# TECHNICAL REPORT

# KMI 2200: (U) SYSTEM DESCRIPTION AND REQUIREMENTS SPECIFICATION FOR KEY MANAGEMENT INFRASTRUCTURE (KMI) CAPABILITY INCREMENT 2 (CI-2)

## VOLUME 3:
## (U) SYSTEM SECURITY ARCHITECTURE AND RELATED REQUIREMENTS

**VERSION 2.x**
**DRAFT**

**E001**

**TECHNICAL TASK ORDER 2086**

***INFORMATION ASSURANCE MISSION ATTAINMENT (IAMAC) CONTRACT***

**MDA904-03-C-1074**

Booz | Allen | Hamilton

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

**20 May 2005**

(This Page Left Blank Intentionally)

**KEY MANAGEMENT INFRASTRUCTURE**

**20 May 2005**
**Version 2.x**
**DRAFT**

# KMI 2200: (U) System Description and Requirements Specification for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)

## Volume 3: (U) System Security Architecture and Related Requirements

(U) This document specifies defense-in-depth for system components and for secure connections between those components; and also specifies role-based, rule-based, and approval-based access control processes.

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

# (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 Office of Primary Responsibility that is identified in Section 1.5.

| Date | Version | Description of Changes |
|---|---|---|
| 4 Oct 2002 | 0.1 | CI-2 Security Architecture Outline – CI-1 Baseline |
| 17 Apr 2003 | 0.2 | Includes material from Section 2.5, "Security Architecture", of KMI 2200/2212. Done except for Sections 4.3-4.5. |
| 25 Apr 2003 | 0.3 | Complete except for Section 5. |
| 2 May 2003 | 0.4 | First complete draft; "near final". |
| 24 Oct 2003 | 0.7 | Major revision: Incorporates existing Role-Based Access Control specification from [KMI2200V2]. Provides new Rule-Based Access Control and new Approval-Based Access Control sections. Issued to support "SRS B". Version # skips from 0.4 to 0.7 in order to synchronize with [KMI2200V2]. |
| 6 Nov 2003 | 0.71 | Released as part of "SRS B". |
| 19 Dec 2003 | 1.0 | Released as part of "SRS C". |
| 30 Sep 2004 | 1.1 | Final draft for "SRS D". |
| 30 Dec 2004 | 1.2 | Final draft of "SRS E" |
| 28 Feb 2005 | 1.25 | Final draft of "SRS F"; update to complete implementation of comments against "SRS D". Submitted as change proposals |
| 11 Apr 2005 | 1.26 | Incorporates results of processing change proposals for version 1.25 and clears change markings. |
| 15 Apr 2005 | 2.0 | Updated draft for community release. |
| TBD 2005 | 2.x | TBD |

# (U) TABLE OF CONTENTS

# (U) TABLE OF FIGURES

# (U) TABLE OF TABLES

(This Page Left Blank Intentionally)

# 1 (U) INTRODUCTION

(U//FOUO) This document is Volume 3 of the three-volume, system-level *Description and Requirements Specification* for Capability Increment 2 (CI-2) of the Key Management Infrastructure (KMI).

- (U//FOUO) Volume 1, *Key Management Functions and Related Requirements*, provides an overall system description and specifies key management requirements. [KMI2200V1]
- (U//FOUO) Volume 2, *System Security Policy and Related Requirements*, states system-wide security policies and specifies requirements for security services.
- (U//FOUO) Volume 3, *System Security Architecture and Related Requirements*, specifies the security architecture for the KMI as a whole and for each of its nodes. [KMI2200V3]

(U//FOUO) For the purposes of these documents, the KMI is defined as follows:

> **DEFINITION** (U//FOUO) Key Management Infrastructure. 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.

## 1.1 (U) Purpose

(U//FOUO) An introduction to the system is provided in the KMI *Concept* document [KMI1001]. The system is being implemented in phases called capability increments, as described in the KMI *Roadmap* document [KMI1011]. Each increment will provide new and evolving key management capabilities and services, as well as updates or enhancements to existing key management systems. This volume, in combination with Volume 2, describes and specifies a security framework for the design, implementation, and operation of components that are implemented as part of Capability Increment 2 (CI-2), and is intended to be the basis for later increments.

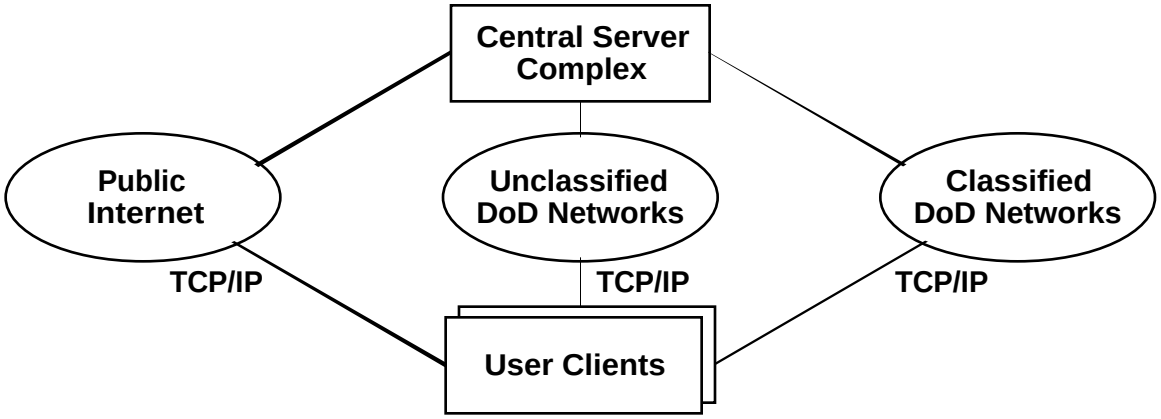
(U//FOUO) A security architecture is a plan and set of principles that describe (A) the security services that a system is required to provide to meet the needs of its users, (B) the system components required to implement the services, and (C) the performance levels required in the components to deal with the threat environment. For CI-2, part A is specified mostly in Volume 2. Part B is specified mostly in this document, which describes how the major components of KMI are structurally organized and protected. Part C is specified partly in this document and partly in Volumes 1 and 2.

## 1.2 (U) Client-Server View

(U//FOUO) This document presents the CI-2 security architecture in a series of progressively more detailed views. In the most general view, illustrated by Figure 1, the KMI is designed to be a distributed, client-server system in which users operate clients to obtain products and services from centralized servers. The KMI program seeks to integrate the set of existing and emerging

systems for producing and managing cryptographic material, and create a single, network-based, client-server infrastructure for ordering and delivering cryptographic products and services. (An overview of the KMI mission, general architecture, and interfaces is provided in [KMI1001].)

**Figure 1. (U) KMI Client-Server View**




**UNCLASSIFIED//FOUO**

(U//FOUO) KMI client nodes connect to the servers across the Public Internet and other Department of Defense (DoD) common-use data networks that also are based on the Internet protocol suite (which is commonly referred to as "TCP/IP"). The servers provide products and services only to registered users.

## 1.3 (U) General Terminology

(U//FOUO) This document uses the following terms to describe and specify the parts of the KMI system. These terms, and additional terms that are defined in this volume and in Volumes 1 and 2, are written with initial capital letters when used in a formal sense, i.e., in **POLICY** statements, in requirement statements, and in other **DEFINITION** statements.

**DEFINITION** (U//FOUO) System Entity. An active element—i.e., either (1) a person or (2) set of persons, or (3) an automated device or (4) set of devices—that is part of either the KMI or the KMI's environment and that incorporates some specific set of capabilities.

**DEFINITION** (U//FOUO) System Resource. Information held in the system, or a service or product provided by the system; or a system capability (e.g., processing power or communication bandwidth); or an item of equipment (i.e., hardware, firmware, software, or documentation); or a facility that houses those things.

**DEFINITION** (U//FOUO) 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 other parts.

**DEFINITION** (U//FOUO) Computer Platform. A combination of computer hardware and an operating system (consisting of software, firmware, or both) for that hardware, that supports automated KMI functions.

**DEFINITION** (U//FOUO) Site. A facility—i.e., a physical space, room, or building together with its physical, personnel, administrative, and other safeguards—in which (1) KMI functions are performed and (2) KMI Components might be housed.

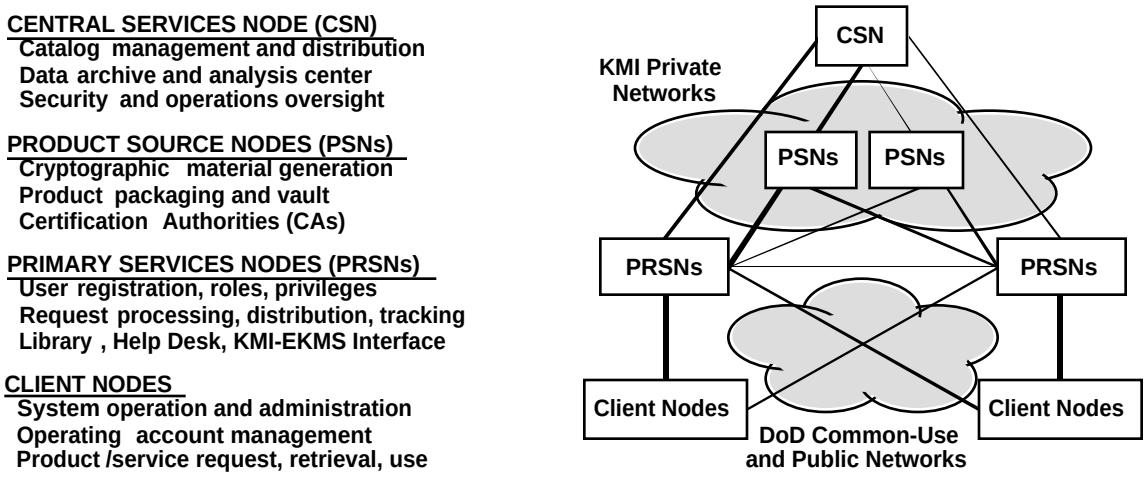
(U//FOUO) The term "component" may be used at more than one level of abstraction, so that components may be nested within each other. In requirement statements that follow in this document, the specific interpretation of "component" depends on the context in which the term is used and the way in which a requirement is implemented.

**DEFINITION** (U//FOUO) Independent Component. A Component that has a defined security perimeter at which, or within which, the Component is responsible for some set of Security Services.

## 1.4 (U) Nodal Goal Architecture

(U//FOUO) This *Security Architecture* takes advantage of the distributed nature of the KMI to enhance protection through separation and independence of components. Figure 2 illustrates that the KMI is a client-server system in which Client Nodes connect to a server complex that includes three other types of nodes: Primary Services Nodes (PRSNs), Product Source Nodes (PSNs), and the Central Services Node (CSN).

**Figure 2. (U) KMI Nodal Architecture**




**UNCLASSIFIED//FOUO**

**DEFINITION** (U//FOUO) Node. A collection of related Components that is (1) located on one or more Computer Platforms at a single Site.

**DEFINITION** (U//FOUO) Core Nodes. The set of Nodes that includes (1) the CSN, (2) all PSNs, (3) all PRSNs, and (4) all Client Nodes that serve Managers playing Internal Management Roles (see "Management Roles" section).

**DEFINITION** (U//FOUO) Client Node (abbreviated as Client). A set of hardware and software with computing and cryptographic capabilities that enable a registered Human User or User Device to obtain products and services.

(U//FOUO) Client Nodes enable users to request and use KMI products and services and to perform operational and administrative management functions. Some clients enable users to obtain products and services from remote PRSNs via a communications network, and some Client Nodes can provide products and services locally.

## 1.5 (U) Office of Primary Responsibility

(U//FOUO) This document is issued by the National Security Agency (NSA) Deputy Director for Information Assurance. Questions about content or interpretation, and requests for changes, should be addressed as follows:

NATIONAL SECURITY AGENCY
CODE I56, KMI PROGRAM MANAGEMENT TEAM
9899 SAVAGE ROAD
FT MEADE MD 20755

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

## 1.6 (U) Requirement Statements

(U) Requirement statements in this volume have a label of the form "**CI2-SAR-1.2.3a**", where "**SAR**" identifies the requirement as a security architecture requirement, and the "**1.2.3a**" is number of the section containing the statement, and a unique identifying letter for the requirement within in the section.

(U) Most of the requirement statements are expected to cause incorporation of specific technical functionality (i.e., hardware or software features) in one or more types of KMI nodes. However, some of the statements either are expected to be satisfied by other, non-technical means or apply very broadly to the system; and those requirements have the suffix "**NT**" (non-technical) on their labels.

(U) A requirement statement normally is followed by either the number of the matching item in the KMI Requirements Database (KRD) (e.g., "[KRD 0001]") or the numbers of items from which the statement has been derived (e.g., "[DRV KRD 1001, 1002]").

(U) This volume includes some requirements that do not apply to CI-2, and each of those has the phrase "Not applicable to CI-2" immediately following its label. These requirements are included to make developers aware of future intentions, so that if the developers have a choice of alternative implementation approaches of nearly equal cost, the developers will be encouraged to choose the alternative that would make it easiest to add the intended capabilities later.

(U) Finally, a requirement statement is followed by a one or more letters in curly brackets, to indicate the main component types to which the requirement is allocated:

- {A} Advanced Key Processor.
- {C} Client Node.
- {P} Product Source Node.
- {R} Primary Services Node.
- {S} Central Services Node.
- {T} EKMS Translator.
- {Z} Allocated to all of the components above.
- {X} Not allocated, because not assigned to CI-2 or not applicable in some other way.

## 1.7 (U) Key Words in Requirements

(U) The key words **required**, **shall**, **shall not**, **may**, and **optional** are to be interpreted as follows when they appear in a requirement statement:

- (U) **Shall** and **required**. These words mean that the statement is an absolute mandate.
- (U) **Shall not.** This phrase means that the statement is an absolute prohibition.
- (U) **May** or **Optional.** These words means that compliance with the statement is optional.

## 1.8 (U) Organization of this Volume

(U) The remainder of this volume consists of the following sections:

- (U) **2. Protection Strategy**, offers reasoning to support the claim that the presented architecture provides adequate protection for the KMI system and its products and services.
- (U) **3. Architectural Concepts**, provides additional rationale for the assignment of security functions to the components of the nodal architecture.
- (U) **4. Nodal Security Architecture,** presents structural requirements for KMI security by decomposing the system in a series of progressively more detailed views.
- (U) **5. Access Control**, presents requirements for role-based, rule-based, and approval-based access control processes.
- (U) **6. Distributed, Two-Level Subsystems**, presents a model for implementing certain system-wide, internal, security service functions.
- (U) **7. Glossary of Acronyms**. (See additional definitions in [KMI2211])
- (U) **8. Glossary of Terms**. Terms for which this volume has DEFINITION statements.
- (U) **9. References**.

(This Page Left Blank Intentionally)

# 2 (U) PROTECTION STRATEGY

(U//FOUO) The CI-2 security architecture provides administrative security, communication security, computer security, emanations security, personnel security, and physical security to protect the KMI against both intentional, intelligent threats and accidental kinds of threats. This section offers reasoning to support the claim that the described security architecture provides adequate protection for the system and its products and services.

## 2.1 (U) Risk Management

(U//FOUO) The CI-2 security architecture is based not only on security objectives derived from National and DoD policies (see Volume 2), but also on a risk management process. Risk management is concerned with identification, measurement, control, and minimization of security risks in information systems, to a level commensurate with the value of the system resources that require protection [CNSSI4009].

(U//FOUO) The KMI threat environment is described in the *Threat Assessment Report* [KMI2204], and the risk environment is described in the *Security Risk Analysis* [KMI2206]. Security objectives and policies to mitigate the identified risks are stated in Volume 2. Implementation requirements to enable the KMI to meet those objectives and enforce those policies are stated partly in this document and partly in Volumes 1 and 2.

## 2.2 (U) Objectives, Policies, and Guidelines

(U//FOUO) Volume 2 defines KMI's basic security objectives as follows:

- (U//FOUO) **Access Control**. Protect all KMI resources from unauthorized use.
- (U//FOUO) **Information Security**. Protect all KMI information from unauthorized disclosure, modification, destruction, or loss.
- (U//FOUO) **Service Availability**. Protect the KMI system against denial of service to its authorized users.
- (U//FOUO) **System Integrity**. Protect all KMI system elements to ensure their continued and correct operation.
- (U//FOUO) **User Authentication**. Verify the identity of system entities before permitting them to access system resources.
- (U//FOUO) **User Accountability**. Enable KMI managers to trace the initiation of system activities to individual users that can be held responsible for the consequences of the activities.
- (U//FOUO) **Management Control**. Enable KMI managers to (1) configure KMI security characteristics, (2) ensure that the system meets applicable security pollicies, and (3) enable interoperation with peer systems, including other key management infrastructures ~~and other external systems~~.

(U//FOUO) These objectives provide a basis for more detailed security policies and functional security requirements that are stated in Volume 2. Among those policies is the following guideline:

> (U//FOUO) **General Policy on System Architecture**. To achieve its security objectives in a manner that supports the goals of the Department of Defense, the KMI must apply a defense-in-depth strategy to an architecture that is based on a set of information enclaves that have well-defined security perimeters.

(U//FOUO) Defense in depth is a concept for deploying protections in multiple places and in multiple layers, so that if one protective mechanism is defeated, one or more other mechanisms (which are thought of as being "behind", "beneath", or "parallel to" the first mechanism) continue to provide security. To provide defense in depth, this *Security Architecture* describes a high-level allocation of architectural security features and assurances to the various KMI nodes and their components, and provides a rationale for the allocation, based on the security objectives.

(U//FOUO) This *Security Architecture* and the rest of the CI-2 functional architecture that is described in Volume 1 state detailed requirements that implement the following general requirements:

> **CI2-SAR-2.2a** (U//FOUO) **Modular components**. The KMI shall implement a modular architecture that will support flexibility to add or delete products, upgrade Components, and add or modify system interfaces, so that the KMI can evolve over time with minimal architectural impact. [DRV KRD 1180] {Z}

> **CI2-SAR-2.2b** (U//FOUO) **Protected connections**. The KMI shall not provide an unprotected direct connection between Components that are dedicated to different isolated information processing Security Domains. [KRD 1387] {Z}

> **CI2-SAR-2.2c** (U//FOUO) **Protected core**. Components of Core Nodes (see "Security Perimeters" section) shall be protected by a NSA-approved suite of network security devices and protections, including in-line network encryption, boundary protection, and detection of intrusions and malicious code. [DRV KRD 0834] {P-R-S-T}

> **CI2-SAR-2.2d** (U//FOUO) **Isolated domains**. The KMI shall be capable of concurrently serving Client Nodes and interacting with other systems, where each Client Node and non-KMI system operates in a specific Security Domain based on classification, nationality, or affiliation (e.g., U.S., CCEB, NATO, Coalition, etc.). [DRV KRD 1386] {R}

## 2.3 (U) Client-Server Model and Transaction Model

(U//FOUO) The KMI includes numerous instances of client-server operations, in which a client process sends a service request to a server process, and the server receives the request, performs the service, and returns a message, perhaps with some resultant data. These client-server operations involve transactions. A transaction is a series of units of work, called events. To achieve the KMI's security objectives, transactions and events need to be designed so that they are atomic, consistent, isolated, and durable [Gray]:

- (U) **Atomic**. An event is an all-or-nothing function; all actions that comprise the transaction should be completed, or else none should happen.
- (U) **Consistent**. An event satisfies correctness constraints defined for the data that is being processed.
- (U) **Isolated**. If two events are performed concurrently, the events do not interfere with each other, and it appears as though the system performs one event at a time.
- (U) **Durable**. System state and event semantics survive system failures.

(U//FOUO) Use of the client-server and transaction models in a distributed architecture also affects how security services are implemented in the KMI.

- (U//FOUO) **Global consistency.** Client-server interactions, and their supporting protocols, need to be designed to ensure database consistency across KMI nodes, particularly during periods of system instability, so that security services that depend on system databases are not compromised.

- (U//FOUO) **Identity authentication.** Client-server interfaces at several levels, not just at the Client-PRSN level, need to incorporate mechanisms to authenticate client and server identities to each other.

- (U//FOUO) **Process authorization.** Transaction processing functions at several levels need to incorporate access control mechanisms to ensure that transactions are authorized for clients that request them.

- (U//FOUO) **Interface restriction.** The number, type, and complexity of interfaces between clients and servers and through which transactions are handled need to be kept to a minimum to better assure that security policies are correctly and consistently enforced at the interfaces.

- (U//FOUO) **State awareness.** If a system function requires that multiple transactions be performed over a relatively long period of time, the function needs to incorporate mechanisms specifically to maintain continued correct awareness of system state to ensure secure operation of the function.

## 2.4 (U) Defense in Depth

(U//FOUO) The DoD *Information Assurance (IA) Technical Framework* (IATF) [IATF] adopts defense in depth as the fundamental strategy for protecting computer systems and their interconnecting networks. This *Security Architecture* follows the IATF guidance for resisting attack from multiple directions by either insiders or outsiders.

(U//FOUO) The defense-in-depth concept is appealing because it aligns with traditional warfare doctrine; but the concept has traditionally been applied to geospatial structures, rather than cyberspace structures. Applying the concept to distributed, network-based information systems involves an assumption that such systems can have a spatial or topological representation. It assumes that one can implement—from the outer perimeter of a network, through its various layers of components, to its center (which consists of the subscriber application systems supported by the network)—a varied series of countermeasures that together provide adequate protection. However, it can be difficult to map the topology of computer systems and make

certain that no path exists by which an attacker can bypass defensive layers and damage the center. Therefore, the IATF enumerates defense-in-depth objectives for various focus areas, and this *Security Architecture* implements those objectives where appropriate.

**CI2-SAR-2.4a** (U//FOUO) The KMI shall incorporate the defense-in-depth security principles of the *Information Assurance Technical Framework* [IATF]. [KRD NEW] {Z}

(U//FOUO) One IATF defense-in-depth focus area is defense of networks and their infrastructure. The IATF states the following guidelines for this area. However, not all are directly applicable to the KMI security architecture; some apply to networks to which the KMI connects but which are not part of the KMI.

- (U) Protect local and wide area communications networks.
- (U) Provide confidentiality and integrity service for data transmitted over these networks.
- (U) Ensure that all data exchanged over wide area networks is protected from disclosure to anyone not authorized to access the network.
- (U) Ensure that wide area networks supporting mission-critical and mission-support data provide appropriate protection against denial-of-service attacks.
- (U) Protect against delay, misdelivery, or nondelivery of otherwise adequately protected information.
- (U) Protect from traffic flow analysis both user traffic and network infrastructure control data.
- (U) Ensure that protection mechanisms do not interfere with otherwise seamless operation with other authorized backbone and enclave networks.

(U//FOUO) Some KMI requirements for the first focus area are stated in this *Security Architecture*, and other requirements for this area are stated in Volume 2. The stated requirements provide for strong separation between networks operating in different security domains and seek to ensure network availability even in the event of denial-of-service attacks.

(U) A second IATF defense-in-depth focus area is defense of enclave boundaries. The IATF states the following guidelines for this area.

- (U) Ensure that physical and logical enclaves are adequately protected.
- (U) Enable dynamic throttling of services in response to changing threats.
- (U) Ensure that systems and networks within protected enclaves maintain acceptable availability and are adequately defended against denial-of-service intrusions.
- (U) Ensure that data exchanged between enclaves or via remote access is protected from improper disclosure.
- (U) Provide boundary defenses for those systems within the enclave that cannot defend themselves due to technical or configuration problems.
- (U) Provide a risk-managed means of selectively allowing essential information to flow across the enclave boundary.
- (U) Provide protection against the undermining of systems and data within the protected enclave by external systems or forces.
- (U) Provide strong authentication, and thereby authenticated access control, of users sending or receiving information from outside their enclave.

(U//FOUO) Some KMI requirements for the second focus area are stated in this *Security Architecture*, and other requirements for this area are stated in Volume 2. The requirements provide a protected perimeter for security enclaves; control the flow of information passing across security levels; control access by remote locations and remote users; and use network-based attack sensing, warning, and response (ASWR) capabilities to identify vulnerabilities, attacks, and suspicious activities and provide appropriate responses. Interconnection of KMI components to outside systems is done only in a controlled fashion with adequate assurance. KMI functions that require open, uncontrolled access to and from other systems are isolated and have adequate safeguards to enforce security policy.

(U) A third IATF defense-in-depth focus area is defense of the computing environment. The IATF states the following guidelines for this area.

- (U) Ensure that clients, servers, and applications are adequately defended against denial of service, unauthorized disclosure, and modification of data.
- (U) Ensure the confidentiality and integrity of data processed by the client, server, or application, both inside and outside of the enclave.
- (U) Defend against the unauthorized use of a client, server, or application.
- (U) Ensure that clients and servers follow secure configuration guidelines and have all appropriate patches applied.
- (U) Maintain configuration management of all clients and servers to track patches and system configuration changes.
- (U) Ensure that applications can be readily integrated with no reduction in security.
- (U) Ensure adequate defenses against subversive acts by trusted persons and systems, both internal and external.

(U//FOUO) Some KMI requirements for the third focus area are stated in this *Security Architecture*, and other requirements for this area are stated in Volume 2. The requirements provide for a protected computing environment to support security services and also provide for host-based ASWR capabilities to identify vulnerabilities, attacks, and suspicious activities and provide appropriate responses.

## 2.5 (U) Compliance

(U//FOUO) This *Security Architecture* ensures compliance with the *Security Policy* [KMI2200V2] through protection and controlled usage of system resources, through user accountability, and through security assurance. In the following subsections, these security topics are informally mapped to the section titles in Volume 2.

### 2.5.1 (U) Resource Protection

(U//FOUO) This *Security Architecture* defines security perimeters for CI-2 nodes and enclaves, and protects system resources inside the perimeters from unauthorized use, modification, disclosure, destruction, or loss. Components inside the perimeters incorporate mechanisms that provide protection for all resources for which the KMI is responsible. Interconnection of protected components to external systems is done only in a controlled fashion. Table 1 informally maps resource protection areas to sections of Volume 2.

**Table 1. (U) KMI Resource Protection Policy Elements**

| | Sections in Volume 2 | |
|---|---|---|
| **Information Protection** | Information Confidentiality | Emanations Security |
| | | Encryption Key Management |
| | Information (Content) Integrity | |
| **Service Protection** | Archive | |
| | Communication between KMI Nodes | |
| | Product Ordering | |
| | Product Generation | |
| | Product Handling | |
| | Product Distribution | |
| | Product Accounting | |
| | Marking | |

**UNCLASSIFIED//FOUO**

(U//FOUO) Controlled usage is the property of the KMI that limits user activities to those for which the users are authorized. Controlled usage is established primarily by the "Access Control" section of Volume 2 and the "Access Control Services" section of this *Security Architecture*. The KMI limits user access to system resources according to (1) attributes associated with the resources (e.g., classification, ownership), (2) attributes associated with the requested function (e.g., authorizations), and (3) attributes associated with user identity (e.g., clearance, roles, domains, "need-to-know").

### 2.5.2 (U) User Accountability

(U//FOUO) User accountability is the property of the KMI that enables system activities to be traced uniquely to individual users or other causes that can be held responsible for the activities. To establish user accountability, the KMI registers users and requires evidence that they are eligible to access the system. Then, the KMI identifies users uniquely whenever they access the system, using strong means of user identity authentication that are incorporated uniformly across the entire system. Administrative activities are tracked by audit and ASWR systems. The KMI records information that associates users with KMI activities performed on their behalf. The KMI enables authorized managers to access and evaluate the accountability information by secure means, within a reasonable amount of time, and without undue difficulty. Table 2 informally maps the user accountability area to sections in Volume 2.

**Table 2. (U) KMI User Accountability Policy Elements**

| | Sections in Volume 2 |
|---|---|
| **Assured Identification** | User Registration |
| | User Identification |
| | Identity Authentication |
| | Peer Entity Authentication |
| | Audit |
| **Activity Tracking** | Data Origin Authentication |
| | Non-repudiation |

**UNCLASSIFIED//FOUO**

### 2.5.3 (U) Assurance

(U//FOUO) Assurance is an attribute of the KMI that provides grounds for believing the system operates in a way that enforces the security policies stated in Volume 2 and satisfies the functional security requirements stated in this *Security Architecture* and in Volumes 1 and 2. The design of KMI components must accurately interpret the security policy and not distort the intent of that policy. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life-cycle. This objective is addressed through requirements for developmental assurance, operational assurance, and continuous operations. Table 3 informally maps the assurance areas to sections in Volume 2.

**Table 3. (U) KMI Security Assurance Policy Elements**

| | Sections in Volume 2 | | |
|---|---|---|---|
| **Developmental Assurance** | Security Services | | |
| | Certification | Security Implementation | Computer Security |
| | | | Communication Security |
| | | | Configuration Control |
| | | | Testing |
| **Operational Assurance** | Accreditation | Extend Trust | |
| | Security Management | System Integrity | Security Configuration |
| | | Attack Sensing, Warning, and Response | |
| | Personnel Security | Personnel Security | |
| | | Security Training and Awareness | |
| | | Outside Users | |
| **Continuous Operations** | System Availability | Physical Security | |
| | | Contingency Planning | |

**UNCLASSIFIED//FOUO**

- (U//FOUO) **Developmental assurance** involves requirements that mandate policies for security services and that ensure secure implementation of the services.

- (U//FOUO) **Operational assurance** involves requirements that mandate the accreditation of KMI components and ensure their secure operation. Secure operation relies on the use of trustworthy KMI management personnel and reliable management features. Also, attack sensing, warning, and response services need to be implemented across all components within the KMI security perimeter.

- (U//FOUO) **Continuous operations** involves requirements that ensure system availability. The KMI should be both available and secure at all times, but in some situations the system also needs to support degraded operational modes.

(U//FOUO) CI-2 components gain approval to operate through a formal process that satisfies the *DoD Information Technology Security Certification and Accreditation Process* (DITSCAP) [DITSCAP], as required by Volume 2 and as interpreted by the *Certification and Accreditation Plan for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)* that will be prepared by NSA. The KMI certification and accreditation actions provide the framework for establishing overall assurance for the KMI, and they provide the basis for system-wide, site-level, and component-level assurance. The KMI certification and accreditation effort addresses developmental, deployment, and post-deployment assurance issues.

(U//FOUO) The DITSCAP is the standard DoD process for identifying information security requirements, providing security solutions, managing information system security activities, and certifying and accrediting both classified and unclassified systems. The DITSCAP defines the activities upon which overall KMI security assurance is based, and the documentation generated by the DITSCAP provides KMI system-wide assurance evidence. Personnel and administrative security measures are expected to be identified and documented as part of the DITSCAP.

(U//FOUO) The KMI is expected to be implemented with robust, commercial-off-the-shelf (COTS) products that provide strong assurance, augmented by Government off-the-shelf (GOTS) products where COTS products do not exist or are not sufficiently robust. As specified in Volume 2, products need to be evaluated or certified against Common Criteria protection profiles, or against other NSA-approved criteria such as the Unified INFOSEC Criteria [REFTBD1]. Components that implement cryptographic functions need to meet Federal Information Processing Standards (FIPS), or meet other NSA-approved standards.

# 3 (U) ARCHITECTURAL ELEMENTS

(U//FOUO) This *Security Architecture*, together with Volumes 1 and 2, assigns security functions to the components of KMI nodes in CI-2, so that the composite system achieves its basic security objectives and also satisfies the following control statement:

> **CONTROL** [NT] (U//FOUO) **DCFA-1 Functional Architecture for AIS Applications (Integrity)**. "For AIS applications, a functional architecture that identifies the following has been developed and is maintained: [DoDI8500.2]"
> – "All external interfaces, the information being exchanged, and the protection mechanisms associated with each interface".
> – "User roles required for access control and the access privileges assigned to each role".
> – "Unique security requirements (e.g., encryption of key data elements at rest)".
> – "Categories of sensitive information processed or stored by the AIS application, and their specific protection plans".
> – "Restoration priority of subsystems, processes, or information".

(U//FOUO) This section explains some of the architectural concepts that support those assignments. The concepts include user roles and their authorizations; user access modes; security perimeters of protected resources; protected channels that connect components; and structures—enclaves and zones—that provide modularity and domain isolation.

## 3.1 (U) User Roles and Permissions

(U//FOUO) A registered user (abbreviated as user) is a system entity authorized to access the KMI by invoking an identity that has previously been established in the system. The KMI cannot prevent unauthorized entities in its environment from attempting to access its system resources, but the KMI blocks such unauthorized access as much as possible. The KMI provides products and services only to authorized entities, and all authorized entities must first be registered as users before they can receive products or services.

(U//FOUO) Whenever a human user accesses the KMI, the user acts in a specific, assigned role and with an assigned set of permissions. (A registered user device is not assigned to a role.) Each permission that has been assigned to a role enables a person acting in that role to perform a specific type of system action against one or more system resource objects.

> **DEFINITION** (U//FOUO) Role. A job title in the KMI system that (1) has a specified set of functional responsibilities within the system, (2) can be granted one or more Permissions, and (3) can have one or more Users assigned to it.

> **DEFINITION** (U//FOUO) Permission. An positively-stated Authorization for Access that (1) can be associated with one or more Roles and (2) enables a User in a Role to access a specified set of System Resources by causing a specific set of System Actions to be performed on the resources.

> **DEFINITION** (U//FOUO) System Action. A specific function or behavior of the KMI that accesses and possibly affects one or more Resource Objects.

**DEFINITION** (U//FOUO) Resource Object. A specific System Resource that (1) can be accessed by a System Action and (2) can be protected by Access Control services.

(U//FOUO) A system action is implemented by an executable image of a computer program, which upon invocation performs some function for a user [ANSI]. A resource object in the context of the KMI usually take the form of a product, a service, or an operational or administrative mechanism.

(U//FOUO) In this *Security Architecture,* permissions are not directly assigned to user identities. Instead, permissions are assigned to Roles so that, as defined in the *Common Criteria* [IS15408-2], a role becomes a set of rules establishing the allowed interactions between a user and the system. Then, user identities are assigned to roles as appropriate for user responsibilities. (The assignment process is fully described in the "Role-Based Access Control" section.) Both role assignments and objects may be assigned attributes that can cause the KMI to constrain the exercise of a permission. (The application of attributes and constraints to the process of requesting and distributing products for Type 1 devices is specified in the "Rule-Based Access Control" section.)

(U//FOUO) Some KMI roles and permissions are built into the system to be available for use at system startup. New permissions may be added to the system through the introduction of new software functionality, and authorized KMI managers can create new roles and add new permissions to existing roles to meet evolving needs. The built-in roles, which are listed in Table 4, include several management roles, and one non-management role. The non-management role is called KOA Agent and is described in the "Approval-Based Access Control Section".

(U//FOUO) Volume 2 describes the processes that register users and authenticate their identities when they access the system. To each registered user identity, the KMI assigns an identifier and associated authentication material. The type of authentication material depends on the authentication mechanism that is used for the role or roles to which the identity is assigned.

### 3.1.1 (U) Management Roles

(U//FOUO) Qualified human users are assigned as managers that operate or administer the KMI.

**DEFINITION** (U//FOUO) Manager. A Human User that directs, controls, or regulates some set of System Resources.

**DEFINITION** (U//FOUO) Management Role. A Role that has Permissions that enable a Registered User to direct, control, or regulate some set of System Resources.

**CI2-SAR-3.1.1a** [NT] (U//FOUO) The KMI shall implement, at a minimum, a set of Management Roles sufficient to perform the system management duties stated in the KRD. [DRV KRD 1787] {Z}

**CI2-SAR-3.1.1b** (U//FOUO) Before permitting a User Identity to access the KMI in a Management Role, the KMI shall authenticate the User Identity through either a Type 1 cryptographic mechanism or another method that has equivalent strength and assurance. [DRV KRD 1062] {Z}

**Table 4. (U) KMI Roles**

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

**UNCLASSIFIED//FOUO**

(U//FOUO) This *Security Architecture* states requirements for several KMI management roles. As shown in Table 4, the management roles can divided into internal and external classes.

**DEFINITION** (U//FOUO) Internal Management Role. A Role that is intended to be performed by a person who is a member of the central organization that controls the KMI.

**DEFINITION** (U//FOUO) External Management Role. A Role that is intended to be performed by a Manager that typically is a member of a KMI customer organization.

(U//FOUO) The management roles also can be divided into operational and administrative.

**DEFINITION** (U//FOUO) Operational Manager. A Manager that performs functions directly involving the production of products and services, or that supervises such functions.

(U//FOUO) Operational managers use KMI-issued 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.

**DEFINITION** (U//FOUO) Administrative Manager. A Manager that performs housekeeping functions that support the work of Operational Managers and KOA Agents but usually do not directly involve KMI products and services.

(U//FOUO) Some examples of administrative functions are installing and maintaining software; configuring accounts, auditing for security, and doing backup and recovery. Many administrative functions are common to all computing and communication platforms. Like operational managers, administrative managers may use KMI-issued credentials and role-based permissions for some work, but they also obtain authorizations through platform-based security mechanisms of operating systems and applications.

### 3.1.2 (U) User Access Modes

(U//FOUO) Users access PRSNs in three different modes.

- (U//FOUO) **Interactive, Web-based access.** A user can employ a web browser to interact with a web server that is a component of a PRSN. This mode is intended for human users who act in a management role or as a KOA Agent and who remotely access a PRSN with a browser that is part of their Client Node. This type of Client-PRSN dialogue is conducted via a protected communication channel.

- (U//FOUO) **Non-interactive, transaction-based users.** A user can participate in a highly structured transaction dialogue between a Client Node and a PRSN. This mode is intended for users that are automated devices acting as a KOA Agent. This type of Client-PRSN dialogue is conducted via a protected communication channel.

- (U//FOUO) **Interactive direct component access.** Human users who act in certain management roles can directly access computer platforms that are components of PRSNs, PSNs, and the CSN. This mode may involve a variety of specific interface types, including web-based, transaction-based, and others. These users often access platforms locally; but when the access is remote, the dialogue is conducted via a protected communication channel.

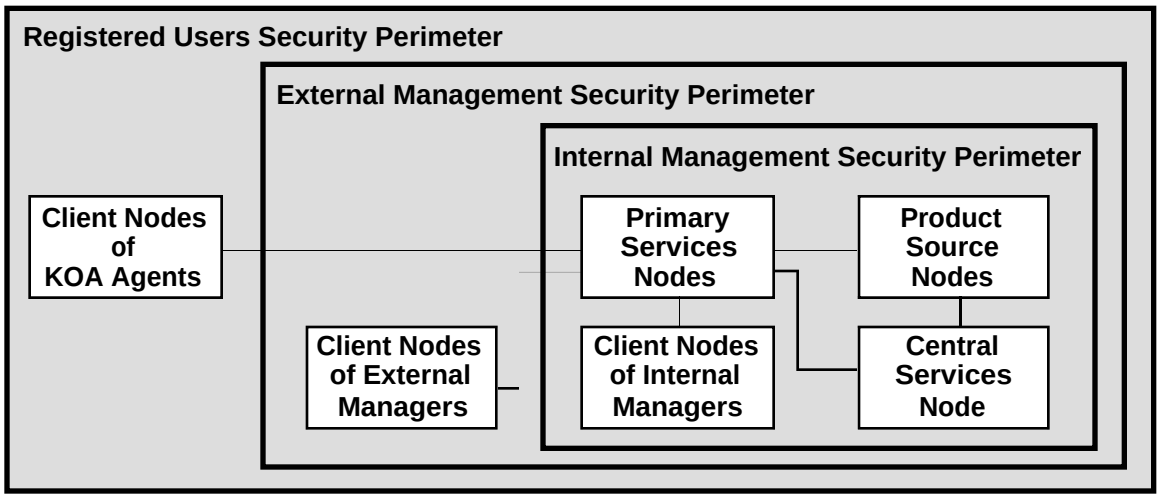
## 3.2 (U) Resource Protection

(U//FOUO) This *Security Architecture* defines layered security perimeters within which system components and resources are protected. It also states requirements for protected channels that enable communications to take place between protected components.

### 3.2.1 (U) Security Perimeters

(U//FOUO) The KMI's defense-in-depth architecture is based on layered and complementary security perimeters that enclose system nodes. Figure 3 illustrates the main conceptual layers:

**Figure 3. (U) KMI Security Perimeters**




**UNCLASSIFIED//FOUO**

- (U//FOUO) **Internal Management Security Perimeter**. Client Nodes that serve users acting in the sensitive internal management roles operate inside the Internal Management Security Perimeter and are subject to rigorous protections that are required for core nodes.

- (U//FOUO) **External Management Security Perimeter**. Client Nodes that serve users acting in external management roles operate inside the External Management Security Perimeter. These nodes also are usually treated as being within security perimeters of mission systems and organizations that operate the nodes. The nodes are primarily subject to KMI security policy and secondarily to policies of those other systems and organizations, but the managers that operate the core nodes are not responsible for protecting these Client Nodes.

- (U//FOUO) **Registered Users Security Perimeter**. Client Nodes that serve users acting in the KOA Agent role are inside the Registered Users Security Perimeter and must be protected in accordance with KMI policy. However, KMI policy is secondary for these nodes. Their security is primarily the responsibility of the organizations that operate them.

(U//FOUO) There are security perimeters in addition to these three. Each node has its own individual security perimeter and is subject to specific protections defined for it. Also, although Figure 3 represents all nodes as single boxes, some nodes, especially PRSNs, are implemented as

clusters or networks of components that each have a local security perimeter defined by KMI policy and architecture. Any data communications that pass between two protected nodes or components and through an unprotected area outside the security perimeters, are required to be carried by a protected communication channel, as described in the next section.

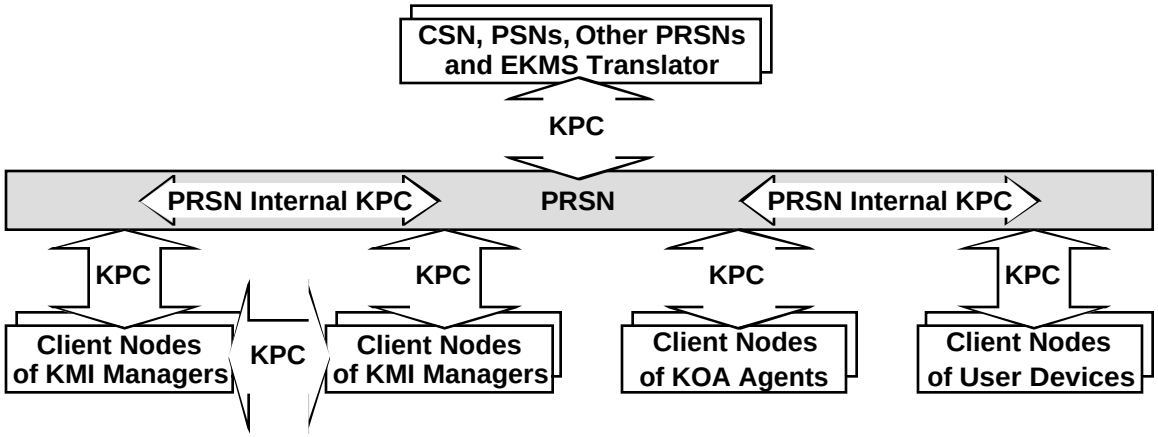
### 3.2.2 (U) Protected Channels

(U//FOUO) A KMI Protected Channel (KPC) is a communication path that provides (1) information integrity service; (2) either data origin or peer entity authentication service, as is appropriate to the mode of communication; and (3), optionally, information confidentiality service (see "Communications Services" section of Volume 2). The specific security services, security mechanisms, and level of assurance of a KPC depend on the channel's purpose and environment, but the following requirements establish the basis for such specifications:

**CI2-SAR-3.2.2a** (U//FOUO) A KPC shall provide (1) Information Integrity Service and (2) either Data Origin Authentication Service or Peer entity Authentication Service, and (3) may optionally provide Information Confidentiality Service. [DRV KRD 0941, 1026] {Z}

(U//FOUO) Figure 4 illustrates that when clients communicate with a PRSN, or when clients of managers communicate with each other, the dialogue is protected by a KPC. Communications between a PRSN and other core nodes—the CSN, PSNs, and other PRSNs—are primarily transaction-based and are carried by a virtual private network created from KPCs. Communications between components inside a PRSN or other core node also may use a KPC if the communication medium passes outside protected areas.

**Figure 4. (U) KMI Protected Channels Between Components**




**UNCLASSIFIED//FOUO**

(U//FOUO) Some operational and administrative functions require Managers to connect directly to native interfaces of computer platforms. In these cases, the needed connection security is provided by physical means or by communication security mechanisms specific to the platform, and are considered to be part of the component being managed.

**CI2-SAR-3.2.2b** (U//FOUO) The KMI shall authenticate Component Identities when necessary to meet its security objectives. [DRV KRD 1027] {Z}

**CI2-SAR-3.2.2c** (U//FOUO) All information that the KMI transfers between a (1) a PRSN Component and (2) a Client Node, through a communication medium outside protected Component security perimeters, shall be carried by a KPC that provides security services appropriate to the information and to the mode of communication. [DRV KRD 0842, 0870, 0941, 0942, 1026] {C-R}

**CI2-SAR-3.2.2m** (U//FOUO) All information that the KMI transfers between two Client Nodes of External Managers (i.e., between two Client Nodes that are not Core Nodes) through a communication medium outside protected Component security perimeters, shall be carried by a KPC that provides security services appropriate to the information and to the mode of communication. [DRV KRD 0842, 0870, 0941, 0942, 1026] {C}

**CI2-SAR-3.2.2d** (U//FOUO) All information that the KMI transfers through a communication medium outside protected Component security perimeters (1) between Independent Components of PRSNs, (2) between a PRSN Component and a PSN Component, (3) between a PRSN Component and a CSN Component, and (4) between a PSN Component and a CSN Component, shall be carried by a KPC that provides security services appropriate to the information and to the mode of communication. [DRV KRD 0842, 0870, 0942, 1026] {P-R-S-T}

**CI2-SAR-3.2.2e** (U//FOUO) All information that the KMI transfers through a communication medium outside protected Component security perimeters, between the KMI and a cooperating non-KMI system shall be carried by a KPC that provides security services appropriate to the information and to the mode of communication. [DRV KRD 0842, 0870, 0942, 1026] {X}

**CI2-SAR-3.2.2f** (U//FOUO) The strength of mechanism and assurance of security services for a KPC shall satisfy the DCAS and DCSR controls of DoD Instruction (DoDI) 8500.2 [DoDI8500.2], according to the sensitivity of the information being transferred. [DRV KRD 1026, 1536] (See “Assurance Levels” section of Volume 2.) {Z}

**CI2-SAR-3.2.2g** (U//FOUO) The KMI shall use NSA-approved cryptography to secure communications between Components, and cryptographic mechanisms must be keyed at least at the highest of the system-high levels of the Components. [DRV KRD 2129] {Z}

**CI2-SAR-3.2.2m** (U//FOUO) The KMI shall use NIST-certified cryptography (or better) to encrypt unclassified “Sensitive” information (as defined in [DoDI 8500.2]) that (1) does not affect the ordering and management of Type 1 products and (2) is transmitted through a commercial or wireless network. [DRV KRD 2133] {A-C-R}

**CI2-SAR-3.2.2h** (U//FOUO) The KMI shall provide Information Confidentiality Service on a KPC when required by the sensitivity of the information being transferred. [DRV KRD 1026] {Z}

**CI2-SAR-3.2.2i** (U//FOUO) Information Confidentiality Service shall be an available option on KPCs between (1) Client Nodes operated by KOA Agents and (2) the PRSN Components through which those users receive KMI products and services. [DRV KRD 1026] {C-R}

**CI2-SAR-3.2.2j** (U//FOUO) Information Confidentiality Service shall be an available option on KPCs between (1) Client Nodes operated by Administrative Managers and (2) the Components they administer. [DRV KRD 0870, 1026] {C-P-R-S-T}

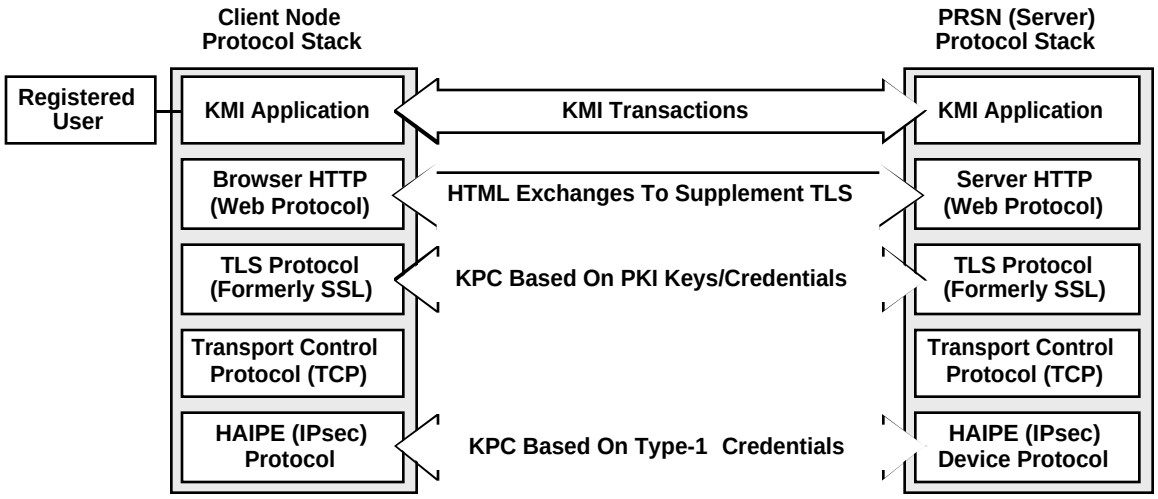
**CI2-SAR-3.2.2k** (U//FOUO) Information Confidentiality Service shall be an available option on KPCs between (1) Client Nodes operated by Operational Managers and (2) the Components they operate. [DRV KRD 0870, 1026] {A-C-R}

**CI2-SAR-3.2.2l** (U//FOUO) Components that relay classified or sensitive messages shall protect those messages from disclosure to local operators. [KRD 0871] {Z}

(U//FOUO) All managers and KOA Agents that use a client to access a PRSN are registered and, therefore, able to authenticate their identity to the PRSN (see discussion of identification and authentication services in Volume 2). All of those managers also have credentials that are needed to establish a KPC. However, only some KOA Agents have such credentials, and not all of the credentials are of the same type. Therefore, as suggested by Figure 4, not all of the KPCs used by KOA Agents are of the same type.

