# (U) KMI CI-2 Nodal Interface Description

**September 30, 2005**

**Draft Version 1.6**

## INFORMATION ASSURANCE MISSION ATTAINMENT (IAMAC) CONTRACT MDA 904-03-C-1074

**Technical Task Order 2104**

**BAH TTO 2104**

**Prepared By:**

Booz | Allen | Hamilton

**900 Elkridge Landing Road**
**Linthicum, Maryland 21090**

(This Page Left Blank Intentionally)

# (U) REVISION PAGE

(U) This page lists the document versions that have been issued. Requests for changes to this document should be submitted in writing to the KMI Office of Primary Responsibility listed in Section 1.4.

| Date | Version | Description of Changes |
|---|---|---|
| 31 Dec 2004 | 1.5 | First widely distributed working draft. |
| 30 Sep 2005 | 1.6 | Revised to correct technical errors and add ESE. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**FOR OFFICIAL USE ONLY**

# (U) TABLE OF CONTENTS



# (U) TABLE OF FIGURES

# 1 (U) INTRODUCTION

(U) This document provides data flow information for Capability Increment Two (CI-2) of the Key Management Infrastructure (KMI). The intent of CI-2 is to build a foundation for management and electronic distribution of all key management products and services in a general-purpose networking environment.

## 1.1 (U) Purpose

(U) The Nodal Interface Description (NID) describes the interfaces and types of data that move between KMI CI-2 nodes, and between the KMI and external systems. KMI nodes can be widely distributed or collocated within central or regional sites that may be connected by a variety of DoD and commercial communications networks.

(U) Version 1.0 of this document is to be considered as a model for the final version, since significant revisions are to be expected due to design and implementation decisions.

## 1.2 (U) Document Structure

(U) This document is organized into four sections. The following presents a high-level description of each section:

- **Section 1 - Introduction:** This section provides a brief introduction to the KMI CI-2 NID.
- **Section 2 – KMI CI-2 Nodes:** This section presents an overview of the KMI CI-2 nodal architecture.
- **Section 3 – KMI CI-2 Internal Interfaces:** This section provides a description of the data types that traverse the KMI CI-2 nodal interfaces.
- **Section 4 - KMI CI-2 External Interfaces:** This section provides a description of the external systems with which the KMI CI-2 interfaces.

## 1.3 (U) System Overview

(U//FOUO) The KMI CI-2 nodal architecture supports a unified infrastructure that provides key management products and related services to a wide variety of clients operated by KMI Users. KMI Users can be KMI Managers, KOA Agents, or KMI-enabled devices.

- The users are either consumers that depend on the KMI for products and services, or managers that allocate and control resources within the KMI. The KMI CI-2 nodal architecture is presented in Figure 1.1 and includes:The **Central Services Node (CSN)** oversees the security of system operations and stores and replicates common data for PRSNs.

- **Product Source Nodes (PSNs)** are dedicated to generation of various key products.

- **Primary Services Nodes (PRSNs)** are dedicated to key management.
- The **EKMS Translator** facilitates interoperability with the Electronic Key Management System (EKMS).
- **Client Nodes** provide access to the PRSN and include the following:
    - AKP equipped Manager Client Nodes supporting key ordering and management.
    - Delivery-only Client Nodes supporting retrieval of key and KMI products from PRSN PDEs.
    - KMI-Enabled cryptographic devices that are capable of directly retrieving key and KMI products from the PRSN, including seed key conversion and rekey via Over The Network Keying (OTNK).

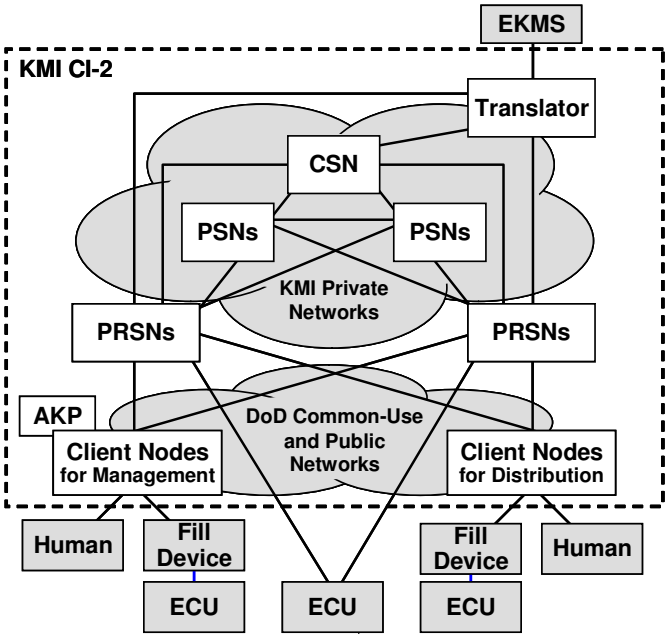
**EKMS TRANSLATOR**
Reenveloping of transactions defined by EKMS standards.

**CENTRAL SERVICES NODE (CSN)**
Catalog management and distribution.
Data archive and analysis center.
Security and operations oversight.

**PRODUCT SOURCE NODES (PSNs)**
Cryptographic material generation.
Product packaging. Product vault.
Rekey. Conversion of seed key.
KMI Naming Authority. Type 1 I&A Certificates. PIN Generation.

**PRIMARY SERVICES NODES (PRSNs)**
User registration, roles, privileges.
Request processing, distribution, tracking.
Customer support. KMI-EKMS interface.

**CLIENT NODES**
Product/service request, retrieval, use.
Product/crypto device management.
Operating account management.




**(U) Figure 1.1: KMI CI-2 System Nodal Architecture**

## 1.4 (U) Office of Primary Responsibility

(U//FOUO) This document is issued by the National Security Agency (NSA) Deputy Director for Information Assurance. Comments on the content should be addressed as follows:

NATIONAL SECURITY AGENCY
STE 6751, KMI PROGRAM MANAGEMENT TEAM
9800 SAVAGE ROAD
FT MEADE, MD 20755-6751

(U//FOUO) For ease of automated mail sorting, the above address should be all upper case and 10-pitch or 12-pitch type.

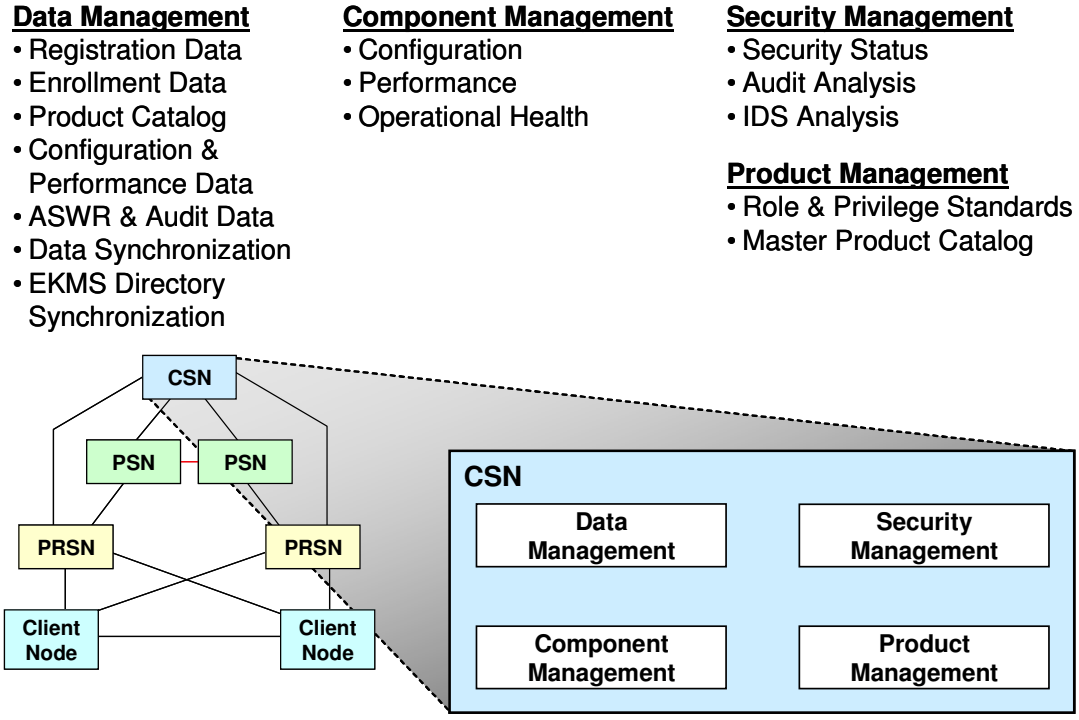
# 2 (U) KMI CI-2 Nodes

## 2.1 (U) Central Services Node (CSN)

(U//FOUO) The CSN oversees the security of system operations and stores and replicates common data for PRSNs. The CSN monitors the system's security state by analyzing state and event information received from the other core nodes, and responses to security incidents affecting multiple nodes are coordinated at the CSN. The CSN manages the KMI Product Ordering Catalog, and provides catalog information to the PRSNs.

(U//FOUO) The CSN maintains archives for data backup, registration, enrollment, tracking, and audit functions. The CSN coordinates the replication of information among PRSNs to support providing equivalent service at multiple PRSNs, and manages the synchronization of KMI information with equivalent data in the EKMS directory service. The CSN is the point of interface between the KMI and the EKMS directory service, and coordinates synchronization of directory information both among the KMI PRSNs and between the KMI and the EKMS.

(U//FOUO) The functions and primary components of the CSN are presented in Figure 2.1.




**(U) Figure 2.1: CSN Functionality**

(U//FOUO) The CI-2 CSN provides management services that ensure functional consistency across all KMI nodes, components, platforms, and sites. The CI-2 CSN is separate from PRSNs and PSNs. CSN functionality is grouped into the following four general categories:

- (U//FOUO) **Data Management**. The CSN supports operations by maintaining databases for important types of data that are handled by the PRSNs and PSNs, including registration and enrollment data, product ordering catalog data, role and privilege data, performance and

ASWR data. The CSN also coordinates the synchronization of information across PRSNs so that a User can receive equivalent service from any PRSN they connect to; this CSN function also include synchronization of KMI data with the equivalent information maintained in the EKMS directory service.

