TECHNICAL REPORT

(U) CONCEPT OF OPERATIONS FOR THE KEY MANAGEMENT INFRASTRUCTURE, CAPABILITY INCREMENT TWO

Version 1.4

E001

IAMAC TECHNICAL TASK ORDER 2104

INFORMATION ASSURANCE MISSION ATTAINMENT (IAMAC) CONTRACT

MDA904-03-C-1074

Booz | Allen | Hamilton

900 Elkridge Landing Road
Linthicum, Maryland 21090

30 September 2005

This Page Intentionally Left Blank

KEY MANAGEMENT INFRASTRUCTURE

30 September 2005
Version 1.4

(U) KMI2212: Concept of Operations (CONOP) for the Key Management Infrastructure (KMI), Capability Increment Two (CI-2)

(U) This document states provides a system overview and also specifies functions for ordering, distributing, and other managing products and services

I56
KMI Program Management Team
NATIONAL SECURITY AGENCY
9800 Savage Road STE 6751
Ft. Meade, MD 20755-6751

TABLE OF CONTENTS

PAGE NUMBER

LIST OF TABLES

LIST OF FIGURES

This Page Intentionally Left Blank

1 (U) Scope

(U) This document presents the concept of operations (CONOP) for the Department of Defense (DoD) Key Management Infrastructure (KMI), Capability Increment 2 (CI-2). It provides an overview of the concepts and functionality for CI-2, and a user-oriented operational view of the system, illustrating common system operations in storyboard form.

1.1 (U) Identification

(U) This document is KMI 2212. This is revision 1.4.

1.2 (U) Document Overview

(U) This document is divided into eight sections. This section provides administrative information, a document overview, and a very brief system overview.

- (U) Section 2 lists reference documents.
- (U) Section 3 describes the existing operational environment into which the capabilities provided by KMI CI-2 will be introduced
- (U) Section 4 presents the justification for developing and fielding KMI CI-2 capabilities
- (U) Section 5 provides a description of the proposed KMI CI-2 system and capabilities
- (U) Section 6 presents operational scenarios for KMI CI-2 in the form of storyboards.
- (U) Section 7 summarizes the impacts that the development and fielding of KMI CI-2 are expected to have on the user community.
- (U) Section 8 presents a brief analysis of the benefits and limitations of CI-2.

1.3 (U) System Overview

(U) The target KMI[1] will be a single, automated, network-accessible, electronic-based key management and predominantly electronic cryptographic product delivery infrastructure. This new infrastructure will provide a means for the secure ordering, generation, production, distribution, management and auditing of cryptographic products (e.g., asymmetric key, traditional symmetric keys, manual cryptographic systems and cryptographic applications). Figure 1 provides an operational overview of the target KMI. KMI CI-2 will be the initial fielding of capabilities for network based management of cryptographic products and services along a development path toward the target KMI.

[1] "Target KMI" is a phrase that refers to the architecture and capabilities that KMI development efforts are intended to realize over time. Each "capability increment" should move the current KMI closer to the target architecture. The initial KMI Target Architecture was defined during 1999-2000; it is the intent of the KMI program that the target architecture be periodically revisited and updated. In this CONOP, "KMI" refers to the capabilities described by the CONOP and should be considered equivalent to "KMI CI-2."

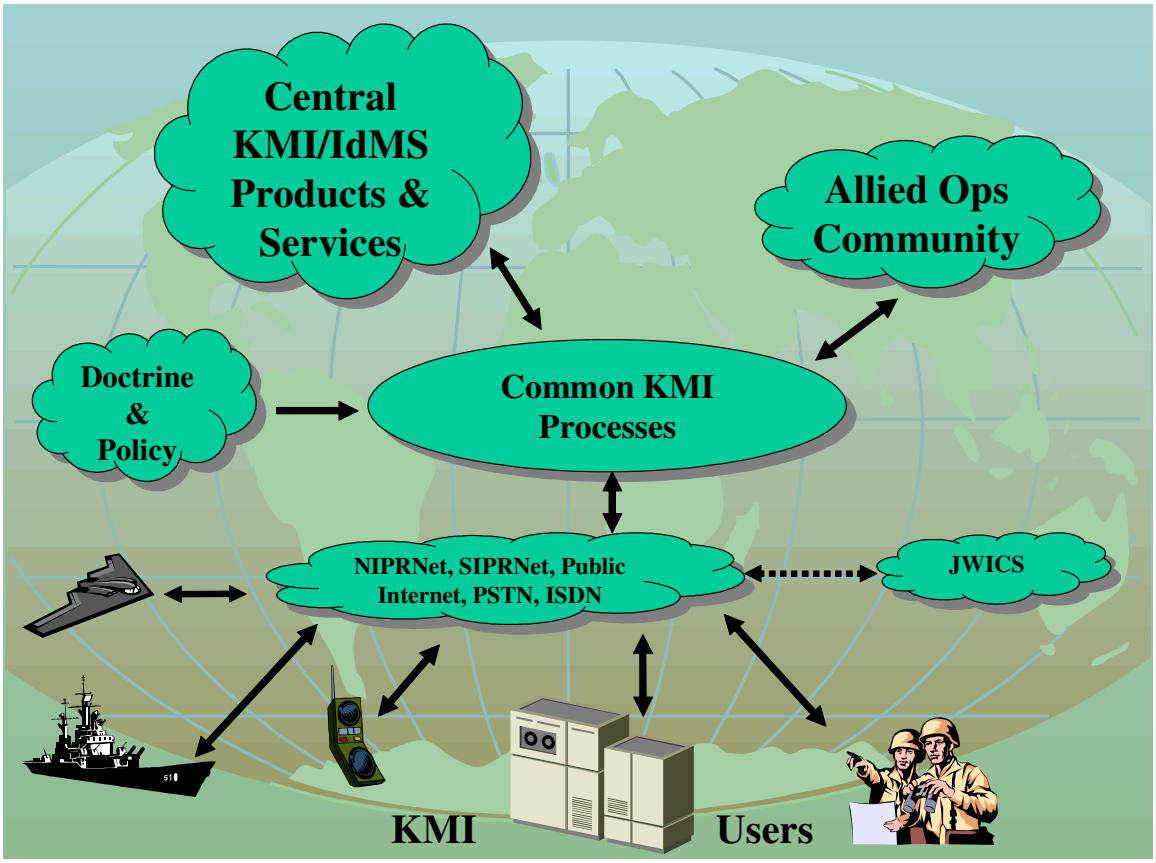


Figure 1: (U) Future KMI Operational View

(U) It is important to note that successful implementation of KMI requires more than transferring cryptographic products from Point A to Point B. Because of their sensitive nature, cryptographic products are strictly controlled from cradle to grave. KMI will accomplish these control and management processes faster and with less user burden than current systems through secure automation. KMI will use common networks such as the Non-classified Internet Protocol Routing Network (NIPRNET) and the Secret Internet Protocol Routing Network (SIPRNET) to the maximum extent allowed by policy and doctrine. Access to some KMI services, such as black key delivery, is expected to be through general-purpose computers not dedicated to KMI-related uses. More sensitive KMI services, however, will continue to require dedicated workstations in the CI-2 timeframe.

(U) KMI will create levels of management including central services (e.g., creation of key, security operations, storage and audit), tactical management (e.g., distribution of key in communication-challenged environments) and local management (e.g., requesting and receiving key for local weapon systems). The target KMI will consolidate existing "stove pipe" key management capabilities. CI-2 will provide network-oriented key management and delivery capabilities and begin to provide a path for transition away from the existing physical and electronic Communications Security (COMSEC) material systems. As a supporting infrastructure for the Global Information Grid (GIG), the KMI will provide products used by End Cryptographic Units (ECUs). CI-2 will both support legacy ECUs and provide the foundation that will evolve to support the modern key management

concepts being developed for ECU management as part of the National Security Agency's (NSA's) Cryptographic Modernization Initiative (CMI). Additionally, KMI is intended to enable approved Mission Planning/Management/Support Systems (MPMSS) to integrate key distribution with other information management functions required for the system the MPMSS supports.

(U) KMI will also support help desks operated by the military services and other KMI customer agencies and electronic key distribution for other systems/devices (e.g., Stand Alone Command and Control (C2) Systems, data transfer devices, etc.). Additionally, KMI will support services associated with security applications in the common operating environment (e.g., operating system security, software downloading, auditing, intrusion detection, and password management).

2 (U) Reference Documents

The following documents are referenced herein:

1. (U) *KMI CI-2 CDD*, draft for Flag level coordination, Version 2, April 14, 2005
2. (U) *A Concept for the KMI* [KMI 1001], 16 June 1999
3. (U) KMI 2200: (U) System Description And Requirements Specification (SDRS) For Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) Volume 1: Key Management Functions And Related Requirements, v. 2.2, 30 September 2005
4. (U) KMI 2200: (U) System Description And Requirements Specification (SDRS) For Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) Volume 2: System Security Policy And Related Requirements, v. 2.2, 30 September 2005
5. (U) KMI 2200: (U) System Description And Requirements Specification (SDRS) For Key Management Infrastructure (KMI) Capability Increment 2 (CI-2) Volume 3: System Security Architecture And Related Requirements, v. 2.2, 30 September 2005

3 (U) Current System

(U) This section summarizes the existing key management infrastructure implementation, capabilities, and user roles.

3.1 (U) Background, Objectives, and Scope

(U//FOUO) The current key management environment is made up of separate and independent infrastructures that provide and manage their own set of security products. These systems will become increasingly cumbersome and costly as new technology and their attendant security solutions continue to advance and the resources available to operate them decline. This key management environment, depicted in Figure 2, is composed of several unique solutions built for specific product lines. While the solutions satisfy unique security needs, they each require different tools and training in order to obtain their respective products and services, imposing an unwarranted strain on resources.

(U//FOUO) Adding a new key management capability has frequently meant creating a new, independent system to support it. Continuing this approach will increasingly tax resources throughout the community.

(U) Several of the systems in Figure 2 have been in existence for a number of years and are in need of upgrade to take advantage of modern communication technology. This technology area has advanced significantly in recent years, providing the market place with many new and worthwhile capabilities that would greatly improve efficiency and performance.

(U) KMI CI-2 will focus on moving Electronic Key Management System (EKMS) and physical key toward a more network-oriented method. This new method will have no impact on the DoD Public Key Infrastructure (PKI) or on the MISSI PKI. The KMI CDD discusses the dependencies between the DoD PKI and KMI CI-2.

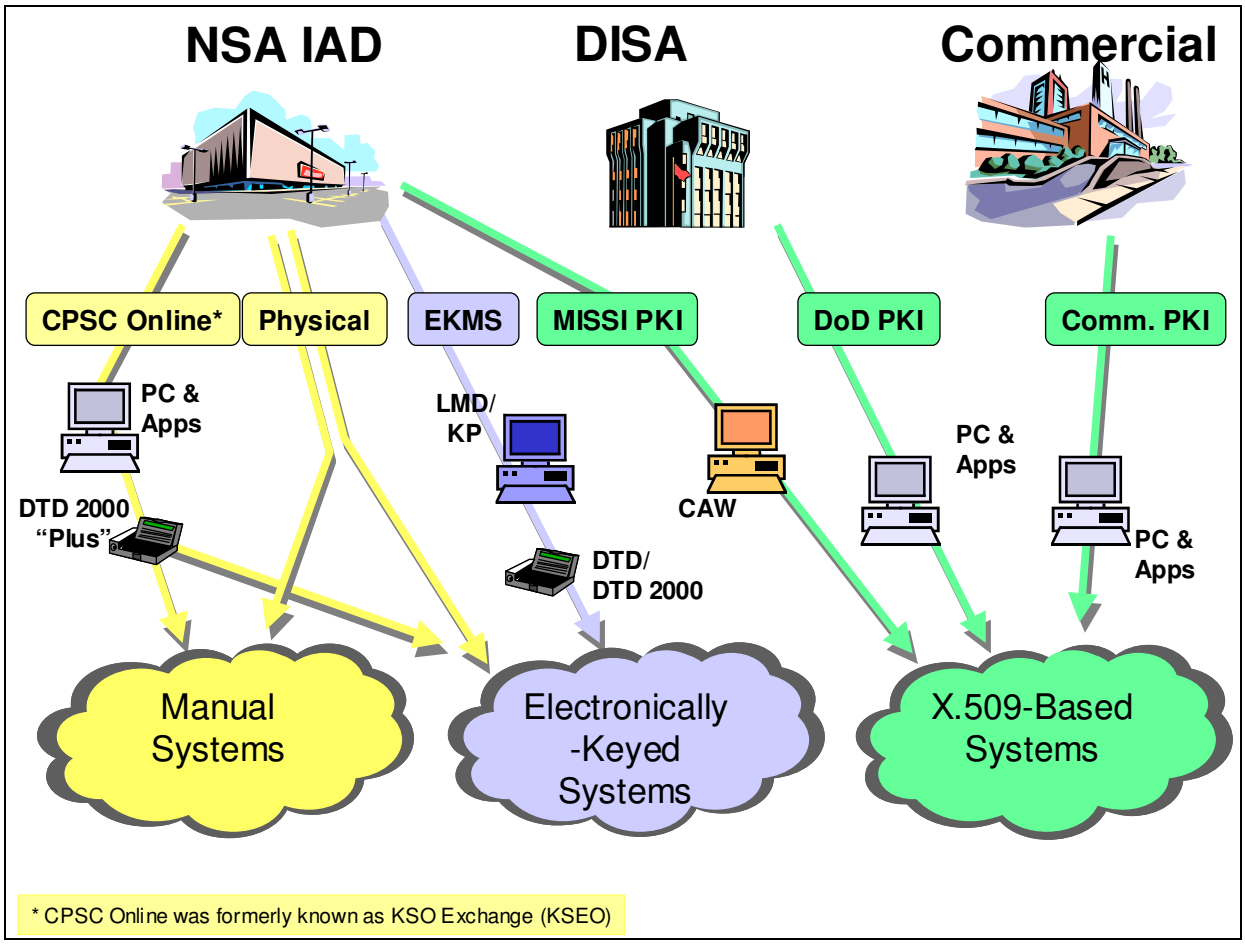


Figure 2: (U) Current Key Management Systems

3.2 (U) Operational Policies and Constraints

(U) DoD COMSEC operations and the EKMS are operated under the guidance of the following policy documents:

- EKMS/ COMSEC Material Control System (CMCS) Policy Documents
  - (U) NSTISSI 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997
  - (U) NSTISSI 4006, Controlling Authorities for COMSEC Material, 2 December 1991
  - (U) EKMS 103A, Security Policy for the Electronic Key Management System (EKMS), 22 January 1997 (EKMS Phase 3 Baseline)
  - (U) Information Assurance Directorate (IAD) Policy Statement 17, Cryptographic Key Protection Policy, 16 July 2002
  - (U) NSTISSI 4005, Annex F, Safeguarding COMSEC Material in Electronic Form, Draft

3.3 (U) Description of the Current System

(U//FOUO) The NSA today operates key management infrastructures in support of the information assurance needs of its customer community, providing cryptographic key products, symmetric, public and private keys, and security services for military, intelligence, allied government, contractor, and business customers worldwide. This support is provided either by the creation and distribution of a physical product, or creation and distribution of a product in an electronic format through the EKMS.

(U//FOUO) EKMS has been evolving since its inception in 1989 and is built on a model of multiple distributed elements using messaging over dial-up or dedicated communication paths. The military services have identified a number of improvements and changes they desire to see in EKMS.

(U//FOUO) The physical COMSEC Material Control System (CMCS) used to provision "hard copy" cryptographic products (e.g. printed key, manual systems) is time consuming and inefficient in comparison to its electronic counterpart. Considerable lead-time and resources are required to support these products and assure their availability when needed.

(U//FOUO) It is anticipated that requirements for support of classified applications will continue to grow as new cryptographic solutions, such as secure wireless and Global Positioning System modernization, are implemented. It is the intent of the KMI to enhance the DoD's capability to support these mission-critical requirements.

3.4 (U) Current Key Management User Roles

(U) The existing systems that constitute the set of current operational key management infrastructures include a number of implicit or explicit user roles (i.e., job functions). Depending on a variety of factors, these roles may be a full-time job or an additional duty as assigned for the individual performing them; in some circumstances, a single user performs multiple roles which taken together constitute a full-time position. The user roles that have been identified for the existing systems are described here; they are related to the roles proposed for KMI CI-2 in Section 5.6.

3.4.1 (U) CMCS / EKMS Roles

(U//FOUO) The roles commonly recognized in the CMCS developed over time based on a mixture of operations and policy. Many of these roles were incorporated into EKMS, sometimes under different names. In addition, the development of FIREFLY-keyed devices during the 1980s led to the creation of roles related to the management of FIREFLY key; the needs of these roles are also supported under EKMS.

- (U//FOUO) **Controlling Authority (CONAUTH).** Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet. A CONAUTH may have responsibility for a single cryptonet, or for a large number of such nets. Key is distributed to the COMSEC accounts supporting the communications stations in the net at the direction of the CONAUTH. The CONAUTH typically manages key distribution to ensure the cryptonet membership is consistent with operational direction received from the communications planning elements. In most cases, CONAUTHs are not participants in the cryptonets they manage. Personnel at the Service Authorities often assist CONAUTHs in carrying out their responsibilities, serving as facilitators for the CONAUTH in interactions with NSA's key production elements (e.g., ensuring that all of the necessary information is provided to NSA).
- (U//FOUO) **Central Office of Record (COR).** A COR is the office of a federal department or agency that keeps records of accountable COMSEC material held by elements subject to its oversight. Each military service currently operates its own COR. In the future the Services will convert to use the EKMS Tier 1 system as the COR, consolidating COR functions to the Tier 1 facilities at San Antonio and Fort Huachuca.
- (U//FOUO) **COMSEC Custodian / COMSEC Manager.** A COMSEC Custodian is the individual designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding, and destruction of COMSEC material assigned to a COMSEC account. Key material and accountable cryptographic equipment is distributed to and locally controlled and managed by COMSEC accounts. The individual responsible for the operations of a COMSEC account is known, variously, as a COMSEC Custodian or COMSEC Manager. If an account is equipped with an EKMS Local Management Device/Key Processor (LMD/KP), the custodian/ manager is the operator of the LMD/KP.
- (U//FOUO) **Command Authority.** The Command Authority is responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges. The Command Authority verifies the identities of User Representatives designated by various parts of the organization to order key, determines the ordering privileges of each User Representative, and communicates that privileging information to the FIREFLY key production system operated by NSA.
- (U//FOUO) **Registration Authority (RA).** The EKMS registration process provides the administrative and technical means by which a Key Management Entity (KME) is established, and the information regarding the KME recorded in

the EKMS directory. The term KME applies to any account/element/organization that can perform key management functions. EKMS RAs are located at Tier 0 (for Civil Agency and NSA accounts) and Tier 1 (for Service accounts). The RA is responsible for registering KMEs and managing their status. As part of the registration process, the RA ensures that a KME's EKMS Identifier (ID) and associated attributes (e.g., clearance level, courier address for COMSEC accounts) are assigned and maintained in the EKMS Directory.

- (U//FOUO) **User Representative.** A User Representative is authorized by an organization to order FIREFLY key and interface with the keying system, provide information to key users, and ensure the correct type of key is ordered. The User Representative acts within the privileges established for that individual by the Command Authority who appointed him or her.
- (U//FOUO) **Local Element (LE).** Local Elements are separate entities, units, or commands, internal or external to the parent COMSEC account that requires COMSEC material. LEs receive their electronic COMSEC material from a parent COMSEC account or Subaccount and never directly from a Tier 1 or Tier 0. LEs are normally issued material for immediate use in ECUs, but some LEs are responsible for routinely issuing material to other LEs. The local element concept is known by other organization-specific names, such as COMSEC Responsible Officer in the Air Force.

4 (U) Justification For and Nature of Changes

(U) This section summarizes the factors that motivate changing key management infrastructure operations from the current approach to that planned for CI-2 and beyond.

4.1 (U) Justification of Changes

(U//FOUO) The KMI CDD identifies the shortcomings of existing capabilities and drivers for change in how key management and key provisioning are performed. While those documents should be consulted for specifics, areas of concern with the current systems include:

1. (U) Slow response to changing operational requirements and conditions
2. (U//FOUO) Incompatibility between EKMS and widely-used military communications systems
3. (U) Inability to integrate key distribution into MPMSS
4. (U) Poor support for tactical operations and Allied interoperability
5. (U) Desire to support modern and in-development cryptographic devices and management techniques
6. (U) Difficult user interfaces and manpower intensive operations

4.2 (U) Description of Desired Changes

(U) In the development of the KMI target architecture and the KMI CDD, along with various meetings with the military service and civil agency customer community representatives, a number of desired changes to the existing key management

infrastructures have been identified. In addition, the on-going development of cryptographic modernization concepts has identified other features needed in the KMI to support the next generation of ECUs. A number of goals have been identified for key management infrastructure modernization, and the concepts for KMI CI-2 include a number of features that move toward achieving those goals.

- (U) Goals
  - (U) Reduce the manpower required for KMI operation and use
  - (U) Minimize the requirement for computer workstations dedicated to KMI operations
  - (U) Use common/open/standard computer platforms
  - (U) Provide communications flexibility, and permit use of widely used backbone network and tactical communications systems
  - (U) Support autonomous operations within combatant commander areas of responsibility
  - (U) Scalability
  - (U) Transparency
  - (U) Releasability and interoperability
  - (U) Graceful evolution
  - (U//FOUO) Key delivery direct to ECUs
  - (U) Develop common/open/standard applications and interface standards for KMI products
  - (U) Develop reusable KMI software applications
- (U) Features
  - (U) Modular architecture with logical division of functions
  - (U//FOUO) Network connectivity to NIPRNET, SIPRNET, Internet
  - (U//FOUO) Type 1 support for tokens
  - (U) Flexibility of client implementation and configuration
  - (U) Improved, more usable human machine interface (HMI)
  - (U) Ready availability of status information
  - (U) Catalog of products and services
  - (U) Accounting automation
  - (U) Autonomous operations
  - (U) Designed for interoperability and releaseability

5 (U) Concept for the Proposed System

(U) This section presents a brief description of the proposed CI-2 system, and provides a context for the operational storyboards presented in Section 6.

5.1 (U) Background, Objectives, and Scope

(U//FOUO) The focus of CI-2 is to build the foundation for the future management of key material in a general-purpose networking environment. Given the risks inherent in such an environment, CI-2 will have correspondingly stringent security requirements.

(U) The CI-2 development will focus on achieving the following objectives:

I. (U//FOUO) *Establish a secure net presence for KMI for Key Management*. This includes complete development of the PRSN, filters, access control, role management, virtual private network (VPN), user interface services, net management services, directory services, etc. needed to provide this capability. There will be a KMI network presence on the NIPRNET, SIPRNET, and public Internet[2]. KMI network interactions will be based on common Internet-standard communications protocols for World Wide Web, email, file transfer and similar functions.

II. (U) *Enable customer transition from EKMS to KMI*. This objective encompasses two major aspects:

1. (U//FOUO) Establishing a translator between the PRSN and EKMS messaging system to facilitate transition of EKMS users to KMI CI-2. The translator will enable EKMS functions and transactions to be transferred between the EKMS messaging system and the PRSN to permit ordering from Tier 1, Tier 1 ↔ Tier 2 accounting transactions, all Tier 1 ↔ Tier 2 distribution transactions, all Tier 2 ↔ Tier 2 distribution transactions, movement of directory information, etc.
2. (U//FOUO) Developing a KMI client set that EKMS users can transition to. The client set must support some or all of the EKMS based functions/transactions listed above, and interface with the PRSN via the network-based user interface services the PRSN provides (e.g., web).

III. (U//FOUO) *Provide web-based key ordering for all key types*. CI-2 will provide KMI customers the means to order all forms of key, including symmetric (traditional) key, asymmetric (modern) key, and manual systems, in a variety of electronic and physical form factors.

IV. (U//FOUO) *Provide Over The Network Keying (OTNK) directly to ECUs*. A part of the KMI vision is to provide key distribution from a PRSN to network-connected ECUs registered in the KMI and capable of direct interactions with the KMI. The High Assurance Internet Protocol Encryptor (HAIPE) family of ECUs will be the first products prepared to make use of this capability. CI-2 will provide an OTNK capability based on the KMI Access Protocol specifications currently being drafted.

V. (U//FOUO) *Enable the integration of key distribution functions into dedicated mission management systems*. Many existing and new systems require dedicated mission management systems. Examples include aircraft and satellite communications terminals. These systems typically include a MPMSS component to collect, organize and distribute data that is required for the other system components to function. CI-2 provides tools that can be used to enable a MPMSS to retrieve black or benign key from a PRSN Product Delivery Enclave (PDE), acting as a KMI Operating Account (KOA) Agent. In the CI-2 timeframe, ordering and

[2] NIPRNET is separated from the Internet here based on the expectation that in the future a DoD PKI certificate will be required for NIPRNET access. Many Allied and coalition partner KMI users with the need to retrieve key material from the KMI will not have such certificates, necessitating direct connections to both Internet and NIPRNET.

management of key will be performed using KMI Manager Clients or EKMS capabilities.

VI. (U//FOUO) *Provide access to non-U.S. Users to manage and retrieve interoperable key management products and services*. Today's operational environment mandates effective interoperability across the DoD and U.S. Federal communities, including Homeland Security, and, when operational needs dictate, with Allies and coalition partners. To this end the KMI must provide controlled access to authorized non-Users to request and obtain interoperable key management products and services. In the CI-2 timeframe authorized non-U.S. Users will be granted appropriate management and product retrieval privileges necessary to ensure mission interoperability. Additionally, registered non-U.S. KMI aware devices will also be granted KMI access for retrieval of benign interoperable key.

VII. (U//FOUO) Provide hardware token support for KMI management functions. KMI CI-2 will support hardware tokens, loaded with Type 1 PKI certificates.

(U) Figure 3 depicts the CI-2 system architecture.

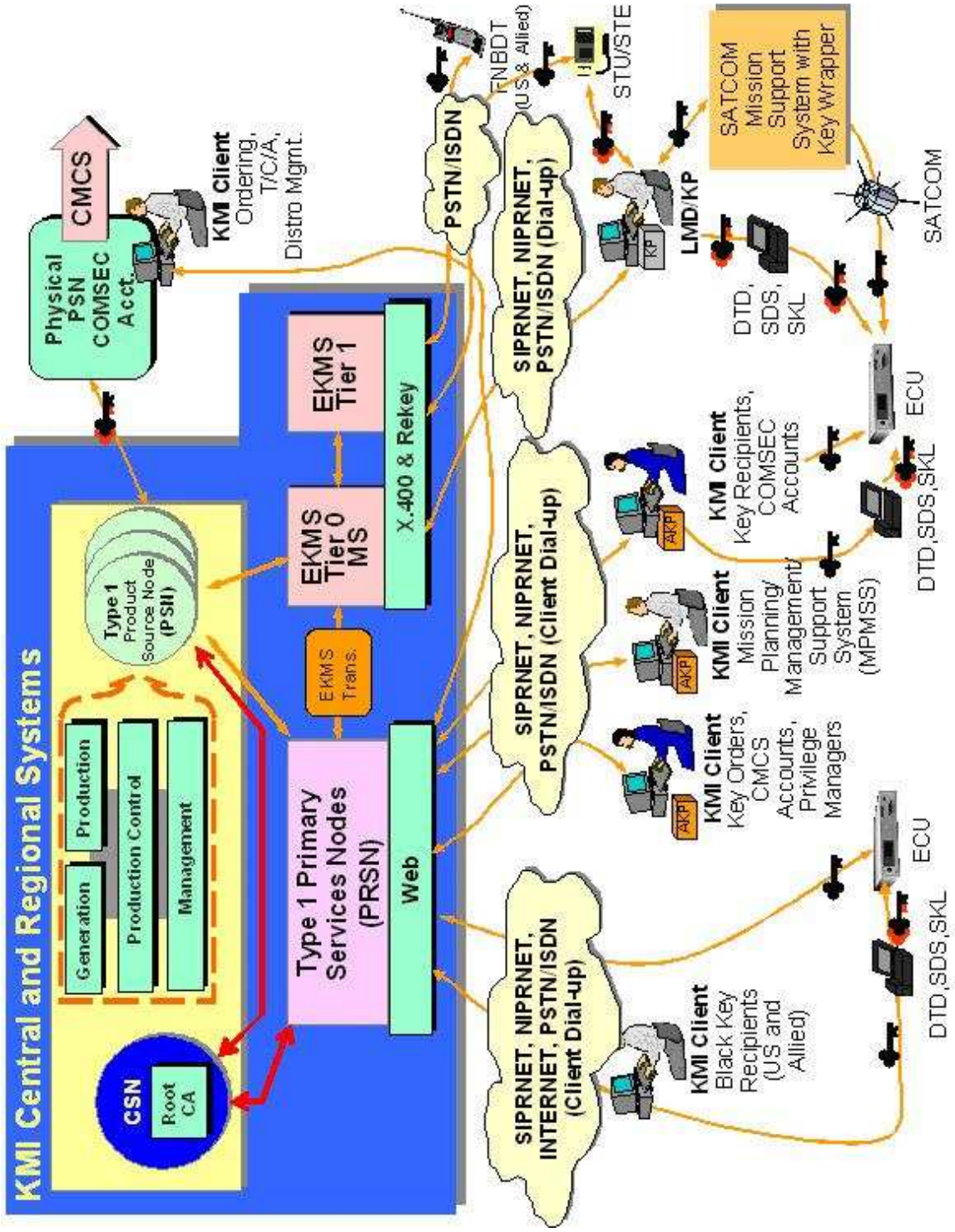


Figure 3: (U//FOUO) KMI CI-2 System Architecture (SV-1)

5.2 (U) Operational Policies and Constraints

(U//FOUO) The KMI CI-2 SDRS, Volume 2 covers the security policies and requirements for CI-2. That document integrates the requirements imposed by the new DoD 8500-series documents. Relevant policy statements from that document are captured in the individual storyboards.

(U) NSTISSI 4005, Annex F discusses policy and processes to be used when generating and delivering electronic key material.

5.3 (U) Description of the Proposed System

(U) This section describes the proposed KMI CI-2 system, including basic architecture, central and client nodes, and system functions, features, and capabilities.

5.3.1 (U) KMI Basic Architecture

(U) The KMI consists of a number of nodes that provide a unified infrastructure for providing key management products and services, supporting a wide variety of users. In the KMI, users are either consumers that depend on the KMI for products and services or managers that allocate and control resources within the KMI; customer organizations will typically have a mixture of users and managers. A logical configuration of KMI node types along with the functions allocated to each node type is shown in Figure 4.

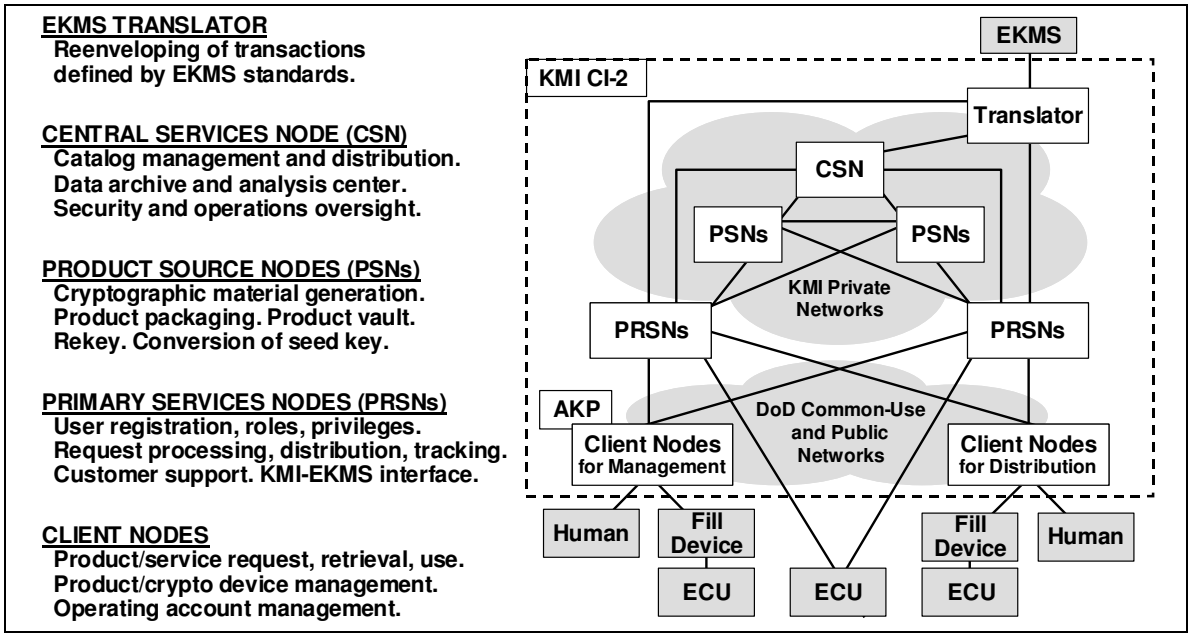


Figure 4: (U) KMI Nodal Architecture

(U//FOUO) Four types of functional nodes comprise the KMI:

- (U//FOUO) PRSN
- (U//FOUO) Central Services Nodes (CSNs)

- (U//FOUO) Production Sources Nodes (PSNs) and
- (U//FOUO) Client Nodes

(U//FOUO) The PRSNs are central to the KMI, and provide services to the Client nodes over one or more communications networks. The PSNs are responsible for generating cryptographic products and the CSN oversees system security operations, provides oversight of storage and replication of common data for PRSN and PSN use, and manages the content and distribution of the KMI Product Catalog to PRSNs and PSNs.

