP
Internet Security Association and Key Management Protocol
INE
Inline Network Encryptor
INFOSEC
Information Security
IP
Internet Protocol
IPsec
Internet Protocol Security
IS
Interoperability Specification
IV
Initialization Vector
JTRS
Joint Tactical Radio System
Kbps
Kilobits Per Second
KEK
Key Encryption Key
KMI
Key Management Infrastructure
KMS
Key Management System
KSD
Key Storage Device
LDR
Low Data Rate
LEF
Link Encryptor Family
LMD/KP
Local Management Device/Key Processor
LOS
Line of Sight
LRU
Line Replaceable Units
LSb
Least Significant Bit

Mbps
Megabits Per Second
MDR
Medium Data Rate
MIB
Management Information Base
MLD
Multicast Listener Discovery
MODEM
Modulator Demodulator
MQV
Menezes-Qu-Vanstone
MSb
Most Significant Bit
MTBF
Mean Time Between Failure
MTU
Maximum Transmission Unit
NCDL
Networked Common Data Link
ND
Neighbor Discovery
NIST
National Institute of Standards and Technology
NSA
National Security Agency
OE
Operating Environment

CM-001-03
OTAR
OTAT
OTAZ
OTNK
PBC
PKI
PMTU
POSIX
PPK
PT
PWS

RF
RFC
RIP
RIPng
RRQ
SA.
SAD
SATCOM
SBU
SCA
SCI
SHA
SNMP
SPD
SPI
SV
TBD
TBR
TBS
TDO
TEK
TEMPEST
TFC
TFTP
TIM
TMOS
TNM
TOD
ToS
TRANSEC
TrKEK
TS/SCI
TSAT
TSK
Over-The-Air Rekey
Over-The-Air Transfer
Over-The-Air Zeroization
Over-The-Network Keying
Per Block Counter
Public Key Infrastructure
Path Maximum Transmission Unit
Portable Operating System Interface
Pre-placed Key
Plaintext
Performance Work Statement
Radio Frequency

Request For Comments
Routing Information Protocol
Routing Information Protocol Next Generation
Read Request
Security Association
Security Association Database
Satellite Communications
Sensitive, But Unclassified
Software Communications Architecture
Sensitive Compartmented Information
Secure Hash Algorithm
Simple Network Management Protocol
Security Policy Database
Security Parameter Index
State Variable
To Be Determined
To Be Revised
To Be Specified
Theory ofDesign and Operation
Traffic Encryption Key
Telecommunications Electronic Material Protected from
Emanating Spurious Transmissions
Traffic Flow Confidentiality
Trivial File Transfer Protocol
Technical Interchange Meeting
Transformational Satellite Mission Operations System
Tactical Network Management
Time of Day
Type of Service
Transmission Security
Transmission Key Encryption Key
Top Secret/Sensitive Compartmented Information
Transformational Satellite
Transmission Security Key

TTL
Time To Live
UDP
User Datagram Protocol
UIC
Unified INFOSEC Criteria

UPA
User Partnership Agreement
URI
Uniform Resource Identifier
USM
User-based Security Model
VITA
VMEbus International Trade Association
WGS
Wideband Gapfiller Satellite
WRQ
Write Request
XDR
Extended Data Rate

Y
'r
ill
UNCLASSIFIED//FOR OFFICIAL USE ONLY
CM-001-03
B.
HAIPE IS REQUIREMENT ALLOCATION
The following table presents the allocation ofithe HAIPE IS 3.0 requirements to the CM, portions of the terminal other than the CM,
or to both. Notes are provided as necessary to provide additional detail or justification.
Requirement II
Requirement Type
Requirement Text
Requirement Source HC3 Allocation
Notes
TP.1
Threshold
HAIPEs shall pre-configure the deviceVersionTable as follows: dvName is "TrafficProtection", and dvVersion is "3.0.0".
1
Traffic Protection Core Terminal
TP.ESP.1