- (U//FOUO) **Security Management**. The CSN provides both operational managers and administrative managers with an overview of security conditions across the KMI, including management of the intrusion detection systems and review of audit trail data.

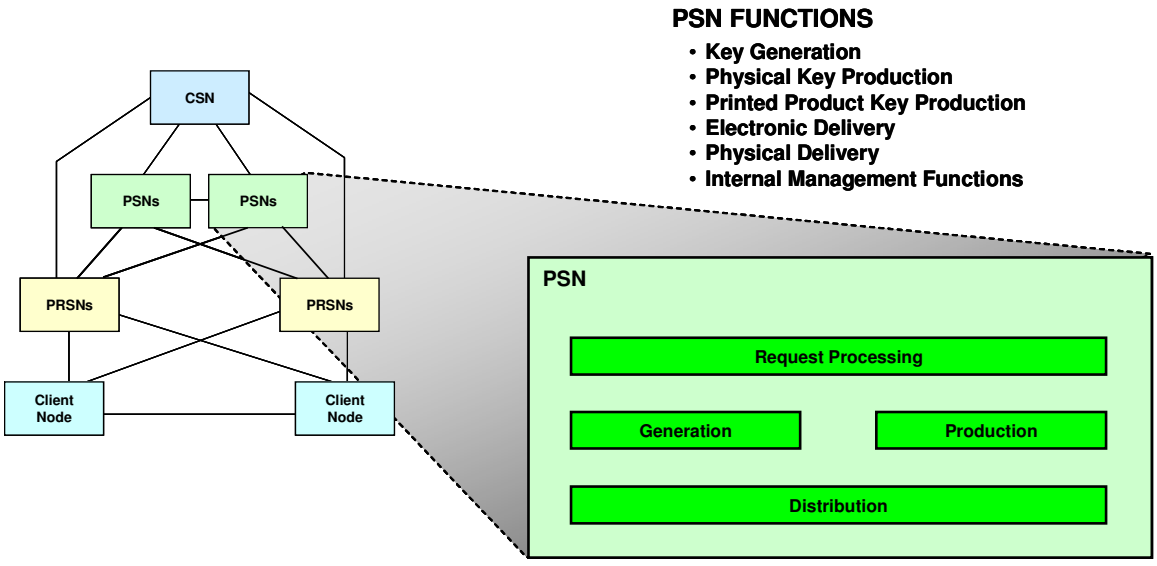
- (U//FOUO) **Component Management**. The CSN performs configuration, performance and system health monitoring functions to support managers in controlling KMI applications, platforms, internal networks and sites.

- (U//FOUO) **Product Management**. The CSN supports the production and delivery of products and services by providing oversight of registration and enrollment processes, setting system role and privilege standards, maintaining the master product catalog and distributing tailored subsets of the catalog to PRSNs.

## 2.2 (U) Product Source Nodes (PSNs)

(U//FOUO) The PSNs generate, format, and package KMI products as directed by orders from PRSNs and according to the specifications of the Product Catalog. CI-2 incorporates PSN capabilities to produce electronic and physical key material in a variety of formats, and also to support Over the Network Keying (OTNK) for future End Cryptographic Units (ECUs). PSNs produce products that range in classification from Unclassified to Top Secret / Special Compartment Information (TS/SCI). However, PSNs connect to PRSNs at the Secret level, and each product package that a PSN delivers to a PRSN is wrapped for the intended consumer device and can be handled as Unclassified.

(U//FOUO) The functions and primary components of the PSN are presented in Figure 2.2.




**(U) Figure 2.3: PSN Functionality**

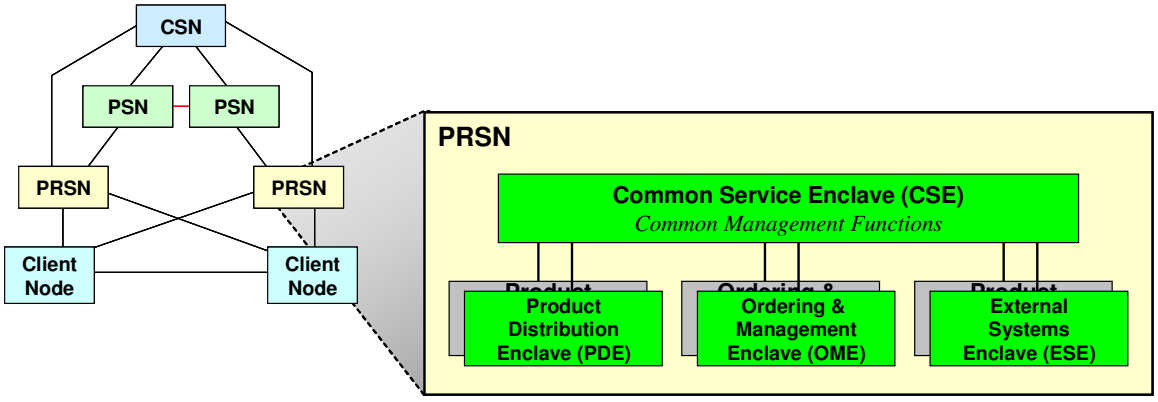
(U//FOUO) PSNs generate and produce cryptographic key material, Type 1 X.509 certificates and other types of credentials. Each PSN supports one or more cryptographic product types. PSNs are modular in structure and make use of existing, updated, and new generation and production capabilities.

(U//FOUO) A PSN receives product or service requests from a PRSN, which provides all relevant information management functions and interfaces associated with the product or service. All keys and products that originate at a PSN for electronic distribution are encrypted for a specific KMI-Aware Device, for a Client Node with an AKP, or for interim storage in the electronic vault before transmission. PSNs never output electronic products in a form that can be unwrapped by anyone other than the intended recipient(s). Products packaged for distribution in this manner will require no special handling as they pass through intermediate components of the KMI.

## 2.3 (U) Primary Services Nodes (PRSN)

(U//FOUO) The PRSNs manage the flow of system events, provide the interfaces for Client Nodes and provide interfaces for communicating with systems external to the KMI. Client Nodes connect to PRSNs via wide-area Transmission Control Protocol/Internet Protocol (TCP/IP) networks, Secret Internet Protocol Router Network (SIPRNet), Unclassified but Sensitive Internet Protocol Router Network (formerly called the Non-secure Internet Protocol Router Net – NIPRNet) and the public Internet. The internal architecture of the PRSN protects the KMI against threats posed by these connections while providing Client Nodes with access to network-based KMI services. PRSNs enable clients to request, receive, and manage KMI products and services for customer organizations. Each PRSN is divided into security enclaves, and each enclave operates at either the Unclassified or the Secret level. The functions and primary components of the PRSN are presented in Figure 2.3.

- Network I/F, Border Protection Suite
- Request Validation Approval
- Event Management
- User Enrollment, Registration
- Role, Privilege Mgmt, Access Control
- PSN Order Negotiation
- PSN Order Fulfillment Coordination
- Status Tracking Requests
- Accounting
- Electronic Key Repository
- PDE Key Locker Management
- Directory, Message Services
- Compromise Recovery Services
- Security-Critical Package Repository
- Real-time Rekey Processing
- PRSN-PRSN Transactions
- External System Interactions
- Local Enclave Maintenance System




**(U) Figure 2.3: PRSN Functionality**

(U//FOUO) PRSNs provide services to Client Nodes over various communications networks. CI-2 is deploying PRSNs that enable users to perform key management functions and to request and receive products and services using web-based technology.

(U//FOUO) A PRSN offers a single point of access to all products, services, and information required by the KMI user community, except for products that are produced locally by AKP-equipped Client Nodes. PRSNs provide product management and distribution services, Device and KOA registration services, User and Manager registration and enrollment services, directory services, support for compromise recovery. Transactions are either processed by a PRSN directly or forwarded to other nodes for processing.

(U//FOUO) PRSNs interface with PSNs to order and receive key products and with the CSN to receive catalog and privileging information, report status and performance data, and provide data necessary to maintain the CSN master databases. Each PRSN also interfaces with other PRSNs to share data, and with external systems (e.g., the DoD Global Directory Services (GDS)) to obtain information necessary for KMI operations. PRSNs are located regionally as necessary to meet requirements for connectivity, availability, survivability and performance.

(U//FOUO) PRSNs are composed of the following:

- **(U//FOUO) Common Services Enclave**. Each PRSN contains a Common Services Enclave (CSE). Within the CSE exist the functions and databases needed to support the PRSN's Ordering and Management Enclaves (OMEs) and Product Distribution Enclaves (PDEs), and to communicate with other KMI core components. The CSE operates as a classified, system high system, and communicates with multiple OMEs and PDEs, which can be either classified or unclassified. The CSE provides connectivity with the External Systems Enclaves (ESEs), CSN and EKMS Translator.

- **(U//FOUO) Ordering and Management Enclave**. KMI Managers connect to an OME to request products and services, or to perform related operational and administrative duties. Each PRSN will have multiple OMEs, which support connections from authorized Managers in a particular user community. Each OME services a specific group of managers, at a specific security level. For instance, one OME may support DoD Classified Managers, while another supports NATO Unclassified Managers – both within a single PRSN. Yet, both OMEs would communicate with and rely upon a single CSE within their PRSN.

- **(U//FOUO) Product Distribution Enclave.** The Client Nodes of KOA Agents, and also user devices that are KMI-aware, connect to PDEs to receive products and services that have previously been ordered or authorized for them by managers. Each PRSN is able to be configured with multiple PDEs. Each PDE operates at a single security level and supports one type of authentication (e.g., Manager credentials, user device FIREFLY credentials, DoD PKI credentials or identifier-password pair). When a KOA Agent or user device logs into a PDE, it is allowed to access and retrieve key material from all KOAs with which it has been registered. For instance, a user may be registered as a KOA Agent with three different KOAs. When that user logs into a PDE, the user will be able to see and retrieve wrapped key directed to all three KOAs.