(U//FOUO) Client Nodes cover a broad category of components and/or software applications that provide a user access to the products and services of the KMI. They can take a variety of forms including security devices (e.g., ECUs), applications installed on workstations (e.g., a KMI client Node) to clients embedded in enterprise systems (e.g., an MPMSS). Clients can securely interface with the PRSN and allow users to perform management functions or request and receive products and services from the KMI.

(U//FOUO) The nodes that comprise the KMI may be widely distributed or collocated within central or regional sites. Such sites may be connected by a variety of DoD and commercial communications networks.

5.3.2 (U) Client Nodes and Transfer Devices

(U) The KMI CI-2 architecture includes a number of different clients intended to address a spectrum of KMI user needs. The client types described here are a proposed set based on KMI operating concepts developed by the CI-2 engineering team; feedback from the customer community regarding the utility of each type is expected to influence the characteristics and quantities of each client.

5.3.2.1 (U) Client-creation Components

(U) Three components are envisioned to serve as "building blocks" for the creation of KMI clients: A computing platform, Key Management Software Applications and the Advanced Key Processor (AKP).

5.3.2.1.1 (U) Advanced Key Processor

(U//FOUO) The AKP is a successor to the EKMS KP, with similar functionality, enhanced performance, and a modular architecture to provide configurability and simplify evolution of the AKP's capabilities. The AKP's modular architecture allows capabilities to be included or omitted as necessary to match the needs of a KMI customer's mission; it also supports the need to provide version of the AKP releasable to allies. Capabilities that can be configured into an AKP will include:

- Symmetric key generation
- Cooperative creation of key encryption keys
- Key wrapping and unwrapping
- Digital signature creation and verification
- Establishment of secure channel from Client Node to PRSN
- Identification and authentication of KMI Managers

- Source authentication and integrity protection of KMI transactions
- Support for secure local storage of electronic key
- Interactions with fill devices

5.3.2.1.2 (U) Key Management Software Applications

(U) Given the varying needs of the KMI user community, KMI clients may need one or more of a collection of key management applications. Examples of such applications would be modules to:

- (U) Support accounting for physical key products
- (U) Assist in ordering and managing modern key
- (U) Assist in managing files containing download encrypted keys and loading appropriate files into transfer devices for ECU loading

(U) The specific set of key management applications software modules for CI-2 will be determined as part of the client engineering effort.

5.3.2.2 (U) KMI Manager Clients

(U//FOUO) Figure 5 illustrates the basic types of client configurations and their connections to the PRSN. Manager Clients (MGCs) connect to PRSN Ordering and Management Enclaves (OMEs) to conduct functions related to registration, enrollment, ordering, and KOA Operations.

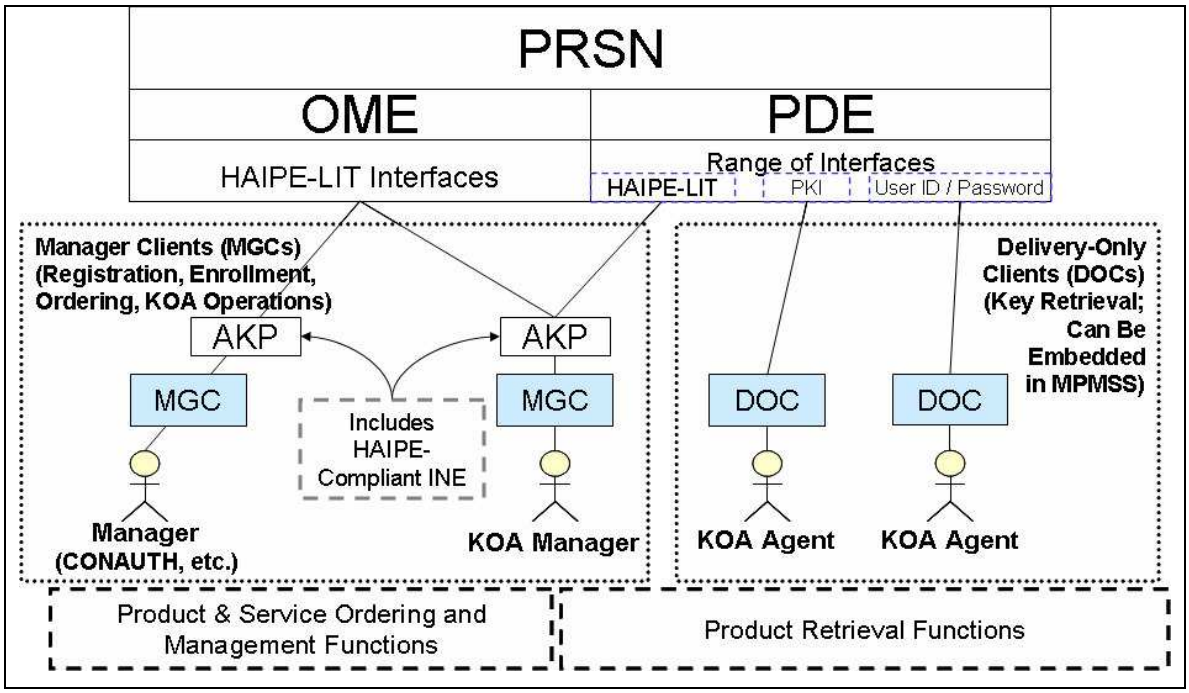


Figure 5: (U) Human User Client Interactions with PRSN

(U//FOUO) An MGC is a KMI client equipped with an AKP, and is used when performing management functions. Such a client is dedicated to KMI management purposes due to the sensitivity of the KMI capabilities is can access. When used for

operation at a KOA (see Section 5.3.4), the MGC is the KMI analog to the EKMS LMD/KP. It is capable of operating independently of a PRSN for many functions, and includes cryptographic processing support using its AKP. Characteristics of MGCs include:

- (U) Supports all KMI functions that can be performed with a non-AKP-equipped client.
- (U//FOUO) Incorporates a HAIPE-compliant In-line Network Encryptor (INE) to establish protected communications channels between the client and the PRSN.
- (U//FOUO) Provides local capability to unwrap and rewrap BLACK key material received from other KMI nodes or EKMS elements.
- (U//FOUO) Provides capability to wrap key material for benign delivery to ECUs.
- (U//FOUO) Provides local capability to wrap key material for transfer to other AKP-equipped clients via the PRSN, or to EKMS LMD/KPs via the PRSN and the EKMS translator.
- (U) Provides the ability to sign messages and verify signatures on received messages.
- (U//FOUO) Locally generates key material using the AKP.
- (U) Maintains local data stores consistent with its operational needs; synchronizes its local data stores with the PRSN when connectivity is available.
- (U//FOUO) Implements security services necessary to protect KMI information and interactions. Enforces access control / privilege restrictions based on information propagated from a PRSN or established at the client by an appropriately privileged KMI Manager.
- (U//FOUO) Unwraps key encrypted for transfer or storage and outputs key in red format for emergency fill capability; use of this capability should be restricted to urgent situations, with benign fill from the client to the ECU or the use of a transfer device that outputs red key being the preferred modes of operation.

(U//FOUO) The specific capabilities of an AKP-equipped manager client are dependent on the configuration of the AKP and the set of key management software applications loaded on the client.

5.3.2.3 (U) Delivery-Only Clients

(U//FOUO) Delivery-only client (DOCs) are not equipped with AKPs. They interface to the PDEs of KMI PRSNs to retrieve wrapped key material.

(U) DOCs are oriented toward the needs of KMI users with no need to unwrap, rewrap, or locally generate key material. The essential components of a DOC are a general-purpose computer with a web browser application operated by a registered User with PKI credentials or a username and password for identification and authentication (I&A). Such a user is known as a KOA Agent. Characteristics of DOCs include:

- (U) Receives key wrapped for delivery to ECUs associated with the KOA.
- (U) Uploads credentials for ECUs and that will be receiving key to PRSN to supporting recipient-specific key wrapping.
- (U) Includes no local data storage or management other than for downloaded BLACK or benign key material and ECU credentials and/or tracking information awaiting upload; dependent on connectivity to PRSN and on data stored at those service nodes.

5.3.2.4 (U) Embedded MPMSS Clients

(U//FOUO) Many existing and, especially, new systems require the supply of various information items to the end user device (e.g., an aircraft, a satellite communications terminal) in order to function. Such systems typically have a MPMSS to collect the relevant data from various sources (e.g., systems that provide meteorological data or frequency allocations), organize it appropriately for the using system's components and distribute it for use. A goal of KMI is to enable the integration of key distribution with the other functions performed by an MPMSS; when key is handled in black or benign form, it can be distributed like any other mission data the system requires. Consequently, CI-2 includes the concept of embedding a DOC into an MPMSS and permitting that embedded MPMSS client to interact directly with the KMI to receive wrapped key material for distribution and use within the customer system. The MPMSS operators who employ this capability must be registered with the KMI and enrolled as KOA Agents.

5.3.2.5 (U) Fill Devices and ECUs

(U//FOUO) While NSA is working on a new generation of ECUs capable of direct interaction with the KMI, in many cases, ECUs that need to be supported by KMI CI-2 will not be network connected. "Last mile" transport of black or benign key material from a KMI client to an ECU will need to be handled by a fill device of some sort. The fill devices available in the CI-2 timeframe will include the Secure DTD2000 System (SDS), the Simple Key Loader (SKL), and the Data Management Device (DMD), which all utilize the KOV-21 COMSEC Card. Legacy AN/CYZ-10 Data Transfer Devices may also still be available. CI-2 will support the use of the fill devices to move encrypted key material from KMI clients to ECUs. In order to wrap key for ECUs, it will be necessary to register them with the KMI and upload credentials (e.g., ECU benign fill FIREFLY credentials) to the KMI. The KMI client Nodes and the fill devices will support this upload function. ECUs that are capable of direct KMI interaction will be able to upload their credential directly. The different ways for an ECU to receive key products are described in the "Key Distribution and ECU Fill" section.

5.3.3 (U) CI-2 Functions

(U) This section describes the functions performed by KMI CI-2.

5.3.3.1 (U) Registration

(U) CI-2 requires the registration of KMI users and managers, and of a range of devices that includes ECUs and AKPs.

- (U//FOUO) *KMI Managers*: KMI CI-2 will register KMI managers and issue them Type 1 identification and authentication credentials for use with the AKP.
- (U//FOUO) *KMI Operating Accounts*: KMI CI-2 will introduce the concept of a KOA. While a KOA is similar in principle to a COMSEC account, its real purpose is to serve as an organizing construct for the set of key destinations (e.g., ECUs, AKPs) associated with a particular organization or unit. For CI-2 all KOAs will also be COMSEC accounts; at some future point in the evolution of the KMI that may no longer be required.
- (U//FOUO) *Devices:* KMI CI-2 will support the registration of devices: AKPs, ECUs, and Manager Identity Tokens. Devices may be registered with the PRSN (general devices) and supported with key wrapped by a PSN, or registered only with the Client Node of a KOA (limited devices) and supported with key wrapped by the Client Node's AKP. All devices will be associated when registered with an owning KOA. Each device that will receive key material generated and wrapped by the KMI (e.g., by a PSN or AKP) must supply credentials that can be used by the KMI to create key encryption keys to wrap key for delivery to that device.

5.3.3.2 (U) Privilege Management

(U//FOUO) In order to manage the security of the KMI, and regulate access to KMI products and services, and detect and deter unauthorized attackers, CI-2 will incorporate a robust privilege management capability.

- (U) CI-2 access control will use role-based access control (RoBAC) concepts, augmented by Rule-Based Access Control (RuBAC) capabilities. A basic set of roles has been defined, and these roles can be specialized to meet operational and security needs.
- (U) The RoBAC system for CI-2 will permit appropriately privileged KMI managers to manage the set of the KMI roles and the privileges associated with each in order to fit the RoBAC approach to mesh with customer organizational and operational concepts.
- (U) CI-2 access control will also incorporate RuBAC features that take into account attributes of the user(s) and product(s) involved when determining if a particular action is permitted.
- (U) Where necessary, Controlling Authorities will also be able to require independent approval of requested actions, such as changes in the distribution of a key product.

(U) Given the risks inherent in operating in a networked environment, access control is a critical security feature of KMI CI-2. The basic CI-2 access control concepts are summarized in Section 5.4 of this CONOP, and described in detail in the CI-2 SDRS, Volume 3.

5.3.3.3 (U) Enrollment

(U//FOUO) The enrollment process is used to establish KMI users as KMI Managers and KOA Agents, and determine the specific roles and privileges those managers will be able

to use. NSA envisions that each customer organization will have a small number of individuals who can act as Enrollment Managers, regulating the KMI Manager privileges of users within their organization. CI-2 will enable an Enrollment Manager to:

- (U) Identify individuals who should have KMI manager privileges
- (U) Determine which KMI manager roles those individuals can access
- (U) Manage the attributes associated with those individuals
- (U) Remove attributes associated with individuals
- (U) Remove KMI manager roles a user can access
- (U) Remove an individual from the role of KMI manager
- (U) Have privileges themselves; but not be able to assign privileges greater than those they have been designated for.

5.3.3.4 (U) Key Ordering

(U//FOUO) A primary CI-2 objective is to provide network-based (including both web-oriented and transaction-oriented interfaces) ordering of all key material[3]. The access control and privileging features of the PRSN will play an important role in enabling this ordering capability while minimizing the potential for abuse. The CI-2 PRSN will:

- (U) Maintain a Product Ordering Catalog (POC) of products and services available from the infrastructure; the POC is distributed to the PRSN from the CSN
- (U) Allow KMI users and managers to view the subset of the POC that is consistent with their roles, privileges, and attributes
- (U) Allow KMI Managers to request new instances of KMI products (e.g., a new short title); these new products are added to the POC, consistent with the requesting manager's roles, privileges, and attributes
- (U) Allow KMI Managers to manage the characteristics of products for which they are responsible, consistent with their roles, privileges, and attributes
- (U//FOUO) Accept orders for symmetric (traditional) key, asymmetric (modern) key and manual systems, and route those orders to the appropriate PSN in accordance with the characteristics of the product and the directions of the ordering manager
- (U) Provide for either automated or manual approval of product management actions, based on the attributes of the product(s) involved and the roles and attributes of the user or manager requesting the action
- (U//FOUO) Allow Controlling Authorities or Product Requestors to request copies of specific products, and route those requests for approval to a KMI Manager with the necessary approval authority (e.g., a controlling authority)

[3] While this primarily refers to Type 1 key, the existing KMI also supplies Type 0 and Type 2 key material; CI-2 will be able to supporting ordering of those as well.

5.3.3.5 (U) Distribution Management

(U//FOUO) CI-2 will provide features to manage the distribution of physical and electronic key.

- (U) Allow the responsible KMI manager (e.g., a controlling authority) to view and edit the account distribution profiles for the physical and electronic key they control.
  - (U//FOUO) Add and delete recipient KOAs, KMEs, and other recipient COMSEC accounts
  - (U) Modify copy counts for traditional key
  - (U) Modify in-place dates and reserve-on-hand quantities for traditional key
- (U) Allow the responsible KMI manager to establish subscriptions (i.e., standing orders and account distribution profiles) of traditional key for those KMI users that should receive the key regularly.
- (U) Allow the responsible KMI manager to view the distribution status information for key products they control.
- (U) Allow product recipients to view the distribution status of products they are scheduled to receive.
- (U) Allow KOA Managers to view and edit the device distribution profiles and manage the key wrapping for the electronic key their KOAs receive, adding and deleting key recipients (e.g., AKP, ECUs) to the device distribution profile for each product.

5.3.3.6 (U) Key Generation and Production

(U//FOUO) KMI CI-2 will generate keys based on the orders it receives. CI-2 will generate a broad range of key types including:

- (U//FOUO) Type 0/1/2 symmetric key
- (U//FOUO) Type 0/1 asymmetric key (e.g., Enhanced FIREFLY)
- (U//FOUO) Manual systems.

5.3.3.7 (U) Key Distribution and ECU Fill

(U//FOUO) CI-2 will distribute the keys it generates, based on the parameters of the key order and any subsequent distribution management instructions from appropriate KMI Managers. Keys generated at a PSN will be wrapped for the end recipient (e.g., an AKP, an ECU) and are inaccessible to the PRSN and other intermediate points along the distribution path.

(U//FOUO) Figure 6 illustrates that a user device may be equipped with one or more of the three logical types of fill ports through which the device can receive KMI products. These three types are identified here as “logical” types in order to avoid making assumptions about the actual physical implementation of future devices.

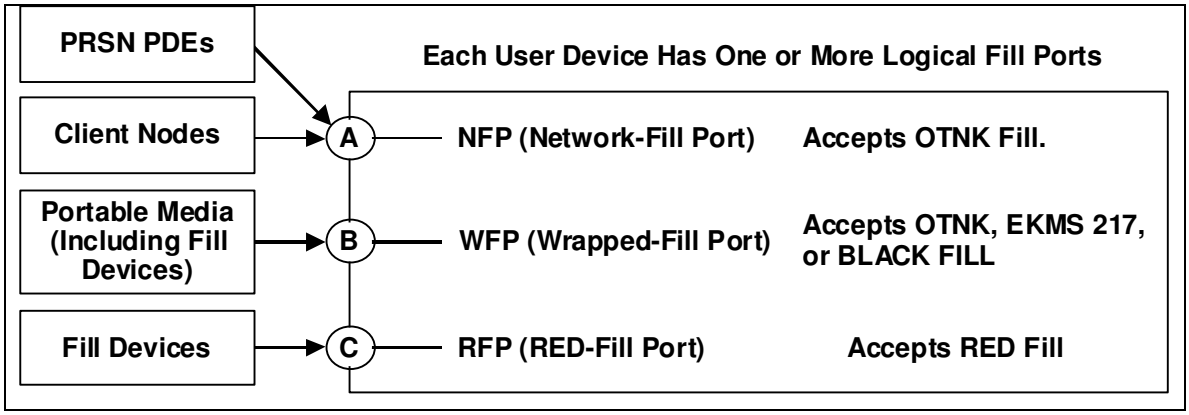


Figure 6: (U) Types of Fill Ports in User Devices

(U//FOUO) **Network-Fill Port (NFP**). The network-fill port is the device's interface through which it can be filled using OTNK. OTNK is a benign method of filling a device, but is distinguished from benign techniques, as defined in EKMS 217, by the use of new formats and protocols that can be used across network backbones between user devices and PRSN PDEs. Network fill is performed across a network connection.

U//FOUO) **Wrapped-Fill Port (WFP)**. The wrapped-fill port is the device's interface through which wrapped (i.e., encrypted) key material can be delivered directly to the device. This port is used to conduct benign fill transactions, as defined in EKMS 217, and to load key material in BLACK form, said material having been wrapped by a supporting Client Node using a Key Encryption Key (KEK) previously loaded into the device in RED form. Wrapped fill is may be performed via media or fill device transport of the information to and from the device; some devices capable of using a network fill port may also be able to accept product fill via the wrapped-fill port.

(U//FOUO) **RED-Fill Port (RFP)**. The RED-fill port is the device's interface through which RED (i.e., unencrypted) key can be delivered directly to the device. RED fill is always performed using a fill device.

(U//FOUO) Figure 7 illustrates the different types of distribution paths through which user devices can receive KMI products.

(U//FOUO) Figure 7 shows that distribution paths may be separated into five basic cases, and provides details about the variations of each type that may exist. In cases 1, 2 and 3, the product is generated by the PSN and wrapped there uniquely for the destination device. In case 4, the source of the product may be a PSN, another client node, or a key source somewhere within EKMS and the product is wrapped for the receiving client node's AKP. In case 5, the key is locally generated by the client node's AKP. In both case 4 and case 5, the product is wrapped for delivery to the user device by the supporting client node's AKP.

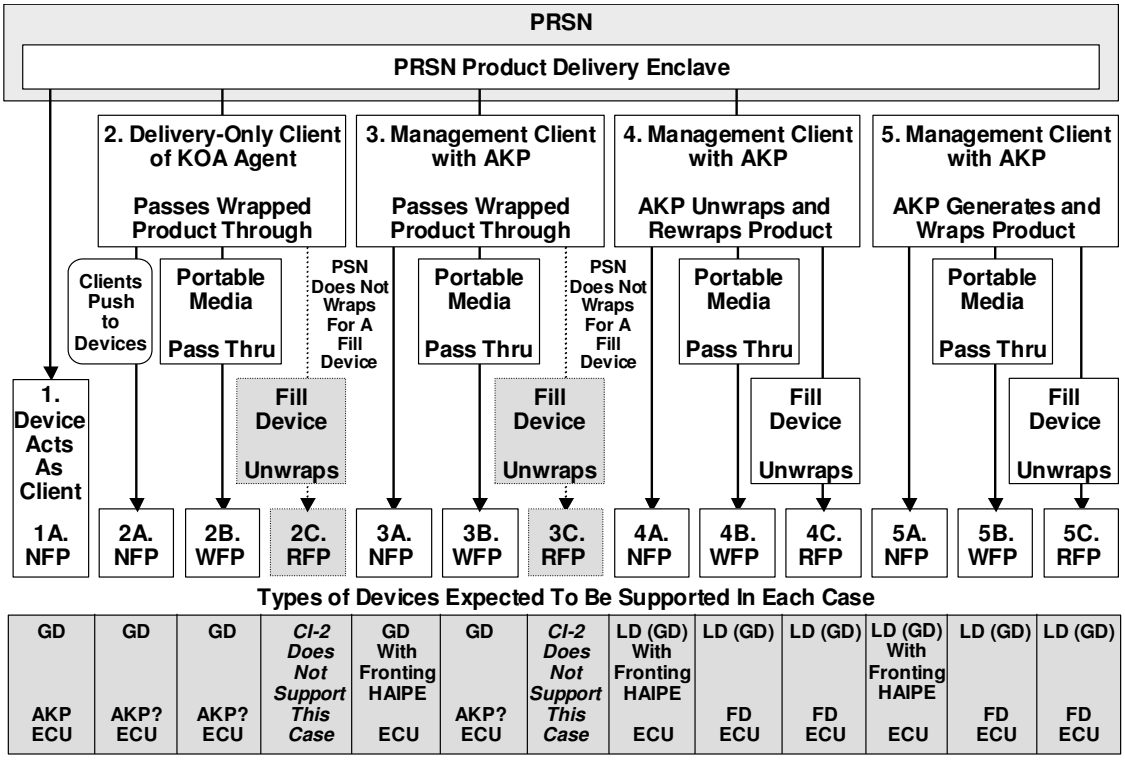


Figure 7: (U//FOUO) Types of KMI Distribution Paths

(U//FOUO) The figure also shows how each of the paths uses one or more of the three logical types of fill ports. Some of the combinations are special cases. CI-2 does not support paths 2C and 3C (which would use a RED-fill port on a user device) because a PSN never wraps a product for distribution to a fill device.

(U//FOUO) For each supported path, the box at the bottom of the figure lists the basic types of user devices that are supported on the path: AKP, ECU, and fill device (FD). The box also lists the type of identity registration that a user device must have to use the path: "GD" indicates a "General Device", and "LD" indicates a "Limited Device". (These two registrations types for user devices are defined and described in the "Registered Users" section of the CI-2 SDRS, Volume 2; in summary, a general device is registered globally and products can be wrapped for it by a PSN, whereas a limited device's registration is only relevant at the client node supporting that device.) In addition to GD and LD, some paths are shown as supporting "(GD)", i.e., GD in parentheses. This is meant to indicate that the path can support user devices that are treated by the management client as a limited device, even though they are also registered as general device. For example, there may be operational circumstances where it is necessary to fill a general device with a product that was generated and wrapped at the supporting client node rather than the PSN.

5.3.3.8 (U) Rekey Services

(U//FOUO) CI-2 will provide on-line and staged (e.g., in accordance with HAIPE concepts) seed key conversion and rekey services for:

- (U//FOUO) ECUs keyed with basic or enhanced FIREFLY key
- (U//FOUO) AKPs

(U//FOUO) This range of capabilities will support rekey for devices compliant with EKMS 218, devices compliant with EKMS 217 (store & forward using EKMS transactions), and devices compliant with forthcoming OTNK specifications.

5.3.3.9 (U) Tracking, Accounting, and Auditing

(U//FOUO) KMI CI-2 will automatically record information regarding events as they occur within the system. Some of these events will be captured to provide information useful for status reporting to KMI users and manager, development and monitoring of performance metrics, etc. Information recorded for these purposes is called "tracking data," and is retained on a temporary basis.

(U//FOUO) Information regarding other events is captured because it is important for deterring KMI managers and others from deliberately compromising cryptographic material. Information recorded for these purposes is called "accounting data," and is retained indefinitely. This information will also be used to perform investigations and damage assessments when it is suspected or determined that a KMI Manager in the KMI product ordering or distribution processes has been involved in a deliberate compromise of cryptographic material. Events that directly or indirectly involve or affect exposing key in RED form, or encrypting key for a KMI User or set of KMI Users are regarded as "accountable" events.

(U//FOUO) Finally, some KMI events are important from a security perspective, but do not directly involve generation or distribution of cryptographic material. Examples of these events are registration and enrollment. These events create audit data, which is also used to deter wrongdoing by KMI Managers, and recover from malicious actions committed by them.

(U//FOUO) The KMI will rely on EKMS/CMCS accounting functionality for CI-2. Transactions that traverse the KMI/EKMS translator will be recorded by existing EKMS accounting functions. Tracking and audit information generated by KMI components will be recorded and maintained by KMI CI-2.

5.3.3.10 (U) Status Reporting

(U) CI-2 will provide the ability for KMI users and managers to request status information regarding product orders and distribution. Status reporting is based on information gathered by the KMI's tracking function. Status information available will include, but not be limited to:

- (U) Approval status (e.g., pending, approved, rejected) of submitted requests that require approval
- (U) Distribution status of KMI products. Individual users will be able to see the status of products they are scheduled to receive. KMI managers will be able to see the status with regard to all recipients of products they control.

5.3.3.11 (U) EKMS Translator

(U//FOUO) In the CI-2 timeframe, interoperability with EKMS will be supported using a translator. See section 5.4.2 for more details on the translator capabilities.

(U//FOUO) This translation functionality will:

- (U//FOUO) Permit the exchange of accounting transactions, electronic key packages and formatted plain text messages between KMI and EKMS, as required
- (U//FOUO) Provide the KMI user community with the ability to communicate with EKMS utilizing a KMI Client node
- (U//FOUO) Facilitate the transition of EKMS users to KMI CI-2.

(U//FOUO) The EKMS translator will reside between the PRSN and the EKMS message server infrastructure. The EKMS translator will record an audit trail for the exchange of information between the two systems. KMI and EKMS will be able to review translator audit data as needed. For more information on the concepts for KMI / EKMS interoperability, see Section 5.4.2.1.1.

5.3.3.12 (U) Destruction

(U//FOUO) Cryptographic products must be destroyed upon reaching their expiration date. To facilitate timely destruction of superseded cryptographic material, the KMI will automatically notify the KOA Manager at the end of the crypto period for the material. The KMI will securely destroy, in accordance with applicable destruction standards, all sensitive cryptographic material in its possession upon command by an authorized KMI manager with the necessary privileges. An interface will be provided on the client Nodes for operators to specify key material to be destroyed. To prevent the inadvertent destruction of material, the KMI will always ask the operator if they are sure they want to destroy the material. Any KMI component (i.e. PRSN, PSN, FD, AKP, and MGC) that has the ability to store classified or sensitive key will also have the ability to zeroize those keys. The KMI will accept destruction reports for all accountable items through electronic or physical mechanisms.

5.3.4 (U) KMI Operating Accounts

5.3.4.1 (U) Overview

(U//FOUO) KMI CI-2 will introduce the concept of a KOA. While a KOA is similar in principle to a COMSEC account, its real purpose is to serve as an organizing construct for the set of key destination (e.g., ECUs, AKPs, and transfer devices) associated with a particular organization or unit. In the CI-2 timeframe, all KOAs will also be COMSEC accounts. As the population of KMI-aware ECUs supported by OTNK grows, in the future some KOAs may no longer need to be COMSEC accounts if, for example, all of the KOA's ECUs are not COMSEC-accountable, and they are benignly keyed with key products that are tracked but not COMSEC-accountable. Since an AKP provides the capability to reroute or expose key material, any KOA equipped with an AKP will be a COMSEC account for the foreseeable future.

(U//FOUO) Hardware accountability: Like a COMSEC account, the KOA is the organizing construct for ECU "ownership." The KMI recognizes only one KOA as the owner of an ECU, and will allow additional KOAs to receive key for that ECU only with the permission of the owning KOA. ECUs will be registered with classification and community attributes and can be assigned only to KOAs having the corresponding attributes.

(U//FOUO) Like a COMSEC account, the KOA is the organizing construct for key distribution profiles. A CONAUTH or Product Requestor places KOAs on the account distribution profile for a key product, and thereby specifies which KOAs will receive that key. The KOA Manager manages device distribution profiles for the key products the KOA receives. The KMI will wrap the keys so that it can be unwrapped by the ECUs on the Device Distribution Profile. Keys will be labeled with classification and community attributes and can be distributed only to KOAs having the corresponding attributes; similarly within a KOA keys can only be assigned to ECUs having appropriate security attributes.

5.3.4.2 (U) Makeup of a KOA

(U) A KOA is:

- (U) A logical entity for organizing KMI support to a set of users, devices and/or systems. In many cases the users and devices are associated with an owning organization (e.g., a military unit). In other cases the users and devices may be the operators of a system that requires KMI products to operate.
- (U) Associated with a unit or organization of some sort that is the source of the requirement for the KOA and responsible for its operations
- (U) An entity that other KMI and EKMS community members can specify as a destination to which key products can be sent.

(U) A KOA is the KMI equivalent to an EKMS Tier 2 element. It has an identity, with associated administrative and technical information, and also has personnel and equipment associated with it. This collection of KOA attributes can be illustrated hierarchically:

- (U//FOUO) Information (similar to EKMS Common Account Data) plus the following specifics (likely some overlap with common account data)
  - (U//FOUO) KOA number would be usable in the EKMS environment, but EKMS might only see a subset of number, depending on whether we need more identifying information for KOAs
- (U//FOUO) Personnel
  - (U//FOUO) KOA Managers (Primary, 1st alternate, one or more additional "working" KOA Managers) The organization that created the KOA (the parent enrollment domain) is responsible for assigning the primary and 1st alternate and identifying their successors as personnel change.
  - (U//FOUO) KOA Agent associated with the KOA. KOA Agents are responsible for getting key from the KOA to ECUs if the key is moved in fill devices.

782 ▪ (U//FOUO) A KOA Manager has the privilege to add and delete KMI
783 Users from the list of KOA Agents that can retrieve key associated
784 with this KOA
785 ▪ (U//FOUO) KOA Agents are not KMI Managers, and do not require
786 KMI Manager credentials
787 ▪ (U//FOUO) Any given KMI User may appear on the list of KOA
788 Agents for multiple KOAs
789 ▪ (U//FOUO) KMI customer organization may implement a process for
790 approving Basic Users to be KOA Agents. KOA Managers must
791 follow their organization's policies when identifying KOA Agents for
792 their KOA. The KMI does not maintain a master list of approved
793 KOA Agents.

794 • (U//FOUO) Equipment: ECUs and FDs associated with the KOA. ECUs and
795 FDs are destinations for key. In order to ensure that key is not improperly
796 directed to an unsuitable ECU or FD, ECUs and FDs need associated RuBAC
797 attributes to enable the KMI to make informed decisions permitting or denying
798 requested key distribution actions. Categories of equipment that may be
799 associated with a KOA are:
800 o (U//FOUO) Benign-fill capable devices. Such devices will have FIREFLY
801 credentials associated with them. Benign fill credentials will be held:
802 ▪ (U//FOUO) Locally if KOA has an AKP-equipped client
803 ▪ (U//FOUO) At the PRSNs for OTNK ECUs
804 o (U//FOUO) BLACK-fill capable devices. Such devices will have KEKs
805 associated with them. Copies of BLACK fill KEKs will be available locally if
806 KOA has an AKP-equipped client
807 o (U//FOUO) Legacy RED fill ECUs. There is no reason to register such ECUs
808 or associate them with the KOA technically but such ECUs may be associated
809 with the KOA for purposes of accountability.

