



CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-8
DISTRIBUTION: A, B, C

CJCSM 6520.01A
9 December 2011

LINK 16 JOINT KEY MANAGEMENT PLAN

Reference(s):

- a. CJCSM 6120.01 Series, "Joint Multi-Tactical Data Link (TDL) Operating Procedures"
- b. NAG-45A, August 2001, "Operational Security Doctrine for Joint Tactical Information Distribution Systems (JTIDS)"
- c. DOC-023-08, December 2008, "Operational Security Doctrine for the Multifunctional Information Distribution Systems (MIDS)"
- d. SSS-M-10001, Rev. EG, January 2011, "System Segment Specification for the Multifunctional Information Distribution System (MIDS) Low-Volume Terminal and Ancillary Equipment"

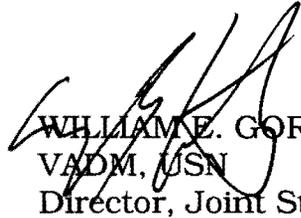
1. Purpose. This manual outlines procedures for production, distribution, and use of Link 16 Communications Security (COMSEC) keying material (KEYMAT). Enclosure A contains the Link 16 Joint Key Management Plan, and Enclosure B provides the Link 16 COMSEC Entities Contact List. The Joint Multi-Tactical Data Link (TDL) Operating Procedures manual (reference a) provides further guidance regarding operational management of Link 16 and other tactical data links. References b and c contain NSA security doctrine associated with Link 16 devices.

2. Cancellation. CJCSM 6520.01, 28 January 2008, "Link 16 Joint Key Management Plan," is canceled.

3. Applicability. This manual provides guidance to Services, combatant commands, unified commands, and Defense agencies involved in the production, distribution, or use of Link 16 KEYMAT.

4. Policy. This manual documents current key management procedures and the procedures applicable to the Electronic Key Management System (EKMS).

5. Definitions. See Glossary
6. Summary of Changes. This document establishes procedures to be used by Services, combatant commands, and Defense agencies in the production, distribution, and management of Link 16 COMSEC material under the current system and EKMS.
7. Releasability. This manual is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this manual online from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.
8. Effective Date. This manual is effective upon receipt.



WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosure(s):

- A - Link 16 Joint Key Management Plan
- B - Link 16 COMSEC Entities Contact List
- GL - Glossary

TABLE OF CONTENTS

	Page
ENCLOSURE A - LINK 16 JOINT KEY MANAGEMENT PLAN	
General Information	A-1
Background	A-1
System Description	A-1
Security	A-4
KEYMAT	A-5
SDU	A-9
Key Loading Devices	A-12
EKMS	A-15
Description	A-15
Purpose	A-15
Functional Description	A-15
EKMS Key Distribution	A-17
EKMS Key Request Process	A-18
EKMS Key Ordering Parameters	A-18
Parameters	A-18
Examples of Typical Parameters	A-20
Joint Operational Keys	A-21
Key Management Infrastructure	A-22
OTAR Management	A-22
Description	A-22
Purpose	A-22
Required Elements	A-22
Procedures	A-23
Other Considerations	A-24
Joint Key Management Plan Procedures	A-25
Introduction	A-25
Responsibilities	A-25
Key Generation	A-28
Key Distribution	A-28
Key Storage	A-29
Key Loading	A-31
Cryptoperiods	A-31
Compromise Procedures	A-31
OPTASKLINK	A-32
ENCLOSURE B - LINK 16 COMSEC ENTITIES CONTACT LIST	B-1
GLOSSARY	
PART I -- ABBREVIATIONS AND ACRONYMS	GL-1
PART II -- DEFINITIONS	GL-5

TABLE

1	Link 16 Terminals, Users, and Associated Platforms.....	A-2
2	KEK Types	A-6
3	Link 16 Terminal/SDU Use	A-11
4	Crypto Period Determination Table.....	A-14
5	Operational Link 16 Key Allocation.....	A-18
6	Nominal Combined Force COMSEC Requirements.....	A-29
7	Crypto Storage Location Guidance	A-30

ENCLOSURE A

LINK 16 JOINT KEY MANAGEMENT PLAN

1. General Information

a. Background. Link 16 is the DOD and NATO primary tactical data link for Service and Defense agency C2, intelligence, and in some cases, weapons systems applications. It is a secure, jam-resistant data link primarily using the Joint Tactical Information Distribution System (JTIDS) (AN/URC-107 Series) and Multifunctional Information Distribution System (MIDS) low-volume terminal (LVT) (AN/USQ-140 Series) family of terminal sets. Link 16 supports functional mission areas including joint theater air and missile defense, attack operations, counter-air, interdiction, suppression of enemy air defenses, close air support, and time-critical targeting prosecution. Link 16 networks may include allied or coalition forces and are protected by COMSEC equipment and KEYMAT. Due to the nature of coordinated Link 16 networks, KEYMAT will normally be generated and distributed by the EKMS, described in paragraph 3. Some KEYMAT may be generated locally by EKMS Tier 2 COMSEC accounts supporting operational forces that may need an ad hoc Link 16 network or Link 16 Network Participation Group (NPG) for training, exercise, or specialized operations. Future Link 16-related developments such as Crypto Modernization and Key Management Infrastructure (KMI) will be added to this plan as they are deployed.

b. System Description. Link 16 uses a uniquely defined waveform and frequency range (960–1215 MHz) for digital voice and packet message communication. Terminals communicate using the Link 16 message standard format defined in Military Standard (MIL-STD) 6016 and a time division multiple access (TDMA) architecture with participant transmissions assigned to specific time slots. Link 16 typically functions as a line-of-sight system capable of operating in the normal mode of operations at ranges up to 300 nm or an extended mode at a range of 500 nm. This range can be further extended through the use of relay platforms.

(1) Hardware. Table 1 describes Link 16 terminals and associated platforms. In addition, Link 16 capability is embedded into the systems architecture of the F-22A Raptor (receive-only) and the F-35 Lightning II, Joint Strike fighter.

Terminal	Size	Power	Users	Platforms
JTIDS Class 1	6 cu ft 310 lb	200/1000 W	NATO	Numerous NATO
JTIDS Class 2	1.6 cu ft 130 lb	200 W	USAF	COMPASS CALL JSTARS MCE SENIOR SCOUT And other variants
JTIDS Class 2H	3.25 cu ft 220 lb	200/1000 W	USAF USN USMC	AWACS And other variants AEGIS CG/DDG CVN/LHD/LCC E-2C TAOM TAOC
JTIDS Class 2M	1.3 cu ft 89 lb	40/200 W	USA	PATRIOT JTAGS ADTOC SHORAD THAAD
MIDS-LVT(1)	0.61 cu ft 65 lb	200/1000 W	U.S. NATO FMS	F/A-18 EF-18 NHPS Asset X EA-6B MH-60R/S
MIDS-LVT(2)	1.35 cu ft 80.9 lb	25/200 W	USA	PATRIOT THAAD ADAM Cell
MIDS-LVT(3) (FDL)	0.61 cu ft 45 lb	50 W	USAF	F-15 ROBE And other variants
MIDS-LVT(4)	0.61 cu ft 65 lb	1/25/200 W + HPA Interface	USAF	LAK BCS-M CAC2S NORAD RAIDER GTACS And other variants
MIDS-LVT(5)			USN	MOS
MIDS-LVT(6)	0.61 cu ft 65 lb	1/25/200 W + HPA Interface	USAF	F-16 AC-130 And other variants
MIDS-LVT(7)	0.61 cu ft 65 lb	1/25/200 W + HPA Interface	USAF	Airborne Laser B-2 And other variants

Table 1. Link 16 Terminals, Users, and Associated Platforms

Terminal	Size	Power	Users	Platforms
MIDS-LVT(11)	1.35 cu ft 80.9 lb	25/200 W	USAF	JSS Pocket J And other variants
MIDS JTRS	0.61 cu ft 65 lb	1/25/200 W	All Services	F/A-18 E/F E-2D EF-18 G JSTARS Rivet Joint Compass Call
FES (Front End System)	0.88 cu ft 45 lb	Receive Only	All Services	Support Systems
Net Enabled Weapons (ex: KOR-8)	80 cu in	45 W	USAF USN	Joint Standoff Weapons
KOR-24 Small Tactical Terminal (STT)	0.2 cu ft 20 lb	50 W	All Services	Dismounted/ Disadvantaged users
Sea Harrier (SHAR) AN/URC-138	0.53 cu ft 39.8 lb	200 W	GBR	Sea King, NIMROD, ASTOR

Table 1. Link 16 Terminals, Users, and Associated Platforms (Continued)

(2) Transmission Characteristics

(a) TDMA. The TDMA transmission structure decomposes data into message sets transmitted during pre-planned intervals (time slots). Each participating terminal is allocated time slots to transmit, receive, or relay data. Within each time slot, radio terminal transmission/reception “hops” among 51 discrete frequencies to improve jam resistance. In some cases, a reduced hop set of frequencies may be used when mandated by spectrum authorities. This pseudo-random frequency-hopping sequence is determined by the transmission security key (TSK). Further information regarding the Link 16 waveform may be found in the MIDS System Segment Specification.

(b) Time Slot. A time slot is a standard interval (7.8125 msec) assigned to individual Link 16 participating units for message transmission. With the exception of voice, round-trip timing (RTT), and free text, data transmitted within a time slot is composed of three, six, or twelve 70-bit words, depending on the packing structure used. The design of the network establishes the assignment of transmit and receive time slots to each participating platform.

(c) Network Participation Groups (NPGs). NPGs are the basic Link 16 communication “circuits.” Each Link 16 network design assigns time slots within NPGs based on the type of information being exchanged. NPGs include net entry, precise participant location and identification (PPLI), RTT, network management, mission management, surveillance, and voice. Messages produced by host combat systems are routed for transmission to specific, but

9 December 2011

arbitrary, NPGs. Since terminals provide NPG filtering and selection, message assignment by NPG may be used for partitioned security and selective filtering.

(3) Network Management

(a) Network Selection. Link 16 networks are utilized based on the theater data link architecture or operational and training requirements. Operational architectures normally require use of a U.S. joint or allied operational key. Training architectures may require the use of a specialized key.