- (U//FOUO) **External System Enclave (ESEs).** The KMI uses information from some external systems to support its operations. The ESEs implement the functionality needed for the KMI to communicate securely with external systems. For example, to validate DoD X.509 public-key certificates of some KOA Agents who access PDEs, the KMI needs the certificates of DoD PKI certification authorities (CAs), and also needs their certificate revocation lists (CRLs) or access to revocation status services. This may require the ESE to act as a client to access a directory server to get certificates and CRLs, or to access an On-Line Certificate Status Protocol (OCSP) server. Each PRSN is able to configured with multiple ESEs, each used to support interactions with a particular type of external system, at a particular security level.

- **(U//FOUO) Boundary Protection Suite.** Whenever components with different security levels must communicate, a Boundary Protection Suite (BPS) will be employed between the PRSN's Security Zones. For instance, a BPS will be deployed between a PRSN and CSN, and also within the PRSN between the CSE's Common Private Zone, and the OME and PDE Buffer Zones. The BPS is intended to counter generic attacks, such as distributed denial-of- service attacks involving lower-layer protocols.

- **(U//FOUO) KMI Protected Channel**. KMI Clients connect to PRSNs using KMI Protected Channels (KPCs). KMI PRSNs also connect to other PRSNs using KPCs. A KPC is a communications path that provides information integrity, data origin authentication (using a KMI Manager's credentials) or peer entity authentication service, and (in most cases) data confidentiality. The security mechanisms used within a given KPC depend on the channel's purpose and environment. A basic KPC, such as would be used between a coalition KOA Agent and a PDE, may only use web-based encryption between the PRSN PDE and the KMI Client. On the other hand, Managers will add a Type 1 encryptor, such as a HAIPE device, to secure the KPC between the Manager's Client and the PRSN OME. Since the protocols and security features of connections to external systems are typically constrained by the capabilities of those systems, PRSN connections to external system are through KPCs that are specific to the requirements of both the KMI and the external system to which the KMI is connecting.

(U//FOUO) Given the risk inherent in operating in a networked environment, maintaining access control is critical. PRSNs regulate access via role, rule and approval based access control concepts.

## 2.4 (U) Client Nodes

(U//FOUO) Client Nodes enable Human Users to interact with the system through the PRSNs and operate independently of the PRSN for local generation, production, and distribution of symmetric key products. The client architecture is modular, and each Client Node incorporates a computing platform and features that support some set of basic KMI interactions. Manager Client Nodes with an Advanced Key Processor operate in support of a variety of KMI Managers, including Product Managers, KOA Managers, Registration Managers, and Enrollment Managers. Delivery-Only Clients (DOCs) support the retrieval of wrapped products from the PRSN by KOA Agents.

(U//FOUO) Within the KMI, the term "Client Node" refers to any version of a KMI Component that allows Human users to perform KMI Functions. Client Node functionality to support human users is provided by application software executing on various types of computing platforms. Any computing platform supporting such Client Node application software is referred to as a Client Host. There are three major types of Client Nodes. They are:

- Management Client (MGC) - the specific configuration of a Client Host which operates in conjunction with an AKP to perform management of products and services for the KMI (e.g., the KMI equivalent of an LMD/KP).

- Delivery-Only Client (DOC) - a specific configuration of a Client Host that operates without an AKP and is limited to handling wrapped key packages, tracking data, and transport of credentials from KMI-aware devices.

- KMI-Aware Device - a User Device that is registered with the KMI and that can receive products from the KMI that have been wrapped for that specific device (e.g., an AKP or a KMI-aware Device).

(U//FOUO) Wrapped key products can be exchanged between MGCs and existing EKMS LMD/KP workstations. The MGS's AKP can wrap and unwrap black and benign key packages, and it can generate symmetric keys. The AKP architecture is modular, so that capabilities can be included or omitted as necessary to match the needs of a KMI customer's mission. MGCs, in various configurations, support a variety of KMI users, including Controlling Authorities responsible for managing Type 1 products, managers of KMI Operating Accounts, and KMI Registration Managers and Enrollment Managers. KMI Operating Accounts are the KMI representation of COMSEC Accounts.

(U//FOUO) The MGC computing platform running configurable application software support the following functions:

- **(U//FOUO) Identity authentication**. Authenticating the identity of the client user to the PRSN, through the use of the user's KMI credentials or identifier-password pair.

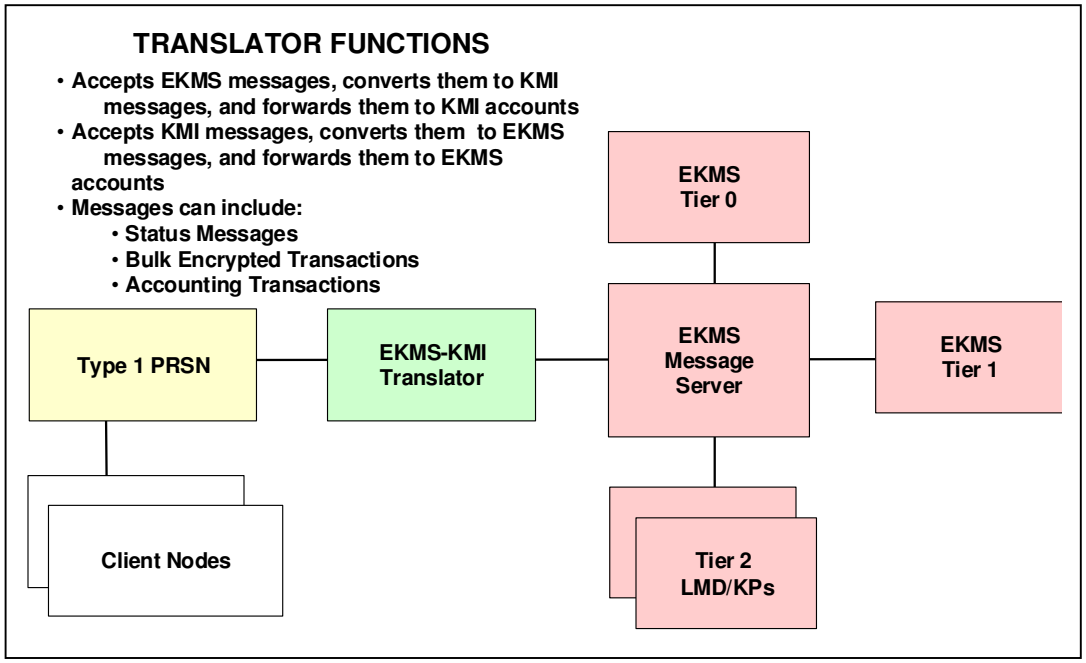
- **(U//FOUO) Data integrity protection**. Protecting transactions submitted from the Client Host to a PRSN, when required, through the use of a digital signature created with a Manager's signature key.

- **(U//FOUO) Data integrity verification**. Checking the integrity of data downloaded to the Client Host from the PRSN, through the verification of digital signatures applied by the PRSN.

## 2.5 (U) EKMS Translator

(U//FOUO) The EKMS Translator (Figure 2.4 below) is the interface between the KMI CI-2 and the EKMS. The purpose of the Translator is to support interoperability between already-fielded EKMS components and CI-2 Clients by supporting required exchanges of accounting transactions, distribution management transactions, Bulk Encrypted Transactions (BET) and formatted plain text messages between KMI and EKMS. The Translator can be seen as a temporary bridge between the KMI CI-2 and the existing EKMS that can be removed from the

KMI when it is no longer required for interoperability with legacy EKMS components. While the Translator is utilized it will provide a mechanism through which the KMI user community can communicate with the EKMS as well as facilitate the transition of EKMS users to KMI.




**(U) Figure 2.5. EKMS Translator Interface**

(U//FOUO) When messages arrive from either the KMI or EKMS, the translator accepts responsibility for the message, re-addresses and re-envelopes the message, and forwards it to the other system. The content of an EKMS message is extracted from the EKMS message envelope format, re-wrapped as a KMI-formatted message, and the recipient's X.400 address is replaced by the recipient's KMI address obtained from the KMI Directory Service. In the same fashion, the content of a KMI message is extracted, rewrapped as a valid EKMS message, and the recipient's KMI address is replaced with the correct EKMS X.400 address.

(U//FOUO) The KMI Directory Service contains the identity information, addresses, and credentials of all KMI and EKMS users and must be made available for use by the Translator. No directory information will be created or modified in the Translator, so it only receives a read-only copy of the current KMI Directory Service information.

(U//FOUO) The connectivity from the translator to the KMI is supported by the PRSN. The PRSN consists of the OME, PDE, and CSE, which provide connectivity to the translator.

The EKMS Translator supports the following system capabilities:

- (U//FOUO) Symmetric key generated and wrapped at EKMS Tier 1 or tier 2 can be sent to KMI for delivery to AKPs or retrieval by authorized KMI Operation Account Agents (KOA). The EKMS message containing the BET is routed to the Translator, where the BET is extracted, reformatted, and forwarded to the KMI PRSN, which then places it into the appropriate PDE for retrieval by a KOA Manager, using a MGC with attached AKP.

- (U//FOUO) Symmetric key generated by a KMI KOA's AKP can be sent to an EKMS LMD/KP by routing it through the Translator, which converts the message to EKMS format for routing and distribution by the EKMS messaging system.

- (U//FOUO) EKMS transactions related to key management and accounting can be sent through the Translator to KOA Managers.