810 • (U//FOUO) Fill Groups: Fill groups are virtual destinations for key products.
811 They are created and managed by the KOA Manager, and comprise collections of
812 functionally or operationally equivalent ECUs or FDs associated with the KOA.
813 Characteristics of fill groups include:
814 o (U//FOUO) A fill group is a locally (i.e., within the KOA's MGC) determined
815 and maintained group of ECUs or fill devices
816 o (U//FOUO) Fill groups should have a convenience label unique with the KOA
817 for which the fill group is established

818 ### 5.3.4.3 (U) KOA Manager and KOA Agent Privileges

819 (U//FOUO) There are certain privilege KMI functions available to KOA Managers. It is
820 conceivable that not all KOA Managers for a KOA should be able to exercise all
821 privileges. KOA Agents also requires a set of privileges, but they are not KMI Managers.

822 #### 5.3.4.3.1 (U) KOA Manager Privileges:

823 (U//FOUO) In addition to the specific KOA Manager privileges identified here, a KOA
824 Manager can exercise all of the privileges associated with a KOA Agent.

- (U//FOUO) Maintain KOA administrative information in KMI (except for centrally managed data element like a highest classification indicator)
- (U//FOUO) Request the cognizant Enrollment Manager to add or remove KOA Managers from the list of KOA Managers for the KOA (at least the primary and 1st alternate KOA Manager should be able to exercise this function to manage the set of "working" KOA Managers that assist them with KOA operations)
- (U//FOUO) Add / remove KOA Agents from the list of KOA Managers for the KOA (primary and 1st alternate KOA Manager)
- (U) Add / remove ECUs from the Device Distribution Profile (DDP) associated with the KOA
- (U) Add / remove ECUs / FDs from the locally maintained fill group
- (U) Assign key product to ECUs / FDs in the locally maintained fill group
- (U) Cancel key product for ECUs / FDs in the locally maintained fill group assignment
- (U) Activate ECU for seed key conversion
- (U) Upload new credentials for ECU in the appropriate DDP to a PRSN
- (U) Identify new KEK for an ECU in a DDP
- (U//FOUO) Associate a short title with an OTNK ECU for ECU-initiated key retrievals
- (U) Cancel a short title / ECU association
- (U//FOUO) Associate a short title with a benign fill / BLACK fill ECU for automated wrapping of routinely superceded key (convenience feature)
- (U//FOUO) Download a BLACK key into a Fill Device (this fill device could then be given to a KOA Agent, but in this case, where the fill device could expose the key in RED form, the involvement of a KOA Manager in the process is needed to ensure that key is not distributed in an uncontrolled manner)
- (U) View tracking reports of tracked and accountable events associated with the KOA
- (U) Review device distribution profiles by viewing the assignment of ECUs and key products to fill groups

5.3.4.3.2 (U) KOA Agent Privileges

(U//FOUO) A KOA Agent can exercise the following privileges when connected to a PRSN

- (U) Download a benign key for an ECU associated with the KOA Agent's KOA
- (U) Upload benign fill credentials for an ECU
- (U) Upload fill device tracking / audit information (including ECU acknowledgements of keys loaded)

5.3.5 (U) CI-2 Communications

(U) Consistent with Objective 1 of Section 5.1, CI-2 will move KMI communications away from the current EKMS dependence on dial-up connections to primarily use TCP/IP-based network communications.

5.3.5.1 (U) Communications Backbones

(U//FOUO) CI-2 will provide network access points to request and receive KMI products and services on the NIPRNET, SIPRNET, and public Internet. KMI clients and nodes will be designed and implemented with the intent of operating across standard networks. In addition to the use of wide-area Transmission Control Protocol / Internet Protocol (TCP/IP) networks, KMI communications will also be possible across campus-area networks on military posts, camps, bases and stations, shipboard networks, and other networks connected to the backbone wide-area networks.

(U//FOUO) In addition to network-based communications between the KMI and various KMI clients and ECUs, the communications between PRSNs, the PSNs from which they obtain products, and the CSN will also be handled via TCP/IP networks, with strong VPN protection applied to those communications interactions.

5.3.5.2 (U) KMI Protected Channels

(U//FOUO) Because KMI communications will be flowing across general purpose DoD networks, there is a need to provide I&A of the endpoints of these communications, and protect the integrity and confidentiality of the information flowing between them. That protection will come through the use of virtual private networking, Transport Layer Security (TLS), and other security protocols to establish KMI Protected Channels (KPCs). The specific security services, security mechanisms, and level of assurance of a KPC depend on the channel's purpose and environment. Consequently, KPCs may be established using a range of devices and strengths of mechanism appropriate to the need, with stronger mechanisms being used, for example, to protect the submission of orders to the KMI than would be needed when protecting the retrieval of key material that is benignly wrapped for a specific recipient device.

(U//FOUO) For MGCs used for sensitive KMI functions, such as use by an Enrollment Manager or KOA Manager, the node will need to be dedicated to KMI functions in addition to being protected by a strong KPC based on HAIPE capabilities integrated into the AKP.

5.4 (U) Modes of Operation for the Proposed System

5.4.1 (U) KMI Access Control Concepts

(U//FOUO) Privileging and access control are central to the KMI mission, and pervasive throughout the KMI concept of operations. These concepts are integrated into each of the Concept of Operations storyboards.

(U//FOUO) The KMI Access Control Framework uses three different access control models in ways intended to complement each other: Role-, Rule-, and Approval-Based

Access Control. These concepts are summarized in this section. The topic of KMI access control is dealt with at length in Volume 3 of the SDRS.

(U//FOUO) KMI utilizes several Identification and Authentication (I&A) concepts ranging from Type 1 (I&A) certificates to user name and password/PIN. KMI will use a Type 1 I&A mechanism to establish the identity for device and non-device entities for the purpose of authenticating KMI-aware devices and identifying and authenticating KMI Managers. In most instances, a DOD PKI certificate or user name and password/PIN will be used to identify and authenticate personnel serving in non-management roles (i.e., KOA Agent).

5.4.1.1 (U) Role-Based Access Control

(U//FOUO) RoBAC is used to grant broad KMI functions to certain groups of KMI Managers. KMI Managers who have been conferred a "role" are thereby granted the ability to perform the "functions" associated with that role. Additional privileges will be granted to KMI entities using the enrollment process. For example, KMI has defined a "Product Requestor" role. KMI Managers granted the Product Requestor role have access to the KMI automated functions necessary to request generation and distribution of KMI products. The process of granting a KMI User a KMI role is called "enrollment." So we say that a KMI User has been "enrolled" as a Product Requestor. The only non-manager role in the KMI is a KOA Agent.

5.4.1.2 (U) Rule-Based Access Control

(U//FOUO) KMI products—especially key products—are used to protect information that ranges from unclassified to TOP SECRET compartmented. There is no more important mission for the KMI than ensuring that classified cryptographic products are not released to entities that are not cleared to receive them. The large number of special accesses used within the cryptologic community makes use of an access control approach specially designed for processing of clearances, security categories and related access control rules (such as country releasability) a good choice for KMI. RuBAC will be used in combination with RoBAC to provide this dimension of KMI access control. Where RoBAC is concerned with matching KMI Managers with broad groupings of KMI functions, RuBAC is strictly concerned with ensuring that access to information is limited to those KMI Managers who hold the privileges associated with the information's sensitivities. In the KMI application, privileges associated with KMI Managers will generally be clearances, security category accesses, and national affiliation. Sensitivities associated with KMI products will be the corresponding classifications, security categories, and national releasability determinations.

5.4.1.3 Approval-Based Access Control

(U//FOUO) The combination of broad allocation of functions based on Roles, and Rule Based privileges based on clearances, security categories and national affiliation will not always provide sufficient granularity of control for the KMI. Key distribution is controlled on a "need to know" basis, with specific KOAs authorized to receive specific key. In addition, some KMI operations may need to be regulated for other than security-related reasons; for example, where logistical considerations apply in determining

whether or not an order can be filled. This sort of control need the fine-grained access controls that only humans, using their judgment can provide. In the KMI, controlling access to information or functions based on human judgment is referred to as "Approval Based Access Control," but the accepted technical term for this kind of technology is "Identity Based Access Control," or simply, "Access Control Lists."

5.4.2 (U) Interoperability Considerations

5.4.2.1 (U) Interoperability with US Legacy Key Management Systems

(U//FOUO) The KMI's evolution is primarily targeted at providing one-stop key management support for the evolving cryptographic devices, components, and systems (hereafter referred to as ECUs) that will result from the CMI. The CMI will introduce new key management techniques and methods that utilize modern technology, new cryptographic algorithms and network-centric communications. KMI CI-2 establishes the foundation for the ordering, generation, delivery and tracking of key management products and services that will be needed in support of CMI ECUs.

(U//FOUO) In the long term it is expected that legacy ECUs with be replaced by CMI-compliant ECUs, and supporting legacy key management systems like EKMS and the Defense Message System (DMS) PKI will be retired. While this is an admirable goal it will take years to accomplish. There are several potential approaches to defining the relationship between KMI and these existing systems, and to supporting legacy devices:

- (U) KMI could be built to provide products and services to legacy devices along with evolving CMI required products and services
- (U) KMI could be operated as another stovepipe system, or
- (U) KMI could be interoperable with existing systems and provide a common front door for all user community access.

(U//FOUO) The KMI CI-2 designers are taking the third approach, a KMI "common front door", that will provide the user community with a single access point for all key management products and services provided by existing and future KMI increments. This common access point will sustain compatibility with existing manual operations and electronic mechanisms, and will also provide on-line access for direct ECU interaction and for interactions between KMI and MPMSS.

5.4.2.1.1 (U) CI-2 / EKMS Interoperability

(U//FOUO) In the CI-2 timeframe interoperability with EKMS and the traditional key management activities will be supported using the EKMS translator described in Section 5.3.12. This translator concept is based upon the following presumptions:

- (U//FOUO) Distribution will be done in accordance with the EKMS Supplemental Ordering and Distribution Agreement that is in effect at the time of CI-2 fielding.
- (U//FOUO) All movement of accounting transactions, distribution management transactions, electronic key packages and formatted plain text messages between EKMS and KMI will occur via the translator (e.g., there will be no CI-2 Client to EKMS LMD/KP direct connections).

- (U//FOUO) Registration and FF credential data exchange will exist between the EKMS directory server and its KMI equivalent to maintain data consistency. Each system will only maintain its own directory element. Synchronization will be bi-directional.
- (U//FOUO) All data exchanged between KMI and EKMS will occur between system elements of the same classification level.
- (U//FOUO) The KMI AKP will be cryptographically compatible with the EKMS KP for key exchange.
- (U//FOUO) No major hardware/software changes will be required to EKMS to accommodate interoperability with the KMI CI-2.
- (U//FOUO) Key generated at a PSN must be able to be distributed to EKMS users, KMI users, or a mixture.
- (U//FOUO) The KOA numbering scheme will be compatible with the operational EKMS numbering scheme.

(U//FOUO) It is important to note that key material can be ordered with the resulting key products delivered to both EKMS and KMI users using the following options:

- (U//FOUO) Via a PRSN, for PSN generation, using a KMI Client
- (U//FOUO) Via an EKMS LMD or EKMS LMD/KP, for Tier 0 generation
- (U//FOUO) Received and manually entered at Tier 1 for Tier 0 or Tier 1 generation

(U) The translator enables interactions between EKMS and KMI including:

- (U//FOUO) Key generated and wrapped at an EKMS LMD/KP can be sent to and unwrapped by a KMI AKP and vice versa, with the key material transfer routed through the EKMS messaging system, translator, and KMI PRSN.
- (U//FOUO) KMI accounting information can be received and processed by Tier 0, Tier 1 and Tier 2 elements. KMI Clients will supply the accounting information expected by EKMS to ensure the success of distribution transactions.
- (U//FOUO) EKMS accounting transactions can be received and processed by a KMI Client Node.
- (U//FOUO) EKMS distribution transactions can be received and processed by a KMI Client Node.
- (U//FOUO) EKMS plain text message transactions can be received and processed by a KMI Client Node[4].
- (U//FOUO) KMI formatted plain text message transactions can be received and processed by Tier 0, Tier 1 and Tier 2 elements.
- (U//FOUO) Translator audit data can be reviewed and analyzed by EKMS and KMI.

[4] This would occur between KMI and EKMS elements of the same classification, as stated in the presumptions listed earlier.

(U) Specific translator capabilities that will not be supported are:

- (U//FOUO) Key order and privileging information between KMI Client and EKMS LMD/KP
- (U//FOUO) Data exchange between KMI and EKMS elements with different classifications
- (U//FOUO) Parent/Sub relationship support between KMI and EKMS
- (U//FOUO) Explicitly controlled key exchange between KMI and EKMS
- (U//FOUO) Single encrypted key[5] exchange between KMI and EKMS (Note: Key exchanges utilizing an EKMS Bulk Encryption Transaction (BET) are possible).
- (U//FOUO) EKMS User Application Software (UAS) transactions between KMI and EKMS

5.4.2.2 (U) Foreign Interoperability/KMI access

(U//FOUO) In the CI-2 timeframe there is no direct connection (i.e., system to system) planned to achieve interoperability with Allied or coalition key management infrastructures for classified products and services. Interoperability with Allied/coalition PKIs will be accomplished through a certification authority bridge in the CI-2 timeframe (e.g., the Federal Bridge Certification Authority)

(U//FOUO) Today's operational environment mandates effective interoperability across the DoD community and when operational needs dictate, with an often dynamically changing set of Allies and coalition partners. In addition to its support for the DoD community, KMI is designed to provide Allies and coalition partners access to appropriate products and services to support ECU interoperability.

(U//FOUO) KMI CI-2 will establish segregated enclaves to accommodate access to KMI for various communities of interest (COIs). The CI-2 architecture provides for two distinct enclave types, one for ordering and managing products and service, and one for delivery of benign products and services.

(U//FOUO) OMEs will be deployed for the US, NATO and CCEB communities. Members of these enclaves will be enrolled as KMI managers and use a Type 1 I&A PKI certificate for identity verification. These managers will utilize an MGC that connects to an OME. Product ordering and management for any coalition COIs, through the KMI, will be handled by an appropriately-privileged KMI manager who is a US citizen. In all cases, a KMI manager who is appropriately privileged and a member of one of the OME COIs can only authorize CI-2 products and services for distribution in CI-2.

(U//FOUO) CI-2 will provide PDEs for retrieval of benign products and services. These enclaves are viewed as database and web server implementations that allow authorized users from any community to access and download their designate products and services. Separate PDEs will support the US, NATO, and CCEB communities. Additional PDEs will be deployed as needed in support of coalition communities. Access to specific PDEs for retrieval of products will be based on verification of I&A data; each PDE will be

[5] This is reference to EKMS transaction 109 (key distribution). The Tier 2 only implements this transaction.

configured to use an I&A mechanism suitable for the COI that it supports (e.g., certificate-based; user name and password/PIN). Users retrieving benign products will require a PC running a KMI –compatible browser and using an approved I&A mechanism. The minimum acceptable I&A mechanism is a password/PIN recognized by the KMI.

5.5 (U) KMI Roles

(U) This section describes the set of roles that have been defined to operate KMI CI-2. A role identifies a job that needs to be performed and groups together access to the system functions needed to perform that job. The need for a role does not correspond to the need for a person; depending on the nature of the role and the workload at a particular operational location, a role may be one of many "hats" worn by a single person or it may require several people to perform the job. Some roles will require very little time and can be an assigned duty for a suitable individual, whereas in large COMSEC operations some roles may require several full-time people to accomplish the mission. For security reasons, certain roles must be assigned to separate individuals. For example, registration and issuance of a Type 1 PKI certificate to a user requires at least two separate authorized individuals, one performing the role of the Personnel Registration Manager and one performing the role of the Local T1 Registration Authority. Within constraints set by KMI to preclude certain combinations of roles, the allocation of roles to people is left to the determination of each organization using the KMI.

(U) Management roles can divided into both internal and external classes. This division of roles is depicted in Table 1. The management roles also can be divided into operational and administrative. Operational managers use KMI-issued Type 1 credentials to authenticate their identity to the system, and they obtain authorizations for their actions through KMI's role-based, rule-based, and approval-based access control mechanisms.

1085 **Table 1 (U) KMI Roles**

Role Types	Role Names
External, operational management roles	Ordering-and-distribution managers • User Registration Managers: – Controlling Authority – Command Authority • Product Requester • KOA Manager Registration managers • KOA Registration Manager • Personnel Registration Manager • Device Registration Manager (includes KLIF Mgr.) • Local Type 1 Registration Authority Access control managers • Enrollment Manager User support managers • Service/Agency Help Desk Manager
External, administrative management roles	Client Node administrators • Client Platform Administrator • Client Platform Security Officer
Internal, operational management roles	Access control service managers • Role Manager • Top-Level Enrollment Manager User support service managers • Library Manager • Help Desk Manager • Event Service Manager Catalog service managers • Catalog Manager
Internal, administrative management roles	Security administrators (a.k.a., System Security Officers) • ASWR Manager • Audit Data Manager • Security Configuration Manager • Incident Response Manager Core Node administrators • Platform/Network Manager • Archive Manager • Backup Manager Database managers • Accounting Data Manager • Tracking Data Manager
Non-management roles	Non-management users • KOA Agent

1086 ### 5.5.1 (U) External Operational Management Roles

1087 (U//FOUO) External operational management roles are assigned mainly to Managers in
1088 customer organizations. These managers are primarily concerned with registration,
1089 enrollment, and product management functions in a particular customer organization or
1090 some sub-unit of such an organization.

(U//FOUO) External management roles are assigned to KMI operational managers in customer organizations who:

- (U) Connect to the KMI exclusively across network interfaces
- (U) Receive their privileges through the KMI manager enrollment process
- (U//FOUO) Authenticate themselves to the KMI using KMI manager credentials
- (U) Have their access to the KMI mediated by the role-, rule-, and approval-based access controls described in the "KMI Access Control Concepts" Section.

(U) The one exception to this description is for client administration roles, described in section 5.5.2. External operational managers are primarily concerned with registration, enrollment, and product management functions. In addition to external operational managers, there are also internal operational and administrative managers (described below), who deal with both the security of the KMI and the internal operation of KMI central nodes.

5.5.1.1 (U) Ordering and Distribution Managers

(U//FOUO) The roles in this category are oriented toward product management functions. Approval-based access control involves the four management roles that deal directly with product ordering and distribution: CONAUTH, Command Authority, Product Requester, and KOA Manager. Enrollment Managers in KMI customer organizations assign identities to these four roles through the role-based access control process. Users are expected to be selected for these roles based on organizational affiliation, geographical location, and other operational factors.

5.5.1.1.1 (U) Controlling Authority

(U//FOUO) The Controlling Authority role is assigned to external managers responsible for determining what key products are operationally needed, and (optionally) identifying the individuals responsible for more detailed management of those products. Controlling Authorities perform the following functions:

- Controlling Authority defines new product. A Controlling Authority can define a new product, (e.g., "Product A"). The Controlling Authority also can place orders for generating and distributing that product, or the Controlling Authority can delegate responsibility for ordering by appointing Product Requesters
- Controlling Authority appoints Product Requester(s). The Controlling Authority for Product A can optionally select one or more user identities that have been enrolled as Product Requesters and authorize them to place orders for the product. (The selections are not constrained by enrollment domains.) The Controlling Authority can require that orders placed by a Product Requester receive per-edition approval before the product is generated and distributed. If such approval is required, the Controlling Authority acts as the approver.
- (U//FOUO) Controlling Authority or Product Requester orders products for operating account(s). A Controlling Authority or an authorized Product Requester can order Product A (i.e., can request that Product A be generated and be distributed to devices under the control of selected KOAs).

5.5.1.1.2 (U) Command Authority

For each specific KMI asymmetric product, relationships are established among the managers. A Command Authority requests the assignment of partition codes and Department/Agency/Organization (DAO) codes for the symmetric products the Command Authority's organization requires. The Command Authority identifies which partition codes and DAO codes may be ordered by each Product Requester.

5.5.1.1.3 (U) Product Requestor

(U//FOUO) A Product Requester is an external manager that is responsible for requesting products and services. Product Requesters must be enrolled as Managers, and their privileges with regard to ordering specific KMI products are then defined by the Product Manager (either Controlling Authority or Command Authority) responsible for those products, using KMI's approval-based access control process. Product Requesters who order asymmetric products perform a function equivalent to User Representatives in existing FIREFLY key management processes.

5.5.1.1.4 (U) KOA Manager

(U//FOUO) A KOA Manager is an external manager who is responsible for the operation of one or more KOAs. KOA Managers are the KMI equivalent of COMSEC custodians / COMSEC managers in the existing system. A KOA Manager manages the distribution of KMI products to the ECUs, fill devices, and AKPs that are assigned to the manager's KOA. The KOA Manager is also responsible for designating and registering KOA Agents.

5.5.1.2 (U) Registration Management Roles

(U) Registration managers are the external manager responsible for making people, devices, and KOAs "known" to the KMI. Each of those three registration functions is distinctive and is addressed with a distinct registration manager role.

5.5.1.2.1 (U) KOA Registration Manager

(U) KOA Registration Manager is the role assigned to individuals responsible for maintaining registration information about KOAs. This information is retained in a data store (e.g., possibly a directory) internal to the KMI; information elements common to both KMI and EKMS are synchronized between the KMI registration data store and the EKMS directory server.

(U//FOUO) Since all KOAs will also be COMSEC accounts in CI-2, there is a need for close coordination between EKMS registration authorities and the KOA Registration Manager. The CI-2 concept is that these duties will be assigned to the same person(s). For the military services, the EKMS Registration Authority is located with the Tier 1 system; the person(s) performing that function will be enrolled as KOA Registration Manager and provided with KMI client node and manager credentials so that they can perform both functions. (U) Personnel Registration Manager

5.5.1.2.2 Personnel Registration Manager

(U//FOUO) Personnel Registration Managers are responsible for registering human users to the KMI). This role will fall under separation of duties considerations. In particular, a Personnel Registration Manager cannot also be a Local Type 1 Registration Authority. The basic functions of a personnel registration manager include:

- (U) Registration of KMI users
- (U) Ability to add, modify, update and delete registration data
- (U) Works with local sponsor/authority to obtain information required to establish an individual's Type 1 identity
- (U) Independently verifies the need for the identity
- (U) Enters the required registration information into KMI using a KMI Manager

5.5.1.2.3 (U) Device Registration Manager

(U) Device Registration Manager is the role assigned to individuals responsible for the registration of devices (i.e., equipment such as ECUs) in the KMI. Device Registration Managers register and initialize ECUs, Type 1 I&A tokens, and any other KMI devices into the KMI, request initial ECU key material (e.g., seed key).

5.5.1.2.4 (U) Local Type 1 Registration Authority

(U) Local T1 Registration Authority is the role assigned to individuals responsible for the endorsement and provisioning of CMI (KMI Aware) and KMI manager Tokens. The basic functions of a Local Type 1 Registration Authority include:

- (U) Performs the face to face check of the user receiving the Type 1 certificate and token
- (U) Processes the individual to obtain their Type 1 token
- (U) Uses a KMI Manager (Client) to process a certificate request and download Type 1 certificate onto a token

5.5.1.3 (U) Enrollment Manager

(U) Enrollment Manager is the role assigned to those individual responsible for assigning KMI User Identities to management roles. The Enrollment Manager also assigns rule-based attributes to KMI manager identities and assigns privileges to a Type 1 identity that has been issued for use in KMI. The Enrollment Manager is a particularly security-sensitive role, as this manager's actions determine what other KMI managers may do. Consequently, this role will fall under separation of duties considerations. In particular, an Enrollment Manager cannot also be a Personnel Registration Manager.

5.5.1.4 (U) Service/Agency Help Desk Manager

(U) Help support for KMI users will be provided by a mixture of customer organization-specific help staff (external) and KMI-wide help staff (internal). Service/Agency Help Desk Manager is the role assigned to external personnel providing customer organization-specific help services.

5.5.2 (U) External Administrative Management Roles

(U) Client administration roles are associated with the need to provide operational and security management and administration for client nodes. While these functions are external, taking place at the client location rather than within central KMI nodes such as the PRSN or PSN, these are not operational manager roles in the KMI and therefore do not require a KMI manager token. Access control for these roles is provided by the client platform operating system's user access control (e.g., name and password login to the platform) combined with physical limitations on access to the client. These roles will normally be assigned to information technology support staff at the customer's operational facility.

5.5.2.1 (U) Client Platform Administrator

(U) Client Platform Administrators are responsible for establishing and assigning platform-based user accounts (for which the authentication material typically is a password), including platform operators, and for setting their privileges, and also for operating system maintenance and updating, etc.

5.5.2.2 (U) Client Platform System Security Officer (SSO)

(U) Client Platform SSOs are responsible for security monitoring and administration of the client platform, including audit data review and archiving, etc.

5.5.3 (U) Internal Operational Management Roles

(U//FOUO) Internal KMI roles are roles assigned to personnel operating within the physical security perimeter of a centralized or regional KMI component, such as a PRSN or PSN. NSA personnel will typically staff internal roles for the CSN, PRSN, and PSN.

The roles listed in subsequent sections are independent roles. Some separation of duties requirements will apply to the security administration roles; for example, it is inappropriate for the same individual that reviews audit data to check for potential security violations to also be able to control audit collection data rules.

5.5.3.1 (U) Access Control Service Managers

5.5.3.1.1 (U) Role Manager

(U//FOUO) Role Manager is the role assigned to individuals who manage the set of roles available in the KMI. The Role Manager's function is to maintain the set of roles defined within the KMI, including the creation of new roles, the removal of unnecessary roles, and the management (i.e., addition and deletion) of the privileges accorded to roles as appropriate to the job functions of individuals who would be enrolled in those roles.

5.5.3.1.2 (U) KMI Top-level Enrollment Manager

(U) The KMI-level enrollment manager for the KMI is responsible for enrolling the highest-level enrollment manager within each KMI customer organization. Those Enrollment Managers, in turn, can either perform all enrollment functions for their organization, or enroll subordinate Enrollment Managers within their organization who will perform the enrollment of other KMI managers within the organization. When

enrolling other managers, the KMI-level enrollment manager is enabled to enroll all roles, and is able to assert all rule-based access control privileges within the KMI.

5.5.3.2 (U) User Support Service Managers

(U) The user support manager roles are related to KMI functions that need to be publicly accessible (i.e., a KMI library, Help Desk).

5.5.3.3 (U) Event Services Manager

(U) Event Services Manager is the role assigned to individuals responsible for the KMI capability that tracks security-relevant events and informs or reminds KMI users of necessary actions related to those events. The KMI provides an event management capability that tracks security-relevant events and informs or reminds users of necessary user actions to respond to those events. Events to be managed shall include the routine and emergency supersession of keys, pending expiration of a user's certificate, and mandatory modifications to equipment.

5.5.3.4 (U) Catalog Manager

(U) Catalog Manager is the role assigned to individuals responsible for managing the KMI product catalog. The KMI product catalog is the basis for presenting product information to users. The information presentation is tailored for the recipient. Catalog Managers are responsible for defining and maintaining filter criteria for the presentation of the catalog.

5.5.4 (U) Internal Administrative Management Roles

(U//FOUO) Internal management roles are assigned to personnel operating within the physical security perimeter of a centralized or regional KMI component, such as a PRSN, CSN or PSN. Internal management roles include both operational and administrative mangers. Administrative managers are responsible for managing the security and operations of the KMI.

5.5.4.1 (U) Security Administration (SSOs)

(U//FOUO) Each site or facility that houses a set of KMI components may need one or more people assigned to SSO roles. These roles group the functions related to establishing, monitoring, and maintaining the security of the KMI.

5.5.4.1.1 (U) ASWR Manager

(U) ASWR Manager is the role assigned to individuals responsible for controlling attack sensors in KMI components and for initiating a response to alerts and warnings.

5.5.4.1.2 (U) Audit Data Manager

(U) Audit Data Manager is the role assigned to individuals responsible for setting audit data collection and recording parameters in KMI components and for maintaining and analyzing the KMI audit trail.

5.5.4.1.3 (U) Security Configuration Manager

(U) Security Configuration Manager is the role assigned to individuals responsible for establishing and monitoring the security configuration parameters in KMI components.

5.5.4.2 (U) Client Node Administrators

(U) System administration managers perform functions that ensure the smooth operation of the KMI. These roles handle network and computer platform administration, archiving, backup and restoration, database management, and other functions necessary for KMI operation.

5.5.5 (U) Non-management Roles

(U) Non-management roles are assigned by KOA Managers to individuals that support "last mile" distributions activities for the KOA. These individuals are referred to as KOA Agents.

5.5.5.1 (U) KOA Agent

(U//FOUO) A KOA Agent is not a KMI management role. KOA Agents are enrolled by an Enrollment Manager but do not need Manager credentials to perform their duties. A KOA Agent is designated by a KOA Manager to access PRSN PDEs for the purpose of retrieving wrapped products that have been ordered for User Devices that are assigned to that KOA. A KOA Manager can designate registered users to be KOA Agents for any KOA to which that manager is assigned. Additionally, KOA Managers are always KOA Agents for their own KOAs.

(U//FOUO) A KOA Agent that is designated by a KOA Manager can perform the following functions when connected to a PDE of a PRSN:

- (U//FOUO) Download a benignly wrapped product for a device held by the KOA.
- (U//FOUO) Upload benign fill credentials for a device held by the KOA.
- (U//FOUO) Upload tracking, audit, and accounting information (including device acknowledgements of products loaded) from a fill device.

5.6 (U) Support Environment

5.6.1 (U) Personnel Support

(U//FOUO) Participants in the existing CMCS and EKMS are known as KMEs and are each assigned EKMS Identifiers. Information about KMEs is recorded in the EKMS directory for use throughout EKMS.

(U//FOUO) The set of EKMS IDs provides a single "name space" within which all KMEs are identified. A KME can be an individual or an organization. Since interoperability must be maintained between KMI, EKMS, and CMCS KMEs, it is necessary that identifiers for entities registered in KMI be able to be mapped uniquely to EKMS IDs and vice-versa. The following table identifies different types of KMEs, summarizes the function they play in key management, and explains how they are handled within KMI CI-2.

1322 **Table 2: (U) Key Management Entities in CI-2**

KME Type	KME Function	KMI CI-2 Concept
Central Office of Record	Maintain central accountability for COMSEC materials	Continue to operate as currently defined. KMI CI-2 is neither replacing nor replicating COR functionality, but will support transfer of accounting information as described in the "KMI Support to CMCS Accounting" section.
FIREFLY Point of Contact	The entity that is responsible for appointing Command Authorities for his organization.	Continue to operate as currently defined. FIREFLY POCs are assigned EKMS IDs and recorded in the EKMS directory, but the functions they perform are conducted off-line.
FIREFLY Command Authority	Defines FIREFLY ordering privileges for User Representatives	Registered as Manager and enrolled as KMI Command Authority. Command Authority functions are privileges within the KMI Command Authority role. Controlling Authorities will delegate specific FIREFLY key ordering privileges to Product Requestors
FIREFLY User Representative	Orders FIREFLY key with limits of ordering privileges defined by associated Command Authority	Registered as Manager and enrolled as KMI Product Requestor. Specific ordering privileges of Product Requestors for FIREFLY key are defined by a Command Authority using KMI Approval-based access control mechanisms.
COMSEC Account	Organizational element designated to receive, store, and control COMSEC material directed to an organization.	Registered as KMI Operating Account. The identifier for a KOA must be able to be mapped to an EKMS ID and vice-versa in order to maintain backward compatibility with existing KMI systems. KOAs will have an associated Primary KOA Manager and one or more supplemental KOA Managers.
Controlling Authority	Define the characteristics for and direct distribution of cryptographic key, especially symmetric key.	Registered as a Manager and enrolled as a Controlling Authority.

1323 ### 5.6.2 (U) Communications Support

1324 (U//FOUO) CI-2 will provide network-oriented key management and delivery
1325 capabilities and establish a path for transition away from the existing physical and
1326 electronic COMSEC material systems. The CI-2 design requires the interconnection of
1327 the KMI CSN, PSNs, PRSNs, and client nodes over a variety of DoD and commercial
1328 communications networks, with an emphasis on common-user TCP/IP wide-area
1329 networks (WANs) as the primary means of communications. The design of CI-2 will
1330 address needed improvements in the communications approach of the EKMS, allowing
1331 dial-up connections and dedicated communications paths to be replaced by TCP/IP
1332 network connections over a variety of communications mediums owned by a variety of
1333 organizations.