(U//FOUO) Figure 5 illustrates that the KMI connects clients to PRSNs through two different types of standard KPCs, which operate in different protocol layers.

**Figure 5. (U) KMI Protected Channel Layers**




**UNCLASSIFIED//FOUO**

- **PKI-Based KPC (TLS KPC).** This type of KPC is layered below the Hypertext Transfer Protocol (HTTP) and KMI application protocols, and above the Transmission Control Protocol (TCP), and is implemented with the Transport Layer Security (TLS) Protocol [RFC3546] (formerly known as Secure Sockets Layer (SSL) Protocol).

- **Type 1 KPC.** This type of KPC is layered below TCP and above network substrate protocols, and it is implemented with Type 1, end-to-end encryption devices. This KPC is implemented by an extended version of Internet Protocol security (IPsec) that is specified for the High-Assurance Internet Protocol Encryptor (HAIPE) [HAIPIS].

  **DEFINITION** (U//FOUO) Type 1 [cryptographic device]. Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to [cryptographic devices], and not to information, key, services, or controls. Type 1 [cryptographic devices] contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation. [CNSSI4009]

(U//FOUO) The type of KPC needed for a client's connection to a PRSN depends on the type of user that operates the client. Table 5 summarizes the various combinations.

**Table 5. (U) KMI Protection for Client Node Connections to PRSNs**

| Type of User and Client | When User's Client Node Connects to PRSN's Server |
|---|---|
| Human User acts in Management Role. | Client uses both TLS KPC and HAIPIS KPCs.<br>• TLS KPC uses PKI credentials that were issued to the user and server.<br>• HAIPIS KPC uses Type 1 credentials that were issued to the Client, and PRSN's Type 1 credentials. |
| Human User acts as KOA Agent; uses same Client Node as when acting as a Manager. | Client uses both TLS KPC and HAIPIS KPCs,<br>• KPCs use the same credentials as when user acts as a manager. |
| Human User acts as KOA Agent; uses non-management client and PKI credentials. | Client uses TLS KPC.<br>• TLS KPC uses the PKI credentials that were issued to the user by the DoD PKI or other PKI recognized by KMI, and also uses server's PKI credentials. |
| Human User acts as KOA Agent; uses non-management client and identifier-password. | Client uses TLS KPC.<br>• TLS KPC uses only server's PKI credentials. |
| User Device with Client capability. | Client uses HAIPIS KPC<br>• HAIPIS KPC uses Type 1 key management credentials of the User Device, and PRSN's Type 1 credentials. |

**UNCLASSIFIED//FOUO**

(U//FOUO) When a Client Node makes a web-based connection to a PRSN, the client's browser or other access software normally establishes a PKI-based KPC in the TLS layer, so that the PRSN can authenticate the identity of the user that is operating the client. The TLS KPC also provides data integrity for the connection. That type of KPC alone may be adequate for when a KOA Agent connects to a PRSN. However, some system functions may require that the KPC also provide data confidentiality service, and it is expected that the default configuration for all TLS KPCs will include having data confidentiality service enabled.

(U//FOUO) The identity authentication in the TLS layer of a Web-based client enables the PRSN server to determine what are the authorized roles and permissions of a web-based user. For a transaction-based client, user identity can be established by digital signatures on the transaction protocol messages.

(U//FOUO) When a user connects to a PRSN in a management role, a KPC is required that is more robust than one based on PKI-based TLS. The client must incorporate a Type 1 encryption device and establish a Type 1 KPC with a counterpart Type 1 device in the PRSN, so that the PRSN can authenticate the Manager–Client combination as belonging to the Type 1 community. The Type 1 KPC is in addition to the TLS KPC, and TLS is carried over the Type 1 KPC.

(U//FOUO) A TLS KPC for client access normally employs the user's PKI private key and public-key certificate in combination with the PRSN server's key and credential, and authenticates the identities of the user and server to each other. In some cases, however, PRSNs may need to deliver key material to users that do not have PKI credentials, or to clients are not able to use their credentials when connecting to the PRSN. In these cases, the TLS KPC uses only the service-side credential and authenticates only the server to the user. The user stills need to be authenticated to the PRSN, but the PRSN authenticates the user with an alternate mechanism, usually an identifier–password mechanism. The alternate mechanism can be incorporated in Hypertext Markup Language (HTML) exchanges or other application exchanges between the client and the PRSN. These exceptional cases are discussed further in the "PRSN Product Delivery Enclaves" section.

### 3.2.3 (U) Domains, Enclaves, and Zones

(U//FOUO) The KMI needs to meet requirements for component modularity (see "Objectives, Policies, and Guidelines" section) and for isolation of components that operate at different levels of sensitivity.

**DCSP-1 Security Support Structure Partitioning (Integrity)**. "The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process. [DoDI8500.2]"

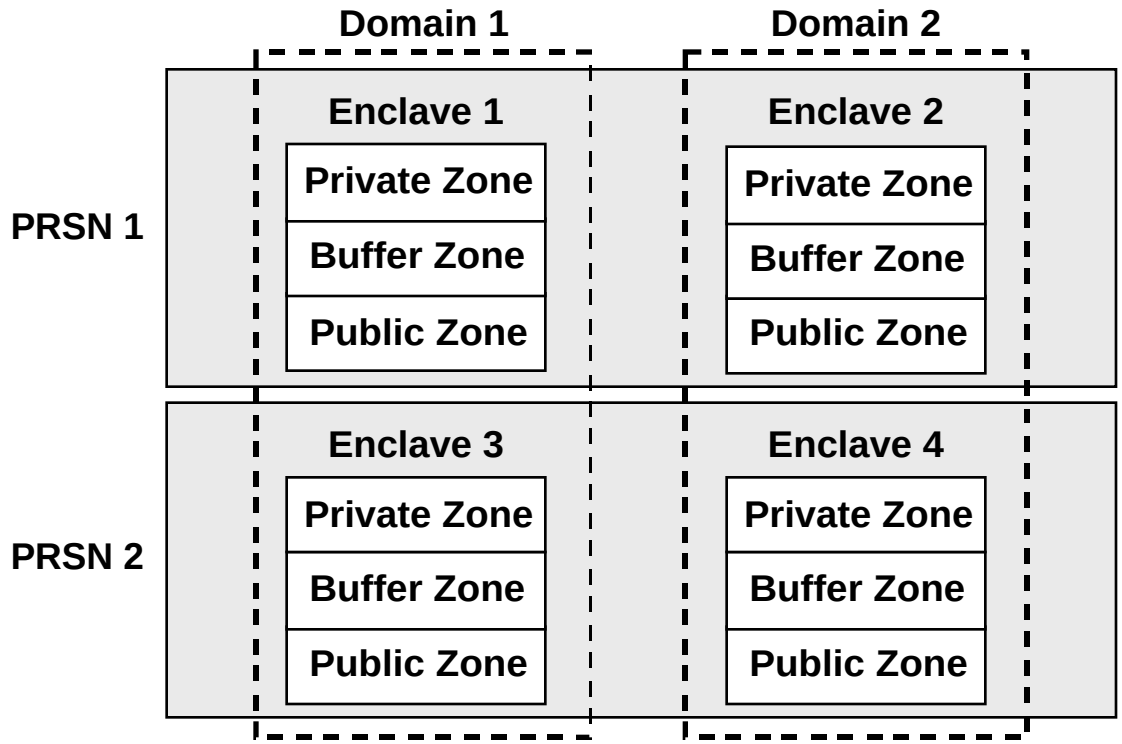
**DCPA-1 Partitioning the Application (Integrity)**. "User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate. [DoDI8500.2]"

**CI2-SAR-3.2.3a** (U//FOUO) The KMI shall ensure that User interface services (e.g., web services) are physically or logically separated from data storage and management services (e.g., database management systems), per DoDI 8500.2 control DCPA-1. [DRV KRD 2120] {R}

(U//FOUO) **EBPW-1 Public WAN Connection (Confidentiality)**. For Components that process sensitive information, "Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ). [DoDI8500.2]"

(U//FOUO) The CI-2 architecture meets requirements for modularity and isolation by using nested structures, as illustrated by Figure 6, to separate components that perform different functions and that serve different communities of clients. KMI nodes (1) intersect security domains, (2) contain security enclaves that lie inside the domains, and (3) contain security zones that are subdivisions of the enclaves.

**Figure 6. (U) KMI Domains, Enclaves, and Zones**




**UNCLASSIFIED//FOUO**

**DEFINITION** (U//FOUO) Security Domain. A set of System Entities that operate under a common security policy, including operating at the same security level.

(U//FOUO) A security level is the combination of a hierarchical classification designation and a set of non-hierarchical category designations, which together represent the disclosure sensitivity of a specified type or item of information.

(U//FOUO) This "Nodal Security Architecture" section incorporates the following assumptions, which ensure that automated components of the KMI system cannot move information from one classification level to another without authorization:

- (U//FOUO) **Single-level platforms**. Except in multilevel guard devices that are specifically designed to connect domains that operate at different security levels (see "Data Replication" section below), each computer platform in a PRSN or the CSN is a single-level component that operates at the security level of its containing domain.

- (U//FOUO) **Single-level clients**. Each Client Node is a single-level component that operates at the security level of its containing domain.

- (U//FOUO) **Single-level tokens**. Each PKI hardware token that the DoD PKI issues to a user is a single-level component that operates at either Unclassified or U.S.-Secret.

(U//FOUO) CI-2 nodes maintain separation between security domains. However, as illustrated by Figure 6, a single node can contain security enclaves belonging to two or more domains.

**DEFINITION** (U//FOUO) Security Enclave. A set of Components that operate in the same Security Domain and share the protection of a common, continuous security perimeter.

(U//FOUO) This is a KMI-specific case of the definition stated in [DoDD8500.1]:

"A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves . . . provide standard IA capabilities such as boundary defense, incident detection and response, and key management . . . may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers."

(U//FOUO) A security enclave within a CI-2 PRSN is composed of one or more security zones:

**DEFINITION** (U//FOUO) Security Zone. A logically contiguous subdivision of a Security Enclave; that is, each Component in a Security Enclave is contained in one of the enclave's Security Zones. Each zone has a well-defined security perimeter, part of which may be formed by the perimeter of the enclave.

(U//FOUO) An PRSN uses three types of`` processing zones—Public, Buffer, and Private, as illustrated by Figure 6—to separate its exposed "front-office" functions from its more sensitive "back office" functions, and this zone structure could be used by other components, too.

- (U//FOUO) **Public Zone**. All interactions with a system entity prior to the user being either authenticated as a registered user or rejected, are intended to be handled entirely by system components that operate in a Public Zone. Thus, this type of zone contains the components that have the greatest exposure to network-based threats.

- (U//FOUO) **Buffer Zone**. After an entity has been authenticated as a registered user, further interactions with the entity are intended to be handled initially in a Buffer Zone. Less sensitive product and service requests are intended to be handled entirely in a Buffer Zone, without any communication with a Private Zone.

- (U//FOUO) **Private Zone**. More sensitive requests are intended to be preprocessed in the Buffer Zone, and then processed in final form in the Private Zone. However, a registered user communicates directly only with the Buffer Zone; communications between a registered user and the Private Zone are handled indirectly, through a proxy in the Buffer Zone.

(U//FOUO) The following statement is the basic requirement for enclaves and zones, and for the boundary protection suites (BPSs) that separate and protect them.

> **CI2-SAR-3.2.3b** (U//FOUO) The KMI shall be divided into multiple Security Enclaves and Security Zones of progressively increasing security sensitivity and overall protection. Access to each enclave and zone, except the least sensitive, shall only be possible via Boundary Protection Suites that enforce authenticated, controlled Access from an adjoining enclave or zone. The least sensitive enclave or zone may permit access via Boundary Protection Suites from general-purpose networks (e.g., NIPRNET and SIPRNET) by entities that initially have not been authenticated. [DRV KRD 1998] {P-R-S}

(U//FOUO) In the previous requirement, NIPRNET is the DoD's common-use Non-Classified Internet Protocol Router Network, and SIPRNET is the DoD's common-use Secret Internet Protocol Router Network. The phrase "initially have not been authenticated" refers, for example, to the fact that a web browser must complete a connection to a web server before the server can request a password from the browser.

(U//FOUO) The following section states requirements that apply to every KMI BPS. Additional requirements for individual zones, enclaves, and BPSs in PRSNs and the CSN are stated in the "Nodal Structures" section; in that section, the specific implementation of zones in a PRSN is described in the "PRSN Security Zones" subsection.

### 3.2.4 (U) Perimeter Defense

(U//FOUO) Communications that pass through security perimeters of domains, enclaves, and zones are mediated by special components.

> **CONTROL** (U//FOUO) **ECIC-1 Interconnections among DoD Systems and Enclaves (Confidentiality)**. "Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance. [DoDI8500.2]"

> **CONTROL** (U//FOUO) **EBBD-3 Boundary Defense (Confidentiality)**. For Components that process classified information, "Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, and at layered or internal enclave boundaries and key points in the network as required. All Internet access is prohibited. [DoDI8500.2]"

(U//FOUO) The Last sentence of EBBD-3 contradicts KRD 2031. This *Security Architecture* interprets the "all Internet access is prohibited" part of the EBBD-3 control to mean that direct,

end-to-end exchanges of data are prohibited between a classified KMI security domain and the unclassified domain of the public Internet (including NIPRNET, which is a DoD-owned part of the Internet). This *Architecture* observes that prohibition for all classified KMI security domains. However, this *Architecture* also uses Type 1, end-to-end encryption devices to create KPCs across the unclassified Internet between classified KMI security enclaves.

> **CONTROL** (U//FOUO) **EBBD-2 Boundary Defense (Confidentiality)**. For Components that process sensitive information, "Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means. [DoDI8500.2]"

(U//FOUO) IDS capabilities of CI-2 components are specified in the "Attack Sensing, Warning, and Response Service" section of Volume 2. To implement ECIC-1, EBBD-3, and EBBD-2, this *Security Architecture* specifies controlled interfaces called "boundary protection suites", and some of the BPSs are "guards".

> **DEFINITION** (U//FOUO) Boundary Protection Suite (BPS). A Component that (1) is a data communication gateway into a Security Enclave or Security Zone and (2) regulates data communication traffic to and from the enclave or zone.

> **DEFINITION** (U//FOUO) Guard. A BPS that (1) connects Components that operate in different Security Domains; (2) is trusted to prevent unauthorized disclosure of data from one domain to the other, if that service is required by the respective security levels of the Components; and (3) is trusted to protect the data integrity and system integrity of each domain against threats actions communicated from the other.

#### 3.2.4.1 (U) Boundary Protection Suites

(U//FOUO) A BPS primarily protects the data integrity and system integrity of components in an enclave or zone against threat actions originating outside, and may also protect components outside the zone from those inside. In some cases, a BPS may provide confidentiality service for data being exchanged with another enclave or zone. Systems that perform BPS functions are often called "firewalls", and the interzone confidentiality service is sometimes called a "virtual private network" (VPN).

(U//FOUO) The word "suite" is used here because contemporary BPSs often consist of multiple components or platforms. For example, a BPS may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated local area network that acts a buffer zone between the two routers. The external router might block attacks that use the Internet Protocol (IP) to break security, while the internal router might block traffic from leaving the protected network except through proxy servers which block attacks that attempt to exploit vulnerabilities in higher layer protocols or services.

(U//FOUO) This section states requirements that apply to all BPSs, and the "Nodal Structures" section states additional requirements for specific BPSs and Guards

**CI2-SAR-3.2.4.1a** (U//FOUO) A Computer Platform that implements functions of a BPS in a Security Zone shall be physically separate from other Components of that zone that the BPS protects. [DRV KRD 1180, 1568] {R-S}

(U//FOUO) The DCPP-1 control is implemented by the four requirements that follow it; the "outsourced" part of this control does not apply to CI-2 because the *System Description and Requirements Specification* [KMI2200] does not incorporate any outsourced components:

**CONTROL** (U//FOUO) **DCPP-1 Ports, Protocols, and Services (Availability)**. "DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD [Service and Agency] guidance**.** [DoDI8500.2]"

**CI2-SAR-3.2.4.1b** (U//FOUO) The application and network services—i.e., (1) the communication protocols and (2) the channel bandwidth—that a BPS permits to pass through itself to a specific Component that the BPS protects shall be the minimum that the Component needs to perform its function. [DRV KRD 0901, 0903, 0906, 1999] {R-S}

**CI2-SAR-3.2.4.1c** (U//FOUO) A BPS shall include features to limit the bandwidth of potential covert channels in the communications that the BPS permits to pass through itself. [DRV KRD 1999] {R-S}

**CI2-SAR-3.2.4.1d** (U//FOUO) A BPS that is a Component of a Core Node and connects that Core Node to another Node via a communication path outside those Nodes shall use only approved ports for supported protocols and services, and shall block all other ports and protocols in accordance with DoD procedures for managing those communication mechanisms [DoDI8500.2]. [DRV KRD 0901, 0903, 0906] {P-R-S-T}

**CI2-SAR-3.2.4.1e** (U//FOUO) A BPS that is a Component of a Core Node and connects that Core Node to another Node via a communication path outside those Nodes shall use Network Address Translation [NAT] technology where appropriate to hide Internet Protocol addresses internal to the Core Node. [KRD NEW] {P-R-S}

(U//FOUO) The ECIM-1 and ECVI-1 controls are implemented by the two requirements that follow them:

**CONTROL** (U//FOUO) **ECIM-1 Instant Messaging (Integrity)**. [Not applicable to CI-2; CI-2 does not implement instant messaging.] "Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function. [DoDI8500.2]"

**CONTROL** (U//FOUO) **ECVI-1 Voice over IP (Availability)**. [Not applicable to CI-2; CI-2 does not implement voice over IP.] "Voice over Internet Protocol (VoIP) traffic to and

from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function. [DoDI8500.2]"

**CI2-SAR-3.2.4.1f** (U//FOUO) The KMI shall not implement (1) an instant messaging capability or (2) a voice-over-Internet Protocol capability. [DRV KRD 2136, 2142] {A-R-S}

**CI2-SAR-3.2.4.1g** (U//FOUO) A BPS that protects a Security Enclave or Security Zone of a Core Node, or of a Client Node that supports External Operational Managers, shall block (1) all instant messaging protocols and (2) all voice-over-Internet Protocol service. [DRV KRD 2142] {P-R-S-T}

(U//FOUO) The following three requirements implement VPN connections to core nodes:

**CI2-SAR-3.2.4.1h** (U//FOUO) A BPS that is a Component of a Core Node and connects that Node to another Core Node shall be able to establish a Type 1 KPC, as needed to protect the communications between those Nodes. [DRV KRD 1062] {P-R-S}

**CI2-SAR-3.2.4.1i** (U//FOUO) A BPS that is a Component of a Core Node and connects that Node to a non-Core Client Node that serves a Manager, shall be able to establish both (1) a PKI-based KPC using DoD Credentials and (2) a Type 1 KPC, as needed to protect the communications between those Nodes. [DRV KRD 1062] {R}

(U//FOUO) The preceding requirement applies to instances of BPS-OME in a PRSN, and the following requirement applies to instances of BPS-PDE in a PRSN, as described in the "Nodal Structures" section.

**CI2-SAR-3.2.4.1j** (U//FOUO) A BPS that is a Component of a PRSN and connects that Node to a Client Node that serves a KOA Agent shall be able to establish (1) both a PKI-based KPC and a Type 1 KPC or (2) only a PKI-based KPC, as needed to protect the communications between the Nodes. [KRD NEW] {R}

### 3.2.4.2 (U) Guards

(U//FOUO) A guard is a BPS that primarily prevents unauthorized disclosure of data from one domain to another. However, a guard might also protect the data integrity, availability, or general system integrity of one system from threats posed by connecting to the other system. Systems that perform guard functions are sometimes called "filters".

**CI2-SAR-3.2.4.2a** (U//FOUO) Components operating at different classification levels shall interconnect only through a high-assurance Guard. [DRV KRD 2134, 2135] {P-R-S}

# 4 (U) NODAL STRUCTURES

(U//FOUO) CI-2 has four basic types of physically separate nodes—Client Nodes, PRSNs, PSNs, and the CSN—as illustrated by Figures 2 and 3. This section describes each of the node types, but concentrates mostly on the structures and functions of PRSNs and their interfaces with other nodes.

**CI2-SAR-4a** (U//FOUO) The functions of each Node shall be implemented by hardware and software systems that are physically separate from all other Nodes. [KRD 1370] {Z}

## 4.1 (U) Client Nodes

(U//FOUO) Client Nodes are information systems through which users interact with PRSNs. The types of components and interfaces that comprise a Client Node vary depending on the KMI role that is played by the node's user. A user accesses the system in one of the several manager roles or in the KOA Agent role.

**CONTROL** (U//FOUO) **EBRU-1 Remote Access for User Functions (Confidentiality)**. "All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session-level encryption equals or exceeds the robustness established in [controls that require encryption to provide confidentiality for data in transit]. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected. [DoDI8500.2]"

**CI2-SAR-4.1a** (U//FOUO) All remote access to the KMI shall be mediated through a managed Access Control point, such as a remote access server in a Security Zone. [KRD 2128] {R}

(U//FOUO) The EBRU requirement is further implemented by several requirements in other sections in this *Security Architecture* and in Volume 2.

### 4.1.1 (U) Client Nodes Serving Managers

(U//FOUO) Operational and administrative managers use Client Nodes to securely communicate with PRSNs in support of system management activities. All Client Nodes that serve KMI managers need to be protected in accordance with Volume 2 and this "Nodal Security Architecture" section. Client Nodes that serve internal managers are inside the more strongly protected Internal Management Security Perimeter (see Figure 3) and must be protected according to additional, stringent security requirements for core nodes.

(U//FOUO) **EBRP-1 Remote Access for Privileged Functions (Confidentiality)**. "Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the [Information Assurance Manager] reviews the log for every remote session. [DoDI8500.2]" [KRD 2125, 2126]

(U//FOUO) DoD Instruction 8500.2 defines the Information Assurance Manager (IAM) as "The individual responsible for the information assurance program of a DoD information system or organization. While the term [Information Assurance Manager] is favored within the Department of Defense, it may be used interchangeably with the IA title Information Systems Security Manager (ISSM)." The IAM is also mentioned in the ECPA-1 control that is quoted in the "Role-Based Access Control" section of this *Security Architecture*. However, the IAM role, which obviously encompasses a very broad range of duties, is not directly implemented by any single role in the KMI role-based access control architecture. Instead, some of the duties of the IAM role are divided among multiple internal administrative management roles in KMI, and other IAM duties are outside the scope of this architecture.

**CI2-SAR-4.1.2a** (U//FOUO) The KMI shall use KPCs (per DoDI 8500.2, EBRP-1 [DoDI8500.2]) to secure connections between a remote Manager Client and a Component of a Core Node. [DRV KRD 2125] {C-R}

(U//FOUO) Additional requirements for connecting remote managers are specified in the "Protected Channels" section.

**CI2-SAR-4.1.2b** (U//FOUO) The KMI shall record for Audit each session between a remote Manager Client and a Component of a Core Node. [DRV KRD 2126] {C-R}

(U//FOUO) Additional requirements for auditing management sessions are specified in the "Audit Services" section of Volume 2.

### 4.1.2 (U) Client Nodes Serving KOA Agents

(U//FOUO) Clients that serve KOA Agents are outside the External Management Security Perimeter (see Figure 3), but the KMI provides the following security services that benefit KOA Agents.

- (U//FOUO) **System availability.** The KMI protects PRSN, PSN, and CSN resources to ensure that KMI products and services authorized for KOA Agents are accessible and usable upon demand by those users.

- (U//FOUO) **Data integrity and origin authentication.** The KMI enables KOA Agents to verify the origin and integrity of data products that the system provides to those users.

(U//FOUO) The clients used by KOA Agents need to be able to perform the network communication protocols through which PRSNs provide access to products and services. This includes being able to establish KPCs by which clients connect to PRSNs (see "Protected Channels for PRSNs" section below); at a minimum, this means performing TLS functions using a server-side X.509 public-key certificate.

(U//FOUO) The products available to a KOA Agent are (1) products that have previously been requested or authorized for that the agent's account by a manager and (2) library resources that are available to all accounts. The general mechanism for providing data integrity and data origin authentication for those products is a cryptographic digital signature. To take advantage of those security services, clients used by KOA Agents may need to be able to verify digital signatures,

including performing any necessary PKI functions, such as obtaining and using public-key certificates and certificate revocation lists.

### 4.1.3 (U) Client Nodes Serving Devices

(U//FOUO) Some user devices are equipped with Client Node functionality that enables them to access PRSNs to retrieve cryptographic products that have been wrapped for the devices. The security services provided by the KMI to such devices, and the KPC requirements that the devices need to meet, are similar to those for client nodes serving KOA Agents.

## 4.2 (U) Primary Services Nodes

(U//FOUO) From the perspective of a user that is supported by a Client Node, PRSNs are servers that offer interfaces from which to obtain KMI products and services. PRSNs provide authorized users with keying material for Type 1 cryptographic systems and provide management services that support the life cycle of that material.

**CI2-SAR-4.2a** (U//FOUO) KMI CI-2 shall implement PRSNs that supply products and related, life-cycle services for Type 1 cryptographic systems. [DRV KRD 1180] {R}

### 4.2.1 (U) PRSN Domains, Enclaves, and Zones

(U//FOUO) Each PRSN is divided into security enclaves that provide separation between specific security domains, including the domain that operates at the unclassified level and the domain that operates at the U.S. Secret level:

- (U//FOUO) **Unclassified domain.** This domain includes registered users that the U.S. Government has authorized to receive KMI credentials for use in unclassified environments. This user population includes human users who are U.S. Federal Government employees; state and local government employees; government contractors; representatives of international organizations; and representatives of foreign governments that are U.S. allies or form coalitions with the U.S. This population also includes registered user devices that are under the control of those people and their organizations. (See definitions in Volume 2.)

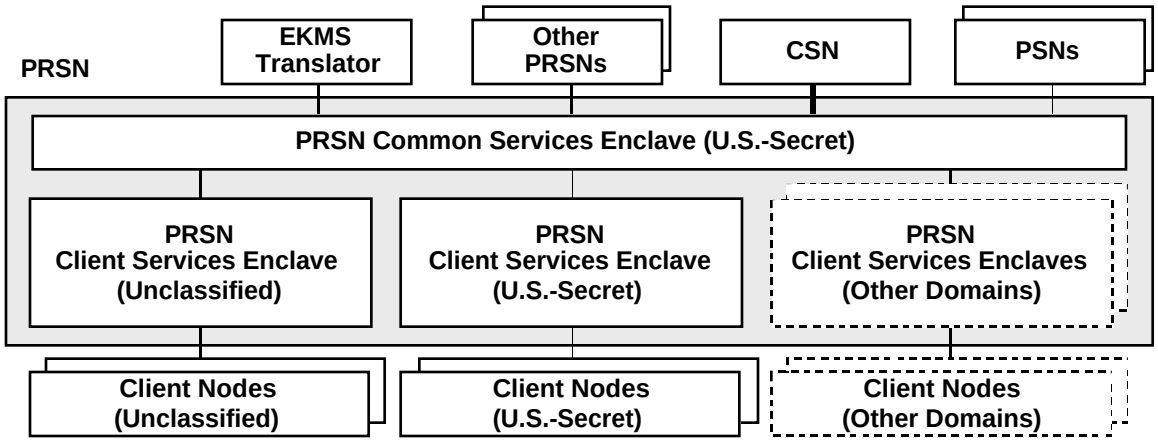
- (U//FOUO) **U.S.-Secret domain**. This domain includes registered users that the U.S. Government has authorized to receive KMI credentials for use in U.S.-Secret environments. The human users in this domain all have a U.S. Secret clearance; otherwise, this user population in this domain may be nearly as diverse as in the unclassified domain.

- (U//FOUO) **Other domains**. Depending on KMI operational requirements, domains could be configured at the unclassified or Secret levels for CCEB, NATO, or coalition users.

(U//FOUO) PRSN enclaves are divided into zones that provide defense-in-depth for accepting connections and processing transactions, and also provide separation between system components and between functions of differing sensitivity. Boundary protection suites limit client access to PRSNs and mediate communication between PRSNs and other nodes, between enclaves within PRSNs, and between zones within enclaves.

(U//FOUO) This *Security Architecture* uses security enclaves as modular building blocks that enable a PRSN to serve a variable number of client domains. As illustrated by Figure 7, each PRSN has a Common Services Enclave and some number of Client Domain Enclaves. The Common Services Enclave operates at the U.S. Secret level and performs functions that cannot or should not be replicated for each of the client domains, or that can be performed more efficiently or effectively when centralized than when distributed.

**Figure 7. (U) KMI PRSN Client Domains**




**UNCLASSIFIED//FOUO**

(U//FOUO) Each PRSN is also expected to have an enclave to serve Client Nodes operating at an Unclassified level (e.g., computers on NIPRNET and the public Internet ) and an enclave to serve clients operating at the U.S.-Secret level (e.g., computers on SIPRNET). Each PRSN may have additional enclaves to serve Client Nodes operating in other security domains.

### 4.2.2 (U) PRSN Service Redundancy and Data Replication

(U//FOUO) A major objective of KMI's nodal architecture is to ensure continued availability of service for a user by providing redundant points of service (i.e., service at two or more PRSNs as illustrated by Figure 2) without requiring the user to have multiple client devices,.

**CI2-SAR-4.2.2a** (U//FOUO) **Replication of points of service**. The KMI shall enable a User's Client Node to obtain all products and services for which the User is authorized, from any PRSN that has an appropriate Security Enclave. [DRV KRD 2092] {P-R-S-T}

(U//FOUO) Therefore, the KMI also has the objective of eliminating the need for a user to enter data repetitively.

**CI2-SAR-4.2.2b** (U//FOUO) **Replication of service data**. The KMI shall enable each User's Client Node to be serviced by all appropriate PRSN Security Enclaves consistent with network connectivity and Access Control restrictions such as classification; and, in support of this requirement, the KMI shall ensure that all data needed to meet functional, security, and availability requirements is made available to all such Enclaves. [DRV KRD 1905] {P-R-S-T}

(U//FOUO) The KMI needs to replicate data between enclaves that are in different PRSNs but in the same security domain. Furthermore, some KMI functions require a unified view of activity in multiple domains, which implies that data must be replicated between KMI components that are in different domains, including between components that operate at different security levels. Thus, CI-2 is designed to satisfy the following general requirements for data replication:

**CI2-SAR-4.2.2c** (U//FOUO) **Replication with upgrade**. If the KMI design requires replicating data from a Component to another Component (or to a network) that operates at a higher level of classification, then the upgrade function shall take place via a Guard device approved by NSA for such functions, or shall use other NSA-approved mechanisms of equivalent assurance; but the KMI should be designed to minimize the need for such functions. [DRV KRD 1899, 1900] {P-R-S}

**CI2-SAR-4.2.2d** (U//FOUO) **Replication with downgrade**. If the KMI design requires replicating data from a Component to another Component (or to a network) that operates at a lower level of classification, then the downgrade function shall take place via a Guard device approved by NSA for such functions, or shall use other NSA-approved mechanisms of equivalent assurance; but the KMI should be designed to avoid the need for such functions. [DRV KRD 1900, 1900] {A-P-R-S}

**CI2-SAR-4.2.2e** (U//FOUO) The KMI shall be able to provide a Client Node with equivalent service at two or more PRSNs that have an appropriate Security Enclave, regardless of the Security Domain in which the Client Node operates. [DRV KRD 1905] {R}

**CI2-SAR-4.2.2f** (U//FOUO) The KMI shall replicate necessary authorized data within the same Security Domain—both between PRSNs and between Components in the same PRSN. [DRV KRD 1905, 1817, 1825] {R}

**CI2-SAR-4.2.2g** (U//FOUO) The KMI shall replicate necessary authorized data from one Security Domain to another—both between PRSNs, and between Components in the same PRSN—subject to data confidentiality requirements. [DRV KRD 1905, 1817, 1825] {R}

**CI2-SAR-4.2.2h** U//FOUO) The KMI shall provide Information Confidentiality Service (as required by the *Security Policy* [KMI2200V2]) for data replicated between Components. [DRV KRD 1026, 1903] {Z}

**CI2-SAR-4.2.2i** (U//FOUO) The KMI shall provide Information Integrity Service and related Data Origin or Peer Entity Authentication Service (as required by the *Security Policy* [KMI2200V2]) for data replicated between Components. [DRV KRD 1901, 1902] {Z}

(U//FOUO) To replicate data between the Common Services Enclave and other enclaves in a PRSN, KMI CI-2 incorporates guards.

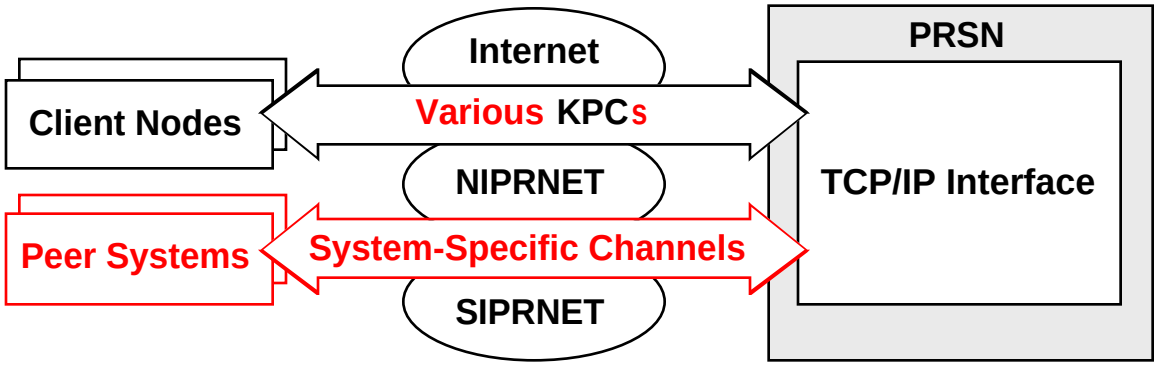
### 4.2.3 (U) PRSN Network Connectivity

(U//FOUO) Figure 8 illustrates that a PRSN supports Client Nodes via TCP/IP-based computer networks, including SIPRNET, NIPRNET, and the public Internet. PRSNs also connects to peer systems via those networks.

**DEFINITION** (U//FOUO) Peer System. An information system (other than the EKMS) that is external to the KMI and with which the KMI exchanges products and services that are needed to support KMI operations.

(U//FOUO) PSE architecture is described in this section, and some peer systems are discussed in the "Relationship to Existing Key Management Systems and External Support Systems" of Volume 1.

**Figure 8. (U) KMI PRSN Client and Peer System Connectivity**




**UNCLASSIFIED//FOUO**

(U//FOUO) Figure 8 also illustrates that a Client Node always connects to a PRSN through a KPC, and a PRSN connects to a peer system through a channel that is specific to the requirements of the two systems. ~~However, t~~The security services, mechanisms, and level of assurance required for the KPC these channels range from very robust to rudimentary, depending on (1) the purpose of the access and (2) the security domain in which the client or peer system operates. (See "Protected Channels for PRSNs" section above.)

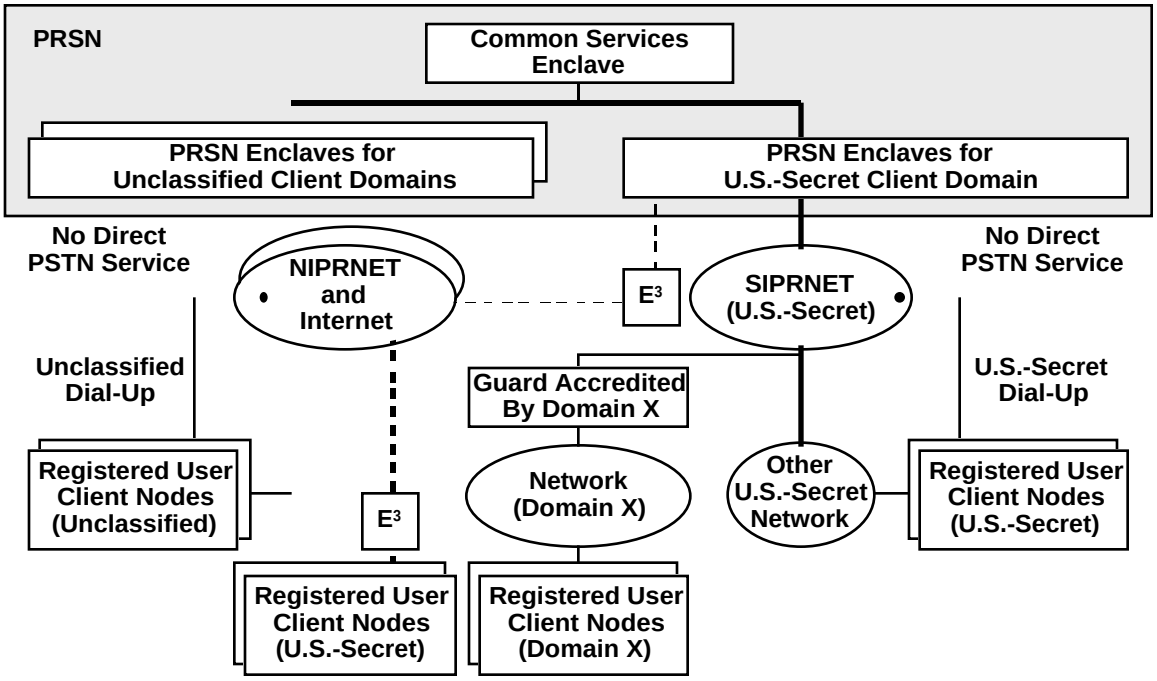
**CI2-SAR-4.2.3a** (U//FOUO) A PRSN shall support Client Node access via TCP/IP-based computer networks. [DRV KRD 1241, 1242, 2031] {C-R}

**CI2-SAR-4.2.3b** (U//FOUO) A PRSN shall support communications with Peer Systems via TCP/IP-based computer networks. [DRV KRD 1241, 1242, 2031] {R}

(U//FOUO) Figure 9 illustrates that clients operating at U.S. Secret can reach the U.S. Secret enclave of a PRSN in four ways:

- By connecting directly to SIPRNET.
- By connecting to other networks that operate at U.S. Secret and are connected to SIPRNET.
- By connecting through a SIPRNET dial-up server.
- By using end-to-end encryption to connect to SIPRNET via NIPRNET/Internet.

**Figure 9. (U) KMI PRSN Client Enclave Access**




**UNCLASSIFIED//FOUO**

(U//FOUO) Figure 9 also illustrates that clients operating at an unclassified level can access the Unclassified enclave of a PRSN in three ways (but clients operating at unclassified are not expected to use end-to-end encryption to connect via SIPRNET):

- By connecting directly to NIPRNET .
- By connecting via the public Internet either directly to a PRSN or through NIPRNET.
- By connecting through a NIRPNET dial-up server.

(U//FOUO) Regarding dial-up access, a PRSN does not support direct connection of Client Nodes via the PSTN. Although clients operating at U.S. Secret might use the PSTN to reach dial-up servers on some network and thereby connect to a PRSN, the dial-up servers are not provided by the KMI.

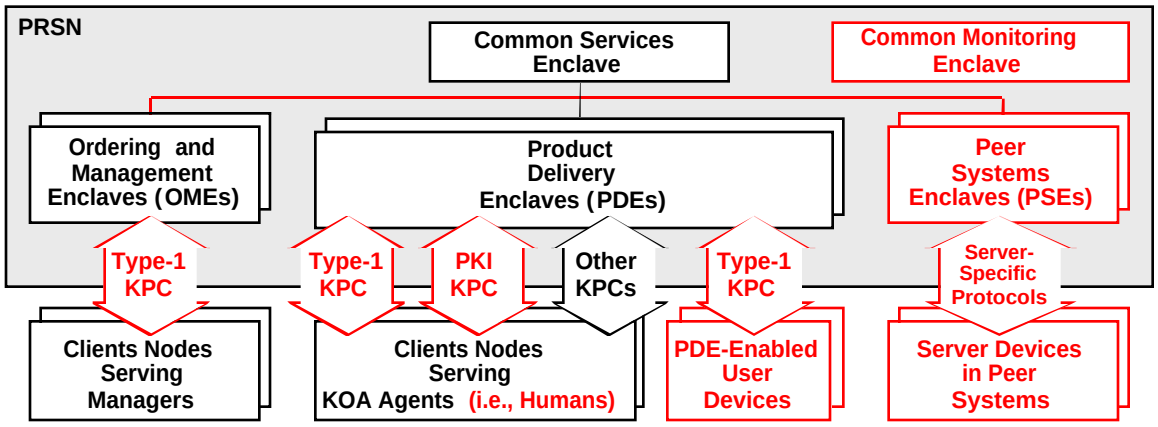
(U//FOUO) A PRSN does not have any enclaves that operate at a security level above Secret and, therefore, cannot directly serve Client Nodes that operate above Secret. Figure 9 illustrates that clients operating at a security level "X" that is higher than U.S. Secret, may connect to a PRSN indirectly, through a guard. However, the KMI does not provide such guards as part of the CI-2. For example, "Network (Domain X)" could be the Joint Worldwide Intelligence Community System (JWICS). The "Guard Accredited by Domain X" would need to be able to permit passage of the required KPCs and other KMI protocols, and would need to be provided and accredited for that purpose by the approving authorities of the JWICS domain.

### 4.2.4 (U) PRSN Security Enclaves

(U//FOUO) Figure 10 illustrates that a PRSN can have five types of security enclaves:

- (U//FOUO) **Ordering and Management Enclave (OME)**. The multiple OMEs serve Client Nodes operated by humans who are acting in KMI management roles.
- (U//FOUO) **Product Delivery Enclave (PDE)**. The multiple PDEs serve (a) Client Nodes operated by humans who are acting in the role of KOA Agent and (b) PDE-enabled devices.
- (U//FOUO) **Peer Systems Enclave (PSE)**. The multiple PSEs access the servers of other information infrastructures from which the KMI obtains needed operational data.
- (U//FOUO) **Common Services Enclave**. This single enclave~~s~~ does not directly serve Client Nodes but supports them indirectly through the OMEs and PDEs.
- (U//FOUO) **Common Monitoring Enclave**. This single enclave oversees the status of the PRSN by receiving and analyzing data from components of the other enclaves. (The Common Monitoring Enclave might be a separate enclave or be part of one of the other enclaves, depending on how monitoring is implemented in PRSNs.)

**Figure 10. (U) KMI PRSN Enclave Types**




**UNCLASSIFIED//FOUO**

(U//FOUO) In addition to the enclaves shown in Figure 10, a PRSN contains various guards. ~~The~~ Guards are used (1) to connect the Common Services Enclave to OMEs, ~~connect the Common Services Enclave to~~ PDEs, and PSEs (in the cases where the security domain of those enclaves differ from that of Common Services) and (2) to connect the Common Monitoring Enclave to the ~~other~~ PRSN components that are monitored.

**CI2-SAR-4.2.4a** (U//FOUO) All functionality of a PRSN shall be divided into two types of Components: [DRV KRD 1180, 1386, 1998] {R}

– (1) Security enclaves: OMEs, PDEs, PSEs, a Common Services Enclave, and a Common Monitoring Enclave (which might be part of one of the other enclaves, depending on how PRSNs are implemented).

– (2) Guards that mediate inter-enclave communications: PDE Guards, OME Guards, PSE Guards, and possibly a separate MON Guard if there is a separate Common Monitoring Enclave.

**CI2-SAR-4.2.4b** (U//FOUO) A Computer Platform that implements functions of a specific Guard in a PRSN shall be physically separate from Computer Platforms that implement other functions of the PRSN, including the functions of other Guards. [DRV KRD 1180, 1387, 1568] {R}

**CI2-SAR-4.2.4c** (U//FOUO) A Computer Platform that implements functions of a specific OME shall be physically separate from Computer Platforms that implement other functions of the PRSN, including the functions of other OMEs. [DRV KRD 1180, 1387, 1568] {R}

**CI2-SAR-4.2.4d** U//FOUO) A Computer Platform that implements functions of a specific PDE shall be physically separate from Computer Platforms that implement other functions of the PRSN, including the functions of other PDEs. [DRV KRD 1180, 1387, 1568] {R}

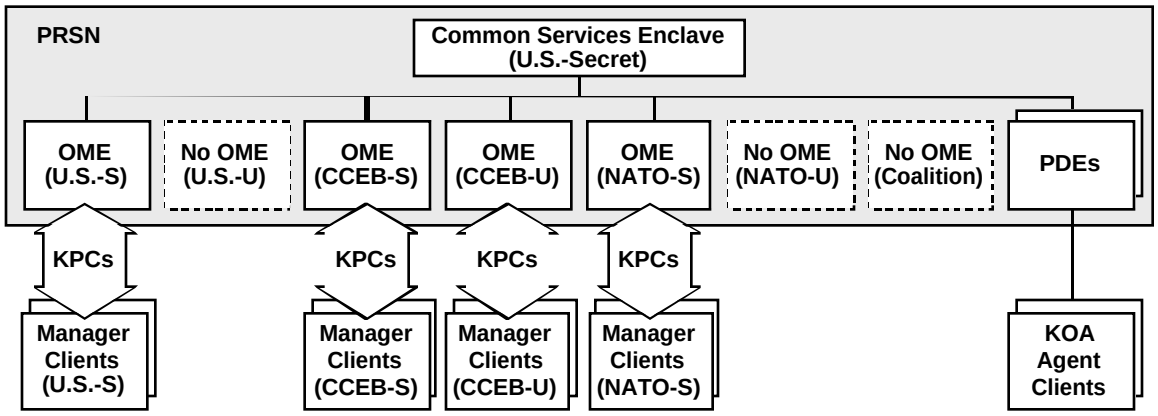
**CI2-SAR-4.2.4e** U//FOUO) A Computer Platform that implements functions of a specific PSE shall be physically separate from Computer Platforms that implement other functions of the PRSN, including the functions of other PSEs. [DRV KRD 1180, 1387, 1568] {R}

(U//FOUO) OMEs support complex operational functions of managers; PDEs only enable KOA Agents to retrieve encrypted products that a manager has previously ordered or authorized through an OME. Separating OME functions from PDE functions enables PDEs to be simpler than OMEs, which in turn simplifies requirements for the guards that connect PDEs to the Common Services Enclave. Minimizing the client population that needs access to the more complex and sensitive OMEs, and also further isolating the most sensitive PRSN functions in the Common Services Enclave, can further simplify security certification of PRSNs. Simplifying PDEs can also reduce their cost, which enables them to be replicated to serve separate communities within KMI's diverse population of Client Nodes.

(U//FOUO) PRSNs are intended to be able to support Client Nodes in multiple security domains, through multiple networks, and through multiple configurations of KPCs, thus requiring multiple OMEs and PDEs. However, there are many possible ways in which a PRSN could be configured to support the client population.

(U//FOUO) For example, Figure 11 illustrates that a CI-2 PRSN could be configured with OMEs to serve four of the domains listed in Table 6. If necessary, a PRSN could be expanded with additional OMEs for those domains, and also for other domains listed in Table 6.