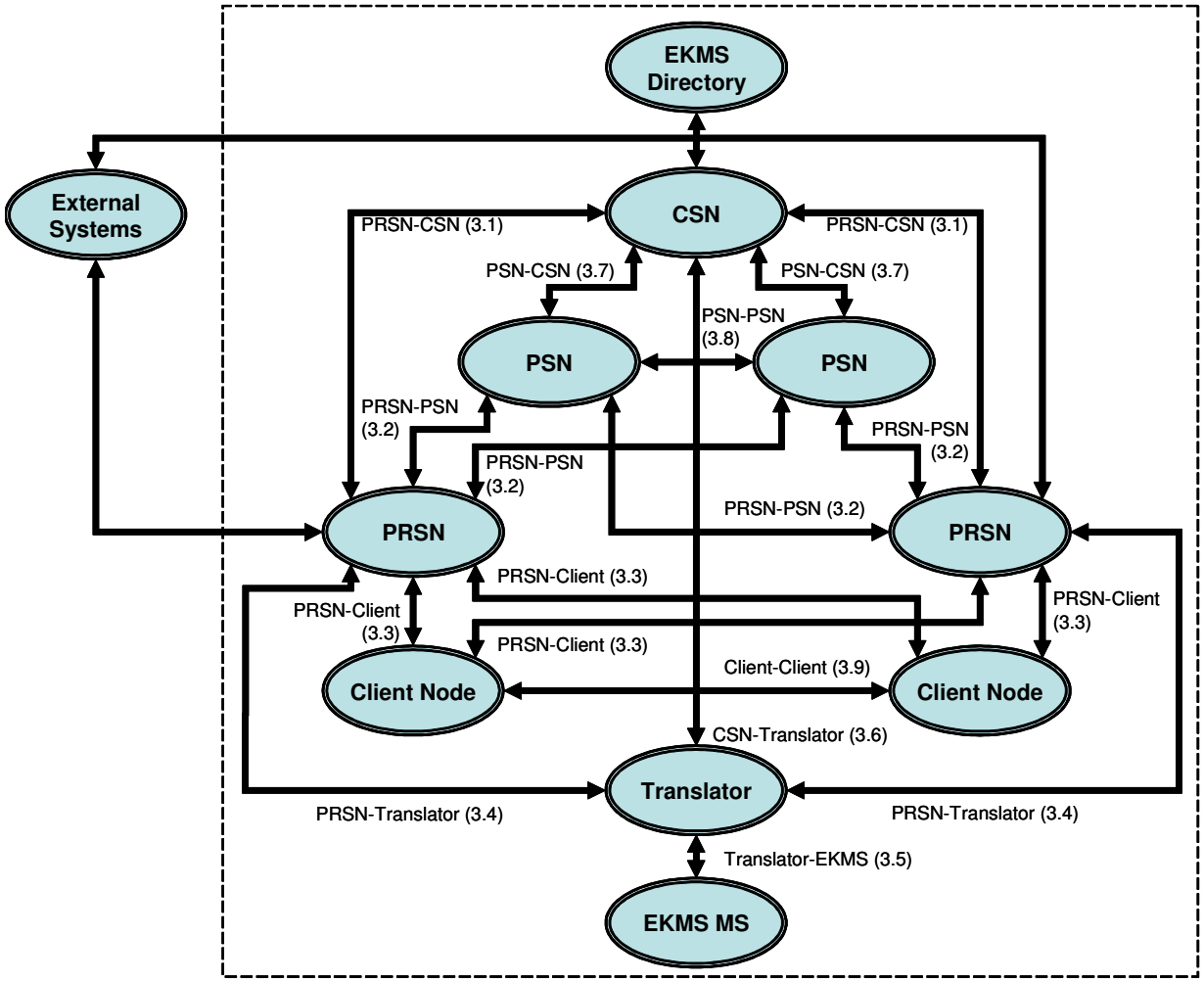
- (U//FOUO) Accounting information generated by KMI components are sent through the Translator to the appropriate Central Office of Record (COR) and/or to EKMS LMD/KPs with which they are involved in a key transfer.

- (U//FOUO) Plaintext messages can be exchanged between KMI Managers and EKMS LMD/KP operators (of like classification level). These messages flow through the Translator, which converts them to the correct format and forwards them to the intended recipients.

- (U//FOUO) KMI audit trail data that is generated by the Translator is maintained at the Translator, and is periodically archived, reduced, and sent to the KMI CSN as required for storage.

# 3 (U) KMI CI-2 Nodal Interfaces

(U//FOUO) The KMI CI-2 will support several node-to-node interfaces. For each of these interfaces a discussion of types of transactions and data that traverse the interface is provided. All transactions that will be exchanged between the Nodes will support source authentication. The nodal to nodal CI-2 interfaces are shown above in Figure 3 include:




**(U) Figure 3. KMI CI-2 Nodal and External Interfaces**

- PRSN-CSN Interface (3.1)
- PRSN-PSN Interfaces (3.2)
  - PRSN–Tier 0 Systems Interface (3.2.1)
  - PRSN–PKI PSN Interface (3.2.2)
  - PRSN–PIN Generator Interface (3.2.3)
- PRSN–Client Node Interfaces (3.3)
  - PRSN OME–Manager Client Node Interface (3.3.1)
  - PRSN PDE–Manager Client Node Interface (3.3.2)
  - PRSN PDE–Delivery-Only Client Node Interface (3.3.3)
  - PRSN PDE–KMI-Aware Device [OTNK] Interface (3.3.4)

- PRSN–Translator Interface (3.4)
- Translator-EKMS Interface (3.5)
- Translator-CSN Interface (3.6)
- CSN-PSN Interface (3.7)
- PSN-PSN Interface (3.8)
- Client-Client Interface (3.9)

## 3.1 (U) PRSN-CSN Interface

(U) The CSN oversees the security of KMI operations and stores and replicates common data for the PRSNs. The CSN is the source of the KMI product and services catalog providing product catalog information to the PRSNs; it is also the source of role and privilege data required by the PRSN both to support enforcement of role-based access control (RoBAC) and to provide Enrollment Managers the current list of system roles. The PRSN-CSN interface supports system backup and restoration services and consolidates security data gathered from other nodes. The types of data that will be exchanged between the CSN and PRSN include Product Catalog Management, Role and Privilege Management, Configuration Management, Registration Data, Enrollment Data, Tracking Data, Attack Sensing Warning and Response, Archive, and Performance Analysis. Appropriate event data and audit records will be generated by the PRSN and forwarded to the CSN for analysis and archival storage.

(U) The VPN employed between the PRSN and CSN is likely to be a COTS VPN product, or a protected circuit if PRSN and CSN are colocated, rather than a Type 1 HAIPE device.

(U) The CSN will act as the hub in a hub-and-spoke replication strategy between KMI PRSNs. Each PRSN will upload local changes to KMI databases to the CSN. Those changes will be applied to the affected databases by the CSN, which will then transmit those changes out to all the other PRSNs.

(U) A description of the data types that traverse the CSN and PRSN interface are found in the table below:

**(U) Table 3.1. PRSN-CSN Interface Data Types**

| Data Type | Description | Data Items |
|---|---|---|
| VPN Session Establishment | The CSN and PRSN exchange VPN session establishment data. The VPN used between PRSN and CSN is likely to be a COTS product instead of Type 1 HAIPE. | The VPN session establishment transaction data includes:<br>• Appropriate Keying for the VPN<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction<br>• Location Information For Each PRSN & VPN |
| Configuration Management | The CSN distributes authorized security configurations/updates | The Configuration Management transaction data includes: |

| (U) Table 3.1. PRSN-CSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| (CSN to PRSN) | and node configurations including the system-wide policy rules for the composition and arrangement of KMI components. | • Policy Rules for Configuration<br>• System-wide Rules for Composition & Arrangement of Components<br>• Authorized Configuration for Nodes<br>• Security Configuration Parameters |
| Network Performance Management<br>(PRSN to CSN) | The CSN gathers network performance information from the PSN and PRSNs and measures internodal network performance. This information is analyzed to determine the baseline for the network and establish thresholds. When a performance threshold is exceeded, an alert is generated and sent to Network Fault Management. | The Performance Analysis transaction data includes:<br>• System State (Health) Data<br>• System Metrics Data<br>• Reduced Audit Data |
| Network Fault Management<br>(PRSN to CSN) | The CSN will detect, log, alert and where possible automatically fix network problems to keep the network running effectively. | The Fault Management transaction data includes:<br>• Network Problem Symptoms<br>• Problem Isolation Data<br>• Possible Problem Resolutions<br>• Solution Testing Data |
| Product Catalog Management<br>(PRSN to CSN)<br>(CSN to PRSN) | The CSN receives incoming transactions from the PRSNs containing updates to products in the Product Catalog.<br>Updates are applied to the Product Catalog and the revised copy is distributed | The Product Catalog transaction data includes but is not limited to:<br>• Product Names (short title additions)<br>• Product Types<br>• Product Classifications<br>• Revisions |
| Role and Privilege Management<br>(CSN to PRSN) | The CSN provides the tools for the Role Manager to create, modify, delete, store and distribute role definitions for use by the Enrollment Manager. | The Role and Privilege Management transaction data includes:<br>• Privilege & Association Definitions<br>• Role Descriptions<br>• Role Name |
| Manager Registration<br>(PRSN to CSN)<br>(CSN to PRSN) | The CSN archives and analyzes registration data that is extracted from the Manager registration process received from the PRSN. | The Registration transaction data for Managers include:<br>• Unique Identity Data<br>  ○ Core Data |