(U//FOUO) To accomplish the system and design goals, CI-2 will rely on a mixture of DoD, non-DoD governmental and commercial communications systems and networks. The networks and communications systems that may be used by CI-2 include:

- (U) TCP/IP wide-area networks
  - (U//FOUO) NIPRNET
  - (U//FOUO) SIPRNET
  - (U) Internet
- (U) Customer-owned local / tactical networks
  - (U//FOUO) Post/Camp/Base/Station/Facility networks connected to the NIPRNET or SIPRNET
  - (U//FOUO) Tactical military communications systems connected to the NIPRNET or SIPRNET

(U) Each of the above systems may be used as a vehicle to provide CI-2 services to CI-2 users and the KMI will depend upon their availability and their ability to support TCP/IP communications such as web connections, ftp, e-mail, and other electronic exchanges.

(U//FOUO) CI-2 is designed to be able to rely on these communication systems owned and managed by a variety of organizations; for reliability of KMI operations and user access to the KMI, multiple communications paths across these backbone networks are needed. By using cryptographically protected traffic wrapped in normal TCP/IP communications packets, CI-2 is able to pass black data over these communication systems without fear of compromise. The ability to support this feature enables CI-2 to remain flexible and become more available to the user community.

5.6.3 (U) Logistical Support

(U) KMI CI-2 will provide a number of features to assist the user in the operation, maintenance and life cycle support of the system including training, on-line availability of data in the KMI library, a help desk, and help features integrated into the HMI.

5.6.3.1 (U) Training

(U) The KMI will provide training programs, including both classroom and computer based on-line training. It is important that KMI users and managers receive the necessary indoctrination and become familiar with the KMI security practices before accessing the KMI. Whenever possible, existing training courses, materials, and other devices (e.g., commercially offered training courses and manuals) will be used to satisfy KMI training requirements.

5.6.3.2 (U) Status Monitoring and System Maintenance

(U) The KMI supports a worldwide customer community and must maintain operations 24 hours a day, 7 days a week. The KMI will employ the mechanisms necessary to make its processes, data, and systems as reliable as possible within the bounds of cost-effectiveness and established system performance. To meet this operational availability it is necessary to know the status of the KMI. The KMI will automatically collect and record any information regarding the current maintenance state and operational availability of the major KMI components and the communications links that service

them. This information will be made available to authorized KMI managers upon command.

(U) Maintenance of the various components of the KMI will be a mix of warranty and service contracts for Commercial off-the-shelf (COTS) products and maintenance of the AKP will follow traditional Government support possibly taking advantage of existing Service/Agency interservicing procedures. The developer will be responsible for the maintenance of the PSN, CSN, and the PRSN's.

5.6.3.3 (U) Help Desk

(U) The KMI will provide support to a staffed help desk to provide users assistance in system operation, resolution of error conditions, and general information on products and services offered by the system. The help desk function will be performed by existing EKMS Phase 4 help desk personnel residing at Tier 0 and Service-specific help desks located at Service facilities to address Service-related support functions. Some of the features to be provided are:

- Troubleshooting assistance
- A list of addresses for access to KMI services that can be configured into a KMI-aware ECU.
- List of Frequently Asked Questions

(U) The KMI Help Desk Manager will provide support in terms of all KMI policy, operational, and procedural issues. To support this role, the KMI will provide the Help Desk Manager access to all KMI customer information and functions through a query capability; provide a decision tree to guide in answering user requests; and provide a capability to add, delete, update, and determine access to contents of the online help desk

(U) The KMI help desk web page will contain at a minimum, a list of Frequently Asked Questions (FAQs), the Help Desk telephone number, and an email link to the KMI Help Desk Manager. The web page will also supply the telephone number and web address of each Service-specific help desk directing users with Service-specific issues and/or problems to these points of contact.

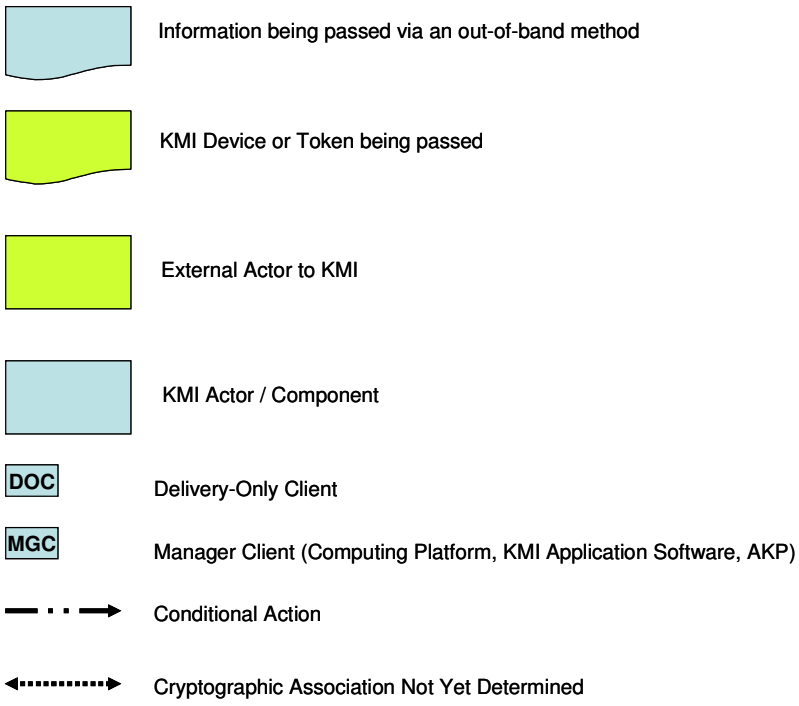
(U) When an initial call is received or a problem report or query arrives, it is placed on a tracking ticket, which remains open until the issue or query has been answered or resolved. The help desk determines the kind of technical help and information the customer may receive based on his identity and assigned role within KMI. To aid in reducing response time from help desk to users, a knowledge database is accessible containing issue and query information from prior resolutions.

6 Operational Scenarios

(U) This section depicts common operating scenarios for KMI CI-2 in the form of storyboards. The storyboards focus on the KMI user's / manager's interactions with the system, and do not attempt to describe internal operating details of the KMI. The scenario set presented here covers a number of common, important aspects of KMI operation, but does not attempt to address every KMI capability or user operation; it is intended, rather, to capture the intended nature of KMI operations.

(U) Several high-level processes have been depicted that group the defined operational scenarios with the appropriate process they belong to. These high-level processes will help to clarify the relationship between operational scenarios. The specific processes include: Manager Activation, KOA Registration, KMI-Aware Device Activation, Product Ordering and Retrieval for Symmetric Keys, and Product Ordering and Distribution for Asymmetric Keys.

(U) The legend key for the sequence diagrams in the operational scenarios:



6.1 Manager Activation Process

(U) There are several steps necessary to activate a KMI Manager, as shown in Figure 8. As a pre-requisite to this process, a new token must be initialized/registered by a KMI Device Registration Manager (using KLIF) that will later be activated for the prospective KMI Manager.

(U) Upon authorization by a Command/Controlling Authority, the prospective KMI Manager is registered by the Personnel Registration Manager. At the same time, the initialized token is endorsed by the Local Type 1 Registration Authority (LT1RA). At this stage, the token receives an Identity Certificate and an Infrastructure key which will be used in the activation process.

(U) After registration, a sponsoring organization requests that a newly registered manager be enrolled in KMI by the KMI Enrollment Manager (EM). During this process, the new KMI Manager is assigned appropriate roles and privileges. In the same timeframe, the

token is activated and personalized for the new KMI Manager by the LT1RA. The KMI Manager is then activated and ready to complete its KMI mission.

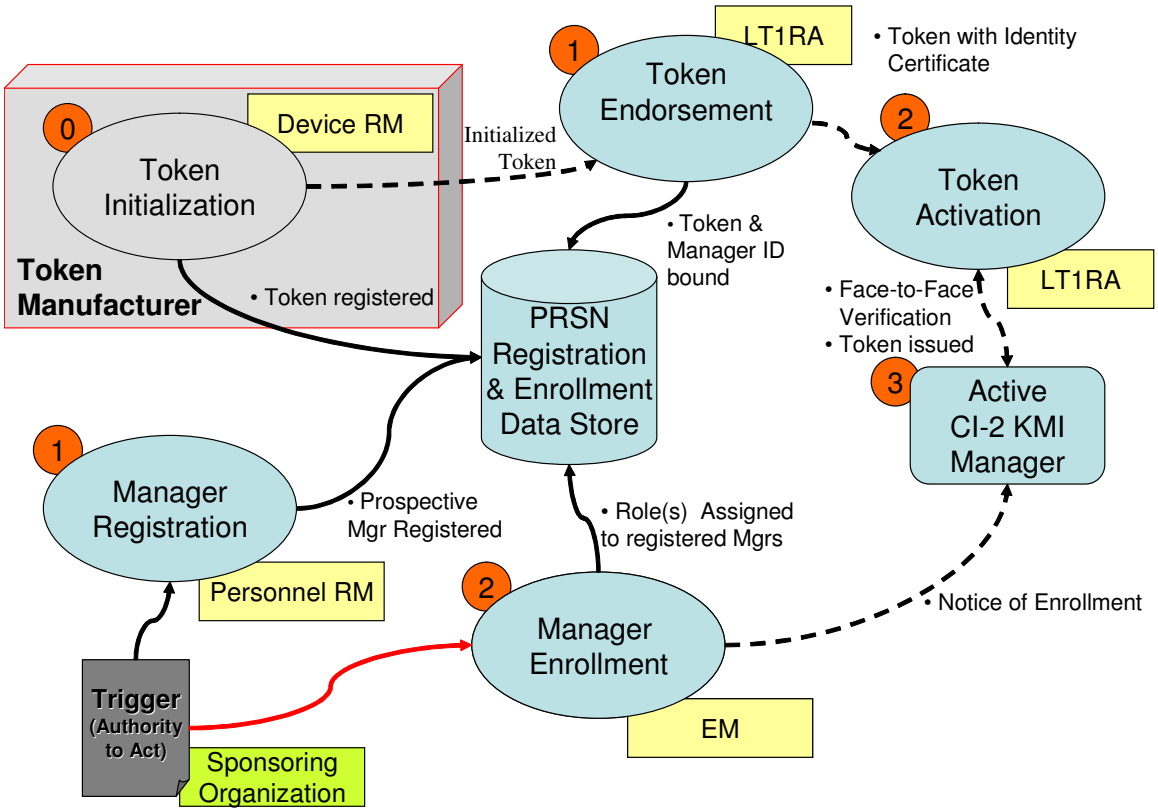


Figure 8: (U) Manager Activation Process

6.1.1 (U) Register KMI Manager

6.1.1.1 (U) Summary

(U) This scenario follows several related activities that lead to a new KMI Manager within KMI. A potential manager is identified and submitted as a candidate. They are subsequently registered within the KMI, creating a manager identity ready for enrollment, and issuances of an identity token.

6.1.1.2 (U) Sequence Diagram

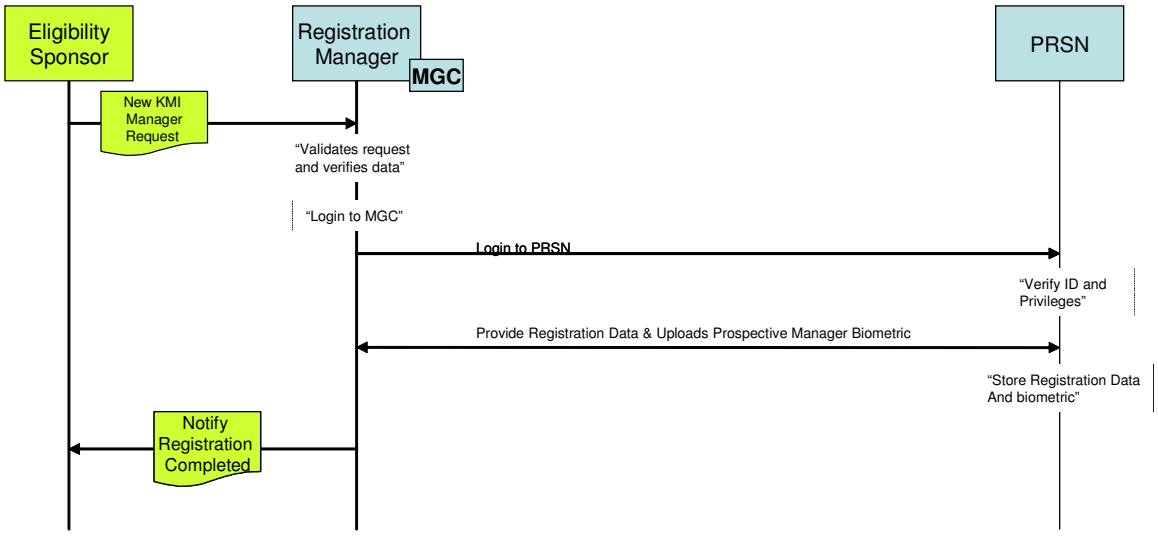


Figure 9: (U) Register KMI Manager

6.1.1.3 (U) KMI Roles Involved

- (U) Eligibility Sponsor
- (U) Personnel Registration Manager

6.1.1.4 (U) KMI Nodes Involved

- (U) Manager Client
- (U) PRSN

6.1.1.5 (U) Prerequisites

- (U) A valid need for access as a KMI Manager exists.
- (U) The candidate has not previously been registered within KMI.
- (U) Personnel Registration Manager is valid and has rights within the appropriate domain.
- (U) Photograph of prospective manager has been captured.

6.1.1.6 (U) Sequence of Events

1. (U) The eligibility sponsor identifies the need for a KMI Manager and a valid candidate, fills out a form requesting the registration and enrollment of a new KMI Manager. The sponsor gathers the required identity and clearance information and a biometric (e.g., a photo) for the candidate, and submits the data via authorized channels.
2. (U) The Personnel RM receives a request to register a new KMI Manager along with clearance verification information (via out of band method) from a sponsor. The Personnel RM validates the request and confirms the citizenship, clearance, and organization of the candidate manager according to the Type 1 Certificate Policy.
3. (U) The Personnel Registration Manager (RM) logs into the MGC.
4. (U) The Personnel RM connects and authenticates to the PRSN using a Manager Client (MGC).
5. (U) The Personnel RM provides the manager candidate's registration data and biometric to the PRSN.
6. (U) The PRSN stores the registration data and biometric.
7. (U) The Personnel RM notifies the appropriate entity (sponsor, candidate) of the registration.

6.1.2 (U) Enrollment of Manager

6.1.2.1 (U) Summary

(U) This scenario follows several related activities that lead to a new KMI Manager within KMI. A registered manager is given the privileges they need to perform their job as a KMI Manager through enrollment.

6.1.2.2 (U) Sequence Diagram

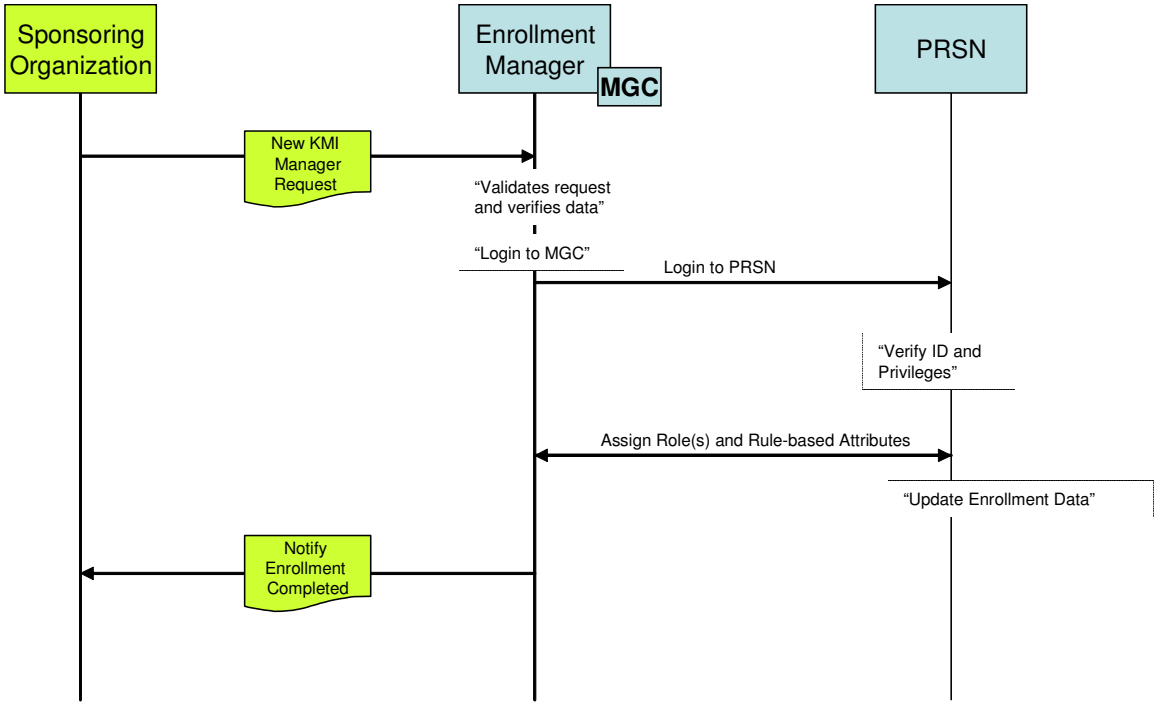


Figure 10: (U) Enrollment of Manager

6.1.2.3 (U) KMI Roles Involved

- (U) Sponsoring Organization
- (U) Enrollment Manager

6.1.2.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.1.2.5 (U) Prerequisites

- (U) A valid need for access as a KMI Manager exists.
- (U) The candidate is registered within KMI.

- (U) Participating KMI Managers are valid and have rights within the appropriate domain.

6.1.2.6 (U) Sequence of Events

1. (U) The Enrollment Manager receives a request to enroll a new KMI Manager (via out of band method) from a sponsor.
2. (U) The Enrollment Manager confirms the need for the candidate manager's requested proposed role and the validity of the request.
3. (U) The Enrollment Manager logs into the MGC.
4. (U) The Enrollment Manager connects and authenticates to the PRSN using a MGC.
5. (U) The Enrollment Manager assigns the role(s) and rule-based attributes to the candidate manager.
6. (U) The PRSN updates the enrollment data for the candidate manager.
7. (U) The Enrollment Manager notifies the appropriate entity (sponsor, candidate) of the enrollment.

6.1.3 (U) Initialization of a Token

6.1.3.1 (U) Summary

(U) This section describes the initial registration of a Token. A Token has its own identity within the KMI, and key can be wrapped specifically for that Token by a KMI PSN, using credentials stored as part of the Token's registration information in the KMI.

6.1.3.2 (U) Sequence Diagram

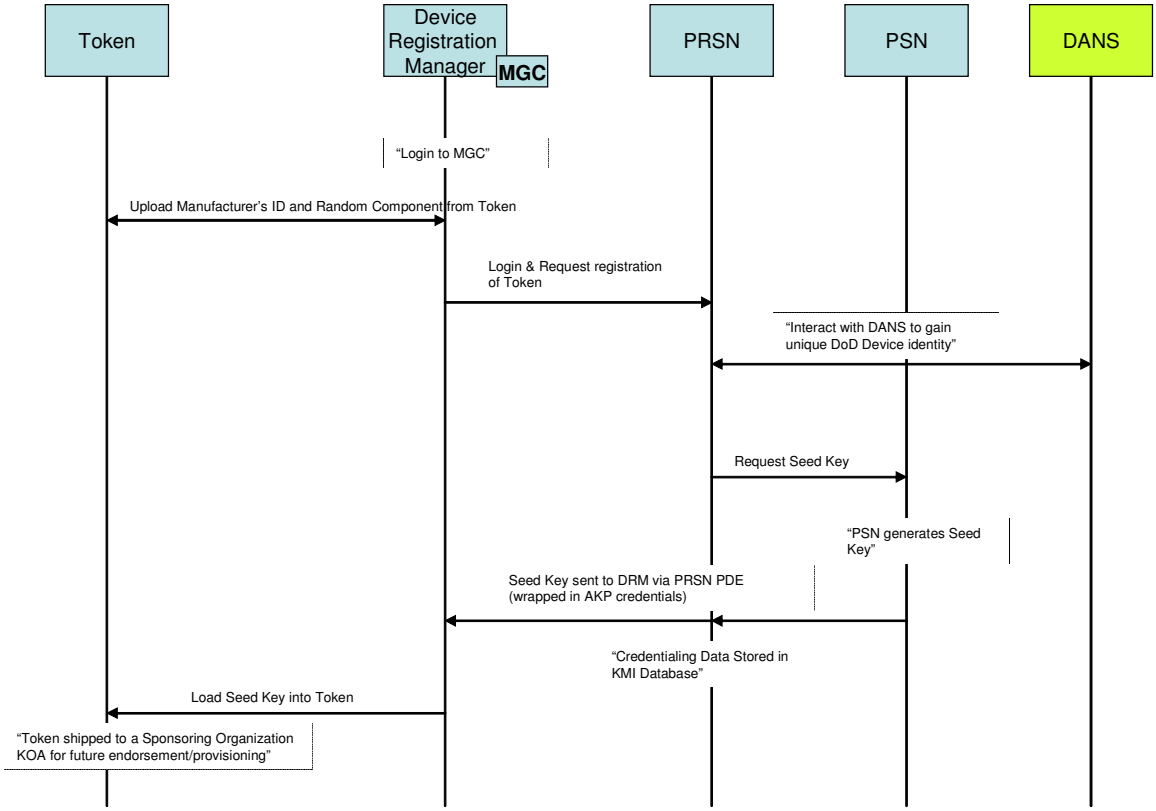


Figure 11: (U) Initialization of a Token

6.1.3.3 (U) KMI Roles Involved

- (U) Device Registration Manager

6.1.3.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN
- (U) PSN

6.1.3.5 (U) Prerequisites

- (U) The Device Registration Manager has a Manager Client (MGC).

- (U) The token has a software baseline from the factory.
- (U) The token has been designed in compliance with KMI Standards.
- (U) The Device Registration Manager is valid and has rights within the appropriate domain.

6.1.3.6 (U) Sequence of Events

1. (U) Device Registration Manager (DRM) logs into MGC and authenticates to KMI using Type 1 Identity/Token.
2. (U) DRM uploads (electronically or physically) a manufacturer's ID and random component from the Token being initialized.
3. (U) DRM logs into PRSN and requests registration of new Token.
4. (U) PRSN interacts with DoD Authoritative Naming Source (DANS) to gain a unique DoD Device Identity (aka - Device Distinguished Name).
5. (U) PRSN requests, from the PSN, a Seed Key that embeds the DANS-provided identity and the random component from the new Token. The Seed Key is linked to the DoD Identity and the Token-generated random component.
6. (U) The PSN generates the Seed Key.
7. (U) The Seed Key is delivered to the DRM via the PRSN PDE, wrapped in the AKP's credentials.
8. (U) This credentialing data is stored in the KMI database (at the PRSN) for the Endorsement process.
9. (U) DRM retrieves and loads seed key and electronic identity into the new Token. The Token is now registered in KMI.
10. (U) The Token is shipped to a Sponsoring Organization KOA and eventually to a mission location for endorsement & provisioning.

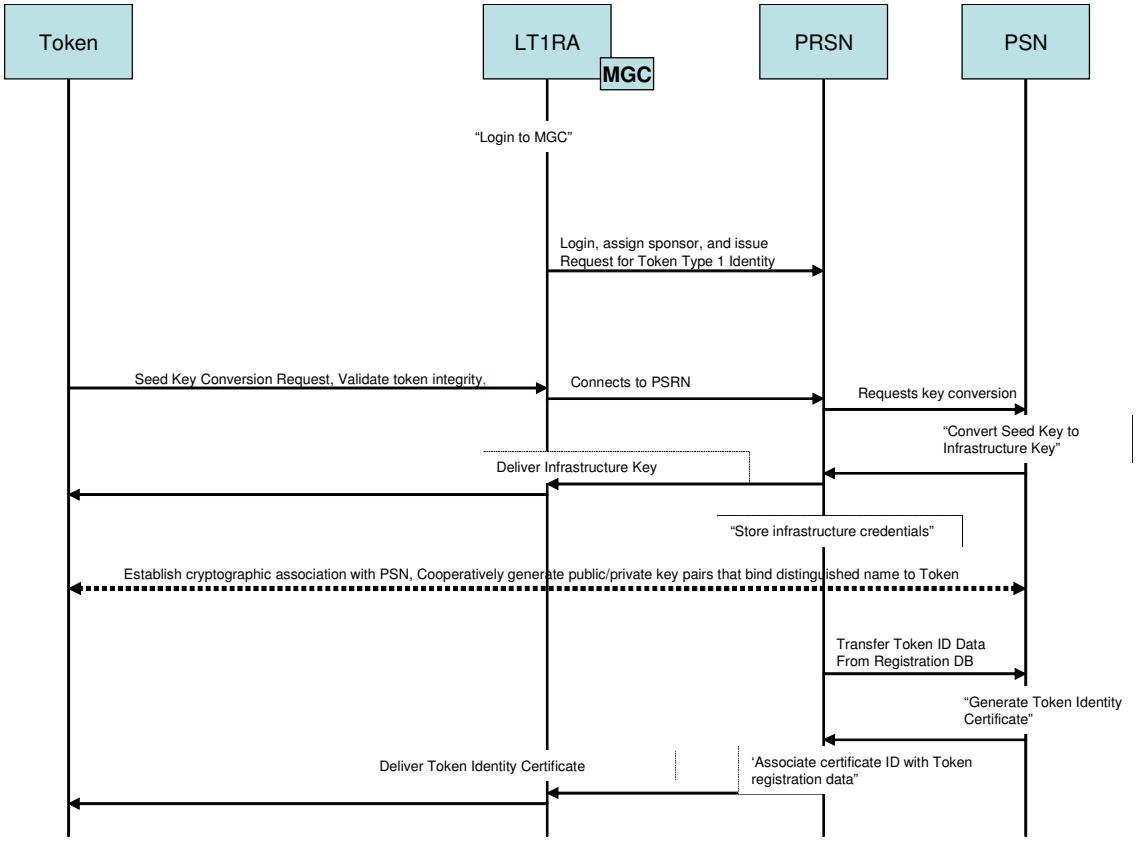
1565 ## 6.1.4 (U) Endorsement of a Token

1566 ### 6.1.4.1 (U) Summary

1567 (U) This section describes the endorsement of a Token. This process establishes a
1568 sponsor for the Token, completes the establishment of the Type 1 Token Identity and
1569 converts the Seed Key to an Infrastructure Key for the Token.

1570 ### 6.1.4.2 (U) Sequence Diagram

1571



1572

1573 **Figure 12: (U) Endorsement of a Token**

1574 ### 6.1.4.3 (U) KMI Roles Involved

1575 • (U) Local Type 1 Registration Authority (LT1RA) (Also enrolled as Product
1576 Requester)

1577 • (U) Sponsor

1578 ### 6.1.4.4 (U) KMI Nodes Involved

1579 • (U) Manager Client (MGC)

1580 • (U) PRSN

1581 • (U) PSN

6.1.4.5 (U) Prerequisites

- (U) The token has been initialized (registered) and shipped to LT1RA.
- (U) PRSN has captured token registration data to be used in the endorsement process.
- (U) LT1RA is valid and has rights within the appropriate domain.

6.1.4.6 (U) Sequence of Events

1. (U) LT1RA receives the Token (out of band process, not shown in figure).
2. (U) LT1RA logs into MGC.
3. (U) LT1RA logs into the PRSN, assigns a sponsor to the Token, and issues a request for a Type 1 Token Identity. (Note: The Identity request is built from the KMI knowledge of the token serial number/token distinguished name that occurred during the initialization process and information provided by the LT1RA).
4. (U) The Token sends a seed key conversion request.
5. (U) The PRSN connects to the PSN and forwards the seed key conversion request for the Token.
6. (U) PSN converts Seed Key to Infrastructure Key.
7. (U) PSN delivers Infrastructure Key to the Token.
8. (U) The Infrastructure credential information is stored within the PRSN.
9. (U) The Token establishes a cryptographic association with the PSN and they cooperatively generate the public and private key pairs that bind the Token's distinguished name to the Token.
10. (U) PRSN sends Token ID data from the registration data store to the PSN.
11. (U) PSN generates Type 1 certificate for the Token.
12. (U) The Type 1 Token certificate is associated with the Token Registration Data at the PRSN.
13. (U) Token receives the Identity Certificate from the PSN.

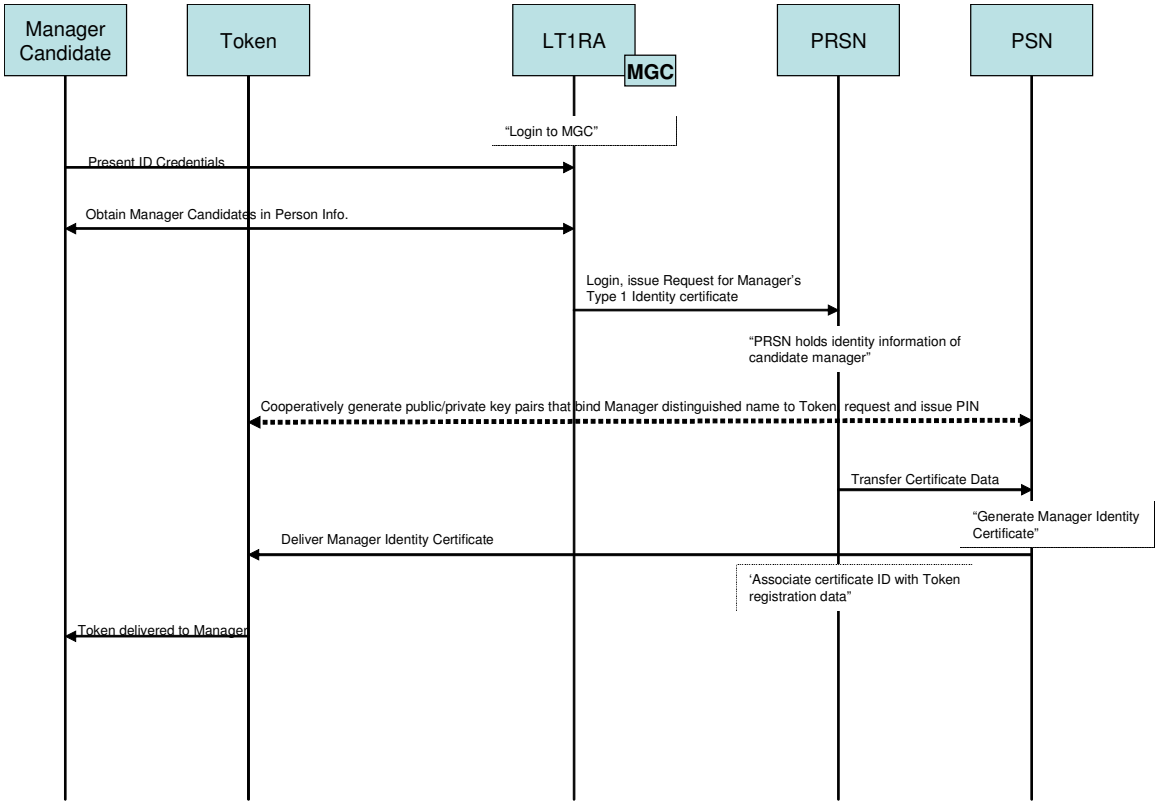
1610 ## 6.1.5 (U) Activation of a Token

1611 ### 6.1.5.1 (U) Summary

1612 (U) This section describes the provisioning of a Token. The provisioning process
1613 transitions the Token to an operational state. This is done by requesting Operational
1614 Mission Key(s), using the Infrastructure Key generated from the endorsement process.

1615 ### 6.1.5.2 (U) Sequence Diagram

1616



1617

1618 **Figure 13: (U) Activation of a Token**

1619 ### 6.1.5.3 (U) KMI Roles Involved

1620 • (U) Local Type 1 Registration Authority (LT1RA) (Also enrolled as Product
1621 Requester)

1622 • Manager Candidate

1623 ### 6.1.5.4 (U) KMI Nodes Involved

1624 • (U) Manager Client (MGC)

1625 • (U) PRSN

1626 • (U) PSN

6.1.5.5 (U) Prerequisites

- (U) The token has been initialized (registered) and endorsed.
- (U) A valid need for access as a KMI Manager exists.
- (U) The candidate is registered within KMI.
- (U) LT1RA is valid and has rights within the appropriate domain.