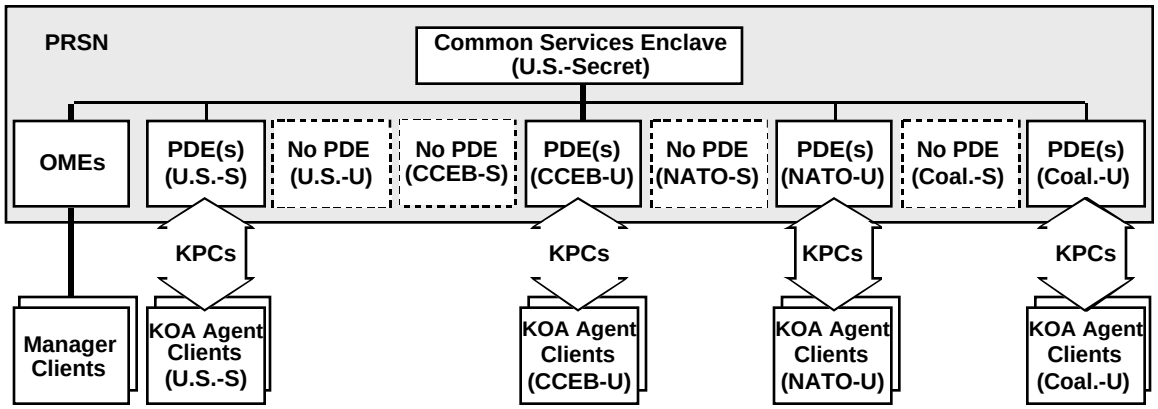
**Figure 11. (U) KMI PRSN OMEs Configuration Example**




**UNCLASSIFIED//FOUO**

(U//FOUO) Figure 12 illustrates that, for example, a PRSN could be configured with PDEs to serve the four domains listed in Table 7. If necessary, a PRSN could be expanded with additional PDEs for those domains or for other domains.

**Figure 12. (U) KMI PRSN PDEs Configuration Example**




**UNCLASSIFIED//FOUO**

(U//FOUO) Tables 6 and 7 describes the hypothetical configuration of OMEs and PDEs shown in Figure 12, which is based on assumptions explained by the notes accompanying the tables. In the two tables, each row describes one possible client-enclave-network-KPC combination through which a Client Node could connect to a PRSN.

**Table 6. (U) KMI PRSN OME Security Domains Configuration Example**

| 1. Client Type (Operational Security Level) | 2. Enclave Type (Operational Security Level) | 3. KPC Required (Security Level At Which Keyed) | 4. Internetworks Served (Operational Security Level) | 5. Security Levels Of Products That Can Be Ordered |
|---|---|---|---|---|
| Manager (U.S.-Secret) U.S. Only | OME (U.S.-Secret) U.S. Only | Type 1 (U.S.-Secret) | SIPRNET (U.S.-S)<br>NIPRNET (U.S.-U)<br>Public Internet (Coal.-U) | U.S.-U&S. CCEB-U&S<br>NATO-U&S<br>Coalition-U&S |
| Manager (U.S.-Unclas) * See Note 6-1 | No OME at this level | | | |
| Manager (CCEB-Secret) * See Note 6-2 | OME (CCEB-Secret) | Type 1 (CCEB-Secret) | SIPRNET (U.S.-S) ?<br>NIPRNET (U.S.-U) ?<br>Public Internet (Coal.-U) | CCEB-U&S<br>NATO-U&S<br>Coalition-U&S |
| Manager (CCEB-Unclas) * See Note 6-2 | OME (CCEB-Unclas) " | Type 1 (CCEB-Unclas) | SIPRNET (U.S.-S) ?<br>NIPRNET (U.S.-U) ?<br>Public Internet (Coal.-U) | CCEB-U<br>NATO-U<br>Coalition-U |
| Manager (NATO-Secret) * See Note 6-3 | OME (NATO-Secret) in CI-2. | Type 1 (NATO-Secret) | SIPRNET (U.S.-S) ?<br>NIPRNET (U.S.-U) ?<br>Public Internet (Coal.-U) | NATO-U&S<br>Coalition-U&S |
| Manager (NATO-Unclas) * See Notes 6-3,4 | No OME at this level in CI-2. | | | |
| Manager (Coalition-Secret) * See Note 5 | No OME at this level in CI-2. | | | |
| Manager (Coalition-Unclas) * See Notes 5 | No OME at this level in CI-2. | | | |
| Manager (U.S.-Top Secret) * See Notes 6 | No OME at this level in CI-2. | | | |

**UNCLASSIFIED//FOUO**

(U//FOUO) The five columns in each table have the following content:

- **Column 1**. Lists the type of client and, in parentheses, the security domain in which the client operates. All clients in Table 6 serve users that are playing a management role, and all clients in Table 7 serve users that are playing the KOA Agent role.

  – (U//FOUO) **U.S. domains.** Managers and KOA Agents in these domains would all be U.S. Government employees.
  – (U//FOUO) **CCEB domains**. Managers in these domains would all be authorized representatives of national governments of CCEB nations.
  – (U//FOUO) **NATO domains**. Managers in these domains would all be authorized representatives of national governments of NATO nations.
  – (U//FOUO) **Coalition domains**. Managers in these domains would all be authorized representatives of national governments of non-CCEB, non-NATO nations.

- **Column 2**. Lists (1) the type of enclave provided at PRSNs to support the client type in column 1 and (2), in parentheses, the security domain in which the enclave operates. All the enclaves in Table 6 are OMEs, and all the enclaves in Table 7 are PDEs.

- **Column 3**. Lists the type of KPC required between the client and the enclave

  – **Type 1**. The KPC is based on IPsec [HAIPIS] and Type 1 key as specified in the "Protected Channels" section.
  – **PKI**. The KPC is based on TLS [RFC2246] and PKI credentials as specified in the "Protected Channels" section.

- **Column 4**. Lists the long-haul internetworks on which the enclave offers a point of connection. For those cases where there is doubt that connections will be offered in CI-2, the table has a "?" after the network name, and there is an explanatory note below the table.

- **Column 5**. In Table 6, this column lists the products that can be managed through the OME. In Table 7, this column lists the products that can be delivered through the PDE.

(U//FOUO) Column 1 of Table 6 references the following notes:

- **Note 6-1**. A U.S.-only Unclassified OME might not be needed. Instead, U.S. Managers operating at Unclassified could access a CCEB-Unclassified OME.

- **Note 6-2**. CCEB nations do not currently have connection approval for the U.S. SIPRNET or NIPRNET. Therefore, this OME need serve SIPRNET and NIPRNET only if CCEB Managers have access to U.S.-controlled clients on those networks.

- **Note 6-3**. NATO nations do not currently have connection approval for the U.S. SIPRNET or NIPRNET. Therefore, this OME need serve SIPRNET and NIPRNET only if NATO Managers have access to U.S.-controlled clients.

- **Note 6-4**. A NATO-Unclassified OME on the Public Internet might not be needed. Instead, U.S. and CCEB Managers of NATO-Unclassified products could use any U.S., CCEB, or NATO Manager Client; and NATO Managers could use a NATO-Secret Manager Client.

- **Note 6-5**. No OME is needed at these levels in CI-2 because Coalition partners (i.e., non-CCEB/non-NATO) are not expected to be permitted to be enrolled as Managers in CI-2.

- **Note 6-6**. CI-2 will not serve Manager Clients at the Top Secret level, but a later KMI capability increment might do so.

**Table 7. (U) KMI PRSN PDE Security Domains Configuration Example**

| 1. Client Type (Operational Security Level) | 2. Enclave Type (Operational Security Level) | 3. KPC Required | 4. Internetworks Served (Operational Security Level) | 5. Products That Can Be Delivered |
|---|---|---|---|---|
| KOA Agent (U.S.-S) | PDE (U.S.-Secret) | PKI Class 3 or higher | SIPRNET (U.S.-S) | All wrapped products. |
| | | Type 1 (U.S.-Secret) | NIPRNET (U.S.-U) | |
| | | Type 1 (U.S.-Secret) | Public Internet (Coal.-U) | |
| KOA Agent (U.S.-U) | PDE (CCEB-Unclas) | PKI Class 4 | NIPRNET (U.S.-U) | All wrapped products |
| | | | Public Internet (Coal.-U) | |
| KOA Agent (CCEB-U) | | PKI Class 4 or equiv. | Public Internet (Coal.-U) | |
| KOA Agent (U.S.-U) | PDE (NATO-Unclas) | PKI Class 2 or higher | NIPRNET (U.S.-U) | All wrapped products |
| | | | Public Internet (Coal.-U) | |
| KOA Agent (CCEB-U) | | PKI Class 2 or higher | Public Internet (Coal.-U) | |
| KOA Agent (NATO-U) | | PKI Class 2 or higher | Public Internet (Coal.-U) | |
| KOA Agent (U.S.-U) | PDE (Coalition-Unclas) | Other | NIPRNET (U.S.-U) | All wrapped products. |
| | | | Public Internet (Coal.-U) | |
| KOA Agent (CCEB-U) | | Other | Public Internet (Coal.-U) | |
| KOA Agent (NATO-U) | | | | |
| KOA Agent (Coal.-U) | | | | |

**UNCLASSIFIED//FOUO**

#### 4.2.4.1 (U) PRSN Ordering-and-Management Enclaves

(U//FOUO) A manager connects to an OME either (1) to request products and services for delivery through PDEs to KOA Agents or (2) to perform related operational and administrative duties, depending on the authorizations held by the manager. Users are not permitted to connect to OMEs in the KOA Agent role.

(U//FOUO) Ordering is the process by which requests are made for the generation and distribution of products and by which the KMI responds to those requests and controls those processes. This architecture assumes that ordering information and other data that an OME exchanges with a manager is never classified higher than Secret.

(U//FOUO) Figure 10 illustrates that managers connect their Client Nodes to OMEs through a KPC based on Type-1 cryptography. The KPC involves a PKI-based ~~TLS KPC~~ channel that is layered above a Type 1 channel ~~KPC~~ (see Figure 5 in "Protected Channels" section above). The ~~KPCs~~ two channels provide the following services for the client connections:

- (U//FOUO) **Authentication.** The two ~~KPCs~~ channels provide different, complementary forms of peer-entity authentication. (1) The Type 1 ~~KPC~~ channel authenticates to the OME server that the Client Node is a member of the Type 1 community, and similarly authenticates the OME server to the client. (2) The PKI-based ~~TLS KPC~~ channel authenticates the manager's registered user identity to the OME, and similarly authenticates the OME to the manager. The identities are stated in the PKI Credentials used for the ~~TLS~~ security association.

- (U//FOUO) **Data confidentiality.** One or both of the ~~KPCs~~ two channels is configured to provide data confidentiality service for the ordering information and other data that is exchanged between the client and the OME.

- (U//FOUO) **Data integrity.** One or both of the ~~KPCs~~ two channels is configured to provide data integrity service for the data that is exchanged.

(U//FOUO) The following requirements establish a basis for OMEs, and other requirements for OMEs are stated in Volume 1.

**CI2-SAR-4.2.4.1a** (U//FOUO) An OME shall be able to receive and process product and service requests from Client Nodes operated by Managers. [DRV KRD 1180] {C-R}

**CI2-SAR-4.2.4.1b** (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to cause selected OMEs temporarily to cease accepting and processing selected types of requests from selected Client Nodes. [DRV KRD 1016] {C-R}

**CI2-SAR-4.2.4.1c** (U//FOUO) The Common Services Enclave of a PRSN shall provide Access Control data and product catalog data to each OME in the PRSN, but only as needed for the Security Domain that is authorized to connect to that OME. [DRV KRD 1645] {R}

(U//FOUO) The following requirements specify the security domains that can be served by OMEs in a CI-2 PRSN:

**CI2-SAR-4.2.4.1d** (U//FOUO) In a PRSN, each OME shall operate in a single Security Domain at a single security level. [DRV KRD 1180, 1386, 1998] {R}

**CI2-SAR-4.2.4.1e** (U//FOUO) A PRSN shall be able to concurrently support Client Node access with multiple OMEs, such that each OME operates in a specified Security Domain. [DRV KRD 0504, 1386, 1998] {R}

**CI2-SAR-4.2.4.1f** (U//FOUO) A PRSN shall be able to be configured with OMEs to support one or more of the following Security Domains: [DRV KRD 0504, 1180, 1386] {R}
- (1) U.S.-Secret.
- (2) U.S.-Unclassified
- (3) CCEB-Secret.
- (4) CCEB-Unclassified.
- (5) NATO-Secret.
- (6) NATO-Unclassified.
- (7) Coalition-Secret.
- (8) Coalition-Unclassified.

**CI2-SAR-4.2.4.1j** (U//FOUO) A PRSN shall be able to be modularly configured with OMEs, or reconfigured with additional or fewer OMEs, to have from one to twenty (20) OMEs. [DRV KRD 0504, 1180, 1386] {R}

(U//FOUO) The following requirements specify the networks on which PRSNs in CI-2 shall be able to provide an OME point of presence:

**CI2-SAR-4.2.4.1k** (U//FOUO) An OME operating at a Secret level shall be able to be connected to and support Client Node access (1) via SIPRNET or some other network operating at that Secret level or (2), by using NSA-approved end-to-end encryption, via NIPRNET, the public Internet, or some other network operating at an unclassified level. [DRV KRD 1241, 1242, 2031] {R}

**CI2-SAR-4.2.4.1l** (U//FOUO) An OME operating at an unclassified level shall be able to be connected to and concurrently support Client Node access via NIPRNET, the public Internet, or some other network operating at that unclassified level. [DRV KRD 0504, 1242, 2031] {R}

**CI2-SAR-4.2.4.1m** (U//FOUO) The connection of a Client Node to an OME shall be through (1) a PKI-based TLS KPC, using KMI Management Credentials [NSAKMICP], layered over (2) a Type 1 KPC using the HAIPE interoperability specification [HAIPIS]. [DRV KRD 1026, 1371] {C-R}

### 4.2.4.2 (U) PRSN Product Delivery Enclaves

(U//FOUO) KOA Agents connect to PDEs to receive products and services that have previously been ordered or authorized for them by managers. (Users that access OMEs as managers might also access PDEs as KOA Agents, because managers might need to receive products and services that have been ordered for them by other managers.) A PDE does not accept new orders; it only services requests to deliver pre-generated material or accepts requests to generate pre-authorized material, such as in rekey operations. A PDE is a essentially a store-and-forward server that relays messages between the Common Services Enclave and Client Nodes; a PDE does not support the more complex forms of client-server interaction that an OME supports.

(U//FOUO) Figure 10 illustrates that Client Nodes connect to PDEs through various types of KPCs. Each PDE offers service through just one kind of KPC configuration: (1) some PDEs use a ~~PKI-based TLS KPC that is layered above a~~ the same kind of Type 1 KPC that is used for OMEs; (2) some use only a PKI-based KPC; and (3) some may support disadvantaged clients through KPCs based on less robust technology (as discussed in "Protected Channels for PRSNs" section above). However, the type and strength of the KPC is less critical in a PDE than in an OME, because essential security services for product delivery are provided by product packaging and not by KPC mechanisms. A KPC that connect a PDE to a Client Node of a KOA Agent provides the following security services for the connection:

- (U//FOUO) **Authentication.** A PDE must be able to learn the user's identity for the purpose of determining which key material to deliver to the user, and must be able to authenticate that identity for product tracking and for countering denial-of-service attacks by clients that falsely connect. (1) A Type 1 KPC, if configured, authenticates to the PDE server that the Client Node is a member of the Type 1 community, and similarly authenticates the PDE server to the client. (2) A PKI-based TLS KPC can authenticate the KOA Agent's registered user identity to the PDE and can similarly authenticate the PDE to the agent. However, if the client is disadvantaged, some mechanism other than a PKI-based TLS KPC may be used to authenticate the agent's identity.

- (U//FOUO) **Data confidentiality.** This architecture assumes that all key material that a PDE receives from the Common Services Enclave and delivers to a Client Node is encrypted, and that the material can be decrypted only by the recipient intended by the PRSN. Furthermore (per [CNSSI40xx]), the delivered material is (1) unclassified and (2) not required to be treated as COMSEC material. However, some labeling and addressing data associated with the material may not be encrypted and may need protection for purposes of operational security. A KPC can provide data confidentiality service for such unencrypted data.

- (U//FOUO) **Data integrity.** Although product packaging can provide end-to-end data integrity service for delivered key material, additional data integrity service provided by a KPC can counter denial-of-service attacks in cases where the user is only relaying the package between the PDE and the intended final recipient.

(U//FOUO) A PRSN needs to be able to establish such additional PDEs rapidly. The additional domains that will need to be supported cannot be predicted with certainty, but the following are examples of domains that the KMI may need to support.

- (U//FOUO) **U.S. Non-Federal.** The KOA Agents include both persons who are authorized representatives of U.S. state and local government.

- (U//FOUO) **Other U.S. allies, partners, and coalitions.** The KOA Agents are authorized representatives and devices belonging to national governments of non-CCEB and non-NATO countries, and of countries that are members of various coalitions that includes the U.S.

- (U//FOUO) **International organizations.** The KOA Agents are representatives and devices belonging to various non-government and quasi-government organizations.

(U//FOUO) The following requirements establish a basis for PDEs, and other requirements for PDEs are stated in Volume 1.

**CI2-SAR-4.2.4.2a** (U//FOUO) A PDE shall be able to (1) deliver pre-generated key material to Client Nodes and (2) receive and process requests from Client Nodes to generate pre-authorized products (i.e., products previously authorized by a Manager through an OME). [DRV 1180] {C-R}

**CI2-SAR-4.2.4.2b** (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to cause selected PDEs temporarily to cease delivering products to, and accepting and processing selected types of requests from, selected Client Nodes. [DRV KRD 1016] {R}

**CI2-SAR-4.2.4.2c** (U//FOUO) The Common Services Enclave of a PRSN shall provide Access Control data and product catalog data to each PDE in the PRSN, but only as needed for the Security Domain that is authorized to connect to the PDE. [DRV KRD 1645] {R}

(U//FOUO) The following requirements specify the security domains that can be served by PDEs in a CI-2 PRSN:

**CI2-SAR-4.2.4.2d** (U//FOUO) In a PRSN, each PDE shall operate in a single Security Domain at a single security level. [DRV KRD 1180, 1386, 1998] {R}

**CI2-SAR-4.2.4.2e** (U//FOUO) A PRSN shall be able to concurrently support Client Node access with multiple PDEs, such that each PDE operates in a specified Security Domain. [DRV KRD 1386, 1998] {R}

**CI2-SAR-4.2.4.2f** (U//FOUO) A PRSN shall be able to be configured to include PDEs that operate in one or more of the following Security Domains: [DRV KRD 0504, 1180, 1386] {R}

- (1) U.S.-Secret.
- (2) U.S.-Unclassified
- (3) CCEB-Secret.
- (4) CCEB-Unclassified.
- (5) NATO-Secret.
- (6) NATO-Unclassified.
- (7) Coalition-Secret.
- (8) Coalition- Unclassified.

**CI2-SAR-4.2.4.2g** (U//FOUO) A PRSN shall be able to be modularly configured with PDEs, or rapidly reconfigured with additional or fewer PDEs, to have from one to forty-two (42) PDEs. [DRV KRD 0504, 1180, 1386] {R}

(U//FOUO) The following requirements specify the networks on which PRSNs in CI-2 provide a PDE point of presence:

**CI2-SAR-4.2.4.2h** (U//FOUO) A PDE operating at a Secret level shall be able to be connected to and support Client Node access (1) via SIPRNET or some other network operating at that Secret level or (2) (by using NSA-approved end-to-end encryption) via NIPRNET, the public Internet, or some other network operating at an unclassified level. [DRV KRD 1241, 1242, 2031] {R}

**CI2-SAR-4.2.4.2i** (U//FOUO) A PDE operating at an unclassified level shall be able to be connected to and concurrently support Client Node access via NIPRNET, the public Internet, or some other network operating at that unclassified level. [DRV KRD 1242, 2031] {R}

**CI2-SAR-4.2.4.2j** (U//FOUO) The connection of a Client Node to a PDE shall be through a KPC that is configured in accordance with the requirements and capabilities of the PDE's Security Domain and its client population. [DRV KRD 1026] {C-R}

(U//FOUO) The following requirement implements the protections described in Table 5:

**CI2-SAR-4.2.4.2k** (U//FOUO) A PRSN shall be able to be configured to include PDEs that each support one of the following types of KPCs for Clients: [DRV KRD 0572, 0574, 1321, 1026] {C-R}

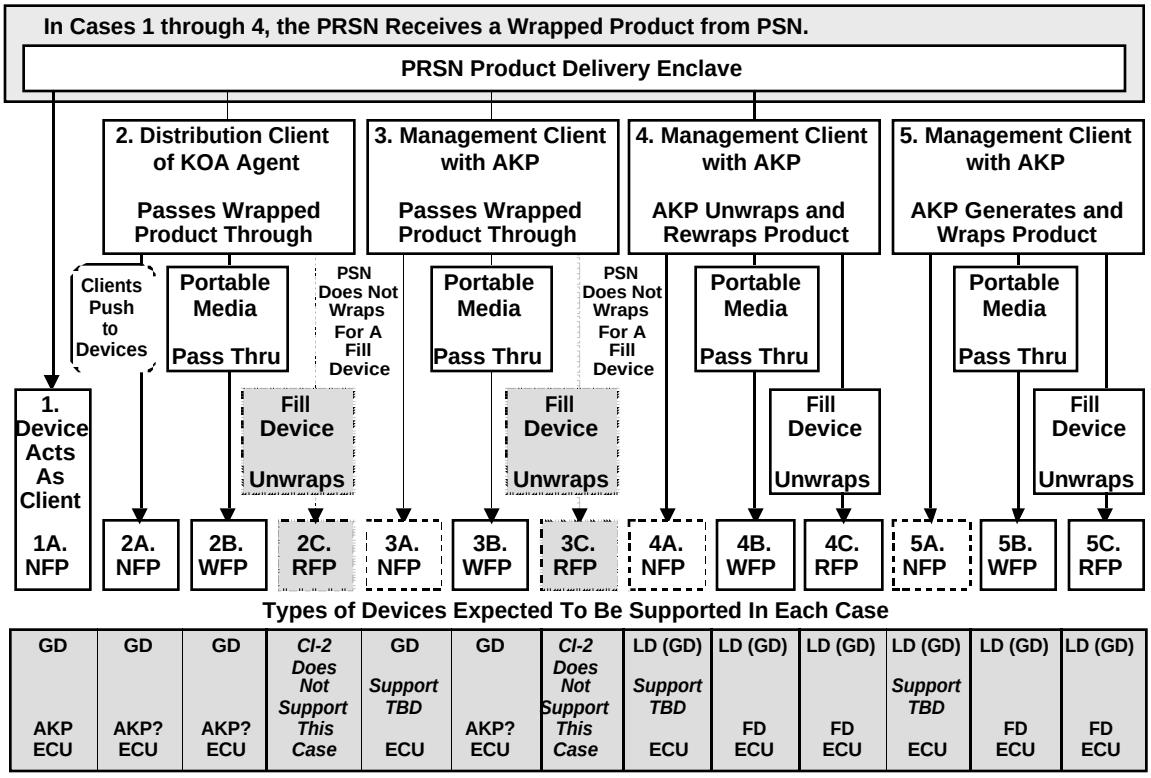
- (1) A TLS KPC that is established with Class 3 (or higher) PKI Credentials [DoDX509CP] for both the PRSN server and the Client's User, and which is layered over a HAIPIS KPC using Type 1 credentials [HAIPIS]

- (2) A TLS KPC that is established with Class 2 (or higher) PKI Credentials [DoDX509CP], or equivalent credentials, for both the PRSN server and the Client's User.
- (3) A TLS KPC that is established with Class 2 (or higher) PKI Credentials [DoDX509CP] for the PRSN server, and an identifier-password authentication mechanism for the Client's User.

#### 4.2.4.3 (U) Fill Ports and Distribution Paths

(U//FOUO) When a Client Node has connected to a PDE and received a wrapped product, or when an AKP has generated and wrapped a product, the product is then distributed to the user device for which the product is intended via one of the several different types of paths that are illustrated in Figure 13. These paths are described in detail, with their related requirements, in the "Key Fill" and "Delivery" sections of Volume 1.

**Figure 13. (U) KMI Product Distribution Paths for User Devices**




**UNCLASSIFIED//FOUO**

(U//FOUO) In brief, there are five basic types of distribution paths, and each of those can use one or more of three types of fill ports in user devices.

- (U//FOUO) Network-Fill Port (NFP). This type of fill port connects to PDEs and to Client Nodes, and it accepts OTNK fill.

- (U//FOUO) Wrapped-Fill Port (WFP). This type of port connects to portable media, including fill devices used to transport wrapped products, and it may accept OTNK, EKMS 217, or BLACK fill.

- (U//FOUO) RED-Fill Port (RFP). This type of port connects to fill devices that unwrap products, and it accepts RED fill.

(U//FOU) For each supported path, the box at the bottom of ~~the figure~~ Figure 13 lists which of the three basic types of user devices—AKP, ECU, and fill device (FD)—are supported on that path. Some paths have "AKP?" to indicate that it has yet to be determined whether or not CI-2 will support AKPs on the path.

(U//FOUO) The box at the bottom of Figure 13 also lists the type of identity registration that a user device must have to use the path: "GD" indicates a globally registered general device, and "LD" indicates a locally registered limited device. (These device types—"General Device" and "Limited Device"—are defined in the "Registered Users" section of Volume 2.) 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 a user device that is treated by the management client as a limited device, even though it has been registered as a general device.

(U//FOUU) Some of the combinations of path type and port type are special cases. First, CI-2 does not support paths 2C and 3C (which would use a RED-fill port on a user device) because in CI-2 there are no fill devices that are general devices for which the PSN can wrap key. Second, it has yet to be determined whether or not CI-2 will supports paths 3A, 4A, and 5A.

#### 4.2.4.4 (U) Peer Systems Enclaves

(U//FOUO) PSEs implement functionality needed for the KMI to communicate with peer 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 revocation status services. This may require the PSE to act as client to access a directory server to get certificates and CRLs, or to access an On-Line Certificate Status Protocol (OCSP) server.

(U//FOUO) In addition to security requirements stated in this volume, safeguards for interoperation with external systems and protections for externally generated information are stated in the following sections of Volume 2: "Non-KMI Systems", "Information Sensitivity", "Control of Import and Export", and "Extend Trust and Outside Users".

(U//FOUO) The following requirements establish a basis for PSEs:

**CI2-SAR-4.2.4.4a** (U//FOUO) A PSE shall be able to initiate communication associations to access specified Peer Systems for the purpose of obtaining needed products and services from those systems or otherwise exchanging data with those systems. [DRV 1023, 1359] {R}

**CI2-SAR-4.2.4.4b** (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to cause selected PSEs temporarily to cease accessing selected Peer Systems. [DRV KRD 1016] {R}

**CI2-SAR-4.2.4.4c** (U//FOUO) A PSE shall not establish any communication association that is initiated by a Peer System. [DRV 1068] {R}

(U//FOUO) All the security domains that will need to be supported by CI-2 PSEs cannot be predicted with certainty, but support is expected to be needed for the following:

- (U//FOUO) **U.S. Federal**. The KMI is expected to connect to some systems operated or controlled by DoD Services and agencies and by some non-DoD Federal agencies.
- (U//FOUO) **U.S. Non-Federal.** The KMI may need to obtain services and data from systems belonging to some U.S. state and local governments.
- (U//FOUO) **Allies, partners, and coalitions.** The KMI may need to obtain services and data from systems belonging to some other national governments or groups of governments.
- (U//FOUO) **International organizations.** The KMI may need to obtain services and data from systems belonging to some quasi-government and non-government organizations.

(U//FOUO) The following requirements specify the security domains in which PSEs of a CI-2 PRSN need to be able to operate:

**CI2-SAR-4.2.4.4d** (U//FOUO) Each PRSN PSE shall operate in a single Security Domain at a single security level. [DRV KRD 1180, 1386, 1998] {R}

**CI2-SAR-4.2.4.4e** (U//FOUO) A PRSN shall be able to concurrently support access to Peer Systems through multiple PSEs, such that each PSE operates in a specified Security Domain. [DRV KRD 1386, 1998] {R}

**CI2-SAR-4.2.4.4f** (U//FOUO) A PRSN shall be able to be modularly configured to include PSEs that operate in one or more of the following Security Domains: [DRV KRD 0504, 1180, 1386] {R}

- (1) U.S.-Secret.
- (2) U.S.-Unclassified
- (3) CCEB-Secret.
- (4) CCEB-Unclassified.
- (5) NATO-Secret.
- (6) NATO-Unclassified.
- (7) Coalition-Secret.
- (8) Coalition-Unclassified.

(U//FOUO) In some cases, a single PSE may be able to connect to more than one peer system; in other cases, a peer system may need a dedicated PSE. Therefore, a PRSN needs to be able to establish additional PSEs as needed.

**CI2-SAR-4.2.4.4g** (U//FOUO) A PRSN shall be able to be modularly configured with PSEs, or rapidly reconfigured with additional or fewer PSEs, to have from one to forty-two (42) PSEs. [DRV KRD 0504, 1180, 1386] {R}

(U//FOUO) The following requirements specify the networks to which PSEs in CI-2 need to be able to connect:

**CI2-SAR-4.2.4.4h** (U//FOUO) A PRSN PSE operating at a Secret level shall be able to access Peer Systems (1) via SIPRNET or some other network operating at that Secret level or (2) (by using NSA-approved end-to-end encryption) via NIPRNET, the public Internet, or some other network operating at an unclassified level. [DRV KRD 1241, 1242, 2031] {R}

**CI2-SAR-4.2.4.4i** (U//FOUO) A PRSN PSE operating at an unclassified level shall be able to access Peer Systems via NIPRNET, the public Internet, or some other network operating at an unclassified level. [DRV KRD 1242, 2031] {R}

(U//FOUO) PSEs do not usually connect to peer systems through KPCs specified by KMI. Instead, as illustrated by Figure 10, a PSE connects to a peer system through a channel defined by that system. In some cases, the peer may define security requirements for the channel, but the KMI has the following security needs for such a channel or for information received through it.

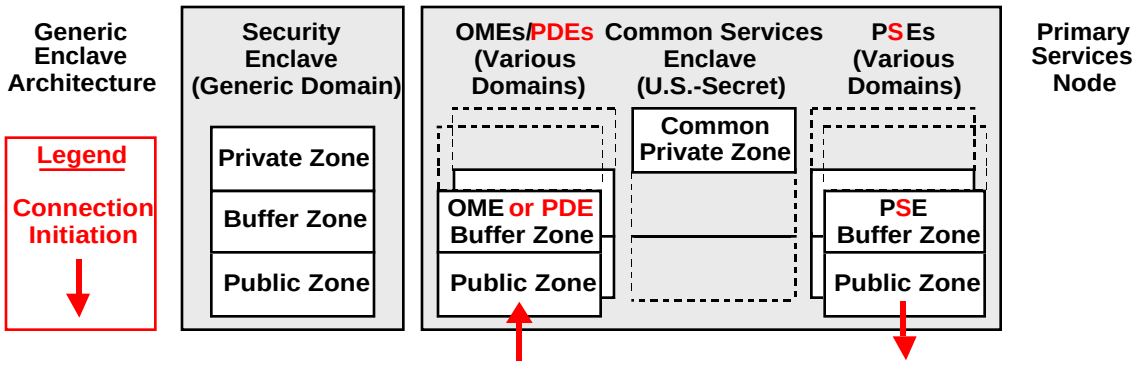
- (U//FOUO) **Authentication.** The KMI usually needs either (a) to authenticate the identity of the external system to which a PSE connects or (b) to authenticate the origin of data received by the PSE from the external system.
- (U//FOUO) **Data confidentiality**. The KMI may need to have the channel provide data confidentiality service for various purposes including operational security.
- (U//FOUO) **Data integrity.** The KMI usualy needs to be able verify the integrity of data obtained by PSEs from peer systems.

**CI2-SAR-4.2.4.4j** (U//FOUO) The connection of a PSE to a Peer System shall be through a communication association that is configured and protected to satisfy the security requirements of both (a) the Peer System (and its Security Domain) and (b) the KMI. [KRD NEW] {R}

### 4.2.5 (U) PRSN Security Zones

(U//FOUO) Figure 14 illustrates how a PRSN is divided into security zones. As described in the "Architectural Elements" section, a security enclave of a KMI core node that serves clients or connects to peer systems needs three security zones—Public, Buffer, and Private—to provide defense in depth. However, a CI-2 PRSN does not provide three separate zones for every enclave. Instead, a PRSN centralizes the functions of Private Zones in a single Common Private Zone that operates at the U.S.-Secret level in the Common Services Enclave. OMEs, PDEs, and PSEs each have their own Public Zone and Buffer Zone but share the services of the Common Private Zone. The Common Services Enclave is connected to and supports all OMEs, PDEs, and PSEs in the PRSN.

**Figure 14. (U) KMI PRSN Enclave Structures**



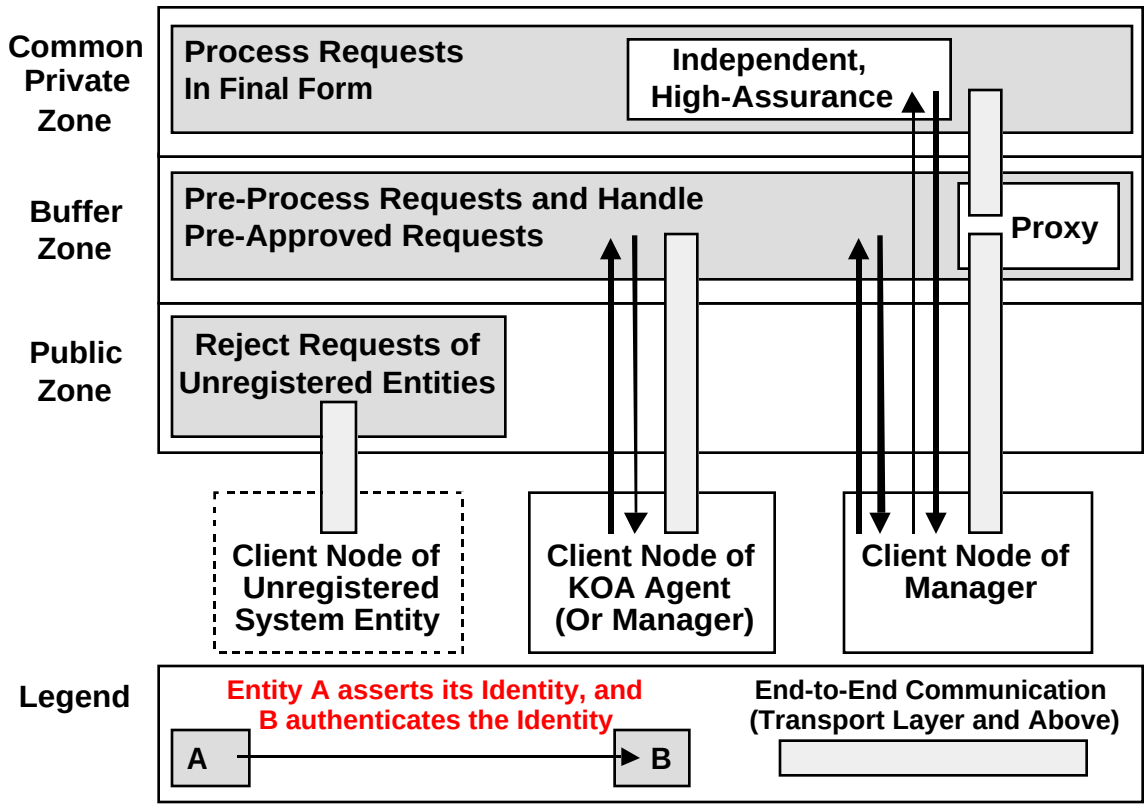

**UNCLASSIFIED//FOUO**

(U//FOUO) Figure 15 illustrates the architectural security strategy for using security zones in PRSNs to handle interactions with Client Nodes. (Although interactions with peer systems are not shown in Figure 15, they are handled similarly to interactions with Client Nodes of Managers.) Both registered and unregistered entities are able to connect Client Nodes to publicly accessible servers in the Public Zone and attempt to log in, but unregistered entities are rejected. Only registered users can log in to the Buffer Zone and submit requests for products and services. The Buffer Zone preprocesses the requests by checking them against KMI specifications, against role and permission information provided from the Private Zone, and against current system state. Requests that pass these checks are forwarded in a canonical form to the Common Private Zone, which again authenticates and checks the requests before acting on them.

- (U//FOUO) **Public Zone**. This type of zone contains the PRSN components that have the greatest exposure to network-based threats. Connections from Client Nodes to a PRSN, and connections from a PRSN to peer systems, pass through this zone. The Public Zone handles initial user interactions, such as by posting welcoming web pages and security warning banners, and manages network connections with clients, such as by balancing communications loads and countering attacks involving flooding or misuse of TCP/IP protocols. However, the Public Zones of OMEs and some PDEs are fronted by an end-to-end encryption device operating at the IP layer, and these zones will typically contain fewer components and have fewer of these public interactions than the Public Zones of the other PDEs and the PSEs.

(U//FOUO) A PSE initiates connections with peer systems, but a PSE rejects any attempt by an peer system to initiate a connection with the PRSN. An OME or PDE of a PRSN does not provide any products or services not to system entities that are not registered, as indicated in Figure 15 by the box labeled “Reject Requests of Unregistered Entities”. This access control could be implemented in a variety of ways, depending on whether access is attempted through a Web-based or transaction-based interface.

Figure 15. (U) KMI Strategy for Security Zones in PRSNs




UNCLASSIFIED//FOUO

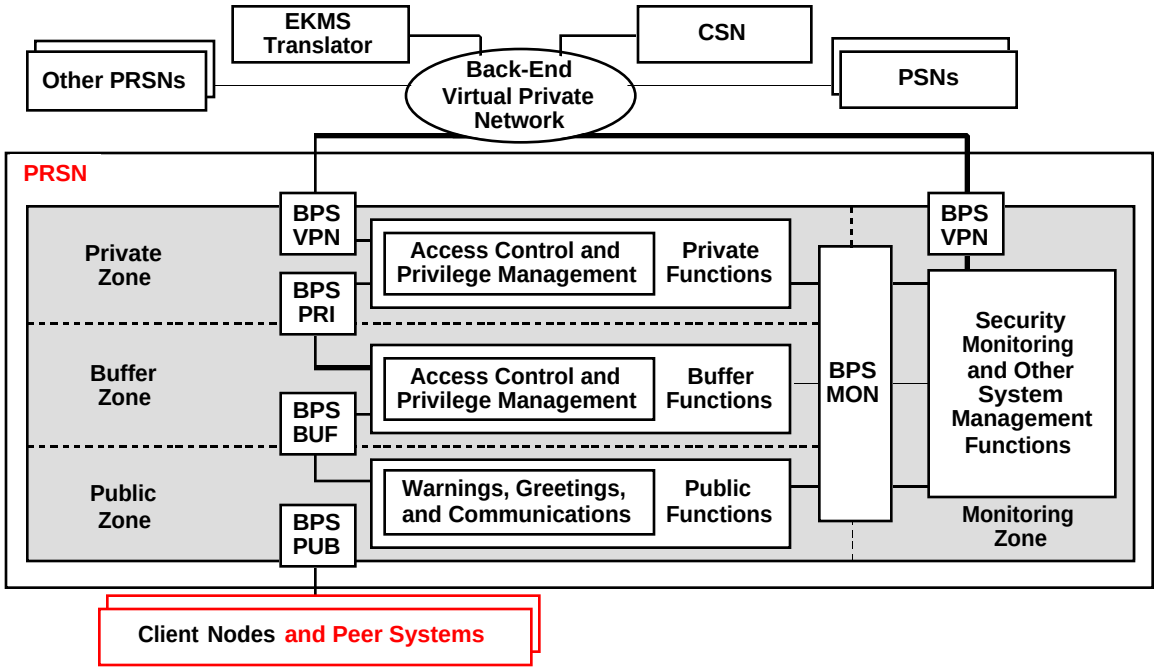
- (U//FOUO) **Buffer Zone**. This type of zone contains the PRSN components that ensure separation between (1) the threat-filled environment of a Public Zone and (2) the sensitive functions of the Common Private Zone, and prevents unauthenticated, unauthorized access to KMI products and services. Product and service requests made by KOA Agents are intended to be handled in a PDE Buffer Zone, usually without any communication with the Common Private Zone. Also, some of the less sensitive requests of Managers may be handled in an OME Buffer Zone, such as a request for a status report on an order that was placed by a previous request. The Buffer Zone always authenticates the identity of ~~the~~ users that access the PRSN, and also enables ~~the~~ clients and peer systems to authenticate the identity of the PRSN.

- (U//FOUO) **Common Private Zone**. This zone contains the components that perform the most sensitive PRSN functions. Connections may be made from this zone to other PRSNs, to PSNs, or to the CSN. Clients do not communicate directly with this zone; communications between Clients and this zone are handled through a proxy in the Buffer Zone. The Common Private Zone always reauthenticates the identity of the user before doing the final processing of a request, and this authentication is of high assurance and independent of the authentication performed by the Buffer Zone. The Common Private Zone also independently enables the client to authenticate the origin of that zone's response to a user's request, in cases when such additional authentication is needed.

(U//FOUO) The separation of PRSN functions into zones is motivated by the likelihood that clients and peer systems will be used to attack PRSNs. Although the Public and Buffer Zones are designed to (a) reject unregistered entities, (b) prevent registered users and approved peer systems from communicating directly ~~communication between clients and~~ with the Common Private Zone, and (c) restrict registered users to authorized activities, it is conceivable that some defenses in these zones might fail. In that case, the zoned structure, by requiring both the Buffer Zone and Private Zone to authenticate ~~registered user~~ interactions and validate service requests independently of each other, reduces the likelihood of a successful attack on the Private Zone.

(U//FOUO) Figure 16 illustrates how PRSN zones are connected to each other, to Client Nodes and peer systems, to other PRSNs, to PSNs, to the CSN, and to the EKMS Translator. The components shown in Figure 16 provide defense-in-depth protection for the PRSN against threat actions carried by communications from other nodes, especially Client Nodes. The zones of a PRSN also provide a defense for the CSN and PSNs that are connected to the PRSN. (Figure 16 only depicts the general relationship of the four types of zones to each other. The actual arrangement of zones in a PRSN is specified differently, as illustrated in Figures 17 and 18.)

**Figure 16. (U) KMI Connections for Security Zones in PRSNs**




UNCLASSIFIED//FOUO

(U//FOUO) Figure 16 also illustrates that a PRSN has a fourth type of zone:

- (U//FOUO) **Monitoring Zone.** This type of zone contains components that monitor the security and the performance of the other three types of zones. This type of zone performs certain secondary PRSN functions, such as managing ASWR and auditing, and separates those functions from the PRSN's primary functions of product ordering and delivery, which are performed by the other types of zones. Connections may be made to a Monitoring Zone

from other types of zones in the PRSN, but such connections are intended to provide only one-way communication into the Monitoring Zone from those other zones.

(U//FOUO) The following are basic requirements for security zones in a PRSN:

**CI2-SAR-4.2.5a** (U//FOUO) All functionality of Security Enclaves in a PRSN shall be divided into four types of Security Zones: Public, Buffer, Private, and Monitoring. [DRV KRD 1180, 1998] {R}

**CI2-SAR-4.2.5b** (U//FOUO) A Computer Platform that implements functions of a Security Zone in a Security Enclave of a PRSN shall be physically separate from Computer Platforms that implement functions of any other zone, enclave, or node. [DRV KRD 1180, 1387, 1568] {R}

**CI2-SAR-4.2.5c** (U//FOUO) All functionality of a PRSN OME shall be divided into a Public Zone, a Buffer Zone, and the BPSs associated with those Security Zones. [DRV KRD 1180, 1998] {R}

**CI2-SAR-4.2.5d** (U//FOUO) All functionality of a PRSN PDE shall be divided into a Public Zone, a Buffer Zone, and the BPSs associated with those Security Zones. [DRV KRD 1180, 1998] {R}

**CI2-SAR-4.2.5c** (U//FOUO) All functionality of a PRSN PSE shall be divided into a Public Zone, a Buffer Zone, and the BPSs associated with those Security Zones. [DRV KRD 1180, 1998] {R}

### 4.2.5.1 (U) Boundary Protection Suites in PRSN Security Zones

(U//FOUO) Figure 16 also illustrates that a PRSN contains five different types of BPSs:

- (U//FOUO) **BPS-PUB.** This type of gateway, from Client Nodes and peer systems into a PRSN, is intended to counter generic network-based attacks, such as distributed denial-of-service attacks involving lower-layer protocols, that are launched from ~~Client Nodes or from~~ any computer platforms that are not part of the PRSN ~~KMI~~. The security countermeasures used in BPS-PUB could include, for example, router-based filtering of TCP/IP protocols, ports, and addresses.

- (U//FOUO) **BPS-BUF.** This type of gateway protects the functions of the Buffer Zone against attacks that might be made by compromised components of the Public Zone or by communications that are allowed to pass through BPS-PUB from Client Nodes or peer systems.

- (U//FOUO) **BPS-PRI.** This type of gateway protects the functions of the Private Zone against attacks that might be made through BPS-BUF or by compromised components of the Buffer Zone.

- (U//FOUO) **BPS-MON.** This type of gateway protects the functions of the Monitoring Zone against attacks that might be made through or by the other three zones.

- (U//FOUO) **BPS-VPN.** This type of gateway provides KPCs for a VPN that enables the PRSN to connect to PSNs, to other PRSNs, to the CSN, and to the EKMS Translator. This type of gateway also protects the functions of the Private and Monitoring Zones against attacks that might be made by compromised components of other nodes.

(U//FOUO) To minimize the risk that BPSs might share vulnerabilities that could negate the defense in depth that the zones are designed to provide, each BPS type needs to be implemented independently of the others.

**CI2-SAR-4.2.5.1a** (U//FOUO) All data communications access to a PRSN Security Enclave ~~of a PRSN~~ from outside the enclave, and all such access from one Security Zone of a Security Enclave to another zone, shall be mediated by BPSs that are incorporated in the functionality of the ~~zones~~enclaves. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.5.1b** (U//FOUO) A Computer Platform that implements BPS functions to protect a Security Zone in a Security Enclave of a PRSN shall be physically separate from any Computer Platforms that implement other functions of that zone and that enclave. [DRV KRD 1180, 1387, 1568] {R}

**CI2-SAR-4.2.5.1c** (U//FOUO) If a set of BPSs provide defense-in-depth in a "serial" or "stacked" fashion along a data path in the PRSN (e.g., the sequence BPS-PUB, BPS-BUF, BPS-PRI), then the software functions of each type of BPS in the set shall be performed by software, including any operating system software, that is implemented separately from the software in the other BPS types. [KRD NEW] {R}

**CI2-SAR-4.2.5.1d** (U//FOUO) A BPS of a Security Zone in a Security Enclave of a PRSN shall restrict data communication to the minimum needed for the intended functions of the zone or zones to which the BPS connects. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.5.1e** (U//FOUO) A BPS shall restrict data communication protocols to those that are essential for the intended functions of the Security Zone or zones to which the BPS connects. [DRV KRD 1999] {R}

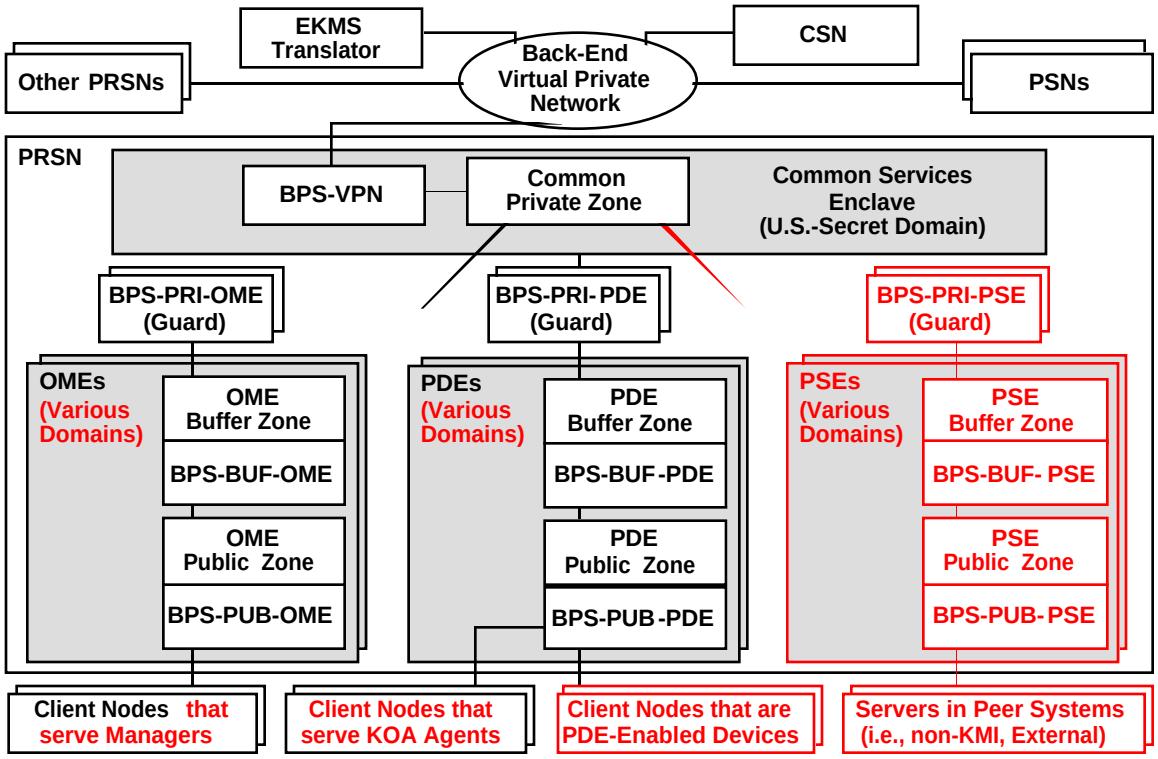
**CI2-SAR-4.2.5.1f** (U//FOUO) A BPS shall, where appropriate, incorporate features to limit the bandwidth of potential covert data channels. [DRV KRD 1999] {R}

### 4.2.5.2 (U) PRSN Public Zones

(U//FOUO) Figure 17 illustrates that Client Nodes and peer systems connect~~s~~ through a BPS-PUB to the Public Zone of a security enclave that operates in the same security domain as the client or peer.

