

ATP 6-02.75

**TECHNIQUES FOR COMMUNICATIONS SECURITY (COMSEC)
OPERATIONS**

August 2015

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at Army Knowledge Online
(<https://armypubs.us.army.mil/doctrine/index.html>).
To receive publishing updates, please subscribe at
http://www.apd.army.mil/AdminPubs/new_subscribe.asp

TECHNIQUES FOR COMMUNICATIONS SECURITY (COMSEC) OPERATIONS

Contents

		Page
	PREFACE	iii
	INTRODUCTION	iv
Chapter 1	COMMUNICATIONS SECURITY	1-1
	Introduction to Communications Security.....	1-1
	Commander Responsibilities.....	1-2
	Directors, Agencies, Commanders of Army Commands, Installations, and Activities.....	1-2
	Authority.....	1-3
	Managers.....	1-3
	Corps and Division G-6	1-3
	Brigade Communications Staff.....	1-4
	User Representative and Individual User Responsibilities.....	1-4
Chapter 2	ELECTRONIC KEY MANAGEMENT SYSTEM AND ARMY KEY MANAGEMENT SYSTEM	2-1
	Electronic Key Management System Overview	2-1
	Tier 0–Central Facility.....	2-1
	Tier 1–Central Office of Record.....	2-1
	Tier 2–Communications Security Account Management	2-2
	Tier 3–User Level Management.....	2-1
	Devices Generation and Verification of Electronic Key Management System Transaction Authentication Signatures.....	2-1
	Army Key Management System Overview.....	2-2
	Modern Key	2-3
	End Cryptographic Unit Interface Specifications	2-6
Chapter 3	KEY DISTRIBUTION	3-1
	Distribution Planning.....	3-1
	Distribution Execution.....	3-2

	Over The Air Rekeying.....	3-3
	Encrypted (Black) Key Distribution	3-3
	Encrypted Key Operations	3-4
	Transfer Key Encryption Key Management	3-6
	Joint/North Atlantic Treaty Organziations/Coalition Operations	3-7
	Exercise and Deployment Communications Security Support	3-7
Chapter 4	ACCOUNTING.....	4-1
	Hand Receipting Communications Security Material.....	4-1
	Issue Key to a Local Element	4-1
	Key Management System Certificate Management	4-3
	Compromise Recovery	4-3
	Manage Two-Person Integrity for Communications Security Support.....	4-4
Chapter 5	CRYPTOGRAPHIC NETWORK PLANNING	5-1
	Establishing Cryptographic Networks	5-1
	Planning Cryptographic Networks.....	5-1
	Signal Operations Instructions and LoadSet Management	5-2
Chapter 6	CRYPTOGRAPHIC DEVICES.....	6-1
	End Cryptographic Unit Software Upgrade Planning.....	6-1
	Periodic Tamper Checks of End Cryptographic Units	6-2
Chapter 7	CONTROLLED CRYPTOGRAPHIC ITEMS	7-1
	Identifying Controlled Cryptographic Items	7-1
	Transfer of Controlled Cryptographic Items Between Army and Navy Accounts	7-2
	Transfer of Controlled Cryptographic Items Between Army and Air Force or Any Other Service and Agency	7-2
	Transfer of Controlled Cryptographic Items from Army Department of Defense Activity Address Code Accounts	7-2
Chapter 8	KEY MANAGEMENT INFRASTRUCTURE	8-1
	Key Management Infrastructure Roles and Responsibilities	8-1
	System Capabilities.....	8-2
	GLOSSARY	Glossary-1
	REFERENCES.....	References-1
	INDEX	Index-1

Figures

Figure 2-1. Electronic key management system tier 0 and 1/Army key management system tier 2 and 3	2-2
--	-----

Preface

Army techniques publication (ATP) 6-02.75, *Techniques for Communications Security Operations*, provides guidance on the management, employment, handling, and storage of communications security materials. It outlines roles and responsibilities for all members of the Army Profession providing communications security planning, management, and accounting services in support of movement and maneuver, intelligence, fires, sustainment, mission command, protection, and the Army's portion of Department of Defense information networks (DODIN) capabilities. This publication addresses methods of key transport, provides the fundamental principles for communications security operations to support all echelons, and provides details of Key Management Infrastructure (KMI).

The principal audience for ATP 6-02.75 is commanders, signal staff officers at all levels, communications security account managers, and members of the Army Profession. Commanders and staffs of Army headquarters serving as joint force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this manual.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. Note: See field manual (FM) 27-10.

ATP 6-02.75 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

The proponent of this publication is the U.S. Army Cyber Center of Excellence. The preparing agency is the Cyber Center of Excellence Doctrine Branch, United States Army Cyber Center of Excellence. Send comments and recommendations on a Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-DT (ATP 6-02.75), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735; or by e-mail to usarmy.gordon.cybercoe.mbx.gord-fg-doctrine@mail.mil.

Introduction

ATP 6-02.75, *Techniques for Communications Security Operations*, expands on the foundation of communications security (COMSEC) found in FM 6-02, *Signal Support to Operations*.

The Army's portion of DODIN provide authorized users with a seamless, secure, and interconnected information environment, meeting real-time and near real-time needs of the Soldier. The Army's portion of DODIN systems and devices must employ a robust encryption capability that will ensure cybersecurity to all Army forces. These systems support our Soldiers as they operate during unified land operations. We rely on cryptography to protect our most sensitive information in transit and at rest. Those responsible for protecting it are constantly seeking ways to deter and prevent those seeking to exploit it. Systems designed to help protect information are continually under attack from systems incorporating extremely sophisticated computers with faster processor speeds. This convergence of age and speed leads to greater vulnerabilities in systems protecting our most critical information within a network that touches nearly every Soldier, weapon system, and installation. Cryptographic capabilities must be interoperable, secure, and available for support of mission critical systems in support of the Army's portion of DODIN. This publication documents current Army communications security operations doctrine. Modernized net-centric cryptography is integral to achieving Department of Defense (DOD) warfighting systems' objectives. This document provides the doctrinal underpinnings supporting COMSEC operations to strategic, operational, and tactical mission objectives. This manual provides techniques that are consistent with Army regulation (AR) 380-40.

Effective tactical communications requires the management of keys, devices and other COMSEC material management at the lowest echelon possible, while maintaining the highest level of physical security for the equipment and material. Managers and operators must be capable of handling contingencies such as emergency key supersession, equipment failures, and removing or eliminating the key with minimal equipment outages. The need for security cannot override the basic requirement to communicate; the Army must balance these requirements.

Note. Where this ATP appears to conflict with Army COMSEC policy and procedures contained in AR 380-40 and AR 710-2, those publications will take precedence. Immediately report all such conflicts to the U.S. Army Cyber Center of Excellence Doctrine Branch. (Refer to the Preface on page v of this ATP.)

ATP 6-02.75 consists of eight chapters—

Chapter 1 defines COMSEC, addresses equipment maintenance and the destruction of COMSEC material. This chapter also addresses the roles and responsibilities for civilian and military personnel providing COMSEC.

Chapter 2 provides Electronic Key Management System (EKMS) and Army Key Management System (AKMS) overview. This chapter also discusses modern keys and end cryptographic unit (ECU) interface specifications.

Chapter 3 addresses distribution planning, distribution execution, over the air rekeying, encrypted (Black) key distribution, encrypted key operations, and transfer key encryption key (TrKEK) management. This chapter includes joint/North Atlantic Treaty Organization/coalition operations, and exercise and deployment COMSEC support.

Chapter 4 describes hand receipting COMSEC material, issuing keys to local element, key management system certificate management, compromise recovery, and managing two-person integrity for COMSEC support.

Chapter 5 addresses cryptographic network planning and signal operating instructions loadset management.

Chapter 6 addresses ECU software upgrade planning and periodic tamper checks of ECUs.

Chapter 7 includes identifying controlled cryptographic items, transfer of controlled cryptographic items between Army and Navy accounts, transfer of controlled items between Army and Air Force or other service or agency, and transfer of controlled items from Department of the Army (DA) activity address code accounts.

Chapter 8 provides an overview of the KMI capabilities to include roles and responsibilities.

The glossary lists acronyms and terms with Army, multi-service, or joint definitions, and other selected terms. Where Army and joint definitions are different, (*Army*) follows the term. The proponent manual for other terms is listed in parentheses after the definition.

This page intentionally left blank.

Chapter 1

Communications Security

Protecting the information that flows through systems comprising the communication infrastructure is vital to the force. This chapter defines communications security, addresses equipment maintenance, the destruction of communications security material, and the roles and responsibilities for civilian and military personnel providing communications security.

INTRODUCTION TO COMMUNICATIONS SECURITY

1-1. Maintaining secure communications is vital to military operations. The weaker the military's communications security efforts, the easier it is for an enemy to exploit communications.

1-2. *Communications security* is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 6-0) COMSEC is a cybersecurity capability, which maintains the confidentiality, integrity, availability, and non-repudiation of Army information. COMSEC allows for proper identification and authentication of data users. The four components of COMSEC include—

- *Cryptographic security*—The component of COMSEC that results from the provision of technically sound cryptographic systems and their proper use.
- *Transmission security*—The component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.
- *Emission security*—The component of COMSEC that results from all measures taken to deny unauthorized persons information of value possibly deriving from the interception and analysis of compromising emanations from cryptographic equipment and telecommunications systems.
- *Physical security* of COMSEC material—The component of COMSEC that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

1-3. COMSEC consists of cryptographic and key management solutions, both providing cryptographic products and services supporting COMSEC operations in joint networked environments. Joint modernization efforts in cryptography and key management result in paradigm shifts with cryptographic key generation, storage, and distribution in support of the Army's modernized network. Modernization of devices, algorithms, and cryptographic key provides the ability to develop governance and technical architecture standards ensuring security of Network elements.

MAINTENANCE

1-4. Under the Two-Level Maintenance Concept, COMSEC personnel perform COMSEC equipment maintenance based on published Army Technical Manual Maintenance Allocation Charts and the type of equipment involved, facilities, support availability, and time considerations. Most COMSEC equipment has a technical manual that includes a maintenance allocation chart. The technical manual maintenance allocation chart limits the level of maintenance of individual organizations to diagnosis and fault isolation. Field maintenance support organizations perform all maintenance tasks coded "C" (operator, crew, signal support specialist) or "F" (maintainer). The Army Depot at Tobyhanna, Pennsylvania performs sustainment maintenance on COMSEC material under maintenance tasks codes "D" in the equipment technical manual maintenance allocation chart according to AR 750-1.

1-5. COMSEC equipment is evacuated through maintenance channels from the unit to the first supporting maintenance unit. Unserviceable classified COMSEC material evacuates through the COMSEC material control system. Controlled cryptographic items are evacuated on work request through maintenance channels for serviceability tests, technical inspection, and repair. Equipment that cannot be repaired at the field maintenance level is evacuated to Tobyhanna Army Depot for repair or disposal.

1-6. Army customers submit authorized COMSEC requirements to the COMSEC Logistics Activity through organizational property book channels via the Army Information System Security Program in accordance with AR 25-2. Customer requisitions for classified COMSEC equipment are released by the COMSEC Logistics Activity through CMCS channels via the local communications security management software (LCMS) or KMI to the supporting COMSEC account.

DESTRUCTION OF COMSEC MATERIAL

1-7. The proper destruction of COMSEC material is critical. The improper destruction of classified or unclassified material is a reportable COMSEC incident and may lead to potential adversaries attaining important information. The four types of reportable COMSEC incidents are physical, cryptographic, personnel, and administrative incidents. Destruction of accountable COMSEC material requires the presence of a destruction official and a witness. Both individuals must possess a clearance for the highest classification of material they are destroying. They assume responsibility for ensuring the proper destruction of COMSEC material, preparing a destruction report and ensuring destruction meets the appropriate standards according to Technical Bulletin (TB) 380-41. Keying material must be destroyed immediately after its suppression date, have served its intended purpose, or becomes obsolete. Within 12 hours of supersession or according to written CONAUTH/CMDAUTH guidance, destroy all material hand receipted to a user, regardless of material location. COMSEC personnel will not destroy defective or faulty key but immediately report it via the COMSEC Incident Management Monitoring System to the National Security Agency (NSA) Information Assurance Directorate and hold key for disposition instructions (refer to AR 380-40, Chapter 2 for further destruction guidance).

COMMANDER RESPONSIBILITIES

1-8. Within Army organizations, the responsibility to safeguard and control COMSEC material in a manner that ensures its continuous integrity and prevents access to unauthorized persons rests with the commander. Safeguarding and controlling COMSEC material is also the responsibility of individuals in possession of the material. AR 380-40 outlines the responsibility for safeguarding and controlling all COMSEC material, both classified and unclassified.

DIRECTORS, AGENCIES, COMMANDERS OF ARMY COMMANDS, INSTALLATIONS, AND ACTIVITIES

1-9. Directors of HQDA Agencies, commanders of Army Commands, installations and activities using COMSEC need to have knowledge of AR 25-55, The Freedom of Information Act, its exceptions, and restrictions pertaining to the release of COMSEC information. The NSA is responsible for developing and prescribing cryptographic principles and standards including development and execution management of Department of the Army cryptographic hardware and software systems.

1-10. The Program Executive Office for Command, Control and Communications-Tactical provide development, procurement, deployment, training, sustainment, and the technical expert for applications and implementation including the primary point of contact for platform integration. Project Director Network Enablers, an organization under Program Executive Office Command, Control Communications Tactical, ensures the security of the information transmitted across the network and streamlines the delivery of hardware and software solutions to meet changing technology needs. Communications Security Logistics Activity is the manager of COMSEC systems and programs responsible for cryptographic key management and distribution. Additional information is provided on their websites.

AUTHORITY

1-11. COMSEC authority levels vary according to responsibilities and assignments. Commanders appoint personnel with specific authority figures to make decisions and enforce compliance when dealing with COMSEC. The following paragraphs outline the different types of authority involving COMSEC.