6.1.5.6 (U) Sequence of Events

1. (U) LT1RA logs into MGC.
2. (U) The Manager Candidate Presents his ID Credentials to the LT1RA for verification.
3. (U) The LT1RA collects the in-person information from the Manager Candidate.
4. (U) LT1RA logs into the PRSN and requests Manager's Type 1 Identity certificate.
5. (U) The Manager Identity information is stored within the PRSN.
6. (U) The Token establishes a cryptographic association with the PSN, they cooperatively generate the public and private key pairs that bind the Manager's distinguished name to the Token, and a PIN is requested and issued.
7. (U) PRSN sends the certification data to the PSN.
8. (U) PSN generates manager identity certificate.
9. (U) The PSN delivers the manager identity certificate to the Token.
10. (U) The PRSN associates the certificate ID with the token registration data.
11. (U) The Token is delivered to the Manager and is now ready to operate.

6.1.6 (U) Deregister Manager from KMI

6.1.6.1 (U) Summary

(U) This scenario describes the activities that encompass deregistration of a KMI Manager within KMI. In deregistration, you are removing the presence of a Manager from KMI. A trigger begins the process of deregistering a KMI Manager. The trigger is validated and the process is completed by the Registration Manager interacting with the PRSN. The process is completed when deregistration has been accomplished and acknowledgement has been received at the user level.

6.1.6.2 (U) Sequence Diagram

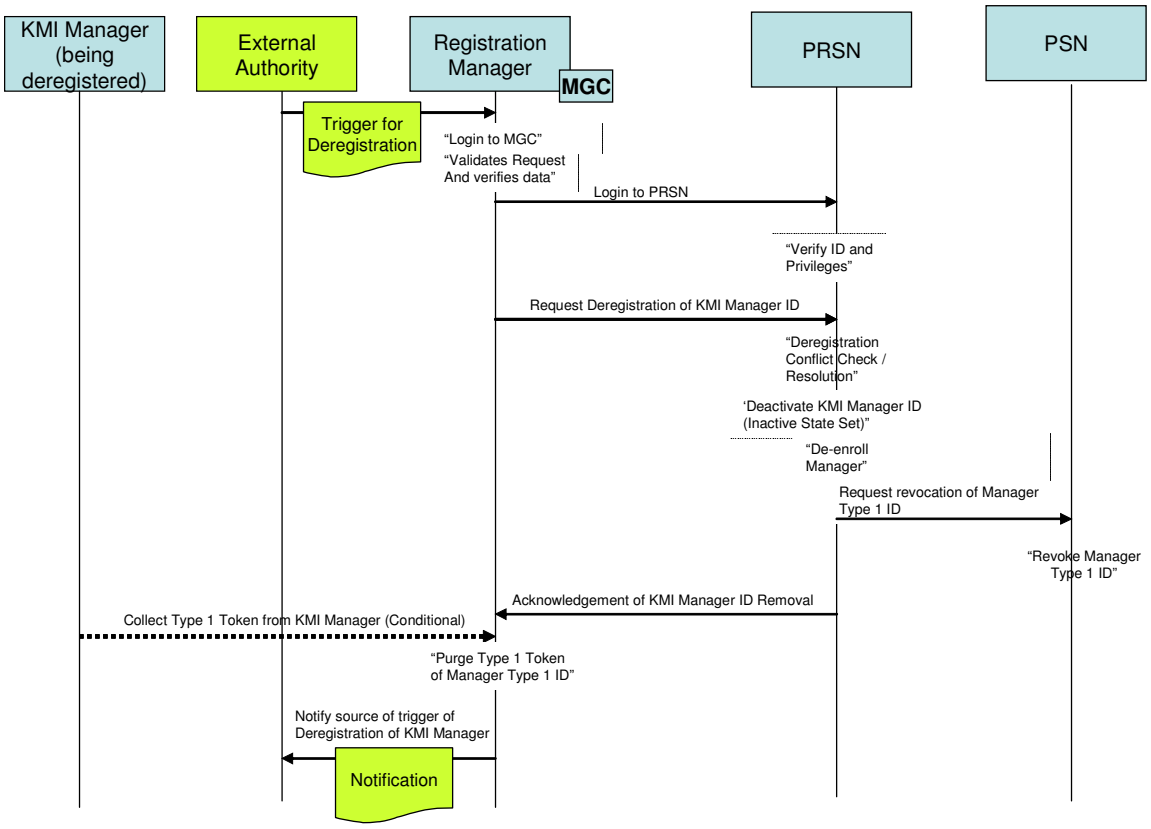


Figure 14: (U) Deregister Manager from KMI

6.1.6.3 (U) KMI Roles Involved

- (U) External Authority
- (U) Registration Manager
- (U) KMI Manager (being deregistered)

6.1.6.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.1.6.5 (U) Prerequisites

- (U) A KMI Manager has been enrolled with a personalized Type 1 Token.
- (U) A valid need for deregistration within KMI exists.
- (U) Participating KMI Managers are valid and have rights within the appropriate domain.

6.1.6.6 (U) Sequence of Events

1. (U) A User Identity that is assigned to a KMI Manager Role will be identified for deregistration by an External Authority that has the right to do so.
2. (U) The Registration Manager validates the request and verifies the identity of the External Authority to ensure that they have the right to request this.
3. (U) The Registration Manager logs onto the PRSN.
4. (U) The Registration Manager requests the PRSN to deregister a user.
5. (U) A check is performed, by the PRSN, to ensure that no deregistration conflicts will arise, and if so, they are resolved.
6. (U) The KMI Manager ID is deactivated by the PRSN. An inactive state is set.
7. (U) The KMI Manager ID is de-enrolled by the PRSN.
8. (U) The PRSN send a request to revoke the KMI Manager's Type 1 ID to the PSN.
9. (U) The PSN revokes the Manager's Type 1 ID.
10. (U) An acknowledgement is sent to the Registration Manager that the KMI Manager ID has been deregistered.
11. (U) The Type 1 Token is collected from the KMI Manager being deregistered (conditional).
12. (U) The Registration Manager purges the Type 1 Token of its Manager Type 1 ID.
13. (U) An acknowledgement is sent to the External Authority whom requested the deregistration of the KMI Manager.

6.1.7 (U) Change Enrollment of KMI Manager

6.1.7.1 (U) Summary

(U) This scenario describes the activities that encompass changing the enrollment of a KMI Manager within KMI. A trigger begins the process of requesting change of enrollment for a KMI Manager. The trigger is validated and the process is completed by the Enrollment Manager interacting with the PRSN. The process is completed when enrollment has been changed and acknowledgement of the change has been received at the user level.

6.1.7.2 (U) Sequence Diagram

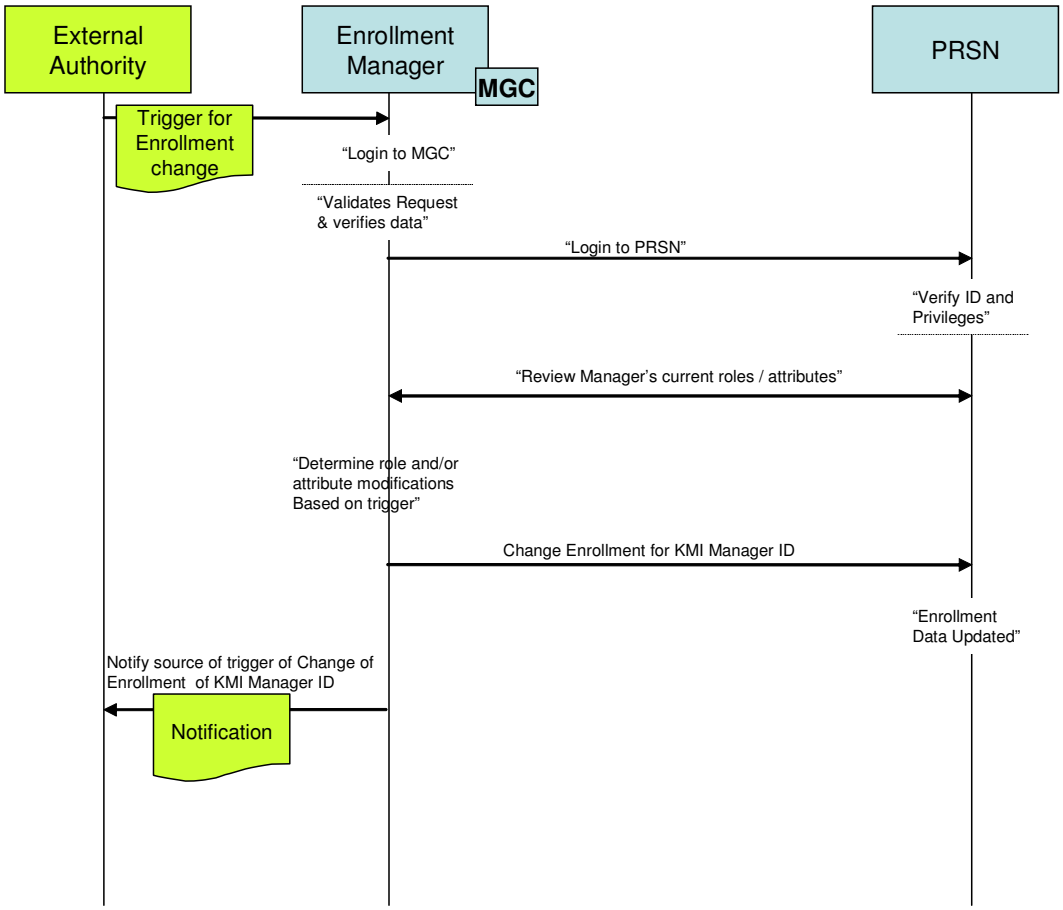


Figure 15: (U) Change Enrollment of KMI Manager

6.1.7.3 (U) KMI Roles Involved

- (U) External Authority
- (U) Enrollment Manager

1711 ### 6.1.7.4 (U) KMI Nodes Involved

1712 • (U) Manager Client (MGC)
1713 • (U) PRSN

1714 ### 6.1.7.5 (U) Prerequisites

1715 • (U) A KMI Manager has been enrolled with a personalized Type 1 Token.
1716 • (U) A valid need for change of enrollment within KMI exists.
1717 • (U) Participating KMI Managers are valid and have rights within the appropriate
1718 domain.

1719 ### 6.1.7.6 (U) Sequence of Events

1720 1. (U) A User Identity that is assigned to a KMI Manager Role will be nominated for
1721 change of enrollment by an External Authority that has the right to do so.
1722 2. (U) The Enrollment Manager will validate the request and verify the identity of
1723 the External Authority to ensure that they have the right to request this.
1724 3. (U) The Enrollment Manager will login to the PRSN.
1725 4. (U) The Enrollment Manager will review the manager's current roles / attributes.
1726 5. (U) The Enrollment Manager will determine role and/or attribute modifications
1727 based on the trigger.
1728 6. (U) The Enrollment Manager will change the enrollment data assigned to the User
1729 Identity for the KMI Manager role.
1730 7. (U) The enrollment data will be updated at the PRSN.
1731 8. (U) An acknowledgement will be sent to the External Authority whom requested
1732 the change of enrollment for the KMI Manager.
1733
1734

6.2 KMI Operating Account (KOA) Registration Process

(U) There are several steps necessary to register a KMI Operating Account (KOA), as shown in Figure 16. The KOA is first registered by the KOA Registration Manager (RM). The KOA RM may also have the role of the EKMS Registration Authority (RA). The registration information is then sent to both the EKMS directory and PRSN Registration Data Store. The EKMS Directory synchronizes the KOA Registration Data with the PRSN Registration Data Store. Finally, a notice of registration is sent to the KOA Manager, from which point the KOA is active.

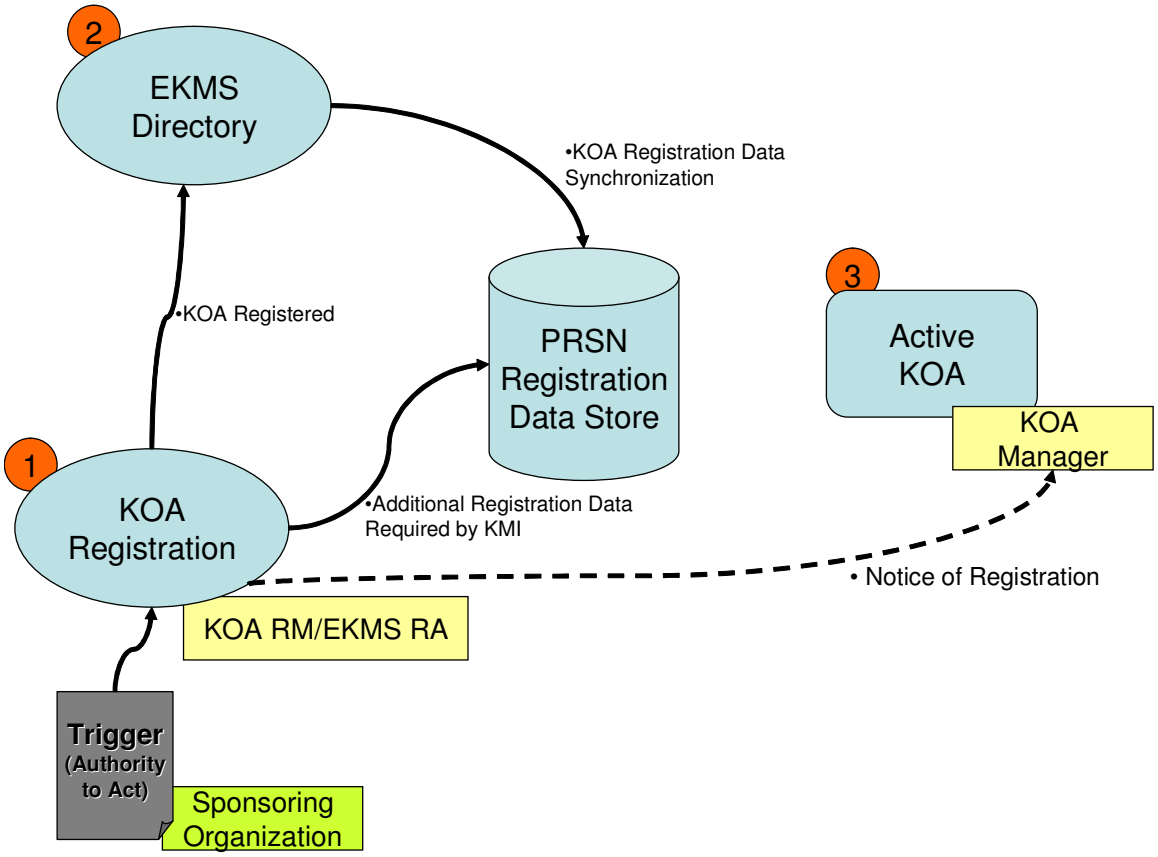


Figure 16: (U) KOA Registration Process

6.2.1 (U) Registration of KMI Operating Account (KOA)

6.2.1.1 (U) Summary

(U) This scenario describes the registration of a KMI Operating Account. The KOA is assumed to be a military service account supporting KMI-aware devices and is assumed to have a MGC with an AKP to provide identification and authentication for its PRSN interactions and security protection for the MGC. This configuration is the equivalent of an LMP/KP-equipped COMSEC account in the current system. At the completion of this process, the KOA is capable of receiving key to be unwrapped by its AKP and filed into the benign and RED fill ECUs, and its KMI-aware ECUs are registered with the KMI and prepared to accept key via OTNK.

6.2.1.2 (U) Sequence Diagram

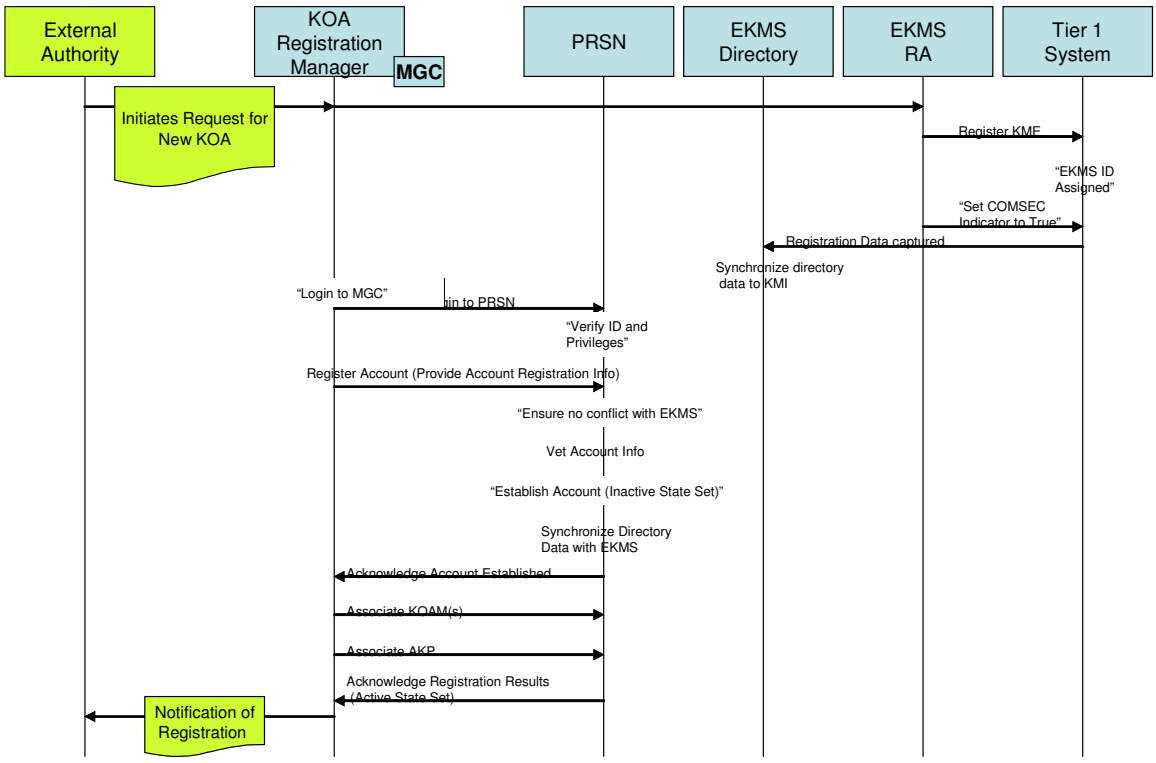


Figure 17: (U) Registration of KMI Operating Account (KOA)

6.2.1.3 (U) KMI Roles Involved

- (U) External Authority
- (U) KOA Registration Manager (EKMS Registration Authority) - Could be same person

6.2.1.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.2.1.5 (U) Prerequisites

- (U) KOA Registration Manager must be enrolled with appropriate privileges and must have privileges for the domain in which the KOA will be registered.
- (U) Administrative / physical actions to create the COMSEC account/KOA and appoint the KOA Manager must be complete (i.e., policy prerequisites must be satisfied).
- (U) KOA must have KMI client and AKP.

6.2.1.6 (U) Sequence of Events

1. (U) An External Authority identifies a need for a KOA. The External Authority will initiate a request and provide account information to the KOA Registration Manager (and EKMS Registration Authority).
2. (U) The EKMS RA will register the new KME using the Tier 1 system. As a result, the KME will have an EKMS ID and basic administrative information will be captured and stored in the EKMS directory
3. (U) The EKMS RA sets the COMSEC account indicator for the new account to true, and enters other administrative data specific to COMSEC accounts.
4. (U) The directory data is synchronized to KMI.
5. (U) Once the registration request has been authorized by the appropriate authority, the KOA Registration Manger will log into the MGC.
6. (U) The Registration Manager provides the account registration information to the PRSN for registration into the system.
7. (U) The PRSN will verify that a conflict does not exist by comparing the data with the EKMS directory data.
8. (U) Once check is complete, the KOA is established. The account is instantiated; but has a status of inactive.

Note: The account will remain inactive until all constraints are met.

- A KOA Manager needs to be enrolled (which first requires registration to the KMI)
- A KOA Manager must first be identified and an AKP needs to be associated with the account.
- A KOA Manager needs to be assigned to a KOA.

9. (U) The directory data is then synchronized with EKMS
10. (U) Once these two constraints have been met, the account status will be set to active.
11. (U) An acknowledgement is sent to the KOA Registration Manager that the account has been established

12. (U) The KOA Registration Manager associates the Key Operating Account Managers KOAM(s).
13. (U) The KOA Registration Manager associates the AKP.
14. (U) A notification is sent back to the external authority that registration of KOA is complete (Active State Set).

6.3 KMI-Aware Device Activation Process

(U) There are several steps necessary to make a KMI-Aware device operational, as shown in Figure 18. The KMI-Aware device must first be initialized (registered) with KMI by the Device Registration Manager (RM). The registration process provides the KMI-Aware device with an initial Seed Key. The KMI-Aware device is then endorsed by the Local Type 1 Registration Authority (LT1RA).

(U) In the endorsement process, the KMI-Aware device receives a sponsor, a Type 1 Identity Certificate, and converts the initial Seed Key to an Infrastructure Key. The KMI-Aware device is then activated by the KOA Manager, at which time the device downloads the Mission Keys. The KMI-Aware device is then ready to operate and begin its mission.

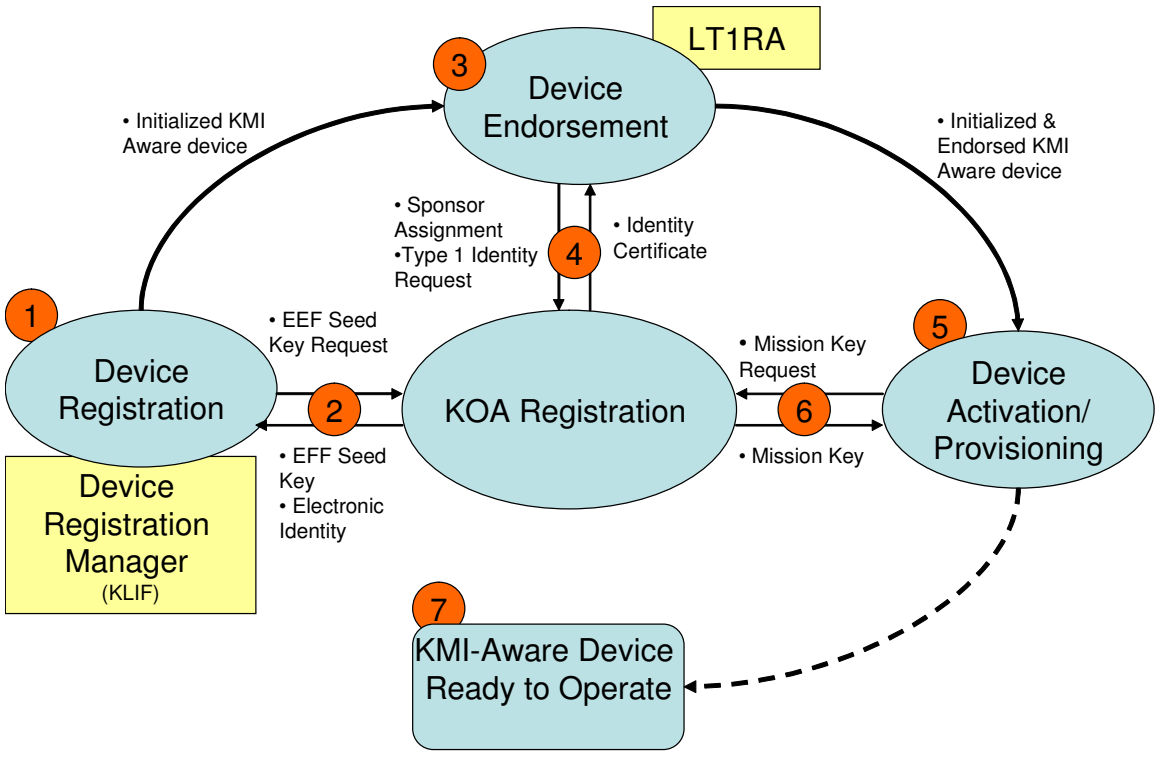


Figure 18: (U) KMI-Aware Device Activation Process

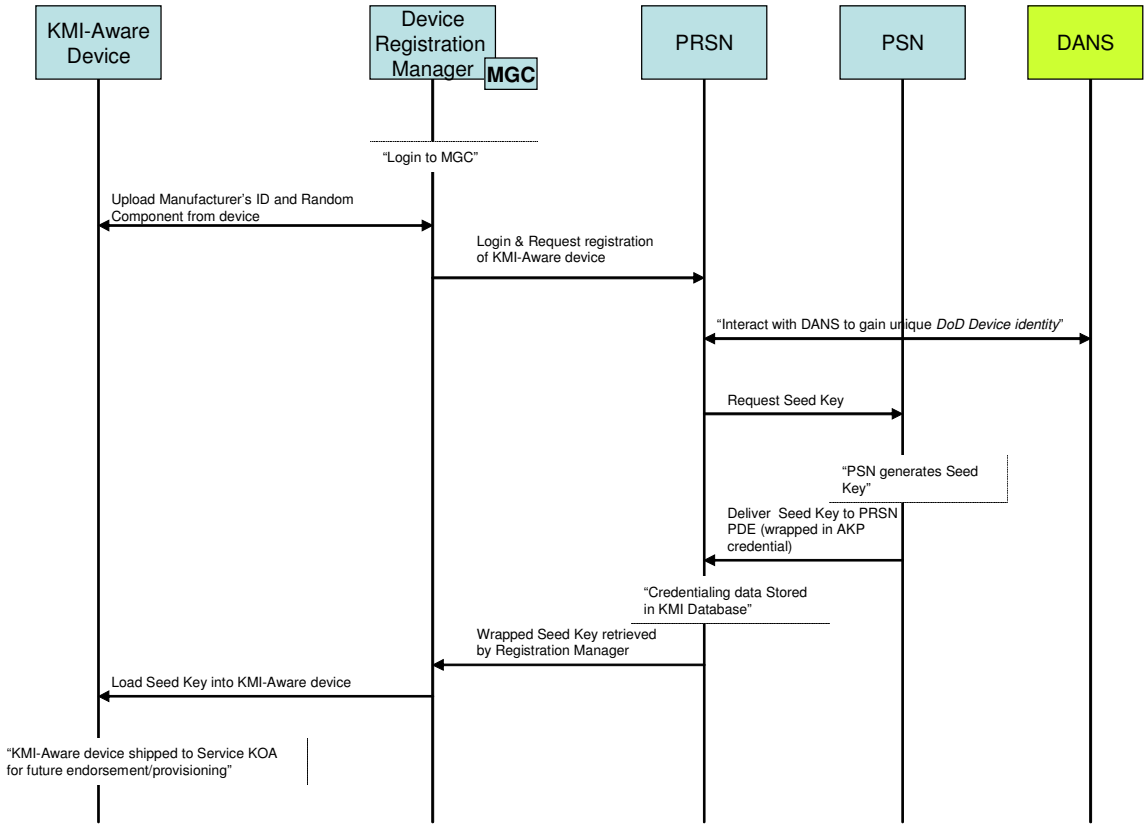
1829 ## 6.3.1 (U) Register KMI Aware Device

1830 ### 6.3.1.1 (U) Summary

1831 (U) This section describes the initial registration of a KMI-Aware device. A KMI-Aware
1832 device has its own identity within the KMI, and key can be wrapped specifically for that
1833 device by a KMI PSN, using credentials stored as part of the device's registration
1834 information in the KMI. This storyboard assumes the use of MGC KLIF capabilities in
1835 the registration of a KMI-Aware device, as this is expected to be a typical scenario with
1836 future devices. It also assumes that the device being registered is capable of over-the-
1837 network interactions with the KMI.

1838 ### 6.3.1.2 (U) Sequence Diagram

1839



1840

1841 **Figure 19: (U) Register KMI Aware Device**

1842 ### 6.3.1.3 (U) KMI Roles Involved

1843 - (U) Device Registration Manager

6.3.1.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN
- (U) PSN

6.3.1.5 (U) Prerequisites

- (U) KLIF is registered as a KOA (most likely at the device manufacturer's site).
- (U) The Device Registration Manager has a Manager Client (MGC).
- (U) Device has a software baseline from the factory.
- (U) Device has been designed in compliance with KMI Standards to permit being "KMI-Aware".
- (U) KLIF knows "nationality, but not mission, for the new device.

6.3.1.6 (U) Sequence of Events

1. (U) Device Registration Manager (RM) logs into MGC and authenticates to KMI using Type 1 Identity/Token.
2. (U) Device RM uploads (electronically or physically) a manufacturer's ID and random component from the KMI-Aware device.
3. (U) Device RM logs into PRSN and requests registration of KMI-Aware device.
4. (U) PRSN interacts with DoD Authoritative Naming Source (DANS) to gain a unique DoD Device Identity (aka - Device Distinguished Name).
5. (U) PRSN requests, from the PSN, a Seed Key that embeds the DANS identity and the random component of the KMI-Aware device. The Seed Key is linked to the DoD Identity and the KMI-Aware device random generated component.
6. (U) The PSN generates the Seed Key.
7. (U) The Seed Key is delivered to the PRSN PDE, wrapped in the AKP's credentials.
8. (U) This credentialing data is stored in the KMI database (at the PRSN) for the Endorsement process.
9. (U) The PRSN delivers the wrapped Seed Key to the Device RM.
10. (U) Device RM retrieves and loads Seed Key and electronic identity into KMI-Aware device. The device is now registered in KMI.
11. (U) The KMI-Aware device is shipped to Service and eventually is shipped to a KOA account or mission location for endorsement and activation.

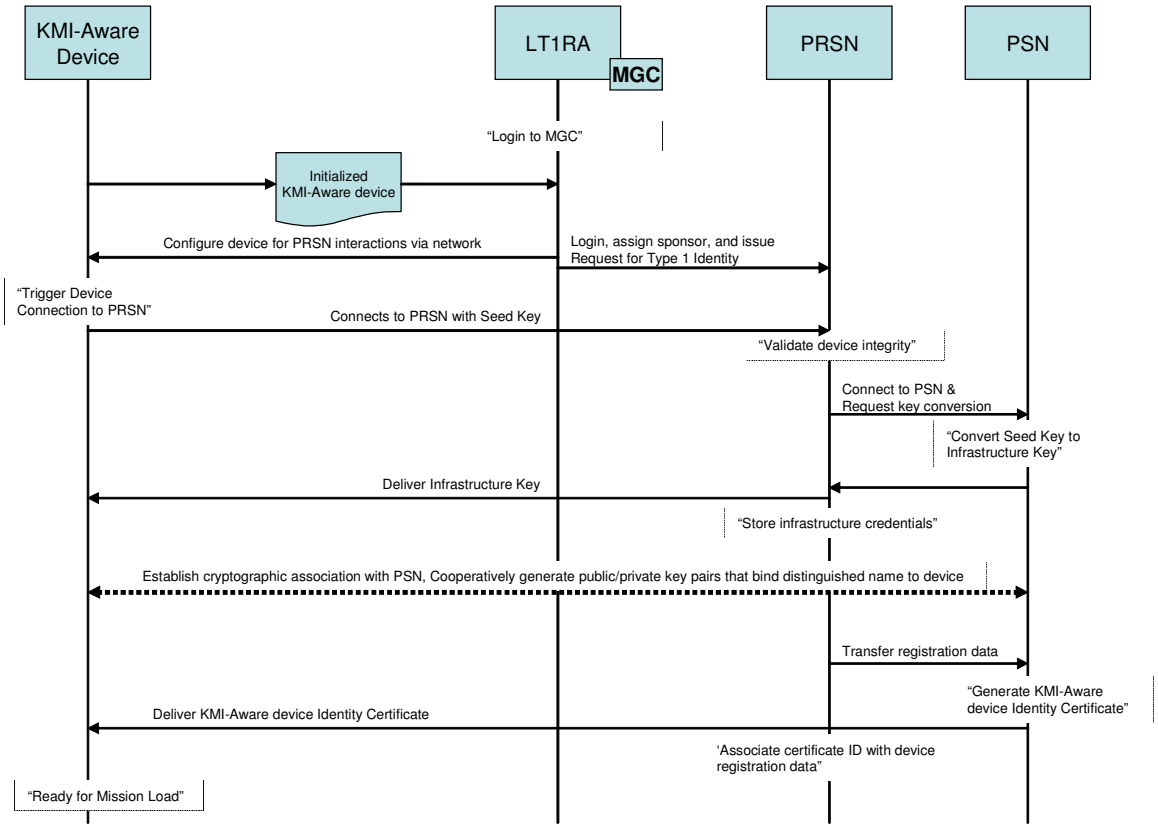
1877 ## 6.3.2 (U) Endorsement of KMI Aware Device

1878 ### 6.3.2.1 (U) Summary

1879 (U) This section describes the endorsement of a KMI-aware device. This process
1880 establishes a sponsor for the KMI-Aware device, completes the establishment of a Type 1
1881 Identity and converts the Seed to an Infrastructure Key for the KMI-Aware device. This
1882 process can occur for both a networked or disconnected KMI-Aware device.