**CI2-SAR-4.2.5.2a** (U//FOUO) The Public Zone of a Security Enclave in a PRSN shall incorporate a BPS ("BPS-PUB") that mediates data communications between (1) that zone and either (2a) Client Nodes that access the enclave from outside the PRSN or (2b) Peer Systems that are accessed by the enclave. [DRV KRD 1998] {R}

**Figure 17. (U) KMI PRSN Components**




**UNCLASSIFIED//FOUO**

(U//FOUO) To avoid cascading security failures, a BPS-PUB needs to be implemented separately from other BPS types.

**CI2-SAR-4.2.5.2b** (U//FOUO) Software that performs functions of a BPS-PUB, including any operating system software, shall be implemented separately from the software in other BPS types (BPS-BUF, BPS-PRI, BPS-MON, and BPS-VPN) in the same PRSN. [DRV KRD 1180, 1387, 1568] {R}

(U//FOUO) A BPS-PUB needs to block unauthorized communications.

**CI2-SAR-4.2.5.2c** (U//FOUO) A BPS-PUB shall permit data communications between (1) the Public Zone of a Security Enclave in a PRSN and (2) Client Nodes or Peer Systems, as needed to support the types of access that have been specified and authorized ~~for~~ between that enclave and entities outside the PRSN ~~both Registered Users~~, and shall prevent all other communications. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.5.2d** (U//FOUO) Components in the Public Zone of a PRSN Security Enclave shall provide only the services that are specified ~~have been authorized~~ for authorized entities—i.e., Registered Users in the case of OMEs and PDEs, and specified Peer Systems in the case of PSEs—and, except for posting warning banners required by this *Specification*, shall not interact with ~~unregistered~~ unauthorized entities any more than is necessary to detect and reject their connection attempts. [DRV KRD 1998, 1999] {R}

### 4.2.5.3 (U) PRSN Buffer Zones

(U//FOUO) Figure 17 illustrates that data traffic from Client Nodes of registered users can enter a Public Zone and continue through BPS-BUF into the associated Buffer Zone. The traffic carries requests for products and services that are authorized for registered users. The Buffer Zone validates and records the requests, limiting each user to initiating only those requests that are authorized for the role the user is playing. Some requests are handled entirely in the Buffer Zone, and other requests and related information are formatted as transactions to be passed through BPS-PRI to the Private Zone for further processing. For these purposes, the Buffer Zone holds selected user registration and authorization data (and, in an OME, also holds ~~and~~ product catalog data and other information), which is loaded into the Buffer Zone from the Private Zone. From the Private Zone, the Buffer Zone receives the results of processed requests, and passes products and other service results back through the Public Zone to Client Nodes.

(U//FOUO) Figure 17 illustrates that a Client Node operated by a Manager connects through a BPS-BUF-OME to an OME Buffer Zone that operates at the same security level (Security Level X) as the client. An OME Buffer Zone processes requests from Managers for various services and for products to be delivered through PDEs to KOA Agents. An OME sends processed requests and related transactions through an OME Guard to the Common Private Zone of the Common Services Enclave. An OME also receives responses and other information from Common Services.

**CI2-SAR-4.2.5.3a** (U//FOUO) A PRSN PSE's Buffer Zone ~~of a Security Enclave in a PRSN~~ shall incorporate a BPS-BUF ("BPS-BUF-PSE") that mediates data communications between ~~the~~ that Buffer Zone and ~~the~~ its associated Public Zone. [DRV KRD 1998, 1999] {R}

**CI2-SAR-4.2.5.3b** (U//FOUO) A PRSN OME's Buffer Zone shall incorporate a BPS-BUF ("BPS-BUF-OME") that mediates data communications between that ~~OME's~~ Buffer Zone and its associated Public Zone. [DRV KRD 1998, 1999] {R}

**CI2-SAR-4.2.5.3c** (U//FOUO) A PRSN PDE's Buffer Zone shall incorporate a BPS-BUF ("BPS-BUF-PDE") that mediates data communications between that ~~PDE's~~ Buffer Zone and its associated Public Zone. [DRV KRD 1998, 1999] {R}

(U//FOUO) To avoid cascading security failures, a BPS-BUF needs to be implemented separately from other BPS types.

**CI2-SAR-4.2.5.3d** (U//FOUO) Software that performs functions of a BPS-BUF, including any operating system software, shall be implemented separately from the software in other BPS types (i.e., BPS-PUB, BPS-PRI, BPS-MON, and BPS-VPN) in the same PRSN. [DRV KRD 1180, 1387, 1568] {R}

(U//FOUO) A BPS-BUF needs to block unauthorized communications.

**CI2-SAR-4.2.5.3e** (U//FOUO) A BPS-BUF-PSE shall permit data communications between (1) the Buffer Zone of a Security Enclave and (2) the Public Zone of that enclave, as needed to support the types of ~~access~~ communications that have been specified and authorized for

~~Registered Users~~ KMI operations, and shall prevent other communications. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.5.3f** (U//FOUO) A BPS-BUF-OME shall permit data communications between (1) an OME Buffer Zone and, via that OME's Public Zone, (2) Client Nodes outside the PRSN, as needed to support the types of OME access that have been specified and authorized for Managers, and shall prevent other communications. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.5.3g** (U//FOUO) A BPS-BUF-PDE shall permit data communications between (1) a PDE Buffer Zone and, via that PDE's Public Zone, (2) Client Nodes outside the PRSN, as needed to support the types of PDE access that have been specified and authorized for KOA Agents and PDE-Enabled Devices, and shall prevent other communications. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.5.3gg** (U//FOUO) A BPS-BUF-PSE shall permit data communications between (1) a PSE Buffer Zone and, via that PSE's Public Zone, (2) Peer Systems outside the PRSN, as needed to support the types of communications that have been authorized for PSEs, and shall prevent other communications. [DRV KRD 0901, 0906, 1999] {R}

(U//FOUO) A Buffer Zone needs to block attacks that exploit vulnerabilities in communication protocols.

**CI2-SAR-4.2.5.3h** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-BUF OME shall be terminated in the OME Buffer Zone. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.3i** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-BUF-PDE shall be terminated in the PDE Buffer Zone. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.3ii** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-BUF-PSE shall be terminated in the PSE Buffer Zone. [DRV KRD 1999] {R}

(U//FOUO) A Buffer Zone needs to authenticate entities with which its enclave communicates.

**CI2-SAR-4.2.5.3j** (U//FOUO) A Buffer Zone of a ~~Security Enclave in a~~ PRSN OME, PDE, or PSE shall authenticate the source of ~~User Identity that initiates a service request (which is received on~~ data ~~packets~~ that ~~are~~ is transported from outside the PRSN, through the Public Zone, to the Buffer Zone~~)~~. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3k** (U//FOUO) An OME's Buffer Zone shall authenticate the User Identity that initiates a service request (which is received on data packets that are transported through the Public Zone to the Buffer Zone), for each request received from a Client Node. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3l** (U//FOUO) A PDE's Buffer Zone shall authenticate the User Identity that initiates a service request (which is received on data packets that are transported through the

Public Zone to the Buffer Zone), for each request received from a Client Node or from a PDE-Enabled Device. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3ll** (U//FOUO) A PSE's Buffer Zone shall perform the authentication functions that are specified for interactions with Peer Systems. [DRV KRD 1998] {R}

(U//FOUO) A security enclave's Buffer Zone needs to validate information before passing it from the enclave's Public Zone to its Private Zone, or vice versa.

**CI2-SAR-4.2.5.3m** (U//FOUO) A Buffer Zone of ~~a security enclave in~~ a PRSN OME, PDE, or PSE shall, before forwarding a ~~received request~~ transaction from the Public Zone to the Common Private Zone, validate the transaction and record the ~~request~~event. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3n** (U//FOUO) A PSE Buffer Zone ~~of a~~ Security Enclave in a PRSN shall, before forwarding an intersystem transaction ~~service request~~ from the Public Zone to the Common Private Zone, ~~enforce role-based Access Control~~ check~~s~~ to ensure that the ~~initiating User Identity has the Permissions needed for the request~~transaction is appropriate for the Peer System that is its source. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3o** (U//FOUO) An OME Buffer Zone shall, before passing a product or service request to the Common Services Enclave, enforce role-based and other Access Control checks to ensure that the initiating User Identity has the Permissions and other Authorizations that are needed for the request. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3p** (U//FOUO) A PDE Buffer Zone shall, before passing a product or service request to the Common Services Enclave, enforce role-based and other Access Control checks to ensure that the initiating User Identity has the Permissions and other Authorizations that are needed for the request. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.3q** (U//FOUO) A Buffer Zone of ~~a Security Enclave in~~ a PRSN OME or PDE shall, before returning to ~~the requesting~~ a Client or Peer System a ~~service~~ transaction result received from the Common Private Zone, validate the result and record the event. [DRV KRD 1999] {R}

(U//FOUO) Information sent to users from the Buffer Zone may require both data confidentiality and data integrity services. The following are some functions implemented in the Buffer Zone:

- (U//FOUO) **Web portal.** A Web server provides Web-based registered users with authorized products and services.
  - (U//FOUO) A mutually authenticated KPC is established with the user's Client Node to support the user's activities. Users that fail the authentication check are denied access.
  - (U//FOUO) Each user is presented with a menu of only the products and services that are authorized for the user.
  - (U//FOUO) The user can make requests and perform actions only as permitted by the permissions of the role the user is playing.

- (U//FOUO) **Transaction portal.** A transaction interface provides transaction-based registered users with authorized products and services.
  - (U//FOUO) Either a mutually authenticated KPC is established with the user's Client Node to carry transaction messages, or messages are authenticated and protected individually. Any transaction that fails an authentication check is rejected.
  - (U//FOUO) The PRSN will accept transactions only for the products and services that are authorized for the user.
  - (U//FOUO) The user can make requests and perform actions only as permitted by the permissions of the role the user is playing.

#### 4.2.5.4 (U) PRSN Common Private Zone

~~(U//FOUO) Figure 17 illustrates that a Private Zone has connections that enable it to communicate with the Buffer Zones other PRSNs, PSNs, the CSN, and the EKMS Translator. The Private Zone receives product and service requests from Buffer Zone, revalidates them, and performs the requested processing. The Private Zone communicates with PSNs as needed to obtain products and services to satisfy valid user requests, and sends results to the Buffer Zone.~~
Tardy cleanup of duplicates after removal of PKI PRSN concept.

(U//FOUO) Figure 17 illustrates that the Common Services Enclave of a PRSN is connected so that it can communicate with the following other components:

- **OMEs**. To receive certain requests, send back replies, and exchange other data.
- **PDEs**. To send products for pickup, to receive certain requests, and exchange other data.
- **PSEs**. To exchange data with peer systems.
- **PSNs**. As needed to obtain products to fulfill requests.
- **PRSNs**. ~~As needed to process requests from OMEs~~ To exchange operational data.
- **CSN**. To exchange operational data (as described in the "CSN Services" section).
- **EKMS Translator**. To exchange ~~products and related~~ operational data with the Electronic Key Management System (EKMS).

**CI2-SAR-4.2.5.4i** (U//FOUO) A PRSN shall include a Common Services Enclave that operates in the U.S.-Secret Security Domain and contains a Common Private Zone to serve the the PRSN's OMEs, PDEs, and PSEs. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.4a** (U//FOUO) ~~A~~ The Common Private Zone of ~~a Security Enclave in~~ a PRSN shall incorporate BPSs ("BPS-PRI") that each mediate data communications between the Private Zone and a Buffer Zone of that PRSN. [DRV KRD 1998] {R}

(U//FOUO) To avoid cascading security failures, a BPS-PRI needs to be implemented separately from other BPS types.

**CI2-SAR-4.2.5.4b** (U//FOUO) Software that performs functions of a BPS-PRI, including any operating system software, shall be implemented separately from the software in the other BPS types (i.e., BPS-PUB, BPS-BUF, BPS-MON, BPS-VPN) in the same PRSN. [DRV KRD 1387, 1568] {R}

(U//FOUO) A BPS-PRI needs to block unauthorized communications.

**CI2-SAR-4.2.5.4c** (U//FOUO) A BPS-PRI in a PRSN shall permit communications between (1) the PRSN's Common Private Zone ~~of the enclave~~ and (2) the Buffer Zone of an OME, PDE, or PSE of that PRSN ~~enclave~~, as needed to support authorized functions of that enclave ~~a PRSN~~, and shall prevent other communications. [DRV KRD 0901, 0906, 1999] {R}

(U//FOUO) OMEs, PDEs, and PSE needs to block attacks that exploit vulnerabilities in communication protocols.

**CI2-SAR-4.2.5.4d** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-PRI shall be terminated in the Common Private Zone and in the associated Buffer Zone. [DRV KRD 1999] {R}

(U//FOUO) The Common Private Zone needs to authenticate entities with which its OME, PDEs, and PSEs communicate, and needs to do that independently of the authentication done in those enclaves.

**CI2-SAR-4.2.5.4e** (U//FOUO) The Common Private Zone ~~of a Security Enclave~~ in a PRSN shall authenticate the User Identity that initiates a product or service request—and authenticate the origin of a data item from a Peer System—that is received through the a Buffer Zone. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.4f** (U//FOUO) The authentication of an identity (i.e., of either a User Identity or the origin of data from a Peer System) that is performed in the Common Private Zone of a ~~Security Enclave in a~~ PRSN shall be performed independently of the associated authentication of that identity that is performed in the Buffer Zone of an attached OME, PDE, or PSE~~that enclave~~. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.4g** (U//FOUO) A Common Private Zone of a ~~Security Enclave in a~~ PRSN shall, when receiving a request passed from the Buffer Zone of that ~~enclave~~PRSN, enforce role-based and other Access Control checks to ensure that the initiating User Identity has the Permissions and other Authorizations that are needed for the request. [DRV KRD 1998] {R}

**CI2-SAR-4.2.5.4h** (U//FOUO) The ~~role-based~~ Access Control checks performed for a request in the Common Private Zone of a ~~Security Enclave in a~~ PRSN shall be both implemented and performed (1) independently of the checks performed in the Buffer Zone from which the request is received and (2) by a high-assurance mechanism. [DRV KRD 1998] {R}

~~**CI2-SAR-4.2.5.4j** (U//FOUO) When receiving a product or service request from an OME or PDE, a Common Services Enclave shall authenticate the User Identity that initiated the request. [DRV KRD 1998] {R}~~ Tardy cleanup from removal of PKI PRSN concept; duplicates revised CI2-SAR-4.2.5.4e.

~~**CI2-SAR-4.2.5.4k** (U//FOUO) The authentication of a User Identity that is performed in a Common Services Enclave shall be performed independently of the authentication of that identity that is performed in the OME or PDE from which the associated request was received. [DRV KRD 1998] {R}~~ Tardy cleanup from removal of PKI PRSN concept; duplicates revised CI2-SAR-4.2.5.4f.

~~**CI2-SAR-4.2.5.4l** (U//FOUO) When receiving a product or service request from an OME or PDE, a Common Services Enclave shall enforce role-based and other Access Control checks to ensure that the initiating User Identity has all of the Permissions and other Authorizations that are needed for the request. [DRV KRD 1998] {R}~~ Tardy cleanup from removal of PKI PRSN concept; duplicates revised CI2-SAR-4.2.5.4g.

~~**CI2-SAR-4.2.5.4m** (U//FOUO) The Access Control checks performed in a Common Services Enclave shall be implemented and performed (1) independently of the checks performed in the associated OMEs or PDEs and (2) by a high-assurance mechanism. [DRV KRD 1998] {R}~~ Tardy cleanup from removal of PKI PRSN concept; duplicates revised CI2-SAR-4.2.5.4h

(U//FOUO) Among KMI's objectives are ensuring continued availability of service for clients by providing redundant points of service, and minimizing the cost of usage by eliminating the need for users either to enter data repetitively or to have multiple client devices to access the KMI. These objectives imply that a Client Node should be able to obtain equivalent products and services at any of two or more PRSNs, as illustrated by Figure 2. That in turn implies that registration data and other information must be replicated between PRSNs. The BPS-VPN enables data to be moved at the Secret level between a PRSN and other PRSNs.

**CI2-SAR-4.2.5.4n** (U//FOUO) The Common Services Enclave~~Private Zone~~ of a PRSN shall incorporate a BPS ("BPS-VPN") that mediates and protects data communications between (1) ~~that zone~~ the Common Private Zone and (2a) other PRSNs, (2b) PSNs, (2c) the CSN, and (2d) the EKMS Translator. [DRV KRD 1998] {P-R-S-T}

**CI2-SAR-4.2.5.4o** (U//FOUO) The functions of a BPS-VPN in a PRSN shall be implemented independently of the other BPS types in the same PRSN. [DRV KRD 1180, 1387, 1568] {R}

**CI2-SAR-4.2.5.4p** (U//FOUO) A BPS-VPN in the Services Enclave~~Private Zone~~ of a PRSN shall implement a KPC that permits authorized communication between (1) that enclave ~~zone~~ and (2) the Common Services Enclaves~~Private Zone~~ of other PRSNs, the PSNs, the CSN, and the EKMS Translator and that (3) prevents all other communications. [DRV KRD 1999] {P-R-S -T}

**CI2-SAR-4.2.5.4q** (U//FOUO) A BPS-VPN in the Common Services Enclave~~Private Zone~~ of a PRSN shall permit replication of one or more of the following data types between (1) that enclave ~~zone~~ and (2) other Core Nodes and the EKMS, as specifically authorized for each type of connection: [DRV KRD 1817, 1825, 1905] {P-R-S -T}

- (1) Identifier credentials.
- (2) User registration data and token registration data.
- (3) Role and Permission data.
- (4) Product Reference Catalog data.
- (5) Request, tracking, and accounting data.
- (6) ASWR data.
- (7) Audit data.

– (8) Key compromise and token compromise reports.
– (9) Credential revocation, identifier revocation, and identity revocation requests

### 4.2.5.5 (U) PRSN Inter-Enclave Guards

(U//FOUO) Figure 17 illustrates that the Common Private Zone in a PRSN is connected by BPSs (BPS-~~BUF~~PRI-OME, BPS-~~BUF~~PRI-PDE, BPS-PRI-PSE) to the OMEs, PDEs, and PSEs in that PRSN. Each PRSN is able to be configured with OMEs, PDEs, and PSEs to support the following security domains: U.S.-Secret and U.S.-Unclassified, NATO-Secret and NATO-Unclassified, CCEB-Secret and CCEB-Unclassified, and Coalition-Secret and Coalition-Unclassified for various coalitions. For any OME, PDE, or PSE that does not operate at the same level as the Common Services Enclave (i.e. at U.S.-Secret), the BPS-PRI~~BUF~~ must be a guard that protects against unauthorized disclosure of U.S.-Secret information from the Common Services Enclave to the OME, PDE, or PSE. (A PRSN also has another kind of inter-enclave guard, which is specified in the following section, "PRSN Monitoring Zones".)

(U//FOUO) The PRSN design also needs to minimize the extent to which it relies on the proper operation of untrusted hardware or software for making security-relevant decisions. In this case, that means not relying on the components of the enclaves that are on either side of those guards. However, the design also should prefer options that minimize the amount and types of data that must be moved through the guards. With regard to data confidentiality, a PRSN could move data rather freely through a guard from an OME, PDE, or PSE into the Common Private Zone; but movement from the Common Private Zone to an OME, PDE, or PSE needs to be minimized. Also, with regard to data integrity and system integrity, data that moves in either direction needs to be carefully filtered, and therefore the flows of information between the Common Services Enclave and the OMEs, PDEs, and PSEs needs to be carefully designed to enable this filtering to be done.

(U//FOUO) A PDE mainly supports retrieval of pre-positioned, self-protecting product packages, and therefore could be viewed as a "write-only" destination from the perspective of the Common Services Enclave. In actual implementation, a return path from a PDE to the Common Private Zone is needed (e.g., to return tracking data about product retrievals), but the data flows on that return path need to be carefully restricted and filtered.

**CI2-SAR-4.2.5.5a** (U//FOUO) For each security level other than U.S.-Secret at which a PRSN operates an OME, the PRSN shall incorporate a BPS-PRI ("BPS-PRI-OME") that is a Guard that mediates data communications between the security level of that OME and the security level of the Common Services Enclave. [DRV KRD 0842, 1387, 1998, 2135] {R}

**CI2-SAR-4.2.5.5b** (U//FOUO) For each security level other than U.S.-Secret at which a PRSN operates a PDE, the PRSN shall incorporate a BPS-PRI ("BPS-PRI-PDE") that is a Guard that mediates data communications between the security level of that PDE and the security level of the Common Services Enclave. [DRV KRD 0842, 1387, 1998, 2135] {R}

**CI2-SAR-4.2.5.5bb** (U//FOUO) For each security level other than U.S.-Secret at which a PRSN operates a PSE, the PRSN shall incorporate a BPS-PRI ("BPS-PRI-PSE") that is a

Guard that mediates data communications between the security level of that PSE and the security level of the Common Services Enclave. [DRV KRD 0842, 1387, 1998, 2135] {R}

**CI2-SAR-4.2.5.5c** (U//FOUO) Each BPS-PRI-OME ~~Guard~~ shall permit communications between (1) its OME and (2) the Common Services Enclave, as needed to support authorized functions of the PRSN, and shall prevent other communications. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.5d** (U//FOUO) Each BPS-PRI-PDE ~~Guard~~ shall permit communications between (1) its PDE and (2) the Common Services Enclave, as needed to support authorized functions of the PRSN, and shall prevent other communications. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.5dd** (U//FOUO) Each BPS-PRI-PSE shall permit communications between (1) its PSE and (2) the Common Services Enclave, as needed to support authorized functions of the PRSN, and shall prevent other communications. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.5e** (U//FOUO) Guard functions of a BPS-PRI (i.e., the functions that separate security domains) shall be modularly implemented separately from other BPS functions of that device. [DRV KRD 1180, 1387, 1568] {R}

(U//FOUO) OMEs, PDEs, and PSE needs to block attacks that exploit vulnerabilities in communication protocols.

**CI2-SAR-4.2.5.5f** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-PRI-OME ~~Guard~~ shall be terminated in the Common Services Enclave and in the OME Buffer Zone. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.5g** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-PRI-PDE ~~Guard~~ shall be terminated in the Common Services Enclave and in the PDE Buffer Zone. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.5gg** (U//FOUO) All packet-switched data communication protocol associations that pass through a BPS-PRI-PSE shall be terminated in the Common Services Enclave and in the PSE Buffer Zone. [DRV KRD 1999] {R}

**CI2-SAR-4.2.5.5h** (U//FOUO) A BPS-PRI-OME ~~Guard~~ shall permit data to pass between the Common Private Zone and OME Buffer Zone only as needed to support the ordering and management of KMI products and services. [DRV KRD 1817, 1825, 1905] {R}

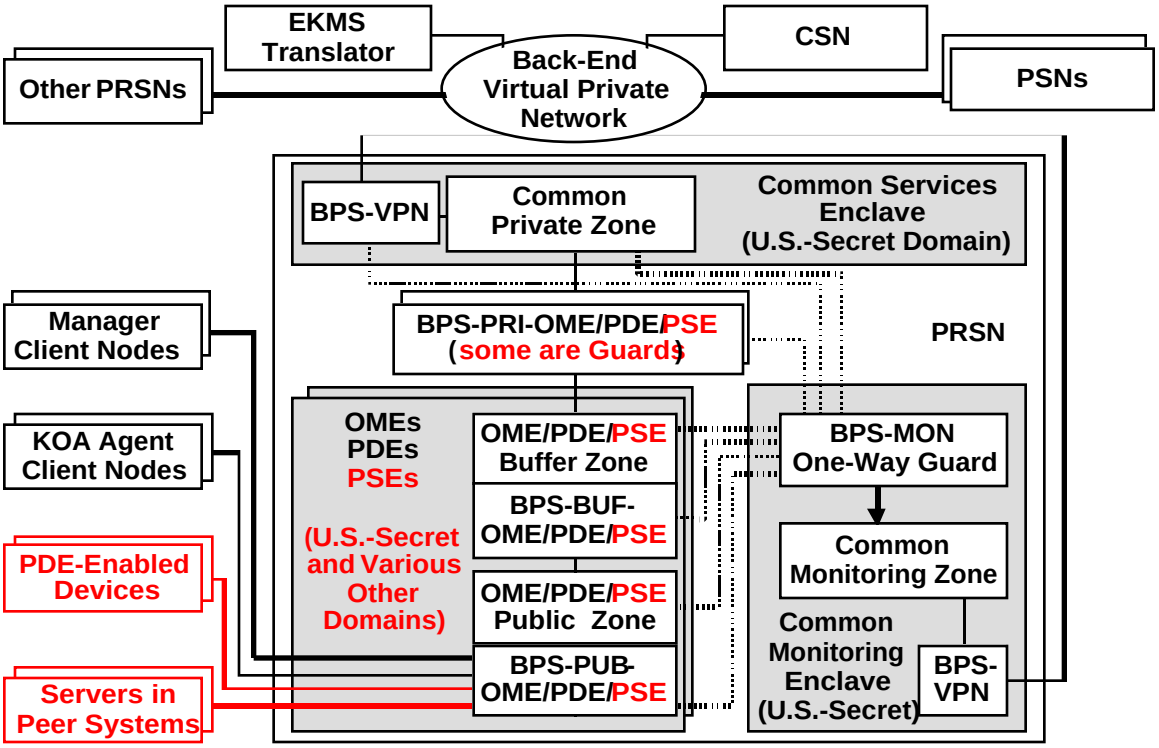
**CI2-SAR-4.2.5.5i** (U//FOUO) A BPS-PRI-PDE ~~Guard~~ shall permit data to pass between the Common Private Zone and PDE Buffer Zone only as needed to support the delivery of KMI products and services. [DRV KRD 1817, 1825, 1905] {R}

**CI2-SAR-4.2.5.5ii** (U//FOUO) A BPS-PRI-PSE shall permit data to pass between the Common Private Zone and PSE Buffer Zone only as needed to support the operation of the KMI. [DRV KRD 1817, 1825, 1905] {R}

### 4.2.6 (U) PRSN Monitoring Zones

(U//FOUO) A Monitoring Zone receives and analyzes intrusion detection event data, audit event data, and other information from computer platforms in other zones and BPSs. Various approaches are possible for implementing this architectural concept in a PRSN: each enclave could have its own Monitoring Zone, or a PRSN could have a single Monitoring Zone as illustrated by Figure 18. A PRSN monitoring zone primarily has responsibility for ASWR functions, as stated in the following requirements:

**Figure 18. (U) KMI PRSN Notional Monitoring Architecture**




UNCLASSIFIED//FOUO

**CI2-SAR-4.2.6a** (U//FOUO) Each PRSN Computer Platform that generates ASWR data shall report the data to its Security Enclave's Monitoring Zone (i.e., to the Monitoring Zone that is responsible for monitoring that Security Enclave) upon demand or periodically, as configured by an ASWR Manager. [DRV KRD 1824] {R}

**CI2-SAR-4.2.6b** (U//FOUO) A Monitoring Zone that is responsible for a PRSN Security Enclave shall include a Computer Platform dedicated to ASWR. [DRV KRD 1816] {R}

**CI2-SAR-4.2.6c** (U//FOUO) PRSN ASWR processes shall enable an ASWR Manager to configure the method and frequency by which ASWR data is reported from Computer Platforms in a Security Enclave to the enclave's Monitoring Zone. [DRV KRD 1408] {R}

**CI2-SAR-4.2.6d** (U//FOUO) ASWR processes in a PRSN Security Enclave's Monitoring Zone shall be able to correlate and analyze ASWR data produced by multiple Components in a Security Zone of that enclave in a manner that facilitates detection and characterization of threat actions that span multiple Components in the zone. [DRV KRD 1817, 1824] {R}

**CI2-SAR-4.2.6e** (U//FOUO) ASWR processes in a PRSN Security Enclave's Monitoring Zone shall be able to correlate and analyze ASWR data produced by multiple Security Zones in that enclave in a manner that facilitates detection and characterization of threat actions that span multiple zones in the enclave. [DRV KRD 1817, 1824] {R}

**CI2-SAR-4.2.6f** (U//FOUO) A PRSN shall have a Common Monitoring Enclave in which ASWR processes shall be able to correlate and analyze ASWR data produced by multiple Security Enclaves in a manner that facilitates detection and characterization of threat actions that span multiple enclaves in the PRSN. [DRV KRD 1817, 1824] {R}

**CI2-SAR-4.2.6g** (U//FOUO) The Common Monitoring Enclave of a PRSN shall periodically, as configured by an ASWR Manager, report ASWR data to the CSN. [DRV KRD 1824] {R-S}

**CI2-SAR-4.2.6h** (U//FOUO) The Common Monitoring Enclave of a PRSN shall notify the CSN of actual or suspected threat actions detected in the PRSN. [DRV KRD 0128, 1824] {R-S}

**CI2-SAR-4.2.6i** (U//FOUO) Each Monitoring Zone in a PRSN shall have a configurable ability to generate reports based on its analysis of received ASWR data and the severity level of actual or suspected threat actions. [DRV KRD 1824] {R}

(U//FOUO) PRSN monitoring zones also have involvement in overseeing system integrity:

**CI2-SAR-4.2.6j** (U//FOUO) Each Computer Platform that generates data concerning system integrity checks shall report the data to its Security Enclave's Monitoring Zone upon demand or periodically, as configured by an Security Configuration Manager. [DRV KRD 1824] {R}

**CI2-SAR-4.2.6k** (U//FOUO) Processes in a PRSN Security Enclave's Monitoring Zone shall be able to check the system integrity of the Components in the enclave. [DRV KRD 1019] {R}

**CI2-SAR-4.2.6m** (U//FOUO) The Monitoring Zone of a PRSN Security Enclave shall notify an Incident Response Manager of any unauthorized change in the system integrity of a Component in the enclave. [DRV KRD 1019] {R}

(U//FOUO) PRSN monitoring zones also have involvement in overseeing system performance:

**CI2-SAR-4.2.6n** (U//FOUO) Each Computer Platform that generates platform performance data and related Computer Network traffic data shall report the data to its Security Enclave's Monitoring Zone upon demand or periodically, as configured by a Security Configuration Manager. [DRV KRD 1865] {R}

(U//FOUO) In the notional, single-monitoring-zone architecture that is illustrated by Figure 18, BPS-MON mediates one-way data communication into (1) the Common Monitoring Zone from the computer platforms of (2a) the Common Private Zone and its associated BPS-VPN and BPS-PRIs, (2b) the OME and PDE Buffer Zones and their associated BPS-BUFs, and (2c) the OME and PDE Public Zones and their associated BPS-PUBs. {R}

**CI2-SAR-4.2.6o** (U//FOUO) A Monitoring Zone shall incorporate one or more BPSs ("BPS-MON One-Way Guard") that mediates data communication into (1) that zone from the (2) Computer Platforms of the PRSN components that are being monitored by that Monitoring Zone. [DRV KRD 1998] {R}

**CI2-SAR-4.2.6p** (U//FOUO) Software that performs functions of a BPS-MON, including any operating system, shall be implemented separately from the software in the other BPS types in the same PRSN enclave. [DRV KRD 1387, 1568] {R}

**CI2-SAR-4.2.6q** (U//FOUO) In a PRSN, the communication media that connect a Component Platform of a monitored Security Zone to a BPS-MON shall be physically separate from those that provide other data paths between platforms. [DRV KRD 1387, 1568] {R}

**CI2-SAR-4.2.6r** (U//FOUO) In a PRSN, all packet-switched data communication protocol associations that pass through a BPS-MON to a Monitoring Zone from a Computer Platform of another Security Zone, BPS, or Guard shall be terminated in that Monitoring Zone and in that other Component. [DRV KRD 1999] {R}

**CI2-SAR-4.2.6s** (U//FOUO) In a PRSN, a BPS-MON shall permit one-way data transfer from the Common Private Zone, Buffer Zones, Public Zones, and BPSs associated with those zones, through the BPS-MON into its associated Monitoring Zone, as needed to support authorized functions of that Monitoring Zone, and shall prevent other communications, including preventing any data transfer out of the Monitoring Zone through BPS-MON. [DRV KRD 0901, 0906, 1999] {R}

**CI2-SAR-4.2.6t** (U//FOUO) In a PRSN, a BPS-MON shall support data replication to the BPS-MON's associated Monitoring Zone, for the purpose of the keeping watch over the PRSN; and that data shall include the following [DRV KRD 1817, 1825, 1905]: {R}
- (1) ASWR event data.
- (2) Audit event data.

[Additional data items are expected to be defined when a detailed design is done.]

### 4.2.7 (U) PRSN Intra-Domain Data Flow

(U//FOUO) The type of BPS that is labeled ~~illustrated as~~ "BPS-VPN" in Figures 17 and 18 enables data to be moved within the same security domain between PRSNs, between a PRSN and a PSN, between a PRSN and the CSN, and between a PRSN and the EKMS Translator.

**CI2-SAR-4.2.7a** (U//FOUO) The Common Services Enclave of a PRSN shall incorporate a BPS ("BPS-VPN") that mediates and protects authorized data communications between (1) that enclave and (2a) the Common Services Enclaves of other PRSNs, (2b) the U.S.-

Secret interfaces of PSNs, and (2c) a U.S.-Secret interface of the CSN, and (2d) a U.S.-Secret interface of the EKMS Translator. [DRV KRD 1998] {P-R-S-T}

**CI2-SAR-4.2.7b** (U//FOUO) The Common Monitoring Enclave of a PRSN shall incorporate a BPS ("BPS-VPN") that mediates and protects authorized data communications between (1) that enclave and (2) only a U.S.-Secret Security Enclave of the CSN. [DRV KRD 1998] {R-S}

**CI2-SAR-4.2.7c** (U//FOUO) The functions of a BPS-VPN in a PRSN shall be performed by software (including the operating system) that is implemented separately from the software in any other BPS types in the same Security Enclave. [DRV KRD 1180, 1387, 1568] {R}

(U//FOUO) When data is replicated between enclaves in the same domain, various integrity checks are needed at the application level. For example, when user registration data is replicated, the KMI needs to compare the core data of replicated users to that of all existing users in the destination domain and, if a duplicate user is found or other data elements do not properly match between the domains, either update the user's data in the destination domain or notify an authorized User Registration Manager or System Security Officer (SSO) to revoke associated identities, identifiers, and credentials as required by established procedures. Similar action is needed when Token Registration Data is replicated. Further discussion of those requirements is provided in [KMI2200V2].

## 4.3 (U) Product Source Nodes

(U//FOUO) Users request KMI products and services from PRSNs, and PRSNs in turn obtain products and services from PSNs. A PSN produces some subset of the products managed by the KMI, and a PSN may additionally provide services related to those products. (Specific types of products and functionality for producing them are specified in Volume 1.)

(U//FOUO) A PSN may respond to product requests from one or more PRSNs, and a PRSN may be served by more than one PSN. PSNs can either be collocated with PRSNs or be remote from them. PSNs do not in principle require human intervention to process requests. Some PSNs are expected to support a "lights-out" cryptographic manufacturing mode in which all PSN operations are automated and PRSNs perform any operations that require interaction with humans.

(U//FOUO) A PSN is comprised of components needed to generate its products and also components needed to interface with other core nodes. PSNs are intended to be modular; new PSNs should be able to be attached to the KMI to meet new requirements of cryptographic systems and their users, and existing PSNs should be removable when no longer needed.

### 4.3.1 (U) PSN Security Characteristics

(U//FOUO) All CI-2 PSNs are subject to the security policies in Volume 2, but otherwise they may be quite different from each other. Each PSN is expected to be designed to meet unique security needs of its product set, and this usually will involve additional, specialized policy and doctrine. Some CI-2 PSNs will be legacy systems now operated by the DoD, some may be new systems developed with CI-2 or developed by other parts of Government, and some may be

commercial systems under contract to serve the Government. Therefore, although this "Nodal Security Architecture" section states basic requirements for PSNs to communicate securely with PRSNs, it does not state requirements for internal structures of PSNs like it does for PRSNs.

- (U//FOUO) **Security level for PSN interfaces.** Since PSNs connect to the Common Private Zone of PRSNs, and since that zone operates at the U.S. Secret level, a PSN needs to include an interface at U.S.-Secret. However, a PSN either may operate at that single level, or may operate in multilevel mode, e.g., to produce key material for multiple levels of use.

  **CI2-SAR-4.3.1a** (U//FOUO) PSNs that are incorporated in KMI CI-2 shall either operate in the U.S.-Secret domain or shall provide one or more interfaces at the U.S.-Secret level for connecting to PRSNs and to the CSN. [DRV KRD 1998] {P-R-S}

- (U//FOUO) **Data confidentiality and data integrity for products**. This "Nodal Security Architecture" section does not state requirements for PRSNs to provide specific data confidentiality or data integrity services for products received from PSNs. Products issued by PSNs include cryptographic secrets and other sensitive information.

### 4.3.2 (U) PSN Communications

(U//FOUO) Figure 17 illustrates that a connection between a PSN and a PRSN is made through a virtual private network implemented by BPSs at the communication end points.

(U//FOUO) **CI2-SAR-4.3.2a** A PSN shall be connected to a data communications infrastructure that enables it to interact with the CSN and with one or more PRSNs. [DRV KRD 1180] {P}

(U//FOUO) **CI2-SAR-4.3.2b** A PSN shall incorporate one or more BPSs that mediate and protect data communication between (1) the PSN and (2) the CSN and one or more PRSNs that the PSN serves. [DRV KRD 1998] {P-R-S}

(U//FOUO) **CI2-SAR-4.3.2c** A BPS that connects a PSN to the CSN or a PRSN shall (1) implement a KPC for authorized communications between the PSN and the CSN or PRSN, and (2) shall prevent other communications. [DRV KRD 1999] {P}

(U//FOUO) In addition to connecting to PRSNs, PSNs in CI-2 will need to connect to the CSN, depending on the extent to which CSN functions are developed in CI-2. This "Nodal Security Architecture" section does not state requirements for a PSN-CSN communication interface, because those requirements are not yet well-defined.

(U//FOUO) A PSN is not expected to connect to other PSNs in either CI-2 or the target architecture.

## 4.4 (U) Central Services Node

(U//FOUO) The KMI target architecture defines the Central Services Node (CSN) as the component that has primary responsibility for providing management services that ensure functional consistency enterprise-wide, i.e., across all KMI nodes, platforms, and sites. The CI-2

CSN is separate from PRSNs and PSNs, and it is intended to operate at a central NSA site. Its components are intended to be replicated at an appropriate remote site to provide a cold-start backup with manual cutover. The CI-2 CSN provides an initial set of both off-line and on-line services, but not the full set of CSN services contemplated by the target architecture. Future capability increments will build on the CI-2 base of CSN services, possibly putting more CSN services on-line. Also, when KMI capabilities are developed to provide PRSN and PSN services to users deployed in tactical or isolated environments, the KMI will provide accompanying CSN services.

### 4.4.1 (U) CSN Services

(U//FOUO) The services provided by the CSN can be grouped into the following four general categories:

- (U//FOUO) **Data management**. Building, maintaining, and publishing centralized databases.
- (U//FOUO) **Security management**. Analyzing event data; issuing warnings and policies.
- (U//FOUO) **Component management**. Monitoring configuration, performance, and health.
- (U//FOUO) **Production management**. Overseeing user roles, catalog.

#### 4.4.1.1 (U) CSN Data Management Services

(U//FOUO) As illustrated by Figure 19, the CSN supports KMI operations by maintaining databases for some important types of data that are handled by PRSNs and PSNs. In most cases, the CSN receives the data from PRSNs and PSNs and stores it in databases both for management use at the CSN and for archival and backup purposes. In a few cases, a database is generated at the CSN, and its contents are distributed to PSNs and PRSNs for their use or for redistribution to Client Nodes. All of the data that is received or generated at the CSN is protected in accordance with Volume 2. In some cases, this involves encrypting or digitally signing data records.

##### 4.4.1.1.1 (U) Data Received by the CSN from PRSNs and PSNs

(U//FOUO) As illustrated by Figure 19, the CSN receives and stores the following types of data from PRSNs and PSNs; some of the data originates at Client Nodes but is passed through PRSNs to the CSN:

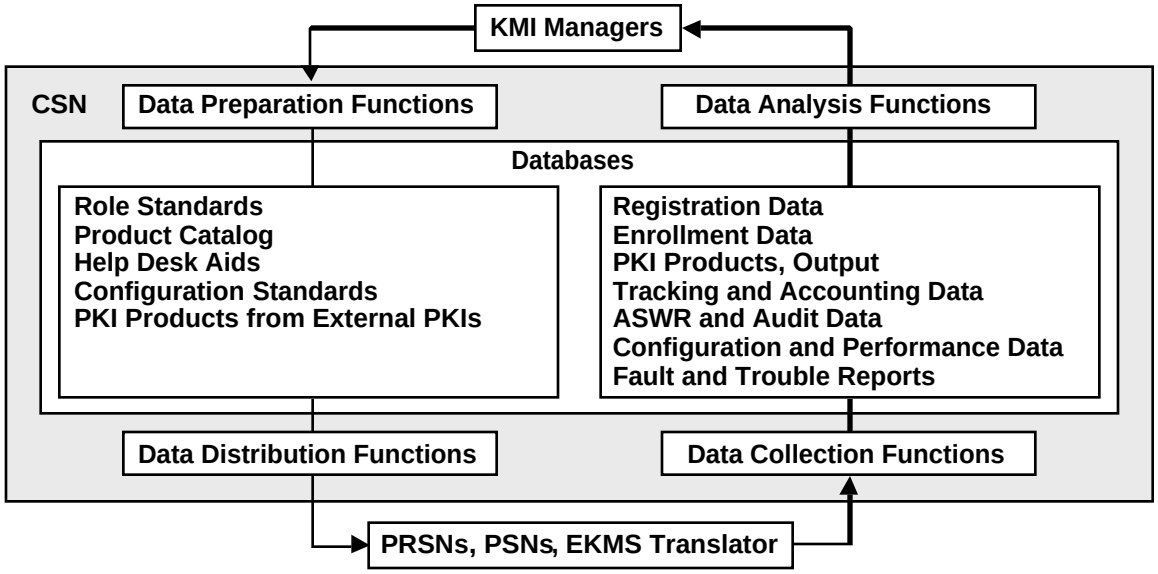
- (U//FOUO) **Registration data**. This database describes users and their PKI hardware tokens, and is used for analyses that are part of the security, component, and production management services provided by the CSN.

- (U//FOUO) **Enrollment data**. This database records assignments of users to manager roles. This data is handled similarly to user registration data.

- (U//FOUO) **PKI Output Repository**. This database contains any PKI products that are generated by the KMI and are required for KMI operation.

- (U//FOUO) **Tracking and accounting data**. This database records the lifecycle status and custody of products and services, including ordering and delivery status.

**Figure 19. (U) KMI CSN Functions and Databases**




**UNCLASSIFIED//FOUO**

- (U//FOUO) **ASWR data**. This database records potentially harmful events reported by intrusion detection sensors.
- (U//FOUO) **Audit data**. This database records significant events reported by platforms and applications.
- (U//FOUO) **Configuration data.** This database records changes that are made in the composition and arrangement of system components.
- (U//FOUO) P**erformance data**. This database records measurements of the effectiveness of system operations
- (U//FOUO) **Fault reports**. This database contains records of errors, failures, and other abnormal operations in system components.
- (U//FOUO) **Trouble reports**. This database contains reports and requests submitted by users to the Help Desk.

(U//FOUO) The CI-2 CSN is mainly a “sink” for the data types listed above. Although the CI-2 CSN might make some of this data available as backup copies for some nodes, the CSN normally neither redistributes these types of data to other nodes nor provides database consolidation or synchronization services for other nodes.

#### 4.4.1.1.2 (U) Data Distributed by the CSN to PRSNs and PSNs

(U//FOUO) As illustrated by Figure 19, the CSN is the source for some types of system-level data needed by other nodes either in common or individually. In these cases, the CSN maintains

a master database and downloads partial images to PRSNs and PSNs. The CSN distributes the following types of data to PRSNs and PSNs:

- (U//FOUO) **Role standards**. This data defines system-wide rules for assignments (1) of permissions to roles and (2) of roles as subordinates of other roles (i.e., the role hierarchy).
- (U//FOUO) **Product catalog**. This database describes and defines KMI products
- (U//FOUO) **Library content**. This database contains master copies of unclassified library objects that are made available to KOA Agents through PDEs. (Classified library objects need to be wrapped for delivery; therefore, they are treated like other products and must be ordered individually. See "Access to Library Objects" section.)
- (U//FOUO) **Help desk aids**. This database contains master copies of material that the help desk provides to users.
- (U//FOUO) **Configuration standards**. This database defines system-wide rules for the composition and arrangement of components.
- (U//FOUO) **PKI Input Repository**. This database contains any PKI products—X.509 certificates and CRLs—that are received from PKIs external to the KMI and are required for KMI operation.

#### 4.4.1.1.3 (U) Purposes for Storing Data at CSN

(U//FOUO) Database administrators at the CSN maintain stored data in formats appropriate for the following uses:

- (U//FOUO) **Management services**. The CSN maintains databases to support security management, component management, and production management functions.
- (U//FOUO) **Long-term archive service**. The CSN maintains copies of KMI data that must be stored for relatively long period of times.
- (U//FOUO) **Backup service**. The CSN maintains reserve copies of some KMI data, for use if an original copy becomes lost or damaged.

(U//FOUO) The CI-2 CSN consolidates data received from other nodes and creates databases that are used at the CSN to perform analyses in support of ongoing management functions, which are described in following sections.

**CI2-SAR-4.4.1.1a** (U//FOUO) The CSN shall maintain databases to support security management, Component management, and production management processes. [DRV KRD 2011] {S}

(U//FOUO) The CI-2 CSN maintains an archive of data that is received from other KMI nodes or generated at the CSN. Each PRSN and PSN includes functions that support archive operations. These functions collect data that meets specified criteria, offload the data to a secure storage

location, and maintain records to support later retrieval of the data from the archive. The locally archived data is also forwarded to the CSN for central archiving. CI-2 has an initial on-line capability for receipt of archive data over a VPN internal to KMI. However, because of the volume of such data, some of it might instead be offloaded to physical media at PRSNs and PSNs and sent to the CSN through off-line channels.

**CI2-SAR-4.4.1.1b** (U//FOUO) The CSN shall maintain archives to support long-duration Security Services and long periods of use of products and services. [DRV KRD 2011] {S}

(U//FOUO) Each PRSN and PSN includes functions that maintain backups for data needed for normal operations. However, copies of some of this data are sent to the CSN to provide a secondary backup, and some data archived at the CSN also serves a backup purpose.

**CI2-SAR-4.4.1.1c** (U//FOUO) The CSN shall maintain backup databases to support Information Integrity Services and System Integrity and Availability Services for Core Nodes. [DRV KRD 1105] {S} (See "Security Service Policies" section of Volume 2 for service definitions and related requirements.)

#### 4.4.1.2 (U) CSN Security Management Services

(U//FOUO) The CSN supports the KMI's security policy and security architecture by providing managers with an overview of security operating conditions across the entire system and, to a limited extent in CI-2, by distributing security information and helping to control security services and mechanisms in other nodes.

(U//FOUO) The CSN receives data that is collected and generated by the ASWR components and audit components in PRSNs and PSNs. The CSN receives the data both on-line and off-line, depending on the time-criticality and volume of the data, and stores the data in appropriate databases. The CSN analyzes the data, both periodically and as requested by managers, to detect and investigate threat actions against the KMI.

- (U//FOUO) **ASWR event data**. The CSN receives data from IDSs in PRSNs and PSNs, merges the datasets to provide an overview of the entire KMI, and analyzes the merged data. Data flowing to the CSN from PRSNs and PSNs can range from complete database transfers to notification of only selected incidents exceeding configurable thresholds. Any decisions to limit flow to the CSN are based on a tradeoff in benefits between localized versus centralized ASWR analysis and response, and on network bandwidth issues.