(b) Network Deconfliction. A Link 16 network is a group of participants in time synchronization and exchanging information. Planning is required to ensure that different networks (encompassing different participants and/or purposes) do not cause mutual interference. There are three ways to ensure successful independent network operations: geographic separation such that synchronization cannot be achieved between two different networks, different key (cryptographic differentiation), or network time offset. When independent operations are sufficiently close that inadvertent synchronization between networks is possible, use of a different key (i.e., a different short title) is the preferred method for resolving independent networks. Network time offset of not more than plus 60 minutes may be used only for training operations unless otherwise approved by the joint interface control officer and stated in the operations task link (OPTASKLINK) message. Time offsets shall be managed to ensure that no single terminal reuses a key. For example, a terminal using a forward time offset cannot revert to a standard (zero) time offset using the same key and commence transmissions until the difference in time between networks has expired. Use of a negative time offset for Link 16 network time is prohibited. Network deconfliction will become a less frequent option as external time reference networks are directed that rely on tight coupling to a Coordinated Universal Time (UTC) source.

c. Security. Link 16 circuits may be used to transmit information up to and including SECRET. Link 16 has been evaluated and is approved by the Director, NSA, for operation in the SECRET HIGH security mode if all network participants are cleared for SECRET and have access approval for all information in the Link 16 net. NSA has also assessed Link 16 for the exchange of compartmented and special access information. Although NSA cannot currently certify Link 16 for operation in compartmented mode, segregation can be accomplished by using a separate key for a specific NPG. Because of these information segregation features, a particular designated accrediting authority or certifying authority can, after their own risk assessment, authorize Link 16 for exchange of compartmented or special access information (up to TOP SECRET HIGH) associated with their program. The full cryptographic and information segregation feature of Link 16 should be used. Each program must evaluate alternatives and specify procedures (e.g., special key, special messages, or additional encryption). All personnel

authorized uncontrolled access to Link 16 terminal areas must be cleared at least to the classification level of the Link 16 data being exchanged. Link 16 terminals currently use a THORNTON-based secure data unit (SDU), making them cryptographically compatible. The SDU provides both transmission security (TRANSEC) and communications security (COMSEC) for message security (MSEC)

(1) TRANSEC. Each Link 16 terminal can operate on any one of 127 different nets with each net defined by a distinct pseudo-random frequency-hopping pattern, increasing resistance to jamming and exploitation. TRANSEC assignment is one of the Link 16 network initialization parameters and, together with the time slot number, determines the hopping sequence for each net and provides symbol interleaving, pulse modulation encryption, carrier frequency hopping, and message start jitter. The TSK is also used to transmit connectivity maintenance messages such as PPLIs.

(2) MSEC. Link 16 messages are transmitted via data blocks and encrypted using an MSEC key assigned by the Link 16 network initialization parameters. Traffic encryption keys (TEKs) provide Link 16 MSEC.

d. KEYMAT. A standard 128-bit TEK provides TRANSEC and MSEC. A standard 256-bit Key Encryption Key (KEK) or RUTTER (KOK-13) KEK encrypts and decrypts TEK to decrease risk of exploitation during distribution, issue, and loading.

(1) TEK. TEK is the basic key for encrypting operational message traffic. TEK provides TRANSEC and MSEC.

(2) KEK. A goal of EKMS is to minimize human access to KEYMAT. One strategy used to protect KEYMAT from exploitation is encryption using KEK. The four types of KEKs (yielding four corresponding types of encrypted KEYMAT) are listed in Table 2, below.

(a) Over-the-Air Rekey (OTAR) KEK. OTAR KEK (sometimes referred to as the “unique” key) is loaded in the SDU and used to encrypt and decrypt a “rekey phrase.” This rekey phrase is transmitted to the Link 16 terminal and processed by the SDU when conducting OTAR and will be subsequently referred to in this document as OTAR encrypted key. Unlike other Link 16 keys, OTAR encrypted keys are always received by the SDU through the terminal interface rather than the fill port interface.

(b) ECU KEK. ECU KEK is installed in the SDU. The encrypted key obtained from the ECU KEK is an ECU encrypted key. ECU encrypted keys are received through the fill port.

KEK	Protected Material	Protected Path	Specific Protected Material	KEK Account/Load	KEK Production Location
OTAR KEK	Individual keys	Over the air from System Controller (SC) Link 16 terminal to remote Link 16 terminal	Link 16 TEKs, OTAR KEKs	At KOK-13 and location 5 of Link 16 SDU	In the KOK-13 or Tier 2
ECU KEK	Individual keys	From Tier 2 through Tier 3 fill device to ECU	Link 16 TEKs, ECU KEKs, ¹ OTAR KEKs	At Tier 2 and ECU	At Tier 1 or Tier 2
TrKEK	Individual keys	From Tier 2 to Tier 3 fill device	Link 16 TEKs, ECU KEKs, OTAR KEKs	At Tier 2 and fill device	At Tier 2
EKMS KEK	Bulk key sets	Between Tier 0, Tier 1, and Tier 2	See EKMS Doctrine	At Tier 0, Tier 1, and Tier 2	At Tier 0, Tier 1, and Tier 2

¹ Although encryption of End Cryptographic Unit (ECU) KEKs in ECU KEKs is technically possible, procedures for accomplishing this have not been developed.

Table 2. KEK Types

(c) Transmission Key Encryption Key (TrKEK). This KEK is installed in the Tier 3 fill device (i.e., AN/CYZ-10 Data Transfer Device (DTD), AN/PYQ-10 Simple Key Loader, Simple Key Loader (SKL)/, KIK-20 Secure Data Transfer Device 2000 System (SDS)). Tier 2 encrypts keys for the user in a TrKEK. The encrypted keys protected by this TrKEK are referred to in this document as fill device encrypted keys. The fill device uses the TrKEK to decrypt the fill device encrypted keys prior to loading into an SDU. Although there are additional KEK and encrypted storage keys internal to EKMS, sometimes also referred to as TrKEK, they will not be addressed here. For the purposes of this document, TrKEK describes KEKs used to encrypt individual keys from Tier 2 to the fill device.

(d) EKMS KEK. EKMS KEK is used for data and key bulk encryption and to protect a key transferred between EKMS Tier 0, Tier 1, and Tier 2.

(3) Key Availability. Link 16 COMSEC is established through use of either the Common Variable Mode (CVM), in which a single TEK is used to provide both TRANSEC and MSEC, or the Partitioned Variable Mode (PVM), in which one TEK is used for TRANSEC and a different TEK is used for MSEC. Coordinated joint operations require that different platforms use both the same TEK short titles and coordinated network from the JTIDS network library (JNL) to supply the initialization parameters to the platforms. Link 16 is structured to support multiple cryptonets using different TEKs (i.e., it can use more than

9 December 2011

one short title at a time), and the system is capable of smoothly operating on four cryptonets simultaneously. Although no maximum size limit is prescribed for Link 16 TEK cryptonets, they should be as small as operationally feasible. To minimize the risk of global compromise, the same TEK short title must not be used worldwide. To facilitate compliance with this requirement, a worldwide key is available for emergency and contingency operations, and numerous TEKs are available for each regional combatant command. Each command may use its collection of short titles as operationally required. Paragraph 4 describes the procedures followed by combatant commands when ordering short titles. EKMS generates and distributes keys to authorized accounts in accordance with the account's reserve-on-board (ROB) requirements. Some Tier 2 accounts hold the key for Tier 3 local elements. Availability of required keys at these EKMS Tier 2 account provider servicing facilities enables rapid distribution to the Tier 3 accounts. Combatant commands should include Link 16 key distribution in operational and contingency plan development.

(4) Key Types. Since the Link 16 key is available in either unencrypted or encrypted format, appropriate KEKs are generated, distributed, and issued along with the encrypted form of any short title at the lowest practical EKMS tier. ECU encrypted keys, both TEK and KEK, shall be used wherever feasible. Encryption of unencrypted keys is the responsibility of the commander at the lowest EKMS Tier 2 distribution element. KEK is used to protect the movement of an underlying unencrypted key from the local EKMS account through to the using ECU. The command encrypting a key is responsible for managing KEK distribution to the ECU for decryption of the ECU encrypted keys. All over the air data transmission in the Link 16 system KEK must be protected by a key of type TEK that is at least classified SECRET.

(a) Operational Keys. These keys are used to support operational missions. They are at least SECRET CRYPTO and change each cryptographic period. Operational keys are designated for special global use or for a specific combatant command.

(b) Maintenance Keys. These global keys are used to support maintenance. They are "For Official Use Only." Maintenance keys are also used in research, development, test, and evaluation. Some users may require SECRET training keys that do not change for each cryptographic period and are used to conduct security training. If training keys are not available, maintenance keys may be used to train personnel on procedures for key loading.

(c) Test Keys. These keys are used to conduct "on-the-air" testing under operational conditions. They include SECRET keys that change for every cryptographic period (global, but not necessarily pre-positioned). Operators should select the appropriate key based on classification requirements precipitated by the test. An operational key may also be used for test purposes

within the valid cryptographic period for that key. Operational keys should be used if the data transmitted has operational value.

(5) Operational Key Allocation. Link 16 requires several operational keys, which are described below.

(a) Emergency Contingency Operational Key. One set of joint keys will be maintained for worldwide emergency contingency use. This set will be held by **all** Link 16 user COMSEC accounts and used only under direction of the Joint Staff to support an emergency in which users from different combatant AORs must arrive in a theater of operations on short notice. The Joint Communications Security Management Office (JCMO) orders the short title for an emergency contingency operational key.

(b) Joint Theater Key. This key is used for operations among U.S. commands within a theater of operations. During normal operations, a separate set of short titles will be used for each combatant command. If units from a supporting combatant command are involved, they will obtain the key from the supported commander as part of the normal planning process. Availability of five short titles provides flexibility and the potential for multiple cryptonets.

(c) Allied Keys. These keys are used within an area of operations that includes allied elements. During normal operations, a separate set of short titles will be used for each combatant command. Units from a supporting command that are involved in operations will obtain keys from the supported Combatant Commander as part of the normal planning process. Allied key distribution may also require NSA to distribute keys outside of EKMS. It may also require Service Acquisition Program Offices to program for Coalition Electronic Key Management Systems (C-EKMS) installation, operations, and maintenance as well as connectivity to Tier 2 accounts of the supported COCOM for electronic keymat distribution to coalition partners not part of NATO or CCEBs.

(6) Cryptographic Period. TEK and ECU KEK are distributed using the edition/segment convention.

(a) TEK. Each TEK edition has a 1-month supersession rate, and each TEK segment has a 1-day cryptographic period. Except when using time offset to operate independent networks, the TEK cryptographic period begins exactly 1 minute before 0001 UTC and ends exactly 1 minute after 2359 UTC. A TEK cryptographic period shall not be extended except in cases in which the Link 16 terminal has been initialized in the 7-day mode. Explicit coordination and a Joint Service agreement are required to use a 7-day cryptographic period. Although all Link 16 terminals are capable of operating in a 7-day

mode, many platform C2 systems are not. If one Link 16 unit in a net uses the 7-day mode, all network participants must operate in the 7-day mode.

(b) ECU KEK. Each ECU KEK edition has a 6-month cryptographic period, and each ECU KEK segment has a 1-month cryptographic period. When a Link 16 ECU KEK is generated, the cryptographic period is prescribed to coincide with the TEK that it encrypts/decrypts.

e. SDU. Link 16 terminals use a THORNTON-based SDU, making them cryptographically compatible. The THORNTON family includes various types of SDUs and supporting equipment. The number of traffic keys that the SDUs may store -- 8, 63, or more -- and the COMSEC key loading protocol distinguish the various SDUs.

(1) SDU Types. SDUs are divided into the following three major categories based on common functional characteristics.

(a) KGV-8(E-2), KGV-8A, KGV-8C, and E-GLD. These devices can store and use only TEK and OTAR KEK. Eight random access memory (RAM) locations are available for daily use key storage. These SDUs are keyed via Data Standard (DS) 102 protocol and can receive keys only in the unencrypted form. An external keyer control panel (KCP) or load control unit (LCU) is required to manually select the desired memory location for the key fill process. All keys stored in RAM are non-extractable and are erased when power is removed from the SDU.