1883 ### 6.3.2.2 (U) Sequence Diagrams

1884



1885

1886 **Figure 20: (U) Endorsement KMI Aware Device (Networked)**

1887

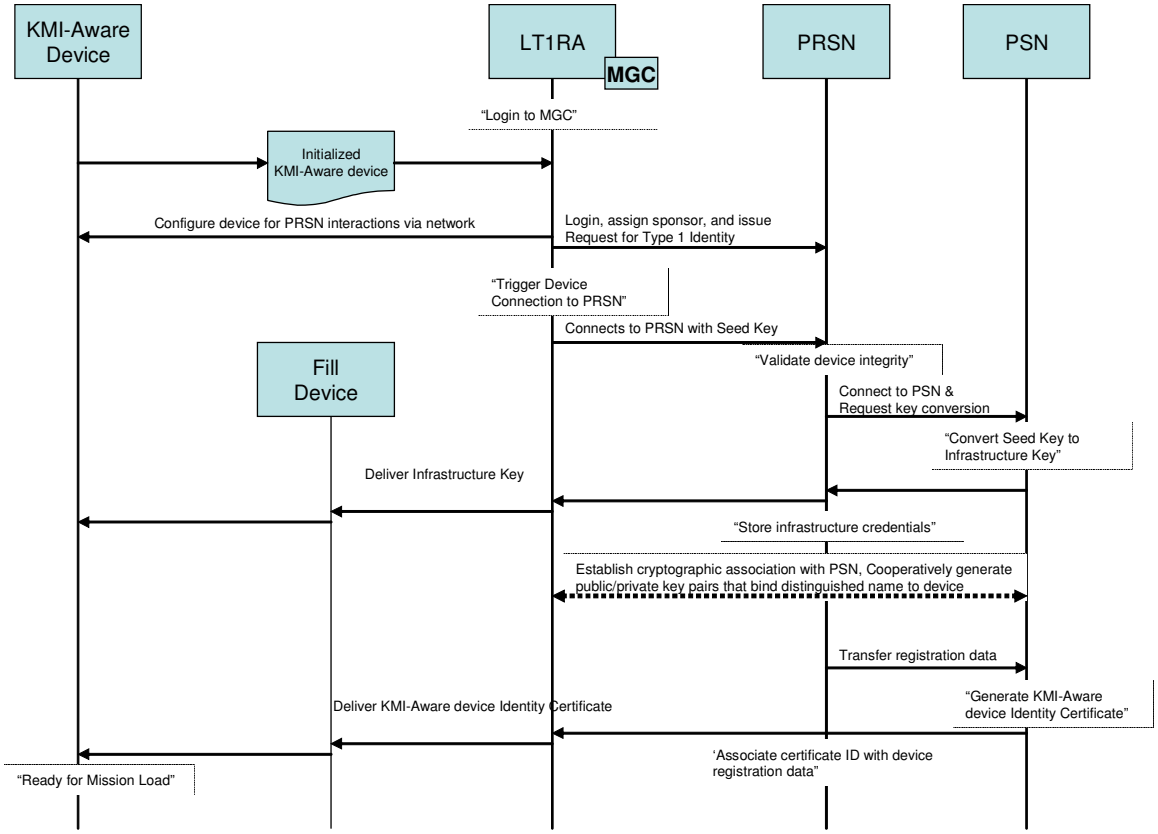


Figure 21: (U) Endorsement KMI Aware Device (Disconnected)

6.3.2.3 (U) KMI Roles Involved

- (U) Local Type 1 Registration Authority (LT1RA) (Also enrolled as Product Requestor)

6.3.2.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN
- (U) PSN

6.3.2.5 (U) Prerequisites

- (U) Device has been initialized (registered) and shipped to the LT1RA.
- (U) PRSN has captured device registration data to be used in the endorsement process.
- (U) Device has been designed in compliance with KMI Standards to permit being "KMI Aware".
- (U) MGC serves as the intermediary device.

6.3.2.6 (U) Sequence of Events

For Networked KMI-Aware device:

1. (U) LT1RA receives the Initialized KMI-Aware device (out of band process).
2. (U) LT1RA logs into MGC.
3. (U) LT1RA configures the KMI-Aware device for PRSN interactions via network.
4. (U) LT1RA logs into the PRSN, assigns a sponsor to the KMI-Aware device, and issues a request for a Type 1 Identity. (Note: The Identity request is built from the KMI knowledge of the device serial number/device distinguished name that occurred during the initialization process and information provided by the LT1RA)
5. (U) KMI-Aware device is triggered for PRSN connection.
6. (U) The KMI-Aware device connects with the PRSN using Seed Key; PRSN validates device integrity.
7. (U) PRSN connects to the PSN and requests seed key conversion.
8. (U) PSN converts Seed Key to Infrastructure Key.
9. (U) PSN delivers Infrastructure Key to KMI-Aware device (via PRSN).
10. (U) The Infrastructure credential information is stored within the PRSN.
11. (U) The PSN and KMI-Aware device cooperatively generate the public and private key pairs that bind the distinguished name to the device.
12. (U) PRSN sends KMI Aware device's registration data to the PSN.
13. (U) PSN generates Type 1 certificate for the KMI-Aware device.
14. (U) KMI-Aware device receives the Identity Certificate from the PSN.
15. (U) The PRSN associates the certificate ID with the device registration data.
16. (U) The KMI-Aware device is now ready for its mission load.

For Disconnected KMI-Aware device:

1. (U) LT1RA receives the Initialized KMI-Aware device (out of band process).
2. (U) LT1RA logs into MGC.
3. (U) LT1RA configures the KMI-Aware device for PRSN interactions via network.
4. (U) LT1RA logs into the PRSN, assigns a sponsor to the KMI-Aware device, and issues a request for a Type 1 Identity. (Note: The Identity request is built from the KMI knowledge of the device serial number/device distinguished name that occurred during the initialization process and information provided by the LT1RA)
5. (U) KMI-Aware device is triggered for PRSN connection.
6. (U) The KMI-Aware device, via Fill Device and MGC, connects with the PRSN using Seed Key; PRSN validates device integrity.
7. (U) PRSN connects to the PSN and requests seed key conversion.
8. (U) PSN converts Seed Key to Infrastructure Key.

9. (U) PSN delivers Infrastructure Key to KMI-Aware device (via PRSN, MGC, and Fill Device).
10. (U) The Infrastructure credential information is stored within the PRSN.
11. (U) The PSN and KMI-Aware device (via MGC) cooperatively generate the public and private key pairs that bind the distinguished name to the device.
12. (U) PRSN sends KMI Aware device's registration data to the PSN.
13. (U) PSN generates Type 1 certificate for the KMI-Aware device.
14. (U) KMI-Aware device receives the Identity Certificate from the PSN (via MGC and Fill Device).
15. (U) The PRSN associates the certificate ID with the device registration data.
16. (U) The KMI-Aware device is now ready for its mission load.

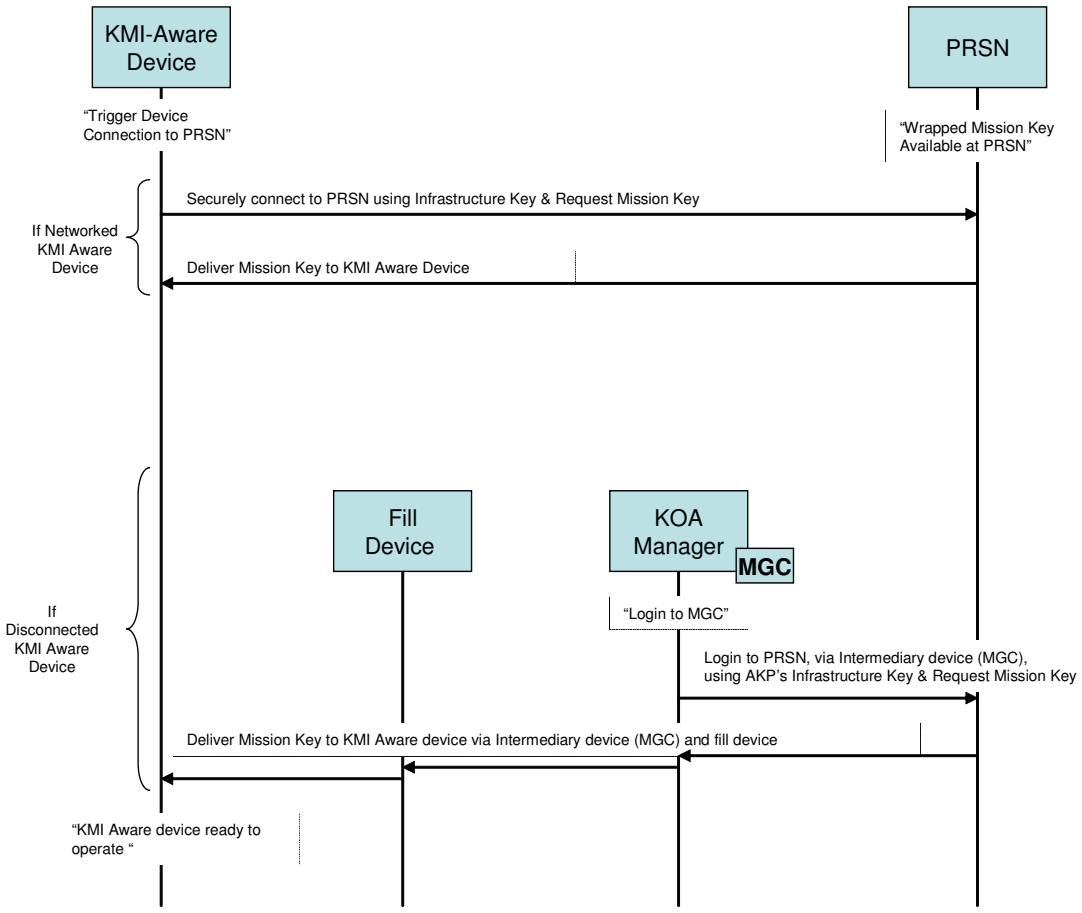
1959 ## 6.3.3 (U) Activation of KMI Aware Device

1960 ### 6.3.3.1 (U) Summary

1961 (U) This section describes the activation/provisioning process of a KMI-Aware device.
1962 This process transitions the KMI-Aware device to an operational state. This is done by
1963 requesting Operational Mission Key(s), using the Infrastructure Key generated from the
1964 endorsement process. This process can occur for both networked and disconnected
1965 devices.

1966 ### 6.3.3.2 (U) Sequence Diagram

1967



1968

1969 **Figure 22: (U) Activation/Provisioning KMI Aware Device**

1970 ### 6.3.3.3 (U) KMI Roles Involved

1971 • (U) KOA Manager (also enrolled as a Product Requestor)

6.3.3.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN
- (U) PSN

6.3.3.5 (U) Prerequisites

- (U) Device has been initialized (registered) and endorsed
- (U) Product for device has been defined by Controlling Authority.
- (U) KOA sponsoring the device has been placed on Account Distribution Profile for product.
- (U) KOA Manager has placed the device on the Device Distribution Profile for the product.
- (U) Product has been generated by PSN and wrapped for receiving device using the device's credential supplied by PRSN.
- (U) MGC serves as the intermediary device (could also be a DOC operated by a KOA Agent).

6.3.3.6 (U) Sequence of Events

If the KMI-Aware device is networked:

1. The KMI-Aware device is triggered to connect to the PRSN.
2. The KMI-Aware device connects with the PDE portion of the PRSN using the Infrastructure key to create a secure connection and Requests Mission Key.
3. Once the device's Type 1 identity is authenticated, the PRSN delivers the Mission Key to the KMI-Aware device. The Mission keys are unwrapped and loaded into mission storage locations within the KMI-Aware device.
4. The KMI-Aware device is now ready to operate.

If the KMI Aware device is disconnected:

1. The KOA Manager logs into the Manager Client (MGC). The MGC will serve as the intermediary device.
2. The MGC connects with the PRSN PDE using the AKP's Infrastructure Key to create a secure connection and Request Mission Key.
3. Once the MGC's Type 1 identity is authenticated by the PRSN, the MGC transfers the mission keys from the PRSN to a fill device, from which the keys are transferred to the KMI-Aware device. The Mission keys are unwrapped by the KMI-Aware device and loaded into mission storage locations within the device.
4. The KMI-Aware device is now ready to operate.

6.4 Product Ordering and Retrieval Process – Symmetric Key

(U) There are several steps of the Product Ordering and Retrieval process for Symmetric Keys, as shown in Figure 23. The first step is for the Controlling Authority to establish the product, in which product requirements and an Account Distribution Profile (ADP) are established. This data is updated in the catalog at the PRSN Product Requirement Data Store and also passed to the KOA Manager. The KOA Manager takes the new product requirements and the ADP to establish the Device Distribution Profile (DDP), which is updated in the Data Store catalog.

(U) When ready to order, the Product Requestor requests the Product Ordering Catalog from the PRSN Product Requirement Data Store. After requesting the required products, this process enters the generation and production phase. Here, the products are generated and produced in the wrapping credentials. The products are then distributed either electronically or physically to their appropriate destinations.

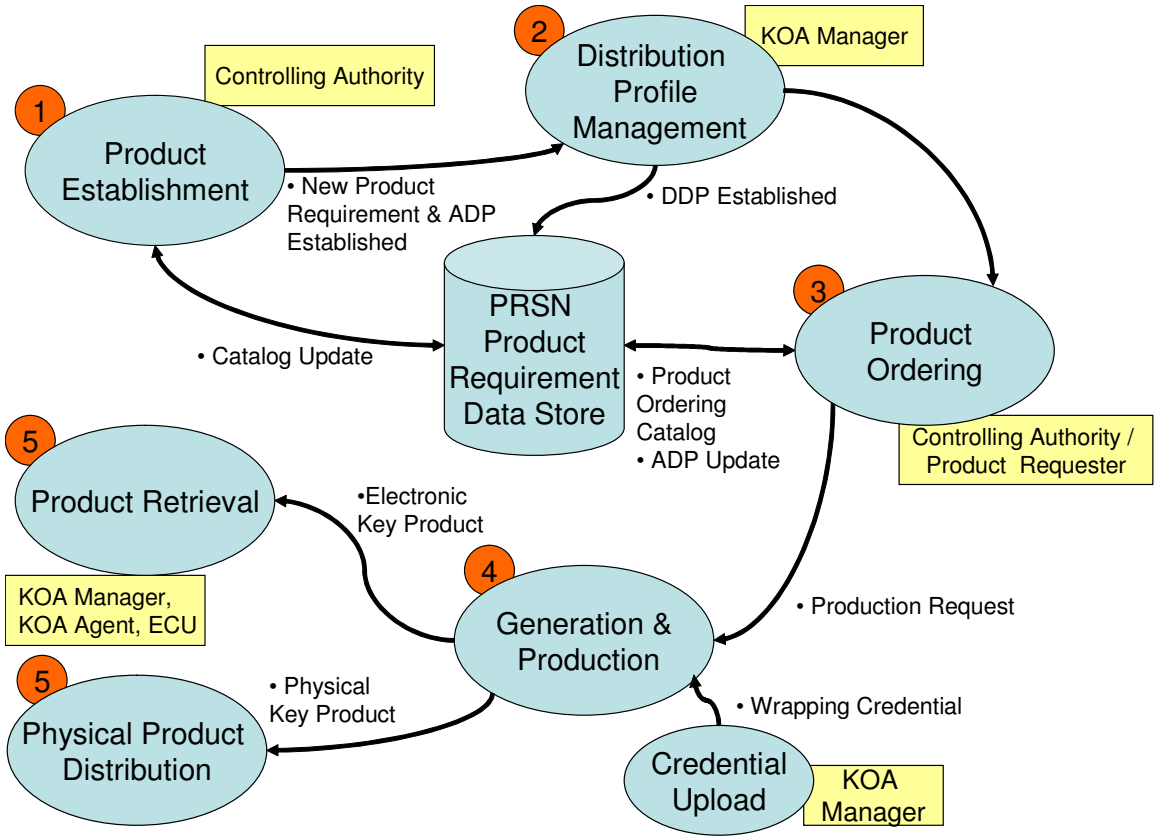


Figure 23: (U) Product Ordering and Retrieval

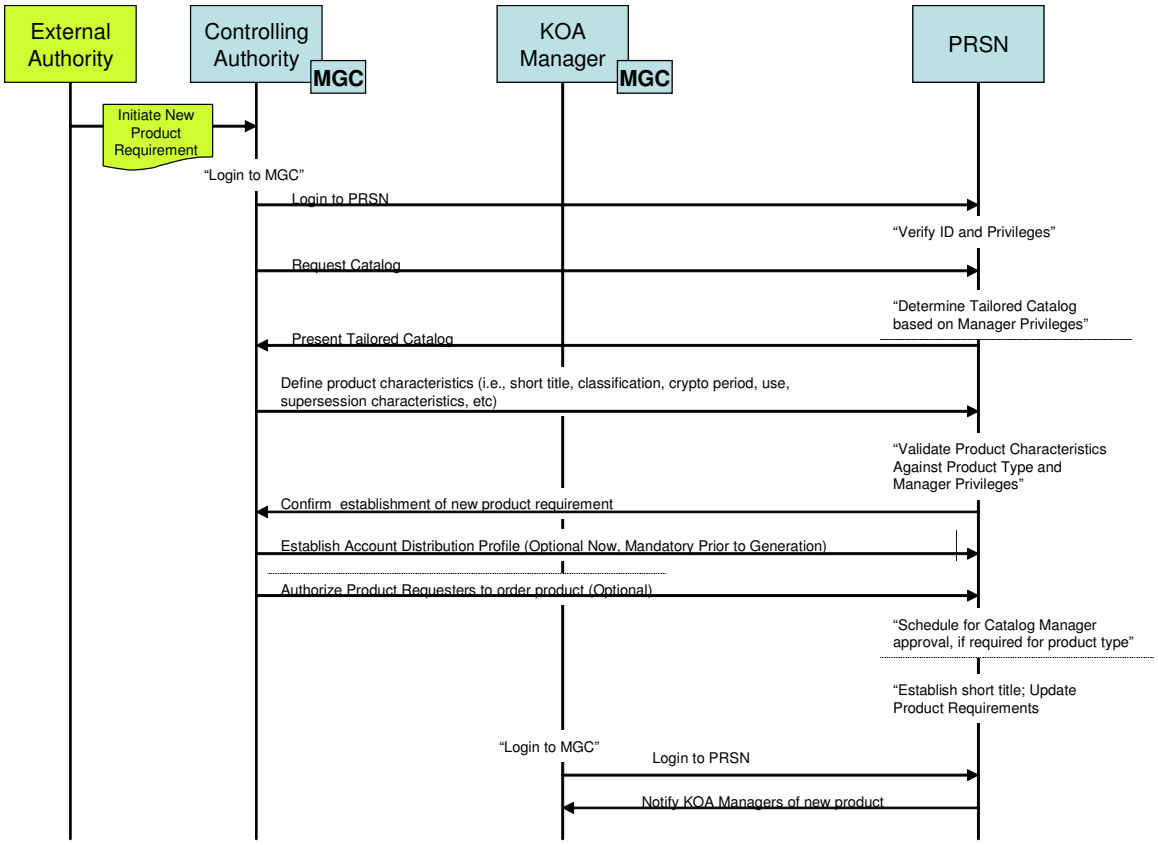
2031 ## 6.4.1 (U) Establishment of New Product Requirement for
2032 ## Symmetric Key

2033 ### 6.4.1.1 (U) Summary

2034 (U) When a product is added to the Ordering Catalog, the requirements for the product
2035 also need to be defined. This process allows the Controlling Authority to request the
2036 products, view the requirements for that product, and modify them, as necessary. This
2037 scenario includes the case where the Controlling Authority is establishing a new
2038 requirement for a known product type that will be handled as a standing order for
2039 regularly superseded operational key, requiring KMI to periodically generate the product
2040 and make it available for retrieval.

2041 ### 6.4.1.2 (U) Sequence Diagram

2042



2043

2044 **Figure 24: (U) Establishment of New Product Requirement for Symmetric Key**

2045 ### 6.4.1.3 (U) KMI Roles Involved

2046 • (U) External Authority
2047 • (U) Controlling Authority
2048 • (U) KOA Manager

6.4.1.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.4.1.5 (U) Prerequisites

- (U) Product type has been previously established.

6.4.1.6 (U) Sequence of Events

1. (U) An External Authority will initiate a request for a product new instance and provides product requirements to the Controlling Authority (via out of band methods).
2. (U) The Controlling Authority logs into the MGC.
3. (U) The Controlling Authority connects and authenticates to the PRSN OME using a MGC.
4. (U) The Controlling Authority requests the catalog.
5. (U) The PRSN determines the tailored catalog based on the privileges of the Controlling Authority.
6. (U) The catalog is sent to the Controlling Authority.
7. (U) Controlling Authority defines new product characteristics (i.e., short title, classification, crypto period, use, supersession characteristics, etc.).
8. (U) The PRSN validates the product characteristics against the product type and Manager privileges.
9. (U) The PRSN confirms establishment of the new product requirement.
10. (U) The Controlling Authority establishes Account Distribution Profile (ADP). *(Optional – This may occur while establishing the new product, or at a later time, but must be done prior to generation.)*
11. (U) The Controlling Authority identifies authorized Product Requesters to order product. (Optional – *This may occur while establishing the new product, or at a later time.*)
12. (U) The PRSN assign new and unique nomenclature appropriate for the cryptographic product type and performs product requirements updates.
13. (U) If required for product type, the PRSN schedules the request for Catalog Manager approval.
14. (U) When a KOA Manager of a KOA on the Account Distribution Profile logs in, the PRSN notifies the KOA Manager of availability of new symmetric product.

6.4.2 (U) Account Distribution Profile (ADP) Management

6.4.2.1 (U) Summary

(U) To ensure that products are delivered to the appropriate ECUs, the KMI will keep an Account Distribution Profile (ADP), which is a collection of information that defines which KOAs are authorized to receive that product. There is an ADP for each instantiation of a product. This scenario shows the steps for developing and modifying an Account Distribution Profile.

6.4.2.2 (U) Sequence Diagram

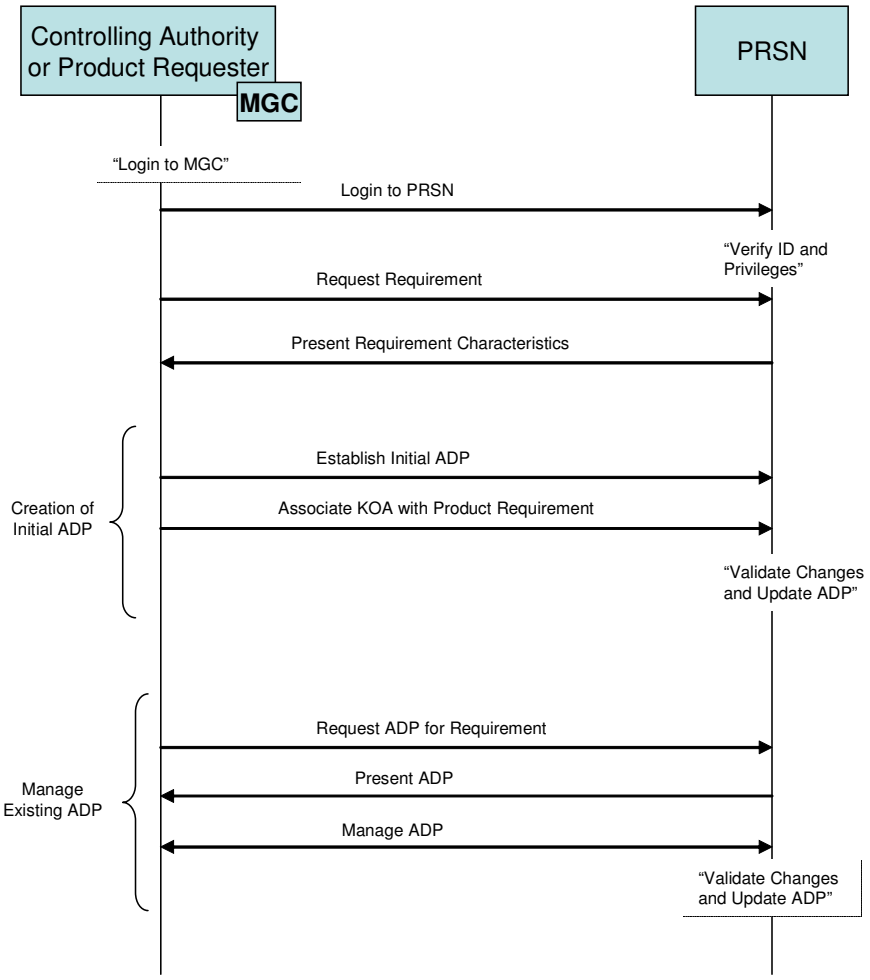


Figure 25: (U) Account Distribution Profile (ADP) Management

6.4.2.3 (U) KMI Roles Involved

- (U) Controlling Authority
- (U) Product Requestor

6.4.2.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)

- (U) PRSN

6.4.2.5 (U) Prerequisites

- (U) Product requirements have been previously established.

6.4.2.6 (U) Sequence of Events

1. (U) The Controlling Authority / Product Requester logs into the MGC.
2. (U) The Controlling Authority / Product Requester logs into the PRSN.
3. (U) The Controlling Authority / Product Requester requests the requirements for a given product from the PRSN.
4. (U) The PRSN sends back the requirements to the Controlling Authority / Product Requester.

If Creating Initial Account Distribution Profile:

1. (U) The Controlling Authority / Product Requester requests the creation of a new ADP, identifying the KOA(s) to be included in the new profile.
2. (U) The PRSN associates the selected KOAs with the Product Requirement.
3. (U) The PRSN validates and updates the ADP changes.

If Managing Existing Account Distribution Profile:

1. (U) The Controlling Authority / Product Requester requests the ADP from the PRSN for a given product.
2. (U) The PRSN sends back the appropriate ADP.
3. (U) The Controlling Authority / Product Requester adds or removes KOAs, as necessary.
4. (U) The PRSN validates and updates the ADP changes.

6.4.3 (U) Device Distribution Profile (DDP) Management

6.4.3.1 (U) Summary

(U) To ensure that products are delivered to the appropriate ECUs, the KMI will keep a Device Distribution Profile (DDP) for each product. There is a DDP for each KOA that is specified to receive the given product. This scenario shows the steps for developing and modifying the Device Distribution Profiles.

NOTE: DDPs only apply to products being delivered to KMI-Aware devices. If there is no DDP for a given product, the default is to wrap a product for the KOA's AKP for the given product.

6.4.3.2 (U) Sequence Diagram

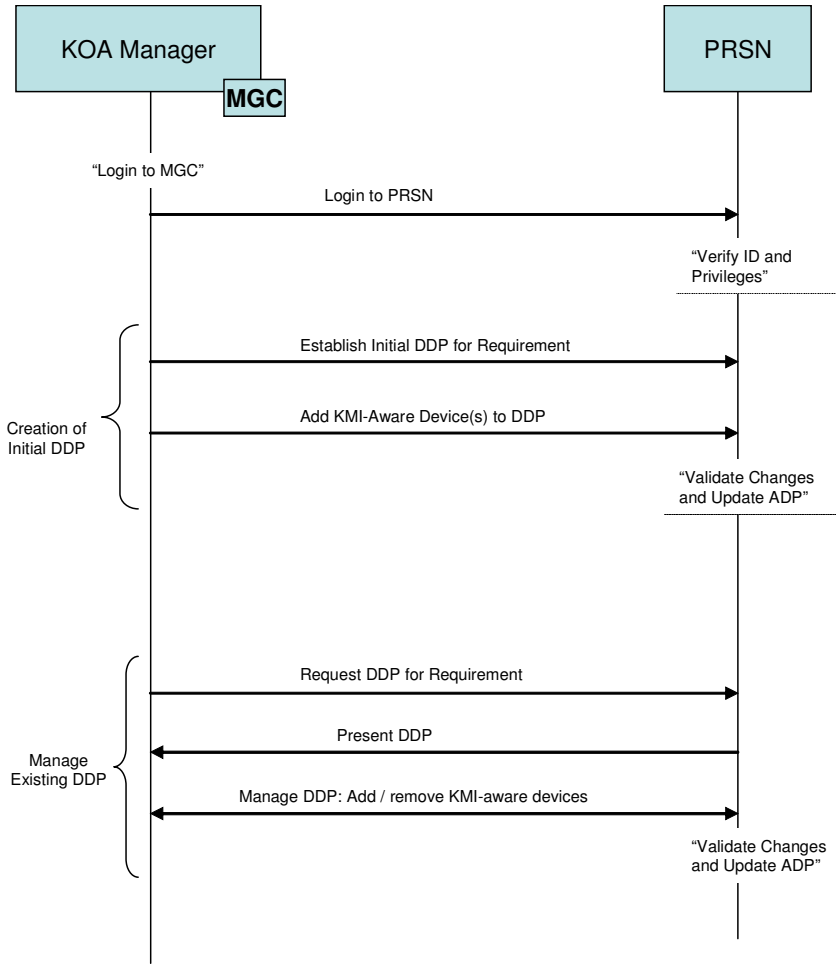


Figure 26: (U) Device Distribution Profile (DDP) Management

6.4.3.3 (U) KMI Roles Involved

- (U) KOA Manager

6.4.3.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.4.3.5 (U) Prerequisites

- (U) Product requirements have been previously established.
- (U) Account Distribution Profile (ADP) has been previously established.

6.4.3.6 (U) Sequence of Events

1. (U) The KOA Manager logs into the MGC.
2. (U) The KOA Manager logs into the PRSN.

If Creating Initial Device Distribution Profile:

1. (U) The KOA Manager requests the creation of a new DDP.
2. (U) The KOA Manager adds KMI-Aware Device(s) to the DDP.
3. (U) The PRSN validates and updates the ADP changes.

If Managing Existing Device Distribution Profile:

1. (U) The KOA Manager requests the DDP for the Manager's KOA from the PRSN.
2. (U) The PRSN sends back the appropriate DDP.
3. (U) The KOA Manager adds or removes KMI-aware devices.
4. (U) The PRSN validates and updates the ADP changes.

6.4.4 (U) Ordering of Symmetric Keys (Other Than Standing Orders)

6.4.4.1 (U) Summary

(U) A designated Controlling Authority or Product Requester can order products on a product-by-product basis. This ordering method will most likely be used for key products such as irregularly superseded operational key, test key, and contingency key. In the this scenario, a Product Requester orders a product that requires secondary approval and the Controlling Authority approves the order.