  **CI2-SAR-4.4.1.2a** (U//FOUO) The CSN shall incorporate processes and procedures to detect threat actions against the KMI and, if and when threat actions are detected, provide warning of them and respond to them with counteractions, in accordance with the "Attack Sensing, Warning, and Response Service" section of the *Security Policy* [KMI2200V2]. [DRV KRD 1016, 1823, 1826] {S}

- (U//FOUO) **Audit data**. The CSN receives audit data from individual PRSNs and PSNs, merges the data, and analyzes it to provide an audit overview of the entire KMI.

**CI2-SAR-4.4.1.2b** (U//FOUO) The CSN shall incorporate processes for recording and analyzing Audit Trail data concerning Security-Sensitive Events and Security-Sensitive Functions, in accordance with the "Audit Service" section of the *Security Policy* [KMI2200V2]. [DRV KRD 0990] {S}

(U//FOUO) Security analyses performed by the CSN can take advantage of the CSN's data management resources by combining ASWR and audit data, and also by combining those types of data with any of the other types received and stored at the CSN.

(U//FOUO) The CSN distributes security management information to PRSNs and PSNs, to support the control of security services and mechanisms and to provide warnings concerning threats and threat actions. In CI-2, however, all such information is distributed off-line with respect to the KMI VPN, using other secure communications.

- (U//FOUO) **Warnings**. Alerts generated by CSN ASWR analyses are disseminated to other nodes to enable them to respond appropriately. The CSN also is the focal point for receiving alerts from non-KMI systems, and for sending alerts to those systems.

- (U//FOUO) **Policies**. Rules and directions for the operation of security components are disseminated to other nodes. Among these are the following:
  - Directions for configuring BPS policies.
  - Directions for configuring other ASWR sensors and reports.
  - Directions for configuring the collection of audit trail data.

### 4.4.1.3 (U) CSN Component Management Services

(U//FOUO) The CSN does configuration monitoring, performance monitoring, and system health monitoring to support managers in controlling applications, platforms, networks, and sites.

- (U//FOUO) **Configuration monitoring**. This function supports configuration control of KMI components, in accordance with the "Configuration Control" section of Volume 2. It involves collecting and analyzing data to support the preparation, initialization, maintenance, and termination of KMI operations and services. The CSN maintains a master database that describes the authorized configuration for all Core Nodes and supports several aspects of configuration management:

  - (U//FOUO) **Establishing and verifying configurations**. This involves defining and maintaining component resources and attributes. Each core node periodically tests whether its installed configuration matches the authorized one and reports to the CSN.

  - (U//FOUO) **Distributing software**. This involves delivering operating instructions and tabular data for use by hardware components. For example, installation of new software at PRSNs is accomplished in CI-2 by using out-of-band physical distribution, but software might be downloaded electronically in later KMI capability increments. The download of software presumably would originate at the CSN.

  - (U//FOUO) **Initializing and terminating operations**. This involves startup and shutdown of components, and routine maintenance functions such as performing

backups. In CI-2, these functions are performed locally at every KMI node. In later KMI capability increments, the CSN might have capabilities to operate nodes remotely.

- (U//FOUO) **Performance monitoring**. KMI core nodes collect data regarding their own functional effectiveness and forward reports to the CSN. The CSN compiles and analyzes that data. KMI managers, both locally and at the CSN, use the data to evaluate and tune system operations and, thereby, control the quality of system services.

- (U//FOUO) **System health monitoring.** Fault detection functions of KMI nodes monitor for, and collect data on, errors and failures in their own components and in other nodes. KMI managers at the nodes use the data to detect, isolate, and correct operating problems and abnormal conditions in local components. The nodes also forward fault data to the CSN, where Managers use the data to detect, isolate, and correct system-wide problems.

#### 4.4.1.4 (U) CSN Production Management Services

(U//FOUO) As illustrated by Figure 19, the CSN supports operations concerned with the production and delivery of products and services to users.

- (U//FOUO) **Registration and enrollment oversight**. The CSN receives user registration data and manager enrollment data from PRSNs, and checks the data for completeness and correctness within the context of system-wide databases maintained at the CSN. These checks help to verify the proper operation of the PRSNs. However, the CSN does not replicate that data to other PRSNs. Instead, the PRSNs replicate registration data between each other as required, or each PRSN maintains a master copy of part of the registration database and cooperates with other PRSNs to support the full database.

- (U//FOUO) **Role management**. The CSN sets system-wide standards for the hierarchy of roles and for assigning permissions to roles, and distributes this information to PRSNs.

- (U//FOUO) **Product Catalog management**. The CSN supports the creation and maintenance of the master version of the product catalog and distributes appropriate subsets to PRSNs and PSNs. Conceptually, the Product Catalog has two main parts:

  – (U//FOUO) **Product Ordering Catalog**. This part of the Product Catalog contains product descriptions that are used by PRSNs (1) to create forms (“templates”) for accepting orders for products and related services and (2) to validate the orders. This *Security Architecture* assumes that this part of the KMI product catalog is Unclassified; if further analysis determines that some product descriptions are classified, they could be stored with the Product Reference Catalog ~~as shown in Figure 19~~.

  – (U//FOUO) **Product Reference Catalog**. This part of the Product Catalog contains product definitions that are used by Type 1 PSNs to generate products. This *Security Architecture* assumes that this part of the Product Catalog, either alone or combined with classified product descriptions, is classified ~~no~~ but not higher than Secret.

- (U//FOUO) **Library content management**. The CSN maintains the master versions of unclassified library objects and distributes copies to PRSNs for release through PDEs.

- (U//FOUO) **Help desk support**. The CSN maintains master versions of material that help desks provide to users, and the CSN distributes copies to various help desk locations.

#### 4.4.1.5 (U) CSN Data Characteristics

(U//FOUO) To provide the services described above, KMI managers that are responsible for the CSN require database management servers together with processors to perform data preparation, data distribution, data collection, and data analysis functions. Figure 19 illustrates those functions and their supporting databases in the CSN.

(U//FOUO) Table 8 lists sources of data that is sent to the CSN, and Table 9 lists destinations of data that is sent by the CSN. For each source and destination, the tables list the types of data and the classification of each type.

**Table 8. (U) KMI Data Received by CSN from Other Nodes**

| Data Source | Data Types | Data Classification |
|---|---|---|
| 1. PRSN's Common Private Zone, which operates at Secret | Registration and enrollment data.<br>Tracking and accounting data<br>ASWR and audit data.<br>Configuration, performance, and fault data.<br>Trouble reports received by Help Desk. | SECRET, because it has been handled on a system-high platform. |
| 2. PRSN's OME.<br>This is an indirect source; data is routed through OME-Guard and Common Services. | Tracking and accounting data<br>ASWR and audit data.<br>Configuration, performance, and fault data. | SECRET & UNCLAS, but all can be moved up to SECRET by OME-Guard. |
| 3. PRSN's PDE<br>This is an indirect source; data is routed through PDE-Guard and Common Services. | Tracking and accounting data<br>ASWR and audit data.<br>Configuration, performance, and fault data. | SECRET & UNCLAS, but all can be moved up to SECRET by PDE-Guard. |
| 4. PSN that operates with an interface at the Unclassified level | PKI products.<br>Tracking and accounting data.<br>ASWR and audit data.<br>Configuration, performance, and fault data. | UNCLAS, because received from PSN interface at that level. |
| 5. PSN that operates with an interface at the Secret level | PKI products.<br>Tracking and accounting data.<br>ASWR and audit data.<br>Configuration, performance, and fault data. | SECRET, because received from PSN interface at that level. |
| 6. EKMS Translator | ASWR and audit data.<br>Configuration, performance, and fault data. | SECRET, because EKMS is at that level. |
| 7. Client Node<br>This is an indirect source; all data is routed through PRSN. | Registration data.<br>Also, interaction with PRSNs causes other types of data to be generated in PRSNs. | SECRET & UNCLAS, according to security level of connection to PRSN. |

**UNCLASSIFIED//FOUO**

- (U//FOUO) Although the data received by the CSN from other components is generated at a variety of security levels, and the data generated and sent by at the CSN is intended to be used by components that operate at a variety of security levels, it is not necessary to use multilevel-secure platforms for the CSN database servers and other CSN functions shown in Figure 19. Instead, CSN services can be hosted on computer platforms that each operate at a single level—either U.S. Secret or Unclassified—except for some Guard devices, and those

Guards need only to move data from the Unclassified domain to the Secret domain. This is because of three characteristics of the data handled by the CSN.

- (U//FOUO) First, the types of data received by the CSN, which are listed in Table 8, are disjoint from the types of data issued by the CSN, which are listed in Table 9. Therefore, the two sets of data can be kept on different servers.

- (U//FOUO) Second, the inbound data listed in Table 8 is generated in KMI components that operate at various security levels, but it can all be stored at the CSN on one or more servers that operate in system high mode at U.S.-Secret. For example, audit data could be generated in a PRSN's OMEs at U.S.-Secret, NATO-Secret, CCEB-Secret, U.S.-Unclassified, NATO-Unclassified, and CCEB-Unclassified. However, these various kinds of audit data need not be kept separated by the CSN, because they never are redistributed by the CSN to other nodes. All the audit data can be aggregated in a single system-high database at U.S. Secret. In fact, audit data is aggregated by each PRSN before it is sent to the CSN, because each PRSN is required to perform its own audit analysis. A PRSN needs to aggregate the data into the Common Private Zone, which operates at U.S. Secret. (U//FOUO) Third, the outbound data listed in Table 9 needs to be sent to KMI components that operate at a variety of security levels, but it all can be generated and stored at the CSN in a server operating at U.S.-Unclassified, except for the classified part of the Product Catalog.

**Table 9. (U) KMI Data Sent by CSN to Other Nodes**

| Data Destination | Data Types | Data Classification |
|---|---|---|
| 1. PRSN's Common Private Zone, which operates at Secret. | Role standards.<br>Product catalog descriptions.<br>Configuration standards.<br>Help Desk aids. | UNCLAS<br>UNCLAS<br>UNCLAS<br>UNCLAS |
| 2. PRSN's OME.<br>This is an indirect receiver; data is routed through Common Services and OME-Guard. | Product catalog descriptions.<br>Configuration standards. | UNCLAS<br>UNCLAS |
| 3. PRSN's PDE.<br>This is an indirect receiver; data is routed through Common Services and PDE-Guard. | Configuration standards. | UNCLAS<br>UNCLAS |
| 4. PSN that operates with an interface at Unclassified level | Product catalog definitions. | UNCLAS |
| 5. PSN that operates with an interface at the Secret level | Product catalog definitions. | SECRET |
| 6. EKMS Translator | Configuration standards. | UNCLAS |
| 7. Client Node.<br>This is an indirect receiver; data is routed through PRSN. | Configuration standards. | UNCLAS |

**UNCLASSIFIED//FOUO**

(U//FOUO) In summary, data handled by the CSN has the following characteristics:

- (U//FOUO) Data that the CSN sends to other components can mainly be generated and stored at the CSN at the U.S.-Unclassified level, and then be moved to the components by upgrading the data to other security levels as needed. Thus, no data need be downgraded.

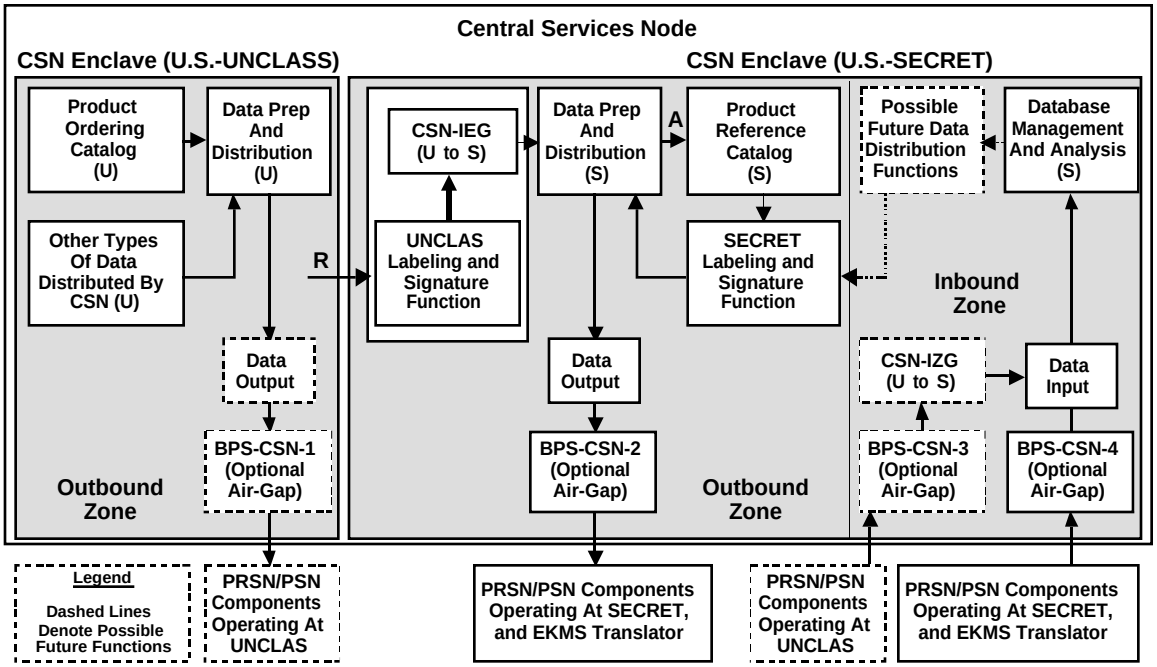
- (U//FOUO) Data that the CSN receives from other components can be stored and processed at the CSN at the U.S.-Secret level, and can be moved from the other components to the CSN by upgrading the data to U.S.-Secret as needed. Thus, none of the data need be downgraded.

### 4.4.2 (U) CSN Enclaves and Data Flows

(U//FOUO) The CSN consists of a suite of high-availability servers, which are replicated at a backup site. The CSN can connect on-line to PSNs and PRSNs via a virtual private network implemented by KPCs, and might communicate only off-line with some of those core nodes. Guard devices internal to the CSN move data between the CSN components that operate at different security level, and between those components and components of PSNs and PRSNs.

(U//FOUO) Figure 20 illustrates CSN components and data flows in the CSN. The CSN is divided into an Unclassified enclave and a Secret enclave. The Unclassified enclave has only an Outbound Zone; but the Secret enclave is divided into an Outbound Zone and an Inbound Zone.

**Figure 20. (U) KMI CSN Enclaves and Data Flows**




**UNCLASSIFIED//FOUO**

**CI2-SAR-4.4.2a** (U//FOUO) All Components of the CSN shall be grouped into two separate Security Enclaves, of which one operates in the U.S.-Unclassified domain and the other in the U.S.-Secret domain. [DRV KRD 1180, 1998] {S}

**CI2-SAR-4.4.2b** (U//FOUO) All Components of the CSN's Unclassified Security Enclave shall be grouped into a single Security Zone—the Outbound Zone. [DRV KRD 1180, 1998] {S}

**CI2-SAR-4.4.2c** (U//FOUO) All Components of the CSN's Secret Security Enclave shall be grouped into two Security Zones—Outbound and Inbound. [DRV KRD 1180, 1998] {S}

**CI2-SAR-4.4.2d** (U//FOUO) A Computer Platform that implements functions of an Inbound or Outbound Zone in a Security Enclave of the CSN shall be physically separate from Computer Platforms that implement functions of all other Security Zones. [DRV KRD 1180, 1568] {S}

(U//FOUO) The Secret enclave of the CSN distributes data directly to Secret enclaves in other nodal components and, via those other enclaves, indirectly to Unclassified enclaves in those components. The Unclassified enclave of the CSN might, in future capability increments, deliver data directly to Unclassified enclaves of other components. The Secret enclave handles data that the CSN receives from Secret enclaves of other components and might, in future capability increments, receive data directly from Unclassified enclaves of those components. The following subsections describe the components and functions of each enclave and zone of the CSN, and the communications between CSN components and components of PSNs, PRSNs, and the EKMS Translator.

(U//FOUO) Figure 20 shows the Product Ordering Catalog data being distributed from the Unclassified Outbound Zone, and the Product Reference Catalog data from the Secret Outbound Zone. This is not intended to specify the architecture for the Catalog database or its maintenance, but only to describe the levels at which Catalog data is distributed to PRSNs and PSNs. The Catalog and its KMI interfaces are described and specified in more detail in Volume 1.

#### 4.4.2.1 (U) CSN Unclassified Enclave

(U//FOUO) Figure 20 illustrates that the Unclassified enclave includes computer platforms to support data preparation, data storage, and data distribution for unclassified data (listed in Table 9) that the CSN sends to PSNs and PRSNs. Data preparation, storage, and distribution functions may be performed on the same platforms or on separate platforms.

**CI2-SAR-4.4.2.1a** (U//FOUO) The Outbound Zone of the CSN's Unclassified Security Enclave shall incorporate one or more Computer Platforms ("Database Prep and Distribution (U)") that operate at U.S.-Unclassified and support (1) preparation of data to send to PSNs and PRSNs, (2) storage of that data, and (3) distribution of that data. [DRV KRD 1998] {S}

(U//FOUO) From the types of data listed in Table 9, the CSN's Unclassified enclave tailors appropriate datasets to send to various enclaves and zones of PSNs and PRSNs, and distributes each dataset directly or through the CSN's Secret enclave. For example, the data maintained in the CSN's unclassified enclave includes the section of the Product Catalog that holds product descriptions. This information is needed by PRSNs to construct the templates (i.e., tailored Web pages) that OMEs display to users who manage products. However, the entire catalog is not intended to be offered in every OME. An OME that operates at U.S.-Secret will probably offer the entire catalog, and an OME that operates at U.S.-Unclassified might offer most of the

catalog. But OMEs that serve NATO and CCEB users will offer only parts of the catalog. Therefore, the CSN's Unclassified enclave prepares an appropriate catalog subset to send to each type of OME, and routes those datasets to the CSN's Secret enclave, which in turn routes them through the Common Private Zone of PRSNs to the OMEs.

(U//FOUO) The CSN's Unclassified enclave might, in future capability increments, distribute data directly to PSNs operating at the Unclassified level (through paths described in the "CSN Communication with Other Nodes" section below). Otherwise, the Unclassified enclave sends a dataset to the Outbound Zone of the Secret enclave, through the path labeled "R" in Figure 20, to be relayed to a PSN or PRSN.

**CI2-SAR-4.4.2.1b** (U//FOUO) The CSN's Unclassified Security Enclave shall be able to route a prepared dataset appropriately, either for direct distribution to a PSN, or for transfer to the Outbound Zone of the CSN's Secret Security Enclave. [DRV KRD 1899] {S}

### 4.4.2.2 (U) CSN Classified Enclave—Outbound Zone

(U//FOUO) Figure 20 illustrates that when the CSN's Secret enclave receives a dataset from the Unclassified enclave, the Secret enclave immediately applies both (1) a security label to indicate that the dataset consists only of Unclassified data and (2) a digital signature. The signature protects the integrity of the dataset and its label and also identifies the CSN as the origin of the dataset. Then, the dataset is transferred into the Secret security domain through the CSN Inter-Enclave Guard ("CSN-IEG").

**CI2-SAR-4.4.2.2a** (U//FOUO) The Outbound Zone of the CSN's Secret Security Enclave shall incorporate a Guard ("CSN-IEG") that (1) permits datasets to be transferred to that enclave from the CSN's Unclassified Security Enclave as needed to support authorized functions of the PRSN, but prevents data from being transferred in the opposite direction, and (2) labels each dataset as unclassified and digitally signs the labeled dataset before transferring it to the Secret domain. [DRV KRD 1387, 1900, 1999] {S}

**CI2-SAR-4.4.2.2b** (U//FOUO) A Computer Platform that supports CSN-IEG shall be physically separate from Computer Platforms that implement other functions of the CSN and functions of other Nodes. [DRV KRD 1180, 1387, 1568] {S}

(U//FOUO) Figure 20 illustrates that the Secret enclave also includes computer platforms to support data preparation, data storage, and data distribution.

**CI2-SAR-4.4.2.2c** (U//FOUO) The Outbound Zone of the CSN's Secret Security Enclave shall incorporate one or more Computer Platforms ("Data Prep and Distribution (U)", as illustrated in Figure 20) that operate at the U.S.-Secret level, and that support (1) preparation of data to send to PSNs and PRSNs, (2) storage of that data, and (3) distribution of that data. [DRV KRD 1998] {S}

(U//FOUO) The Secret Outbound Zone prepares and stores the classified part of the Product Catalog, i.e., the product definitions that the CSN sends to PSNs.

(U//FOUO) The Secret Outbound Zone sends data directly to PSNs and to the Common Private Zones and Monitoring Zones of PRSNs (through paths described in the "CSN Communication with Other Nodes" section below). The Secret Outbound Zone sends data indirectly to OMEs and PDEs in various domains, via PRSN Common Services.

**CI2-SAR-4.4.2.2d** (U//FOUO) The Outbound Zone of the CSN's Secret Security Enclave shall be able to route a prepared dataset either for direct distribution to a PSN or to a PRSN Common Services Enclave, or for indirect distribution, via PRSN Common Services, to a PRSN OME or PDE. [DRV KRD 1999] {S}

(U//FOUO) The CSN's Secret Outbound Zone and the Common Services Zone and Monitoring Zone of a PRSN all operate system high at the U.S.-Secret level. Therefore, when the Secret Outbound Zone passes a dataset to a PRSN, the Common Services or Monitoring Zone must handle the dataset as being Secret. However, if the dataset is intended for an OME or PDE, Common Services can pass the dataset to the appropriate OME Guard or PDE Guard. The guard is able to verify a CSN signature and validate an "UNCLASSIFIED" label and, therefore, transfer a dataset from the Secret level of Common Services to an OME or PDE that operates at a lower level than Secret.

#### 4.4.2.3 (U) CSN Classified Enclave—Inbound Zone

(U//FOUO) Figure 20 illustrates that the Inbound Zone includes computer platforms to support databases that store the data (listed in Table 8) received from PSNs and PRSNs and to support analysis of that data for management purposes. Analysis functions may be performed on the same platforms that hold the databases or on separate platforms.

**CI2-SAR-4.4.2.3a** (U//FOUO) The Inbound Zone of the CSN's Secret Security Enclave shall incorporate one or more Computer Platforms ("Database Management and Analysis (S)") that operate at U.S.-Secret, support databases created from data received by the CSN from PSNs and PRSNs, and support analysis of that stored data. [DRV KRD 1998] {S}

(U//FOUO) The dashed box and dotted line the Secret Inbound Zone in Figure 20 are not intended for CI-2 implementation. They represent "Possible Future Data Distribution Functions" that might be implemented in CI-3 or later. These possibilities are noted in the figure to alert CI-2 implementers to avoid designs that would make it difficult to add such functions to the KMI in later capability increments. The "CSN-IZG", "BPS-CSN-3", and "BPS-CSN-4" components that are shown in the Inbound Zone in Figure 20 are discussed in the following section.

#### 4.4.2.4 (U) CSN Communication with Other Nodes

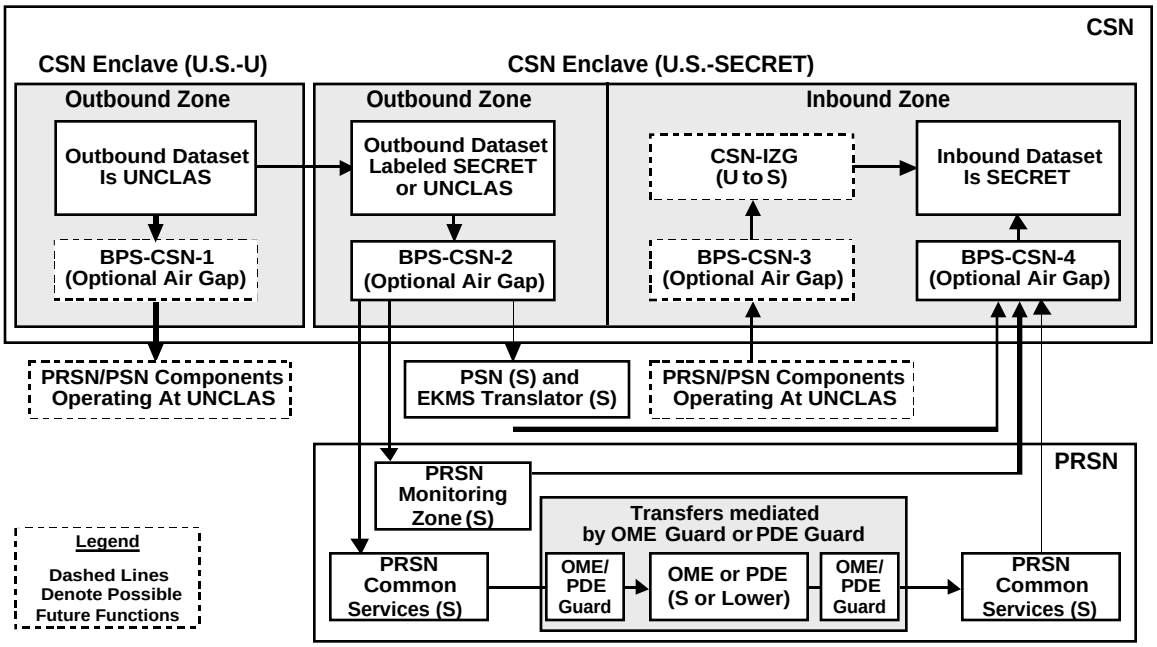
(U//FOUO) Figure 21 illustrates the types of communication associations between CSN components and components of PSN and PRSNs.

**CI2-SAR-4.4.2.4a** (U//FOUO) The CSN shall be connected to a data communications infrastructure that enables it to interact with PSNs and PRSNs. [KRD 1180] {S}

**CI2-SAR-4.4.2.4d** (U//FOUO) The Outbound Zone of the CSN's Secret Security Enclave shall include an interface for sending data at the U.S.-Secret level to (1) Common Services

Zones and Monitoring Zones of PRSNs and (2) PSN interfaces operating at the Secret level. [DRV KRD 1998] {S}

**Figure 21. (U) KMI CSN Connections to Core Nodes**




UNCLASSIFIED//FOUO

**CI2-SAR-4.4.2.4e** (U//FOUO) The Outbound Zone of the CSN's Secret Security Enclave shall incorporate a BPS ("BPS-CSN-2") that mediates and protects data sent from that zone—either on-line or, optionally, through an air gap—to Components that operate at the U.S.-Secret level [DRV KRD 1998] {S}

**CI2-SAR-4.4.2.4i** (U//FOUO) The Inbound Zone of the CSN's Secret Security Enclave shall include an interface for receiving data at the U.S.-Secret level from (1) Common Services Zones of PRSNs, (2) Monitoring Zones of PRSNs, (3) PSN interfaces operating at the Secret level, and (4) the EKMS Translator. [DRV KRD 1998] {S}

**CI2-SAR-4.4.2.4j** (U//FOUO) The Inbound Zone of the CSN's Secret Security Enclave shall incorporate a BPS ("BPS-CSN-4") that mediates and protects data received at the Secret level—either on-line or, optionally, through an air gap—from specified PSN and PRSN Components that operate at the U.S.-Secret level. [DRV KRD 1998] {S}

**CI2-SAR-4.4.2.4k** (U//FOUO) Each BPS-CSN that connects the CSN to specified Components of PSNs or PRSNs shall (1) implement a KPC for communications that are authorized between the CSN and those Components and (2) shall prevent other communications. [DRV KRD 1999] {S}

**CI2-SAR-4.4.2.4l** (U//FOUO) A Computer Platform that implements BPS functions to protect a Security Zone in the CSN shall be physically separate from any Computer

Platforms that implement functions of other Components of the CSN. [DRV KRD 1180, 1387, 1568] {S}

## 4.5 (U) EKMS Translator

(U//FOUO) PRSNs in CI-2 need to communicate with the Electronic Key Management System (EKMS) as specified in the "EKMS Translator" section of Volume 1 and in Appendix A of Volume 1, and some transactions generated in PRSNs need to be translated into EKMS transactions (and vice versa). For this purpose, CI-2 provides one or more EKMS Translator components that connect PRSNs to the EKMS message server infrastructure. As illustrated in Figure 16, a Translator is a KMI component that is separate from the CSN, PSNs, PRSNs, and Client Nodes.

### 4.5.1 (U) Translator Security Characteristics

(U//FOUO) A Translator is subject to applicable security policies and requirements that are stated in Volume 2 and in this volume, and also is subject to applicable EKMS security policies and requirements [EKMS103, EKMS202]. KMI has been designed to be compatible with EKSM security. The EKMS operates in system-high mode at the U.S.-Secret level [EKMS103], and PRSN Common Private Zones operate at that same level. Therefore, a Translator, which connects to both the EKMS and Common Private Zones, needs to operate at U.S-Secret.

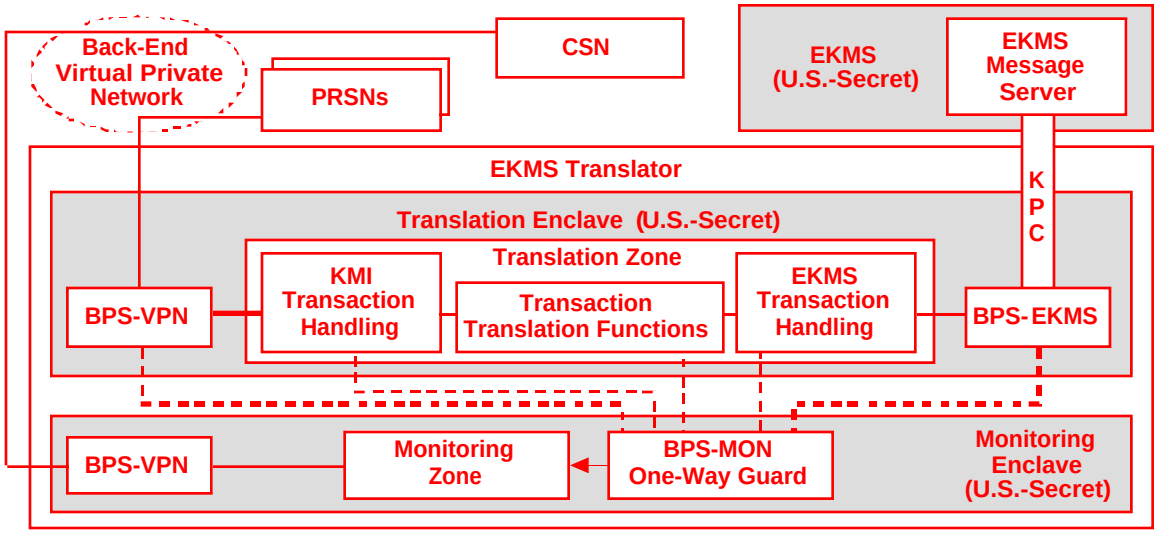
**CI2-SAR-4.5.1a** (U//FOUO) An EKMS Translator that is incorporated in KMI CI-2 shall operate in the U.S.-Secret domain ~~or~~ and shall provide interfaces at the U.S.-Secret level for connecting (a) to one or more PRSNs, (b) to the CSN, and (c) to an EKMS Message Server. [DRV KRD 1998] {R-S-T}

(U//FOUO) A Translator also needs to meet KMI requirements for component modularity and isolation of components that operate at different levels of sensitivity, as stated in the "Domains, Enclaves, and Zones" section of this volume. Figure 21B illustrates that a Translator is divided into two enclaves.

**CI2-SAR-4.5.1b** (U//FOUO) All Components of an EKMS Translator shall be grouped into two separate Security Enclaves—the Translation Enclave and the Monitoring Enclave—both of which operate in the U.S.-Secret domain. [DRV KRD 1180, 1998] {T}

**CI2-SAR-4.5.1c** (U//FOUO) A Computer Platform that implements functions of one Security Enclave of an EKMS Translator shall be physically separate from Computer Platforms of (a) the other Security Enclave of the Translator, (b) other KMI Nodes, and (c) any other EKMS Translators. [DRV KRD 1180, 1568] {T}

**Figure 21B. (U) KMI EKMS Translator Enclaves and Data Flows**




UNCLASSIFIED//FOUO

### 4.5.2 (U) Translator Communications

(U//FOUO) Figure 21B illustrates that a connection between a~~n EKMS~~ Translator and a PRSN is made through a back-end, virtual private network (as was previously illustrated in Figure 16). Figure 21B also illustrates that a KPC connects a Translator to the EKMS. However, that connection is shown as being separate from the VPN, because a Translator is likely to be connected to an EKMS Message Server by a short, point-to-point link that is separate from the back-end network used for other, internodal KMI communications. However, the requirements stated in this section only mandate appropriate protection for the connection and are not specific with regard to the implementation of that connection.

**CI2-SAR-4.5.2a** (U//FOUO) An EKMS Translator (a) shall be connected to a data communications infrastructure that enables it to interact with the CSN and with one or more PRSNs that the Translator serves and (b) shall be connected to an EKMS Message Server. [DRV KRD 1180] {T}

**CI2-SAR-4.5.2b** (U//FOUO) An EKMS Translator shall incorporate one or more BPSs that mediate and protect data communication between (1) the Translator and (2a) one or more PRSNs which the Translator serves, (2b) the CSN, and (2c) an EKMS Message Server. [DRV KRD 1998] {R-S-T}

**CI2-SAR-4.5.2c** (U//FOUO) A BPS of an EKMS Translator that connects the Translator to the CSN, a PRSN, or an EKMS Message Server shall (1) implement a KPC for authorized communications between the Translator and the other Component and (2) shall prevent other, unauthorized communications. [DRV KRD 1999] {R-S-T}

**CI2-SAR-4.5.2d** (U//FOUO) Any KMI Component that receives an EKMS message requiring relay shall transfer the message to the destination Component without modification,

except for the Components that perform necessary EKMS-KMI translation functions. [DRV KRD 1288] {R-T}

### 4.5.3 (U) Translator Security Zones and Data Flows

(U//FOUO) Figure 21B illustrates that a Translation Enclave contains a Translation Zone and two types of BPSs:

**CI2-SAR-4.5.3a** (U//FOUO) All Components of an EKMS Translator's Translation Enclave shall be grouped into (1) a Translation Zone that handles and translates transactions exchanged between PRSNs and the EKMS, (2) a BPS ("BPS-VPN") that connects the Translator to PRSNs, and (3) a BPS ("BPS-EKMS") that connects the Translator to the EKMS. [DRV KRD 1180, 1998] {T}

(U//FOUO) Figure 21B illustrates that a Translator's Monitoring Enclave contains a Monitoring Zone, a BPS, and a one-way guard.

**CI2-SAR-4.5.3b** (U//FOUO) All Components of an EKMS Translator's Monitoring Enclave shall be grouped into (1) a Monitoring Zone that receives and analyzes information from Computer Platforms in the Translation Enclave, (2) a BPS ("BPS-VPN") that connects the Monitoring Zone to the CSN, and (3) a one-way guard ("BPS-MON") that connects the Monitoring Zone to Components of the Translation Enclave. [DRV KRD 1180, 1998] {T}

(U//FOUO) The Monitoring Zone receives and analyzes intrusion detection event data, audit event data, performance data, and other types of information.

**CI2-SAR-4.5.3c** (U//FOUO) Each of a Translator's Computer Platforms that generate ASWR data shall report the data to its the Monitoring Zone upon demand or periodically, as configured by an ASWR Manager. [DRV KRD 1824] {T}

**CI2-SAR-4.5.3d** (U//FOUO) A Translator's Monitoring Zone shall include a Computer Platform dedicated to ASWR. [DRV KRD 1816] {T}

**CI2-SAR-4.5.3e** (U//FOUO) The ASWR processes in a Translator shall enable an ASWR Manager to configure the method and frequency by which ASWR data is reported to the Monitoring Zone from Computer Platforms that are monitored. [DRV KRD 1408] {T}

**CI2-SAR-4.5.3f** (U//FOUO) ASWR processes in a Translator's Monitoring Zone shall be able to correlate and analyze ASWR data produced by multiple Components of the Translator in a manner that facilitates detection and characterization of threat actions that span multiple Components. [DRV KRD 1817, 1824] {T}

**CI2-SAR-4.5.3g** (U//FOUO) A Translator's Monitoring Zone shall periodically, as configured by an ASWR Manager, report ASWR data to the CSN. [DRV KRD 0128, 1824] {S-T}

**CI2-SAR-4.5.3h** (U//FOUO) A Translator's Monitoring Zone shall notify the CSN of actual or suspected threat actions detected in the Translator. [DRV KRD 0128, 1824] { S-T }

**CI2-SAR-4.5.3i** (U//FOUO) A Translator's Monitoring Zone shall have a configurable ability to generate reports based on its analysis of received ASWR data and the severity level of actual or suspected threat actions. [DRV KRD 1824] {T}

(U//FOUO) A Translator's Monitoring Zone also has involvement in overseeing the system integrity of the Translator:

**CI2-SAR-4.5.3j** (U//FOUO) Each of a Translator's Computer Platforms that generate data concerning system integrity checks shall report the data to the Translator's Monitoring Zone upon demand or periodically, as configured by a Security Configuration Manager. [DRV KRD 1824] {T}

**CI2-SAR-4.5.3k** (U//FOUO) Processes in a Translator's Monitoring Zone shall be able to check the system integrity of monitored Components. [DRV KRD 1019] {T}

**CI2-SAR-4.5.3m** (U//FOUO) A Translator's Monitoring Zone shall notify an Incident Response Manager of any unauthorized change that the zone detects in the system integrity of a Component in the Translator. [DRV KRD 1019] {T}

(U//FOUO) A Translator's Monitoring Zone also has involvement in overseeing the system performance of the Translator:

**CI2-SAR-4.5.3n** (U//FOUO) Each of a Translator's Computer Platforms that generate platform performance data and related Computer Network traffic data shall report the data to the Translator's Monitoring Zone upon demand or periodically, as configured by an Security Configuration Manager. [DRV KRD 1865] {T}

(U//FOUO) In the architecture illustrated in Figure 21B, BPS-MON mediates one-way data communication into the Monitoring Zone from the computer platforms of the Translation Enclave.

**CI2-SAR-4.5.3o** (U//FOUO) A Translator's Monitoring Enclave shall incorporate one or more BPSs ("BPS-MON One-Way Guard") that mediate data communication into (1) the Monitoring Zone from (2) the Computer Platforms of monitored Components of the Translation Enclave. [DRV KRD 1998] {T}

**CI2-SAR-4.5.3p** (U//FOUO) Software that performs functions of a Translator's BPS-MON, including any operating system, shall be implemented separately from the software in the other BPS types in that Translator. [DRV KRD 1387, 1568] {T}

**CI2-SAR-4.5.3q** (U//FOUO) In a Translator, the communication media that connect a monitored Component Platform of the Translation Enclave to a BPS-MON shall be physically separate from those that provide other data paths between platforms in that enclave. [DRV KRD 1387, 1568] {T}

**CI2-SAR-4.5.3r** (U//FOUO) In a Translator, all packet-switched data communication protocol associations that pass through a BPS-MON to the Monitoring Zone from a

Computer Platform of the Translation Zone shall be terminated in the Monitoring Zone and in that other Component. [DRV KRD 1999] {T}

**CI2-SAR-4.5.3s** (U//FOUO) A BPS-MON of a Translator shall permit one-way data transfer from Components of the Translation Enclave, through the BPS-MON into the Monitoring Zone, as needed to support authorized functions of the Monitoring Zone, and shall prevent other communications, including preventing any data transfer out of the Monitoring Zone through BPS-MON. [DRV KRD 0901, 0906, 1999] {T}

**CI2-SAR-4.5.3t** (U//FOUO) A BPS-MON of a Translator shall support data replication from the Translation Enclave to the Monitoring Zone, for the purpose of the keeping watch over the Translator; and that data shall include the following [DRV KRD 1817, 1825, 1905]: {T}

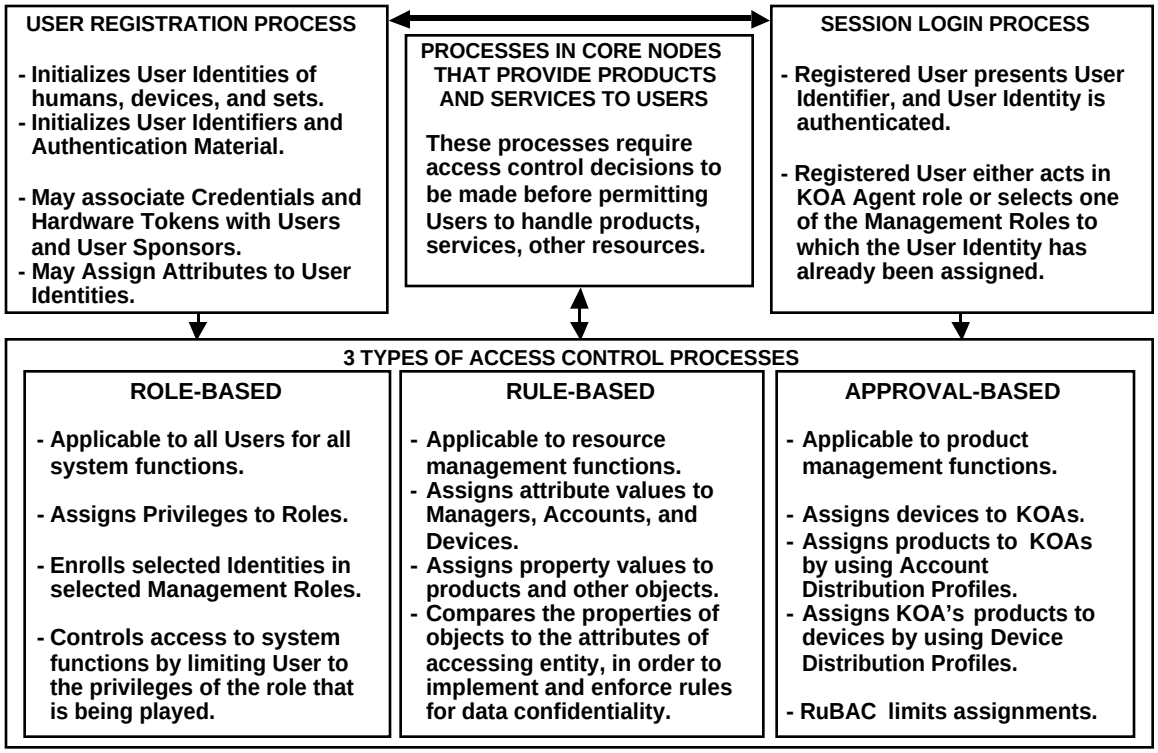
– (1) ASWR event data.
– (2) Audit event data.

[Additional data items are expected to be defined when a detailed design is done.]

# 5 (U) ACCESS CONTROL PROCESSES

(U//FOUO) This section specifies how CI-2 restricts access to system resources, in accordance with policies stated in the "Access Control" section of Volume 2. Figure 22 illustrates that functional processes in core nodes provide products, services, and other system resources to users. However, access control decisions need to be made before those processes can permit users to handle products, services, and other system resources.

**Figure 22. (U) KMI Access Control Framework**




**UNCLASSIFIED//FOUO**

(U//FOUO) Figure 22 shows that KMI access control decisions are made by three types of access control processes—role-based, rule-based, and approval-based. However, most COTS platforms currently do not incorporate KMI's PKI-based authentication mechanisms and role-based access control mechanisms. Therefore, for some cases of administrative access, KMI needs to use other access control mechanisms, such as identifier-password pairs, that are native to the platforms (see "Administrative Security for Platforms and Applications" section of Volume 2).

(U//FOUU) The three types of access control are supported by processes for user registration and session login. The basic registration process for users is described and specified in the "User Registration and Identification Service" section of Volume 2; when users are assigned to management roles, the basic registration process is supplemented by a more rigorous registration process, called "enrollment", which is described in this "Access Control Services" section.

- (U//FOUO) **User registration process**. User registration (1a) initializes one or more identities for an authorized user and (1b) associates one or more identifiers with each identity, (2) may also associate authentication material with each identifier, and (3), depending on the authentication mechanism being used, may also issue identifier credentials and tokens.

- (U//FOUO) **Session login process**. When a user accesses the KMI by presenting a registered user identifier, session login processes authenticate that identity, as described in the "Identity Authentication Service" section of Volume 2. The KMI then associates the identity with a role, either automatically or by permitting the user to select from among a set of roles to which the user's identity has previously been assigned.

- (U//FOUO) **Access control processes**. CI-2 incorporates three types of access control, which complement each other to protect against unauthorized use of system resources:

  – **Role-based access control**. These processes associate user identities with roles, and also associate permissions with roles. When a user acts in an assigned role during a session, the user can exercise the permissions that have been assigned to the role.

  – **Rule-based access control**. These processes associate attributes (e.g., clearance level) with certain user identities and role assignments, and associate counterpart properties (e.g., data classification) with system resources. When a user (acting in a specific identity and role assignment) attempts to access a resource during a session, the session's attributes (which are a combination of the attributes of the identity and role assignment) are compared to the resource's attributes to enforce pre-defined access rules.

  – **Approval-based access control**. These processes enable the authorizations conferred by role-based and rule-based access control to be further tailored for each user organization on a finer-grained, least-privilege, need-to-know basis that addresses individual products and other resources.

**CI2-SAR-5a** (U//FOUO) The KMI shall provide three types of Access Control: role-based, rule-based, and approval-based. [DRV KRD 0425, 0949, 1152, 1613, 1792, 1794, 2008] {A-R-S}

(U//FOUO) The KMI grants various types of access rights to registered users. In discussing access rights, Volume 2 and this *Security Architecture* usually use the term "authorization". Volume 1 and other KMI documents, and some DoD publications, also use the synonym "privilege".

**DEFINITION** (U) Authorization (or Privilege). A right that is granted to a Registered User or other System Entity to Access a System Resource for a specific purpose.

**CI2-SAR-5b** (U//FOUO) The KMI shall ensure that changes in Authorization data for Access Control processes are made available within two hours to all Components that require them, assuming that there are no communication system interruptions. [DRV KRD 1898] {A-R-S}

(U//FOUO) This *Security Architecture* uses other, more narrowly defined terms for access rights that are specifically associated with one type of access control process. For example, as explained below, a "permission" is an authorization controlled by a role-based process.

(U//FOUO) The three types of access control cooperate to ensure that sensitive functions are performed only by authorized managers, and that products and services are received only by authorized users. However, KMI access controls combine rigorous assurance with flexibility.

- User communities can define domains for access control and select their own managers, but product ordering and distribution can cross domain boundaries when necessary.

- The duties of a management role may be divided among multiple persons when required by a large workload or the distributed nature of an organization, or the duties of multiple roles may be combined and performed by a single person when personnel resources are scarce.

(U//FOUO) All three types of CI-2 access control processes are designed to incorporate and support the following principles and general requirements:

**DEFINITION** (U//FOUO) Principle of Positive Authorization. The practice of granting Access to System Resources only in a positive way.

**CI2-SAR-5c** (U//FOUO) The KMI shall grant Access to System Resources only in a positive way; in the absence of an explicit Authorization that grants Access, the default action shall be to refuse Access. [KRD 1551] {A-R-S}

**DEFINITION** (U//FOUO) Principle of Least Privilege. The practice of granting to each System Entity the minimum Authorizations that the entity needs to do its legitimate work.

**CI2-SAR-5d** (U//FOUO) The KMI shall provide means to restrict each System Entity to only the minimum Authorizations and capabilities that the entity needs to perform its function. [DRV KRD 0952] {Z}

**DEFINITION** (U//FOUO) Principle of Separation of Duties. The practice of dividing the functions of a system process among different System Entities, to prevent a single entity from subverting the process. (The "Role Separation Constraints" section specifies a general capability for separating roles, and the "Specifically Separated Roles" section identifies some required separations.)

**CI2-SAR-5e** (U//FOUO) The KMI shall provide means to divide management duties and system functions among multiple System Entities to protect against security violations. [DRV KRD 0951] {Z}

(U//FOUO) This *Security Architecture* applies these three general requirements to implement the following control:

**CONTROL** (U//FOUO) **ECLP-1 Least Privilege (Confidentiality)**. "Access procedures enforce the principles of separation of duties and 'least privilege'. Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged

functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization. [DoD8500.2]"

(U//FOUO) This *Security Architecture* applies these three principles to all three types of access control—role-based, rule-based, and approval based—to support prevention and detection of security violations, which are acts by users and other system events that disobey or otherwise break the rules of the system's security policy.

(U//FOUO) The following requirements also apply to all three types of KMI access control. These requirements are included here as an overall statement but also are implemented by more specific statements in this and other sections of [KMI2200].