(b) KGV-8B and CDH. These devices can be filled with either unencrypted or encrypted TEK in any of 8 (or 64 for MIDS-LVT(2)) RAM storage locations. All keys are stored in unencrypted form. Encrypted keys are decrypted by their associated pre-loaded KEK prior to storage in RAM. Nine electronic erasable programmable read-only memory (EEPROM) locations are available for KEK storage. Keys stored in EEPROM are also stored in unencrypted form. All keys stored in RAM or EEPROM are protected from extraction and exploitation by other means. All keys stored in RAM are erased when power is removed from the SDU. Keys stored in EEPROM can be erased only upon receiving an external command from a fill device. These SDUs are filled via the DS-101 protocol and do not require a KCP. User Application Software (UAS) running on modern fill devices provides the correct DS-101 loading information to set the SDU location into which the key is to be stored. A data management system such as the Joint Mission Planning System (JMPS), Automated Communications Engineering Software (ACES), or the Data Management Device (DMD) is required to format and load encrypted TEK, distributed by EKMS Tier 0 or Tier 2, into a fill device. In addition, programmable COMSEC systems such as the MIDS Joint Tactical Radio System (JTRS) require ACES or DMD to provide tagging information to the fill device for encrypted or unencrypted key loading.

(c) Programmable COMSEC. Emerging systems such as MIDS JTRS, NEW, STT, F-22A, and F-35 use embedded programmable COMSEC solutions to support Link 16. These devices can be filled with encrypted and unencrypted TEK. They can store many days or months of TEK. Internal key management functionality allows these systems to select the correct TEK for the correct crypto period and NPG. These systems also require a data management system such as JMPS, ACES, or DMD to format and load encrypted TEK. In addition, some programmable COMSEC systems such as MIDS JTRS require ACES or DMD to provide tagging information to the fill device for encrypted or unencrypted key loading.

(2) Characteristics. SDUs are distinguished by the number of keys they may store and the COMSEC key loading protocol -- NSA Specification standard DS-102 common fill device interface protocol and NSA Specification Standard DS-101 Data Packet Exchange Protocol. The CDH can be configured to work with either protocol (DS-102 or DS-101), but the only terminal that allows both protocols is the JTIDS Class 2 using the common signal processor (CSP) card. All other uses of the CDH are set to one protocol or the other in the terminal design. Table 3, below, shows the Link 16 terminal types and their associated SDUs.

(a) Fill Port. The SDU fill port is designed in accordance with the Interoperability Standards for Electronic Key Management Systems 308 protocol standard. Keys can be loaded into the E-GLD, KGV-8(E-2), KGV-8A, and KGV-8C using the common fill device interface protocol (commonly referred to as DS-102). Keys can be loaded into the KGV-8B, CDH, and programmable COMSEC using the DS-101 data packet exchange protocol as limited and augmented by NSA Specification 90-2A.

(b) Cryptographic Periods. Link 16 KEYMAT cryptographic periods extend from exactly 1 minute before 0001 UTC to exactly 1 minute after 2359 UTC.

(c) Cryptographic Engine. JTIDS, MIDS, Front End System (FES) and SHAR Link 16 terminals currently use an SDU with a THORNTON-based communications security/transmission security integrated DS-101 Hybrid (CDH) as the primary cryptographic engine. The CDH encrypts and decrypts messages for each time slot. Although the SDU can use the same key for generating the bits used for TRANSEC as well as for encrypting and decrypting messages (MSEC), a different key may be used for MSEC if desired. Eight SDU RAM locations may be used to store keys (64 locations in the MIDS-LVT(2)). Normally half the locations are used for the current day, and half are reserved for the next day. At exactly 1 minute after 2359 UTC, the terminal triggers the SDU to switch to the next day's keys and erase previously used keys. Programmable COMSEC Link 16 systems also use the THORNTON-based

cryptographic solution. The only differences in capabilities are that the programmable COMSEC systems can store many more keys, and are not limited to current and next day functionality.

	SDU	Key Format/Protocol
Class 1	KGV-8	8 keys/DS-102
Class 2	KGV-8 KGV-8A/C KGV-8B ¹	8 keys/DS-102 8 keys/DS-101
Class 2 PIP	CDH on CSP Card ²	8 keys/DS-102 or DS-101
Class 2H	KGV-8 KGV-8A/C KGV-8B ¹	8 keys/DS-102 8 keys/DS-101
Class 2M	E-GLD (EMD models only) CDH embedded on CSP Card ²	8 keys/DS-102 8 keys/DS-101 or DS-102
MIDS-LVT(1)	CDH embedded on SMP Card ¹	8 keys/DS-101
MIDS-LVT(2)	CDH embedded on SMP Card ¹	64 keys/DS-101
MIDS-LVT(3) (FDL)	CDH embedded on SMP Card ¹	8 keys/DS-101
MIDS JTRS	Embedded programmable crypto	8 keys ³ /DS-101
FES	CDH embedded on TCU Card ¹	8 keys/DS-101 or DS-102
STT	Embedded programmable crypto	8 keys/DS-101
SHAR	CDH	8 keys/DS-101

¹ The DS-101 ECU, such as the KGV-8B and CDH, may be filled with an encrypted ECU encrypted key that uses an ECU KEK for encryption and decryption. Consequently, there are nine additional EEPROM key locations for storage of KEKs.

² The CSP (CDH) can be installed as either DS-102 or DS-101. There are switches on the card itself to select which protocol will be used.

³ 8 keys can be loaded at one time but MIDS JTRS supports multiple days.

Table 3. Link 16 Terminal/SDU Use

(d) Special Capabilities. The terminal can also insert an OTAR encrypted key in the SDU at a prescribed time and instruct the SDU to decrypt and store this key in any of its memory locations. An OTAR KEK must have been previously loaded into location 5 and the terminal initialized for OTAR. Programmable COMSEC Link 16 systems do not support OTAR. The capability will be added in the future as part of the NSA crypto modernization initiative.

(e) Automatic Rollover. Unlike systems that require key loading at the change of each cryptographic period (e.g., daily), Link 16 is designed to automatically roll over to a new key at the end of each cryptographic period. Except when using time offset to operate independent networks, Link 16 rollover occurs at the end of the minute defined by 2359 UTC.

(f) SDU Location Pairs. Link 16 utilizes its SDU RAM storage locations in pairs (0/1, 2/3, 4/5, 6/7). Keys for successive cryptographic periods are loaded into each pair. If the terminal is using a key in SDU RAM location 0, the terminal begins using the key in location 1 at rollover and will erase the key in location 0. This relieves the system operator from loading a new key or performing a manual switch. Keys may be loaded for the next succeeding cryptographic period at the operator's convenience. At the end of the next cryptographic period, the terminal begins using the key in location 0 (provided a new key has been loaded) and erases the key in location 1. The same procedure applies for pairs 2/3, 4/5, and 6/7 (the 4/5 pair does not roll over if the terminal has been initialized to use OTAR). The Link 16 terminal is required to roll over all the locations in the same way, from even to odd or odd to even (the terminal will not roll over a 0 to a 1 and at the same time, a 7 to a 6). To keep the Link 16 in continuous operation, key fill must take place daily. It is imperative that successive key fill take place before the second rollover. The programmable COMSEC Link 16 systems are not restricted to the location in pairs paradigm. An internal key management functionality allows these systems to select the correct TEK for the correct crypto period and NPG.

f. Key Loading Devices. COMSEC key loading devices that support Link 16 include the SKL (see paragraph 3d(4)(a)), SDS, KOI-18 and other modern fill devices. The SKL and SDS are the primary EKMS fill devices. The SKL and SDS are used to load the DS-102 or DS-101 protocol SDU and are the only devices that can use the DS-101 protocol. The key is loaded into the fill device using the EKMS Tier 2 workstation. If EKMS cannot provide an electronic or digital key and paper keys are necessary, a key can be loaded into the fill device by attaching a KOI-18 and pulling the paper key through the KOI-18 as directed by the fill device software.

(1) Fill Device Preparation. Prior to loading the SDU, the fill device UAS is set up for the specific SDU. The fill device UAS supports Link 16 by providing an automated set of procedures for assistance in loading a key. Optimally, the UAS allows the user to press one button on the keypad to initiate key loading. Specific identifying data is associated with each SDU in the form of a station identifier (STATION ID) and a station bus address (STATION ADDRESS) for use in single point keying configurations. A PC-based UAS provides users with an automated means of gathering, collating, and formatting the data for transfer to the fill device using either an RS-232 serial or high-level data link control protocol. The data includes key tag, cryptographic period, classification, a unique text identifier (TEXT ID) and

effective date information for the required keys, SDU RAM or EEPROM storage location, and a unique terminal/equipment STATION ID. Additionally, data obtained from the OPTASKLINK message (i.e., key short title, SDU memory location, cryptographic period) is transferred from the PC to the fill device. Data is transferred from the PC to the fill device before or during key loading. Provisions are available for manual entry of identifying data directly into the fill device. Only after the identifying data has been transferred to the fill device can keys be loaded into the Link 16 SDU. Keys are loaded into a fill device from a LMD/KP, another fill device, or a KOI-18 tape reader. An electronic key distributed through Over-The-Air-Transfer (OTAT) can be received directly by a fill device.

(2) Loading TEK. To support automatic rollover, TEKs must be loaded into the SDU in adjacent pair RAM storage locations. Key management data pre-loaded into the fill device establishes which TEK segment is to be loaded into which SDU RAM location. TEK is loaded into the Link 16 SDU daily. During continuous Link 16 operations in which the terminal is not powered off daily, only the next day TEK should be loaded. If the terminal has been powered off, both the current day and next day TEK must be reloaded. The fill device UAS manages daily key loading. Terminals utilizing the KGV-8B must be loaded with the current and next day's TEK each time a key is loaded. CT3 software is designed to do this automatically.

(3) Current Cryptographic Period Designator (CCPD)/Cryptographic Period Designator (CPD). The initialization parameter referred to as the CCPD governs and standardizes which locations are in use on a given day. The CCPD was zero on 1 January 1985 and alternates between zero and one IAW Table 4. Within the terminal initialization load parameters, each of the terminal SDU locations has a CPD associated with it. The terminal will use only the location in which the CPD agrees with the CCPD. The even-numbered locations have the same CPD and the odd-numbered locations have the opposite CPD. It is important that the terminal operator provide the terminal with information required to establish the correct CCPD. Some system installations require the CCPD to be entered manually from the operator's console. Other systems may require only that the correct date (day, month, and year) be maintained by or entered into the system. A standardized CPD initialization ensures interoperability among universally distributed JNL networks. When loaded into the Link 16 system, the same default CPD is set by the initialization data. The current CPD for the network initialization data load must be modified immediately prior to or after KEYMAT loading or reloading.

(4) Key Loading. To ensure that the terminal has the correct CCPD, personnel must ensure that keys are loaded into memory locations that match the CPD assigned by the terminal initialization parameters. The fill device UAS manages this function for DS-101 SDUs. For DS-102 protocol key loading, the user must manually set the appropriate switches on the terminal or KCP to

select the appropriate SDU RAM storage location to match the automated assignment being made by the fill device UAS. The appropriate location information is obtained from the applicable OPTASKLINK message and the crypto period determination table (Table 4). For Link 16 terminals using a DS-102 type SDU, indications for success of a key load are displayed on the KCP or LCU immediately after each key segment is loaded. For DS-101 SDUs, the fill device will display the status of the key load after the load has been completed. The fill device also records this information in the key load status log. This log can be reviewed or reset at the fill device or uploaded to a PC for storage or printing.