6.4.4.2 (U) Sequence Diagram

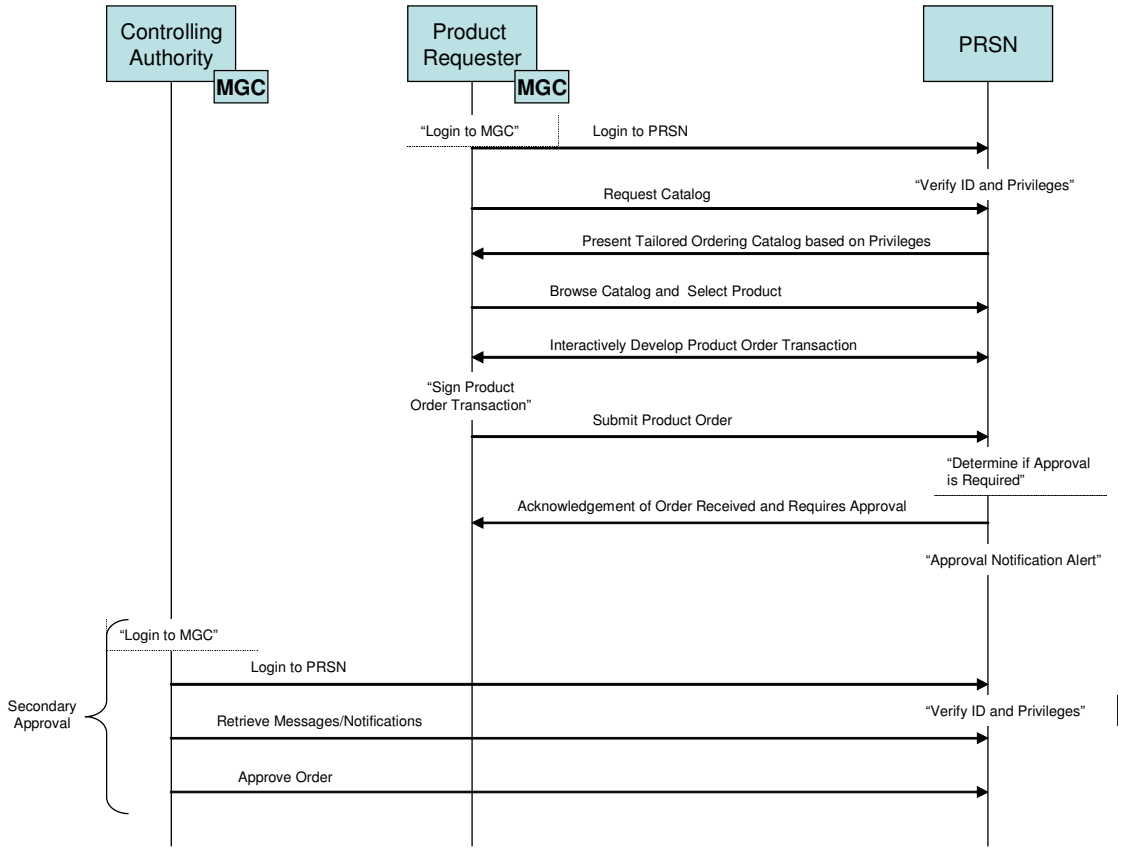


Figure 27: (U) Ordering of Symmetric Keys

6.4.4.3 (U) KMI Roles Involved

- (U) Controlling Authority
- (U) Product Requestor

6.4.4.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.4.4.5 (U) Prerequisites

- (U) The key material being ordered is in the Product Ordering Catalog (POC).
- (U) The Product Requester has been granted the necessary privileges to order the product.

6.4.4.6 (U) Sequence of Events

1. (U) The Product Requester logs into the MGC.
2. (U) The Product Requester authenticates to the PRSN.
3. (U) The MGC requests the product catalog from the PRSN on behalf of the Product Requester.
4. (U) The Product Requester requests the catalog.
5. (U) The PRSN determines the products that the given Product Requester has the authority to order, based on the Product Requester's privileges, and tailors the catalog appropriately.
6. (U) The tailored catalog is transmitted to the MGC; where it is presented to the Product Requester.
7. (U) The Product Requester browses the tailored ordering catalog for the desired product to be ordered.
8. (U) The Product Requester and PRSN interactively develop the product order transaction.
9. (U) The Product Requester signs the product order transaction.
10. (U) The Product Requester submits the order to the PRSN.
11. (U) The PRSN determines if the product order requires approval.
12. (U) The PRSN acknowledges the order is received and determines that the order requires secondary approval.
13. (U) The PRSN provides a notification alert for the Controlling Authority when they next log in.
14. (U) The Controlling Authority logs into the MGC.
15. (U) The Controlling Authority authenticates to the PRSN.
16. (U) The Controlling Authority receives approval notification.
17. (U) The Controlling Authority reviews and approves the product order.

6.5 Product Ordering and Distribution Process – Asymmetric Key

(U) There are several steps of the Product Ordering and Retrieval process for Asymmetric Keys, as shown in Figure 28. The first step is for the Command Authority to establish the product, in which the partition and DAO codes are established. This data is updated in the catalog at the PRSN Product Requirement Data Store.

(U) When ready to order, the Product Requestor requests the Product Ordering Catalog from the PRSN Product Requirement Data Store. After requesting the required products, this process enters the generation and production phase. Here, the products are generated and produced in the wrapping credentials. The products are then distributed either electronically or physically to their appropriate destinations.

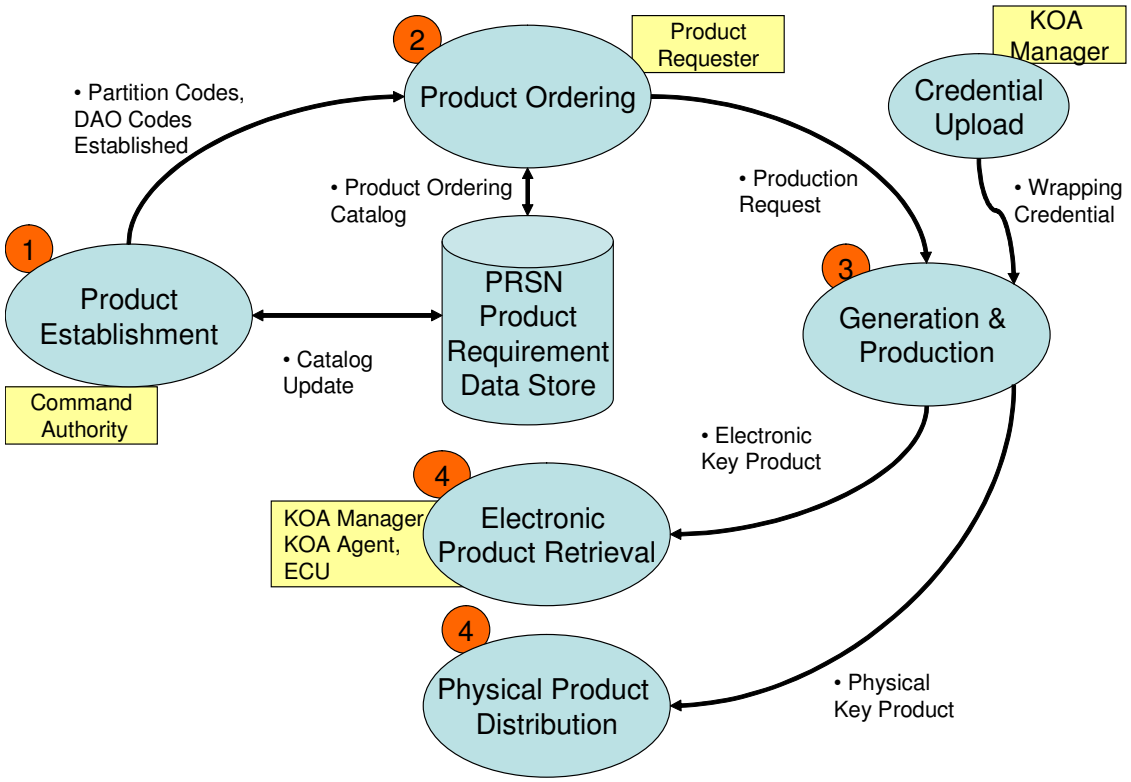


Figure 28: (U) Product Ordering and Distribution Process– Asymmetric Key

6.5.1 (U) Establishment of Partition/DAO Code Privileges for Asymmetric Key Ordering

6.5.1.1 (U) Summary

(U) This scenario describes the events associated with the establishment of partition/DAO code privileges for asymmetric key ordering. The scenario includes a Command Authority establishing a partition code and/or DAO code and assigning ordering privileges to a Product Requester.

6.5.1.2 (U) Sequence Diagram

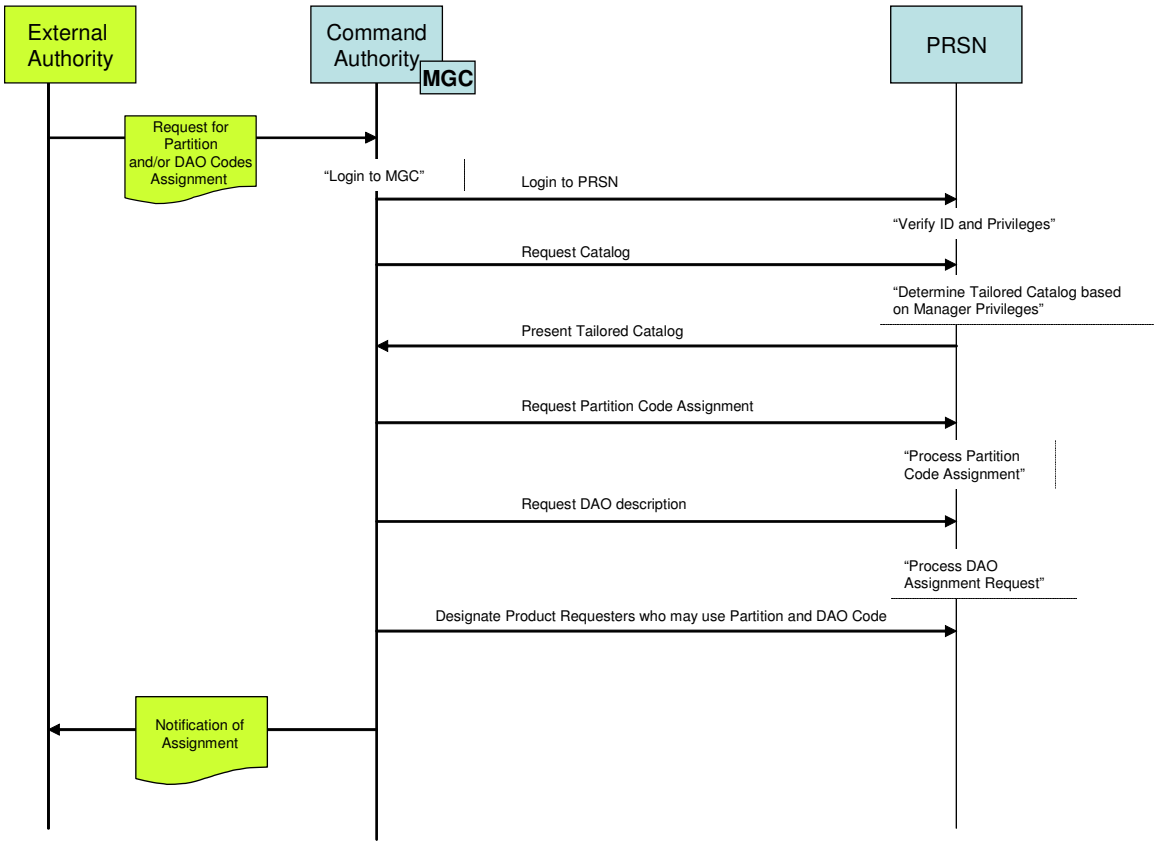


Figure 29: (U) Establishment of Partition/DAO Code Privileges for Asymmetric Key Ordering

6.5.1.3 (U) KMI Roles Involved

- (U) Command Authority

6.5.1.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.5.1.5 (U) Prerequisites

- (U) Product type has been previously been established.

6.5.1.6 (U) Sequence of Events

1. (U) The External Authority sends a notice to the Command Authority, typically out-of-band, that a new DAO code or partition code is needed.
2. (U) The Command Authority logs into the MGC.
3. (U) The Command Authority connects and authenticates to the PRSN using the MGC.
4. (U) The Command Authority requests the catalog.
5. (U) The PRSN determines the tailored catalog based on the privileges of the Command Authority.
6. (U) The Catalog is sent to the Command Authority.
7. (U) The Command Authority requests a Partition Code assignment.
8. (U) The PRSN processes the partition code assignment.
9. (U) The Command Authority requests a new DAO description.
10. (U) The PRSN processes the DAO code assignment request.
11. (U) The Command Authority designates Product Requesters who may use specific Partition and DAO codes**.**
12. (U) The Command Authority notifies the External Authority.

6.5.2 (U) Ordering of Asymmetric Key

6.5.2.1 (U) Summary

(U) This scenario describes the events associated with ordering asymmetric key.

6.5.2.2 (U) Sequence Diagram

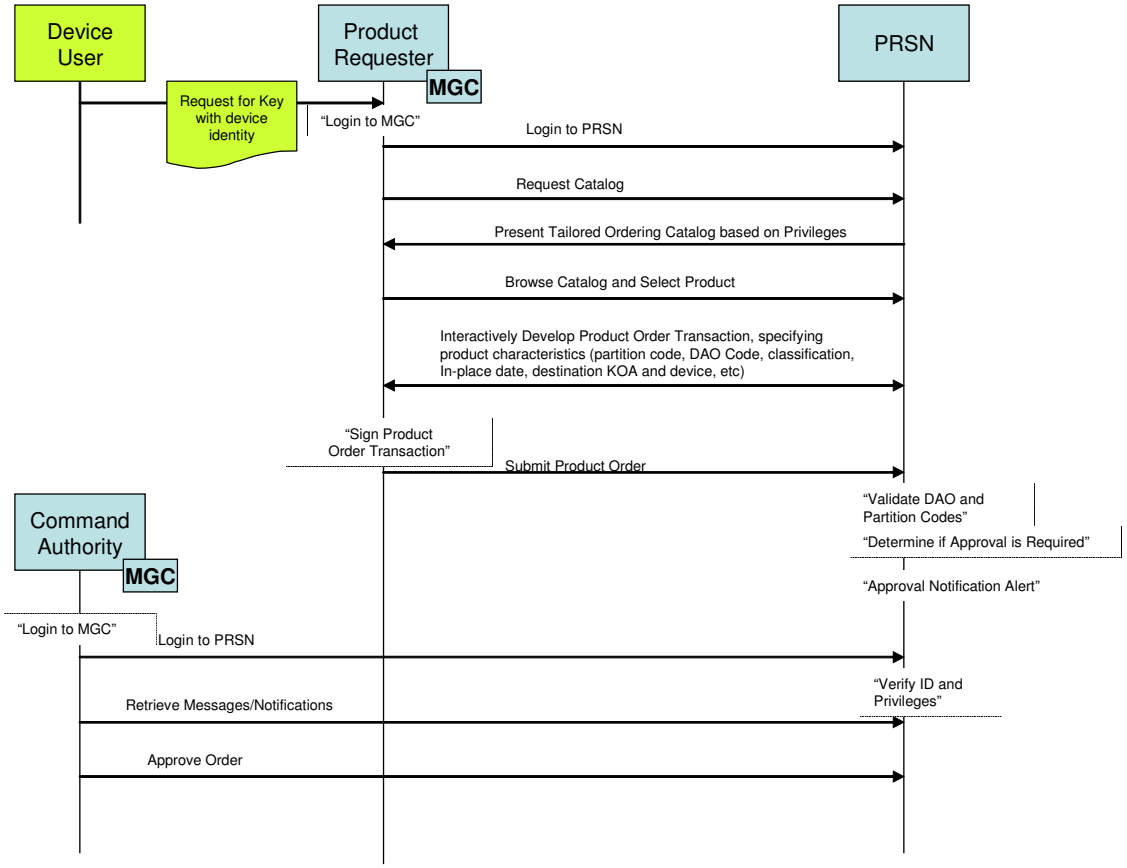


Figure 30: (U) Ordering of Asymmetric Key

6.5.2.3 (U) KMI Roles Involved

- (U) Command Authority
- (U) Product Requestor

6.5.2.4 (U) KMI Nodes Involved

- (U) Manager Client (MGC)
- (U) PRSN

6.5.2.5 (U) Prerequisites

- (U) Product type has been previously been established.

- (U) The Command Authority must have assigned, along with other product specific data, partition and DAO codes (if applicable) to a designated Product Requestor.

6.5.2.6 (U) Sequence of Events

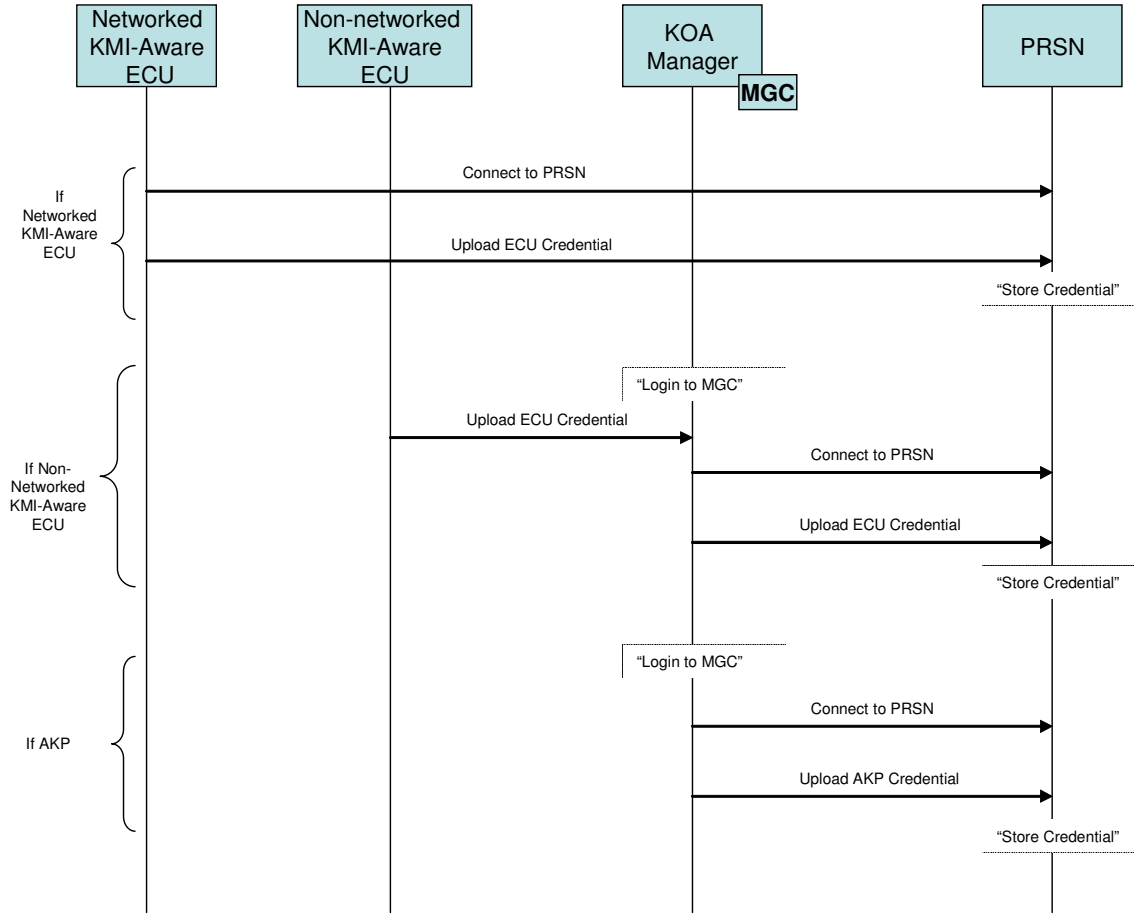
1. (U) The Device User sends a request for key for the device identity to the Product Requester.
2. (U) The Product Requester logs into the MGC.
3. (U) The Product Requester authenticates to the PRSN.
4. (U) The MGC requests the product catalog from the PRSN on behalf of the Product Requester.
5. (U) The PRSN determines the products that the given Product Requester has the authority to order, based on the Product Requester's privileges, and tailors the catalog appropriately.
6. (U) The tailored catalog is presented to the Product Requester.
7. (U) The Product Requester browses the tailored catalog for the desired product to be ordered.
8. (U) The Product Requester and PRSN interactively develop the product order transaction, specifying product characteristics (partition Code, DAO Code, classification, in-place date, destination KOA and device, etc).
9. (U) The Product Requester signs the product order transaction.
10. (U) The Product Requester submits the order to the PRSN.
11. (U) The PRSN validates the DAO and partition codes.
12. (U) The PRSN determines if the product order requires approval.
13. (U) The PRSN provides a notification alert for the Command Authority when they next log in.
14. (U) The Command Authority logs into the MGC.
15. (U) The Command Authority authenticates to the PRSN.
16. (U) The Command Authority receives approval notification.
17. (U) The Command Authority reviews and approves the product order.

2302 ## 6.5.3 (U) Credential Upload

2303 ### 6.5.3.1 (U) Summary

2304 (U) This scenario describes the process for credential upload of Networked KMI-aware
2305 ECUs, Non-networked KMI-Aware ECUs, and AKPs, as appropriate, to the PRSN to
2306 support key wrapping.

2307 ### 6.5.3.2 (U) Sequence Diagram



2308

2309 **Figure 31: (U) Credential Upload**

2310 ### 6.5.3.3 (U) KMI Roles Involved

2311 - (U) KOA Manager

2312 ### 6.5.3.4 (U) KMI Nodes Involved

2313 - (U) Manager Client (MGC)
2314 - (U) PRSN

2315 ### 6.5.3.5 (U) Prerequisites

2316 - (U) Credentials have been generated and are available for upload.

6.5.3.6 (U) Sequence of Events

If Credential Upload for Networked KMI-Aware ECU:

1. The ECU connects to the PRSN.
2. The ECU uploads its credential to the PRSN.
3. The PRSN stores the credential.

If Credential Upload for Non-networked KMI-Aware ECU:

1. The KOA Manager logs into the MGC.
2. The ECU's credential is uploaded to the KOA's MGC.
3. The KOA Manager connects to the PRSN.
4. The KOA Manager uploads the ECU credential to the PRSN.
5. The PRSN stores the credential.

If Credential Upload for AKP:

1. The KOA Manager logs into the MGC.
2. The KOA Manager connects to the PRSN.
3. The KOA Manager uploads the AKP credential to the PRSN.
4. The PRSN stores the credential.

6.5.4 (U) Generation and Production

6.5.4.1 (U) Summary

(U) This scenario describes the process where an order request is triggered by a provisioning schedule or an on-demand order and the resulting electronic and/or physical key material is generated and produced.

6.5.4.2 (U) Sequence Diagram

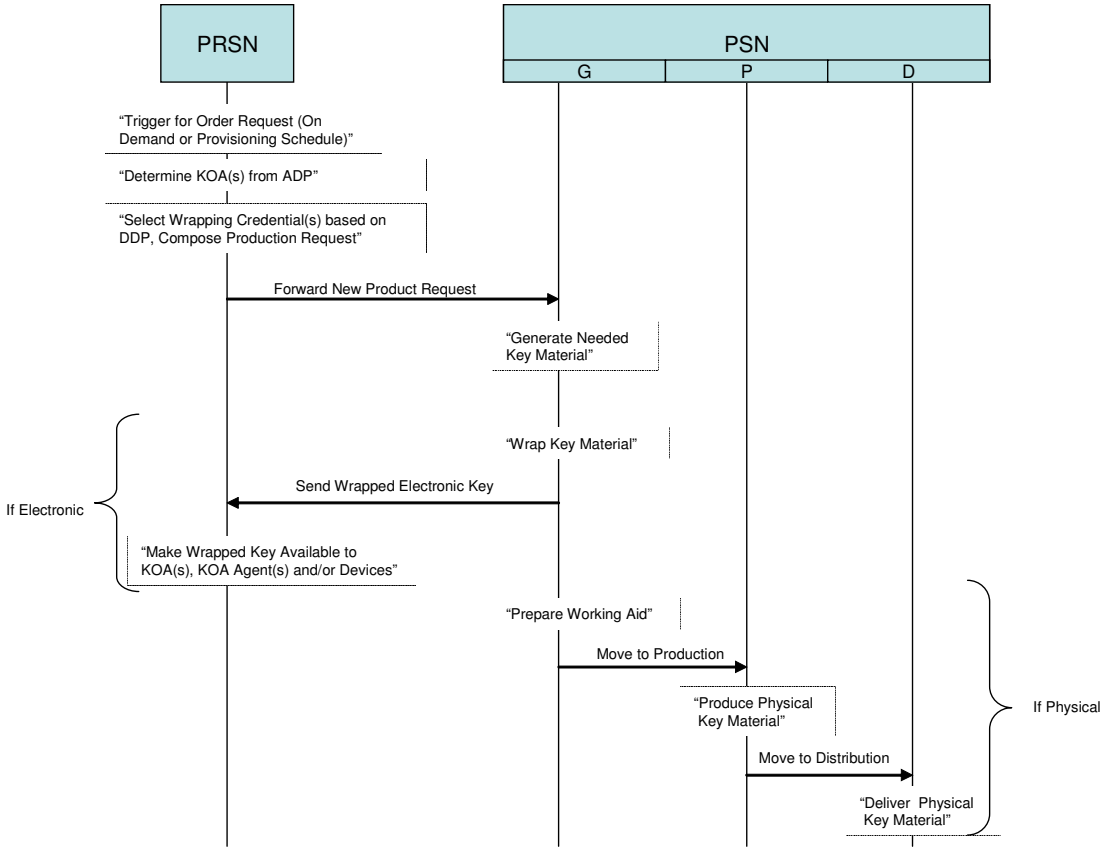


Figure 32: (U) Generation and Production

6.5.4.3 (U) KMI Roles Involved

- (U) None

6.5.4.4 (U) KMI Nodes Involved

- (U) PSN
- (U) PRSN

6.5.4.5 (U) Prerequisites

- (U) A requested product has been approved by the PRSN.
- (U) A standing order has been established.
- (U) Wrapping credentials have been uploaded to the PRSN.

6.5.4.6 (U) Sequence of Events

1. (U) A trigger for an order request (On Demand or Provisioning Schedule) occurs at the PRSN.
2. (U) The PRSN checks the product's Account Distribution Profile to determine which KOAs should receive the product.
3. (U) The PRSN evaluates the product order, selects the appropriate wrapping credential(s) based on the Device Distribution Profile(s), and composes a production request.
4. (U) The PRSN forwards the production request, including the wrapping credential(s), to the PSN.
5. (U) The PSN generates and produces the needed material to fill the production request.

If Electronic Key:

1. (U) The electronic key is wrapped by the PSN according to the production request.
2. (U) The wrapped electronic key is returned to the PRSN from the PSN; if there are multiple recipients of the key, separate, individually-wrapped key copies will be returned.
3. (U) The wrapped key(s) is stored in the PDE for retrieval by an appropriate entity(s) (e.g. KOA Manager, KOA Agent, KMI device).

If Physical Key:

1. (U) The physical key is moved to Production using a working aid.
2. (U) The physical key is transferred to the appropriate format (e.g. floppy, CD-ROM, etc).
3. (U) The physical key is moved to Distribution for physical delivery.

6.5.5 (U) Electronic Product Retrieval

6.5.5.1 (U) Summary

(U) This scenario describes the processes used by ECUs, and KMI clients to retrieve key products for use. The scenario will present options for key retrieval options for (1) Networked KMI-Aware ECUs, (2) Non-networked KMI-Aware ECUs, and (3) AKPs.

6.5.5.2 (U) Sequence Diagram

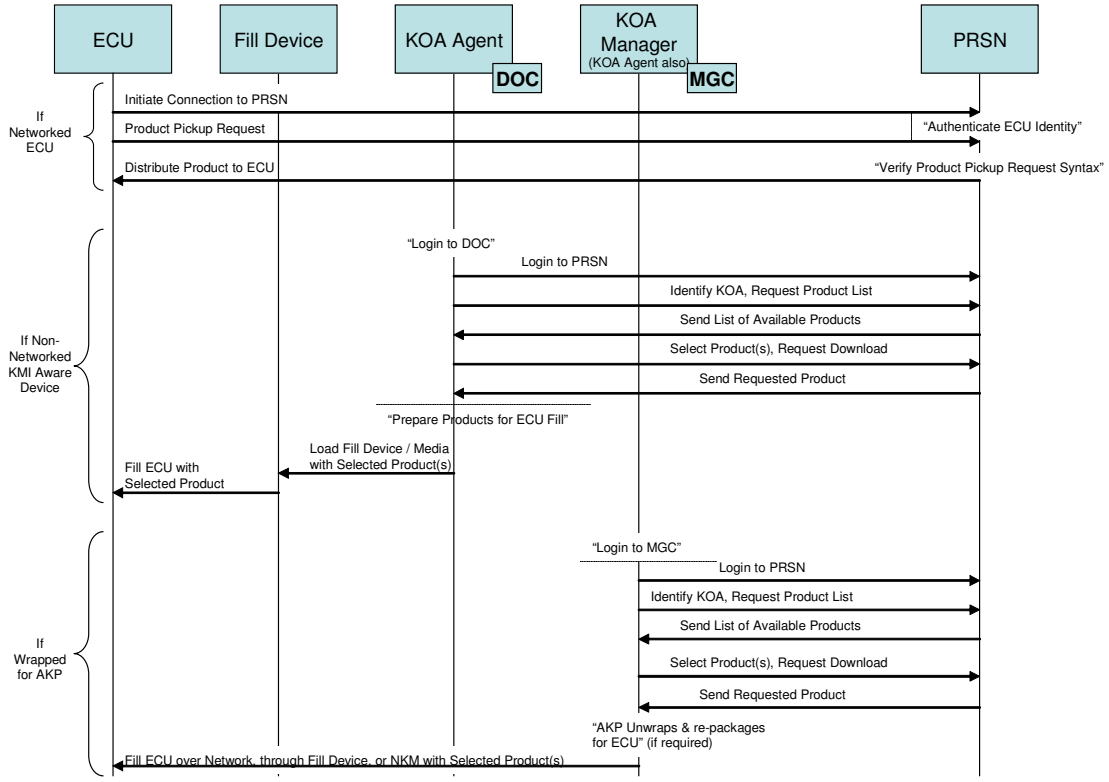


Figure 33: (U) Electronic Product Retrieval

6.5.5.3 (U) KMI Roles Involved

- (U) KOA Agent

6.5.5.4 (U) KMI Nodes Involved

- (U) ECU
- (U) Fill Device
- (U) Manager Client (MGC)
- (U) Delivery-Only Client (DOC)
- (U) PRSN

6.5.5.5 (U) Prerequisites

- (U) KOA Manager must be registered or KOA Manager must have designated a KOA Agent.
- (U) One or more key products have been requested and directed to the KOA by appropriately privileged KMI Managers.
- (U) ECU is associated with a KOA.
- (U) Key product for ECU must have been generated and made available at the PRSN for retrieval.

6.5.5.6 (U) Sequence of Events

By ECU Directly:

1. (U) The ECU initiates a connection to the PRSN.
2. (U) The PRSN verifies that the product pickup request syntax is correct.
3. (U) The PRSN authenticates the identity of the ECU.
4. (U) The PRSN delivers all products authorized and available for the requesting ECU.

By KOA Agent for Relay to ECU:

1. (U) The KOA Agent logs into the DOC.
2. (U) The KOA Agent logs into the PRSN.
3. (U) The KOA Agent identifies the KOA for which they wish to retrieve key. The KOA Agent requests the product list for the identified KOA from the PRSN.
4. (U) The PRSN sends the list of available products to the MGC.
5. (U) The KOA Agent selects the product(s) they wish to download and the request is sent to the PRSN.
6. (U) The PRSN sends the requested product(s) to the MGC.
7. (U) If ECU loading is performed later, the KOA Manager logs into the MGC.
8. (U) The product is prepared for the ECU it is destined for. (Note: this does not include any unwrapping or rewrapping of the product.)
9. (U) The MGC loads the product into a fill device or other portable media.
10. (U) The FD or portable media loads the key into the ECU.

By KOA Manager for Further Processing / Distribution:

1. (U) The KOA Manager logs into the MGC.
2. (U) The KOA Manager logs into the PRSN.
3. (U) The KOA Manager identifies the KOA for which they wish to retrieve key. The KOA Manager requests the product list for the identified KOA from the PRSN.
4. (U) The PRSN sends the list of available products to the MGC.

5. (U) The KOA Manager selects the product(s) they wish to download and the request is sent to the PRSN.
6. (U) The PRSN sends the requested product(s) to the MGC.
7. (U) If ECU loading is performed later, the KOA Manager logs into the MGC.
8. (U) The MGC's AKP unwraps the package and re-packages it for the destined ECU (if required).
9. (U) The MGC fills the ECU with the selected product over the network, through a fill device, or via the Net Key Management.

6.5.6 (U) Physical Product Distribution

6.5.6.1 (U) Summary

(U) This scenario shows the process for the delivery of finished KMI products from the Production segment, storing them, and preparing shipment of orders, aggregating products, which are packaged and transferred to a carrier or courier, and accounting actions that take place internally and externally to KMI.