| (U) Table 3.1. PRSN-CSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | New or updated Manager information is provided to the other PRSNs. | ○ Core Name<br>○ Token Type<br>○ Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| KOA Registration<br>(PRSN to CSN)<br>(CSN to PRSN) | The CSN archives and analyzes data that is extracted from the KOA registration process. New or updated KOA information is provided to the other PRSNs. | The Registration transaction data for KOAs include:<br>• Unique Account ID<br>• Associated Identifiers<br>○ Administrative<br>○ Configuration<br>• Account Clearances<br>• Account Address<br>• Registration Date |
| KOA Agent Registration<br>(PRSN to CSN)<br>(CSN to PRSN) | The CSN archives and analyzes registration data that is extracted from the KOA Agent registration process received from the PRSN. New or updated KOA Agent information is provided to the other PRSNs. | The Registration transaction data for Non-Managers include:<br>• Unique Identity Data<br>• Associated Identifier<br>• Associated Authentication Material<br>• Registration Date<br>• Responsible KOA Manager |
| KMI-Aware Device Registration<br>(PRSN to CSN)<br>(CSN to PRSN) | The CSN archives and analyzes data that is extracted from the KMI-Aware Device registration process. New or updated KMI-Aware information is provided to the other PRSNs. | The Registration transaction data for KMI-Aware Devices include:<br>• Unique Identity Data<br>• Associated Identifier with a KOA<br>• Registration Date |
| Enrollment for Managers<br>(PRSN to CSN)<br>(CSN to PRSN) | The CSN receives updates to the enrollment database from the PRSNs. The new or updated enrollment information is then provided to the other PRSNs. | The Enrollment transaction data for Managers include:<br>• Associate Management Role with Registered Manager Identity<br>• Rule-Based Attributes<br>○ Clearance<br>○ Security Category<br>○ National Affiliations<br>○ Organizational Domain |
| Compromise Recovery<br>(PRSN to CSN)<br>(CSN to PRSN) | The PRSNs send data that regarding any certificate or credential related data compromises to the CSN for analysis and archiving. New or | The Compromise Recovery data being exchanged includes:<br>• CKL<br>• CRL<br>• Credential |

| (U) Table 3.1. PRSN-CSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | updated information is sent to the other PRSNs. | |
| Directory Services<br>(PRSN to CSN)<br>(CSN to PRSN) | The PRSNs exchange Directory Services data that need to be retrieved for KMI Users and KMI Nodes. | The Directory Services data being exchanged includes:<br>• Identity information for KMI human users and user devices<br>• Routing information for KOA Managers, AKPs, and EKMS KME accounts<br>• Credentials Associated with KMI Managers, KOAs, KMI-Aware Devices<br>• Role & Privilege<br>• Compromise Data<br>• Revocation information (CRLs and possibly CKLs) |
| Messages<br>(PRSN to CSN)<br>(CSN to PRSN) | Text messages created by Managers and KMI system notifications can be routed through the CSN in order to distribute them to multiple PRSN OMEs, in order to provide them to multiple PRSNs to ensure survivability and availability of service. | The data being exchanged in the text messages and notifications can include:<br>• Product Status<br>• Compromise Notification<br>• Registration<br>• Enrollment<br>• Attack Sensing And Warning Notification<br>• Notification Of Suspended Items or Events<br>• Expired Tokens and/or Certificates |
| Attack Sensing Warning & Response (ASWR)<br>(PRSN to CSN) | The CSN consolidates and merges the data collected from the PRSNs for analysis to provide an overview of the results to the SSO. | The ASWR transaction data includes:<br>• Security Configuration Parameters<br>• Abnormal Activity<br>• IDS Sensor Data |
| Archive and Backup<br>(PRSN to CSN) | The PRSN pushes the requested data to be archived from the CSN. Archive and backup data can either be stored in bulk or placed it on appropriate portable media. | The Archive and Backup transaction data includes:<br>• Registration Data<br>• Privilege Management Data<br>• Help Desk Report Data<br>• System Backup Information<br>• Cryptographic Products & Services |
| Performance Analysis | The CSN reduces and merges | The Performance Analysis |

| (U) Table 3.1. PRSN-CSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| (PRSN to CSN) | data collected from the PRSNs for analysis of the health of the KMI. | transaction data includes:<br>• System State (Health) Data<br>• System Metrics Data<br>• Reduced Audit Data |
| Security Management (PRSN to CSN) | The CSN consolidates and merges the security data collected from the PRSNs for analysis. | The Security Management transaction data includes:<br>• Consolidated ASWR<br>• IDS<br>• Auditable Event |
| Audit (PRSN to CSN) | The CSN reduces and merges security-critical system data collected from the PRSN for analysis and archive, as available. | The data used in an audit collection includes:<br>• Product Generation Data<br>• Delivery Data<br>• Internal Management Functions |

**(U) Table 3.1. PRSN-CSN Interface Data Types**

### 3.2 (U) PRSN-PSN Interfaces

(U) The PSNs generate, format, and package KMI products as directed by requests from PRSNs. Within the CI-2 will be three different types of PSNs. These are:

- Legacy Central Generation Systems – The PRSNs will include an interface to the current Tier 0 systems that produce symmetric and FIREFLY products. Orders from KMI Product Managers and Requestors will flow from the PRSN to this interface, and the requested wrapped key products will flow back through this interface for distribution by the PRSN.

- Type 1 PKI – Registration Authorities will request Type 1 certificates for authorized Managers. Validated requests will flow from the PRSN to the Type 1 PKI, which will generate the required certificates and pass them back to the PRSN for distribution.

- PIN Generator – CI-2 will include a PSN specifically for the generation of Personal Identification Numbers (PINs) and passwords. Whenever a PIN/password is required by the KMI, the PRSN will make the request of the PIN Generator and receive a valid PIN/password. The requested PIN/password can be returned in the clear (for instances such as provisioning KOA Agents who will use only User ID and passwords), wrapped for transmission to a specific entity or loaded onto tokens or Cryptographic Ignition Keys (CIKs).

#### 3.2.1 (U) PRSN–Legacy Central Generation (PSN) Systems Interface

(U) The types of data that will traverse the PRSN-PSN (Legacy Central Generation Systems) interface will include Production Request, Product Generation and Audit Data.

| (U) Table 3.2.1. PRSN-Legacy Central Generation Systems (PSN) Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The PRSN and Tier 0 exchange VPN session establishment data. The VPN implemented between the PSN and the Tier 0 gateway is likely to be COTS rather than a Type 1 HAIPE device. | The VPN session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| Symmetric Production Request (PRSN to PSN) | The PRSN forwards request for symmetric products to be generated by the PSN. | The types of data included in a symmetric product ordering transaction include:<br>• KOA's Client Encryption Credential<br>• Short Title<br>• Product Type<br>• Product Name<br>• Transaction<br>• Status Query |
| Asymmetric Production Request (PRSN to PSN) | The PRSN forwards request for asymmetric (FF & EFF) products to be generated by the PSN. | The types of data included in a symmetric product ordering transaction includes:<br>• Type 1 Credential (of receiving device or delivering AKP)<br>• Product Type<br>• Product Name<br>• Transaction<br>• Status Query |
| Provide Product (PSN to PRSN) | The PSN generates and provides symmetric and asymmetric products from requests sent by the PRSN. | The types of data included in a Product Generation transaction includes:<br>• Product Type<br>• Quantity<br>• Product Name<br>• Transaction<br>• Provisioning Projections<br>• Status Information |
| FIREFLY Rekey/Seed Conversion Request (PRSN to PSN) | The PRSN forwards a FIREFLY Rekey/Seed request to the PSN. | The FIREFLY Rekey/ Seed Conversion Request transaction data includes:<br>• Type 1 Credential<br>• Product Type<br>• Product Name<br>• Status Query |
| FIREFLY Rekey/Seed Conversion Return (PSN to PRSN) | The PRSN receives completed FIREFLY Rekey/Seed conversion from the PSN. | The FIREFLY Rekey/ Seed Conversion Return transaction data includes: |

| (U) Table 3.2.1. PRSN-Legacy Central Generation Systems (PSN) Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | | • FF Key Material<br>• Status Query |
| Tracking<br>(PSN to PRSN) | The PRSN receives tracking and audit data from the PSN to integrate data into status reports for the requesting Manager. | The Tracking and transaction data includes:<br>• Order/Delivery Data<br>o Product Type/Identifier<br>o Product Quantity<br>o Date<br>o Product Requester<br>• Tracking Status Data<br>o Auditable Events<br>o Event ID<br>o Date & Time<br>o Node Performing Event<br>o Transaction ID |

**(U) Table 3.2.1. PRSN-Tier 0Systems Interface Data Types**

### 3.2.2 (U) PRSN–PKI PSN Interface

(U) The Local Type 1 Registration Authority (LT1RA) will request identity certificates for authorized Managers from the PKI PSN. These requests will be routed from the PRSN to the PKI PSN. The resulting certificates will be sent back to the PRSN where they will be placed into the KMI Directory and also provided back to the Registration Manager.

| (U) Table 3.2.2. PRSN-PKI PSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The PRSN and PKI PSN exchange VPN session establishment data. | The VPN session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| Certificate Request | In processing a LT1RA's request for a (pre-registered) User Type 1 identity certificate, the PRSN passes the request (including the public key to be used in creation of the certificate) to the PKI PSN. | The Certificate Request transaction data includes:<br>• Key materials to be used in creating the certificate, wrapped for CA<br>• Registration Authority signature |
| New Certificate | The resulting certificate is sent back to the PRSN, where it is inserted into the KMI Directory and routed back to the requesting Registration Authority,. | The New Certificate transaction data includes:<br>• New Identity Certificate<br>• PKI CA Signature |

**(U) Table 3.2.2. PRSN-PKI PSN Interface Data Types**

### 3.2.3 (U) PRSN–PSN (PIN Generator) Interface

(U) The PIN Generator PSN provides PINs and passwords as requested by the PRSN. If required, it can also wrap a newly generated PIN and password for distribution to a specific entity.