SERVICE AUTHORITY

1-12. The Service authority is the department or agency senior staff component or command level element in each military Service that oversees COMSEC operations, policies, procedures, accounting, resource management, material acquisition, and training. In the Army, COMSEC Service Authority responsibilities at Headquarters, Department of the Army (HQDA) are allocated and executed by the HQDA Deputy Chief of Staff, G-2, Safeguarding and Controlling COMSEC, Cyber Chief Information Officer, and COMSEC Program Director. The HQDA Assistant Chief of Staff, Intelligence delegates certain functional Service authority responsibilities to the Communications Security Logistics Activity.

COMMAND AUTHORITY

1-13. The commander appoints the command authority. The individual is responsible for managing modern key assets to include associated key ordering privileges. See TB 380-40, Chapter 2 for Army procedures.

CONTROLLING AUTHORITY

1-14. The controlling authority is the commander of the organization or activity responsible for establishment, operation, and management of traditional cryptographic key used in a command network. The commander of the organization or activity is responsible for directing establishment and operation of a cryptographic network, and for managing the operational use and control of keying material assigned to the cryptographic network. The commander may delegate controlling authority responsibilities to a subordinate, in writing. The controlling authority should be organizationally senior to cryptographic network members, have the staff and expertise to perform essential management functions, and have the authority to ensure COMSEC personnel follow through with instructions. See TB 380-40, chapter 1 for Army procedures.

MANAGERS

1-15. The management of COMSEC material is critical to the security of the Warfighter and the Army's portion of DODIN. The following paragraphs outline the different types of managers and their responsibilities.

COMSEC ACCOUNT MANAGER AND PRIMARY ALTERNATE COMSEC ACCOUNT MANAGER

1-16. The COMSEC Account Manager is the individual appointed, in writing, by the commander or director who is responsible for receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of COMSEC material (TB 380-41). The COMSEC Account Manager is also responsible for the supervision and oversight of local element hand receipt holders to ensure compliance with existing COMSEC material security; accounting; operational policies and procedures; acquisition, control, and distribution of all classified COMSEC material and cryptographic key to support organizational missions. The Primary Alternate COMSEC Account Manager is the individual responsible for the receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of COMSEC material in the absence of the COMSEC Account Manager. For automated accounts, the COMSEC Account Manager and the Primary Alternate COMSEC Account Manager completes the United States Army Training and Doctrine Command approved COMSEC Account Manager Course and LCMS Course before appointment.

CORPS AND DIVISION G-6

1-17. The assistant chief of staff, signal (G-6) officer plans and directs cybersecurity activities and information operations vulnerability and risk assessments in coordination with the: assistant chief of staff,

intelligence, assistant chief of staff, operations; assistant chief of staff, information engagement; operational chain of command; and the Regional Cyber Center. At the corps and division level, the COMSEC Account Manager and Primary Alternate COMSEC Account Manager are members of the Network Operations and Security Center staff. The COMSEC Account Manager and Primary Alternate COMSEC Account Manager are responsible for all COMSEC material, including storing keys in encrypted form and performing key generation and automatic key distribution.

BRIGADE COMMUNICATIONS STAFF

1-18. Brigade COMSEC personnel perform the same duties as G-6 COMSEC personnel. The brigade cybersecurity staff officer provides oversight and coordination of COMSEC operations including storage, management, distribution, inspection, and compliance.

USER REPRESENTATIVE AND INDIVIDUAL USER RESPONSIBILITIES

1-19. The user representative is the person authorized by an organization's command authority to order modern COMSEC keying material. The user representatives also interface with key managers at the NSA Central Facility and Communications Security Logistics Activity, and key users, ensuring the correct type of key is ordered. The cryptographic network planner may share this responsibility. The user representative does not have to be a COMSEC Account Manager, but keeps the COMSEC Account Manager informed about keying material(s) they have requested, and for what purpose.

1-20. Individual users physically protect COMSEC material in their possession or under their control. Individual users have the primary responsibility for reporting any occurrence, circumstance, or act that could jeopardize the COMSEC material's integrity. Individual users are responsible for following the COMSEC Account Managers instructions for protecting and controlling material. Individual users also comply with instructions provided by the property book officer for controlling and safeguarding controlled cryptographic item. Personnel in the Department of the Army Cryptographic Access Program are subject to random counterintelligence scope polygraph examinations. For a detailed description of all responsibilities pertaining to COMSEC material control, see AR 380-40 or TB 380.41.

Chapter 2

Electronic Key Management System and Army Key Management System

Key management architecture and systems provide for the distribution, operation, management, support, and protection of communications security related items. This chapter provides Electronic Key Management System and Army Key Management System overview. This chapter also discusses modern keys, and end cryptographic unit interface specifications.

ELECTRONIC KEY MANAGEMENT SYSTEM OVERVIEW

2-1. The EKMS is a key management, COMSEC material distribution, and logistics support system. The EKMS is the U.S. Government's system to organize and automate comprehensive key management to support authorized users. These users include military as well as non-military users and Government contractors with interoperable COMSEC systems and controlled items. EKMS utilizes an integrated, multi-tiered key management approach to plan, order, generate, distribute, store, fill, use, and destroy electronic keys and other types of COMSEC material. The system consists of automated workstations using LCMS. EKMS also provides these capabilities to manage physical key and non-key COMSEC related items. Non-key COMSEC related items consist of equipment, devices, documents, and software that secure or authenticate communications and perform COMSEC functions for physical or electronic key and other COMSEC Material Control System controlled items.

2-2. The management of cryptographic keys at each of the four separate levels comprises the EKMS and AKMS architecture. Each tier has specific functions and duties that may or may not interface with another tier depending on the function initiated. This chapter addresses generation and verification of EKMS and AKMS transaction authentication signature at tier 0—central facility; tier 1—central office of record, tier 2—COMSEC accounts supporting field operations; and tier 3—user level management (includes: hand receipt holder and local element fill device). Upcoming paragraphs explain the make-up and functionality of each tier.

TIER 0—CENTRAL FACILITY

2-3. Tier 0 consists of the central facility at Fort Meade, Maryland and the central facility at Finksburg, Maryland. Tier 0 facilities can generate all types of key currently used in U.S. cryptographic systems. The central facility at Fort Meade produces and distributes physical key (through the U.S. National Distribution Authority) and selected electronic key (via EKMS bulk encrypted transaction). Tier 0 acts as the central office of record for non-military accounts not serviced by a tier 1 civil central office of records; and as the registration authority for accounts operated by NSA, contractors, and other civilian entities. The Central Facility at Finksburg produces and distributes secure data network system key and message signature key. The Central Facility at Finksburg performs FIREFLY seed key conversion and rekey, supports compromise recovery functions, and provides the EKMS help desk. FIREFLY is an NSA system based on public key cryptography.

TIER 1—CENTRAL OFFICE OF RECORD

2-4. The central office of record is responsible for ensuring accounts under their authority comply with the NSA and Department/Agency COMSEC accountability requirements. The central office of record has overall responsibility for oversight and enforcement of Army policies and approved procedures, for maintaining a record of all accountable material held by the accounts, and for performing regular inventory. The tier 1

system provides interfaces to tier 0, the tier 2 EKMS accounts, local and remote tier 1 operators, and directs physical key distribution to personnel operating COMSEC vaults, depots, and logistics systems facilities. The tier 1 system utilizes X.400 electronic messaging to communicate with EKMS elements, and uses the X.500 directory; composed of its own data, along with data replicated from the COMSEC facility.

PRIMARY TIER 1 SEGMENT

2-5. Each of the designated primary military tier 1 facilities (Fort Huachuca, Arizona and Lackland Air Force Base, Texas) has a primary tier 1 segment installed. The primary tier 1 segment generates and distributes traditional electronic key; manages distribution of physical COMSEC material; and serves as the registration authority, privilege manager, central office of record, and data repository for all Service accounts, including EKMS accounts supporting combatant commanders and joint task force.

2-6. Each primary tier 1 segment provides primary database functionality for its supported accounts, and automatically updates the other primary tier 1 segment so the databases remain synchronized. The primary tier 1 segment also provides data to each physical material handling segment updating their databases and further enabling their missions. The primary tier 1 segment employ load sharing providing the total tier 1 sizing and throughput capacity. If one primary tier 1 segment becomes unavailable, the other primary tier 1 segment provides all tier 1 support, including key generation and distribution, flexible disk production, message server throughput, and communications throughput, for all EKMS.

PHYSICAL MATERIAL HANDLING SEGMENT

2-7. Each Service vault, depot, and logistics systems facility (Tobyhanna Army Depot, PA; Norfolk, VA; San Antonio, TX) has a physical material handling segment installed. The Naval Communications Security Material System site in Washington, DC has a physical material handling segment like interface into primary tier 1 segment at San Antonio, and can perform central office of record and Service authority functions. These facilities use the tier 1 system to automate Navy COMSEC material and equipment logistics management. The physical material handling segment provides a user interface that allows exchange of distribution management and accounting information between the primary tier 1 segment and the vaults, depots, and logistics systems. The physical material handling segment provides limited physical material management.

TIER 2—COMMUNICATIONS SECURITY ACCOUNT MANAGEMENT

2-8. Tier 2 is comprised of an AN/GYK-49 (LCMS) or AN/GYK-72 (KMI) system supporting field user operations. These accounts exchange information directly with their respective tier 1 (central office of record). All accounts are automated and have EKMS components (the LCMS, local management device or computer, key processor, secure telephone equipment and/or key generator-250 in-line network encryptor), or simple key loader, or other modern field devices to manage physical and electronic key and other COMSEC material.

COMMON USER APPLICATION SOFTWARE

2-9. The common user application software resides on the LCMS workstation, works in conjunction with the local management device and key processor (KOK-22A) to facilitate creating and loading Black key to removable media, and integrates tier 2 key management into a single, comprehensive system to access the local management device and key processor data. The common user application software performs a number

of functions, which include producing specific forms and reports; enhancing the ability to account for physical COMSEC material; packaging encrypted key; an improved interface with the common tier 3 and data management device components; and providing integrated on-line help.

LOCAL MANAGEMENT DEVICE

The local management device provides automated services for the management of key and other COMSEC material and serves as an interface to the key processor. The local management device is central to EKMS, and is composed of a Service or agency supplied, personal computer, an operating system, LCMS software, and user application software as required.

KEY PROCESSOR

2-10. The key processor is a classified device (the trusted component of tier 2) that performs all required cryptographic processing and access control for the EKMS account, and COMSEC material ordering and accounting functions. This includes generating traditional electronic key, FIREFLY encryption and decryption of electronic key transferred among EKMS elements, encryption and decryption of electronic key stored in the local management device database, and issue of electronic key to an EKMS.

TIER 3–USER LEVEL MANAGEMENT

2-11. Tier 3 is the lowest level of the EKMS architecture comprising local element hand receipt holders utilizing modern fill devices to interface between tier 2 workstations and end users crypto devices used to pass key, audit data, crypto variables and other required information. Tier 3 elements receive keying material from tier 2 activities through electronic fill devices or in canisters (for physical keying material).

DEVICES GENERATION AND VERIFICATION OF ELECTRONIC KEY MANAGEMENT SYSTEM TRANSACTION AUTHENTICATION SIGNATURES

2-12. The key processor (KOK-22A) receives commands and data from the LCMS, checks the validity and integrity of received commands and data, performs the required cryptographic services, and returns data to the LCMS. The key processor creates, stores, and outputs an audit trail of its processing activity to the local management device. The key processor includes a zeroize switch to allow the operator to rapidly delete all classified information in an emergency. Any tampering (such as removing the cover) automatically zeroizes the key processor. Figure 2-1 on page 2-4 depicts the EKMS architecture displaying tiered structure.

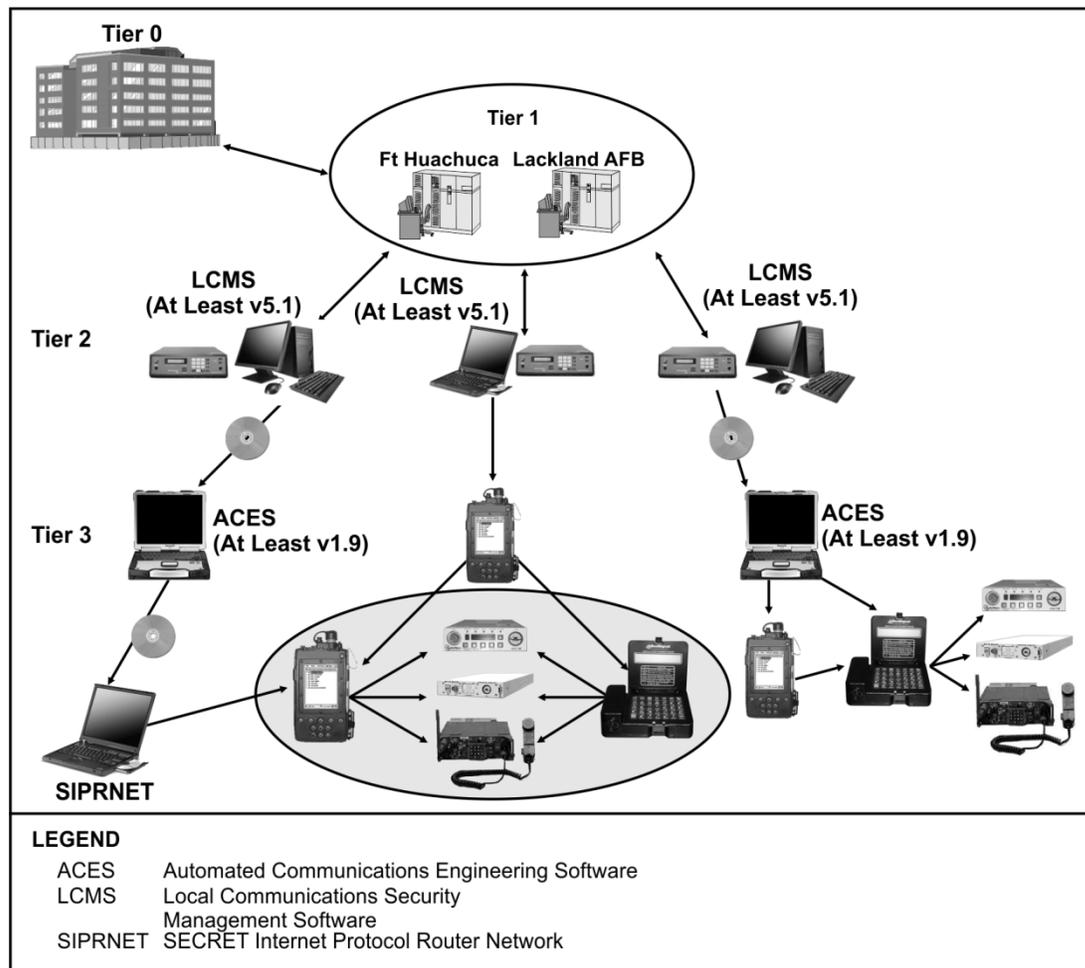


Figure 2-1. Electronic key management system tier 0 and 1/Army key management system tier 2 and 3

Note. Automated Communications Engineering Software (ACES) v1.9 is the baseline version, v3.3 is the latest available software version.