CCPD Table Non-Leap Years				CCPD Table Leap Years							
2013,2015,2018, 2021,2023,2026, 2029,2031,2034, 2037,2039,2042, 2045,2047,2050, 2053,2055,2058, 2061,2063,2066, 2069,2071,2074, 2077,2079,2082, 2085,2087,2090, 2093,2095,2098		2011,2014,2017, 2019,2022,2025, 2027,2030,2033, 2035,2038,2041, 2043,2046,2049, 2051,2054,2057, 2059,2062,2065, 2067,2070,2073, 2075,2078,2081, 2083,2086,2089, 2091,2094,2097, 2099		2016,2024,2032, 2040,2048,2056, 2064,2072,2080, 2088,2096		2012,2020,2028, 2036,2044,2052, 2060,2068,2076, 2084,2092,2100					
Month	Day is...		Month	Day is...		Month	Day is...		Month	Day is...	
	Odd	Even		Odd	Even		Odd	Even		Odd	Even
JAN	1	0	JAN	0	1	JAN	0	1	JAN	1	0
FEB	0	1	FEB	1	0	FEB	1	0	FEB	0	1
MAR	0	1	MAR	1	0	MAR	0	1	MAR	1	0
APR	1	0	APR	0	1	APR	1	0	APR	0	1
MAY	1	0	MAY	0	1	MAY	1	0	MAY	0	1
JUN	0	1	JUN	1	0	JUN	0	1	JUN	1	0
JUL	0	1	JUL	1	0	JUL	0	1	JUL	1	0
AUG	1	0	AUG	0	1	AUG	1	0	AUG	0	1
SEP	0	1	SEP	1	0	SEP	0	1	SEP	1	0
OCT	0	1	OCT	1	0	OCT	0	1	OCT	1	0
NOV	1	0	NOV	0	1	NOV	1	0	NOV	0	1
DEC	1	0	DEC	0	1	DEC	1	0	DEC	0	1

Table 4. Crypto Period Determination Table

9 December 2011

(5) Programmable COMSEC System Key Loading. Some programmable COMSEC systems such as MIDS JTRS and F-22A do not use a location to store keys. These systems use internal key management functionality to select the proper key for the date and the NPG/Cryptologic Variable Logic Label (CVLL). Keys are loaded into these systems by the fill device along with the necessary information for the systems to properly select the keys for use. That information is provided to the fill device by a data management system such as DMD. The SKL is currently the only fill device that can support key loading for these programmable COMSEC systems

2. EKMS

a. Description. The EKMS is a key management, COMSEC material distribution and logistics support system consisting of interoperable Service and Defense agency key management systems. NSA established EKMS to meet multiple objectives, including supplying an electronic key to COMSEC devices in a secure and timely manner and providing COMSEC account managers with an automated system capable of ordering, generating, producing, distributing, storing, securing, accounting, and controlling access. Other EKMS features include automated auditing capabilities to monitor and record security-relevant events, account registration, and extensive system and operator privilege management techniques to provide flexible access control to sensitive key, data, and functions within the system. Common EKMS components and standards will facilitate interoperability and commonality among the Services.

b. Purpose. The goal of EKMS implementation is to reduce the potential for KEYMAT exploitation by reducing human access to KEYMAT during distribution.

c. Functional Description. EKMS consists of the four tiers described below.

(1) Tier 0. The National Security Agency Central Facilities (NSACF) provides a broad range of capabilities to the Department of Defense and other government agencies. These facilities comprise the EKMS Tier 0 and include the facilities located at Fort Meade (CFFM) and Finksburg (CFFB), Maryland. CFFM will continue to produce the modern (FIREFLY and other electronic short titles) key.

(a) NSACF Functions

1. Seed conversion and rekey.
2. Compromise recovery and management of certain key material.

3. Physical and electronic key order processing.
4. Electronic key generation and distribution.
5. Conversion of the existing key to EKMS (ensuring backward compatibility is retained).

(b) Communications. The NSACF communicates with other EKMS elements through a variety of media, communication devices, and networks including direct distance protected data communication access (STE) or dedicated link access (Omni, Omega, and KG-84/KIV-7HS). Direct communication between tiers is always available. During transition to the full electronic key the 3.5-inch floppy disk will be supported. Once fully operational, a TCP/IP-based message server will be the primary means of communication with the NSACF. This service will permit EKMS elements to store messages that include the electronic key for later retrieval by other elements.

(2) Tier 1. Each Service maintains a central office of record (COR) that performs basic key and COMSEC management functions, including key ordering, distribution, and inventory control. The EKMS Common Tier 1 serves as the distribution point for the Service CORs.

(3) Tier 2. Tier 2 comprises the local account holders at user activities and consists of a Service- or agency-supplied local management device (LMD) and an NSA-supplied key processor (KP). The LMD is a Service- or agency-supplied commercial off-the-shelf PC. NSA-supplied local communications security management software (LCMS) was developed to replace Service-unique automated software. LCMS is the cryptographic engine providing COMSEC account managers with the capability to electronically generate the local COMSEC key; order COMSEC material; distribute, inventory, and destroy KEYMAT; and perform other COMSEC management functions. The CUAS has been developed to provide key management for newer COMSEC equipment and weapons systems and may serve as the operator interface for LCMS.

(a) Software. LCMS provides the interface between the LMD and the KP and tools for COMSEC management. Specialized application programs have been developed by several departments and agencies that overlay the LCMS and provide tailored human-machine interface.

(b) Platform. The LMD operates the Santa Cruz Operations (SCO 5.0) operating system and hosts LCMS. When the LMD and KP are used together, the account custodian/manager is able to order and account for all forms of COMSEC key material, store the key in encrypted form, perform key generation and automatic key distribution, perform COMSEC material accounting functions, and communicate directly with other EKMS elements.

(c) KP. The KP performs cryptographic functions, including encryption and decryption, key generation, and electronic signature operations. The KP is capable of secure field generation of a traditional key. A locally generated key can be employed in cryptonet communications, TRANSEC applications, point-to-point circuits, and virtually anywhere that paper-based keys are used today. Electronic keys can be downloaded directly to a fill device for further transfer or fill to the ECU.

(4) Tier 3 AN/CYZ-10 DTD. The AN/CYZ-10 DTD is an NSA-developed, portable handheld device capable of securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. This DTD is capable of storing 1,000 symmetric keys, maintains an automatic internal audit trail of all security-relevant events that can be uploaded to the LMD/KP, encrypts the key for storage, and is programmable. The DTD, SDS, and SKL devices are capable of replacing members of the family of common fill devices (CFD): KYK-13, KYX-15, and KOI-18. The fill device is capable of keying multiple COMSEC devices and is compatible with such COMSEC equipment as single-channel ground and airborne radio system radios, VINSON, KG-84, and others that are keyed by CFDs. The fill device is designed to be fully compatible with future COMSEC equipment meeting DS-101 and benign fill standards.

(a) Tier 3 AN/PYQ-10(C) SKL. The SKL has been designed around the concept of the personal digital assistant devices that are used today by the general public. The SKL is backward compatible with existing ECUs and forward compatible with future equipment. The SKL is a handheld digital computer running a Windows CE.Net operating system hosting the core library and SKL UAS programs that interface with the LCMS workstations, DMD software, and ECUs on the battlefield. The SKL provides for the receipt, display, transmission, preparation, storage, and accountability of key material and signal operating instructions information. The SKL has been ruggedized to withstand battlefield conditions. The SKL is a controlled cryptographic item (CCI) because of the KOV-21 information security card imbedded in it. When classified database information resides in the SKL, the SKL takes on the classification of the data.

(b) Tier 3 KIK-20 SDS. The SDS is a portable handheld device capable of securely receiving, storing, and transferring electronic data between compatible communications equipment. SDS provides the same functionality as and is backwards compatible with the CT3 UAS that resides in the AN/CYZ-10 DTD.

d. EKMS Key Distribution. Paper tape key distribution will be available to users that do not have electronic distribution capability. The connection between Tier 2 and Tier 3 can be remote using various secure communication

systems. The key may be loaded into the fill device directly by connecting the fill device to the LMD or KP, remotely by loading the key into a local fill device and then transferring the keys and database to another fill device via secure communication connection to a remote site, and remotely by loading the key into a local fill device and then sending the keys to a remote site via the secure transfer where the key is collected in a remote fill device at the user site.

e. EKMS Key Request Process. Much of the TEK will still be generated at Tier 0 due to the requirement for some paper key output and the need to distribute the key to allies. TEK for U.S. ONLY exercises may be generated at Tier 1. ECU encrypted key is encrypted at Tier 2 using locally available KP.

3. EKMS Key Ordering Parameters

a. Parameters. The following subparagraphs describe typical parameters for ordering operational keys. It is expected that each command would order its own keys. Table 5 describes the keys that each command may desire to order.

	Worldwide Emergency	Joint Theater	Allied
USEUCOM	Note 1	Note 2	Note 9
USPACOM	Note 1	Note 3	Note 10
USCENTCOM	Note 1	Note 4	Note 11
USSOUTHCOM	Note 1	Note 5	Note 12
NORAD	Note 1	Note 6	Note 13
USNORTHCOM	Note 1	Note 7	Note 14
DHS	Note 1	Note 8	Note 15

- Note 1: Allied key is to be ordered by the CONAUTH designated by JCMO.
- Note 2: U.S. keys to be ordered by the CONAUTH designated by USEUCOM.
- Note 3: U.S. keys to be ordered by the CONAUTH designated by USPACOM.
- Note 4: U.S. keys to be ordered by the CONAUTH designated by USCENTCOM.
- Note 5: U.S. keys to be ordered by the CONAUTH designated by USSOUTHCOM.
- Note 6: Allied keys to be ordered by the CONAUTH designated by NORAD.
- Note 7: Allied keys to be ordered by the CONAUTH designated by USNORTHCOM.
- Note 8: Allied keys to be ordered by the CONAUTH designated by DHS.
- Note 9: Allied keys to be ordered by the CONAUTH designated by USEUCOM.
- Note 10: Allied keys to be ordered by the CONAUTH designated by USPACOM.
- Note 11: Allied keys to be ordered by the CONAUTH designated by USCENTCOM.
- Note 12: Allied keys to be ordered by the CONAUTH designated by USSOUTHCOM.
- Note 13: Allied keys to be ordered by the CONAUTH designated by NORAD.
- Note 14: Allied keys to be ordered by the CONAUTH designated by USNORTHCOM.
- Note 15: Allied keys to be ordered by the CONAUTH designated by DHS.

Table 5. Operational Link 16 Key Allocation

(1) Equipment Type. Although Link 16 uses a variety of SDUs based on the THORNTON cryptographic family, EKMS recognizes only the KGV-8B and the KGV-8. Since both of these devices use the same TEK type, KGV-8 has been established as the standard equipment type for ordering a key. Equipment differences are selected in the LMD Common User Application

Software (CUAS) or the fill device software or downloaded from the DMD or ACES software into the fill device.

(2) Desired Order Type. The desired order type cues EKMS to create the short title.