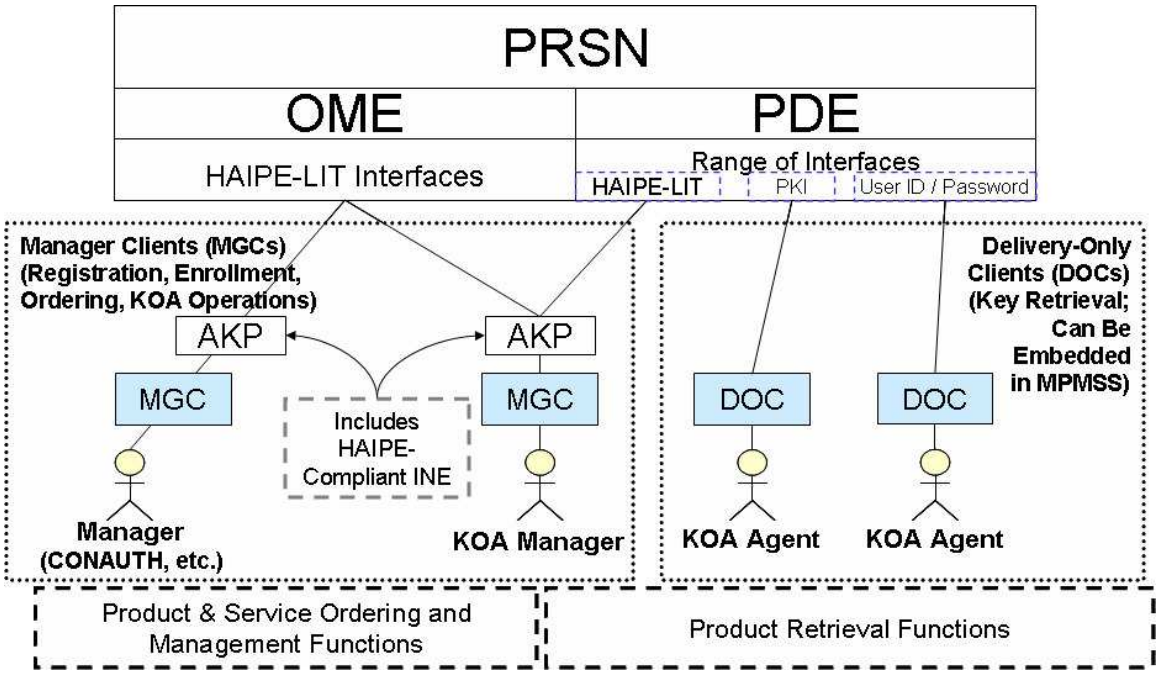
| (U) Table 3.2.3. PRSN-Pin Generator Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The PRSN and PSN (PIN Generator) exchange VPN session establishment data. | The VPN session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| PIN/Password Request | A Manager requests a new PIN or password. The Manager can also request that the PIN/Password be wrapped for receipt by a specific KMI User. | The PIN/Password Request transaction data includes:<br>• Request for PIN or Password<br>• Requesting Manager signature<br>• Identity for which result is to be wrapped (if applies) |
| New PIN/Password | The resulting PIN/Password is sent back to the PRSN, where it is routed back to the requesting Registration Authority. | The New PIN/Password transaction data includes:<br>• New PIN or Password, possibly wrapped for a specific KMI User<br>• PKI PIN Generator Signature |

**(U) Table 3.2.3. PRSN-PIN Generator Interface Data Types**

### 3.3 (U) PRSN-Client Node Interfaces

(U) The PRSNs manage the flow of system events and provide the interface for Client Nodes. Client Nodes connect to PRSNs via wide-area Transmission Control Protocol/Internet Protocol (TCP/IP) networks, SIPRNET, NIPRNET, and the public Internet. The internal architecture of the PRSN protects the KMI against threats posed by these connections while providing Client Nodes with access to network-based KMI services. PRSNs enable clients to request, receive, and manage KMI products and services for customer organizations. There are three interfaces presented in Figure 3.5 that support the PRSN/Client Node interface capability, they include:

- PRSN OME-Manager Client Node supporting key ordering and management.
- PRSN PDE-Manager Client Node supporting delivery of key and key management services.
- PRSN PDE-Delivery-Only Client Node supporting delivery of wrapped key products.
- PRSN PDE-KMI-Aware Device Client Node capable of retrieving wrapped key products or performing Over The Network Keying (OTNK).




**(U) Figure 3.3. PRSN/Client Node Interfaces**

### 3.3.1 (U) PRSN OME-Manager Client Node Interface

(U) Table 3.5.1 describes the types of data that will be exchanged between the OME of the PRSN and the Client Node.

| (U) Table 3.3.1. PRSN OME-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| Session Establishment | The PRSN OME and Client Node exchange TLS or comparable KPC session establishment data. | The Session Establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction<br>• Location Information For Each PRSN & KPC<br>• Directory Synch Messages |
| KMI Client Identification and Authentication | The PRSN OME verifies and validates KMI Client identification data in order to gain access to the PRSN OME. | The data used to identify and authenticate a KMI Client includes:<br>• Type 1 Credential<br>• Access And Privilege Database<br>• Credential Signature<br>• Integrity Signature<br>• Signature Validation Information<br>• KMI Directory<br>• CKL/CRL |
| KOA Registration | The PRSN OME analyzes registration data that is | The Registration transaction data for KOAs include: |

| (U) Table 3.3.1. PRSN OME-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | extracted from the KOA registration process received from the Client. | • Unique Identity Data<br>o Core Data<br>o Core Name<br>o Common Access Card (CAC)<br>o Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| KMI-Aware Device Registration | A Device Registration Manager provides the manufacturer's device information to the PRSN. The PRSN provides a device name and seed key (obtained from PSNs) to be loaded onto the specified device. A copy of the credentialing data is stored on the PRSN. | The Device Registration transaction data for KMI Aware Devices include:<br>• Device Identity Data<br>o Core Data<br>o Core Name<br>o I&A Mechanism Used for KMI-Aware Device<br>o Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| KMI-Aware Device Endorsement | LT1RA provides sponsor and token data to PRSN and requests Type 1 identity. The KMI-aware device has its seed key converted to operational key using OTNK. The device's Identity certificate (obtained from PKI PSN) is associated with sponsor data and stored on the token. | The Endorse Device transaction data for Manager Tokens include:<br>• Device Identity Data<br>o Core Data<br>o Core Name<br>o Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| KMI-Aware Device Activation | The KOA Manager receives a Device and adds it to the local KOA Device Distribution Profile, making it read to be rekeyed. This information is provided to the PRSN. | The Activate Device transaction data includes:<br>• Proof of Device Identity<br>• KOA and KOA Manager Data |
| Manager Token Registration | Device Registration Manager provides the manufacturer's token information to the PRSN. The PRSN provides a token name and seed key (obtained from PSNs) to be | The Register Token transaction data for Manager Tokens include:<br>• Unique Identity Data<br>o Core Data<br>o Core Name<br>o Registration Date<br>• Associated Identifier |

| (U) Table 3.3.1. PRSN OME-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | loaded onto the specified device. A copy of the credentialing data is stored on the PRSN. | • Associated Authentication Material |
| Manager Token Endorsement | LT1RA provides sponsor and token data to PRSN. The token's seed key is converted to operational infrastructure key. The token's Identity certificate (obtained from PKI PSN) is associated with sponsor data and stored on the token. | The Endorse Token transaction data for Manager Tokens include:<br>• Unique Identity Data<br>o Core Data<br>o Core Name<br>o Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| Manager Registration | The PRSN OME analyzes registration data that is extracted from the Manager registration process received from the Client. | The Registration transaction data for Managers include:<br>• Unique Identity Data<br>o Core Data<br>o Core Name<br>o Type 1 Credential<br>o Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| Manager Token Activation (Provisioning) | The Registration Authority provides information verifying the identity of the KMI User and the KMI Manager Token to be activated. The PRSN binds this information together, stores it, and returns the Manager identity credentials to be stored on the token. | The Activate Manager transaction data include:<br>• Manager Identity<br>• Proof of Identity<br>• Token Identity<br>• Sponsor Identity<br>Manager Credentials to be installed on Token |
| Manager Enrollment | The PRSN OME analyzes data from the Client Node that is created during the enrollment process for Managers. | The Enrollment transaction data for Managers include:<br>• Associate Management Role with Registered Manager Identity<br>• Rule-Based Attributes<br>o Clearance<br>o Security Category<br>o National Affiliations<br>o Organizational Domain |
| Non-Manager (KOA Agent) Registration | The PRSN OME analyzes registration data that is | The Registration transaction data for KOA Agents include: |

| (U) Table 3.3.1. PRSN OME-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | extracted from the KOA Agent registration process received from the Client. Note that KOA Agents are a special case, and are granted the role of KOA Agent at time of registration. | • Unique Identity Data<br>o Core Data<br>o Core Name<br>o Username & Password<br>o Registration Date<br>• Associated Identifier<br>• Associated Authentication Material |
| Product Ordering | The PRSN OME verifies and validates KMI Client identification data and product order requests. The exchange of data between these Nodes will be interactive to support the KMI ordering capability. | The Product Ordering transaction data includes:<br>• Type 1 Credential<br>• Product Type<br>• Product Template<br>• Quantity<br>• Role And Privilege |
| Establishment of New Product Requirement for Symmetric Key | The Controlling Authority dialogues with the PRSN, obtaining and updating the product characteristics. The PRSN acknowledges the addition. The Controlling Authority can then Establish an Account Distribution Profile or Authorize Product Requestors. | The Establish New Symmetric Key Product Requirement transaction data includes:<br>• Controlling Authority identity credentials<br>• Role And Privilege<br>• Product Catalog Data<br>• Product Characteristic Data |
| Establishment of Partition/DAO Codes | Command Authority requests product catalog, then supplies partition and DAO codes for a specific product. Optionally, the Command Authority can specify Product Requestors. | The Establish Partition/DAO Codes transaction data includes:<br>• KOA Manager Identity Credential<br>• KMI Manager Identity to be Enrolled as Requestor<br>• Product Catalog Data<br>• Partition and DAO Code Data |
| Establishment of Product Requestor | Controlling Authority requests enrollment of KMI Manager to become a product requestor for a specific product. | The Establish Product Requestor transaction data includes:<br>• KOA Manager Identity Credential<br>• KMI Manager Identity to be Enrolled as Requestor<br>• Product Identitification |
| Account Distribution Profile | The PRSN OME verifies and validates KMI Client identification data and product standing order | The Account Distribution Profile transaction data includes:<br>• Type 1 Credential<br>• Product Type |

| (U) Table 3.3.1. PRSN OME-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | requests or modifications to a standing order. | • Product Template<br>• Quantity<br>• Frequency of Standing Order<br>• Role And Privilege |
| Product Catalog Management-- View Information from OME Product Catalog | The KMI Client can view Product Catalog information based on Manager privileges and attributes. | The data that is transacted in this process includes:<br>• Type 1 Credential<br>• Product Type<br>• Product Template<br>• Role And Privilege |
| Establish Device Distribution Profile (DDP) | The KOA Manager provides information about devices that are to be added to Device Distribution Profiles for specific products. | The Establish DDP transaction includes the following data:<br>• KOA Manager credentials<br>• Product Identifier<br>• Device Identifier |
| Client Software Update | The PRSN OME notifies the KMI Client that updates are available to downloaded. | The data used to conduct software updates includes:<br>• Type 1 Credential<br>• Client Software List<br>• Software Update Log<br>• Privilege Database |
| Messaging | The PRSN OME receives and stores system messages for the KMI Client that can connect to an OME to retrieve, create and respond to messages. | The data used in message transactions includes:<br>• Type 1 Credential<br>• Message Text |
| COMSEC Accounting | The PRSN OME receives accounting transactions required of a KOA that are independent of an electronic product delivery. | The Accounting for Physical Delivery transactions includes:<br>• Inventory Reconciliation<br>• Transfer Reports<br>• Destruction Reports<br>• Possession Reports |