ARMY KEY MANAGEMENT SYSTEM OVERVIEW

2-13. The AKMS provides planners and operators the capabilities of providing secure communications at theater, tactical, strategic, and sustaining base levels. The system provides organic key generation capabilities and provides secure electronic key distribution along with electronic protection, COMSEC distribution, and signal operating instructions (SOI) information. The AKMS consists of three subcomponent platforms—

- ACES workstation.
- LCMS.
- Any approved tier 3 device.

2-14. The ACES workstation plans, creates, distributes, manages, and verifies cryptographic networks and key-related information. It also generates electronic protection data and SOI. The ACES resides on a common hardware and software laptop computer. Additional functions include network-based radio planning and management, and encrypted by key distribution (EKD) planning. It associates key tags with network, platform, equipment key location, and distribution path. Depending on the operational structure of each organization, the ACES Workstation may reside within the COMSEC account, or at a separate location with

the Network Manager, in the assistant chief of staff; operations and battalion or brigade operations staff officer operational staff office.

2-15. LCMS is the software application that performs detailed accounting for COMSEC accounts. It performs the processes required to generate and distribute electronic keys. COMSEC Account Managers utilize the common user application software to generate, manage, and distribute black key. Tier 2 (management level at the COMSEC account) are Service or DOD agencies providing local management device running the LCMS, as well as user application software key processors, and secure telephone equipment. Tier 3 (user management level) contain fill devices such as simple key loader and ECU.

2-16. The simple key loader is the replacement for the Army's data transfer device. The simple key loader is a handheld digital computer running the Windows CE.NET operating system, and host the core library and simple key loader user application software programs. The programs interface with the LCMS and ACES workstations. Simple key loaders integrate the functions of COMSEC key management; control, distribution, electronic protection management; SOI management; benign fill; and other specialized capabilities into one comprehensive system. It handles, stores, views and loads signal operating instructions and electronic protection data quicker. It also provides interface between the LCMS and ACES.

Note. Microsoft does not identify CE as letters that represent any words to form an acronym.

MODERN KEY

2-17. Modern key uses the public key infrastructure with FIREFLY key management protocol. The FIREFLY key establishes a session key between two entities. Two separate (but mathematically related) input keys (asymmetric keys) perform encryption and decryption functions. This key pair consists of a private key and a public key. The public key encrypts the data, and the private key decrypts.

TYPES OF MODERN KEYS

2-18. The two types of modern keys supported by EKMS are—

- **Message signature key**—cryptographic material used in the electronic signature process to assure source authentication, message integrity, and non-repudiation.
- **Secure data network system key**—an asymmetric key that does not include the Public Key Infrastructure and is a set of variables used in a key exchange algorithm to produce a traffic encryption key.

TEST KEY

2-19. The intent of the test key is online testing of COMSEC equipment or systems. The test key is classified based on network circuitry or intended level of information and equipment parameters protected. Test keys are marked cryptographic.

OPERATIONAL KEY AND SEED KEY

2-20. The intent of the operational key is over-the-air protection of operational information, key production, or secure electrical transmission of key streams. The seed is the initial key which starts an update or key generation process. Operators use the key to communicate with the central facility to receive an operational key.

KEY GENERATION

2-21. Key generation is the process that creates the first instance of a key. This includes all mission system independent or mission system dependent data derivable from a standard key order in the format required by the destination COMSEC equipment.

LOCAL KEY GENERATION

2-22. LCMS produces electronic traditional keys, such as transfer key encryption keys (TrKEK), key encryption keys, and traffic encryption keys. Appropriate privileges are registered or generated before generating these keys. LCMS, together with the key processor, is capable of generating keys and short titles.

END CRYPTOGRAPHIC UNIT INTERFACE SPECIFICATIONS

2-23. The electronic system ECU receives the electronic key at the lowest end-user level. It consists of several interfaces that include internal, LCMS operator, system administrator, and external. The following paragraphs outline the different types of interface specifications.

INTERNAL INTERFACES

2-24. The internal interfaces consist of all physical or functional paths across which information or processes pass inside the LCMS workstation. These include the local management device operator interface, system administrator interface, and key processor operator interface.

TIER 2 LCMS WORKSTATIONS

2-25. The LCMS workstation can exchange data with other LCMS workstations using the LCMS direct communications functions or through the secure telephone equipment. Operationally, the LCMS and ACES workstations, combined with the modern fill device, constitute the AKMS.

COMMON AND MODERN FILL DEVICES

2-26. Legacy common fill devices (KYK-13, KYX-15, and the data transfer device) are being phased out of the Army inventory. Modern fill devices read in, transfer, or store keys. An example of a modern fill device is a simple key loader. Modern fill devices can provide an audit trail of all key actions and transactions. The local management device can upload audit data from a modern fill device, and send encrypted key and application data to a modern fill device.

END CRYPTOGRAPHIC UNIT

2-27. An ECU is the device that encrypts and decrypts data passed over the network. The ECU exchanges data with the LCMS workstation.

KEY STORAGE DEVICE-64A AND CRYPTOGRAPHIC IGNITION KEY

2-28. The key storage device 64A is used by the key processor as a fill device and cryptographic ignition key. The key processor has a cryptographic ignition key interface and an auxiliary key storage device 64A interface. The cryptographic ignition key provides access control to the key processor; only an authorized operator who inserts a valid cryptographic ignition key can use the key processor. An operator uses the auxiliary key storage device-64A interface to load initialization data into the key processor and to program cryptographic ignition keys with key processor operator information.

RED FILL INTERFACE

2-29. The key processor sends encrypted or unencrypted key to a modern fill device or simple key loader, as well as unencrypted key to a modern fill device. The key processor can also accept audit data from the modern fill device connected to the red fill interface or accept a key from a modern fill device.

Chapter 3

Key Distribution

This chapter addresses distribution planning and execution, over the air rekeying, encrypted (Black) key distribution, encrypted key operations, and transfer key encryption key management. This chapter also addresses joint/North Atlantic Treaty organization operations, exercise, and deployment communications security support.

DISTRIBUTION PLANNING

3-1. Key distribution is the secure, accountable process of moving key from the point of generation to the point of use in the ECU. Distribution includes sending and receiving key electronically, as well as the necessary packaging, copying, reformatting, encryption, and relaying requirement to transfer the key from its origin to the point of use. EKMS distributes encrypted keys from the point of generation to the point of issue. When possible, the keys remain encrypted until they are loaded into the end user equipment. EKMS enforces security restrictions to preclude key delivery unless the receiving element establishes the proper clearance.

3-2. Generate the key to fulfill a validated order. The control of an electronic key is either implicit or explicit. Implicit key distribution is at the discretion of the operator at an LCMS workstation. The operator at an LCMS workstation may distribute the explicit key only if there is a valid distribution authorization for that key in the local management device and key processor platform. Key distribution between a tier 2 account and a local element differs from distribution between COMSEC accounts. COMSEC account distribution uses—

- Transfer—distribution of COMSEC material from one account to another. In a transfer, accounting responsibility for the transferred COMSEC material shifts from the sending account to the receiving account.
- Issue—distribution of one or more accountable COMSEC items from a COMSEC account to a local element. The issuing element retains accountability for the material. Issuing and filling key are the two functional areas of key distribution between a tier 2 account and a local element.

3-3. The issue function is the local accountability of one or more accountable items from a tier 2 account to a local element or from a local element to a user. To aid the COMSEC Account Manager in the issue process, elements have issue sets that contain the information required to issue key. These issue sets contain a list of keys, the fill devices, and other required parameters for issue actions the COMSEC Account Manager handles on a regular basis. This eliminates the need for routinely entering the same requests for issue. The issue function contains most of the processing required to prepare key material for fill. This includes removing a key from local storage, mapping the key to its ECU, preparing the key for acceptance, transmission, and loading it into the ECU.

3-4. A local element initiates the LCMS key distribution process by requesting a specific key or issue set. The key filling function moves the key into ECUs. The exact process to load (fill) key into an ECU varies, based on the ECU and the transfer device used.

DISTRIBUTION EXECUTION

3-5. The key distribution method depends on the media type and the sending and receiving local elements capabilities. Key transfers may be in hardcopy form, on magnetic media, in a fill device, or over a communications channel. The media for a key transfer depends on the current storage media of the key. When storing a key electronically, an operator may transfer via a communications channel, magnetic media, or in a fill device.

3-6. A key may be distributed using over-the-air distribution procedures, over-the-air rekeying, and over-the-air transfer at any time during its effective cryptographic period, or the immediately preceding cryptographic period. Before transmitting the key, the network control station notifies all recipients, via a secure communications link (for example; voice, record message), outlining the details of the key to be transmitted. This notification includes the following information—

- Transmission of time key.
- Identity of the circuit on which key will be sent.
- Destination instructions for recipients (for example, device or circuit for the intentions of the key).
- Identity of the key including short title, classification, effective period, and controlling authority.

3-7. Following key distribution from any source other than the local management device into a modern fill device or ECU, the recipient acknowledges receipt of the key by signing local custody documents. Minimum accounting information for the key includes—

- Short title or designator.
- Classification.
- Date of generation and loading.
- Date of issue or transfer.
- Identity of issuer and recipient.
- Controlling authority of key.
- Effective period of key.

KEY WRAPPING AND DISTRIBUTION TECHNIQUES

3-8. Over-the-air rekeying changes the traffic encryption key, or the transmission security key (TSK) in remote cryptographic equipment by sending new key. Over-the-air transfer electronically distributes a key without changing the traffic encryption key used on the secured communications path over which the transfer is accomplished.

3-9. The National Advisory Group (NAG) is the standard user manual for planning and conducting electronic key generation, over-the-air rekeying, and over-the-air transfer. Procedures detailed in this section supplement those contained in NAG-16F, and provide standardization within the Army. NAG-16F provides detailed instructions on the following—

- Over-the-air rekeying and over-the-air transfer communications procedures using the modern fill device.
- Allied over-the-air rekeying doctrine.
- Use of inter-theater COMSEC package generic key as over-the-air rekeying and over-the-air TrKEK.
- Procedures for distributing key via Defense Switched Network, general service message system, or secure telephone equipment.
- Unsuccessful over-the-air rekeying situations.
- Late joiners to networks.
- List of approved 128-bit cryptographic-equipment.
- Procedures for transferring key and tag between modern fill devices via secure telephone equipment.

DEFENSE COURIER DIVISION

3-10. The U. S. Transportation Command Defense Courier Division (DCD) provides secure, timely, and efficient end-to-end global distribution of classified and sensitive material for the U.S. and its allies. Normally, regularly scheduled DCD missions allows for distribution of COMSEC material. U.S. Transportation Command Joint Directorate of Operations approves request for special mission to transport or ship COMSEC material before execution. The material eligible for shipment via the DCD is assigned one of two priorities in the defense courier service levels—

- Regular movement—represents the bulk of the material movement by defense courier. This material moves via regularly scheduled DCD missions. The majority of COMSEC material transport uses this method.
- Special movement—represents material moved expeditiously at the expense of the requesting command if regularly scheduled DCD missions cannot satisfy deadlines. The DCD may require the requesting customer to rendezvous with mission courier at a pre-coordinated site.

OVER THE AIR REKEYING

3-11. The variable generate option allows a simple key loader operator to generate a key with user-specific attributes. This over-the-air distribution option allows the operator to generate a key and store it in the simple key loader for later distribution to an ECU. The controlling authority authorizes use of the variable generate.

3-12. The variable update option provides the capability to send a key encryption key (KEK) to a device with variable update capabilities to perform a deterministic key update, and return the revised key to the simple key loader. The simple key loader retains both the original and updated KEKs. The original tag applies to the updated KEK, except the segment number and suffix fields, which are incremented by one.

3-13. The manual rekey option allows the network control station to send a traffic encryption key to the network members. The network control station contacts the network members and they prepare their equipment for receiving a traffic encryption key. The network control station informs network members on how and when to switch to the new traffic encryption key. Net members may delete the old traffic encryption key, depending on the equipment type. There are five important steps to perform before the manual rekey procedure. They include—

- Know the network control station KEK short title and text identity.
- Know the outstation KEK short title and text identity.
- Know what channel on the outstation's radio the traffic encryption key is going to be stored.
- Review all steps before performing the manual rekey operation.
- Know the new or replacement traffic encryption key short title and key attributes.

ENCRYPTED (BLACK) KEY DISTRIBUTION

Note. Encrypted key and black key are synonymous. Encrypted key will be used throughout the remainder of the document.