(3) EKMS ID. Only Tier 0 can meet the requirements for generating allied and paper keys; therefore, the EKMS ID for key generation will normally be 880091 (NSACF). If the key is generated locally or by a Tier 1 entity, the appropriate EKMS ID shall be used.

(4) Key Use. The only key of interest for the joint community is the TEK. OTAR KEK, TrKEK, and ECU KEK that are generated by the Services or locally are not discussed here.

(5) Key Purpose. Typically, this field will be "Operational." Other types of keys (training, test, or maintenance) may be ordered as needed by using the parameters of this enclosure.

(6) Handling Restrictions. Keys are to be handled IAW EKMS doctrine.

(7) Net Size. Cryptographic nets should be as small as operationally practical.

(8) Cryptoperiod. Except when using time offset to operate independent networks, Link 16 KEYMAT for a daily key has a cryptographic period beginning exactly 1 minute before 0001 UTC and ending exactly 1 minute after 2359 UTC.

(9) Segments/Edition. Daily keys are designed around the concept that the segment number and day of the month are the same. Thirty-one segments per edition are used to reflect this correspondence.

(10) Accounting Legend Code (ALC). Since the operational key is reportable to the COR, the ALC number is ALC-6. Locally accountable training, test, or maintenance keys are designated ALC-7.

(11) Classification. Any key used for Link 16 operations must be at least SECRET. Maintenance keys may be UNCLASSIFIED For Official Use Only.

(12) Supersession Rate. Link 16 keys are subject to monthly supersession.

(13) Distribution Control. An entry of "Implicit" indicates that the key may be copied IAW the directions of the CONAUTH. The CONAUTH must add

9 December 2011

any new accounts to the distribution profile (see subparagraph 3a(20)) to ensure that the account's ROB is adequately supported by the Tier 0 key generating account. For nonoperational keys with no standing order, copies may be adequate.

(14) Auth ID. [List all CONAUTHs.] This would be the combatant command or JCMO ID for the operational key. The nonoperational key may specify a different CONAUTH.

(15) Release. [Restrictions on release.] For example, NOFORN, USA/CAN/GBR ONLY.

(16) In-Place Date. This is the date the user requests for KEYMAT delivery.

(17) Effective Date. [Date the first key segment is effective.] No entry is currently required. The CONAUTH can establish this at a later time.

(18) Standing Order. This field indicates whether the key will be produced on a continuing basis to meet the ROB requirement of all receiving accounts.

(19) Edition Info. This is the number of editions to be generated at one time. One edition is generally adequate. The maximum ROB of all the accounts to receive the key will dictate the actual number of editions produced. If there is no standing order for the key, the ordering agent must determine the number of editions to be generated as a one-time production.

(20) Distribution Profile. [List intended recipient(s) EKMS ID(s).] At least one account must be provided. The CONAUTH may add additional accounts as needed.

(21) [NATIONALITY]. This field indicates whether the key is U.S. or allied. Although "NATIONALITY" is included here as a placeholder, the title of this field is currently undetermined.

b. Examples of Typical Parameters

- (1) Equipment Type: KGV-8
- (2) Desired Order Type: Assign
- (3) EKMS ID: 880091 (EKMS ID of the generating element; Tier 0)
- (4) Key Use: TEK

- (5) Key Purpose: Operational
- (6) Handling Restrictions: No restrictions
- (7) Net Size: 40
- (8) Cryptoperiod: Daily
- (9) Segments/Edition: 31
- (10) ALC: ALC-6
- (11) Classification: SECRET
- (12) Supersession Rate: Monthly
- (13) Distribution Control: Implicit
- (14) Auth ID: (combatant command (COCOM) or JCMO ID)
- (15) Release: (NOFORN, USA/CAN/GBR, U.S. ONLY)
- (16) In-Place Date: (Date the key is required to be in place at the destination; when ordering the joint operational key, date must match the Defense Courier Service delivery date.)
- (17) Effective Date: (Date the first key segment is effective.)
- (18) Standing Order: Y
- (19) Edition Info: 1
- (20) Distribution Profile: (combatant command or JCMO ID)
- (21) U.S. or Allied (See Table 5.)

c. Joint Operational Keys. Short titles for the keys described in Table 5 are dynamic, and not currently available; they will be provided in future revisions of this manual as they are developed. The baseline CONAUTH responsibilities are described in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4006, "Controlling Authorities of COMSEC Material." CONAUTH responsibilities are detailed in the corresponding Service manual of the supported Service.

4. Key Management Infrastructure (KMI). Link 16 does not currently support KMI.

5. OTAR Management

a. Description. OTAR is the rekeying of remote sites via the Link 16 communication system. Although the Link 16 system does not have OTAT capability since keys are not extractable, the system has the capability to rekey remote Link 16 equipment. The basic requirement for OTAR is the installation of an OTAR KEK in the Link 16 equipment and transmission of J31.0 and J31.1 messages to the terminal. J31.1 contains the rekey phrase and J31.0 contains supporting data for rekey. Programmable COMSEC Link 16 systems do not support OTAR. The capability will be added, in the future, as part of the NSA crypto modernization initiative.

b. Purpose. OTAR requirements include providing rapid compromise recovery, enforcing need-to-know data distribution, extending the number of cryptonets that can be serviced, reducing exposure of critical data, and rekeying Link 16 units that are difficult to physically access. OTAR is not a preferred standard operating procedure due to the requirements for a unique key at each receiving terminal. Since OTAR KEK is not retained during power down, OTAR cannot support recovery from a power interrupt.

c. Required Elements

(1) TRANSEC/KOK-13. The KOK-13 is an NSA-developed cryptographic peripheral used to support local key generation and OTAR and may be used to generate OTAR KEK. KOK-13 control is performed over an Institute of Electrical and Electronics Engineers (IEEE) 488 interface by the network control processor. It requires a key production key (KPK) to deterministically generate OTAR KEKs and TEKs. The KOK-13 "seed" keys are accountable within the EKMS system and currently distributed as paper keys loaded with the KOI-18.

(2) System Controller (SC). Normally embedded in or interfaced to the Link 16 host combat system, the SC maintains a record of station identification numbers and their unique OTAR KEKs and maintains a record of which Cryptographic Variable Logic Label (CVLL) is associated with which memory location. The SC also tracks which keys are currently installed in each Link 16 terminal and which keys have received a rekey command for a specified time. Finally, the SC provides synchronization information for use by the KOK-13. A human operator is responsible for knowing which keys to send and directs most SC functions. The SC must also have the capability to send a special non-communicating key to each location to recover from compromise.

(3) OTAR KEK. OTAR KEK must be loaded in the receiving Link 16 terminal SDU RAM location 5, and the terminal must be set to expect OTAR messages. OTAR KEK has a monthly cryptographic period and is unique for each terminal.

(4) Rekey Messages. The J31.1 provides the terminal rekey phrase and the J31.0 provides synchronization and other supporting OTAR information.

d. Procedures

(1) Generate OTAR KEK. OTAR KEK may be generated by the KOK-13 (locally), EKMS, or NSA. Each recipient Link 16 terminal is required to have a unique OTAR KEK to perform OTAR, although NSA may waive this requirement under special circumstances. The SC directs the KOK-13 to encrypt the TEKs and create the rekey phrase. The KOK-13 is instructed to send the rekey phrase back to the SC, which then determines the time and properly inserts the rekey phrase into J31.0 and J31.1 messages.

(2) Load OTAR KEK. EKMS-generated OTAR KEKs must be loaded into the KOK-13 to create the rekey phrases. KOK-13-generated OTAR KEKs are retained by the KOK-13 and issued to a fill device to be loaded into the appropriate Link 16 SDUs. The association between each terminal's unique ID and unique OTAR KEK is established and recorded by the SC.

(3) Prepare the Receiving Terminal. Each recipient Link 16 terminal must be initialized with the OTAR activation bit set to ON.

(4) Transmit the Rekey Instructions. J31.1 and J31.0 messages are transmitted from a host combat system equipped with SC functionality. For cases in which a KOK-13 is being used, transmitted TEKs must either be produced by the KOK-13 or have been received via the fill port.

(5) Receive the Rekey Instructions. When the terminal receives the J31.0 and J31.1 messages addressed to its unique ID, it acknowledges receipt and extracts the time at which the OTAR is to be accomplished. At the specified time, the terminal extracts the rekey phrase from the J31.1 message and the synchronization bits from J31.0 and transfers the key to the appropriate SDU RAM location. The SDU CVLL is updated to a new memory table from the data in the J31.0 message, and the terminal transmits a "HAVCO" message to indicate a successful rekey ("CANTPRO" is transmitted if the rekey fails for any reason). Note that since the Link 16 SDU will not change the key in any crypto variable location until it has successfully decrypted a received rekey phrase, caution should be exercised to ensure that terminals have received rekey phrases before a network reconfiguration is initiated. Failure to verify successful rekey could result in exclusion of the affected terminal from the reconfigured network.

e. Other Considerations

(1) TEK Extraction. TEKs that are accounted for by the EKMS and have been issued to a KOK-13 may not be extracted from the KOK-13 into a fill device.

(2) TEK Redistribution. KOK-13-generated TEKs may be issued to a Tier 3 fill device for further distribution.

(3) OTAR KEK Redistribution. KOK-13-generated OTAR KEKs may be issued to a Tier 3 fill device for further distribution.

(4) OTAR KEK Locations. If OTAR use is anticipated, the number of short titles in continuous use that may be loaded at one time into a Link 16 SDU is reduced from four to three. Location 5 is used for the OTAR KEK. Location 4 is not used or is used as a scratch pad. Technically, the locations 0, 1, 2, 3, 6, and 7 could all be used independently but would require complex coordination to ensure that participating units transition together at cryptographic period rollover.

(5) KPK. The KPK needs greater protection than the other keys. In many cases the KPKs are classified as TOP SECRET CRYPTO and must be handled according to doctrine for TOP SECRET keys.

(6) KOK-13 Transfer. TEKs provided or accounted for by EKMS are allowed to be issued to a KOK-13 for encryption and OTAR distribution. Most fill devices are capable of issuing a standard key to the KOK-13.

(7) KOK-13-Generated OTAR KEK. Although the KOK-13 may be used to generate OTAR KEK, this function should be used only in highly localized networks where multiplatform coordination is not required. EKMS should be used to generate OTAR KEK in all other circumstances.

(8) Terminal Loading. Note that since each Link 16 terminal can hold only one key for future use at a time, the SC operator should not allow keys to be sent to a terminal if a key is already in memory waiting to be loaded.

(9) KOK-13 Key Redistribution. Although keys produced by the KOK-13 can be used in Link 16 equipment for data encryption, the KOK-13 key should not be distributed through EKMS since it is not accountable for these keys. Tier 3 fill devices may be used to receive keys from the KOK-13 and fill equipment (the CT3 is designed to do this).

(10) KOK-13 as a Key Storage Device. The KOK-13 shall not be used as a key depository for EKMS accountable keys. EKMS accountable keys issued to the KOK-13 are for encryption and OTAR distribution only.