**CI2-SAR-5f** (U//FOUO) The KMI shall record as Mandatory Audit Events the request, assignment, receipt, modification, deletion, and rejection of any Authorization pertaining to Access Control. [DRV KRD 0071, 0876] {Z}

**CI2-SAR-5g** (U//FOUO) The KMI shall notify an Incident Response Manager of any request for products, services, or other System Resources from a System Entity that cannot be authenticated or has insufficient Authorization for the request. [DRV KRD 0867] {Z}

**CI2-SAR-5h** (U//FOUO) The KMI shall record as a Mandatory Audit Event any request for products, services, or other System Resources from a System Entity that cannot be authenticated or has insufficient Authorization for the request. [DRV KRD 0419, 0844, 0866] {Z}

**CI2-SAR-5i**(U//FOUO) Each Independent Component shall record as Mandatory Audit Events, at a minimum, (1) identification and authentication checks; (2) attempts to access, modify, or delete Authentication Material or Access Control information; and (3) failed attempts to access System resources. [DRV KRD 0844] {Z}

**CI2-SAR-5j** The KMI shall record as a Mandatory Audit Event each success or failure of Access Control checks performed prior to delivery of classified or sensitive KMI products. [DRV KRD 0419] {R}

## 5.1 (U) Role-Based Access Control

(U//FOUO) CI-2 uses role-based access control [Ferraiolo] that enables functional permissions to be assigned to user roles flexibly and in accordance with the principles of need-to-know and least privilege (see "User Roles and Permissions" section above).

**CONTROL** (U//FOUO) **ECPA-1 Privileged Account Control (Integrity)** "All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The [Information Assurance Manager] tracks privileged role assignments. [DoDI8500.2]"

(U//FOUO) It is expected that CI-2 will need to use COTS platforms that do not support role-based access control. In those cases, CI-2 needs to use other access control mechanisms, typically mechanisms that are native to those platforms, as described in "Administrative Security for Platforms and Applications" section of Volume 2.

**CI2-SAR-5.1a** (U//FOUO) The KMI shall restrict access to System Resources based on the attributes of the accessing entity's authenticated User Identity and the Permissions of the Roles to which that identity has been assigned. [DRV KRD 1289, 1552, 1613] {R}

(U//FOUO) The way that permissions are assigned differs depending on the type of role:

- (U//FOUO) Management roles. For most management roles, role-based access control is implemented fully, including the ability to dynamically assign and remove permissions; but the permissions of Role Manager are assigned statically, i.e., they are "built in" when the system is implemented.

- (U//FOUO) KOA Agent. Role-based access control in PDEs is intended to be implemented only minimally, because only KOA Agents access PDEs using Client Nodes. General functional permissions are intended to be assigned statically to the role of KOA Agent during implementation of PDE functionality. (The authorizations that enable KOA Agents to act for specific KOAs are not role-based permissions; instead, they are approval-based authorizations that are assigned dynamically by KOA managers.)

**CI2-SAR-5.1b** (U//FOUO) The KMI shall record for Audit any attempt to access System Resources by a System Entity that does not have the necessary Permissions. [DRV KRD 0867] {Z}

**CI2-SAR-5.1c** (U//FOUO) The KMI shall provide a capability to manage Roles and Permissions. [DRV KRD 0403, 1792, 1794] {R-S}

(U//FOUO) CI-2 role-based access control is designed to conform with basic parts of the model contained in a American National Standards Institute draft [ANSI]. The draft standard has the following four parts, but CI-2 uses features from only the first three:

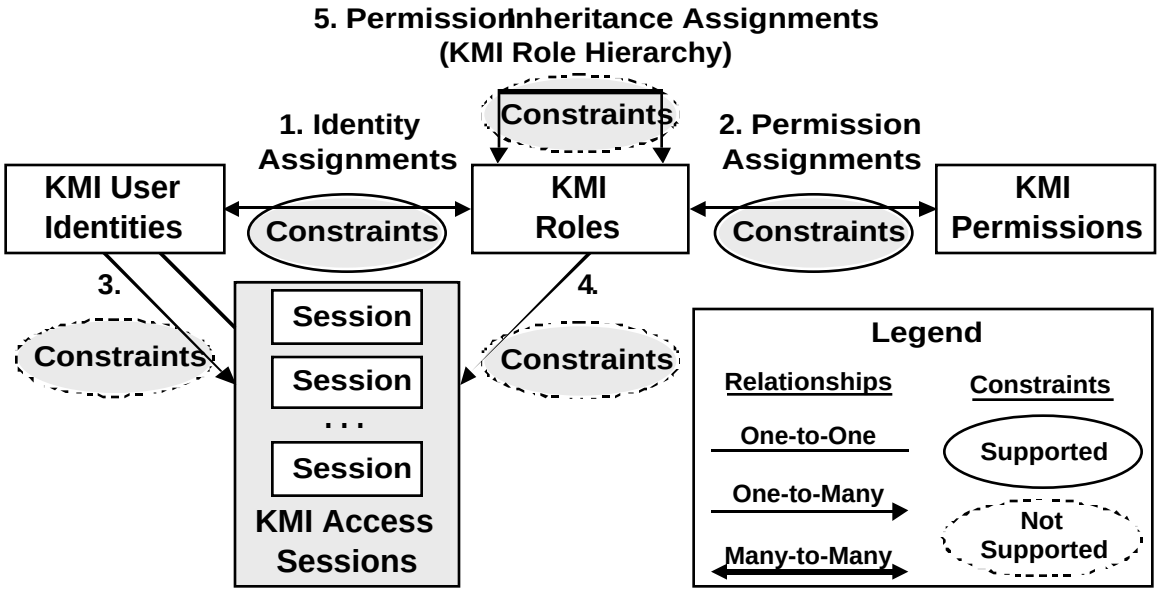
- **Core role-based access control**. CI-2 supports a minimal set of elements and relations.
- **Hierarchical role-based access control**. CI-2 supports partial ordering of roles.
- **Static Separation of Duty**. CI-2 supports exclusivity for role assignments.
- **Dynamic Separation of Duty**. CI-2 prohibits playing concurrent roles in a single session.

(U//FOUO) Figure 23 illustrates entities and relationships that comprise a role-based access control system. The system model includes the following five relationships:

- (U) Assignment of User Identities to Roles.
- (U) Assignment of Permissions to Roles.
- (U) Association of a User Identity with a Session.
- (U) Association of a Role with a Session.
- (U) Assignment of a Role to be inherit the permissions of another Role.

(U//FOUO) Figure 23 also illustrates that CI-2 supports constraints on relationships 1 and 2, but not on 3, 4, or 5.

**Figure 23. (U) KMI Role-Based Access Control**




UNCLASSIFIED//FOUO

### 5.1.1 (U) Definition and Maintenance of Roles and Permissions

(U//FOUO) A Role Manager maintains built-in roles and creates any new roles that are needed.

**CI2-SAR-5.1.1a** (U//FOUO) The KMI shall enable a Role Manager, and only a Role Manager, to create, review, modify, and delete Roles, in order to maintain built-in Roles and establish and maintain additional Roles. [DRV KRD 0404, 0406, 1203] {S}

(U//FOUO) The built-in roles are intended to be sufficient for initial KMI operation. However, the KMI needs to be extensible to managing new products in new situations, and thus new roles may be needed in the future.

(U//FOUO) Permissions identify actions the system is capable of performing. New permissions may be needed in the future and can only be added with software upgrades to the system. If a software upgrade contains new permissions they will be added to the list of permissions available for assignment to roles by the Role Manager. Also, Role Managers may need to treat sets of permissions as units in order to simplify their assignment to roles.

**CI2-SAR-5.1.1c** (U//FOUO) The KMI shall enable a Role Manager to establish and maintain new Permissions that are defined as sets of other, already existing Permissions. [DRV KRD 0404, 0406, 0873, 1794] {S}

### 5.1.2 (U) Assignment of Permissions to Roles

(U//FOUO) A Role Manager also administers the assignment of permissions to roles.

**CI2-SAR-5.1.2a** (U//FOUO) The KMI shall enable a Role Manager, and only a Role Manager, to assign Permissions to Management Roles (except for the Role of Role Manager), subject to any Constraints that may be in force at the time. [DRV KRD 0873, 0875, 0949, 1203, 1609, 1794, 2008] {S}

(U//FOUO) The principle of separation of duties implies that managers should not be able to assign their own authorizations:

**CI2-SAR-5.1.2b** (U//FOUO) A Role Manager shall not be able to assign Permissions to the Role of Role Manager. [DRV KRD 1560] {S}

(U//FOUO) Thus, all permissions needed by a Role Manager must be statically assigned to the role, i.e., built-in during implementation or configured during installation, to be available at system startup.

**CI2-SAR-5.1.2c** (U//FOUO) The KMI shall enable a Role Manager, and only a Role Manager, to remove Permissions from Management Roles. [DRV KRD 0873, 1203, 1560] {S}

**CI2-SAR-5.1.2d** (U//FOUO) The KMI shall record as a Mandatory Audit Event each action by a Role Manager that either (1) assigns a Permission to a Management Role or (2) removes a Permission from a Management Role. [DRV KRD 071, 0844, 0876, 1609] {S}

### 5.1.3 (U) Permission Inheritance in the Role Hierarchy

(U//FOUO) It is expected that managers will need to organize the set of KMI roles into a hierarchy to reflect lines of authority and responsibility in the KMI and in user organizations. Role hierarchies can be defined by using “Permission Inheritance” relationship illustrated by Figure 23. (This relationship is supported by the draft standard [ANSI].)

**DEFINITION** (U//FOUO) Role Hierarchy. A subordination relationship, “≤”, among Roles, where “A≤B” means that Role A is subordinate to Role B. The relationship is many-to-many and is a partial ordering of the set of all Roles. That is, for any three Roles A, B, and C, the following are always true: (1) A≤A; (2) if A≤B and B≤C, then A≤C; and (3) if A≤B and B≤A, then A and B must be the same Role.

**CI2-SAR-5.1.3a** (U//FOUO) The KMI shall maintain the set of all Management Roles as a Role Hierarchy. [DRV KRD 0403] {S}

(U//FOUO) A role can hold permissions directly, by having permissions assigned to it, and also can hold permissions indirectly, by inheriting permissions that are held by subordinate roles.

**CI2-SAR-5.1.3b** (U//FOUO) The KMI shall enable a Role Manager, and only a Role Manager, to assign one or more Roles in the Role Hierarchy to be subordinate to one or more

other Roles in hierarchy, so that the each superior Role inherits the Permissions that have previously been assigned to, or inherited by, its subordinate Role(s). [DRV KRD 0403] {S}

**CI2-SAR-5.1.3c** (U//FOUO) The KMI shall enable a Role Manager to remove a Role from a position of subordination to another Role in the Role Hierarchy. [DRV KRD 0403] {S}

**CI2-SAR-5.1.3d** (U//FOUO) The KMI shall record for Audit all User actions that assign a Role to be subordinate to another Role in the Role Hierarchy, or that remove a Role from a position of subordination. [DRV KRD 0071, 0844, 1609] {S}

### 5.1.4 (U) Assignment of Identities to Roles

(U//FOUO) User identities acquire access permissions when they are assigned to roles. The following requirements apply to all instances of assignment of an identity to a role:

**CI2-SAR-5.1.4a** (U//FOUO) The KMI shall record as a Mandatory Audit Event each action that either (1) assigns a User Identity to a Role or (2) removes an Identity from a Role. [DRV KRD 0071, 0844, 0876] {R}

(U//FOUO) Assignments of identities to management roles are subject to role-based access control constraints that are described in the “Constraints on Identities, Roles, Permissions, and Sessions” section.

**CI2-SAR-5.1.4b (U//FOUO)** The assignment of a User Identity to a Management Role shall be subject to applicable, existing Constraints on the relationships of the KMI role-based Access Control system. [DRV KRD 0872] {R-S}

**CI2-SAR-5.1.4c** (U//FOUO) The KMI shall permit a User Identity to be assigned to two or more Roles, in any combination that is not prohibited by a requirement stated in this *Specification* [KMI2200] or by a Constraint imposed by an Administrative Manager. [DRV KRD 1576, 1604, 1617, 1618, 1620] {R-S}

**CI2-SAR-5.1.4f** (U//FOUO) The KMI shall permit a User Identity that has been assigned to the Role of Enrollment Manager to be assigned also to either or both of the Roles of Controlling Authority and Product Requester. [DRV KRD 1620] {R-S}

(U//FOUO) If a user identity is assigned twice or more to the same role, then the user has the same role-based permissions in each assignment. However, if the role is one that receives rule-based or approval-based authorizations, then those authorizations can be different for each of the two or more assignments.

**CI2-SAR-5.1.4e** (U//FOUO) The KMI shall permit a User Identity to be assigned twice or more to the same Role; but such assignments shall be treated as distinct Managers, each with its own rule-based and approval-based Authorizations, if such Authorizations apply to the Role. [DRV KRD 1617, 1618] {R}

**CI2-SAR-5.1.4d** (U//FOUO) If a Registered User is acting in a Management Role that can assign a User Identity to a Management Role, the KMI shall not permit the User to assign

any of the User's own User Identities (including Set Identities) to any Management Role. [DRV KRD 1560] {R}

(U//FOUO) In this *Security Architecture,* the role of Enrollment Manager can make assignments to management roles, and the role of KOA Manager can make assignments to the KOA Agent role. These assignment functions are specified in the following subsections.

#### 5.1.4.1 (U) Assignment of Identities to the KOA Agent Role

(U//FOUO) A KOA Manager assigns users only to the KOA Agent role.

**CI2-SAR-5.1.4.1a** (U//FOUO) The KMI shall enable an authorized KOA Manager to assign a User Identity to the Role of KOA Agent, and only to that Role, either at the time of initial registration of the identity or at a later time, according to approved procedures. [DRV KRD 0405, 1487, 1599, 1617] {R}

(U//FOUO) System functions associated with KOA Agents are described in detail in the "KMI Operating Accounts" section.

#### 5.1.4.2 (U) Assignment of Identities to Management Roles

(U//FOUO) In addition to the primary registration process that establishes user identities, CI-2 also has a secondary registration process, called "enrollment", for performing additional steps that are required to assign identities to management roles, which hold the sensitive authorizations needed to operate and administer the KMI and which are restricted to relatively few users.

**DEFINITION** (U//FOUO) Enrollment. The KMI process that assigns a User Identity to a Management Role.

(U//FOUO) During the enrollment process, as illustrated by Figure 24, an Enrollment Manager assigns an existing user identity to a management role, and thus creates an instance of a manager. The Enrollment Manager is said to confer the management role on the identity. In the simplified example shown in the figure, an Enrollment Manager has made five different assignments involving two human users, three identities, and three roles, resulting in five different manager instances.

(U//FOUO) For some roles, the enrollment process assigns attribute values for rule-based access control (RuBAC), which constrains permissions granted by role-based access control (see "Rule-Based Access Control" section). If the new manager is an Enrollment Manager, the process also provides the manager with (1) authorizations to confer specific roles and (2) authorizations to assign specific RuBAC attributes to managers (see "Enrollment Managers" section).

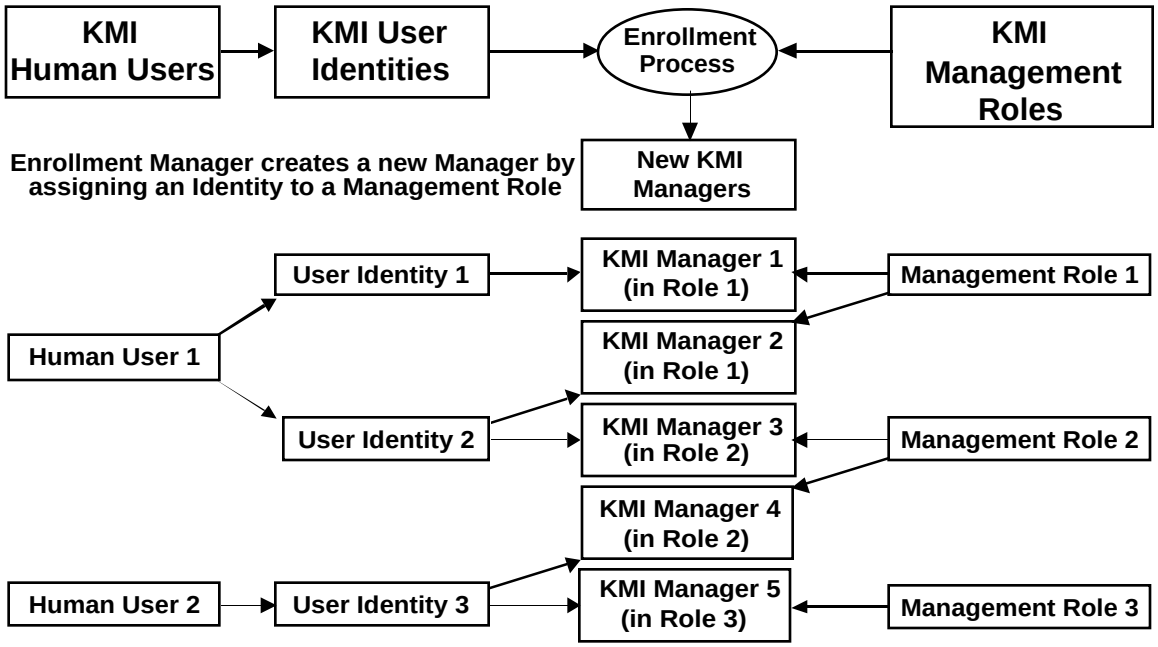
**CI2-SAR-5.1.4.2a** (U//FOUO) The KMI shall enable an Enrollment Manager, and only an Enrollment Manager, to assign a Singular Identity of a Human User to any Management Role. [DRV KRD 0405, 0671, 1487, 1617, 1618, 2008] {R}

**CI2-SAR-5.1.4.2b** (U//FOUO) The KMI shall enable an Enrollment Manager, and only an Enrollment Manager, to assign a Shared Identity of a User Set of Human Users to any

External Management Role, but not to any Internal Management Role. [DRV KRD 0405, 0671, 1487, 1617, 1618, 2008] {R}

(U//FOUO) The two foregoing requirements do not enable an identity of a user device to be assigned to a management role.

**Figure 24. (U) KMI Enrollment of Managers with Examples**




**UNCLASSIFIED//FOUO**

**CI2-SAR-5.1.4.2e** (U//FOUO) The KMI shall enable an Enrollment Manager, and only an Enrollment Manager, to assign a Group Identity to a Management Role, if and only if the Enrollment Manager has been granted specific Authorization to make such an assignment. [DRV KRD 0863, 1487, 1585] {R}

(U//FOUO) The foregoing requirement recognizes that although the KMI needs to maintain strict, individual accountability for access by users acting as managers, the user community needs operational flexibility to help them adjust to new technology that the KMI is introducing. The best practice would be to prevent assignment of a group identity to any management role, because the KMI cannot maintain individual accountability within a group identity. However, in early capability increments, the best way to meet the operational needs in some situations might be to keep a single authentication token locked in a safe for use by a group identity that collectively performs the manager function. Thus, exceptional circumstances may require that a group identity be assigned to a management role, even if accountability for that identity can be maintained only at the group's local site by physical, personnel, and administrative security measures. However, such assignments should require special authorization.

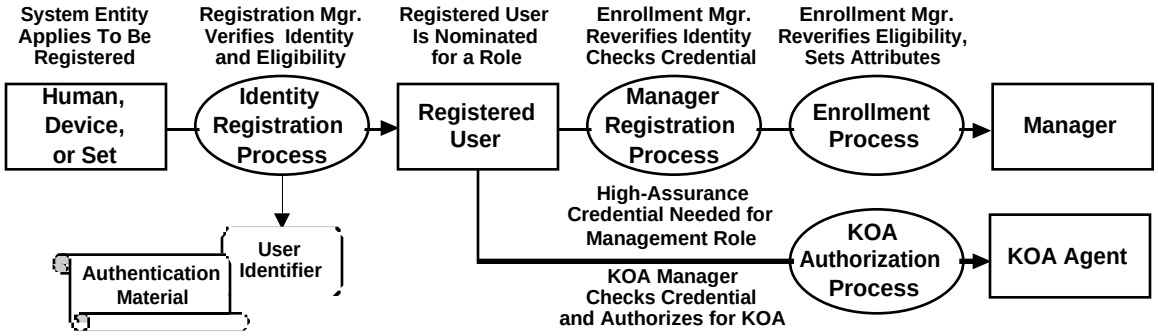
**CI2-SAR-5.1.4.2d** (U//FOUO) The KMI shall permit a User Identity to be enrolled twice or more by either the same Enrollment Manager or different Enrollment Managers. [DRV KRD 1604, 1617, 1618] {R}

(U//FOUO) The foregoing requirement enables a user identity to be assigned to two or more roles, or be assigned twice or more to the same role in different situations.

### 5.1.4.3 (U) Verification of Authenticity and Eligibility for Managers

(U//FOUO) Figure 25 illustrates how the basic registration process for user identities is followed by supplemental registration and enrollment processes when a registered user is nominated to be a manager. (Although the figure shows the "Manager Registration" step preceding the "Enrollment" step, these steps could be done in the opposite order or in parallel, depending on the specific operational procedures that are adopted for CI-2.)

**Figure 25. (U) KMI User Registration and Manager Enrollment**




**UNCLASSIFIED//FOUO**

(U//FOUO) When a user identity is assigned to a management role, the KMI establishes authentication material for a very strong authentication mechanism, as specified in the "Issuance of Identifier Credentials" section of Volume 2. When a user identity is assigned only to the KOA Agent role, the KMI establishes authentication material for whatever type of authentication mechanism the user is able to support, ranging from the same strong form used for managers to a simple, password-based form.

(U//FOUO) For each user identity that the KMI registers, a User Registration Manager examines evidence to verify the user's authenticity (i.e., that the user has the right to claim the identity being registered) and eligibility (i.e., that the identity is eligible for KMI registration), as described in the "User Identity Authenticity and Eligibility" section of Volume 2. When a user identity is assigned to a management role, the Enrollment Manager reverifies that authenticity and eligibility, and also verifies or certifies that the assignment is authorized.

**CI2-SAR-5.1.4.3a** (U//FOUO) For each assignment of a User Identity to a Management Role, the KMI shall record and maintain data elements that (1) describe the evidence that was presented and examined to verify the authenticity and eligibility of the Identity and (2) ensure accountability for approval of the evidence. [DRV KRD 0923, 1593] {R-S}

(U//FOUO) Appendix A of Volume 2 proposes a partial, draft listing of acceptable forms for evidence of authenticity and eligibility of managers.

**CI2-SAR-5.1.4.3b** (U//FOUO) When an Enrollment Manager assigns a User Identity to a Management Role, the KMI shall prompt the Enrollment Manager to verify and enter (1) evidence of the identity's authenticity and eligibility to be a Registered User and Manager and (2) the organizational source of authority for the assignment. [DRV KRD 0923, 1593] {R}

(U//FOUO) The following requirements restrict eligibility for assignment to certain management roles according to nationality. These requirements are marked "NT" because it is assumed that they will be implemented procedurally, at the time when an Enrollment Manager determines whether an identity is eligible for assignment to a role. (Implementing these requirements as PRSN functions would at least require the system to record and adequately maintain nationality information for user identities.)

**CI2-SAR-5.1.4.3c** [NT] (U//FOUO) The KMI shall not assign a Singular Identity of a Human User to an Internal Management Role unless that person belongs to a U.S. Security Domain. [KRD NEW] {R}

**CI2-SAR-5.1.4.3d** [NT] (U//FOUO) The KMI shall not assign a Singular Identity of a Human User to an External Management Role unless that Identity belongs to a U.S. Security Domain, NATO Security Domain, or CCEB Security Domain. [KRD NEW] {R}

**CI2-SAR-5.1.4.3e** [NT] (U//FOUO) The KMI shall not assign a Shared Identity of a User Set of Human Users to an External Management Role unless each Identity in the User Set belongs to a U.S. Security Domain, NATO Security Domain, or CCEB Security Domain. [KRD NEW] {R}

**CI2-SAR-5.1.4.3f** [NT] (U//FOUO) The KMI shall not assign a Singular Identity of a User Device to the Role of Product Requester unless that Identity belongs to a U.S. Security Domain, NATO Security Domain, or CCEB Security Domain. [DRV KRD 1601, 2149] {R}

(U//FOUO) A consequence of the three preceding requirements is that non-NATO, non-CCEB Coalition Partners cannot perform the roles of Controlling Authority, Product Requester, and KOA Manager and, therefore, are prevented from ordering products. Products for such Coalition Partners are ordered and distributed only by U.S. managers.

### 5.1.4.4 (U) Manager Reverification and Reconfirmation

(U//FOUO) The "User Identity Reverification" section of the *Security Policy* states requirements for periodically reverifying the authenticity and eligibility of each active user identity, in the same manner as if the identity were being newly registered. Those requirements are extended by the following statements:

**CI2-SAR-5.1.4.4a** (U//FOUO) For each existing assignment of a User Identity to a Management Role in an Enrollment Domain, the KMI shall periodically prompt an Enrollment Manager in that Enrollment Domain to examine and reverify evidence of the

Identity's authenticity and eligibility, in accordance with the *KMI Policy for Registration of Users* [NSAKMIUR]; and if that is not done within a specified time interval, the KMI shall revoke the assignment. [DRV KRD 0925] {R}

**CI2-SAR-5.1.4.4b** (U//FOUO) The KMI shall enable a Security Configuration Manager to configure the periodicity of reverification by an Enrollment Manager of the authenticity and eligibility of a User Identity assigned to a Management Role. [DRV KRD 0925] {R-S}

**CI2-SAR-5.1.4.4c** (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to set the time interval within which an Enrollment Manager must complete reverification of a User Identity that is assigned to a Management Role. [DRV KRD 0925] {R-S}

(U//FOUO) To verify a user identity with sufficient assurance for assignment to management roles, the KMI might require the user to make a personal appearance before some official, but this type of reverification might be done only infrequently. On the other hand, reconfirmation that an assignment is authorized might be done more frequently and, therefore, is specified here separately from reverification of the basic authenticity and eligibility of the identity.

**CI2-SAR-5.1.4.4d** (U//FOUO) For each existing assignment of a User Identity to a Management Role in an Enrollment Domain, the KMI shall periodically prompt an Enrollment Manager in that Enrollment Domain to review and reconfirm the need for, and organizational source of authority for, the assignment, in accordance with the *KMI Policy for Enrollment of Managers* [NSAKMIEM]; and if that is not done within a specified time interval, the KMI shall revoke the assignment. [DRV KRD 0952] {S}

**CI2-SAR-5.1.4.4e** (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to configure the periodicity of reconfirmation by an Enrollment Manager of an assignment of a User Identity to a Management Role. [DRV KRD 0952] {R-S}

**CI2-SAR-5.1.4.4f** (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to set the time interval within which an authorized Enrollment Manager must complete reconfirmation of an assignment of a User Identity to a Management Role. [DRV KRD 0952] {R-S}

### 5.1.5 (U) Sessions and Principals

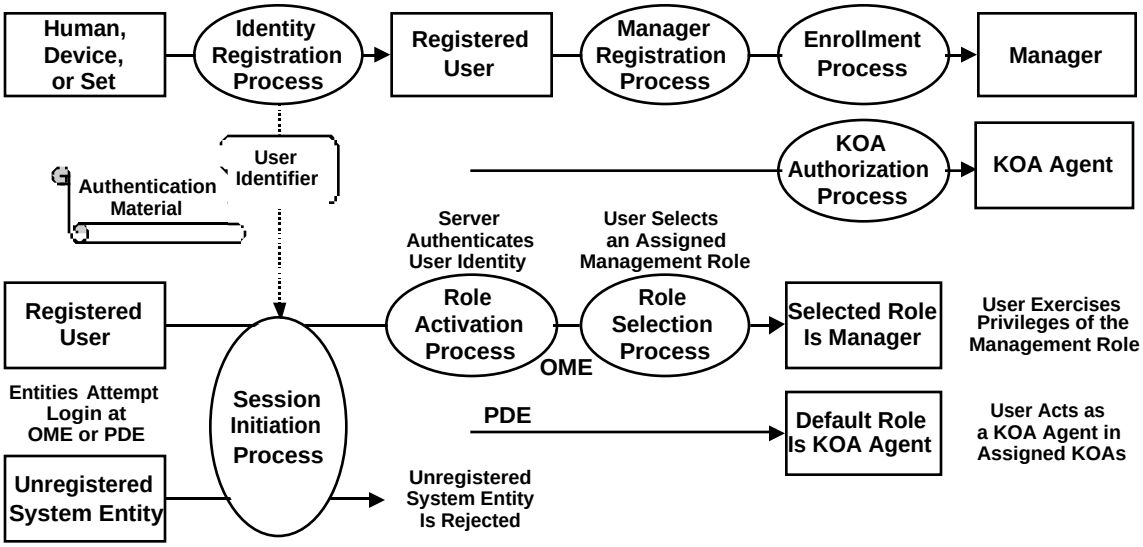
(U//FOUO) As illustrated by Figure 26, a user gains accesses to the KMI by presenting an identifier for a registered identity.

**DEFINITION** (U//FOUO) Principal. A specific User Identity that is asserted and activated by a Registered User when accessing the system.

(U//FOUO) The user then selects a role to which that identity has been assigned, and the KMI establishes a session.

**DEFINITION** (U//FOUO) Session. A temporary mapping of a Principal to a Role or Roles (especially when a Client Node accesses a PRSN).

**Figure 26. (U) KMI Registration, Enrollment, and Login**




**UNCLASSIFIED//FOUO**

(U//FOUO) Figure 26 illustrates two cases in which a session is established with a role:

- **Management role**. If a registered user has been assigned to one or more management roles, the user can select one of those roles for a session when logging in at an OME or some other node that supports role-based access control.

- **KOA Agent role**. If a registered user has been assigned to the KOA Agent roles, selection of that role is implicit when the user logs in at a PDE.

(U//FOUO) The session abstraction has various concrete interpretations, depending on the type of user and the mode of access. This specification of role-based access control for CI-2 is directed mainly at the case of a Client Node accessing a PRSN, through either a Web-based or transaction-based interface, but this specification also covers other pairs of nodes or components. An access session usually involves all three of the following aspects:

- (U) **Platform access.** A session is a continuous period of time, typically initiated by an identity authentication process, during which a user accesses a server computer system.

- (U) **Application access.** A session is a set of transactions or other actions that are performed by or for a user during a period of time.

- (U) **Network access.** A session is a persistent but, usually, temporary communication association between a client (or agent) and a server (or peer), usually involving a KPC.

(U//FOUO) Each session is associated with a single principal and, therefore, is controlled by a single user.

**CI2-SAR-5.1.5a** (U//FOUO) An Independent Component shall prevent a Singular Identity from initiating two or more concurrent Sessions under the control of that Component. [DRV KRD 0953] {R} (Also see "Separation of Duties" in "Access Control Services" section.)

**CI2-SAR-5.1.5b** (U//FOUO) An Independent Component may permit a Group Identity to initiate either a single Session or two or more concurrent Sessions under the control of that Component. [DRV KRD 2105] {R}

**CI2-SAR-5.1.5c** (U//FOUO) If an Independent Component permits a Shared Identity to initiate two or more concurrent Sessions, the Component may permit the Session's Principals to play either the same Role or different Roles. [DRV KRD 2105] {R}

**CI2-SAR-5.1.5d** (U//FOUO) If the design of a Component enables a User Identity to initiate two or more concurrent Sessions, the Component shall enable a Security Configuration Manager to limit the number of concurrent Sessions. [DRV KRD 2139] {R}

### 5.1.6 (U) Session Restrictions and Permission Checking

(U//FOUO) The permissions available to a principal in a session are those that are currently assigned to the role that the principal is playing in the session. The KMI permits a principal to access only system resources for which the role has permissions, but managers need to be careful to assign to each role only the minimum permissions that the role needs to perform its duties.

**CI2-SAR-5.1.6a** (U//FOUO) When a Registered User accesses an Independent Component in a User Identity that is authenticated at the start of a Session, the KMI shall permit the User to select and play any of the Roles, and only those Roles, to which the Principal identity is currently assigned and for which the authentication process provides sufficient assurance. [DRV KRD 0865, 1550, 1552] {P-R-S}

**CI2-SAR-5.1.6b** (U//FOUO) When a Registered User accesses an Independent Component in an User Identity that is currently assigned twice or more to the same Role, then the KMI shall enable the User to distinguish among those assignments and to select one of them for the Session. [DRV KRD 1617, 1620] {R}

(U//FOUO) Assigning an identity to the same role twice probably makes sense only when the assignments are made in two different enrollment domains where neither is a subdomain of the other (see "Enrollment Domains" section below). For example, an identity could be enrolled twice as a Controlling Authority to enable someone to jointly support two different DoD Services or agencies that operate separate enrollment authorities. In that case, when presenting the two assignments to the user for selection at login time, the KMI could them distinguish them by, for example, appending the domains' names.

**CI2-SAR-5.1.6c** (U//FOUO) When a Registered User accesses an Independent Component in a Session, the KMI shall permit the User to play only one Role at a time during the Session. [DRV KRD 0953] {R}

(U//FOUO) Note that the foregoing requirement does not prevent a user from selecting the same role in concurrent Sessions at different Core Nodes.

**CI2-SAR-5.1.6d** (U//FOUO) When a Registered User accesses an Independent Component in an authenticated User Identity, the KMI shall permit the session's Principal to play a Management Role only if the identity has been authenticated to the KMI using a mechanism approved by NSA for Managers. [DRV KRD 1603] {R}

**CI2-SAR-5.1.6e** (U//FOUO) When a Registered User accesses the KMI in an User Identity that is authenticated with a mechanism approved for Management Roles, the KMI shall enable the User to switch during the Session from one Role to another, without having either to reauthenticate the User Identity or to end the Session and begin a new one. [DRV KRD 1604, 1607] {R}

**CI2-SAR-5.1.6f** (U//FOUO) When a Registered User accesses the KMI in a Role, the KMI shall permit the User to exercise only those Permissions that are currently assigned to that Role. [DRV KRD 0407, 0865, 1289, 1552] {P-R-S}

**CI2-SAR-5.1.6g** (U//FOUO) The KMI shall check the Permissions associated with the Role being played by a Principal before permitting access to products, services, or other System Resources, and shall reveal to the User only those resources which the Principal is authorized to access. [DRV KRD 0865, 0946, 1290, 1552] {P-R-S}

(U//FOUO) The KMI needs to control access to its resources not only by entities that are outside the system but also by entities inside the system, including access to one component by another component. The definitions of "System Entity" and "User" that are stated in the "User Entities**"** section enable this policy to specify such inter-component, intra-system controls.

**CI2-SAR-5.1.6h** (U//FOUO) Each Independent Component shall check the eligibility of another Component to access selected KMI capabilities, products, or information prior to permitting access by the other Component. [DRV KRD 1546.] {Z}

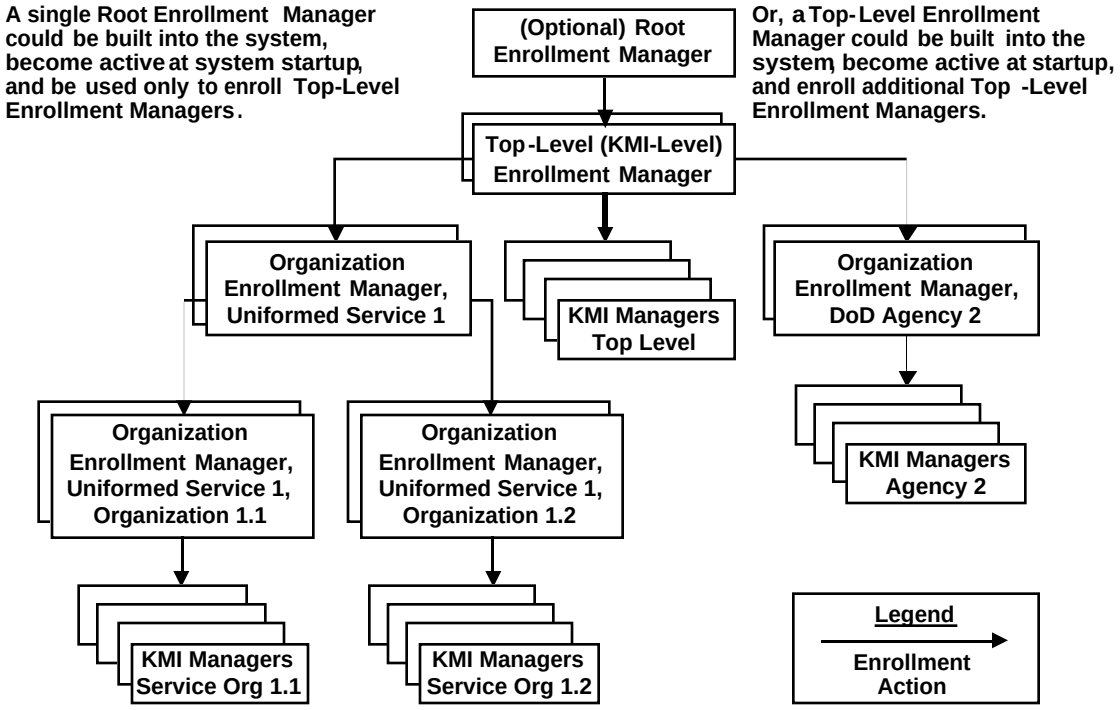
**CI2-SAR-5.1.6i** (U//FOUO) No operator at a Component shall be able to employ Permissions in excess of the capabilities or security attributes of that Component. [KRD 0881] {Z}

### 5.1.7 (U) Enrollment Managers

(U//FOUO) During the system startup process, at least one user identity needs to be initialized as an Enrollment Manager. As illustrated by Figure 27, this manager is called a Top-Level Enrollment Manager because it operates at the highest of, potentially, multiple levels of Enrollment Managers. Alternatively, this manager could be called a KMI-Level Enrollment Manager, because it can confer roles for which the scope of operation extends over the entire KMI.

**DEFINITION** (U//FOUO) Top-Level Enrollment Manager. A KMI job position held by a Human User who has a User Identity that is initialized in the Role of Enrollment Manager as part of the KMI startup process, and is then able to enroll other User Identities in Management Roles. (An Enrollment Manager also has RuBAC management responsibilities, as described in the "Rule-Based Access Control" section.)

**Figure 27. (U) KMI Enrollment Manager Examples**




**UNCLASSIFIED//FOUO**

(U//FOUO) As illustrated by Figure 27, a single Root Enrollment Manager position could be built into the system, be made active at startup, and be used only to enroll all of the Top-Level Enrollment Managers. Alternatively, a Top-Level Enrollment Manager position could be built into the system, be made active at system startup, and be used to enroll additional Top-Level Enrollment Managers as well as perform the other duties of a Top-Level Enrollment Manager. Other highly sensitive roles for internal, operational management might also be built into the system so that they would not have to be assigned after system startup.

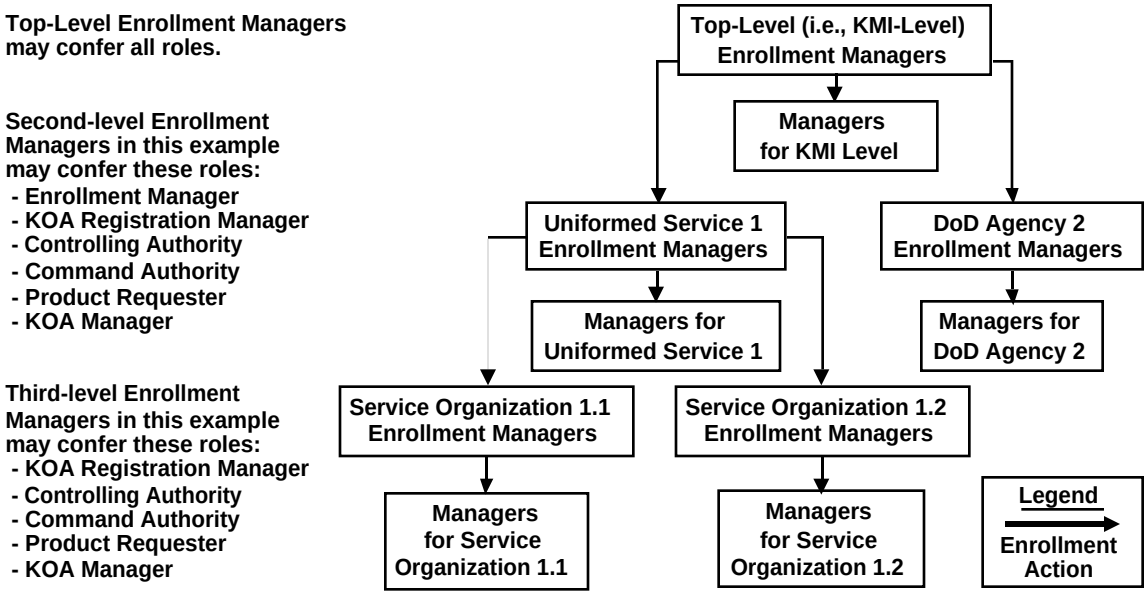
(U//FOUO) As illustrated by the simplified example in Figure 27, a Top-Level Enrollment Manager enrolls other Enrollment Managers—one or more for each of the user organizations named "Uniformed Service 1" and "DoD Agency 2". The figure assumes that Service 1 chooses to delegate enrollment authority to Organizations 1.1 and 1.2 (i.e., organizations within Service 1), and so an Enrollment Manager at the Service 1 headquarters level enrolls one or more additional Enrollment Managers for each suborganization. In contrast to Service 1, Agency 2 chooses to centralize its enrollment authority; therefore, Enrollment Managers at the Agency 2 headquarters level do not enroll any other Enrollment Managers.

(U//FOUO) Not every Enrollment Manager can confer every role. Especially sensitive roles need to be either (1) built into the system so that they are available at startup or (2) capable of being restricted so that they can be conferred only by Top-Level Enrollment Managers. For example, as illustrated by Figure 28, a Top-Level Enrollment Manager might enroll one or more additional Enrollment Managers for each user organization that wants to operate its own enrollment process, but give those organization Enrollment Managers only the ability to confer six different

roles: (1) Enrollment Manager, (2) KOA Registration Manager, (3) Controlling Authority, (4) Command Authority, (5) Product Requester, and (6) KOA Manager.

(U//FOU) The decision whether to delegate or centralize enrollment is left to each organization. However, an Enrollment Manager of a user organization at any level can create an Enrollment Manager for a suborganization without conferring the authority to create further Enrollment Managers. For example, as illustrated by Figure 28, the Enrollment Managers at the headquarters level of Uniformed Service 1 create Enrollment Managers for Service Organizations 1.1 and 1.2, but those new managers cannot themselves create Enrollment Managers.

**Figure 28. (U) KMI Enrollment Authorization Examples**




UNCLASSIFIED//FOUO

**CI2-SAR-5.1.7a** (U//FOUO) The KMI shall initialize, at system startup, at least one User Identity in the Role of Top-Level Enrollment Manager. [DRV KRD 1617] {R-S}

**CI2-SAR-5.1.7b** (U//FOUO) The KMI shall authorize a Top-Level Enrollment Manager to confer all defined Management Roles (i.e., including that of Enrollment Manager) except for any special positions that might be built into the system as part of the startup process. [DRV KRD 1617] {R}

**CI2-SAR-5.1.7c** (U//FOUO) The KMI shall enable an Enrollment Manager, when conferring the Role of Enrollment Manager, to restrict the enrollment capabilities of the new Enrollment Manager, by specifying which Roles the new Enrollment Manager is authorized to confer. [DRV KRD 1618] {R}

**CI2-SAR-5.1.7d** (U//FOUO) The KMI shall enable an Enrollment Manager, when conferring the Role of Enrollment Manager, to authorize the new Enrollment Manager to confer any subset, up to and including the entire set, of the roles that the conferring

Enrollment Manager itself is authorized to confer, but only those roles. [DRV KRD 1618] {R}

**CI2-SAR-5.1.7e** (U//FOUO) The KMI shall prevent an Enrollment Manager from enrolling a User Identity in any Role which the Enrollment Manager has not been authorized to confer. [DRV KRD 1618] {R}

**CI2-SAR-5.1.7f** (U//FOUO) The KMI shall prevent a User Identity that is acting in the Role of Enrollment Manager from being able to enroll any User Identity that belongs to the same User. [DRV KRD 1560] {R}

### 5.1.8 (U) Constraints on Identities, Roles, Permissions, and Sessions

(U//FOUO) Some of the requirements that are stated in the "Enrollment Managers" section are examples of being able to apply the principles of (1) separation of duties and (2) least privilege. More detailed capabilities for implementing and enforcing the principle of least privilege are stated in subsections that follow.

**CI2-SAR-5.1.8a** [NT] (U//FOUO) The KMI shall be designed to minimize the number of distinct Management Roles that must be staffed by separate persons, while still separating management duties and Permissions sufficiently to ensure security. [DRV KRD 0951, 1196] {Z}

**CI2-SAR-5.1.8b** (U//FOUO) The KMI shall enable a Security Configuration Manager to (1) set and modify limits on the assignment of Permissions to Roles and (2) constrain the exercise of Permissions. [DRV KRD 0872, 0952] {S}

**CI2-SAR-5.1.8c** (U//FOUO) The KMI shall enable a Security Configuration Manager to set and modify resource consumption limits for Management Roles. [DRV KRD 2008] {R-S}

(U//FOUO) To control proliferation of management permissions, reduce the chances of making mistakes when granting those permissions, or limit the exercise of permissions, it could be desirable to constrain the assignment and selection relationships that are shown in Figure 23.

**DEFINITION** (U//FOUO) Constraint. A limitation, implemented by role-based Access Control, on a relationship or function of a User Identity, a Role, or a Permission. (In effect, a constraint is a form of security policy.)

(U//FOUO) This *Security Architecture* specifies constraint mechanisms for relationships 1 and 2. However, to reduce the complexity of implementing CI-2, this *Architecture* does not support constraints on relationship 3 (for example, preventing a specified role from being made subordinate to another role). Also, this *Architecture* supports only static constraints in CI-2. Therefore, constraints are not supported for relationship 4 (e.g., setting a maximum number of concurrent sessions for an identity) or relationship 5 (e.g., setting a maximum number of concurrent sessions permitted for a role).

### 5.1.8.1 (U) Static Separation Constraints

(U//FOUO) The security of the KMI access control processes depends on separating the duties of certain specific roles.

**CI2-SAR-5.1.8.1a** (U//FOUO) The KMI shall prevent a Registered User from having one of its User Identities assigned to the Role of User Registration Manager and also concurrently having that identity or another of its identities assigned to the Role of Enrollment Manager. [DRV KRD 0951, 1619] {S}

(U//FOUO) KMI security administrators also need to be able to set other constraints to enforce separation of duties.

**CI2-SAR-5.1.8.1d** (U//FOUO) The KMI shall enable a Security Configuration Manager to specify sets of two or more Management Roles such that the KMI shall prevent a Registered User from having a User Identity or Identities concurrently assigned to two Roles in a set. [DRV KRD 0951, 1621] {S}

**CI2-SAR-5.1.8.1e** (U//FOUO) The KMI shall enable a Security Configuration Manager to specify sets of two or more Management Roles such that the KMI shall prevent a Registered User from having a User Identity or Identities concurrently assigned to all the Roles in a set. [DRV KRD 951, 1621] {S}

**CI2-SAR-5.1.8.1f** (U//FOUO) The KMI shall enable a Security Configuration Manager to specify sets of two or more Management Roles such that the KMI shall prevent a specified Permission from being assigned to more than one Role in a set. [DRV KRD 0952] {S}

**CI2-SAR-5.1.8.1g** (U//FOUO) The KMI shall enable a Security Configuration Manager to specify sets of two or more Permissions such that the KMI shall prevent more than one Permission in a set from being concurrently assigned to the same Management Role. [DRV KRD 0952] {S}

### 5.1.8.2 (U) Static Cardinality Constraints

(U//FOUO) KMI SSOs need to be able to set constraints to limit the granting of permissions.

**CI2-SAR-5.1.8.2a** (U//FOUO) The KMI shall enable a Security Configuration Manager to prevent more than a specified number of User Identities from being concurrently assigned to a specified Management Role. [DRV KRD 0951] {S}

**CI2-SAR-5.1.8.2b** (U//FOUO) The KMI shall enable a Security Configuration Manager to prevent a specified User Identity from being concurrently assigned to more than a specified number of Management Roles. [DRV KRD 0951] {S}

**CI2-SAR-5.1.8.2c** (U//FOUO) The KMI shall enable a Security Configuration Manager to prevent more than a specified number of Permissions from being concurrently assigned to a specified Management Role. [DRV KRD 0952] {S}

**CI2-SAR-5.1.8.2d** (U//FOUO) The KMI shall enable a Security Configuration Manager to prevent a specified Permission from being concurrently assigned to more than a specified number of Management Roles. [DRV KRD 0952] {S}

### 5.1.9 (U) Enrollment Domains

(U//FOUO) KMI management roles are usually conferred on individual persons. However, KMI customers often want to control the assignment of these roles, and the authorizations associated with them, from an organizational viewpoint rather than an individual viewpoint. Therefore, CI-2 enables the processes that confer these and their authorizations to be aligned with administrative procedures of customer organizations, by grouping managers into enrollment domains.