3-14. Encrypted key management provides an improved security posture by using locally generated TrKEKs. Additionally, the options for the distribution of black application keys add a degree of flexibility not otherwise available through current tier 3 operations. Encrypted key provides an additional layer of protection since it allows the key to be delivered to the ECU in an encrypted form, significantly reducing the risk of compromise. EKD provides improved security using locally generated KEKs. The distribution options for black application keys add a degree of flexibility not otherwise available. Common user application software developments compensate for shortcomings of the LCMS. These programs also consider the evolution of EKMS to KMI and have maximum portability design. Baseline software and hardware versions are required for encrypted key handling and distribution.

3-15. The required **baseline** software and hardware for encrypted key handling and distribution via the EKD process are—

- **LCMS v5.x**—the base line for Army encrypted key implementation is LCMS version 5.0.3 including the integration of common user application software on the LCMS workstation. LCMS provides for the management of electronic key, physical COMSEC materials, non-cryptographic services, and communications. **Local management device and key processor** is a classified device that performs all required cryptographic processing and access control services for the EKMS account.
- **ACES v1.9**—is an automated system for secure cryptographic network planning and distribution of communications materials, including COMSEC key tagging information, electronic protection materials and signal operating instruction. Encrypted key implementation requires the ACES version 1.9 (ACES v1.9 is the baseline version. Version 3.3 is the latest available software version.)
- **Common user application software v5.1**—is user application software that works together with the local management device and key processor platform. Common User Application Software interacts with LCMS and the key processor using the LCMS provided application programming interface.
- **Simple key loader (AN/PYQ-10C) v8.0**—receives stores, manages, and distributes electronic key for loading ECUs. The simple key loader also handles mission data distribution and loading for various systems (for example, hop-sets or loadsets). The simple key loader can also receive, store, distribute and display signal operating instruction information. The simple key loader is an enhanced version of the data transfer device, hosting user application software that is interoperable with common tier 3. The simple key loader can receive encrypted key downloads from the ACES workstation for subsequent loading into applicable ECU. The simple key loader is backward compatible with existing ECUs, and intended to be compatible with future security equipment and systems.

ENCRYPTED KEY OPERATIONS

3-16. Battalion or brigade signal staff officers and members of their COMSEC Staffs coordinate with and obtain assistance from appropriate sections or personnel to successfully conduct EKD missions. For example, the ACES terminals in most units are under control of the spectrum manager who uses ACES terminal for spectrum management operations. Battalion or brigade signal staff officers and staff coordinate with respective Spectrum Manager to use ACES terminal required to conduct EKD. Battalion or brigade signal staff officers and staff also coordinate with appropriate personnel to use SECRET Internet Protocol Router Network (SIPRNET) terminal on both the local end and distant end of EKD process. Units vary with respective force structure and modified table of organization and equipment requirements. Therefore, pertinent point of contact's are required for successful EKD operations vary in respect to unit structure.

3-17. The reconfiguration of the Army LCMS workstation to host common user application software and LCMS, coupled with the fielding of ACES v1.9, provide users the capability to deliver encrypted keys as encrypted key packages to tier 3 modern fill devices; thereby providing an enhanced capability not available in the previous LCMS workstation. Encrypted key packaging adds an additional layer of security for key distribution by preventing compromise, and adds the capability of securely distributing relatively large amounts of key between elements.

3-18. Current AKMS operations limit key distribution options. Key can be moved between LCMS workstations via standard EKMS connectivity in quantity, but movement of key from the LCMS workstation to a ECU requires tier 3 (modern fill devices or simple key loader) devices. The key moves between tier 3 devices using secure communications links. ACES workstations do not currently handle key, with the exception of TSK for a few selected systems.

3-19. The ACES workstation enhancement allows the import of encrypted key received from an LCMS workstation. This encrypted key handling capability facilitates distribution of encrypted key between ACES workstations and downloading to the simple key loader. ACES workstations are more widely distributed than LCMS workstations enhancing significantly to key distribution options throughout tactical echelons. More ACES workstations provide the ability to get the key closer to the point of use.

3-20. The reconfigured LCMS workstation, hosting both LCMS 5.x and common user application software 5.1, provides the capability to issue wrapped products in an ECU KEK for distribution to a compact disc (CD). The ACES workstation manually receives this encrypted key package stored on a CD for import and subsequent processing. The encrypted key packaging capability available in LCMS 5.x and common user application software 5.1, coupled with the capability incorporated in ACES v1.9, satisfies the encrypted key handling requirement for mode 5 identification friend or foe (IFF). The following paragraphs describe receiving, managing, and distributing the red and encrypted key.

3-21. Encrypted key packaging in LCMS 5.x starts with the receipt and identification of the red key from the NSA central facility. Distribution via EKMS to each COMSEC account requiring a specific key normally occurs on a regularly scheduled basis. At the unit COMSEC account level, COMSEC planners determine the best method for distributing required key to all supported ECU platforms. Depending on the deployment scenario, this may involve distributing a single encrypted key package to one ACES workstation, or multiple packages to multiple ACES workstations. Planners also decide key distribution quantity. Under some circumstances, only a limited quantity of future key may be distributed.

3-22. The next step in the process involves the LCMS workstation operator generating a red symmetric key. The symmetric key serves as the ECU KEK for an ECU. This step involves generating the appropriate KEK in LCMS via the symmetric key option.

3-23. Using the common user application software operators perform issuing of keys encrypted by the red symmetric key. Using the local element issue setup procedure, and then performing routine issue of encrypted electronic keys via CD, the LCMS workstation operator selects the keys to encrypt, select the red KEK to use for encryption, and distribute the resulting encrypted key package to a CD. The encrypted key, wrapped in the symmetric key, is ultimately loaded into the ECU. The ACES workstation imports encrypted keys from the CD and transfer them to a simple key loader for distribution and loading into the ECU.

3-24. COMSEC planners make provisions to distribute the red KEK to each ECU. The only means for red KEK distribution is via the simple key loader, and there are several possible scenarios for delivery of the key. For IFF mode 5, NSA has granted approval to distribute the red KEK in the same simple key loader used to distribute the encrypted key. Distribution and redistribution requirements for the key directly relate to individual ECU mission requirements. The ACES workstation operator receives the simple key loader containing the red KEK to allow for download of the encrypted key and further distribution of all keys to ECUs. The operator may distribute the red KEK separately to the ECUs. Once the red KEK is distributed and loaded in the targeted ECU, the unwrapping of encrypted key can occur.

3-25. Encrypted key may have classified or sensitive data (such as header or tagging information) associated with it. The associated data may be encrypted or unencrypted. If the associated data is unencrypted, the entire data package is sensitive or classified. When possible, the equipment systems security doctrine or applicable classification guidance specifies the sensitivity of the associated data. The NSA, with the controlling authority and user community, makes this determination.

ENCRYPTED KEY DISTRIBUTION VIA SIPRNET

3-26. Generic EKD facilitates the distribution of electronic key using LCMS, ACES and a SIPRNET platform. It is the method of distribution for all encrypted key packages loaded into the ECU. EKD requires an accountability audit trail for electronic key distribution using the electronic key management worksheet in TB 380-41 appendix D. The EKD process varies somewhat when applied to Advanced Extremely High Frequency, Blue Force Tracking, and IFF Mode 5. Each of the three process variations are specific to either Advanced Extremely High Frequency, Blue Force Tracking, and IFF Mode 5. Appendix B of FM 6-02 covers the three processes.

ECU TRANSMISSION OF ENCRYPTED DATA

3-27. Encrypted key, encrypted software, and other encrypted data may be sent via means authorized for UNCLASSIFIED or FOR OFFICIAL USE ONLY data such as secure internet protocol router network. Encrypted key is not considered cryptographic. After receiving and decrypting a data package containing encrypted keying material, no further accounting for the original encrypted data package is necessary.

3-28. The decrypted keys become cryptographic and subsequently safeguarded, controlled, and accounted for according to the procedures for red key. Unencrypted keying material intended to encrypt operational data remains cryptographic and is accountable for in the COMSEC material control system.

Note. Decrypted keys are accountable in the COMSEC material control system. Keys decrypted in a machine from which unencrypted key cannot be extracted (such as benign fill equipment) does not require additional accounting.

DESTRUCTION

3-29. Destruction of red key on removable media, unless offloaded to another device or to other approved media, may only be accomplished after the last key on the media has been superseded. Destruction of encrypted electronic key with an associated KEK may be accomplished by zeroizing (or the equivalent) all copies of the KEK. Zeroize include overwriting the key. Zeroize the KEK as soon as practical.

Note. Destroy all unencrypted (red) copies of electronic keys within 12 hours following supersession. Storage media having held keying material marked cryptographic is reusable, but it retains the highest classification of any key previously held. Remove the cryptographic caveat if the media is either degaussed using an approved device, or overwritten using an NSA-approved procedure (Approved procedures are contained in NSA/Central Security Service manual 9-12, Storage Device Declassification.)

TRANSFER KEY ENCRYPTION KEY MANAGEMENT

3-30. The TrKEK encrypts keys during transfer from a local management device and key processor to a modern fill device; between modern fill devices via secure telephone equipment; or other NSA-approved over-the-air distribution devices and methods. The receiving secure data system or simple key loader needs TrKEK loaded to decrypt the traffic encryption key or KEK for use in the ECU.

3-31. Managing and accounting for the TrKEK used to encrypt and decrypt user key is at the tier 2 account, except when the local element issues the TrKEK to an end user. Then the local element manages and accounts for the TrKEK on an electronic key management worksheet. An LCMS operator can generate and distribute TrKEKs based on cryptographic network or unit design. A TrKEK's cryptographic period may be quarterly or yearly.

3-32. The cryptographic period is quarterly when utilizing a TrKEK in a large network, or transmitting its associated encrypted key via secure means other than the secure telephone equipment or other approved device. The yearly cryptographic period should be used only if a TrKEK is utilized in a small network (for example, within one COMSEC account), and its associated encrypted key is transmitted via a secure telephone equipment or other approved device. Do not store key longer than one year in the secure data system or simple key loader. TrKEKs are classified the same as the highest classification of key they encrypt.

FILL DEVICE TRANSFERRING

3-33. Pre-placement of TrKEKs are in the receiving secure data system or simple key loader. Do not send TrKEKs unencrypted via secure telephone equipment secure mode except in an emergency. No more than one-year worth of TrKEKs may be pre-placed.

3-34. If a remote activity holds at least two secure data system or simple key loaders with distinct TrKEKs that supersede on different dates, it need not return its secure data system or simple key loaders to their supporting local management device and key processor for periodic TrKEK replacement. The site may transfer the new TrKEK from one secure data system or simple key loader to another via over-the-air transfer from the supporting local management device and key processor. The receiving secure data system or simple key loader can extract new TrKEK. This practice can continue indefinitely.

CAUTION

Do not attach universal serial bus devices to the secure data system or simple key loader during red key transfer through the fill port.

TACTICAL LOCAL AREA NETWORK ENCRYPTION FIELD TAMPER RECOVERY TO TACTICAL LOCAL AREA NETWORK ENCRYPTION SUPPORT

3-35. Ship the field tamper recovery cryptographic ignition key separately from its associated tactical local area network encryption. Property book officers turn in tactical local area network encryptions through normal installation supply support channels for shipment to the Tobyhanna Army Depot, according to AR 710-2.

JOINT/NORTH ATLANTIC TREATY ORGANIZATIONS/COALITION OPERATIONS

3-36. The joint force commander may direct establishment of a Joint Theater COMSEC Management Office to provide long-term COMSEC material support in the area of operations. Combining a Marine Corps COMSEC management office and an Army theater COMSEC management office with other COMSEC personnel of the Air Force, Navy, Coast Guard or elements thereof forms this facility. This structure is not finite and may be task organized in any combination. The Communications Electronics Directorate COMSEC planning and management section administratively controls the Joint Theater COMSEC Management Office.

3-37. The Joint Theater COMSEC Management Office provides a forward-deployed COMSEC management office capable of storing, maintaining, distributing, destroying, issuing, processing, and transporting large amounts of COMSEC material in the area of operations. Each unit commander should be prepared to initiate required COMSEC agreements with the Joint and Army Theater COMSEC Management Office, or the Marine Corps COMSEC management office to prevent a potential gap of vital physical or electronic keying material required to support their operations.

3-38. Units deploying with COMSEC accounts to Southwest Asia should contact the Joint Theater COMSEC Management Office for coordination. The office provides oversight for all theater account, keying material to deploying accounts, processes and aids accounts with key ordering requests, and keying material disposition to accounts. The Joint Theater COMSEC Management Office will aid accounts with DCD shipments while in theater. The management office receives equipment and physical COMSEC material for accounts, and serves as the central distribution point for a replacement LCMS or local management device and key processor (KOK-22A). COMSEC Account Managers will consider suspending key material not needed in theater until shortly before they redeploy to home station in order to prevent accounting for, storing and destroying extra COMSEC material.

3-39. North Atlantic Treaty Organization and coalition operations require communications interoperability. The servicing COMSEC management office will provide policy and procedural guidance to the command for releasing COMSEC material and controlled cryptographic item to North Atlantic Treaty Organization coalition forces. All COMSEC keying material and equipment that require a transfer to coalition forces and NATO allies requires HQDA G-2 approval. Identify cryptographic systems in operation orders, signal operating instructions, and related documents as necessary to support joint operations. Establish eligible coalition partners as local element hand receipt holders according to national policy, regulations and guidelines.

EXERCISE AND DEPLOYMENT COMMUNICATIONS SECURITY SUPPORT

3-40. Upon notification of a pending deployment, the commander needs to determine if the unit shall deploy with or without its COMSEC account. To assist the commander of the deploying unit in finalizing unit

deployment plans, and assist the commander in determining the operation conditions and assigned mission, the commander of the deploying unit should—

- Coordinate with the Army command.
- Coordinate with the Army Service component command, or direct reporting unit assistant chief of staff, intelligence and assistant chief of staff, operations.
- Coordinate with the combatant commander gaining command assistant chief of staff, intelligence and assistant chief of staff, operations.

3-41. Refer to TB 380-41 for the procedures to move a COMSEC account. In addition to the guidelines for moving an account, each deploying unit prepare a detailed standard operating procedures for deploying and operating its COMSEC account while deployed, tailored to its own distinct situation.