6. Joint Key Management Plan Procedures

a. Introduction. The following subparagraphs establish key management responsibilities for various DOD entities.

b. Responsibilities

(1) Combatant Commanders. Combatant Commanders will:

(a) Provide network design criteria to their Service Network Design Facilities (NDFs) to include COMSEC key structure. These criteria will be in the form of specifying details such as cryptonet requirements, CVM or PVM, or OTAR usage. Additionally, prior to implementation of OTAR in operational units design, coordination with Service NDFs is required to engineer certain network file changes for participating platforms.

(b) Prepare and distribute OPTASKLINK message preparation guidance and specific key management instructions to include current CPD assignments to allow rollover in a common direction.

(c) Notify CONAUTHs of joint theater key requirements.

(d) Implement standing orders and/or dynamic ordering procedures to support anticipated robust network structures.

(e) Order short titles for joint and combined in-theater requirements.

(f) Anticipate and fund C-EKMS requirements to enable electronic key distribution to coalition partners.

(g) Coordinate with Service acquisition agencies, Coalition partners, and U.S. country teams on U.S. requirement for U.S. COMSEC custodians to transition to C-EKMS and the need for FMS account to fund this transition.

(2) NDFs. Service NDFs develop networks for operations, tests, exercises, experiments, and training. Cryptonets must include only the participants that have a need to see data protected by the network. This is managed by maintaining the sequential pairing of SDU locations 0-1, 2-3, 4-5, and 6-7 with single CVLLs.

(3) EKMS Managers/COMSEC Account Managers (CAMs)/COMSEC Custodians

(a) Normal Functions. Each Service has instructions concerning the CAM's duties, including the requirement to maintain a COMSEC inventory and ROB adequate to support the command operational mission. Each Service is responsible for ordering short titles for intra-Service operations and testing.

(b) EKMS Support. EKMS levies additional responsibilities on the CAM. In addition to the EKMS functions, there are Service-specific UAS programs on the Tier 2 LMD used to support the CT3 system on the fill device. The CAM will need to operate the CUAS to support the Link 16 system. In some cases, the CAM will be responsible for loading all platform and equipment data as well as loading the keys into the fill device. The CUAS on the LMD/KP will support Link 16 operations and other cryptographic material by providing the COMSEC Account Manager with a method of identifying and creating all the management information required by the fill device. The CUAS is capable of requesting key and key encryption with an ECU KEK and providing that information to a DMD or a fill device. The CUAS is also capable of requesting a key and encrypting in a specified fill device TrKEK for key transfer when the ECU must receive an unencrypted key. If the user has a workstation and software, the user may provide all data on a floppy disk or on a paper sheet. In that case, the COMSEC account manager needs only to assist in loading the fill device or ECU KEKs and operate CUAS on the LMD/KP to provide the data and encrypted keys on a floppy or download this information into the fill device. The user on a workstation or DMD has the responsibility of ensuring the correct assignments of the keys to the memory locations.

(c) Audit Log Maintenance. Maintenance of the audit log is directed by Service instructions and will be followed by users. The local commander is responsible for implementing the procedures and doctrine specified for the fill device as developed by the various Services. The COMSEC Account Manager is responsible for ensuring that proper procedures are carried out regarding uploading, viewing, and resetting of the fill device audit log. Additionally, the COMSEC Account Manager is responsible for instructing the user in the user's responsibilities.

(4) Users

(a) Loading Keys. The user is responsible for loading the correct keys for the mission into the SDU. The fill device will assist the user in the selection of the correct segments for key loading.

(b) Zeroizing Equipment. All Link 16 SDUs, including the programmable COMSEC systems, will zeroize TEK upon removal of power. Link 16 terminal operators must zeroize the SDU if the unit is likely to fall into

enemy hands. Some aircraft provide a switch that will zeroize all equipment including Link 16, while in some systems the operator of the host system must send an initiate command to zeroize the Link 16 equipment. The fill device can also be used to zeroize the TEK keys and is the only way to zeroize the ECU KEK keys. During normal operation, the ECU KEKs need to be zeroized only if the SDU is to be stored for more than a month or shipped through commercial shipping.

(c) Monitoring Alarms. The SDU alarm sensors monitor internal operations and perform self-tests on the alarm circuitry. Alarm conditions can be caused by loss of power sources, invalid key transfers to the SDU, time slot number errors, and physical parts within the SDU. If an alarm condition occurs, it is reported to the host terminal. The SDU then performs a series of internal checks and attempts to restore the keys in use. If the internal test failures persist, the SDU will not operate. It is the user's responsibility, upon observing an alarm condition, to evaluate the condition, determine what action is necessary to ensure security of the communication data, and take corrective action where appropriate. SDUs for which alarms cannot be removed should be evaluated for repair. The terminal CRYPTO HOLD battery, not the SDU, causes the most common problems. Proper terminal battery care will minimize the occurrence of SDU alarms.

(d) Maintaining Audit Log. Service instructions establish requirements and procedures for audit log maintenance. At their discretion, local commanders may provide additional guidance to the COMSEC account manager. Users are responsible for complying with all applicable guidance.

(e) Preparing Data for the Fill Device. The software in the fill device requires that platform and equipment data be loaded into the fill device in addition to the key. The user will be required to either manually enter this platform and equipment data or retrieve the data from a workstation. An operator can create the platform and equipment information by using the ACES system or the DMD. If the CUAS provides the encrypted key to the ACES or DMD, it can also assign the key to the appropriate ECU.

(f) Monitoring Cryptographic Material Access. Access control for KEYMAT and COMSEC equipment is defined in the applicable COMSEC and EKMS doctrine for each Service. Normally, when the SDU has a KEK installed, the equipment is handled as CCI containing COMSEC data classified to the level of the KEK. NSA has specific restrictions on the SDU with a KEK loaded when the KEK is not in use and is stored for a month or more or is to be transported to another location. Every effort should be made to zeroize KEKs prior to storage or shipment. If this is not possible, the equipment is to be treated as an item at the classification level of the KEK. Since the KEK cannot be extracted, however, it shall not be marked "CRYPTO." Link 16 terminals are considered high-value items. Protection afforded to the Link 16 terminal is

adequate for the SDU that is associated with it. No special clearance is required to observe filling of any Link 16 SDU by an electronic fill device. Access to a fill device, which is also a CCI device, is covered in each Service EKMS or COMSEC doctrine. Viewing of a fill device or fill process, by personnel without COMSEC training or user status is permitted, except when loading a key marked "CRYPTO" in paper form.

(g) Monitoring Link 16 System Access. Since the keys are not extractable from the SDU, personnel possessing clearances to the level of the traffic transmitted or received are permitted access to the areas operating a Link 16 terminal. CMS user status is not required unless the key is exposed. Anyone may observe the Link 16 equipment with or without the SDU being visible. Link 16 SDUs for all operational units are CCIs and should be handled IAW current CCI doctrine. The MIDS-LVT family and the JTIDS Class 2 terminals with CSP are considered CCIs. Special handling doctrine should be utilized to accommodate the large equipment.

(h) Accounting. Link 16 key accounting is accomplished via the EKMS accounting system and will comply with Service COMSEC doctrine and EKMS UAS capabilities.

c. Key Generation

(1) EKMS TEK. Joint TEK will normally be generated at EKMS Tier 0 or Tier 1. TEK may be generated at the Tier 2 level in special circumstances. Each Service may have the keys used for their operations generated at EKMS Tier 0, 1, or 2 levels.

(2) EKMS ECU KEK. When ECU KEKs are required, they should be generated at the lowest level with facilities to support distribution (normally Tier 2). Common KEKs are required for locations in which there is shared fill device usage, even if it is only for emergency backup. For example, all elements of a USN battle group will have the same ECU KEKs, allowing any fill device with Link 16 ECU encrypted keys to load any Link 16 SDU.

(3) EKMS Fill Device KEK. Fill device KEKs are part of the EKMS concept of operations. There is often only one fill device KEK per COMSEC account; however, the number of fill device KEKs is dictated by Service guidance, local SOP, and the operational mission.

d. Key Distribution. Table 6 details the nominal operational requirements for a key to support a combined task force. Short titles listed are only examples. At a minimum, two coalition-releasable and two U.S.-only cryptographic short titles are required. The number of short titles that may be loaded at one time is reduced from four to three if OTAR is anticipated, except for programmable COMSEC systems. The contingency key is included to

9 December 2011

support emergent COMSEC interoperability requirements. Each Service is responsible for ordering short titles for intra-Service operations and testing.

Link 16 Key Type	Users	Purpose
TRANSEC	All Users	Network Synchronization
MSEC ¹	All Users	Coalition Tactical Data
MSEC	All U.S. Forces Users	U.S. Force Tactical Data
MSEC	Specified U.S. Forces Users	U.S. Air-to-Air
MSEC	Specified Coalition Users	Coalition Air-to-Air
TRANSEC or MSEC	All Users	Emergency Contingency

¹ One short title may be used to satisfy common TRANSEC and MSEC requirements.

Table 6. Nominal Combined Force COMSEC Requirements

(1) Requesting Key. The required key must be requested by the EKMS Tier 2 COMSEC account supporting the user from the EKMS Tier 0 or Tier 1 facilities. To minimize risk of compromise and vulnerability to exploitation, ECU encrypted keys, both TEK and KEK, shall be used wherever feasible.

(2) USMC Key Management. USMC Link 16 terminals use unencrypted TEKs and KEKs in electronic form. To request keys, the COMSEC Manager, per EKMS 1B, will submit a Modification of Allowance through his chain of command to the appropriate Marine Forces Command. The Controlling Authority (CONAUTH) will be courtesy copied on a final endorsed message generated by NSA and then transferred electronically to user accounts by the NSA-managed National Distribution Authority. Encrypted TEKs are loaded into fill devices using black key management support software. Local COMSEC account managers submit key requests through the responsible CONAUTH.

(3) Receiving Key

(a) ECU KEK. Tier 2 distribution points may receive ECU KEK from Tier 1 or generate KEK for distribution to their user accounts. User COMSEC accounts may receive Link 16 KEK in their Tier 2 LMD/KP directly from Tier 1 or from their serving EKMS Tier 2 distribution point for further issue to a fill device for loading into an ECU.

(b) TEK. User COMSEC accounts may receive TEK in their Tier 2 LMD/KPs from either Tier 1 or Tier 0 or their serving EKMS Tier 2 distribution point. TEKs may be encrypted at Tier 2 using a KEK obtained from a Tier 1 facility (or generated locally) upon request from a Tier 2 UAS (e.g., CUAS) and the resulting encrypted TEK distributed by the Tier 2 UAS to fill device.

e. Key Storage

(1) SDU. All JTIDS SDUs are capable of storing eight unencrypted keys in RAM. The CDH can store 64 keys in RAM. The KGV-8B and CDH can store

KEK in any of nine EEPROM locations. Programmable COMSEC systems can store 1000, or more, keys of all types. All keys stored in the SDU are non-extractable.

(a) RAM Storage. In an SDU with eight or more key storage locations, the convention described in Table 7 will normally apply, although changes may be made according to operational requirements. The network selected for terminal initialization controls the actual locations used. Once a network has been selected (or constructed by an NDF based on operational requirements), the locations and the use of those locations are fixed by that network. Short titles are promulgated in the OPTASKLINK based on the usage defined in the Network Description Document COMSEC Cross-Reference Table. Planners use this table to determine the number of CVLLs and, thus, the number of separate keys required to operate the network as well as the SDU loading locations for each key.