**DEFINITION** (U//FOUO) Enrollment Domain. A set of Managers (i.e., a set of assignments of User Identities to Management Roles) that includes (1) one or more Enrollment Managers and (2) any additional Managers of other types that have been placed into the domain.

(U//FOUO) CI-2 enables enrollment domains to be arranged in a hierarchy aligned with the command structures of customer organizations. If an Enrollment Manager belongs to a enrollment domain, then that manager can enroll additional managers of various types, and can control rule-based authorizations, both in that enrollment domain and in other, subordinate enrollment domains in the hierarchy. (The concept of hierarchical domains is also potentially applicable to other functions in KMI. For example, access to tracking, accounting, or audit data for management actions could be limited to managers that are at or above the hierarchical level of the managers that performed the actions. However, this *Security Architecture* does not now specify any such additional applications.)

#### 5.1.9.1 (U) Hierarchy of Enrollment Domains

(U//FOUO) CI-2 enables enrollment domains to be arranged in a hierarchy that is a rooted tree.

**DEFINITION** (U//FOUO) Enrollment Domain Hierarchy. A subordination relationship among all Enrollment Domains, that is one-to-many and is transitive. (That is, if enrollment domain A is subordinate to domain B, and B is subordinate to C, then A is also subordinate to C. If A is subordinate to B, then B is said to be superior to A.)

(U//FOUO) The Enrollment Domain Hierarchy starts out with at least a top-level domain, which is the root of the tree.

**CI2-SAR-5.1.9.1a** (U//FOUO) The KMI shall, at system startup, initialize a hierarchy of Enrollment Domains by (1) establishing an Enrollment Domain called the “Top-Level Enrollment Domain” and (2) enrolling in that domain one or more Enrollment Managers called “Top-Level Enrollment Managers”. [DRV KRD 1618] {R}

(U//FOUO) After system startup, Enrollment Managers in existing enrollment domains may establish new enrollment domains that are subordinate to their own.

**CI2-SAR-5.1.9.1b** (U//FOUO) The KMI shall enable each Enrollment Manager in an existing Enrollment Domain to create a new Enrollment Domain that is subordinate to the

Manager's own domain (i.e., place the new Enrollment Domain into the Enrollment Domain Hierarchy in a position either (1) immediately subordinate to the Manager's own domain or (2) immediately subordinate to an existing, third domain that is already subordinate to the manager's own domain). [DRV KRD 1618] {R}

(U//FOUO) Figure 29 illustrates a fictitious enrollment domain hierarchy that has the following:

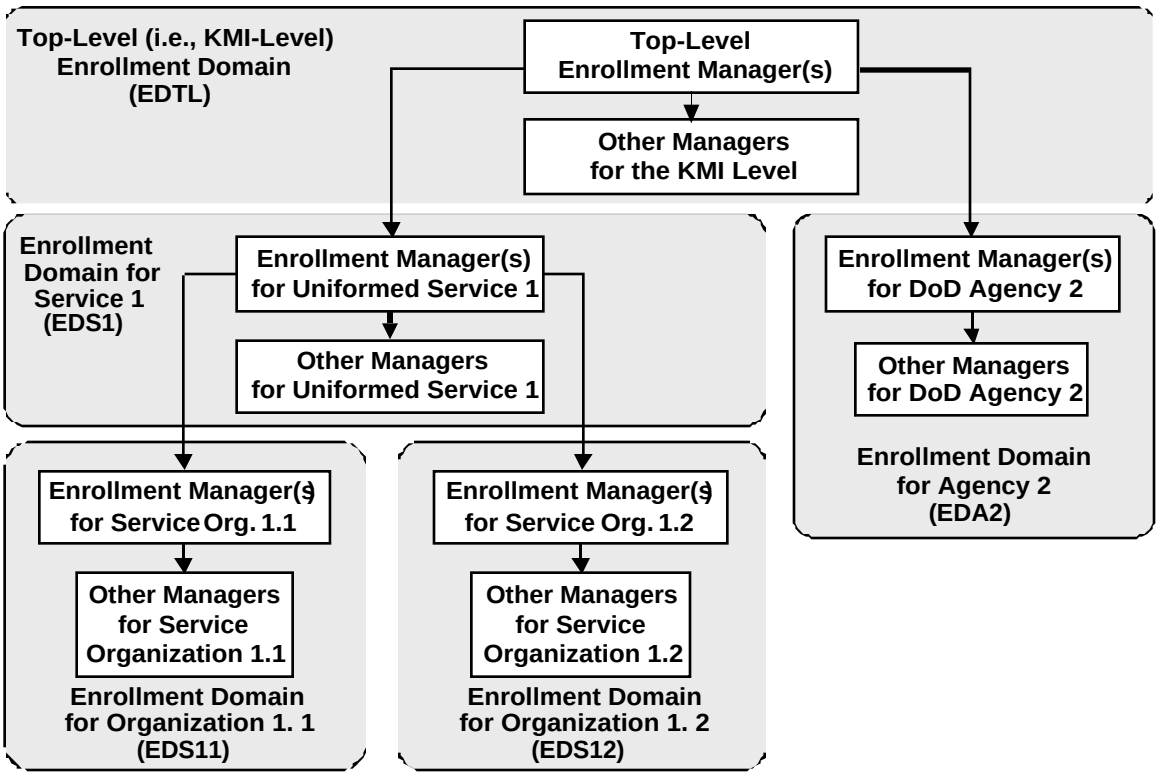
- The enrollment domain for Service 1 ("EDS1") and the one for Agency 2 ("EDA2") are both immediately subordinate to Top-Level Enrollment Domain ("EDTL").
- The enrollment domains for Service Organizations 1.1 and 1.2 ("EDS11" and "EDS12") are both immediately subordinate to EDS1.
- Because the domain subordination relationship is transitive, EDS11 and EDS12 are subordinate to EDTL.
- Also, EDTL is superior to all of the other Enrollment Domains.

**CI2-SAR-5.1.9.1c** (U//FOUO) When an Enrollment Manager creates a new, subordinate Enrollment Domain, the KMI shall (1) enable the Manager to choose for that domain an "Enrollment Domain Identifier" that can be unambiguously represented by a printable, non-blank character string and (2) ensure that the name is unique among any peer subordinate domains that have the same immediately superior domain. [DRV KRD 1618] {R}

(U//FOUO) When CI-2 is deployed, the actual domains that are immediately subordinate to the Top-Level Enrollment Domain might, for example, be the following:

- (U) United States Army
- (U) United States Navy
- (U) United States Air Force
- (U) United States Marine Corps
- (U) United States Coast Guard
- (U) United States Public Health Service
- (U) National Oceanic and Atmospheric Administration
- (U) Other (for other KMI user organizations).

**Figure 29. (U) KMI Enrollment Domain Examples**




**UNCLASSIFIED//FOUO**

### 5.1.9.2 (U) Enrolling Managers in Enrollment Domains

(U//FOUO) Each Enrollment Manager can enroll managers in (1) that Enrollment Manager's own domain and in (2) any domains that are subordinate to that Manger's domain.

**CI2-SAR-5.1.9.2a** (U//FOUO) When an Enrollment Manager assigns a User Identity to a Management Role, the KMI shall require the Enrollment Manager to place the new Manager in either (1) the Enrollment Manager's own Enrollment Domain or (2) an Enrollment Domain that is subordinate to the Enrollment Manager's domain. [DRV KRD 1618] {R}

(U//FOUO) Figure 29 illustrates the foregoing requirement with these examples:

- At least one "Top-Level Enrollment Manager" had to be initialized as part of system startup, but each additional Top-Level Enrollment Manager could have been enrolled by a Top-Level Enrollment Manager.

- Each of the "Other Managers for the KMI Level" (i.e., managers in EDTL that are not Enrollment Managers) had to be enrolled by a Top-Level Enrollment Manager (because an Enrollment Manager cannot enroll Managers into a domain superior to its own).

- After EDS1 had been created, at least one of the "Enrollment Managers for Service 1" had to be enrolled by a Top-Level Enrollment Manager; but then each of the others could have been

enrolled either by a Top Level Enrollment Manager or by an existing Enrollment Manager for Service 1. Similarly after EDA2 had been created, at least one of the "Enrollment Managers for Agency 2" had to be enrolled by a Top-Level Enrollment Manager; but then each of the others could have been enrolled either by a Top Level Enrollment Manager or by an existing Enrollment Manager for Agency 2.

- After EDS1 had been created, each of the "Other Managers for Uniformed Service 1" could have been enrolled either by an Enrollment Manager for Service 1 or by a Top-Level Enrollment Manager. Similarly, after EDA2 had been created, each of the "Other Managers for DoD Agency 2" could have been enrolled either by an Enrollment Manager for Agency 2 or by a Top-Level Enrollment Manager.

- After EDS11 had been created, at least one "Enrollment Manager for Organization 1.1" had to be enrolled either by a Enrollment Manager for Service 1 or by a Top-Level Enrollment Manager; but then each of the others could have been enrolled by an existing Enrollment Manager for EDS11, by an Enrollment Manager for Service 1, or by a Top-Level Enrollment Manager. Similarly, after EDS12 had been created, its Enrollment Managers could have been enrolled by a Top-Level Enrollment Manager, by an Enrollment Manager for Service 1, or by an existing Enrollment Manager for EDS12.

- After EDS11 had been created, each of the "Other Managers for Service Organization 1.1" could have been enrolled by an Enrollment Manager for Organization 1.1, by an Enrollment Manager for Service 1, or by a Top-Level Enrollment Manager. Similarly, after EDA12 had been created, each of the "Other Managers for Service Organization 1.2" could have been enrolled by an Enrollment Manager for Organization 1.2, by an Enrollment Manager for Service 1, or by a Top-Level Enrollment Manager.

(U//FOUO) The procedures, structures, or operations of a KMI customer organization might result is needing to enroll a user or a user identity in multiple enrollment domains.

**CI2-SAR-5.1.9.2b** (U//FOUO) The KMI shall permit the same User Identity, or User Identities of the same Registered User, to be enrolled in two or more Enrollment Domains, by either the same Enrollment Manager or different Enrollment Managers. [DRV KRD 1618] {R}

**CI2-SAR-5.1.9.2c** (U//FOUO) The KMI shall not permit a User Identity to be assigned twice to the same Management Role in a single Enrollment Domain. [DRV KRD 0952, 1618] {R}

(U//FOUO) Also, an enrollment may need to be undone at some later point in time.

**CI2-SAR-5.1.9.2d** (U//FOUO) The KMI shall enable an Enrollment Manager to withdraw an existing assignment of a User Identity to a Management Role (i.e., "disenroll" a Manager), regardless of which Enrollment Manager originally made the assignment, if (1) the Enrollment Manager has authority to confer that Role, (2) the assignment is contained in either (a) the Enrollment Domain of that Enrollment Manager or (b) an Enrollment Domain that is subordinate to that one, and (3) the User Identity is not one that belongs to the same User that is acting as the Enrollment Manager. [DRV KRD 1203, 1618] {R}

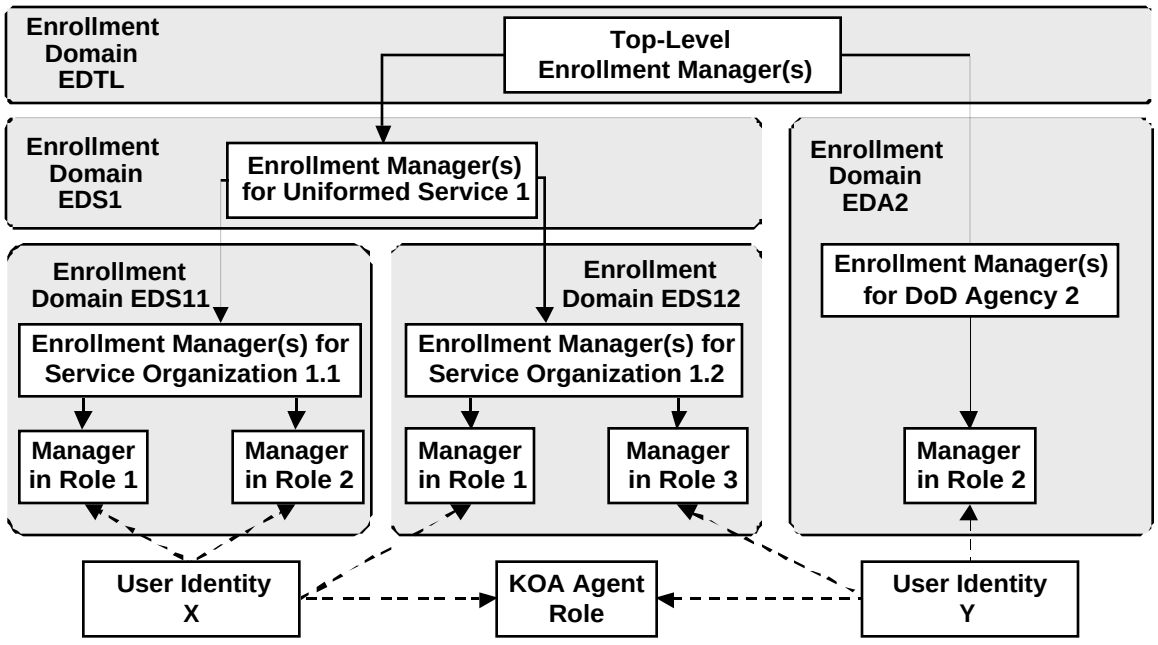
**CI2-SAR-5.1.9.2e** (U//FOUO) The KMI shall enable an Enrollment Manager to request and view information concerning all assignments of User Identities to Management Roles that (1) currently exist in either (a) that Manager's Enrollment Domain or (b) any Enrollment Domain subordinate to that one, (2) for all Roles which that Enrollment Manager has authority to confer, (3) regardless of which Enrollment Manager made the assignment. [DRV KRD 1618] {R-S}

### 5.1.9.3 (U) Implications of Enrollment Domains

(U//FOUO) The requirements stated in this "Enrollment Domains" section bestow strong capabilities on an Enrollment Manager, including (1) the ability to create a subdomain at the manager's own level in the Domain Enrollment Hierarchy or a subordinate level, (2) the ability to enroll managers at its own domain level or a subordinate level, and (3) the ability to remove managers at its own domain level or a subordinate level, regardless of how the management roles were originally conferred. These strong and flexible capabilities are needed by Enrollment Managers to enable the KMI to deal with contingencies. For example, as illustrated by Figure 29, if the failure of a long-haul network prevented the Client Nodes of Enrollment Managers in EDS1 from communicating with a PRSN, then the Top-Level Enrollment Managers, at least some of which are expected to be collocated with core nodes, could perform the duties of the incapacitated managers. However, the KMI and its user organizations will need to institute equally strong procedures to control these capabilities.

(U//FOUO) Figure 30 illustrates additional KMI capabilities that are implied by the requirements pertaining to the enrollment process:

**Figure 30. (U) KMI User Enrollment Examples**




UNCLASSIFIED//FOUO

- A user identity can be assigned to one or more management roles and also to the KOA Agent role. For example, identity X is assigned to management roles 1 and 2, and identity Y is assigned to management roles 2 and 3.

- A user identity can be assigned to two or more management roles in the same enrollment domain. For example, identity X is assigned to both management role 1 and management role 2 in EDS11.

- A user identity can be assigned to management roles in two or more enrollment domains, and the roles can be either the same in each domain or different. For example, identity X is assigned to management role 1 in both EDS11 and EDS12, but identity Y is assigned to management role 3 in EDS12 and management role 2 in EDA2.

- A user identity can be assigned to multiple management roles at either the same level of the Enrollment Domain Hierarchy or at different levels. For example, identity X is enrolled only in subordinate enrollment domains that are two levels below EDTL, but identity Y is assigned to management role 3 in a subordinate domain (EDS12) two levels below EDTL and to management role 2 in a subordinate domain (EDA2) only one level below EDTL.

- Finally, CI-2 uses the Enrollment Domain concept only to control the enrollment of managers and the assignment of their RuBAC attributes. Therefore, a KOA Agent does not belong to any enrollment domain. For example, user identities X and Y are both assigned to the KOA Agent role, but these agents are not treated as belonging to any enrollment domain.

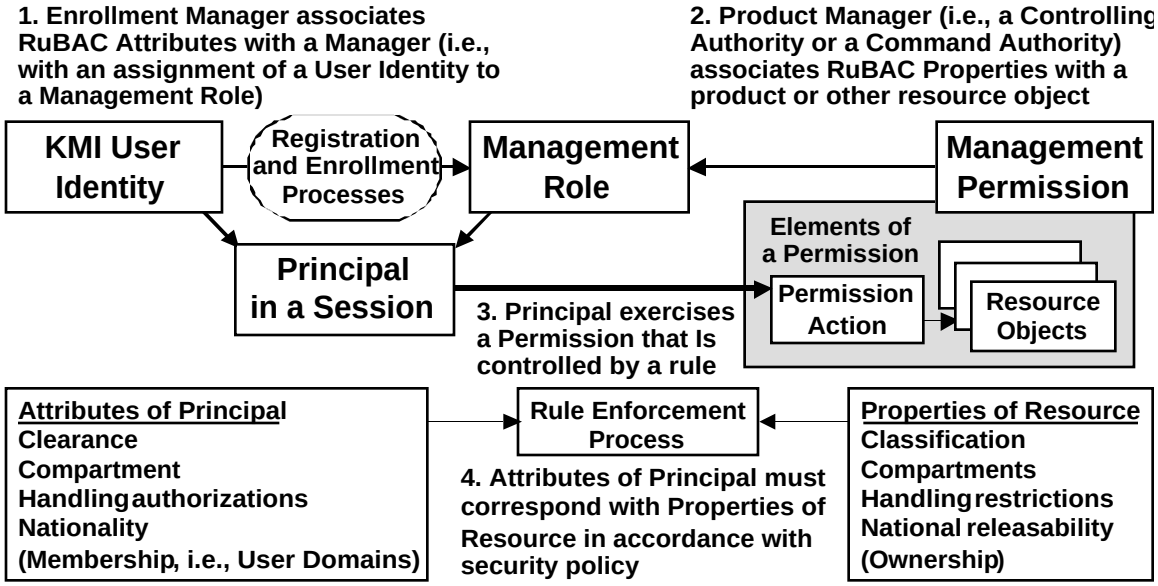
## 5.2 (U) Rule-Based Access Control

(U//FOUO) The role-based access control process specified in the previous section assigns permissions to management roles. Each permission enables a user identity acting in a role to perform a specific type of system action against one or more system resource objects. The rule-based access control (RuBAC) processes that are specified in this section constrain the actions of role-based permissions in the context of a specific session and specific resource objects.

(U//FOUO) As illustrated by Figure 31, managers can associate RuBAC attribute values with role assignments and also associate counterpart RuBAC property values with resource objects. Then, during a session, system actions associated with a permission are constrained by requiring the attributes of the session's principal, which is exercising the permission, to match (i.e., correspond according to pre-specified confidentiality rules) with properties of the affected resource objects. This *Security Architecture* specifies RuBAC properties only for Type 1 products, but RuBAC properties could be specified for other types of system resource objects. For example, RuBAC could be applied to reports generated for managers. Also, RuBAC concepts could be adapted to other types of security services, using other types of properties. However, this *Architecture* does not specify any such additional properties or applications.

(U//FOUO) The terminology here has been chosen carefully. Although the RuBAC characteristics associated with role assignments (RuBAC attributes) are similar in nature to the characteristics associated with resource objects (RuBAC properties), different nouns have been used to prevent ambiguity in requirement statements.

**Figure 31. (U) KMI Rule-Based Access Control**




UNCLASSIFIED//FOUO

**CI2-SAR-5.2a** (U//FOUO) The KMI shall restrict the Access of System Entities to Resource Objects by comparing (1) the RuBAC Properties of an object to (2) the RuBAC Attributes of the accessing entity. [DRV KRD 0612, 0872, 1332, 1613] {R}

**CI2-SAR-5.2b** (U//FOUO) The KMI shall record for Audit any attempt to access a Resource Object by a System Entity that does not have the necessary RuBAC Attribute values. [DRV KRD 0867] {R}

**CI2-SAR-5.2c** (U//FOUO) The KMI shall provide a capability to manage RuBAC Attributes of Managers and the corresponding RuBAC Properties of Resource Objects. [DRV 1610] {R-S}

(U//FOUO) Role-based access control could be adapted to support confidentiality rules by itself; this could be done by binding RuBAC attributes into role definitions. However, that would greatly increase the complexity of role management functions, because it would increase both the number of roles to be managed and the number of times that an identity's role might need to be changed. Therefore, CI-2 manages RuBAC separately, enabling roles to be more easily managed.

### 5.2.1 (U) RuBAC Properties for System Resource Objects

(U//FOUO) As illustrated by Figure 31, RuBAC property values are assigned to KMI products and could be assigned to other system resources, such as library objects. KMI products are used to protect information ranging from unclassified to compartmented Top Secret, and the KMI needs to ensure that the products are released only to properly authorized system entities. CI-2 uses RuBAC to implement data confidentiality requirements (see "Data Confidentiality" section of Volume 2) for products. The properties that KMI needs for products are numerous and varied,

and the KMI must be able to support new ones as needs arise. Therefore, this *Security Architecture* specifies types of properties, but does not specify individual values.

**DEFINITION** (U//FOUO) RuBAC Property. A characteristic of a System Resource object, where the value of the characteristic is used to make Access Control decisions that enforce data confidentiality. [DRV KRD 1614]

(U//FOUO) When a Product Manager establishes a new product (see "Approval-Based Access Control" section), that manager assigns values for the product's RuBAC properties. A product has at least the following RuBAC properties (which, in effect, comprise a security label):

- **Basic classification**. Single-valued; a hierarchical sensitivity level, such as "SECRET".
- **Security categories**. Multi-valued; non-hierarchical sensitivity designations.
- **National releasability**. Multi-valued; country designations.
- **Handling restrictions**. Multi-valued; other handling requirement designations.

### 5.2.2 (U) RuBAC Attributes for System Entities

(U//FOUO) As illustrated by Figure 31, RuBAC attribute values are assigned to managers. The values that the KMI needs for managers are numerous and varied, and the KMI must be able to support new ones as needs arise. Therefore, this *Security Architecture* specifies types of attributes, but does not specify individual values.

**DEFINITION** (U//FOUO) RuBAC Attribute. A characteristic of a System Entity, where the value of the characteristic is used in making Access Control decisions that enforce data confidentiality.

(U//FOUO) When an Enrollment Manager creates a new manager, i.e., assigns a user identity to a management role, the Enrollment Manager also assigns values for the RuBAC attributes of the new manager. The values represent the new manager's authorizations for ordering and distributing products or for performing managerial functions related to the RuBAC and approval-based access control processes. A Manager at least has the following four RuBAC attributes:

- **Basic clearances**. Possibly multi-valued; hierarchical sensitivity levels, comparable to Basic Classification attribute of a product or other resource object.

- **Security categories**. Possibly multi-valued; non-hierarchical sensitivity designations, comparable to the Security Categories attribute of a product or other resource object.

- **Nationality**. Single-valued; a country designation comparable to the National Releasability attribute of a product or other resource object.

- **Handling approvals**. Multi-valued; comparable to Handling Restrictions attribute of a product or other resource object.

(U//FOUO) This *Security Architecture* specifies RuBAC attributes only for (1) certain managers, (2) certain user devices, and (3) accounts that are used to manage devices and products. Potentially, RuBAC attributes could be specified for other types of system entities and

constructs, including KOA Agents and operational components. For example, the KMI could treat "sponsoring organization" as a RuBAC attribute of a User Identity or of the assignment of a User Identity to the KOA Agent role (see "Static User Domain Constraints"). The value of this attribute could be matched against the value of an "ownership" attribute of system resource objects, to implement access control based on organizational affiliation; and this form of RuBAC could be used to limit access to tracking, accounting, and or audit data. However, this *Architecture* does not specify such additional attributes or applications.

(U//FOUO) The enrollment process assigns one or more sets of RuBAC attribute values to certain managers.

**DEFINITION** (U//FOUO) RuBAC Access Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute values, (2) is associated with a Manager, and (3) is used in determining the limits of the Manager's Permissions with regard to accessing Resource Objects.

(U//FOUO) A RuBAC access set contains the following types of values, which must be consistent (i.e., semantically non-contradictory):

- **Basic clearances**. One or more values.
- **Security categories**: Zero or more values.
- **Nationality**. A single value.
- **Handling approvals**. Zero or more values.

**DEFINITION** (U//FOUO) RuBAC Conferral Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute Values; (2) is associated with an Enrollment Manager, Device Registration Manager, or KOA Registration Manager; and (3) is used to constrain the RuBAC Attribute values that the Manager can assign.

(U//FOUO) A RuBAC conferral set functions as follows:

- (1) For an Enrollment Manager, it constrains the attribute values that the Manager can assign to the Access Sets and Conferral Sets of other Managers.
- (2) For a Device Registration Manager, it constrains the attribute values that the Manager can assign to User Devices—ECUs, fill devices, and AKPs.
- (3) For a KOA Registration Manager, it constrains the attribute values that the Manager can assign to KOAs.

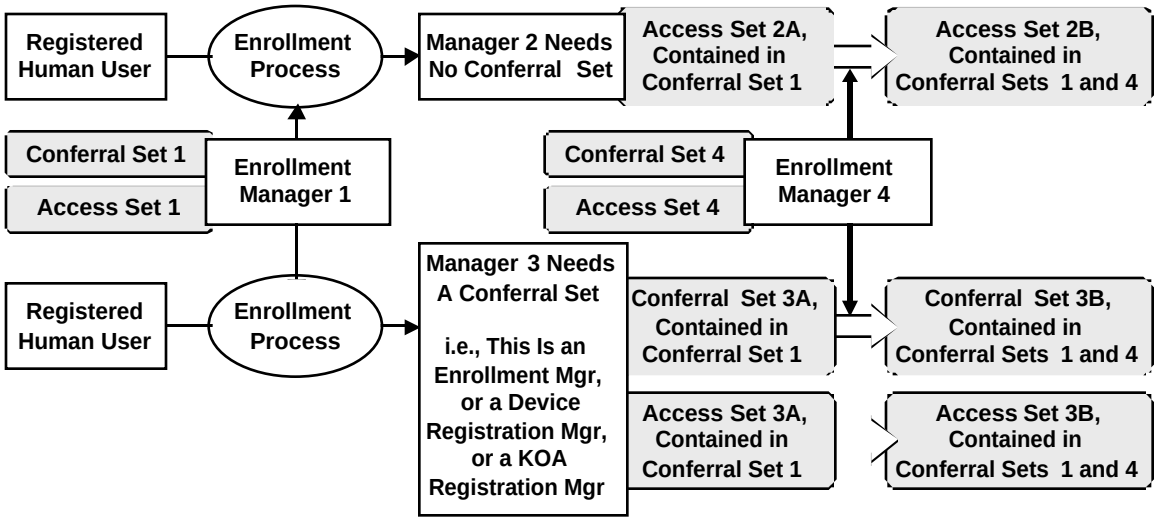
(U//FOUO) A conferral set contains the same attributes as in an access set, but each attribute may have several values, possibly all the values defined in the KMI:

- **Basic clearances**. One or more values.
- **Security categories**. Zero or more values.
- **Nationalities**. One or more values.
- **Handling approvals**. Zero or more values.

(U//FOUO) Figure 32 illustrates that when an Enrollment Manager (Manager 1) confers a role that does not need a RuBAC conferral set, the enrolling manager (Manager 1) assigns the

RuBAC access set (Access Set 2A) of the new manager (Manager 2); and the new access set (Access Set 2A) must be contained in the enrolling manager's conferral set (Conferral Set 1).

**Figure 32. (U) KMI RuBAC Attribute Set Initialization and Change**




**UNCLASSIFIED//FOUO**

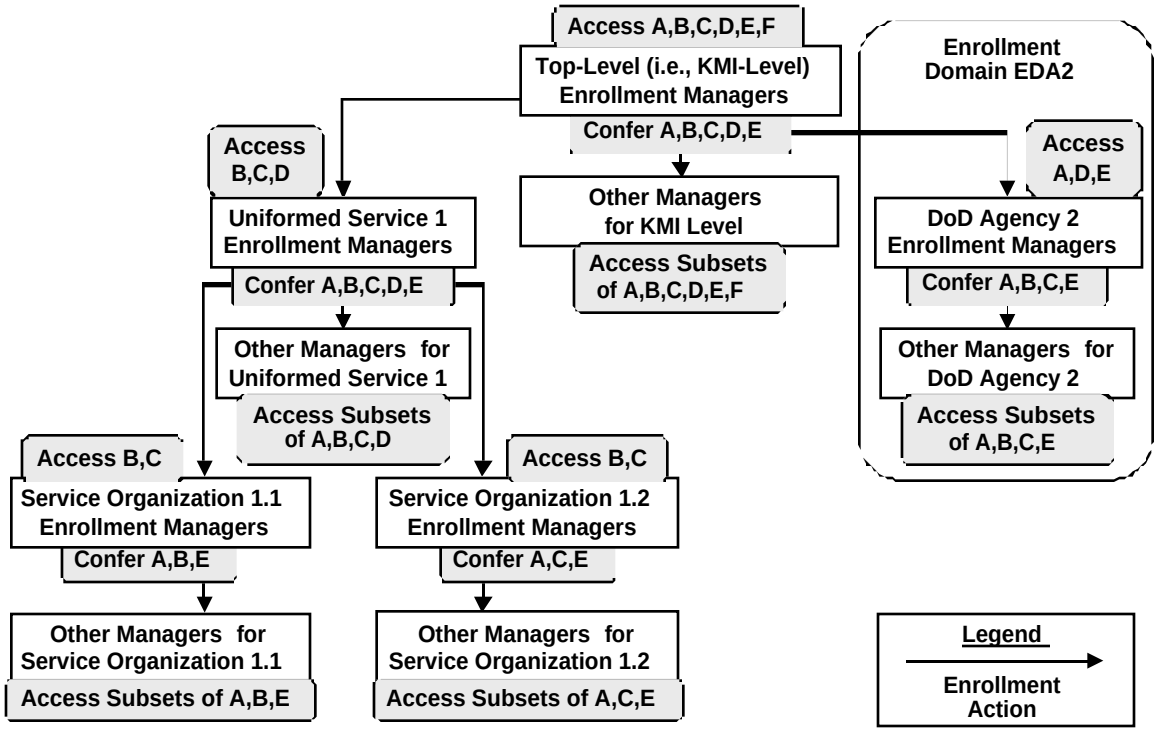
(U//FOUO) Figure 32 also illustrates that when an Enrollment Manager (Manager 1) confers a role that needs a RuBAC conferral set—Enrollment Manager, Device Registration Manager, or KOA Registration Manager—the enrolling manager (Manager 1) assigns to the new manager (Manager 3) both the conferral set (Conferral Set 3A) and also a RuBAC access set (Access Set 3A), and each set must be contained in the enrolling manager's conferral set (Conferral Set 1). However, the new access set (Access Set 3A) and the new conferral set (Conferral Set 3A) do not need to be either identical to, or contained in, each other.

(U//FOUO) Figure 32 further illustrates that sometime after a manager (either Manager 2 or Manager 3) has been enrolled, either the original enrolling manager (Manager 1) or another Enrollment Manager (Manager 4) may change the new manager's access set or conferral set by adding or deleting values. The Enrollment Manager that makes the change can add or delete only values that are in its own conferral set.

(U//FOUO) An Enrollment Manager's access set need not be contained in that manager's conferral set. For example, Figure 33 illustrates that the total set of RuBAC attribute values that is supported by the system is {A, B, C, D, E, F}. Each Top-Level Enrollment Manager is authorized to access F but not confer F. This might be designed to ensure that only Top-Level Managers can ever access data labeled F.

(U//FOUO) Conversely, a manager's conferral set need not be contained in that manager's access set. In Figure 33, the Enrollment Managers for Uniformed Service 1 can confer A, B, C, D, and E; but can access only B, C, and D. For example, an Enrollment Manager that is a citizen of Country A probably would not have the access value for Country B citizenship, but might be authorized to confer that access value when supporting a multinational organization.

**Figure 33. (U) KMI RuBAC Attribute Set Examples**




UNCLASSIFIED//FOUO

**CI2-SAR-5.2.2a** (U//FOUO) The KMI shall grant to any Top-Level Enrollment Manager that is initialized at system startup, a RuBAC Conferral Set that is an appropriate subset of all the RuBAC Attribute values that have been defined for data confidentiality for Type 1 products, which includes at least the following four attribute types: [DRV KRD 1611] {R}

- (1) Hierarchical data sensitivity designations.
- (2) Non-hierarchical data category designations.
- (3) Nationality designations.
- (4) Other data handling authorization designations.

**CI2-SAR-5.2.2b** (U//FOUO) The KMI shall give to any Top-Level Enrollment Manager that is initialized at system startup a RuBAC Access Set that is an appropriate subset of all the RuBAC Attribute values that have been defined for data confidentiality for Type 1 products. [DRV KRD 1615, 2008] {R}

**CI2-SAR-5.2.2c** (U//FOUO) The KMI shall enable an Enrollment Manager, when assigning a User Identity to any Management Role, to give the new Manager a RuBAC Access Set containing only a consistent (i.e., non-contradictory) set of the RuBAC Attribute values that are contained in the enrolling Manager's own Conferral Set. [DRV KRD 1615, 2008] {R}

**CI2-SAR-5.2.2d** (U//FOUO) The KMI shall enable an Enrollment Manager, when assigning a User Identity to the Role of (1) Enrollment Manager, (2) Device Registration Manager, or (3) KOA Registration Manager, to give the new Manager a RuBAC Conferral Set containing

only a consistent (i.e., non-contradictory) set of the RuBAC Attributes that are contained in the enrolling Manager's own Conferral Set. [DRV KRD 1615, 2008] {R}

(U//FOUO) The foregoing requirement means that the enrolling manager establishes the initial authority of the new manager to confer RuBAC attributes. However, this authority can be changed later, as stated in the following requirement.

**CI2-SAR-5.2.2e** (U//FOUO) The KMI shall enable an Enrollment Manager to either view, add, or delete an attribute value in either the RuBAC Access Set or RuBAC Conferral Set of another existing Manager if and only if all of the following conditions hold: [DRV KRD 1560, 1611, 2146] {R}

- (1) The value is contained in the Conferral Set of the Enrollment Manager that is making the change.
- (2) The Manager being changed is contained in either (a) the Enrollment Domain of the Enrollment Manager that is making the change or (b) an Enrollment Domains that is subordinate to the Enrollment Manager's own domain.
- (3) The User Identity of the Manager being changed does not belong to the same User as does the User Identity of the Enrollment Manager that is making the change.

(U//FOUO) For example, any one of the Top-Level Managers illustrated by Figure 33 could add or delete values A, B, C, D, or E in either the RuBAC Access Set or the RuBAC Conferral Set of any manager in the domain EDTL, i.e., of (1) any other Top-Level Enrollment Manager or Other Manager for the KMI Level, or (2) any Enrollment Manager or Other Manager for Uniformed Service 1, DoD Agency 2, Service Organization 1.1, or Service Organization 2.2. In other words, any Top-Level Manager could change any RuBAC attribute set for any manager shown in the figure.

(U//FOUO) However, any one of the DoD Agency 2 Enrollment Managers could add or delete values A, B, C, or E in either the Access Set or the Conferral Set of only managers in the domain EDA2. A DoD Agency 2 Enrollment Manager could not change any RuBAC attribute value of any manager outside of EDA2.

(U//FOUO) After CI-2 is deployed, the KMI is expected to have several thousand external managers that are distributed throughout the world and that operate within many user organizations that take different approaches to selecting those managers. Regardless of these differences, all Enrollment Managers need to be knowledgeable of their local command structure and its operational procedures, so that they can select the other managers appropriately and verify that those persons have authorization to be granted the RuBAC attribute values that are needed to operate in their various roles. Enrollment Managers need to have strong lines of communication with personnel security offices to ensure that RuBAC attributes assigned to managers are based on proper authority, are accurate, and are kept up-to-date, including being revoked if needed.

## 5.3 (U) Approval-Based Access Control

(U//FOUO) In addition to role-based and rule-based access controls, CI-2 implements a third form of access control called "approval-based". The role-based form provides functionality

controls based on roles and permissions, and the rule-based form provides confidentiality controls based on classification, handling restrictions, and nationality. However, role-based and ruled-based controls do not provide sufficient granularity for managing the distribution of products to cryptographic devices.

**DEFINITION** (U//FOUO) KMI Operating Account (KOA). A KMI business relationship that is established to manage (1) the set of User Devices that are under the control of a KMI customer organization and (2) the distribution of KMI products to those devices.

(U//FOUO) For distributing products to KOAs and to devices held by KOAs, the KMI needs controls based on need-to-know that is approved by managers. For example, not every KOA that operates at the Secret level should be able to receive every Secret product.

**CI2-SAR-5.3a** (U//FOUO) The KMI shall implement an approval-based Access Control process that enables the Authorizations conferred by role-based and rule-based Access Control processes to be restricted on a need-to-know basis for KOAs and selected Managers. [DRV KRD 0425, 1034] {A-R}

**CI2-SAR-5.3b** The KMI shall record as a Mandatory Audit Event each approval by a Manager for Access to a KMI product, service, or other System Resource. [DRV KRD 1564] {A-R}

(U//FOUO) Approval-based access control involves the four management roles that deal directly with product ordering and distribution: Controlling Authority, 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.

(U//FOUO) The operational flow and access control considerations for key ordering depend on the type of product being ordered. At the highest level, there are two groups of products to consider:

- **Symmetric key and netted FIREFLY key**. The ordering and management of these product types are based on short titles corresponding to cryptonets, and typically involve distribution of key to multiple destination KOAs and/or COMSEC accounts. (In this section, the requirements and descriptions that address “symmetric key” should be understood as applying to both symmetric key and netted FIREFLY key, unless otherwise stated.)

- **Basic and Enhanced FIREFLY key (other than netted FIREFLY key)**. The ordering and management of FIREFLY key is based on key attributes, particularly partition codes and Department / Agency / Organization (DAO) codes. Each FIREFLY key is ordered for and delivered to a single destination KOA or COMSEC account.

(U//FOUO) Table 10 summarizes the ordering and management distinctions among symmetric key, FIREFLY key, and netted FIREFLY key.

**Table 10. (U) KMI Management Differences for Major Key Product Types**

| Product Type | Managed By | Specified By | Ordered By | Recipients |
|---|---|---|---|---|
| **Symmetric Key** | Controlling Authority | Short Title | Controlling Authority or Product Requester | Multiple |
| **FIREFLY Key** | Command Authority | Partition Code, DAO Code | Product Requester | Single |
| **Netted FIREFLY Key** | Controlling Authority | Short Title | Controlling Authority or Product Requester | Single (but coordinated with other recipients in the same net) |

**UNCLASSIFIED//FOUO**

(U//FOUO) The first subsection that follows, "Approval-Based Access Control for Symmetric Key Products", begins with an overview and then provides details and states basic requirements. The second subsection, "Approval-Based Access Control for Symmetric Key Products", parallels the first but is shorter because much of the material that applies to symmetric key products also applies to asymmetric key products. However, these two types of products are under the management control of two different Product Manager roles.

(U//FOUO) Controlling Authority is the Product Manager role for symmetric products. Traditionally, the Controlling Authority role has had the following definition, and the first subsection interprets that definition in terms of KMI responsibilities:

> **DEFINITION** (U//FOUO) Controlling Authority. Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet. [CNSSI4009].

(U//FOUO) Command Authority is the Product Manager role for asymmetric products. Traditionally, the Command Authority role has had the following definition, and the second subsection interprets that definition in terms of KMI responsibilities:

> **DEFINITION** (U//FOUO) Command Authority. Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges. [CNSSI4009]

(U//FOUO) A third subsection, "KMI Operating Accounts", provides more detail concerning processes that apply to both symmetric and asymmetric products. Additional specifications and descriptions for approval-based access control are provided in Volume 1 and in the *Concept of Operations* [KMI2212].

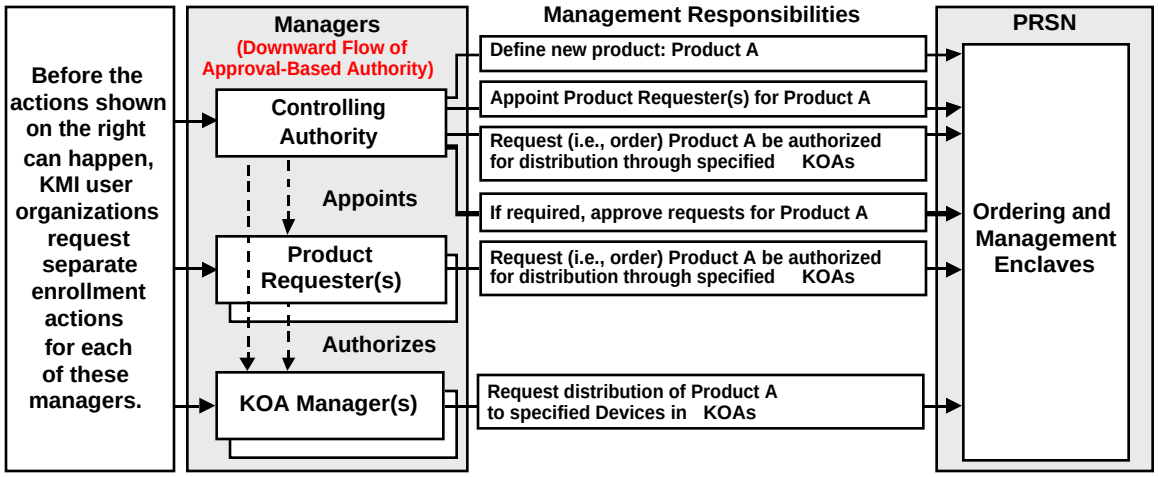
(U//FOUO) Approval-based access control for symmetric (and netted FIREFLY) products involves three management roles that deal directly with product ordering and distribution: KOA Manager, Product Requester, and the Product Manager role of Controlling Authority. For asymmetric products the roles are KOA Manager, Product Requester, and the Product Manager role of Command Authority.

(U//FOUO) As specified in the "Verification of Authenticity and Eligibility for Managers" section, the KMI does not assign a user identity to a management role unless the identity belongs to either a U.S., NATO, or CCEB Security Domain. Consequently, non-NATO, non-CCEB Coalition Partners cannot perform the roles of Controlling Authority, Command Authority, Product Requester, and KOA Manager and, therefore, are prevented from ordering either symmetric or asymmetric products. Products are ordered for Coalition Partners only by U.S. managers.

### 5.3.1 (U) Approval-Based Access Control for Symmetric Key Products

(U//FOUO) For each specific symmetric key product, relationships are established among the Controlling Authority, Product Requesters, and KOA Managers, as illustrated by Figure 34. A Controlling Authority defines a product. The Controlling Authority and, possibly, Product Requesters determine which KOAs are authorized to distribute the product to devices, based on the relationship of those accounts to communications networks in the context of an operational mission. In each of those KOAs, a KOA Manager determines which of that KOA's devices are to receive the product.

**Figure 34. (U) KMI Management Roles in Distribution of Symmetric Products**




**UNCLASSIFIED//FOUO**

#### 5.3.1.1 (U) Overview of Distribution of Symmetric Key Products

(U//FOUO) The approval-based distribution process shown in Figure 34 has the following steps:

- (U//FOUO) Controlling Authority defines new product. A Controlling Authority can define a new product, e.g., "Product A" in Figure 34. 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.

- (U//FOUO) 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).

- (U//FOUO) KOA Manager directs product to devices. A KOA Manager of a KOA for which Product A has been ordered, can request that Product A be distributed to specific devices that are managed by that account.

(U//FOUO) The management of symmetric products involves all three types of access control:

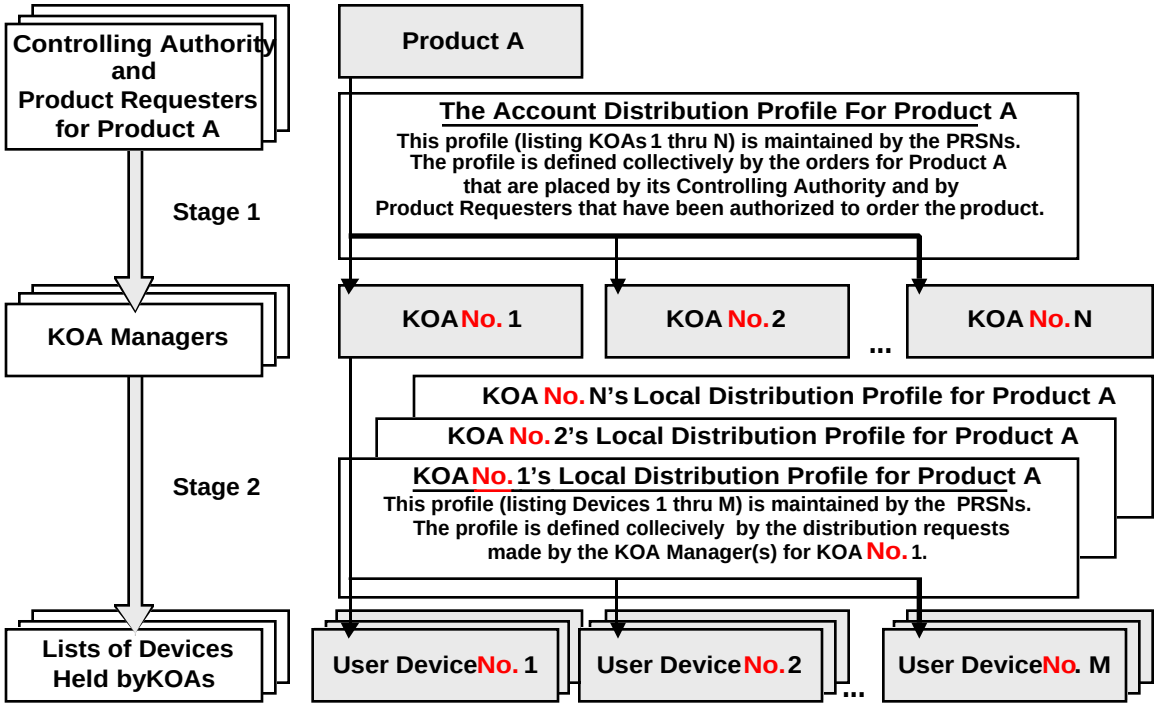
- Role-based processes determine which users are Controlling Authorities, Product Requesters, and KOA Managers.
- Approval-based processes restrict ordering to authorized Controlling Authorities and Product Requesters, and restrict distribution to KOAs and devices that have a legitimate need.
- Rule-based processes ensure that only appropriately authorized KOAs may distribute products to devices, and that only authorized devices may receive products.

(U//FOUO) As illustrated by Figure 30, a human user could be assigned to one of the three product management roles in some enrollment domain, and then be assigned to the same role in another enrollment domain. Each assignment would receive a separate set of RuBAC authorizations, and would be constrained to what is allowed in its own enrollment domain; and the user would be able to act in only one of these management roles at a time. Thus, the user would not be able to use the authorizations granted in one domain to manage products in the other domain. Although this kind of dual assignment might be made only rarely, this could be useful in special situations, such as joint operations. For example, a member of the Army who is enrolled as a Product Requester in an Army domain, might also temporarily need to order products for Air Force devices for which the Army domain does not have access. In that case, an Enrollment Manager in an Air Force domain could also enroll the user as a Product Requester. When the need for the Air Force access has expired, the Air Force could revoke the enrollment in their own domain without affecting the user's ability to order products for the Army.

(U//FOUO) Figure 35 illustrates that the distribution process for a symmetric product ("Product A") has two stages:

- (U//FOUO) **Stage 1: Distribution Directed by Product Requesters**. The Controlling Authority or a Product Requester requests that Product A be distributed to selected KOAs. Collectively, all such requests create an access control list for Product A, and the list is maintained by PRSNs.

**Figure 35. (U) KMI Two-Stage Distribution of Symmetric Key Products**




**UNCLASSIFIED//FOUO**

**DEFINITION** (U//FOUO) Account Distribution Profile. An approval-based Access Control list for a specific product that (1) names the KOAs to which PRSNs distribute the product and (2) states conditions of distribution (e.g., requires per-edition approval).

- (U//FOUO) **Stage 2: Distribution Directed by KOA Managers**. A KOA Manager of a KOA for which Product A has been ordered, can request that Product A be distributed to specific, selected devices owned by that account. The KOA Manager's requests for Product A are entered on an access control list that is maintained by PRSNs.

**DEFINITION** (U//FOUO) Device Distribution Profile. An approval-based Access Control list for a specific product that (1) names the User Devices in a specific KOA to which PRSNs distribute the product and (2) states conditions of distribution for each device.

(U//FOUO) In summary, for each product there is a separate device distribution profile in each KOA for which the product has been approved by a Product Requester. Conversely, for each KOA, there is a separate device distribution profile for each product for which the KOA has been approved.