3-42. The commander decides how material will go forward with the deploying account (packaged and escorted [courier] at the time of unit's deployment by COMSEC personnel, or shipped separately to the new destination via the DCD). If the material moves via separate shipment through the DCD, the COMSEC Account Manager contacts the supporting COMSEC management office in theater before deploying and before shipping COMSEC material. The COMSEC Account Manager coordinates with the servicing COMSEC management office to receive and secure the incoming DCD shipment until the unit arrives.

3-43. When preparing COMSEC material for shipment, whether by escort or DCD, all material is packaged properly and addressed to identify the property owners' account (refer to TB 380-41 for shipping instructions). If a deployed unit establishes a fixed COMSEC facility at the deployment location, a new COMSEC facility approval request is required when the account arrives at its new location.

Chapter 4

Accounting

This chapter addresses hand receipting communications security material, issuing keys to local element, key management system certificate management, compromise recovery, and managing two-person integrity for communications security support.

HAND RECEIPTING COMMUNICATIONS SECURITY MATERIAL

4-1. Accounting is creating and maintaining records of the status of accountable items (COMSEC material) and the exchange of data contained within these records. The LCMS creates and maintains records of accountable items, and manipulates and modifies data contained within these records. Accountable items include traditional and modern key, COMSEC equipment (classified or CMCS controlled), and COMSEC aids; such as operating and maintenance manuals and other items as defined according to AR 380-40.

ISSUE KEY TO A LOCAL ELEMENT

4-2. National policy does not allow a tier 2 COMSEC account to transfer keying material to a tier 3 account. This section addresses issuing and hand receipting electronic key and COMSEC material from an AKMS account to a local element hand receipt holder.

4-3. The commander or designated representative may designate an individual as a COMSEC local element hand receipt holder, provided the individual has a valid need for the material. The local element hand receipt holder is a U.S. citizen, or a legal U.S. resident alien, with the necessary security clearance and the means (facilities) to properly secure and protect the material. This includes U.S. Government contractors providing services to U.S. military organizations, whether in continental U. S. or at overseas U.S. installations. In the absence of the COMSEC Account Manager, Primary Alternate COMSEC Account Managers may not issue COMSEC material to individuals not previously authorized as a local element hand receipt holder without prior approval from the commander or equivalent.

4-4. Hand receipting COMSEC material from a COMSEC Account Manager to a local element hand receipt holder transfers and delegates responsibility for the COMSEC material to the local element hand receipt holders. The COMSEC Account Manager retains overall accountability to the central office of record for that material. Hand receipted material is controlled at all times, until returned to the COMSEC Account Manager or otherwise properly disposed of and reported to the COMSEC Account Manager.

4-5. When issuing COMSEC material to a local element hand receipt holder, a LCMS-generated standard form (SF) 153, COMSEC Material Report accompanies the material. The material may remain on a hand receipt for either a specific or an indefinite period. SF 153 hand receipts remain valid for a period of up to two years. When a local element hand receipt holder accepts possession of the material, they assume full responsibility for safeguarding it according to AR 380-40 and TB 380-41. Transfer COMSEC material between accounts and document as an account-to-account transfer. A COMSEC account may not treat another account as a local element hand receipt holder. Under unusual or emergency conditions (for instance, when a tactical mission is affected) utilize forms other than the SF 153, providing they contain the basic information listed on the hand-receipted item.

4-6. The COMSEC Account Manager ensures all local element hand receipt holders are properly educated on the safeguarding, destruction, inventory and operating instructions for the material provided. Local element hand receipt holders receive a COMSEC briefing and cryptographic access briefing as required and sign attesting completion of briefing.

4-7. Local element hand receipt holders for SECRET and Top Secret (TS) material maintain security clearances and enroll in the Department of the Army Cryptographic Access Program. Two personnel (the

local element hand receipt holder and a cleared witness) also signs the SF 153 for all TS material issued by the COMSEC Account Manager in order to maintain two-person integrity controls.

- 4-8. Before taking possession of the material, the receiving local element hand receipt holder—
- Inventories the material against the LCMS-generated SF 153.
 - Verifies the presence of all pages of unsealed key material and publications, or verify presence of all electronic keying material received into a modern fill device or simple key loader.
 - Corrects the SF 153, if necessary, and initials all corrections.
 - Has a second authorized individual sign block 16 when receiving TS material from the COMSEC Account Manager to meet two-person integrity requirements.
- 4-9. The issuing COMSEC Account Manager keeps the original SF 153. The local element hand receipt holder receives a duplicate copy and disposition records (DA Form 5941-R, COMSEC Material Disposition Record, or electronic key management worksheet) for material being used.
- 4-10. Both the issuing COMSEC Account Manager and the local element hand receipt holder maintain files that serve as the record of accountability and responsibility for material issued to a local element receipt holder. Upon return of the material, or verification of final destruction, the COMSEC Account Manager removes the original SF 153 from the file and returns it to the local element receipt holder. This indicates completion of, and closes the transaction. The local element hand receipt holder is not required to retain a file copy of the SF 153 (refer to TB 380-41 for all hand receipting procedures).

KEY MANAGEMENT SYSTEM CERTIFICATE MANAGEMENT

- 4-11. The EKMS use asymmetric FIREFLY keying to transfer keying material securely between elements. Each element uses a FIREFLY vector set that cryptographically identifies the element by its EKMS identification. This FIREFLY vector set is valid for one year from generation and operators may electronically rekey the set each year to remain valid indefinitely.
- 4-12. This vector set creates a set of FIREFLY credentials (public keys), which are the KEKs that protect transfers. These credentials are valid for one month, and the user can create a set of up to 12 upon command.
- 4-13. The controlling authority posts the credentials to the EKMS directory service, which is a repository for all EKMS elements' credentials. When a user needs to transfer keying material to another element, they connect to the directory service to download the distant end's credentials and account information. The local key processor uses the distant end's current public FIREFLY credential to encrypt the keying material. This process produces a bulk-encrypted transaction. The bulk encrypted transaction is sent to the distant end, where it is decrypted using the private key.

COMPROMISE RECOVERY

- 4-14. Compromised keys are vulnerabilities controlling authorities address immediately. The controlling authority should have a plan for replacing compromised key material. The plan must be realistic and the controlling authorities must be knowledgeable of appropriate times that keying material is due for replacement. The controlling authority immediately notifies all cryptographic network members when a network key is compromised, and determines whether to extend the cryptographic period of the network key or activate a replacement. All personnel who possess, handle, operate, maintain, or repair COMSEC material is familiar with, and follow, physical and cryptographic security policies and procedures. Report security violations to the COMSEC facility supervisor, COMSEC Account Manager, and commander. Undetected or unreported incidents or compromises are security violations that could possibly cause damage to national security.
- 4-15. Where substantial evidence exists of a COMSEC keying material compromise (electronically generated or hard copy), the controlling authority immediately announces precautionary supersession, and directs early implementation of an uncompromised replacement key. Immediately report emergency supersession of hard copy keys to the Communications Security Logistics Activity and NSA (I5107) so they can initiate resupply, produce replacement material, and correct status documents. The controlling authority directs reviews of any record traffic encrypted using the compromised keying material, when warranted.

MANAGE TWO-PERSON INTEGRITY FOR COMMUNICATIONS SECURITY SUPPORT

4-16. TS key protects the most sensitive U.S. national security information. Its loss to an adversary can compromise all of the information protected by the key. There is a significant body of information indicating that foreign intelligence Services consider TS key is a high-priority target for exploitation. For this reason, TS key receives special protection. Two-person integrity and no-lone zones meet this requirement. Violations of two-person integrity are reportable COMSEC incidents, as specified in AR 380-40 and TB 380-41, Chapter 6.

4-17. Two-person integrity is a system of storage and handling designed to prohibit individual access to TS COMSEC keying material by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the tasks being performed. Two-person integrity rules contained in this section may be modified for users operating in designated hostile fire, imminent danger, and combat zones (tactical situations), according to TB 380-41, Chapter 4 paragraph 4.1.3b.

4-18. Access to future editions of unencrypted keying material is limited to COMSEC account personnel until its issue for use. When an unencrypted key is stored electronically, use system or procedural safeguards to limit access to account personnel. Exceptions may apply to these access restrictions in tactical situations, when mission requirements dictate.

4-19. No-lone zones will be established whenever top secret key can be accessed from COMSEC equipment, either in physical or electronic form. A no-lone zone is an area, room, or space where no person will have unaccompanied access. A no-lone zone must always be occupied by 2 or more appropriately cleared people who can observe each other's actions. (Refer to AR 380-40 for more information on no-lone zone.)

PROTECTIVE TECHNOLOGY

4-20. NSA provides state-of-the-art tamper-revealing products for information processing equipment and keying material. The level of protection obtainable from these products depends almost entirely upon the inspection and control programs conducted by users. To ensure the integrity of protective technologies, the COMSEC Account Manager ensures personnel who routinely handle or use protectively packaged keying material or tamper-sealed information processing equipment receive training in the inspection and disposal of used protective technologies.

This page intentionally left blank.

Chapter 5

Cryptographic Network Planning

This chapter addresses cryptographic network establishment and planning, signal operations instructions, and loadset management.

ESTABLISHING CRYPTOGRAPHIC NETWORKS

5-1. The controlling authority considers which type of cryptographic network is most beneficial for the unit and establishes cryptographic network configurations at the minimum operational size necessary for the mission. Examples of cryptographic networks include satellite circuits, local area networks, wide area networks, and single channel radios. The controlling authority determines the number of key to issue to users. The controlling authority determines requirements based on the types of organizations requesting support for electronic key distribution. The operational security doctrine defines the national policy on types of keys, cryptographic network size, cryptographic periods, and key changeover times for equipment. Request operational security doctrine through Communications Security Logistics Activity.

5-2. COMSEC personnel utilize electronic key to establish cryptographic networks. Using the physical key for establishing cryptographic network is an exception and requires specific justification. The controlling authority is also responsible for advising all users, and Communications Security Logistics Activity, of disposition instructions of unused, cancelled, or superseded key.

PLANNING CRYPTOGRAPHIC NETWORKS

5-3. The component operations and G-6 network managers may have the responsibility for planning the networks that consist of transmission systems, circuit switches, data switches, router, and other devices. The signal unit has responsibility for engineering the networks. The network managers consider such things as the objective of the mission; what units will participate in the mission; what type of communications will be required; the duration of the mission; and many other areas of mission interest. The establishment of a cryptographic network involves identifying individual or operational requirements in a command or unit. The cryptographic network elements intercommunicate in a secure mode; and all networks must possess compatible equipment and associated key material.

5-4. The network manager develops an operation order or communications plan for unit missions. The ACES operator receives the operation order or communications plan to develop a cryptographic network plan.

5-5. The ACES operator develops a cryptographic network overlay for the mission based on the operation order, and or communications plan, and identifies COMSEC requirements. The ACES software architecture provides the ability to tailor the software loaded on the ACES workstation to meet a variety of planning requirements. The three network categories are combat network radio, area common user system, and general purpose. Within each network category there is a planning module.

5-6. The general purpose planning module application will develop a cryptographic network overlay for the mission based on the communications network. Identify and process key requirements through the general-purpose module application. The general-purpose cryptographic networks exist independently of other networks. This provides the capability that manually creates special purpose cryptographic networks to meet any distinct need. The ACES operator will deliver key requirements to the COMSEC Account Manager.

5-7. The local management device and key processor operator processes key requirements; provides the necessary short title information concerning each key to add to the ACES cryptographic network overlay; and passes this information to the ACES operator. When the plan is complete with the short titles, the COMSEC Account Manager returns the cryptographic plan to the ACES operator. The ACES operator

finishes processing the cryptographic network, and provides the entire cryptographic network plan along with SOI and loadset data to the tier 3 users. The COMSEC Account Manager generates and distributes red key to the end user by loading keys into the user's modern fill device at the tier 3 level. The end user then keys the ECUs from the modern fill device. .

SIGNAL OPERATIONS INSTRUCTIONS AND LOADSET MANAGEMENT

5-8. The corps G-6 spectrum manager generates and disseminates the data, or may delegate those responsibilities to subordinate divisions. The G-6 COMSEC personnel can generate SOI data, COMSEC data, and the corps' traffic encryption key. The G-6 COMSEC personnel also generate frequency hopping data, corps-wide hop-sets, network identity, and the corps' TSK.

5-9. The division G-6 COMSEC personnel either use the data the corps generates, or if authorized generate their own frequency hopping and COMSEC data. The division has the equipment and capability to generate and merge SOI data. The division G-6 can also generate COMSEC data (division traffic encryption keys and generate frequency hopping data, network identity, and division TSKs).

5-10. Echelons below division do not normally generate SOI, traffic encryption keys, TSKs, and network identity assignments. The exceptions are when brigade and separate battalion operators have authorization to generate traffic encryption keys to meet emergency requirements. When lower echelons generate traffic encryption keys, they process through higher headquarters to the controlling authority for consolidation.

5-11. The brigade receives SOI, frequency hopping, and COMSEC data from the division. The brigade is primarily responsible for SOI data and preparing loadsets. The brigade tailors the SOI for organization usage, generates company-level KEKs, and develops loadsets.

5-12. The battalion and subordinate units are recipients and users of generated data. Their responsibilities are limited to distributing SOI data, distributing loadsets, including Zulu time, and loading data into radios. Most echelons can distribute frequency hopping and COMSEC data using physical or electronic means.

5-13. Upon notification of a possible joint contingency mission planning and operations, identify organizational tasks along with helping commanders fine tune and determine the unit and user needs. Concurrently, G-6 frequency managers coordinate with higher-level frequency managers to obtain usable frequencies.

5-14. COMSEC personnel generate mission-specific TSKs, and disseminate them through spectrum managers to the supporting forces. A separate message indicates specific TSK usage. During this time, COMSEC Account Managers coordinate COMSEC key requirements and produce a COMSEC callout message to identify specific keys for joint, Army Forces, corps, or division use. As Army Forces and subordinate units identify specific network requirements, they compile a master network list. Upon receipt of approved frequencies from G-6, the ACES operator generates SOIs for use by Army forces.