6.5.6.2 (U) Sequence Diagram

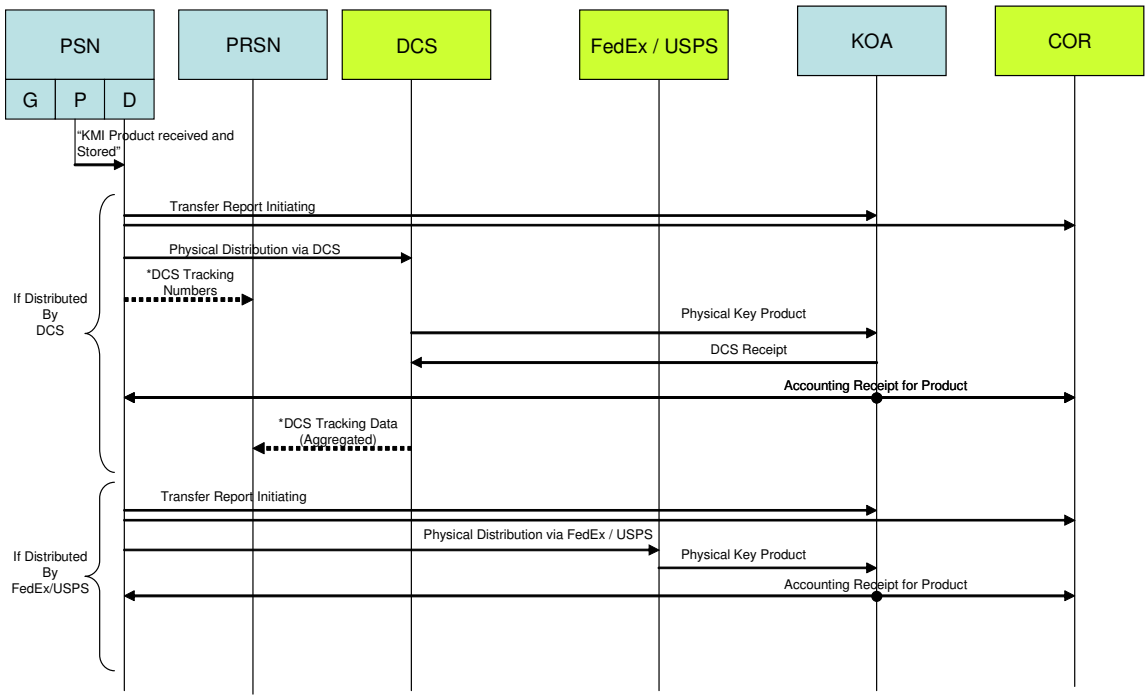


Figure 34: (U) Physical Product Distribution

6.5.6.3 (U) KMI Roles Involved

- (U) PRSN
- (U) Recipient KOA
- (U) COR

6.5.6.4 (U) KMI Nodes Involved

- (U) PRSN
- (U) PSN
- (U) KOA

6.5.6.5 (U) Prerequisites

- (U) KMI products have been received from the Production segment of the PSN.
- (U) Products have been authorized for shipment.

6.5.6.6 (U) Sequence of Events

1. (U) The PSN Distribution Enclave physically receives products from the Production Enclave of the PSN.
2. (U) The PSN Distribution Enclave stores these products until they are ready for shipment.

If Distribution By DCS:

1. (U) The PSN sends a "Transfer Report Initiating" to the recipient KOA and the KOA's COR.
2. (U) The PSN Distribution Enclave ships product via DCS (Defense Courier Service).
3. (U) The PSN sends DCS tracking numbers to the PRSN.
4. (U) The physical key product is delivered to the recipient KOA via DCS.
5. (U) DCS receives a delivery confirmation from the recipient KOA.
6. (U) The recipient KOA sends an accounting receipt back to the PSN and to the COR.
7. (U) The PRSN collects tracking data (aggregate) from DCS.

(Note: This step does not happen in sync with the real time distribution of physical products via DCS).

If Distribution By FedEx / USPS:

1. (U) The PSN sends a "Transfer Report Initiating" to the recipient KOA and the COR.
2. (U) The PSN Distribution Enclave ships product via FedEx / USPS.
3. (U) The physical key product is delivered to the recipient KOA via FedEx / USPS.
4. (U) The recipient KOA sends an accounting receipt back to the PSN and to the COR.

7 (U) Summary of Impacts

7.1 (U) CI-2 and Legacy Key Management Systems

(U//FOUO) One of the goals of Capability Increment 2 of the KMI is to move the infrastructure closer to the KMI Target Architecture. It should be kept firmly in mind, however, that CI-2 is just that – an *increment*. After decades of development and operation of the current set of legacy components, policies, and procedures, it is neither

possible nor desirable to replace everything that has been deployed with something new in one step.

(U//FOUO) CI-2 has to find a balance between implementing features of the Target KMI (such as providing web-based capabilities and implementing a logical split between customer interfaces and the key generation components), providing backward compatibility with existing components (such as the ability to use LMD/KPs to receive encrypted keys and order material) so as not to have to transition away from those components immediately, and enhancing ease of use (such as minimizing duplication of data entry).

(U//FOUO) A major difference between the concepts of the Target and the concepts in use today is that the Target is largely human user-oriented, while the current key management system is KME-oriented. The EKMS ID of the group of users and components at any particular location is the identity used as the basis for decisions in the current system, whereas the Target architecture focuses on individual identity as the basis for privileging and decision-making. One of the lines that had to be drawn for CI-2 is how much of each type of focus would be maintained. The result is a concept of tying roles and privileges to human user identities, but then additionally linking the human users to the collection of users and components that share an EKMS ID, bridging the two paradigms in this interim stage.

(U//FOUO) The following subsections highlight some of the impacts that balancing the various goals will have, operationally and organizationally. Two of the more complex areas of the CI-2 system and impacts are those of access control/privilege management and accounting, and those issues will be addressed as well.

7.2 (U) Operational Impacts

(U//FOUO) One of the critical pieces of maintaining continuity with the various new and legacy infrastructure components and subsystems will be the use of the EKMS ID (though in CI-2, as today, having an EKMS ID does not imply use of EKMS components). Use of these IDs has a variety of implications, especially when coupled with the need for backward compatibility. For instance, in EKMS, there is a one-to-one relationship between a KP, a COMSEC Account, and an EKMS ID. A KP cannot support more than one COMSEC Account/ID, and more than one KP cannot support a single COMSEC Account/ID. This paradigm implies that there must be one AKP per KOA/COMSEC Account that is somehow identified as the primary AKP, the peer to the KP/primary AKP at other accounts.

(U//FOUO) CI-2 will provide a transition path for operational key management support to move from EKMS LMD/KPs to KMI client nodes. While the goal is to minimize need for parallel EKMS and KMI workstations for user-level operations, it may prove necessary to have multiple workstations at certain locations (e.g., a Registration Authority at the EKMS Tier 1 system might need both Tier 1 and KMI workstations in order to perform all of their registration duties).

(U//FOUO) Transition — both at the long-term system level, moving from CMCS/EKMS to the KMI Target Architecture, and at the user level, moving from legacy automation or no automation at all to CI-2 clients — is at the heart of many of the biggest challenges of

CI-2. Additional information on specific transition issues is included in the remaining subsections.

7.3 (U) KMI CI-2 Transition Philosophy

(U//FOUO) The initial focus of CI-2 transition would be to migrate key ordering and management functions to operate via the PRSN. So the approach taken when CI-2 capabilities initially become available would be to:

- (U) Encourage a rapid transition to KMI for those job functions and personnel whose mission can be conducted using a client node without an AKP
- (U//FOUO) Begin transition of paper-based[6] and LMD-only COMSEC accounts to KMI client nodes
- (U//FOUO) Continue using the EKMS LMD/KP at COMSEC accounts where it is operating effectively (this may be the Phase 4 LMD/KP or an updated version, depending on EKMS development activities between now and CI-2 IOC)
- (U//FOUO) Continue EKMS Tier 1 operations

(U//FOUO) Once the transition of ordering and management functions is accomplished, then the focus of transition activities will shift to COMSEC accounts. Activities at this point would be:

- (U//FOUO) Continue efforts to transition paper-based and LMD-only COMSEC accounts to KMI client nodes
- (U//FOUO) Begin transitioning COMSEC accounts away from LMD/KPs to the use of KMI client nodes.

(U) Over time, more and more COMSEC account activity will be moved to KOA operating with KMI client nodes. However, there will likely be a considerable period of time where a mixture of EKMS and KMI equipment and processes are used to perform the overall key management mission.

7.4 (U) KMI CI-2 Transition Implementation

(U) Specific actions to implement the transition philosophy described above include:

- (U//FOUO) At CI-2 IOC, enroll Controlling Authorities handling traditional key as KMI Controlling Authorities and equip them with KMI Manager clients
- (U//FOUO) At CI-2 IOC, enroll Command Authorities for FIREFLY key as KMI Command Authorities and equip them with KMI Manager clients
- (U//FOUO) At CI-2 IOC, enroll User Representatives for FIREFLY key as Product Requestors and equip them with KMI Manager clients, unless the User Rep is using an LMD or LMD/KP for ordering

[6] "Paper-based" refers to any COMSEC account not using EKMS technology for its operation. It is inclusive of accounts operating with non-EKMS automation packages developed over time by a number of customer organizations.

(U//FOUO) To support this approach, the following information needs to be installed in the PRSN at IOC:

- (U//FOUO) A Product Ordering Catalog containing all physical and electronic products currently being produced by Tier 0 / Central Facility Finksburg and Fort Meade, as well all electronic products being produced by the EKMS Tier 1 system.
- (U//FOUO) Privileging information for Controlling Authorities, Command Authorities, and User Representatives as described in section 7.6.

7.4.1 (U) EKMS Tier 1 System

(U) Under CI-2, EKMS Tier 1 operations and personnel should be to continue operating as they have prior to CI-2, except that:

- (U//FOUO) EKMS Registration Authorities are the logical candidates to perform KOA Registration Manager functions for KOAs. Consequently, personnel serving as EKMS Registration Authorities will have to be enrolled as KOA Registration Managers and will need a KMI client node in addition to their EKMS tools.
- (U//FOUO) Tier 1 should be configured to accept orders submitted via the PRSN in electronic form. Such orders will originate from the EKMS Translator and should be easily distinguished from orders originating at EKMS LMD or LMD/KP workstations.

7.4.2 (U) COMSEC Account Transition Options

(U) There are a number of options that may be considered for the transition of an existing COMSEC Account to operations under CI-2. The parent organization responsible for each account will need to define their overall approach to operating with KMI and then make an corresponding determination of the appropriate transition approach for each of their COMSEC accounts:

- (U//FOUO) LMD/KP-equipped accounts potentially have several transition paths, depending on the operational requirements and communications situation of the account:
  - (U//FOUO) Convert from the LMD/KP to an AKP-equipped KMI client node. This replaces the LMD/KP with a functionally analogous KMI element and account operations should be able to continue in a similar manner to operating under EKMS.
  - (U//FOUO) Convert from the LMD/KP to a KMI client node; depending on the needs of the account, this client could be employed in one of two ways:
    - (U//FOUO) The KOA could receive its cryptographic support directly from the KMI PRSN, using the KMI client node to download BLACK/benign key wrapped for the account's ECUs.

(U//FOUO) The technical details of supporting each of the transition paths from LMD/KP or paper operations to an appropriately configured KMI client node will be determined as part of the KMI client development activities.

7.5 (U) Organizational Impacts

(U//FOUO) Customer agencies will need to develop criteria for the appropriate KOA / KMI Client Node configurations for current COMSEC/EKMS accounts and other KMEs. Things to be considered include the capabilities provided by each client-type and application, the roles and privileges to be held by the human users of the client nodes, the communications environment, and the local organizational structure. Some KMEs that are currently supported by LMD/KPs (e.g., smaller COMSEC Accounts) might be able to move to a lighter-weight client node without cryptographic support, while some KMEs that currently don't have any automated components (e.g., many Controlling Authorities) will benefit from the use of a CI-2 client node.

(U//FOUO) It should be noted again that despite the use of new terminology, which is meant to bring together the various key management stovepipes that exist today, CI-2 is not expected to increase the workload of the customer or impose new staffing requirements on the customer. A goal of CI-2 is to provide the customer with the tools needed to carry out the necessary functions in the way best suited to the individual customer. Therefore, there should not be significant organizational impact caused by the development and deployment of CI-2.

7.6 (U) Transition of Privileges from EKMS to KMI

7.6.1 (U//FOUO) FIREFLY Management and Privileging

(U//FOUO) One component of the infrastructure which is not currently slated for major retooling in the CI-2 timeframe is the Central Facility – Finksburg (CFF) FIREFLY management and generation system. Retention of that component more or less as-is has implications for the whole life cycle of modern asymmetric key, from creation of new DAO and partition codes to the privileging of User Representatives to the ordering of the material. The existing Command Authority and User Representative structure and ordering capabilities will be left intact, which meets the goal of backward compatibility but does not move toward the Target or provide new features.

(U//FOUO) Therefore a new interface to the existing capability needs to be implemented in CI-2. Command Authorities will be able to carry out their modern key management tasks either through existing means or via a CI-2 Manager client. When using a CI-2 Manager client, the Command Authorities must additionally hold the relevant Command Authority role and approvals so that the CI-2 PRSN can perform the necessary KMI validations. Translation of the KMI-style requests into CFF-style requests is then the task of the PRSN and/or EKMS translator. Likewise, User Reps will be able to order modern key via the existing mechanisms or via a CI-2 Manager client.

(U//FOUO) To minimize duplication of effort in granting the appropriate privileges to Command Authorities and User Reps, CI-2 will have to have the capability to share data between the PRSN and the CFF backend system on privileges. For instance, when an existing Command Authority with an EKMS ID becomes a CI-2 human user, that Command Authority will need to be enrolled through the appropriate KMI process as a Command Authority, but the association of that human user with his/her EKMS ID will enable the PRSN to translate and associate all the existing privileges at the CFF to that human user as a Command Authority. Privileges maintained via the existing methods

will flow through the CFF to the PRSN, and privileges maintained via the new CI-2 mechanisms will similarly reside in both places.

(U//FOUO) This approach requires a small amount of additional work to transition existing Command Authorities and User Reps to Command Authorities and Product Requestors, respectively, for those who choose to make use of the new CI-2 clients, but the maintenance of those users' privileges should be able to be done via either the old or new mechanisms with the duplication of the privileging data handled by the CFF and the PRSN rather than by those establishing the privileges. Additionally, this approach has the advantage of meeting both legacy and Target requirements and will make it easier to transition completely away from the existing mechanisms for privilege establishment and enforcement in the future.

7.6.2 (U) Traditional Key Management and Privileging

(U//FOUO) Privileging for the management and ordering of traditional symmetric key should in many cases be less complex than that for asymmetric key management, because more of the existing legacy systems will be rebuilt. Also, in many cases those doing management of traditional material today are not highly automated and not dependent on electronic privilege enforcement mechanisms. However, CI-2 can be expected to make transitioning those symmetric key privileges that exist electronically in EKMS today as seamless as possible.

7.6.3 (U//FOUO) COMSEC Account Privileges

(U//FOUO) In the EKMS Phase 4 timeframe, KMEs are given EKMS IDs to represent them in any key management role they might play. One of the roles that can be given to a KME is that of COMSEC Account. The EKMS Directory is the mechanism by which the details of a KME's COMSEC Account privileges are shared with those other KMEs that need to make use of that information for privilege enforcement decisions (such as whether a certain key can be shipped to that KME).

(U//FOUO) The concept of the COMSEC Account is not one that will disappear in the CI-2 era. KMEs that need to be COMSEC Accounts will still be assigned EKMS IDs, have COMSEC Account privilege information associated with them, and be placed in the EKMS Directory. Additionally, data on those COMSEC Account-privileged KMEs will be kept synchronized with the CI-2 PRSN for use in new KMI functions. The assumption behind this approach is that the EKMS Registration Authority and Central Office of Record functions that have been built into Tier 0 and Tier 1 will not be able to be retooled to perform these registration functions a new way in the CI-2 timeframe. However, the intention is not to constrain the Services and agencies from using KMI tools to accomplish registration functions should it be desirable to make the necessary changes to the existing systems to support the new functionality.

7.7 (U) Accounting

(U//FOUO) The area of Accounting is one where what is defined in the Target architecture (referred to as "control") and what exists today (referred to for convenience in this section as "traditional accounting") are considerably different in terms of implementation if not intent.

(U//FOUO) The new tracking concepts apply to new "pure" CI-2 functions. There is already a system in place today for handling traditional accounting, with the Central Offices of Record at Tiers 0 and 1 and accounting transactions implemented both physically and electronically. Where the new KMI functions and the legacy functions come together, for instance when sending a key from an LMD/KP to an AKP-equipped KMI client node, or using a client to manage physical COMSEC assets, the accounting questions become much more complicated.

(U//FOUO) The legacy accounting systems are some of the most complex pieces of the entire key management infrastructure, and to completely replace them with new functionality is simply not possible in the CI-2 timeframe. Therefore, the balancing of the various system goals in this area has led to an approach which reuses EKMS accounting transaction body definitions as well as the existing COR implementations at Tiers 0 and 1 for the traditional accounting of material which requires accounting back to a COR (physical or electronic key and equipment in accordance with the relevant policies), while adding Target-type tracking for new KMI transactions, to include key encrypted for KMI-aware ECUs.

(U//FOUO) One of the client applications that can be run locally on a client node will support “traditional” accounting functionality for those clients that need it. Clients that need to exchange “traditional” accounting data with their COR will be able to pass EKMS transaction bodies through the PRSN and the EKMS translator to their COR (and back).

(U//FOUO) Implementation of accounting and tracking as defined for CI-2 will involve modification to a variety of existing policies and procedures. The definition of concepts in CI-2 assumes certain outcomes to these policy questions: encrypted key is Unclassified//For Official Use Only (i.e., no longer unclassified *crypto*), key encrypted for an ECU is not traditionally accountable, etc. Significant work to make these policy changes happen is necessary at all levels.

8 (U) Analysis of the Proposed System

(U) This section provides a brief analysis of the proposed CI-2 with respect to existing key management systems and operations.

8.1 (U) Summary of Improvements

- (U) Ability to conduct key management operations using common user TCP/IP backbones
- (U) Improved support for Controlling Authority key ordering and management functions over that available through EKMS
- (U//FOUO) Replacement of complex and difficulty to support LMD workstation with web-based user interface on commonly used hardware platforms
    - (U) Easier to maintain, update and improve user interface
    - (U) Eliminates need to support a unique operating just for the LMD
- (U) Support for over-the-network keying to next-generation ECUs that support that feature

- (U) Support for integrating KMI client features into customer-developed/operated MPMSS to simplify providing key distribution support to complex systems
- (U) Architecture designed to simplify providing interoperable key management support for CCEB, NATO, and other allied / coalition partners
- (U) Next generation AKP to build on concepts and capabilities of existing EKMS KP while addressing some of its shortcomings

8.2 (U) Disadvantages and Limitations

- (U) Some dedicated workstations still required:
  - (U) Certain sensitive functions must be kept secure
  - (U) Must maintain separation of material at different classifications (no MLS)
  - (U) Will require purchase, configuration, support of high-assurance INEs and cooperation with managers of customer-provided networks to develop acceptable operating configurations
- (U) Dependent on availability of communications networks not under KMI control
- (U) Uncertain impact on communications network bandwidth – goal is to minimize impact but lacking good models of network loading and given potential for shifts in how COMSEC operations are conducted with new technology it is very difficult to predict the actual impact
- (U) Need separate token and registration / enrollment processes for KMI Managers responsible for cryptographic activities
- (U//FOUO) KMI Client nodes used at KOAs will, in general, continue to operate at the SECRET level, system-high
- (U//FOUO) Last mile solutions for CI-2 are based on existing fill devices (i.e., KOV-21 family, AN/CYZ-10)

(U) Glossary

Access: The ability and the means to communicate with, or otherwise interact with, a system's resources in order to either (1) handle data held by the system or (2) control system components and their functions
Access Control: A service that protects against unauthorized access to system resources (including protecting against use of a resource in an unauthorized manner by a user that is authorized to use the resource in some other manner).
Account Distribution Profile: Structured, formatted information regarding which KMI Accounts are authorized to receive specific products. Account distribution profiles are maintain at the PRSN on the basis of orders provided by Controlling Authorities and Product Requestors.
Accounting: (also called product accounting or COMSEC accounting): The process of collecting, recording, and managing information that describes the status and custody of designated key management products during each product's lifecycle. (KMI definition)
Advanced Key Processor (AKP): A cryptographic device for use with KMI clients capable of performing key management functions such as key generation, key distribution, and key redistribution.
Authorization: A right or a permission that is granted to a User or other system entity to access a system resource for a specific purpose.
Basic User: A Role that enables a Registered User to receive and consume certain KMI products and services in addition to those granted to Public Users, and including those services necessary to maintain the products received.
Client Node: A device that is capable of interacting with a KMI Primary Services Node via a computer network to obtain needed KMI products and services or to perform KMI operational or administrative management functions.
Component: A collection of system resources that form a physical or logical part of the KMI system that (1) has specified functions and interfaces and (2) is treated, by policies or requirement statements, as existing independently of the other parts.
COMSEC Incident Analysis Report: Report generated by the PRSN on the basis of a request from a Controlling Authority that indicates which products within the Controlling Authority's purview have been encrypted for a specific ECU (or set of ECUs). In addition, the report will describe which products are known to have been delivered to a specific ECU via direct interactions with the PRSN. The COMSEC Incident Analysis Report will also provide any additional tracking and auditing information that may assist in assessing the damage associated with loss of control of the ECU. The COMSEC Incident Analysis Report assists the Controlling Authority in determining which products (e.g., Short Title and Editions) may have been compromised when an ECU is the subject of a COMSEC incident.

Common Account Data: Information stored in the EKMS Directory about a Key Management Entity. Common Account Data includes KME-specific information such as identification number, attributes (e.g., administrative data, role, restrictions, etc.), and equipment configurations. This information is initially identified during the account registration process and maintained by the KME and its EKMS RA as appropriate.
Credentials: Information supplied by a key recipient (e.g., an ECU) that permits a sender (e.g., the KMI PRSN) to authenticate the recipient and encrypt key uniquely for that recipient.
Domain: A set of KMI Users for which a defined set of access control attributes may be added, modified and withdrawn by a specific related named set of KMI Managers. A KMI User may belong to several domains, associated with access control attributes conferred by several different KMI Managers.
End Cryptographic Unit (ECU): A device, normally a component of a larger system, that provides security services to the larger system and, from the viewpoint of a supporting security infrastructure, is the lowest identifiable component with which a management transaction can be conducted.
Enrollment: The KMI process that assigns a KMI User Identity to a KMI Manager Role.
Event: An occurrence within the KMI that causes an event record to be generated. Event records are generated automatically during routine operations of all types by KMI components. When necessary, an event can be recorded through the manual entry of information, such as accounting events for physical items. (Proposed update to KMI Glossary definition from T/C/A Study)
Event Record: A set of data corresponding to a traceable or accountable occurrence that is retained within the KMI.
Group Identity: An User Identity that is registered for a User Set for which the KMI does not maintain a record of the members of the set (i.e., the KMI does not have knowledge of the User Persons, or User Devices, that belong to the set).
Information Integrity: The property that ensures that information has not been changed, destroyed, or lost in an unauthorized or accidental manner. (This property is concerned with the constancy of data values, i.e., information content that is encoded in data, and not with how accurately the information was recorded or how trustworthy the information source was.)
Key Loading and Initialization Facility (KLIF): A facility designed to support registration of User Devices with KMI and orders, receives, loads any KMI products needed to initialize those devices.

Key Management Infrastructure (KMI): All parts—computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine—that form the system that manages, and supports the ordering and delivery of cryptographic material and related information products and services to users.
Key Recovery: An intentional, alternate (i.e., secondary) process for learning the value of a cryptographic key that was previously used to perform a cryptographic operation. Specifically, "Production of a copy of an escrowed key and delivery of that key to an authorized requestor"
KMI Aware: An application or device that contains the necessary protocols and supports KMI interface specifications.
KMI Management Role: A Role that has privileges that are greater than the privileges of a Basic User and that enable a User to direct, control, or regulate some set of KMI system resources.
KMI Manager: A User that directs, controls, or regulates some set of KMI system resources.
KMI Operating Account: (KOA) A KMI Operating Account is the registered KMI user associated with an organizational unit. A KOA has associated ECUs and KMI Managers, is the KMI corollary to a COMSEC account, and provides a mechanism for bridging between the EKMS and KMI implementations of registration and privileging.
KMI Token: A User's individual cryptographic device that carries the User's PKI private keys and associated public-key certificates, algorithms, and related material.
KMI protected channel (KPC): A KMI communication channel that provides information integrity service, either information origin authentication service or peer entity authentication service (as is appropriate to the mode of communication), and, optionally, information confidentiality service.
KMI Role: A User job title within the KMI system that (1) incorporates a specific set of capabilities, (2) can be assigned Privileges, and (3) can be assigned to Users.
Device Distribution Profile: Structured, formatted information regarding which ECUs, fill devices, fill groups, and/or the AKPs within an account that are authorized to receive specific products. Device distribution profiles are generated by KOA Manager for the products their account receives, and are maintained at the PRSNs.
Operational Compromise Notification Message: E-mail message released by a Controlling Authority in response to a compromise that describes how KMI Account Managers should respond to compromise of a particular KMI product.
Operational Recovery Product Service Request: Product Service Request released by a Controlling Authority that requests product necessary to recover from a compromise.

Privilege: An positively-stated authorization (i.e., a permission) that (1) can be assigned to a Role and (2) enables a User acting in that Role to handle one or more specific KMI system resources, usually in the form of products, services, and operational and administrative functions and mechanisms.
Product Catalog: The product catalog will include all currently available KMI products. The KMI shall provide, via a common user interface, a KMI user tailored version of that catalog that gives descriptive information on cryptographic products the user is authorized to order and receive.
Product Ordering: the process by which KMI Users request products, services, and related information resources from the KMI.
Registered User: A User that accesses the KMI by invoking an identity that has been registered in the system.
Sponsor: A User Identity of a User Person who (1) requests that a new User Identity be registered for a User Device or a User Set and (2) officially represents the Government organization that is accountable for use of the new identity.
Subscription: A standing cryptographic product order and account distribution list established and maintained in the KMI by the Product Requestor. A subscription prompts the KMI to periodically generate, wrap, and post key for delivery.
System integrity. A security service that protects system components in a verifiable manner against unauthorized change throughout their lifetime.
Template Compromise Notification Message: E-mail message composed in advance of a compromise that describes how KMI Account Managers should respond to compromise of a particular KMI product. The template Compromise Notification Message is generally modified by a Controlling Authority prior to release as an operational Compromise Notification Message.
Template Recovery Product Service Request: Product Service Request composed in advance of a compromise that requests product necessary to recover from a compromise. The template Compromise Recovery Product Service Request is generally modified by a Controlling Authority prior to release as an operational Compromise Recovery Product Service Request.
Tracking: The KMI function that provides current status (“state”) information about products and requests across the system to KMI users, and events leading to their current state, based on the user’s role and privileges. (Proposed update to KMI Glossary definition from T/C/A study)
Transaction: The sequence of events that transpires from the time cryptographic materials are ordered until they are delivered to the end user or ECU. (Proposed new definition from TCA study)
User: A KMI system entity that accesses KMI products and services.
User Set: A set that consists either (1) entirely of human users or (2) entirely of device users.

Unregistered User: A User that accesses the KMI without invoking a registered identity.
User Authentication: A security service that verifies a User Identity that is claimed by or for a system entity that attempts to access the KMI.
User Device: An automated, client process—a specific hardware unit with specific software running on it—that is registered to act as a KMI User.
User Identity Registration State: A User Identity is in the active state if the identity is currently authorized to be used to access the KMI. Otherwise, the identity is in the inactive state.
User Identity: The collective aspect of a set of attribute values (i.e., characteristics) by which an identity (i.e., a specific individuality) of a KMI User is recognized or known by the KMI and which is sufficient to distinguish that identity (1) from all other identities of that same User and also (2) from all identities of all other Registered Users.
User Number: A KMI-unique value that KMI assigns to a User and that is used in KMI's internal database as an index, label, or short name for associating data elements pertaining to that User.
User Registration Data: The set of attribute values acquired by, and stored and maintained in, the KMI to establish and describe a User.

(U) Acronyms

ADP	Account Distribution Profile
AKP	Advanced Key Processor
BET	Bulk Encrypted Transactions
C2	Command and Control
CDD	Capability Development Document
CFF	Central Facility – Finksburg
ALC	Accounting Legend Code
CI	Capability Increment
CMCS	COMSEC Material Control System
CMI	Cryptographic Modernization Initiative
COI	Community of interest
COMSEC	Communications Security
CONAUTH	Controlling Authority
CONOP	Concept of Operations

COR	Central Office of Records
COTS	Commercial off-the-shelf
CSN	Central Services Node
DAO	Department/Agency/Organization
DDP	Device Distribution Profile
DMD	Data Management Device
DN	Distinguished Name
DoD	Department of Defense
ECU	End Cryptographic Unit
FNBDT	Future Narrowband Digital Terminal
EKMS	Electronic Key Management System
FAQ	Frequently Asked Questions
FD	Fill Device
FOUO	For Official Use Only
GD	General Device
GIG	Global Information Grid
GPS	Global Positioning System
HAIPE	High Assurance Internet Protocol Encryptor
HMI	Human Machine Interface
I&A	Integrity and Authentication
ID	Identifier
INE	In-line Network Encryptor
IOC	Initial Operating Capability
KEK	Key Encryption Key
KLIF	Key Loading and Initialization Facility
KME	Key Management Entity
KMI	Key Management Infrastructure
KOA	KMI Operating Account
KP	Key Processor
KPC	KMI Protected Channel
LD	Limited Device
LE	Local Element
LMD	Local Management Device
LT1RA	Local Type 1Registration Authority

MPMSS	Mission Planning/Management/Support Systems
NFP	Network-Fill Port
NIPRNET	Non-classified Internet Protocol Routing Network
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OME	Ordering and Management Enclave
OTNK	Over the Network Keying
PC	Personal Computer
PDE	Product Delivery Enclave
PKI	Public Key Infrastructure
PIN	Personal Identification Number
POC	Product Ordering Catalog
PSTN	Public Switched Telephone Network
PRSN	Primary Services Node
PSN	Product Source Node
RA	Registration Authority
RFP	Red-Fill Port
RoBAC	Role-Based Access Control
RuBAC	Rule-Based Access Control
SAASM	Selective Availability Anti-Spoof Module
SDRS	System Description And Requirements Specification
SDS	Secure DTD2000 System
SIPRNET	Secret Internet Protocol Routing Network
SKL	Simple Key Loader
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
U	Unclassified
UAS	User Application Software
VPN	Virtual Private Network
WAN	Wide-Area Network
WFP	Wrapped-Fill Port
IAD	Information Assurance Directorate

2774

2775

Appendix A EKMS Transactions

(U) A list of supported EKMS transaction includes; but is not limited to:

- (U) Accounting Transactions
  - (U//FOUO) Conversion Report – Used for communications between COR and client node
  - (U//FOUO) Destruction Report – Used by client node to notify COR of destruction of product
  - (U//FOUO) Generation Report – Used by client node, when centrally accountable material is generated. Report is sent to the COR.
  - (U//FOUO) inventory Report – Used for communications between COR and client node
  - (U//FOUO) Key Conversion Notice – From Tier 1/0 to notify client node that seed FIREFLY key has been converted to operational key.
  - (U//FOUO) Possession Report – Used client node to notify COR of possession.
  - (U//FOUO) Cancel DistrTrans – Used to cancel a transaction. Can be sent from client node to COR, or between client node and LMD.
  - (U//FOUO) relief Accountability Report – Used by a COR to notify a client node of its relief from accountability for an item.
  - (U//FOUO) Tracer Notice – Used when the COR does not receive receipt of product. Can be sent from COR to client node, or between client node and LMD.
  - (U//FOUO) Transfer Report Initiating – Sent from a client node to the element receiving the key, and its COR for centrally-accountable material, giving the details of the shipment.
  - (U//FOUO) Transfer Report Receipt All – Sent from a client node to the COR or between client nodes and LMD to notify receipt of product.
  - (U//FOUO) Transfer Report Receipt Exception - Sent from a client node to the COR or between client nodes and LMD to notify receipt of product.
  - (U//FOUO) Transfer Report Receipt Individual - Sent from a client node to the COR or between client nodes and LMD to notify receipt of product.
  - (U//FOUO) Inventory Reconciliation Status – A list of unreconciled items, sent from the client node to the COR.
  - (U//FOUO) Request Inventory - Sent by a COR to an account or a parent account to a subaccount, requesting an inventory report
  - (U//FOUO) Issue Report Initiating - Sent from a parent account to an automated subaccount when issuing material.
  - (U//FOUO) Issue Report Receipt All – Sent from an automated subaccount to a parent account to receipt for issued key.
  - (U//FOUO) Issue Report Receipt Exception – Sent from an automated subaccount to a parent account to receipt for issued key.

- (U) Distribution Transactions
  - (U//FOUO) Bulk Encrypted TransBody - Used to send multiple encrypted keys
  - (U//FOUO) Key Distribution - Used to send a single encrypted key
- (U) Nonstandard Messages
  - (U//FOUO) FreeForm Text – Free form text between EKMS element and client node, usually in the form of an email.
  - (U//FOUO) Response Trans – The translator must support this transaction for communication between EKMS elements and KMI client nodes.

(U) Detailed information on EKMS transactions can be found in the Volume 1 of the CI-2 SDRS.