**(U) Table 3.3.1. PRSN OME-Manager Client Node Interface Data Types**

### 3.3.2 (U) PRSN PDE-Manager Client Node Interface

(U) Table 3.3.2 describes the types of data that will be exchanged between the PDE of the PRSN and the MGC.

| (U) Table 3.3.2. PRSN PDE-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| Type 1 Credential Identification and Authentication for KMI | The PRSN PDE receives identification & authentication data from the | The Type 1 Credential Identification and Authentication for KMI Manager transaction data |

| (U) Table 3.3.2. PRSN PDE-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| Managers | KMI Client to verify and validate. The Privilege Database is queried for I&A data status. | includes:<br>• Type 1 Credential<br>• ID Format<br>• Access & Privilege Database<br>• Credential Signature<br>• Signature Validation Information |
| Client Update | The PRSN PDE interrogates Client configuration to determine if it is current. If not, the user may choose to download updated software. | The Client Update transaction data includes:<br>• Client Configuration<br>• Process Configuration<br>• Latest SW Configuration Information<br>• Download Estimates<br>• SW Downloads |
| Interactive/ Web Services: Rekey/Seed Conversion Request | The PRSN PDE provides an interactive capability for the KMI Client to create a rekey/seed conversion transaction request. | The data used to ensure a successful transaction includes:<br>• I&A Mechanism<br>• Role And Privilege<br>• Process Selection (Selection on Interactive Screen)<br>• Forwarded Generated Screen<br>• Key Packages (Labeled with Destination KOA and Device Identities)<br>• Transaction Format |
| Interactive/ Web Services: KOA Folder Request and Receipt | The PRSN PDE authorizes KOA Manager access to queried KOA folders in the PRSN PDE User Access & Privilege Database. | The data used to validate users to the database includes:<br>• I&A Mechanism<br>• Role And Privilege<br>• Community of Interest (COI) Related<br>• Credential<br>• KOA Identifiers<br>• Folder Content |
| Messaging: Receives and Delivers System Generated Messages using Type 1 Credential | The PRSN PDE receives and delivers system-generated messages addressed to KMI Clients. | The data used in this transaction includes:<br>• Type 1 Credential<br>• Messages |
| Key Delivery | The PRSN PDE supports the delivery of key material to a KMI Client. | The Key Delivery transaction data includes:<br>• I&A Mechanism<br>• Product List<br>• Fill Group Profile |

| (U) Table 3.3.2. PRSN PDE-Manager Client Node Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | | • Distribution Profile<br>• Key Material |
| Rekey | The PRSN PDE supports the rekey of a KMI Client. | The Rekey transaction data includes:<br>• I&A Mechanism<br>• PRSN Certificates<br>• Session Key |

**(U) Table 3.3.2. PRSN PDE-Manager Client Node Interface Data Types**

### 3.3.3 (U) PRSN PDE-Delivery-Only Client Interface

(U) Table 3.3.3 describes the data flows between the PDE and the DOC.

| (U) Table 3.3.3. PRSN PDE-Delivery-Only Client Node Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The CSN and PSN exchange VPN session establishment data. | The VPN session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| KMI Authorized Class 3 or 4 Credentials (e.g. CAC) Identification and Authentication for KOA Agents | The PRSN PDE receives identification & authentication data from the KMI Client to verify and validate. The Privilege Database is queried for I&A data status. | The KMI Authorized Class 3 or 4 Credentials Identification and Authentication transaction data includes:<br>• KMI Authorized Class 3 or 4 Credentials<br>• Request Format<br>• Access &Privilege Database<br>• Credential Signature<br>• Signature Validation Information |
| Username/Password Identification and Authentication for Non-Managers | The PRSN PDE receives identification & authentication data from the KMI Client to verify and validate. The Privilege Database is queried for I&A data status. | The Username/Password Identification and Authentication for Non-Manager transaction data includes:<br>• Username/Password<br>• ID Format<br>• Access & Privilege Database<br>• Signature Validation Information |

**(U) Table 3.3.3. PRSN PDE-Delivery-Only Client Node Interface Data Types**

### 3.3.4 (U) PRSN PDE-KMI-Aware Device (OTNK)

(U) Table 3.3.4 describes the types of data that will be exchanged between the PDE of the PRSN and a KMI-Aware Device.

| (U) Table 3.3.4. PRSN PDE-KMI-Aware Device Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| KMI-Aware Device Identification and Authentication | The PRSN PDE receives identification & authentication data from the KMI-Aware Device to verify and validate. The Privilege Database is queried for I&A data status. | The data used in this transaction includes:<br>• I&A Mechanism Used for KMI-Aware Device<br>• ID Format<br>• Access & Privilege Database<br>• Credential Signature<br>• Signature Validation Information |
| Credential Validation | The PRSN PDE verifies the technical correctness, expiration and revocation of credentials supplied by the KMI-Aware Device. | The data used in a credential validation transaction include:<br>• I&A Mechanism Used for KMI-Aware Device<br>• Date<br>• CKL<br>• Trust Path Validation Information |
| Key Delivery | The PRSN PDE supports the delivery of key material to a KMI-Aware Device. | The Key Delivery transaction data includes:<br>• I&A Mechanism Used for KMI-Aware Device<br>• Product List<br>• Fill Group Profile<br>• Distribution Profile<br>• Key Material |
| Seed Key Conversion | A KMI-Aware Device requests conversion of its seed key to operational or infrastructure key. The PRSN passes the request to the GRFE and provides the result to the device. | The Seed Key Conversion transaction data includes:<br>• Device identity<br>• Seed Key<br>• Converted Operational or Infrastructure Key |
| Rekey | The PRSN PDE supports the rekey of a KMI-Aware Device. | The Rekey transaction data includes:<br>• I&A Mechanism Used for KMI-Aware Device<br>• PRSN Certificates<br>• Session Key |

**(U) Table 3.3.4. PRSN PDE-KMI-Aware Device Interface Data Types**

### 3.4 (U) PRSN-Translator Interface

(U//FOUO) To support communications between KMI and EKMS a translator will be used to support the interface. Each system will be responsible for maintaining its own audit data however; the translator will be able to record an audit trail for the exchange of information between the two systems.

(U) The types of data that will traverse the PRSN/Translator/EKMS Message Server (MS) interface include Distribution Management, Text Messages, Accounting and Bulk Encrypted Transaction Data.

| (U) Table 3.4. PRSN-Translator Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The PRSN and Translator exchange VPN session establishment data. | The VPN session establishment transaction data includes:<br>• Appropriate Keying For The VPN<br>• Connection Request<br>• Location Information For Each PRSN & VPN |
| KMI Sends Formatted Message To EKMS MS | The PRSN sends the Translator a signed transaction, validates the source, strips header information, checks directory for recipient address, repackage transaction in X.400 and sends it to the EKMS MS and an event record is generated. | The KMI Sends Formatted Message To EKMS MS transaction data includes:<br>• KMI Formatted Transaction (Appendix A)<br>• Sender Identity<br>• Recipient Identity<br>• Message Data<br>• Signature |
| Tracking Data | Tracking events will be collected, formatted, signed and provided to the PRSN CSE through the PRSN VPN interface from the translator. | The Tracking Data transaction data includes:<br>• Sender Identity<br>• Recipient Identity<br>• Message Identifier |

**(U) Table 3.4. PRSN-PKI PSN Interface Data Types**

### 3.5 (U) Translator-EKMS Interface

U//FOUO) To support communications between KMI and EKMS a translator will be used to support the interface. Each system will be responsible for maintaining its own audit data however; the translator will be able to record an audit trail for the exchange of information between the two systems.