5-15. Army spectrum managers pass a list of units and networks supporting joint operations to the communications-electronics directorate. Once the communications-electronics directorate provides frequency hopping data to the G-6, the G-6 will disseminate the data to subordinate commands and each level will prepare loadsets. Files may transfer back to the next higher level at this point for archives. Receipt of the COMSEC callout message and specific TSK use message will effect finalization. Prepared SOIs may be passed to subordinate units by secure electronic or physical means. Time, distance, operational security, courier personnel security, and urgency dictate the most appropriate means of distributing data.

Chapter 6

Cryptographic Devices

Network managers maintain awareness of all cryptographic devices in their networks. During their lifecycle, modern cryptographic devices may require software updates. Network managers should track all software versions installed in end cryptographic units to ensure compatibility, to facilitate planning and scheduling. This chapter addresses end cryptographic unit software upgrade planning and periodic tamper checks of end cryptographic units.

END CRYPTOGRAPHIC UNIT SOFTWARE UPGRADE PLANNING

6-1. A software upgrade may be required for compatibility, to enhance function, or to meet mission needs. Mandatory software upgrades are available for download from the Army Key Management Portal website. Install mandatory software upgrades to assure compatibility and continued operation.

6-2. The best verification is for the system owner to confirm the software and device performs as expected in the system. The Army Cryptographic Modernization website maintains roadmaps of planned software upgrades and releases by equipment family and type. In the joint environment, where other services may be running different versions, the Army controlling authorities determine when and which upgrades to implement to minimize disruptions. Some cryptographic devices require crypto-ignition keys be installed in order for them to operate. Devices, which use an operator crypto-ignition key, must be checked to ensure the assigned crypto-ignition key is present.

6-3. There generally are four avenues for assistance outside of your organization—

- Communications Security Logistics Activity, AKMS and EKMS Help Desk (877) 896-8094 or Defense Switched Network 879-9900.
- Army Key Management Portal website.
- Item manager.
- Vendor customer support.

6-4. Notifications will be made via—

- DA message.
- Communications Security Logistics and TB announcement.
- Program management office web site announcement.

Note. Vendor software upgrades may require additional coordination through a COMSEC account after approval from the software engineering center.

CAUTION

Do not load a new vendor software upgrade from the Internet until the Army Service authority approves its use. Contact the wholesale inventory manager for the cryptographic device for guidance.

PERIODIC TAMPER CHECKS OF END CRYPTOGRAPHIC UNITS

6-5. All COMSEC devices require inspection for signs of tampering when delivered to a COMSEC account or property book officer, maintenance turn-in, upon re-certification, and during change of hand receipt holder or COMSEC Account Manager inventory. Visually inspect installed device by partially withdrawing it from its mount before the activation. Also visually inspect devices during command inspections. Report suspected tampering to the COMSEC Logistics Activity.

6-6. Below are examples and signs the device has been opened or an attempt has been made to open it. They include—

- Missing or loose screws.
- Bent, broken, or scratched metal access plates.

6-7. Tamper detection labels are damaged when—

- Missing, cut, or broken.
- Discolored.

6-8. Indicators and displays that indicate a possible tamper state of the device, such as when—

- Indicators may flash, or go out to indicate a tamper state.
- Display screen may indicate a tamper state.

6-9. All operational COMSEC devices subject to periodic recertification require validation. The COMSEC Account Manager determines which devices require certification. Apply tamper detection labels according to NSA instructions. Certifying activities record the serial numbers of the labels they apply to each device so the information is available to investigating elements if suspicion of tampering exists. Compare recorded serial numbers with those removed from each device if recertification is at the same facility two or more consecutive times. Report unexplained serial number discrepancies as COMSEC incidents.

6-10. Indicators and displays that indicate a tamper state may be false indications. Some devices will go into tamper mode if they lose external power while their internal battery is inoperable. It is important to know the possible reasons a device might indicate a tamper state. Notify the commander, supervisor, and COMSEC Account Manager when there is a tamper situation.

Chapter 7

Controlled Cryptographic Items

Controlled cryptographic item equipment requires access controls and physical protection against actions that could affect its continued integrity. This chapter identifies controlled cryptographic items, transfer of controlled cryptographic items between Army and Navy accounts, transfer of controlled items between Army and Air Force or other service or agency, and transfer of controlled items from Department of the Army activity address code accounts.

IDENTIFYING CONTROLLED CRYPTOGRAPHIC ITEMS

7-1. Controlled cryptographic items are unclassified COMSEC equipment that contains a cryptographic logic design. This design encrypts and decrypts classified and unclassified communications information. Controlled cryptographic item markings or labeling identifies items of COMSEC hardware, microcircuits to the end item, and assembly level when they are designated controlled cryptographic item by the NSA. Items designated controlled cryptographic item possess a classified cryptographic logic in their design. The hardware or firmware embodiment of that logic is unclassified but controlled. However, the associated cryptographic engineering drawings, logic descriptions, theory, or operation computer program and related source data remain classified (refer to AR 380-40, Chapter 8).

7-2. Keyed controlled cryptographic item assumes the security classification of the key and material or information it is protecting. Never handle or process keyed controlled cryptographic item through standard logistics systems. As a minimum, safeguard unkeyed controlled cryptographic item as sensitive valuable property. No security clearance is required for access to unkeyed controlled cryptographic item. However, access will be limited on a need-to-know basis to U.S. citizens. Non-U.S. citizens, including foreign nationals and immigrant aliens employed by the U.S., may be authorized limited access to controlled cryptographic item. Requests for granting such access is fully justified and based on operational need.

7-3. When keying controlled cryptographic item equipment, individuals loading the key, or otherwise operating the equipment, possess a security clearance, at least equal to the classification level of any key contained in the equipment. A security clearance is not required for visual access, if properly escorted.

7-4. Each Army activity receiving, storing, operating accounts for or otherwise handling controlled cryptographic item will establish a standing operating procedure for controlled cryptographic item (refer to AR 380-40). The standard operating procedures contain instruction to secure devices in a manner that precludes loss or compromise during operations.

7-5. The COMSEC material control system has a central office of record and COMSEC accounting infrastructure at depot, retail, and user levels. COMSEC Account Managers manage the system and are accountable officers as defined in AR 735-5. The Army does not maintain controlled cryptographic item material in COMSEC accounts. Property book officers account for the items through the standard logistics system in accordance with AR 710-2. Property book officers list all controlled cryptographic item class II and VII end items on formal accountable property records and send controlled cryptographic item transactions to the Army central database. The records list the items by serial number and item unique identification and sends records to the Army central database. The Army Material Command, Logistics Support Activity at Redstone Arsenal, AL manages the Army central database contract. Unless specifically defined for the U.S. government contractor or vendor in a U.S. government contract, controlled cryptographic item material ships to the appropriate supporting Army Department of Defense activity address code (DODAAC) or property book account.

7-6. All shipments of controlled cryptographic item material to the Army will go to an Army property book officers and DODAAC account. U.S. Government contractors or vendors will obtain a proper DODAAC for

the unit to ensure the proper shipment of controlled cryptographic item material. The transfer of controlled cryptographic item equipment from a contractor COMSEC account to an Army DODAAC/PBO property account is via a SF 153. Upon receipt of the controlled cryptographic item shipment, the receiving property book officer completes and signs the SF 153, and returns a copy to the originator. The Army property book officer maintains serial number accountability for all controlled cryptographic item.

7-7. The release of controlled cryptographic items is the responsibility of the Army Deputy Chief of Staff for Intelligence and Army Chief Information Officer. They share responsibilities and approval authority for the release of Army-owned COMSEC material to nonmilitary agencies, the general public, foreign nationals, or foreign governments. Submit release request through command channels to HQDA with justification. Personnel handling controlled cryptographic items should never package material for shipment in a keyed state. Before shipment, technically qualified and certified (on DD form 2625, Controlled Cryptographic Item [CCI] Briefing) individuals ensure equipment is zeroized (unkeyed) and batteries are removed.

TRANSFER OF CONTROLLED CRYPTOGRAPHIC ITEMS BETWEEN ARMY AND NAVY ACCOUNTS

7-8. The Navy tracks controlled cryptographic items in the COMSEC material control system, and only allows valid EKMS account numbers in the form or to account block of transaction reports. DODAAC numbers are registered locally, and with the Navy tier 1 central office of record by the Navy COMSEC account as a user account.

TRANSFER OF CONTROLLED CRYPTOGRAPHIC ITEMS BETWEEN ARMY AND AIR FORCE OR ANY OTHER SERVICE AND AGENCY

7-9. The transfer of most controlled cryptographic item material from the Air Force to the Army processes from the Air Force Equipment Management System to the Army property book officer, and should not involve the Air Force COMSEC account. However, the Air Force does require some equipment designated as controlled cryptographic item be controlled in the COMSEC account.

7-10. All Services, agencies, and organizations other than the Army and Air Force utilize the COMSEC material control system in order to account for all controlled cryptographic item material. When properly authorized, direct transfer of controlled cryptographic item material between the COMSEC accounts of agencies, Services, and organizations occurs other than to the Air Force or Navy.

7-11. Transfers of COMSEC equipment, including controlled cryptographic item, from Army elements to any other Service, agency, or organization, including NSA requires HQDA approval and authorization in writing by the Wholesale National Inventory Control Point, Inventory Manager. AR 700-131 provides Army procedures to request approval for the loan of controlled cryptographic items.

TRANSFER OF CONTROLLED CRYPTOGRAPHIC ITEMS FROM ARMY DEPARTMENT OF DEFENSE ACTIVITY ADDRESS CODE ACCOUNTS

7-12. Transfers to other Services and agencies use the military standard requisitioning and issue procedure and documentation. Receiving agencies accounting for controlled cryptographic item in the COMSEC material control system will bring the equipment into their COMSEC account, with a SF 153, using the military standard requisitioning and issue procedure shipping or transfer voucher from the Army DODAAC account as a supporting document to the SF 153 prepared by the receiving account.

Chapter 8

Key Management Infrastructure

Joint Department of Defense Services and Agencies developed Key Management Infrastructure as a replacement system for the electronic key management system. This new system has begun fielding and provides a means for a more secure generation, production, distribution, management, and auditing of cryptographic products (such as public key certificates, asymmetric key, traditional symmetric keys, manual cryptographic systems and cryptographic applications). This chapter provides an overview of the Key Management Infrastructure roles and responsibilities and system capabilities.

KEY MANAGEMENT INFRASTRUCTURE ROLES AND RESPONSIBILITIES

8-1. KMI manager roles permit access controls to perform a prescribed set of role-defined activities according to specific privileges of that role. An individual KMI manager may have privileges in multiple roles. KMI uses a role based operations process where assigned user roles control privileges. During the enrollment process, each user is designated a particular role or set of roles to perform through use of a token, a portable cryptographic universal serial bus form factor hardware module that provides type 1 services, such as digital signatures, signature verification, encryption, and decryption. The following are some of the KMI manager roles (all are external operational management roles)—

- KMI operating account manager is the accountable officer responsible for KMI operating account including the distribution of keying material and products from the Management Client to the ECU and fill devices. The KMI operating account manager is responsible for management and accountability of all keying material and physical COMSEC materials (accountable in the COMSEC material control system from receipt or production to destruction or transfer to another KMI operating account). The KMI operating account manager is the KMI equivalent of a COMSEC Account Manager.
- KMI Operating Account Registration Manager is responsible for registering KMI operating account.
- Command authority is responsible for the request on behalf of a department, agency, or organization to create partition codes for creation of modern keying material. Command authorities may delegate, through the Management Client, privileges to specific user representative (who are product requestors) to request product and services, maintain and update the account distribution profile on behalf of the command authority.
- Controlling authority is responsible for directing the operation of a cryptographic network using traditional key, managing the operational use and control of keying material assigned to the cryptographic network. The controlling authority receives EKMS and KMI identifications and registrations in KMI. Controlling authorities may delegate, through the Management Client, privileges to specific product requestors to request product services, maintain and update the account distribution profile on behalf of the controlling authority.
- Product requestor may request products and services, maintain and update the account distribution profile on behalf of a controlling authority (for traditional key) and command authority (for modern key).

8-2. KMI uses role exclusion. Role exclusion prevents an individual user from performing roles in one specific process from performing functions related to them as a user. The three categories of KMI role exclusion include lifetime, concurrent, and limited exclusion.

SYSTEM CAPABILITIES

8-3. KMI is a single, automated, network-accessible, electronic-based key management system, and a predominantly electronic cryptographic product delivery infrastructure. KMI consists of nodes. The central services node provides central security and data management services, and the product source node provides central generation of cryptographic keying material. The primary services node handles product ordering, management and distribution. The client node enables customers to access primary service nodes to obtain products and services to generate, produce, and distribute symmetric key products. The client node consists of a user workstation with specific KMI software and may include an advanced key processor.

8-4. Additional nodes exist within the KMI. The delivery-only client node is the KMI Aware ECU that secures and authenticates information. The delivery-only client hosts a web browser application that enables authorized KMI user interface with the primary services node product delivery enclave to receive electronic key encrypted (wrapped) products. The management client node allows COMSEC Account Managers and KMI Operating Account Managers to operate KMI business processes. This node is a specific configuration of the client node that includes the client host platform component; a client advanced key processor component, and a high assurance internet protocol encryptor device. The client host only allows the KMI Operating Account Manager who does not require cryptographic capabilities by the product source node to perform their mission functions.