Storage Locations	0-1	2-3	4-5	6-7
Network Defined Key Use	Normal Operational Key in CVM or TRANSEC in PVM	1st MSEC	OTAR or 2d MSEC	Allied Key or 3d MSEC if required

Table 7. Crypto Storage Location Guidance

(b) EEPROM Storage. Although the KGV-8B and CDH are capable of storing TEK in EEPROM, the ability to later use these TEKs requires fill device capabilities for which no software currently exists. Access to these devices would also be affected if TEKs were stored in the EEPROM. A detailed plan and formal request for authorization from NSA is required prior to use of EEPROM for TEK storage. Additionally, EKMS UAS must be modified to accommodate EEPROM TEK loading. If a Service requires this capability, an engineering change proposal must be submitted to the applicable software support activity for the requesting fill device UAS.

(2) LMD. The LMD stores only encrypted keys. The KP must first encrypt the unencrypted key before it is stored in encrypted form on the LMD hard drive.

(3) Fill devices. The fill devices can store at least 1,000 unencrypted TEKs and their associated key tags. ECU encrypted keys are larger than unencrypted keys; consequently, fewer encrypted keys can be stored. They can be secured by removing the crypto ignition key (CIK) from the device. Stored keys can be selectively deleted or zeroized. The fill device must be zeroized to remove all keys and downgrade the fill device UNCLASSIFIED CCI.

9 December 2011

f. Key Loading. For the KGV-8, KGV-8B, and CDH, TEKs shall be loaded into the SDU in adjacent pair RAM storage locations. Successive key segments shall be loaded into the SDU if operation is anticipated through a cryptographic period transition. If the terminal has been turned off, both the current day and next day TEK must be reloaded. Terminals using the KGV-8B must be loaded with the current and next day TEKs needed for the network configuration every time a key is loaded. Currently, key loading may be accomplished only through the fill port or OTAR. Single point keying (where several cryptographic devices using the DS-101 protocol can be keyed at the same time over a fill bus) has been implemented in some Link 16 platforms. A bus (STATION) address is used during DS-101 key loading to direct keys to the correct terminal SDU. The management of station addresses for bussed SDUs is the responsibility of each Service platform program office (e.g., NAVAIR PMA-265 for the F/A-18). EKMS supports single point keying.

g. Cryptoperiods

(1) KEK. The cryptoperiod for each Link 16 KEK is 1 calendar month commencing at the beginning of the minute defined by 010001 UTC.

(2) TEK. The cryptoperiod for each Link 16 TEK is 1 day and, except when using time offset to operate independent networks, commences at the beginning of the minute defined by 0001 UTC.

(3) CPD Initialization. As applicable, even-numbered RAM locations shall be initialized to the same CPD and the odd locations shall have the opposite CPD.

(4) Cryptoperiod Extension. The Link 16 design does not permit operator-initiated extension of the key cryptoperiod. The cryptographic period for Link 16 is 24 hours, normally commencing at the beginning of the minute defined by 0001 UTC. Explicit coordination and a joint Service agreement are required to use a 7-day cryptoperiod and will be addressed in a separate addendum to this plan when the engineering is accomplished to use this capability.

h. Compromise Procedures. COMSEC incidents are reported in accordance with NSTISSI 4003, "Reporting and Evaluating COMSEC Incidents," and its Service implementers.

(1) Unencrypted TEK Compromise. If an unencrypted TEK is compromised, the encrypted copy of the same TEK is also compromised. Compromise recovery strategy is to supersede the compromised TEK edition and use the next sequential TEK edition. If TEK recovery requires a KEK change, the appropriate KEK segment used to encrypt/decrypt the encrypted TEK must be superseded, and the next KEK segment shall be used.

(2) Encrypted Key Compromise. Loss of an encrypted TEK or encrypted KEK is not a compromise. A physically lost key shall be replaced with an identical key.

(3) Unencrypted KEK Compromise. If an unencrypted KEK is compromised, all keys encrypted with that KEK are also compromised. The recovery procedure for a compromised KEK **segment** is to supersede that segment and all editions of keys encrypted by that KEK and implement the next KEK segment and corresponding key edition encrypted by that KEK. The recovery procedure for a compromised KEK **edition** is to supersede all key editions encrypted by that KEK and implement the next KEK edition and corresponding key editions encrypted by that KEK. If no uncompromised KEK editions and associated encrypted keys are available, new KEKs and TEKs must be requested from the EKMS Tier 1 or Tier 2 facility.

i. OPTASKLINK. The formatted message for OPTASKLINK defined by MIL-STD-6040 is used to provide detailed instruction regarding the tactical data link operations. The OPTASKLINK contains COMSEC key identification, link operating frequencies, channelization, and initialization plans. The OPTASKLINK is used by terminal platforms to plan and conduct joint tactical communications for a designated period. Instructions for the preparation and loading of the COMSEC/CRYPTO keys required for link operation are included in the Link 16 portion. Each OPTASKLINK message contains network start times, which specify the effective period of operation for the tactical data links. The cryptographic data section of the OPTASKLINK message specifies unique COMSEC requirements. It relates COMSEC short titles to CVLL and indicates into which SDU storage location each short title should be loaded. It also provides the CCPD, advising Link 16 users whether to load keys into even or odd SDU locations. The CCPD is in accordance with Table 4.

ENCLOSURE B

LINK 16 COMSEC ENTITIES CONTACT LIST

Agency	Message Address	Web Address
SPAWARSYSCEN Pacific 58120 53560 Hull St San Diego, CA 92152-5001	SPAWARSYSCEN PACIFIC CA//58120//	https://Link16.navy.mil
Director, National Security Agency 9800 Savage Rd Ft. George G. Meade, MD 20755-6000	DIRNSA FT GEORGE G MEADE MD//1824/1541//	
ESC/HNC DK 304 North Frank Luke San Antonio, TX 78236-1851	DIR TIER 1// SAN ANTONIO TX//	
ESC/HNC DK 304 North Frank Luke San Antonio, TX 78236-1851	HQ CPSD SAN ANTONIO TX//NIX//	https://afekms.lackland.af.mil
Joint COMSEC Management Office 8532 Marina Bay Dr MacDill AFB, FL 33611	JCMO MACDILL AFB FL	http://vela.stratcom.smil.mil/restrict/jcmo
Naval COMSEC Material Systems, NAC 1560 Colorado Ave Camp Springs, MD 20707-6108	NCMS WASHINGTON DC// N3//	http://www.ncms.navy.mil
Joint Interoperability Test Command Ft. Huachuca, AZ 85635	CDRJITC FT HUACHUCA AZ//JTEB//	
U.S. ARMY CECOM LCMC CSLA 2133 Cushing St, STE 3600 Fort Huachuca, AZ 85613-7041	DIRUSACSLA FT HUACHUCA AZ//AMSEL- LCA-KEY	Tier 1-5A8240-COR@CONUS.ARMY.MIL
AFNIC/ECAP 203 W. Losey St Rm. 2200 Scott AFB, IL 62225-5222	HQ AFNIC SCOTT AFB IL//ECAP//	
USPACOM J63 Bldg. 700 Camp Smith, HI 96861-4029	HQ USPACOM HONOLULU HI//J63//	

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

ACES	Automated Communications Engineering Software
ALC	Accounting Legend Code
C2	Command and Control
C2P	Command and Control Processor
CAM	COMSEC Account Manager
CCI	Controlled Cryptographic Item
CCPD	Current Cryptographic Period Designator
CDH	Communications Security/Transmission Security Integrated Circuit Data Standard 101 Hybrid
CECOM	Communications-Electronics Command
C-EKMS	Coalition Electronic Key Management System
CFD	Common Fill Device
CFFB	Central Facility Finksburg
CFFM	Central Facility Fort Meade
CIK	Crypto Ignition Key
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMS	Communications Security Material System
COMSEC	Communications Security
CONAUTH	Controlling Authority
COR	Central Office of Record
CPD	Cryptographic Period Designator
CPSD	Cryptologic Systems Division (USAF)
Cryptonet	Cryptographic Network
CSLA	Communications Security Logistics Activity
CSP	Common Signal Processor
CT3	Common Tier 3
CUAS	Common User Application Software
CVLL	Cryptographic Variable Logic Label
CVM	Common Variable Mode
DHS	Department of Homeland Security
DMD	Data Management Device
DOD	Department of Defense
DS	Data Standard
DTD	Data Transfer Device
ECU	End Cryptographic Unit
EEPROM	Electronic Erasable Programmable Read-only Memory

EKMS	Electronic Key Management System
EMD	Engineering and Manufacturing Development
FDL	Fighter Data Link
FES	Front-end System
FOC	Full Operational Capability
HPA	High Power Amplifier
IEEE	Institute of Electrical and Electronics Engineers
IJMS	Interim Joint Tactical Information Distribution System Message Specification
JCMO	Joint Communications Security Management Office
JMPS	Joint Mission Planning System
JNL	Joint Tactical Information Distribution System Network Library
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
KCP	Keyer Control Panel
KDSUAS	Key Distribution Support User Application Software
KEK	Key Encryption Key
KEYMAT	Keying Material
KMGA	Key Management Goal Architecture
KMI	Key Management Infrastructure
KP	Key Processor
KPK	Key Production Key
LCMS	Local Communications Security Management Software
LCU	Load Control Unit
LMD	Local Management Device
LVT	Low-Volume Terminal
MHz	Megahertz
MIDS	Multifunctional Information Distribution System
MIL-STD	Military Standard
MROC	Minimum Required Operational Capability
msec	Millisecond
MSEC	Message Security
NATO	North Atlantic Treaty Organization
NCMS	Naval Communications Security Material Systems
NCS	National Command System

NDF	Network Design Facilities
nm	Nautical Mile
NORAD	North American Aerospace Defense Command
NPG	Network Participation Group
NSA	National Security Agency
NSACF	National Security Agency Central Facilities
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OPTASKLINK	Operations Task Link
OTAR	Over-the-Air Rekey
OTAT	Over-the-Air-Transfer
PC	Personal Computer
PPLI	Precise Participant Location and Identification
PVM	Partitioned Variable Mode
RAM	Random Access Memory
ROB	Reserve On Board
RTT	Round-Trip Timing
SC	System Controller
SDS	Secure Data Transfer Device 2000 System
SDU	Secure Data Unit
SKL	Simple Key Loader
SMP	Signal Message Processor
SSA	Software Support Activity
STE	Secure Telephone Equipment
STT	Small Tactical Terminal
TAMPS	Tactical Aircraft Mission Planning System
TCP/IP	Transmission Control Protocol/Internet Protocol
TCU	Transmission Security/Communications Security Unit
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
TRANSEC	Transmission Security
TrKEK	Transmission Key Encryption Key
TSK	Transmission Security Key
UAS	User Application Software
U.S.	United States
USA	U.S. Army
USAF	U.S. Air Force
USCENTCOM	U.S. Central Command

USEUCOM	U.S. European Command
USMC	U.S. Marine Corps
USN	U.S. Navy
USNORTHCOM	U.S. Northern Command
USPACOM	U.S. Pacific Command
USSOUTHCOM	U.S. Southern Command
UTC	Coordinated Universal Time
W	Watt

GLOSSARY

PART II -- DEFINITIONS

Allied. A term used within this document to refer to operations between or keys used by the United States and member nations of a treaty organization (i.e., NATO), coalition, or combined force.