(U) The types of data that will traverse the PRSN/Translator/EKMS Message Server (MS) interface include Distribution Management, Text Messages, Accounting and Bulk Encrypted Transaction Data.

| (U) Table 3.5. Translator-EKMS Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| EKMS Session Establishment | The EKMS and Translator establish a secure session using Type 1 link encryption. | The VPN session establishment transaction data includes:<br>• Appropriate Keying For the Session<br>• Connection Request |
| EKMS MS Sends Formatted Message To KMI | The EKMS MS sends an EKMS transaction to the Translator, the directory checks for recipient address, the transaction's protocol is converted to KMI format, and an event record is generated. | The EKMS MS Sends Formatted Message To KMI transaction data includes:<br>• EKMS X.400 Formatted Message<br>• Sender Identity<br>• Recipient Identity<br>• Message Data<br>• Signature |
| Tracking Data | Tracking events will be collected, formatted, signed and provided to the PRSN CSE through the PRSN VPN interface from the translator. | The Tracking Data transaction data includes:<br>• Sender Identity<br>• Recipient Identity<br>• Message Identifier |

**(U) Table 3.5 Translator-EKMS Interface Data Types**

### 3.6 (U) Translator-CSN Interface

(U) The EKMS Translator will provide Audit, Security Management, and Performance Management information to the CSN for analysis and archiving. The VPN employed between the Translator and the CSN is likely to be a COTS product rather than Type 1 HAIPE.

| (U) Table 3.6. Translator-CSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The CSN and PSN exchange VPN session establishment data. | The VPN session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| Configuration Management (CSN to Translator) | The CSN establishes and manages authorized nodal configurations including the policy rules for the composition and arrangement of components. | The Configuration Management transaction data includes:<br>• Policy Rules for Configuration<br>• System-wide Rules for Composition & Arrangement of Components |
| Audit (Translator to CSN) | The CSN reduces and merges security-critical system data collected from the PSN for | The data used in an audit collection includes:<br>• Product Generation Data |

| (U) Table 3.6. Translator-CSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | analysis and archive, as available. | • Delivery Data<br>• Internal Management Functions |
| Security Management (Translator to CSN) | The CSN consolidates and merges the security data collected from the PSNs for analysis, as available. | The Security Management transaction data includes:<br>• Security Configuration Parameters<br>• Consolidated ASWR<br>• IDS |
| Performance Management (Translator to CSN) | The CSN reduces and merges data collected from the PSNs for analysis of the health of the KMI. | The Performance Analysis transaction data includes:<br>• System State (Health) Data<br>• System Metrics Data |

**(U) Table 3.6. Translator-CSN Interface Data Types**

### 3.7 (U) CSN-PSN Interface

(U) The CSN provides configuration management
the KMI Product Catalog and provides catalog information to the PSN as required for the production of products.

| (U) Table 3.7. CSN-PSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The CSN and PSN exchange VPN session establishment data. It is likely that this will use COTS VPN technology instead of Type 1 HAIPE devices. | The VPN session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| Configuration Management (CSN to PSN) | The CSN establishes and manages authorized nodal configurations including the policy rules for the composition and arrangement of components. | The Configuration Management transaction data includes:<br>• Policy Rules for Configuration<br>• System-wide Rules for Composition & Arrangement of Components |
| Audit (PSN to CSN) | The CSN reduces and merges security-critical system data collected from the PSN for analysis and archive, as available. | The data used in an audit collection includes:<br>• Product Generation Data<br>• Delivery Data<br>• Internal Management Functions |
| Security Management (PSN to CSN) | The CSN consolidates and merges the security data collected from the PSNs for analysis, as | The Security Management transaction data includes:<br>• Security Configuration |

| (U) Table 3.7. CSN-PSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | available. | Parameters<br>• Consolidated ASWR<br>• IDS |
| Performance Management (PSN to CSN) | The CSN reduces and merges data collected from the PSNs for analysis of the health of the KMI. | The Performance Analysis transaction data includes:<br>• System State (Health) Data<br>• System Metrics Data |

**(U) Table 3.7. CSN-PSN Interface Data Types**

## 3.8 (U) PSN-PSN Interface

(U) The Tier 0 key generation systems (e.g., PSNs) currently share specific historical transaction information with each other, to facilitate load balancing and other operational requirements. Details of these transactions is not available at present, but notation is being made in order to ensure completeness.

| (U) Table 3.8. PSN-PSN Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| VPN Session Establishment | The Tier 0 PSNs will establish a secured connection, either by use of a VPN or by link encryptors. | The VPN/link session establishment transaction data includes:<br>• Connection Request<br>• Transaction Package<br>• Signed Transaction |
| PSN Historical Data | Historical transaction and state data is shared amongst PSN systems, format and specifics TBSL. | TBSL. |

**(U) Table 3.8. CSN-PSN Interface Data Types**

## 3.9 (U) Client-Client Interface

(U) KMI Client Nodes will be able to communicate directly with each other in order to facilitate local key management in environments where reach-back to the KMI infrastructure may be intermittent or unavailable. Client-client interfaces will be simple peer-to-peer connections over TCP/IP networks or via dial-up. Link encryption will be used on this connection to to prove the identity of the remote client prior to establishing a connection and to prevent unauthorized disclosure of data.

| (U) Table 3.9. Client-Client Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| Session Establishment | The KOA manager's client establishes a connection with another client using a protocol | Session establishment will require the exchange of information such as: |

| (U) Table 3.9. Client-Client Interface Data Types | | |
|---|---|---|
| **Data Type** | **Description** | **Data Items** |
| | such as PPP or SLIP, based on pre-existing addressing and configuration information. | • Connection Request and Response<br>• Identity Credentials<br>• Cooperatively Generated Session Key |
| Send Bulk Encrypted Transaction | A KOA Manager will create a BET, encrypted for the remote client's AKP (or possibly KP) and will send that BET over the active session. | TBSL. |
| Receive Bulk Encrypted Transaction | A KOA Manager will receive a BET sent by a remote KOA Manager, and store the BET on the manager's client node for future use. | TBSL. |
| Acknowledge Receipt | When the receiving KOA Manager unpacks the BET, and acknowledgement is sent back to the sending KOA Manager. This may be stored and shipped when connectivity exists. | TBSL. |
| Query for Receipt | A KOA Manager can query a remote KOA manager for the status of BETs transmitted. | TBSL. |

**(U) Table 3.9. Client-Client Interface Data Types**

# 4 (U) KMI CI-2 Interfaces to External Systems

(U//FOUO) The KMI CI-2 will interface with several external systems. These systems may include:

- Defense Courier Service (DCS)
- External Directory Systems
  - Global Directory System (GDS)
  - Foreign Directories
- DoD PKI
- Incident Reporting Center
- Helpdesk

(U//FOUO) The KMI will interface to these systems via a PRSN External Systems Enclave (ESE). A specific configuration of ESE will be created and deployed to interface with each of these external systems. The interface specification for each must be defined for each specific system with which the KMI must interoperate.

## 4.1 (U) Defense Courier Service Interface

(U) The KMI will interface with Defense Courier Service (DCS) to support physical delivery of products. The products are requested through CI-2 and directed into DCS for delivery. Product Managers will be allowed to query the DCS for tracking data regarding the delivery status of physical material.

## 4.2 (U) Directory Interfaces

(U) The directory interfaces supported by the CI-2 include both the DoD Global Directory System (GDS) and the Foreign Directories.

### 4.2.1 (U) CI-2 to Global Directory System Interface

(U) The KMI will rely on the DoD GDS for making certificate related information (e.g. CRL) available to the KMI CI-2 user community for certificate validation.

### 4.2.2 (U) Foreign Directories

(U) The KMI will interface with Foreign Directories to receive selected user certificate related information (e.g. CRLs) to support communications with foreign users.

## 4.3 (U) DoD PKI Interface

(U) This interface is TBD.

## 4.4 (U) Incident Reporting Center Interface

(U//FOUO) The KMI will manage, monitor, assess, and report information on attacks mounted against it at both the PRSNs and CSN. When such incidents occur, they will be reported to a DoD IA Incident and Response System via telephone, messaging or e-mail, or other communications methods. At present, no automated interface with the KMI CI-2 is planned.

# Appendix A - EKMS Transactions Supported by KMI CI-2

(U//FOUO) The interface between the EKMS Message Server and KMI CI-2 Translator will support the following:

- Required exchanges of accounting transactions, distribution management transactions, electronic key packages and formatted plain text messages between KMI and EKMS.
- Provides a mechanism through which the KMI user community can communicate with the EKMS.
- Facilitates the transition of EKMS users to KMI CI-2

(U//FOUO) Table A includes the EKMS transactions that are supported by CI-2 and traverse the interface between the EKMS Message Server and Translator.

**(U) Table A. EKMS Transactions Supported by KMI CI-2**

| EKMS Formatted Transactions | Description |
|---|---|
| EKMS Formatted Transaction: Conversion Report | Describes change in item identifiers or ALC for equipment & key/aids. |
| EKMS Formatted Transaction: Destruction Report | Sent by a COMSEC Account to its COR to notify of destruction of an accountable item. |
| EKMS Formatted Transaction: Generation Report | Sent by a generating element to its COR when centrally accountable material is generated, or by a sub account to its parent for all ALC 6 or 7 material. |
| EKMS Formatted Transaction: Inventory Report | Sent by a COMSEC Account to its COR to notify of current holdings as believed by the Account; sent by a COR to an Account to notify of current holdings as believed by the COR. |
| EKMS Formatted Transaction: Key Conversion Notice | From CFF (or Tier 1) to COMSEC Accounts notifying of FIREFLY 9+ seed key converted to operational key and initial rekey of operational key. |
| EKMS Formatted Transaction: Possession Report | From a COMSEC Account to its COR notifying of unexpected possession of material; also can be used COR to COR. |
| EKMS Formatted Transaction: Cancel Distribution Transaction | Used to cancel a Transfer/Transfer Report Initiating for centrally accountable material. |
| EKMS Formatted Transaction: Relief | From a COR to a COMSEC Account notifying it of relief from accountability for an |

| | |
|---|---|
| Accountability Report | item (e.g., following an investigation). |
| EKMS Formatted Transaction: Tracer Notice | Sent subsequent to a Transfer Report Initiating when no receipt is received. Sent from sender of key (COR where appropriate) to the key recipient. |
| EKMS Formatted Transaction: Transfer Report Initiating | From an element shipping a key to the element receiving the key, and its COR for centrally-accountable material, giving the details of the shipment. Also referred to as the Advance Shipping Notice. |
| EKMS Formatted Transaction: Transfer Report Receipt | Mechanisms for a key recipient to receipt for received key shipments. Sent from the key recipient to the sender of key (or COR where appropriate). |
| EKMS Formatted Transaction: Inventory Reconciliation Status | Refers to an initial Inventory Report: list of all unreconciled items, sent from the recipient of an Inventory Report to the sender of the Inventory Report. |
| EKMS Formatted Transaction: Request Inventory | Sent by a COR to an account or a parent account to a sub account, requesting an Inventory Report. |
| EKMS Formatted Transaction: Bulk Encrypted Transaction Body | Used to send multiple encrypted keys; can be created by an LMD/KP, CFF, CFFM, and Tier 1. |
| EKMS Formatted Transaction: Free Form Text | From any EKMS element to any other, EKMS e-mail. |