8-5. Nodes run in the background as users simplify interface processes through a single access point known as the KMI storefront. The KMI workstation is backwards compatible with the LCMS workstation allowing back and forth communication between through the storefront at the NSA. KMI accommodates three categories of users—

- Human users—
 - U.S. federal, state, tribal, and local governments.
 - Uniformed military service members.
 - Intelligence community.
 - Civil and law enforcement agencies.
 - Reserve components military forces.
 - U.S. allies and coalition partners.
 - DOD and civil agency-sponsored foreign nationals.
 - DOD and civil agency support contractors.
 - Industry partners.
- Software applications—
 - KMI software applications.
 - Mission support and management systems.
- Devices—
 - ECU.
 - Cryptographic product transfer devices.
 - Cryptographic authentication devices.

8-6. KMI supports the requirements for all cryptographic material needed to achieve information advantage. KMI supports the following systems and services—

- IFF.
- Electronic commerce and electronic data interchange with government and commercial partners.
- Secure e-mail.
- Wide-area network security.
- Wired telephony.
- Wireless local area network and data device encryption.
- Video teleconferencing.
- Virtual private networking technology.
- Backbone and link encryption.

- Secure tactical radio systems.
- Mobile radio and cell phones.
- Space systems.
- Global positioning system.
- Integrated Broadcast System.
- Global broadcast system.
- Weapon system mission planning systems.
- Minimum essential emergency communications network.

8-7. KMI supports initiatives to enable web applications that support logistics, personnel, administrative, and other enterprise information systems. KMI products necessary to perform the mission are available for operational use, including operations in a constrained environment (such as reduced bandwidth, combat, mobile units, forward deployment), whether planned or unplanned. KMI will comply with DODIN requirements.

PROVIDE CATALOG OF PRODUCTS AND SERVICES

8-8. The user community requires access to a library of KMI cryptographic product descriptions (with information regarding the correct usage of those products), KMI policy documentation, and other KMI technical information. Additionally, the users need a catalog that displays specific KMI products and services they can order.

8-9. KMI provides catalogs that include all currently available KMI products and services. The KMI will provide a user-tailored version of that catalog with descriptive information about cryptographic products the users may order and receive, via a common user interface.

PREPARE USER REQUESTS FOR PRODUCTS AND SERVICES

8-10. KMI addresses cryptographic product and service modernization, and is oriented toward modern information technology methods and network connectivity. For example, authorized KMI users have the capability of ordering products and services for multiple organizations (such as batch ordering). However, because some customers have operational or fiscal constraints, legacy capabilities will continue providing support, as needed, until the end of the legacy product's lifecycle.

8-11. Preparing request for products and services require—

- The ability to order via any connected network. The KMI manager client, operating over SIPRNET or Nonsecure Internet Protocol Router Network provides the means for users to order KMI-produced cryptographic products and services.
- KMI provide electronic forms for ordering products and services using a KMI manager client.
- KMI templates, or similar conventions, group products used together to prevent inappropriate orders.

REQUESTER NOTIFICATION

8-12. Upon receipt of a product request, KMI notifies users of its success or failure. Failure notifications include the feedback necessary for the user to determine the cause of the failure. The user measures the response interval from the reception of the request by the KMI to the end of the KMI response. This performance measure does not include communications delays outside the control of KMI.

MANAGE REQUESTS FOR PRODUCTS AND SERVICES

8-13. KMI managers (controlling authority and command authorities) require the ability to automate the approval of key material routinely required by KMI users and the ECU. KMI managers also require the ability to review and approve non-routine or unusual product requests.

8-14. KMI will—

- Allow KMI managers (controlling authority and command authorities) to establish priorities for KMI product and service production and delivery.
- Allow KMI managers to reallocate cryptographic material they control.
- Allow KMI managers to establish lists of pre-approved cryptographic products specific KMI users and devices can request.
- Identify user requests for cryptographic products outside the user's pre-approved list, and route these requests to the appropriate KMI manager.
- Provide KMI managers the capability to approve key authorization.
- Provide KMI managers an automated web-based tool to manage and track authorized key products.

PROVIDE STATUS INFORMATION TO USERS

- 8-15. KMI provides user-initiated status information. The status information requirements include—
- **Product Status Requests.** The KMI client node provides authorized and validated users their product request status. Status is available on any KMI product including—
 - User requests for products and services.
 - Product generation, distribution, and delivery.
 - Lists of KMI products for which the user is responsible.
 - Effective dates of cryptographic products.
 - Lists of compromised and superseded cryptographic products.

REPORT CAPABILITY

8-16. KMI client node provides standard report templates for KMI users. However, KMI users require the ability to create custom reports from the available data fields to meet the mission requirements.

PRODUCE CRYPTOGRAPHIC PRODUCTS

8-17. Cryptographic products secure communications, protect information, process data and provide information advantage. Additional cryptographic products include protected software that generates, regenerates, or processes keys and certificates.

- 8-18. KMI users should follow these requirements when producing cryptographic products—
- KMI provides key products for cryptographic devices.
 - KMI produces documentation (such as policy documents, equipment operator manuals, and specifications) needed to support the cryptographic user community.
 - KMI support the key product needs of the cryptographic modernization initiative h. ECUs can request either symmetric or asymmetric keys to support their operational needs.
 - KMI support customers' surge requirements in case of emergency supersession.
 - KMI produce type 1 certificates to support identification and authentication of an ECU, KMI nodes, and KMI managers (controlling authority and command authorities KMI operating accounting managers, product requestors, registration managers, and enrollment managers).

SUPPORT MULTIPLE CRYPTOGRAPHIC ALGORITHMS

8-19. KMI products protect information at all levels, from UNCLASSIFIED to TS or sensitive compartmented information, in network environments ranging from the public Internet to highly protected defense and intelligence networks. Non-DOD agencies, multinational, and coalition networks require a variety of releasable algorithms.

DELIVER CRYPTOGRAPHIC PRODUCTS

8-20. Key delivery is from the production source to the users (human users, software applications, and devices). Paper product deliveries begin at the production source and extend to the COMSEC account.

Electronic product deliveries start at the production source and extend to the user devices via communications channels outside the responsibility of KMI.

8-21. KMI requirements of delivering cryptographic products include—

- Providing common user interfaces.
- Interfaces supporting user-initiated product delivery. The user-initiated delivery will validate for integrity, thus ensuring the product requested is the product received.
- Delivering electronic cryptographic products using the following forms and methods—
 - A primary service node delivers key to the ECU over a network via benign techniques.
 - Benign and encrypted key delivery from a client to the ECU over a network.
 - Benign key delivery to the ECU via a fill device (no cryptographic processing takes place in the fill device).
 - Encrypted key and red key delivery to the ECU via a fill device.

Note. Benign delivery technique means that there is never an exposure of the key and encrypting key, except in a cryptographic boundary, and ideally only in the ECU. KMI provides in-stock physical products to the specified delivery service.

- Supporting electronic delivery of cryptographic products to support dynamic networks (such as swapping out the ECU), communities of interest, and changing operational conditions.
- Delivering the following cryptographic keys via various physical media (such as CD, universal serial bus, and smart card)—
 - Black cryptographic key.
 - Red cryptographic key.
 - Bulk-encrypted multiple cryptographic key editions.
- Clients are capable of operating at a minimum data rate of 9.6 kbps. A KMI-aware ECU is capable of operating at a minimum data rate of 9.6 kbps.

DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE SUPPORT

8-22. KMI provides two types of certificates—type 1 and DOD public key infrastructure. An ECU uses either a DOD public key infrastructure or a type 1 certificate, based on its design and the mission application. The design of a KMI-aware ECU requires a type 1 certificate to support cybersecurity component management operations. KMI managers performing ordering and management functions utilize a type 1 certificate. KMI managers who are performing delivery only functions only require a DOD public key infrastructure certificate.

8-23. KMI depends on the DOD public key infrastructure in three distinct ways—

- Coordinates the assignment of device identifiers.
- Supports the request and issue of DOD public key infrastructure certificates to a type 1 ECU (device) designed to use those certificates. These ECUs should be able to receive all DOD public key infrastructure support through the KMI.
- Relying party validate public key infrastructure certificates that authenticate individuals connecting to the KMI to retrieve products.

8-24. DOD public key infrastructure support requirements include—

- Interface with an authorized, authoritative naming source to obtain distinct identifiers for use in a type 1 ECU to support the issuance of either DOD public key infrastructure or type 1 device certificates.
- Interface with the DOD public key infrastructure enterprise system to request and deliver public key infrastructure device certificates to a type 1 ECU.
- Validation of certificates issued by the DOD public key infrastructure or KMI (for example type 1 certificates) to authenticate users seeking to retrieve encrypted products from the KMI, via an approved network (SIPRNET or Nonsecure Internet Protocol Router Network).

DISTRIBUTE CRYPTOGRAPHIC ALGORITHMS

8-25. KMI distributes new cryptographic algorithms and cryptographic applications securely. KMI supports software downloads, including algorithms. The software encryption is with an approved algorithm, and downloads using the approved cybersecurity management protocol. In capability increment two, KMI will not perform ECU configuration management. KMI will securely distribute new cryptographic algorithms and applications electronically to KMI users.

AUTOMATED ACCOUNTING PROCESSES

8-26. Current cryptographic management systems require labor-intensive procedures to ensure cryptographic product and equipment accountability. KMI establishes automated processes and procedures to reduce the labor spent on accounting.

- 8-27. KMI automated accounting processes consist of the following requirements—
- Automated accounting processes for accountable physical and electronic cryptographic products and equipment. The automated processes include, but are not limited to—
 - Automatic key receipting.
 - Inventory reconciliation.
 - Key destruction reports.
 - Reducing accounting material types to equipment and key only.
 - Consistently implementing accounting standards across KMI nodes and components.
 - Option to maintain centralized inventories.
 - Track benign products to the point of the first client node or ECU to retrieve these products from the primary services node.

CRYPTOGRAPHIC PRODUCT DESTRUCTION

8-28. A primary function of any KMI system is destroying expired or compromised cryptographic products. Certain cryptographic products (such as cryptographic keys stored in software by a KMI user) require local destruction by the KMI user. Other cryptographic products require the ability for remote destruction (or zeroize) by the KMI. Other cryptographic products require return to a designated destruction agent.

- 8-29. Cryptographic product destruction requirements include—
- Allowing KMI users to destroy cryptographic products locally, when policy allows.
 - Procedures for destruction of all cryptographic products created, used, and supported by the KMI.

RECOVER FROM COMPROMISE

- 8-30. There are two categories of keys and each may be compromised—
- KMI user keys.
 - Distributed infrastructure keys.

8-31. KMI user keys are those held by operational users. These keys are the most vulnerable to compromise, since they are the most numerous, and often placed in compromising situations subjected to overrun or loss.

8-32. KMI uses distributed infrastructure keys exclusively to secure all system components. Users cannot generate these keys locally or distribute to KMI users. These keys are less likely to be compromised, but their loss is generally more damaging since loss of a single distributed infrastructure key may compromise many KMI user keys (an unauthorized user using a KMI distributed infrastructure key could gain access to the KMI and all key products produced and distributed throughout the system).

- 8-33. Compromise recovery address the following types of compromises—
- Catastrophic (for example, a root certification authority or global network segment).
 - Localized (KMI client node, base-level network).
 - Discrete, isolated instances (individual cryptographic material components).

8-34. The following are the requirements to recover from a compromise—

- **Notice of symmetric key compromise.** The KMI will automatically respond to a symmetric key compromise when notified by a KMI manager (controlling authority). KMI will notify known recipients of the compromised symmetric key and identify the replacement key.
- **Asymmetric key compromise.** When notified of the compromise of an asymmetric key, the KMI shall provide an updated compromised key list for distribution via device rekey.
- **Initiate emergency key download.** When the KMI manager (controlling authority) initiates a recovery action, and the emergency key is available in the affected users' delivery enclaves for download, KMI will download the emergency key within the following times, measured from receipt of a valid download request from a KMI client node.

AUTONOMOUS OPERATIONS

8-35. Disruption of communications to deployed task forces and units are expected. Communications loss affects deployed task forces and unit capability to perform mission tasks using security-enabled applications. KMI provides cryptographic product provisioning capability to enable deployed units to conduct local mission tasking when reach-back communications to KMI elements are unavailable (such as when communications are lost or operational requirements dictate termination of all electronic transmissions).

8-36. KMI provides the capability for local symmetric key generation and encryption to support—

- Encrypted key fills.
- Benign fills.
- Key distribution.

KEY MANAGEMENT INFRASTRUCTURE CLIENTS

8-37. The KMI user community needs to minimize operations and maintenance costs, including client platform (such as computer workstation) procurement, maintenance, and operator training costs. KMI design supports migration from legacy key management systems (such as EKMS), while avoiding the need for multiple KMI clients at a single operational site and minimizing disruptive changes to the KMI human-machine interfaces.

8-38. KMI client requirements—

- **End user manpower.** KMI operates without increasing customer organizations' dedicated manpower requirements.
- **Non-dedicated KMI client.** KMI enables users to retrieve benign products using computer platforms not dedicated to KMI (they can be connected to both KMI and mission support networks).
- **Transition strategy support.** KMI supports a transition strategy that does not require new KMI clients to operate alongside legacy workstations, (EKMS local management device and key processor) at the same operational site. New KMI clients will support legacy workstation ECU requirements, so that new KMI clients may replace legacy workstations.
- **Standardized KMI human-computer interface.** KMI human-computer interfaces support common operational concepts for cybersecurity operation. KMI human-computer interfaces include the following features, when appropriate—
 - Common user interfaces (such as graphic user interfaces and character-based interfaces) across all new KMI user components.
 - Context-based help function.
 - Consistent use of terminology and screen layouts across all KMI user components to leverage using common user application software to the maximum extent possible.
- **Differentiate between error types.** KMI user devices differentiate between user data input errors and other errors. User data input errors result in error response messages that aid the user in correcting the error.
- **User interface definition techniques.** KMI use techniques such as human-machine interface prototyping and focus groups to obtain KMI user community feedback continually throughout implementation and fielding.