BLACK Key. An encrypted key.

Common Signal Processor (CSP). A product of the Joint Tactical Information Distribution System Class II Terminal Embedded Crypto Card Product Improvement Program.

Common Tier 3 (CT3) software. Data transfer device software used to fill all operational crypto devices.

Common Variable Mode (CVM). The mode of operation in which the same key is used for traffic encryption/decryption and transmission security.

Controlled Cryptographic Item (CCI). Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements.

Controlling Authority (CONAUTH). The official responsible for directing the operation of a cryptonet and managing the operational use and control of keying material assigned to the cryptonet. In Link 16, the official responsible for the proper security and use of a COMSEC short title.

Coordinated Universal Time (UTC). A measure of time that conforms, within a close approximation, to the mean diurnal rotation of the Earth and serves as the basis of civil timekeeping. Used to establish the valid cryptographic interval for Link 16 keying material.

Cryptographic Network (cryptonet). A collection of operational units whose data is being protected from all others by the encryption process provided from a single crypto key. Link 16 can operate with multiple cryptonets simultaneously. Note that multiple network participation groups can be operating in the same cryptonets.

Cryptographic Variable Logic Label (CVLL). The tie between short titles and network design. Also, the tie between secure data unit memory locations and network design.

Current Cryptographic Period Designator (CCPD). A one-bit parameter used to determine what set of keys is in use on a particular day. See Table 4.

Data Management Device (DMD). A USAF software package that runs on a PC or Palm top that creates the management information for the Common Tier 3. It also will interface with the KOV-21 to act as a fill device. The DMD will operate with or without the KOV-21.

Data Transfer Device (DTD). The common name for AN/CYZ-10.

Data Transfer Device Encrypted Key. Key data that results from a key being encrypted in a transmission key encryption key.

DS-101. The Electronic Key Management System standard for electronic key transfer.

DS-101 Key Encryption Key. The key encryption key used in the KGV-8 and CDH to encrypt/decrypt keys transferred via DS-101.

Electronic Key Management System Key Encryption Key. The key encryption key used to encrypt data for transport from one COMSEC account to another.

End Cryptographic Unit (ECU). The generic name for any crypto device. Sometimes referred to as Tier 4.

End Cryptographic Unit Key Encryption Key (ECU KEK). Key data that results from a key being encrypted in an ECU KEK.

Fighter Data Link (FDL). Multifunctional Information Distribution System (MIDS) Low-Volume Terminal 3. The MIDS variant used in F-15s.

Front-End System (FES). A receive-only Link 16 terminal. The CDH is embedded on the transmission security/communications security unit. The unit can be set from the front panel to be either DS-101 or DS-102.

Interim Joint Tactical Information Distribution System Message Specification (IJMS). The message standard for Class I Joint Tactical Information Distribution System terminals. IJMS is still used in NATO and some USAF E-3 aircraft.

Interoperability Standards for Electronic Key Management Systems. Replaces the previous standards: DS-100, DS-101, DS-102, and NSA 87-27 are contained.

Joint Tactical Information Distribution System Network Library (JNL). Compendium of Joint Tactical Information Distribution System networks, normally distributed as a single magnetic media item.

Joint Tactical Information Distribution System Unit Data. An operations task link data field.

Key. In this context, “key” refers to the information bits that specify the generation of protection hiding bit stream, which is used to hide the intelligent information transmitted through the communication system. In many older documents, the name crypto variable is used. The Director, NSA, has directed that key be used instead of crypto variable.

Key Distribution Support User Application Software (KDSUAS). USN user application software to work with the local communications security management software in the Electronic Key Management System to provide support data and keys to the Common Tier 3 on a data transfer device from the local management device/key processor.

Key Encryption Key (KEK). The key used to encrypt or decrypt other keys for transmission or storage.

Key Processor (KP). KOK-22A.

Keyer Control Panel (KCP). A device used to set the memory address into which the key goes. The load control unit is a KCP in a box for USN aircraft ship use on flight deck. The KCP is required for DS-102 key fill. The DS-101 key fill does not require a KCP; the software in the AN/CYZ-10 sets the memory location.

Link 16. A jam-resistant, line-of-sight tactical data and voice communication system with relative navigation capabilities.

Load Control Unit (LCU). The LCU mechanically encapsulates a keyer control panel.

Local Communications Security Management Software (LCMS). This software runs on the local management device to control and utilize the key processor. A basic part of Tier 2.

Local Management Device (LMD). The central element of Tier 2 accounts.

Megahertz (MHz). One million cycles per second.

Message Security (MSEC). Security afforded to transmit textual data by a machine cryptographic system. A field in the Link 16 terminal that

designates the isolating crypto short title to protect the message content of designated network participation groups using the cryptographic variable logic label.

Military Standard (MIL-STD) 6016A. The document defining message formats and data elements for Link 16 messages.

Multifunctional Information Distribution System Low-Volume Terminal (MIDS-LVT). The family of Link 16 transceivers designed for integration in various airborne and air defense platforms. Current variants include the MIDS-LVT(1), LVT(2), and LVT(3), also commonly referred to as the fighter data link terminal.

National Distribution Authority. The NSA key production and distribution authority.

National Security Agency Central Facilities (NSACF). Key Production Tier 0.

Network Participation Group (NPG). A unique list of applicable Link 16 messages used to support an agreed technical function without regard to subscriber identities. This list is a means of transmitting a common set of Link 16 messages to all interested users. Frequently used NPGs include electronic warfare, C2, network synchronization, etc.

Network Time. Network time is that time maintained by a JU designated as the Network Time Reference (NTR) and is the common time reference with which all other JTIDS Units (Jus) synchronize.

NSA Specification 90-2A. The THORNTON smart fill data standard. It is a DS-101 base standard with the special fields required for the THORNTON smart fill defined.

Operations Task Link (OPTASKLINK). The U.S. message text format that provides detailed instructions regarding tactical data link operations, including information required to establish these links.

Over-the-Air Rekey (OTAR). Changing the traffic encryption key or transmission security key in remote cryptographic equipment by sending a new key directly to the remote cryptographic equipment of the communications path it serves. In Link 16, a special capability of the communications security/transmission security integrated circuit cryptographic engine that enables over-the-air key delivery without the need for a physical fill device.

Over-the-Air Rekey (OTAR) Encrypted Key. Key data that results from a key being encrypted in an OTAR key encryption key, sometimes referred to as

the “rekey phrase.” These encrypted keys can be loaded only from the transmission side of the Link 16 terminal via J31.0 and J31.1 messages; they cannot be loaded through the fill port.

Over-the-Air rekey (OTAR) Key Encryption Key (KEK). The KEK used in a secure data unit to decrypt keys received via OTAR. Sometimes referred to as a “unique” key. In the Electronic Key Management System, OTAR KEK is referred to as KGV-8 KEK or OTAR KEK. The OTAR KEK can be loaded through the fill port.

Partitioned Variable Mode (PVM). The mode of operation in which a different message security traffic encryption key is used to secure specific compartmented data that is used for other Link 16 data and for Link 16 transmission security for traffic encryption/decryption and transmission security.

Random Access Memory (RAM). Computer memory that provides the main internal storage available to the user for programs and data. Sometimes referred to as “volatile” memory. There are eight memory locations in the secure data unit that are volatile and used for traffic encryption keys and over-the-air rekey key encryption keys. The USA Multifunctional Information Distribution System variant (MIDS-LVT(2)) has 64 RAM locations.

RED Key. An unencrypted key.

Rekey Phrase. See over-the-air rekey (OTAR) encrypted key.

Reserve On Board (ROB). The amount of key required to be present at an account for future use because that account will not be able to communicate with the account that generates the key for a period of time.

Round-Trip Timing (RTT). Messages sent and received that are used to accurately assess the distance between terminals.

Secure Data Transfer Device 2000 System (SDS) KIK-20. The SDS was developed by NSA. It is designed to securely receive, store, and transfer electronic data between compatible communication equipment.

Secure Data Unit (SDU). The functional name for the THORNTON cryptographic equipment used in Link 16 terminals. Link 16 SDUs include the KGV-8/A/B/C in the Joint Tactical Information Distribution System Class II, the E-GLD in some of the USA systems, and the CDH in the common signal processor card and in the signal message processor card of the Multifunctional Information Distribution System.

Signal Message Processor (SMP). The processing card of the Multifunctional Information Distribution System terminal that processes signals and raw messages.

Simple Key Loader (SKL) AN/PYQ-10. A handheld data transfer device used to transfer keys between Electronic Key Management System devices.

Software Support Activity (SSA). Each COMSEC software package is required by the Director, NSA, to have an SSA established to correct problems and add new capabilities.

Tactical Aircraft Mission Planning System (TAMPS). The system used to build the network to be installed in the Link 16 system. The National Command System (NCS) for the U.S. Army and the command and control processor (C2P) for the ships perform similar functions. TAMPS is offline, whereas C2P and NCS are online and exercise communication functions as well.

THORNTON. The project name that refers to the KGV-8 equipment and the THORNTON embedded products.

Tier 0. The Central Facility at NSA. This facility is capable of doing Tier 1 functions. It also forms the bridge between the United States and other countries.

Tier 1. The Service key production, distribution, and accounting facility. This tier has large production capabilities for the electronic key but none for the physical key. Personnel from each Service staff Tier 1.

Tier 2. Designation of the local account holder. The local communications security management software running on the local management device connected to the key processor makes up the backbone of this tier.

Tier 3. This is the user level of the system. The user holds and uses the AN/CYZ-10 to fill Tier 4 equipment.

Tier 4. This tier is generally identified with the end cryptographic units.

Time Slot. The minimum burst of communication possible in Link 16. One or more Link 16 messages are transmitted in each time slot. A time slot is 7.8125 msec in duration and 128 time slots are transmitted each second, or 1,536 time slots within each 12-second frame.

Traffic Encryption Key (TEK). The key used to encrypt plain text or to super encrypt previously encrypted text and/or to decrypt cipher text. Within

the Link 16 system, TEK provides both transmission security and message security.

Transmission Key Encryption Key (TrKEK). The key encryption key used to decrypt keys in the AN/CYZ-10 data transfer device.

Transmission Security (TRANSEC). The component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. Within the context of this document, it is used to identify fields in the Link 16 terminal that tie TRANSEC and message security (MSEC) of network participation groups (NPGs) supporting normal communication messages to the short title via the cryptographic variable logic label. Special NPGs may use MSEC for the message security and TRANSEC for the transmission security.

Transmission Security/Communications Security Unit (TCU). Part of the front-end system that is a controlled cryptographic item and handles the interface to the CDH.

Transmission Security Key (TSK). Keying material that provides transmission security in a system. In the Link 16 system, the traffic encryption key (TEK) performs both the TEK and TSK functions. Although the Electronic Key Management System provides the selection of the TSK, there is no way to distinguish the TSK from the TEK within the Link 16 terminals. The Director, NSA, generally considers the TSK to be a lower risk than the TEK. The Link 16 terminal will very likely use any key it is given to perform, as with the TEK function. Therefore, all traffic keys should be designated as TEKs and never as TSKs.

(INTENTIONALLY BLANK)