- **Local symmetric product support.** KMI client (KMI client and advanced key processor) supports local symmetric electronic key generation.
- **Local Service Node support.** KMI supports regional and local distribution of electronic key to KMI users and other clients through the network key management system.
- **Client to client distribution.** KMI provides for key distribution between the following clients—
 - KMI client to EKMS client.
 - EKMS client to KMI client.
 - KMI client to KMI client.
- **Dedicated KMI client.** KMI utilize dedicated KMI clients to perform key ordering, management, generation and wrapping or unwrapping functions over KMI-supported networks.

KEY MANAGEMENT INFRASTRUCTURE BENIGN FILL OPERATIONS

8-39. KMI's design support benign key operations, reducing the operational burden as compared with a current ECU and EKMS. The mechanisms in capability increment two are key loading initialization facility functions, and over the network keying to a KMI-aware ECU. Key loading initialization facility functions are modular to implement them at various locations (such as a separate key loading initialization facility workstation at a dedicated facility, on a KMI manager client and advanced key processor, or on a KMI operating accounting client and advanced key processor). The users of these clients have appropriate permissions to access and perform key loading initialization facility functions. This gives the Services maximum flexibility in deciding where to perform benign fill ECU registration and initialization.

8-40. KMI benign fill operations requirements—

- Device registration—KMI registers KMI-aware devices.
- Device initialization—KMI initializes KMI-aware devices following registration to obtain a KMI-aware state.
- Single trip—KMI provides electronic cryptographic products (including rekey) in a manner that requires a single trip from the product delivery point (such as a KMI client) through a fill device (such as a simple key loader, or secure data system to a KMI-aware ECU).

8-41. KMI provide user support—

- Twenty-four hours a day.
- Status information to support a Service-provided KMI help desk.

CONNECTED NETWORKS

8-42. Capability increment two provides key products ranging from UNCLASSIFIED to TS and sensitive compartmented information, either via a KMI client node or over the network keying services. Capability increment two only provides over the network keying services via Nonsecure Internet Protocol Router Network and SIPRNET to devices operating managed on those networks. In capability increment two, KMI clients deliver these products to supported devices operating on TS and sensitive compartmented information networks.

Glossary

The glossary lists acronyms and terms with Army, multi-service, or joint definitions, and other selected terms. Where Army and joint definitions are different, (Army) follows the term. The proponent manual for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ACES	Automated Communications Engineering Software
AKMS	Army key management system
AR	Army regulation
ATP	Army techniques publication
CD	compact disc
COMSEC	communications security
DA	Department of the Army
DCD	Defense Courier Division
DOD	Department of Defense
DODAAC	Department of Defense activity address code
DODIN	Department of Defense information networks
FM	field manual
ECU	end cryptographic unit
EKD	encrypted key distribution
EKMS	Electronic Key Management System
G6	assistant chief of staff, signal
HQDA	Headquarters, Department of the Army
IFF	identification friend or foe
KEK	key encryption key
KMI	Key Management Infrastructure
LCMS	Local Communications Security Management Software
NSA	National Security Agency
SF	standard form
SIPRNET	SECRET Internet Protocol Router Network
SOI	signal operating instructions
TB	technical bulletin
TrKEK	transfer key encryption key
TS	Top Secret
TSK	transmission security key
U.S.	United States

SECTION II – TERMS

Army Key Management System

(Army) The Army's implementation of the EKMS. It provides real-time electronic key generation, distribution and management of existing COMSEC material. AKMS provides compatibility and interoperability to systems within the Department of Defense. AKMS is made up of 3 components; Local COMSEC Management software, Automated Communications engineering Software, and the simple key loader. (AR 380-40)

automated communications engineering software

(Army) Automated communications engineering software is an Army-developed system. The combination of a platform Central Processing Unit (CPU) and the automated communications engineering software together comprise an automated communications engineering software Workstation. ACES software is not accredited separately from the Army-designated laptop computer it resides on. (TB 380-41)

common user application software

(Army) CUAS is a Government-owned User Application Software (UAS) that resides on the LCMS workstation. CUAS works in conjunction with the LMD/ KP, and interacts with the KP to facilitate creating and loading Black Key to removable media. (TB 380-41)

Communication Security Logistics Activity

(Army) The Communications Security Logistics Activity is the Army wholesale logistics manager for communications security equipment and keying material. The Communications Security Logistics Activity operates a national inventory control point, national maintenance point, central office of record for COMSEC centrally accountable material, and one of the primary tier 1 sites for the Department of Defense to administer the Electronic Key Management System. Communications Security Logistics Activity information security representatives in the continental U.S. and outside the Continental U.S., Europe, Korea, and Southwest Asia. Personnel assigned to these offices are available to provide on-site assistance to any communications security material user, communications security account manager, or property book officer, or to resolve problems related to account automation. (AR 380-40)

communications security

(DOD) The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (JP 6-0)

communications security account manager (formerly called communications security custodian)

(Army) The individual appointed, in writing, who is responsible for receipt, custody, security, accountability, safeguarding, inventory, transfer, and destruction of communications security material. (TB 380-41)

controlling authority

(Army) Designated official responsible for directing the operation of a circuit or cryptographic network and for managing the operational use and control of keying material assigned to a circuit or cryptographic network. (TB 380-41)

cryptographic network planning

(Army) Identifying those individual operating elements that must intercommunicate in a secure mode. Planning is conducted together with communications network planning to ensure compatibility and interoperability with joint organizations as well as Army commands. The cryptographic network is made up of elements that secure these networks. The establishment of a cryptographic network involves identifying individual or operational requirements in a command or unit. The cryptographic network elements intercommunicates in a secure mode and all nets must possess compatible equipment and associated key material. (TB 380-41)

end cryptographic unit

(NSA) the cryptographic solution requiring modern key material. (EKMS 004 Glossary)

Electronic Key Management System

(NSA) An interoperable collection of systems for planning, ordering, generation, distribution, storing, filling, using and destroying electronic key and management of other COMSEC material. (EKMS 004 Glossary)

FIREFLY

(NSA) Key management protocol based on public key cryptography. (Committee on National Security Systems Instructions No. 4009)

key encryption key

(Army) A key used to encrypt and/or decrypt other keys for transmission (re-keying) or storage. (TB 380-41)

local account

(Army) The term used to identify an account that provides communications security support to other commands or elements. More often than not, these commands or elements are organizationally subordinate to the account command and are called local elements (issuing and using). (TB 380-41)

modern key

(Army) a collective name for asymmetric key such as secure data network system FIREFLY key, and message signature key. It does not include the public key infrastructure system or keys. (TB 380-41)

no-lone zone

(Army) An area, room, or space which, when manned, must be occupied by two or more appropriately cleared individuals who remain within sight of each other. (Committee on National Security Systems Instruction No. 4009)

Public key infrastructure

(Joint) An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for Department of Defense functional enterprise programs, including generation, production, distribution, control, and accounting of public key certificates. (JP1-02)

secure data network system

(Army) A mission system that provides end-to-end security services for the exchange of data between automatic data processing systems over common carrier networks, where no security services are provided by the common carriers. SDNS is a subscriber of the EKMS services. (EKMS 004 Glossary)

traffic encryption key

(Army) A key used to encrypt plain text or to superencrypt previously encrypted text and/or decrypt cipher text. (TB 380-41)

transfer key encryption key

(Army) A TrKEK's purpose is to encrypt keying material for transportation between an LCMS workstation and its final destination where the key is "filled" into an ECU or SKL. The encrypted key may be Traditional Key, Modern Key (FIREFLY), other TrKEKs (to be filled later to sub-LE SKLs), or ECUKEKs. TrKEKs may be filled directly to an SKL from a KOK-22A/KOK-32, or issued to a Primary LE so that it may be further filled to a sub-LE's SKL. The quantity and classification of TrKEKs used by an account will be determined by mission and risk. Different TrKEKs for each subordinate element reduces risk of compromise and of unauthorized sharing of mission data and/or Crypto keying material between adjacent elements. (TB 380-41)

two-person integrity

(Army) A system of storing and handling designated to prohibit individual access to certain COMSEC keying material by requiring the presence of at least 2 authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the tasks being performed. (AR 380-40)

user

(Army) Individual responsible for the proper security, control, accountability, and disposition of the communications security material placed in his or her charge. A material user is known as a local element in the Electronic Key Management System infrastructure. (TB 380-41)

zeroize

(Army) To remove or eliminate the key from a cryptographic equipment or fill device. (AR 380-40)

References

REQUIRED PUBLICATIONS

These documents must be available to the intended users of this publication.

ADRP 1-02. *Terms and Military Symbols*. 2 February 2015.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 08 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available online: www.dtic.mil/doctrine/new_pubs/jointpub.htm.

JP 6-0. *Joint Communications System*. 10 June 2015.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: www.apd.army.mil.

AR 25-2. *Information Assurance*. 24 October 2007.

AR 25-55. *The Department of the Army Freedom of Information Act Program*. 01 November 1997.

AR 380-40. *Safeguarding and Controlling Communications Security Material*. 09 July 2012.

AR 700-131. *Loan, Lease, and Donation of Army Materiel*. 23 August 2004.

AR 710-2. *Supply Policy Below the National Level*. 28 March 2008.

AR 735-5. *Property Accountability Policies*. 10 May 2013.

AR 750-1. *Army Materiel Maintenance Policy*. 12 September 2013.

FM 6-02. *Signal Support to Operations*. 22 January 2014.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

TB 380-40. *Security: Army Controlling Authority and Command Authority Procedures*. 10 September 2012.

TB 380-41. *Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material*. 15 August 2013.

OTHER PUBLICATIONS

Committee on National Security Systems Instruction No. 4009. *National Information Assurance (IA) Glossary*. 26 April 2010. http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

EKMS 004. *Glossary of EKMS Terms*. 08 April 2011.

<https://www.iad.gov/KeySupport/documents.cfm?m9rwbTucdJkfjY0Cf+CLevnXjNCAI49ku1/6Xm62p1Y=>

NAG-16F. *Field Generation and Over-the-Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises*. May 2001. <https://csla.army.mil/Sections/COMSEC/DocNSA.aspx>

National Security Agency/Central Security Service 9-12. *Storage Device Sanitization Manual*. 15 December 2014.

https://www.nsa.gov/ia/files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf

PRESCRIBED FORMS

None

REFERENCED FORMS

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate (APD) web site: www.apd.army.mil.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DA Form 5941-R. *COMSEC Material Disposition Record*.

DD Forms are available on the Office of the Secretary of Defense (OSD) website: www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

DD Form 2625. *Controlled Cryptographic Item (CCI) Briefing*.

Standard Forms (SF) are available on the U.S. General Services Administration (GSA) web site:

SF 153. *COMSEC Material Report*.

www.gsa.gov.

WEB SITES

APD Web site at www.apd.army.mil

Army Key Management Portal at <https://www.kc.us.army.mil/KMhome.nsf/HomeFORM?openform>

Army Training Network at <https://atiam.train.army.mil/>

CADD AKO Doctrine Web site at <https://www.us.army.mil/suite/grouppage/125801>

Communications Security Logistics Activity Web Site at <https://csla.army.mil>

National Information Assurance Training and Education Center at <http://niatec.info/Glossary.aspx>

Program Executive Office Command Control Communications-Tactical at <http://peoc3t.army.mil/c3t/>

Project Director Network Enablers at <http://peoc3t.army.mil/nete/>

Index

Entries are by paragraph number.

A

AKMS, overview, 2-4
authority, command, 1-3
authority, COMSEC, 1-3
authority, controlling, 1-3
authority, service, 1-3

C

capabilities, KMI, 8-2, 8-3, 8-4, 8-5, 8-6, 8-7, 8-8
CCI, identifying, 7-1
CCI, transfer, Army-Air Force or other Service or agency, 7-2
CCI, transfer, Army-Navy, 7-2
CCI, transfer, from Army DODAAC, 7-2
certificate management, 4-3
common and modern fill devices, 2-1
common user software application, 2-2
compromise recovery, 4-3
COMSEC material, destruction, 1-2
COMSEC support, exercise and deployment, 3-7
COMSEC, introduction, 1-1
cryptographic network, establishing, 5-1
cryptographic network, planning, 5-1

D

distribution execution, 3-2
distribution planning, 3-1
distribution, black key, 3-3
distribution, defense courier division, 3-3
distribution, ECU transmission of encrypted data, 3-5
distribution, encrypted key distribution via SIPRNET, 3-5

distribution, OTAR, 3-3

E

EKMS, device generation and transaction authentication, 2-3
EKMS, overview, 2-1

F

fill device, transferring, 3-6

G

G-6, corps and division, 1-3

H

hand receipting, 4-1

I

interface, ECU, 2-1
interface, ECU, red fill device, 2-1
interface, key storage device-64A and cryptographic ignition key, 2-1
internal interface, 2-1

K

key issue, local element, 4-1
key modern, key generation, 2-5
key modern, local key generation, 2-1
key modern, operational key, 2-5
key modern, test key, 2-5
key modern, types, 2-5
key processor, 2-3

L

local management device, 2-2

M

maintenance, 1-1
management, SOI and loadset, 5-2
management, TrKEK, 3-6
managers, 1-3

managers, COMSEC account managers, primary and alternate, 1-3

O

operations, encrypted key, 3-4
operations, joint, NATO, and coalition, 3-7

P

physical material handling segment, 2-2
planning, ECU upgrade, 6-1

R

responsibilities, commander, 1-2
responsibilities, directors, agencies, commanders of army commands, installations, and activities, 1-2
responsibilities, KMI, 8-1
responsibilities, user representative and individual user, 1-4

S

S-6, brigade, 1-4

T

tamper checks, ECU, 6-2
techniques, key wrapping and distribution, 3-2
tier 0 central facility, 2-1
tier 1 central office of record, 2-1
tier 1 segment, 2-2
tier 2 COMSEC account management, 2-2
tier 2 LCMS workstations, 2-1
tier 3 user level management, 2-3
two-person integrity, 4-4

This page intentionally left blank.

ATP 6-02.75
17 August 2015

By order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

A handwritten signature in black ink, appearing to read "Gerald B. O'Keefe". The signature is written in a cursive style with a large initial "G" and "O".

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1521001

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).