(U//FOUO) The following sections provide a further, more detailed description of the approval-based access control process for symmetric products and specify its basic system requirements. Additional descriptions and specifications for the operation of the process are provided in the *Concept of Operations* [CONOP] and Volume 1.

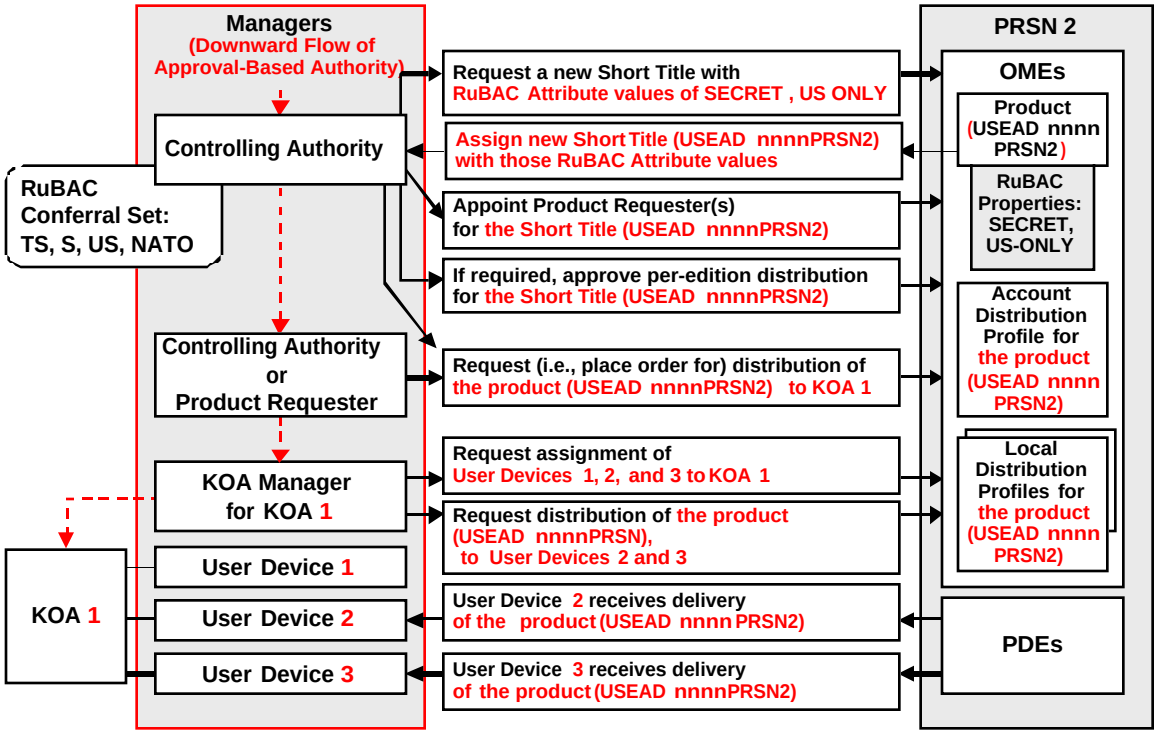
### 5.3.1.2 (U) Controlling Authority for Symmetric Key Products

(U//FOUO) In the KMI, the role of Controlling Authority is assigned responsibility for (1) determining the need for a new instance of an available product type (e.g., a new cryptonet); (2) specifying RuBAC attribute values for the new product; (3) requesting a short title for the new product; (4) either ordering the product for KOAs and COMSEC accounts that should receive it, or authorizing Product Requestors to do the ordering, or both; and (5) approving per-edition distribution of the product to devices, if the Controlling Authority deems such approval is needed.

**DEFINITION** (U//FOUO) Short Title. An identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling. [CNSSI4009].

(U//FOUO) Figure 36 provides a simplified example, involving one symmetric product short title ("USEAD nnnn PRSN2") and three ECUs, to illustrate that establishing a new product involves the following steps:

**Figure 36. (U) KMI Approval-Based Steps for Symmetric Key Product**




UNCLASSIFIED//FOUO

- (U//FOUO) **Establish a short title**. A Controlling Authority working at a Management Client Node connects to an OME of a PRSN and requests that a new short title be assigned for some basic product type that that KMI is capable of generating. The PRSN assigns a short title for the product (e.g., "USEAD nnnn PRSN2") and designates the product to be under the control of the requesting Controlling Authority.

- (U//FOUO) **Assign the RuBAC property values**. The Controlling Authority specifies RuBAC values for the product (e.g., "SECRET" and "US-ONLY"). The PRSN checks that the specified values are contained in the manager's RuBAC conferral set and, if so, associates the values with USEAD nnnn PRSN2.

(U//FOUO) Each product is a resource object that has RuBAC properties. The following requirements enable a Controlling Authority to establish products:

**CI2-SAR-5.3.1.2a** (U//FOUO) The KMI shall enable a Controlling Authority to establish a new product that is based on an existing product type. [KRD NEW] {C-R-S}

**CI2-SAR-5.3.1.2b** (U//FOUO) The KMI shall assign management control of a newly requested product to the Controlling Authority that makes the request. [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.1.2c** (U//FOUO) The KMI shall enable a Controlling Authority to assign to a new product a set of RuBAC Property values that are the counterparts to a consistent subset of the RuBAC Attributes that are contained in that Controlling Authority's Access Set. [DRV KRD 1332, 1614] {C-R}

**CI2-SAR-5.3.1.2g** (U//FOUO) The KMI shall enable a Controlling Authority to attach one and only one of the following conditions to a new product: [DRV KRD 1484] {C-R}
- (1) For all orders that are placed for the product by Product Requesters, explicit approval by the Controlling Authority is required each time before an edition of the product is distributed.
- (2) Per-edition approval is not required for all orders, but the Controlling Authority may require approval for the orders received from selected Product Requesters.

**CI2-SAR-5.3.1.2d** (U//FOUO) The KMI shall maintain an Account Distribution Profile for each symmetric product that is established by a Controlling Authority, and the profile shall contain the following data items: [DRV KRD 0910, 0911] {R}
- (1) The product's RuBAC Property values.
- (2) A list of any KOAs for which distribution orders are active, with necessary information about each order, including (a) the User Identity of the Manager (either the Controlling Authority or a Product Requester) who placed the order; (b) distribution requirements, such as routing, required quantities, and need dates; and (c) whether per-edition approval is required.
- (3) A list of any non-KOA Key Management Entities (KMEs) (i.e., COMSEC accounts) for which distribution orders are active, with necessary information about each order
- [Additional data items are defined in Volume 1, and still more items are expected to be defined when a detailed design is done.]

**CI2-SAR-5.3.1.2e** (U//FOUO) The KMI shall enable a Controlling Authority to cause the KMI temporarily to cease distributing a product under the Authority's control, and to restart a distribution that has been temporarily stopped. [DRV KRD 1016] {C-R}

**CI2-SAR-5.3.1.2f** (U//FOUO) The KMI shall enable a Controlling Authority to manage the Account Distribution Profile for a product under the Authority's control. [DRV KRD 0910, 0911] {R}

### 5.3.1.3 (U) Product Requester for Symmetric Key Products

(U//FOUO) After a short title has been established, the product's Controlling Authority can request that the product be made available to specific KOAs (i.e., can place orders for the product). Optionally, a Controlling Authority can delegate that responsibility, by authorizing one or more Product Requesters to order the product, as illustrated by the next step in Figure 36:

- (U//FOUO) **Appoint the Product Requesters**. The Controlling Authority selects one or more user identities that have previously been enrolled as Product Requesters, and authorizes those Managers to request USEAD *nnnn* PRSN2 for KOAs.

**CI2-SAR-5.3.1.3a** (U//FOUO) The KMI shall permit only the Roles of Controlling Authority and Product Requester to be assigned Permissions that enable a Manager to order symmetric products. [DRV KRD 0910, 0949] {R}

**CI2-SAR-5.3.1.3b** (U//FOUO) The Role of Controlling Authority shall, in addition to the Permissions that are assigned to that Role, have the Permissions that are assigned to the Role of Product Requester. [DRV KRD 0910, 1721] {S}

**CI2-SAR-5.3.1.3c** (U//FOUO) The KMI shall enable a Controlling Authority to order any of the products, and only those products, that are under the control of that Authority. [DRV KRD 0425, 0910, 0946, 1034, 1720, 1721] {C-R}

**CI2-SAR-5.3.1.3d** (U//FOUO) If a Registered User acting in the Role of Controlling Authority orders a product for which that Authority has required per-edition approval, then approval shall be automatic and implicit; that is, a Controlling Authority shall not be required to explicitly approve per-edition distributions for the Authority's own orders. [KRD 0910] {C-R}

(U//FOUO) Note that the foregoing requirement purposely does not implement KRD 1621, which says, "The KMI shall not allow a [Manager] to approve any request that [the Manager originates]." To do so would conflict with the intent of KRD 0910, which says, "The KMI shall provide a means for a Controlling Authority … to authorize the distribution of a key from any appropriate KMI component to a user who previously was not authorized to receive the key." (Of course, a user could be separately assigned to both the role of Controlling Authority and the role of Product Requester; and that user, while acting as the Controlling Authority, could grant an ordering authorization to itself as Product Requester for a product that requires per-edition approval. In that case, it is clear that if the user places an order for the product while acting as the Product Requester, then the user would need to act as the Controlling Authority to grant explicit per-edition distribution approvals for that order. However, it is not apparent that any KMI customer organization would want to institute such a product management arrangement.)

**CI2-SAR-5.3.1.3e** (U//FOUO) The KMI shall enable a Controlling Authority, and only a Controlling Authority, to authorize one or more Product Requesters (i.e., User Identities that are currently assigned to the Role of Product Requester) to order one or more of the products that are under the control of that Controlling Authority. [DRV KRD 0949, 1720, 1721, 1722] {C-R}

**CI2-SAR-5.3.1.3f** (U//FOUO) The KMI shall enable a Controlling Authority to withdraw or modify any ordering authorization previously granted to a Product Requester for a product under the control of that Controlling Authority. [DRV KRD 1722] {C-R}

**CI2-SAR-5.3.1.3g** (U//FOUO) The KMI shall enable a Product Requester to order any of the products, but only those products, for which ordering authorization has been granted to the Requester by a Controlling Authority. [DRV KRD 0425, 0946, 0949, 1034, 1720, 1722] {C-R}

**CI2-SAR-5.3.1.3h** (U//FOUO) The KMI shall enable a Controlling Authority or Product Requester to order a product for distribution through a KOA (i.e., list the KOA Identifier on the Account Distribution Profile of the product; i.e., authorize the KOA to distribute the product to User Devices). [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.1.3i** (U//FOUO) The KMI shall enable a Controlling Authority or Product Requester to order a product for distribution through a non-KOA KME; that is, the Manager can list a COMSEC Account's EKMS identifier on the Account Distribution Profile of the product. [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.1.3j** (U//FOUO) The KMI shall permit a Controlling Authority or Product Requester to order a product for a KOA only if the RuBAC Property values of the product are contained in the RuBAC Access Set of the KOA. [DRV KRD 0946, 1332] {R}

**CI2-SAR-5.3.1.3k** (U//FOUO) The KMI shall enable a Controlling Authority or Product Requester to request that a product be distributed through a KOA regardless of whether the requester and the KOA belong to the same Enrollment Domain or not. [DRV KRD 0949] {R}

(U//FOUO) Controlling Authorities can authorize a Product Requester for a product either for a limited period of time or indefinitely, but may withdraw the authorization at any time. Once an order is placed, each edition of the product is distributed as ordered, until the approval expires or is withdrawn. However, a Controlling Authority may also require per-edition approval before distribution, i.e., require a separate, pre-distribution authorization action for each individual edition of the product, either for all orders for that product or for orders for that product that are received from selected Product Requesters.

**CI2-SAR-5.3.1.3l** (U//FOUO) The KMI shall require a Controlling Authority to attach one and only one of the following conditions to an ordering Authorization granted to a specific Product Requester for a specific product: [DRV KRD 1484] {R}

– (1) The Authorization is for an indefinite period of time (unless the Controlling Authority withdraws or modifies the Authorization), specified as a "not before" time.

– (2) The Authorization is for a limited period of time (unless the Controlling Authority withdraws or modifies the Authorization before the end of the period), specified as "not before" and "not after" times.

**CI2-SAR-5.3.1.3m** (U//FOUO) The KMI shall require a Controlling Authority to attach one and only one of the following conditions to an ordering Authorization granted to a specific Product Requester for a specific product: [DRV KRD 1484] {C-R}

– (1) For an order that is placed for the product by that Requester, explicit approval by the Controlling Authority is required each time before an edition is distributed.
– (2) Per-edition approval is not required for orders for that product from that Requester, unless the Controlling Authority has required per-edition approval for every order of the product regardless of which Requester places the order.

**CI2-SAR-5.3.1.3n** (U//FOUO) The KMI shall notify a Controlling Authority when a distribution of an edition of a product requires approval by the Authority. [DRV KRD 1483, 1776] {R}

**CI2-SAR-5.3.1.3o** (U//FOUO) The KMI shall enable a Controlling Authority to approve or disapprove a distribution of an edition of a product, but only for a product that the Authority controls. [DRV KRD 1483, 1563, 1776] {R}

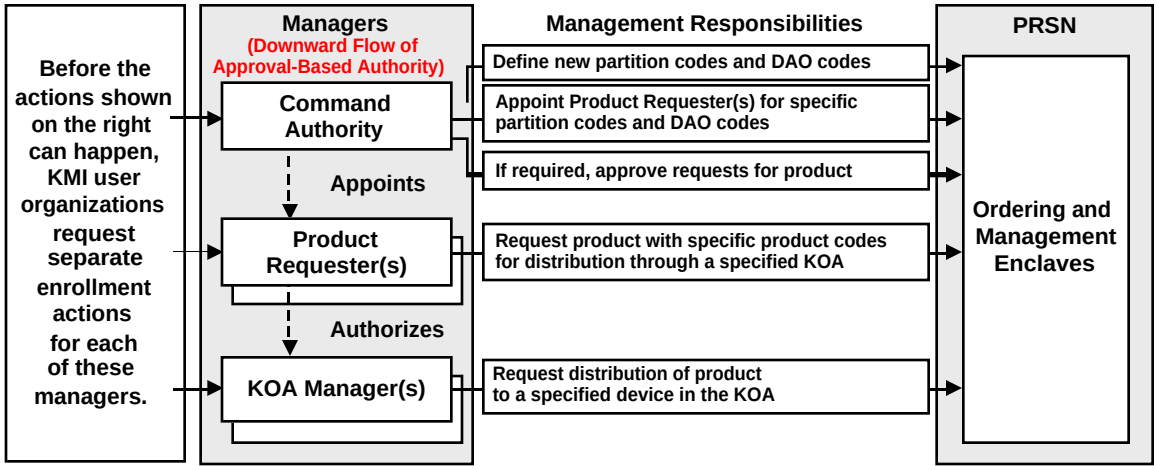
**CI2-SAR-5.3.1.3p** (U//FOUO) The KMI shall not perform the distribution of an edition of a product that requires per-edition approval until the KMI has received an authenticated approval from the product's Controlling Authority. [DRV KRD 1484, 1561, 1563, 1564, 1777] {R}

**CI2-SAR-5.3.1.3q** (U//FOUO) The KMI shall record for Audit any approval given by a Controlling Authority for the per-edition distribution of a product. [DRV KRD 1564] {R}

### 5.3.2 (U) Approval-Based Access Control for Asymmetric Key Products

(U//FOUO) For each specific KMI asymmetric product, relationships are established among the managers, as illustrated by Figure 37. A Command Authority requests the assignment of partition codes and Department/Agency/Organization (DAO) codes for asymmetric products that the Command Authority's organization requires. The Command Authority identifies which partition codes and DAO codes may be ordered by each Product Requester. Product Requesters, in response to key material needs identified by the organization(s) they support, order asymmetric key products and identify the KOA or COMSEC account that should receive each product. A KOA Manager at the receiving KOA determines which device should receive the product.

**Figure 37. (U) KMI Management Roles in Distribution of Asymmetric Products**




UNCLASSIFIED//FOUO

### 5.3.2.1 (U) Overview of Distribution of Asymmetric Key Products

(U//FOUO) The approval-based distribution process shown in Figure 37 has the following steps:

- (U//FOUO) Command Authority defines new product codes. A Command Authority can define new partition codes and DAO codes:

  **DEFINITION** (U//FOUO) Partition Code. A mechanism used to divide an asymmetric (e.g., FIREFLY) universal into smaller nets, such that only devices in a specific partition can interoperate, even though they would otherwise be cryptographically compatible.

  **DEFINITION** (U//FOUO) Department/Agency/Organization (DAO) Code. An encoded, unique identifier assigned to an Department, Agency, or Organization description and used in generation of FIREFLY key credentials.

- (U//FOUO) Command Authority appoints Product Requester(s). The Command Authority selects one or more user identities that have been enrolled as Product Requesters and authorizes them to place orders containing specific partition codes and DAO codes. The Command Authority can require that orders placed by a Product Requester receive per-order approval before the product is generated and distributed. If such approval is required, the Command Authority acts as the approver.

- (U//FOUO) Product Requester orders product for operating account. A Product Requester can order an asymmetric product containing partition codes and DAO codes for which that Product Requester is authorized, and identify the KOA or COMSEC account that should receive the product.

- (U//FOUO) KOA Manager directs product to device. A KOA Manager of the KOA for which an asymmetric product has been ordered can request that the product be distributed to a specific device managed by that account.

(U//FOUO) The management of asymmetric products involves all three types of access control:

- Role-based processes determine which users are Command Authorities, Product Requesters, and KOA Managers.
- Approval-based processes restrict ordering of DAO and partition codes to designated Product Requesters, and restrict distribution to KOAs and devices that have a legitimate need.
- Rule-based processes ensure that only appropriately authorized KOAs may distribute the product to devices, and that only authorized devices may receive the product.

(U//FOUO) The two-stage distribution process for symmetric products, which is shown in Figure 35, also applies to asymmetric products, with the following exceptions:

- An asymmetric product is ordered only by Product Requesters (not the Command Authority role).
- Each asymmetric key is delivered to a single destination device; thus, the account distribution profile for an asymmetric product will list only a single KOA or COMSEC account.
- For the same reason, the product's device distribution profile in that account will list only one destination device.

(U//FOUO) The following sections provide a further, more detailed description of the approval-based access control process for asymmetric products and specify its basic system requirements. Additional descriptions and specifications for the operation of the process are provided in the *Concept of Operations* [CONOP] and Volume 1.

#### 5.3.2.2 (U) Command Authority for Asymmetric Key Products

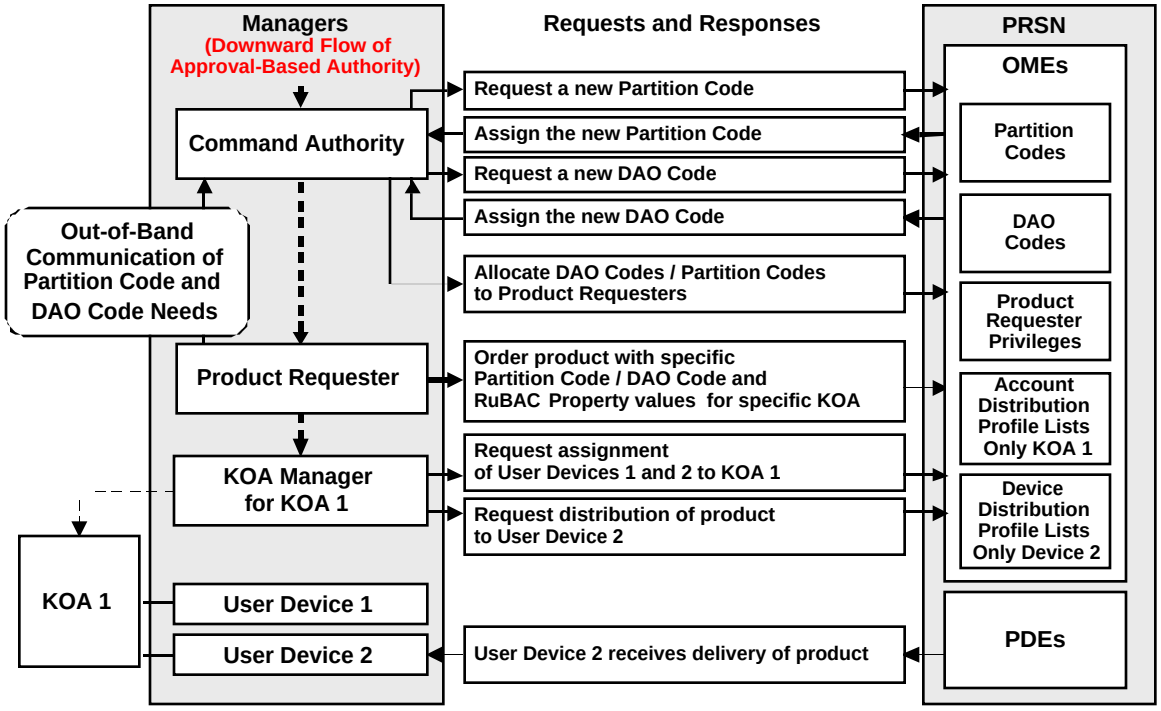
(U//FOUO) In the KMI, the role of Command Authority role is assigned responsibility for (1) determining the need for partition codes and DAO codes based on organizational requirements; (2) requesting the assignment of partition codes and DAO codes; (3) specifying the partition code and DAO code ordering privileges of Product Requesters; and (4) approving asymmetric key orders by Product Requesters, if such approval is needed.

(U//FOUO) Figure 38 provides a simplified example illustrating the establishment of partition codes and DAO codes, and their use by a Product Requester.

- (U//FOUO) **Request Partition Codes and DAO Codes**. A Command Authority receives notice (typically by out-of-band means) from a Product Requester that a new DAO code or partition code is needed. Working at a Management Client Node, the Command Authority connects to an OME of a PRSN and requests that a new code be assigned. The PRSN assigns a DAO code or partition code for the product and designates the code to be under the control of the requesting Command Authority.

(U//FOUO) The following requirements enable a Command Authority to establish partition codes and DAO codes for asymmetric products:

**Figure 38. (U) KMI Approval-Based Steps for Asymmetric Key Products**




UNCLASSIFIED//FOUO

**CI2-SAR-5.3.2.2a** (U//FOUO) The KMI shall enable a Command Authority to establish a new Partition Code for an available asymmetric product type. [KRD NEW] {C-R-S}

**CI2-SAR-5.3.2.2b** (U//FOUO) The KMI shall assign management control of a newly established Partition Code to the Command Authority that requested it. [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.2.2c** (U//FOUO) The KMI shall enable a Command Authority to establish a new DAO Code for an available asymmetric product type. [KRD NEW] {C-R-S}

**CI2-SAR-5.3.2.2d** (U//FOUO) The KMI shall assign management control of a newly established DAO Code to the Command Authority that requested it. [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.2.2e** (U//FOUO) The KMI shall enable a Command Authority to attach one and only one of the following conditions to product requests containing Partition Codes and DAO Codes over which the Command Authority has management control: [DRV KRD 1484] {C-R}

- (1) For all orders that are placed by Product Requesters for products containing specific Partition Codes and/or DAO Codes, explicit approval by the Command Authority is required for each order.
- (2) The Command Authority may require approval for the orders received from selected Product Requesters.

### 5.3.2.3 (U) Product Requester for Asymmetric Key Products

(U//FOUO) After appropriate partition codes and DAO codes have been established, the Command Authority responsible for those codes can authorize one or more Product Requesters to order products containing those codes, as illustrated by the next step in Figure 38:

- (U//FOUO) **Allocate Codes to Product Requesters**. The Command Authority selects one or more user identities that have previously been enrolled as Product Requesters, and authorizes those managers to request asymmetric products containing specific partition codes and DAO codes that the Command Authority has established.

(U//FOUO) If a person who is acting as a Command Authority also needs to be able to order asymmetric products, then that person must also become enrolled as a Product Requester.

**CI2-SAR-5.3.2.3g** (U//FOUO) The KMI shall permit only the Role of Product Requester to be assigned Permissions that enable a Manager to order asymmetric products. [DRV KRD 0910, 0949] {R}

**CI2-SAR-5.3.2.3a** (U//FOUO) The KMI shall enable a Command Authority, and only a Command Authority, to authorize one or more Product Requesters (i.e., User Identities that are currently assigned to the Role of Product Requester) to order asymmetric products containing Partition Codes and DAO Codes that are under the control of that Authority. [DRV KRD 0949, 1720, 1721, 1722] {C-R}

**CI2-SAR-5.3.2.3b** (U//FOUO) The KMI shall enable a Command Authority to withdraw or modify any ordering authorization previously granted to a Product Requester for use of any Partition Code or DAO Code under the control of that Authority. [DRV KRD 1722] {C-R}

**CI2-SAR-5.3.2.3h** (U//FOUO) The KMI shall enable a Product Requester to order and specify the RuBAC Property values for any of the asymmetric products, but only those products, for which the necessary Partition Code and/or DAO Code ordering authorization has been granted to the Requester by a Command Authority. [DRV KRD 0425, 0946, 0949, 1034, 1720, 1722] {C-R}

**CI2-SAR-5.3.2.3i** (U//FOUO) The KMI shall enable a Product Requester to order an asymmetric product for distribution through a KOA (i.e., list the KOA Identifier on the Account Distribution Profile of the product; i.e., authorize the KOA to distribute the product to User Devices). [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.2.3j** (U//FOUO) The KMI shall enable a Product Requester to order an asymmetric product for distribution through a non-KOA KME; that is, the requester can list a COMSEC Account's EKMS identifier on the Account Distribution Profile of the product. [DRV KRD 0949] {C-R}

**CI2-SAR-5.3.2.3k** (U//FOUO) The KMI shall permit a Product Requester to order an asymmetric product for a KOA only if the RuBAC Property values of the product are contained in the RuBAC Access Set of the KOA. [DRV KRD 0946, 1332] {R}

**CI2-SAR-5.3.2.3l** (U//FOUO) The KMI shall maintain an Account Distribution Profile for each asymmetric product that is ordered by a Product Requester, and the profile shall contain the following data items: [DRV KRD 0910, 0911] {R}

- (1) The product's RuBAC Property values.
- (2) The KOA (or non-KOA Key Management Entity (KME), i.e., COMSEC account) to which the product is distributed, with necessary information about the order, including (a) the User Identity of the Product Requester who placed the order; (b) distribution requirements, such as routing, required quantities, and need dates; and (c) whether per-order approval is required.
- [Additional data items are defined in volume 1, and still more items are expected to be defined when a detailed design is done.]

**CI2-SAR-5.3.2.3m** (U//FOUO) The KMI shall enable a Product Requester to request that an asymmetric product be distributed through a KOA regardless of whether the requester and the KOA belong to the same Enrollment Domain or not. [DRV KRD 0949] {R}

(U//FOUO) A Command Authority may require per-order approval before distribution, i.e., require a separate, pre-distribution authorization action for each individual order of a product, either for all orders for that product or for orders for that product that are received from selected Product Requesters.

**CI2-SAR-5.3.2.3c** (U//FOUO) The KMI shall notify a Command Authority when an order for an asymmetric product requires approval by that Authority. [DRV KRD 1483, 1776] {R}

**CI2-SAR-5.3.2.3d** (U//FOUO) The KMI shall enable a Command Authority to approve or disapprove an order for an asymmetric product containing Partition Codes and DAO Codes that the Authority controls. [DRV KRD 1483, 1563, 1776] {R}

**CI2-SAR-5.3.2.3e** (U//FOUO) The KMI shall not generate and distribute an asymmetric product based on an order that requires approval until the KMI has received an authenticated approval from the appropriate Command Authority. [DRV KRD 1484, 1561, 1563, 1564, 1777] {R}

**CI2-SAR-5.3.2.3f** (U//FOUO) The KMI shall record for Audit any product order approval given by a Command Authority. [DRV KRD 1564] {R}

### 5.3.3 (U) KMI Operating Accounts

(U//FOUO) A KOA is KMI's logical construct for managing the distribution of products and providing related services to a set of registered User Devices, typically a set being used by a unit of a DoD Service or agency. Each KOA has one or more KOA Managers that are able to request the distribution of products to the devices held in the KOA.

(U//FOUO) In the CI-2 timeframe, some products that are ordered through PRSN OMEs will be distributed to User Devices through PRSN PDEs, and some will be distributed through legacy EKMS mechanisms or physical means. In all cases, however, the distribution must be associated with a COMSEC account. Therefore, each KOA will be associated with a specific COMSEC account in the CI-2 timeframe.

#### 5.3.3.1 (U) KOA Registration and Associated Data

(U//FOUO) Each KOA is established by a registration process that records administrative data for the account.

**DEFINITION** (U//FOUO) KOA Registration Data. The set of data values that is maintained by the KMI for managing a KOA.

(U//FOUO) The KMI retains part of the data on a long-term basis for compromise recovery, and uses other parts on a day-to-day basis for performing ordering and distribution functions.

**CI2-SAR-5.3.3.1a** (U//FOUO) The KMI shall enable a KOA Registration Manager to establish new KOAs. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.1b** (U//FOUO) The KMI shall, when establishing a new KOA, place the KOA in either (1) the Enrollment Domain of the KOA Registration Manager that establishes the account or (2) an existing Enrollment Domain that is subordinate to that Manager's domain. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.1c** (U//FOUO) The KMI shall require a KOA Registration Manager, when establishing a KOA, to associate the KOA in a one-to-one relationship with an existing COMSEC Account, and shall present to the Manager a list of the EKMS Identifiers of COMSEC Accounts that are available for selection. [KRD NEW] {R}

**CI2-SAR-5.3.3.1d** (U//FOUO) The KMI shall enable a KOA Registration Manager to record KOA Registration Data when establishing and operating a KOA, including the following subsets: [DRV KRD 0949] {R}

- (1) Core Data.
- (2) RuBAC Access Set.
- (3) Data about the KOA Managers that are assigned to the account.
- (4) Data about the User Devices that are assigned to the account.
- (5) Data about Device Distribution Profiles of products that have been ordered for the account.

[Additional data items are expected to be defined when a detailed design is done.]

(U//FOUO) A COMSEC Account is a type of Key Management Entity (KME), and each KME is listed in the EKMS Directory. Because KOAs have a one-to-one relationship with COMSEC Accounts, the set of data items that comprise the KOA Registration Data is expected to overlap with the set of the data items that comprise the EKMS Common Account Data.

**CI2-SAR-5.3.3.1e** (U//FOUO) The KMI shall enable a KOA Registration Manager to record KOA Core Data when establishing a KOA. [DRV KRD 0949] {R}

**DEFINITION** (U//FOUO) KOA Core Data. A subset of the KOA Registration Data that distinguishes a KOA from all other KOAs and relates it to non-KMI systems and organizations.

(U//FOUO) KOA Core Data items are intended to have values that remain essentially constant over the life of the KOA.

**CI2-SAR-5.3.3.1f** (U//FOUO) The KOA Core Data shall include at least the following: [DRV KRD 0949] {R}
- (1) The EKMS Identifier of the associated COMSEC account.
- (2) The assigned KOA Identifier.
- (3) Identification and contact information for the organizational authority that sponsors the KOA's registration, i.e., a unit of a DoD Service or Agency, or of some other Department of the U.S. Government.
- [Additional data items are expected to be defined when a detailed design is done.]

**DEFINITION** (U//FOUO) KOA Identifier. A name that can be unambiguously represented by a printable, non-blank character string.

(U//FOUO) Each KME has an EKMS Identifier. In support of the intended transition from EKMS to KMI, each KOA Identifier is expected to be algorithmically derivable from the EKMS Identifier of the KOA's associated COMSEC account, and vice versa.

**CI2-SAR-5.3.3.1g** (U//FOUO) The KMI shall require a KOA Registration Manager, when establishing a KOA, to assign to that KOA a permanent, KMI-unique KOA Identifier. [DRV KRD 0949] {R}

(U//FOUO) Each KOA has a RuBAC access set that contains values for the same set of RuBAC Attributes that are defined for managers (see "RuBAC Attributes for Managers" section). Just as a manager's access set limits the manager's access to system objects in general, a KOA's Access Set limits the products that can be distributed to the account.

**CI2-SAR-5.3.3.1h** (U//FOUO) The KMI shall enable a KOA Registration Manager, when establishing a KOA, to assign to the new account a RuBAC Access Set that contains only values that are also contained in the manager's RuBAC Conferral Set. [KRD NEW] {R}

**CI2-SAR-5.3.3.1i** (U//FOUO) The KMI shall enable a KOA Registration Manager to either add or delete a RuBAC Attribute value in the RuBAC Access Set of a KOA only if both of the following conditions hold: [KRD NEW] {R}
- (1) The value is contained in the RuBAC Conferral Set of the KOA Registration Manager that is making the change.
- (2) The KOA being changed is contained in either (a) the Enrollment Domain of the KOA Registration Manager or (b) an Enrollment Domain that is subordinate to that Manager's domain.

**CI2-SAR-5.3.3.1j** (U//FOUO) If a KOA Registration Manager deletes a RuBAC Attribute value in the RuBAC Access Set of a KOA, then for every product that (a) has the counterpart

value in its RuBAC Property set and (b) has the KOA on its Account Distribution Profile, the KMI shall do all of the following: [KRD NEW] {R}

- (1) Delete the KOA from that product's Account Distribution Profile
- (2) Delete that product's Device Distribution Profile from the KOA, if such a profile exists.
- (3) Provide appropriate notice of the deletion actions to the KOA Manager, the product's Controlling Authority, and every Product Requester that ordered the product for the KOA.

**CI2-SAR-5.3.3.1k** (U//FOUO) The KMI shall record for Audit (1) the assignment of a RuBAC Access Set to a KOA and (2) any change in a KOA's RuBAC Access Set. [DRV KRD 1564] {R}

**CI2-SAR-5.3.3.1l** (U//FOUO) The KMI shall enable a KOA Registration Manager to terminate an existing KOA only if both of the following conditions hold: [KRD NEW] {R}

- (1) The RuBAC Access Set of the KOA being terminated is contained in the Conferral set of the KOA Registration Manager.
- (2) The KOA being terminated is contained in either (a) the Enrollment Domain of the KOA Registration Manager or (b) an Enrollment Domain that is subordinate to that Manager's domain.

### 5.3.3.2 (U) KOA Managers

(U//FOUO) A KOA Manager performs two primary functions: (1) associating ECUs with a KOA and (2) determining which ECUs within a KOA should receive each specific product that has been ordered for the KOA. A KOA Manager also performs secondary functions that are described and specified in following subsections.

(U//FOUO) Each KOA can have one or more associated KOA Managers, of whom one is the Primary KOA Manager. (A KOA also may have one or more associated KOA Agents, as described in the "KOA Agent" section below.) The work of managing a KOA can be divided among its KOA Managers. The KMI permits only the Primary KOA Manager (and cognizant KOA Registration Managers) to assign other KOA Managers to the account, but any other division of labor among an account's KOA Managers is defined by local operating procedures and is not specified here.

**CI2-SAR-5.3.3.2a** (U//FOUO) The KMI shall enable each KOA to have one or more KOA Managers be assigned to the account, of which exactly one at a time is designated as the Primary KOA Manager. [KRD 0951] {C-R}

**CI2-SAR-5.3.3.2b** (U//FOUO) The KMI shall require that when a KOA Registration Manager establishes a KOA, that Manager must assign to the account a KOA Manager that is designated as the account's Primary KOA Manager. [KRD 0951] {C-R}

**CI2-SAR-5.3.3.2c** (U//FOUO) The KMI shall enable each of the following Managers to assign one or more additional KOA Managers to a KOA to assist the Primary KOA Manager: [KRD 0951] {C-R}
- (1) The KOA Registration Manager that established the KOA.
- (2) A KOA Registration Manager in either (a) the same Enrollment Domain as the KOA Registration Manager that established the KOA or (b) a Domain that is superior to that of the establishing Manager.
- (3) The KOA's Primary KOA Manager.

**CI2-SAR-5.3.3.2d** (U//FOUO) The KMI shall enable a KOA Manager to be assigned to a KOA only if the Manager belongs to the same Enrollment Domain as does the KOA. [DRV KRD 0951] {C(NT)-R}

**CI2-SAR-5.3.3.2e** (U//FOUO) The KMI shall permit a KOA Manager to be assigned to a KOA only if the RuBAC Access Set of the KOA is contained in the RuBAC Access Set of the Manager. [DRV KRD 0425, 0951, 1034] {C-R}

**CI2-SAR-5.3.3.2f** (U//FOUO) The KMI shall ensure that the User Identity of a KOA Manager assigned to a KOA belongs to a different Human User than any other KOA Manager assigned to that KOA. [DRV KRD 0951] {C-R}

**CI2-SAR-5.3.3.2g** (U//FOUO) The KMI shall permit an enrolled KOA Manager to have a current status of being assigned to just one KOA, to two or more KOAs, or to none. [KRD 1196] {R}

(U//FOUO) A KOA's Primary KOA Manager can be replaced, but the position cannot be left vacant. A KOA's other KOA Managers can simply be removed; a KOA is not required to have any KOA Managers in addition to the Primary.

**CI2-SAR-5.3.3.2h** (U//FOUO) The KMI shall enable each of the following Managers to replace a KOA's Primary KOA Manager with another KOA Manager: [KRD 0951] {R}
- (1) The KOA Registration Manager that established the KOA.
- (2) A KOA Registration Manager in either (a) the same Enrollment Domain as the KOA Registration Manager that established the account or (2) a Domain that is superior that of the establishing Manager.

**CI2-SAR-5.3.3.2i** (U//FOUO) The KMI shall enable each of the following Managers to view a KOA's list of currently assigned KOA Managers and remove any that are not the Primary: [KRD 0951] {C-R}
- (1) The KOA's Primary KOA Manager.
- (2) The KOA Registration Manager that established the KOA.
- (3) A KOA Registration Manager in either (a) the same Enrollment Domain as the KOA Registration Manager that established the account or (2) a Domain that is superior to that of the establishing Manager.

### 5.3.3.3 (U) KOA Device Assignment

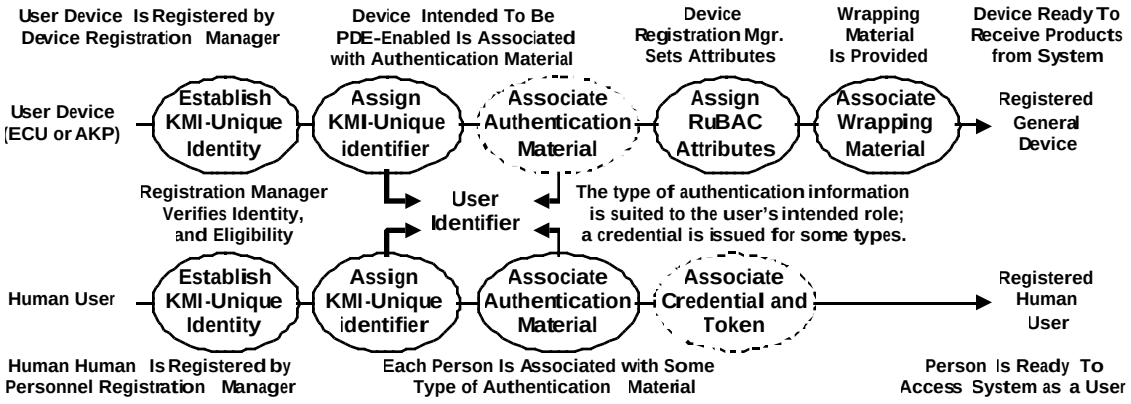
(U//FOUO) A KOA's managers maintain a list of devices that are administratively assigned to the account. Maintaining the list involves the following step, as illustrated by Figures 36 and 38:

- **Request to associate device with account**. A KOA Manager, working at a Client Node, connects to a PRSN OME and requests that a device be assigned to a specific KOA.

(U//FOUO) As described in the "User Devices" section of Volume 2, the KMI supports three types of user devices as KMI registered users: End Cryptographic Unit (ECU), Fill Device, and Advanced Key Processor (AKP). ECUs and AKPs can be registered as general devices, i.e., user devices for which the registration has significance across the entire KMI and for which a product can be generated and wrapped by a PSN for distribution to that specific device. In CI-2, fill devices can be registered only as limited devices, i.e., devices for which the registration has significance at only one Management Client Node, at which products can be wrapped by an AKP for distribution to that specific Device. Some ECUs can be registered only as a limited device; also, an ECU that is registered as a general device can be treated like a limited device by the KOA to which the device is assigned.

(U//FOUO) Figure 39 illustrates the registration process for general devices and compares it to that for human users. As described in the "Client Support for Registered Users" section of Volume 2, a device that is registered as a general device may also be constructed, registered, and installed so that it is PDE-enabled, i.e., able to connect as a Client Node to a PRSN PDE to obtain KMI products and services. A PDE-enabled general device needs to be registered with associated authentication material (in addition to its key wrapping material); and, depending on the authentication technology being used, the device may be issued a credential. Thus, the registration process for PDE-enabled general devices is similar to that for human users.

**Figure 39. (U) KMI Registration of General Devices at PRSN**




**UNCLASSIFIED//FOUO**

(U//FOUO) Registration as a limited device is described and specified in the "Local Device Registration Management" section of Volume 1. The registration process for a limited device is similar to that shown in Figure 39. However, the registered identity is unique only within the

scope of the Client Node that supports the device, and the device does not need authentication material for logging in at a PRSN.

(U//FOUO) As illustrated by Figure 39, the registration process for devices also has steps that are not needed for humans:

- Assign RuBAC Attributes. Each device is assigned a Device Registration RuBAC Set that controls the distribution of products to the device.

- Associate wrapping material. Each device is associated with cryptographic material that can be used to wrap products that are distributed to the device.
  - ECUs that are over-the-network-keyable or benign techniques-capable have FIREFLY credentials.
  - ECUs and Fill Devices that accept BLACK fill have key-encryption keys (KEKs).
  - AKPs have FIREFLY credentials.

(U//FOUO) Although Figure 39 shows "Associate Wrapping Material" as the last step of the registration process for devices, the figure is only notional; wrapping material could be loaded before registration, or at any point during or after the process, depending on the procedures required for manufacture, initialization, and registration of a specific type of device.

(U//FOUO) General devices are normally expected to be registered at a key loading and initialization facility (KLIF). When any user is registered, the User Registration Manager records items of user registration data, including user core data and identifier registration data (as described and specified in the "User Identity Registration and Identification Service" section of Volume 2). Among those items is at least one user identifier. When the user being registered is a device, the User Registration Manager is a Device Registration Manager, and that manager records additional data items that are specific to devices:

**CI2-SAR-5.3.3.3a** (U//FOUO) The KMI shall enable a Device Registration Manager to record the following additional items of User Registration Data (in addition to those specified in the *Security Policy* [KMI2200V2]) when registering a User Device: [DRV KRD 0949, 1332, 1965] {C-R}
- (1) As part of the User Core Data for the device:
  - The device's globally unique Device Serial Number [KMI3001].
- (2) As part of the Identity Registration Data for the device:
  - The device's Device Registration RuBAC Set.
  - Identification of key material to be used for wrapping products for distribution to that device. (See Volume 1 for other requirements regarding wrapping material.)
- [Additional data items are expected to be defined when a detailed design is done.]

**DEFINITION** (U//FOUO) Device Serial Number. A centrally registered, electronically processed identifier that is assigned to a KMI User Device or other information assurance device for the purpose of remote management and is unique across all NSA equipment programs.

**DEFINITION** (U//FOUO) Device Registration RuBAC Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute values, (2) is associated with a User Device Identity, and (3) controls the distribution of products to the device in any KOA to which the device is assigned.

(U//FOUO) Concurrent with registration at a KLIF, a device is normally expected to be assigned to an initial KOA.

**CI2-SAR-5.3.3.3b** (U//FOUO) The KMI shall require each newly registered General Device to be assigned to an initial KOA when the Device is registered in the KMI. [DRV KRD 0949] {C-R}

(U//FOUO) This *Security Architecture* does not specify requirements to differentiate KOAs according to specialized functions, but the initial KOA might be called a "factory KOA" or "depot KOA". In a small KLIF, the same person might act as both (1) the Device Registration Manager and (2) a KOA Manager of the depot KOA.

**CI2-SAR-5.3.3.3c** (U//FOUO) The KMI shall enable a KOA Manager that is currently assigned to a KOA, to assign a registered User Device (specified by a User Identifier, Device Serial Number, or some other KMI-unique identifier) to that KOA. [DRV KRD 0949] {C-R}

(U//FOUO) For each device, the KMI recognizes exactly one KOA at a time as being in charge of the device; that KOA needs to give permission before another KOA may distribute products to the device or receive products for it.

**CI2-SAR-5.3.3.3d** (U//FOUO) The KMI shall ensure that each General Device is assigned to at most one KOA at a time. [DRV KRD 0949] {C-R}

(U//FOUO) A device is expected to be held in a depot KOA until it is transferred to a "working KOA" that fields the device and loads it with operational keying material.

**CI2-SAR-5.3.3.3e** (U//FOUO) The KMI shall enable a KOA Manager to request that a General Device (specified by its KMI-Unique User Identifier) that is currently assigned to a KOA of that Manager (the "old" account) be transferred to another KOA (the "new" account) specified by that Manager (i.e., be deassigned from the old account and reassigned to the new account). [DRV KRD 0949] {C-R}

(U//FOUO) The KOA Manager that requests a KOA-to-KOA transfer for a device may be a manager only for the old account or also for the new account, but cannot be a manager only for the new account.

**CI2-SAR-5.3.3.3f** (U//FOUO) When the KMI receives a request to transfer a General Device from one KOA to another, the KMI shall notify one or more KOA Managers that currently are assigned to the intended destination KOA and request consent for the transfer. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.3g** (U//FOUO) The KMI shall not carry out a KOA-to-KOA transfer of a General Device until at least one of the currently assigned KOA Managers of the destination account has consented to the transfer. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.3h** (U//FOUO) When the KOA transfers a General Device from one KOA to another KOA, the KMI shall terminate distribution of products to the device from the first KOA (i.e., shall remove the device from all of the first KOA's Device Distribution Profiles on which the device is listed). [DRV KRD 0425, 1034] {R}

**CI2-SAR-5.3.3.3i** (U//FOUO) The KMI shall record for Audit the transfer of a General Device from one KOA to another KOA. [DRV KRD 0990] {C-R}

(U//FOUO) When a device that is assigned to a working KOA is no longer needed, it might be transferred back to its initial depot KOA or to some other depot KOA. Then, it might be transferred to another working KOA that needs it. Finally, if a device is decommissioned, destroyed, lost, or otherwise no longer usable by a working KOA, it might be transferred to a "disposal KOA".

**CI2-SAR-5.3.3.3j** (U//FOUO) The KMI shall permit a General Device to be held by a KOA only if the device's Device Registration RuBAC Set is contained in the KOA's RuBAC Access Set. [DRV KRD 0424, 1332] {C-R}

**CI2-SAR-5.3.3.3k** (U//FOUO) The KMI shall record for Audit any request by a KOA Manager to assign a User Device to a KOA when the device's Device Registration RuBAC Set is not contained within the KOA's RuBAC Access Set. [DRV KRD 1564] {C-R}

**CI2-SAR-5.3.3.3l** (U//FOUO) When a KOA Manager assigns a General Device to a KOA or consents to the transfer of a General Device to a KOA from another KOA, the KMI shall record the following items of Device Data, which are in addition to those specified in the *Security Policy and Related Requirements* [KMI2200V2]: [DRV KRD 1332] {C-R}

- (1) The KOA Identifier of the KOA to which the Device is newly assigned or transferred.
- (2) A Device Convenience Label for the Device.
- (3) An (optional) Device Account RuBAC Set for the Device.
- [Additional data items are expected to be defined when a detailed design is done.]

(U//FOUO) When a user device is assigned to its initial KOA or transferred to another KOA, that KOA becomes the User Device Sponsor that is discussed in the "Registration of Singular Identities" section of Volume 2.

**DEFINITION** (U//FOUO) Device Convenience Label. A non-blank printable text string that is assigned to a User Device, is unique among the User Devices in the KOA to which the device is currently assigned, and can be used by the KOA Managers to assist in identifying and managing the device.

**DEFINITION** (U//FOUO) Device Account RuBAC Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute values, (2) is associated with a

User Device Identity in the context of the KOA to which the device is currently assigned, and (3) controls the distribution of products to the device within that KOA.

(U//FOUO) The constraints imposed by a device's Device Registration RuBAC Set cannot be relaxed by the KOA Managers of a KOA to which the device is assigned; but those managers can, by assigning a Device Account RuBAC Set to the device, impose additional constraints, in order to assist in managing the device within that account.

**CI2-SAR-5.3.3.3m** (U//FOUO) The KMI shall ensure that a Device Convenience Label proposed by a KOA Manager for a User Device in a KOA is a non-blank printable text string that is unique among the User Devices currently assigned to that KOA, before permitting the label to be associated with that User Device. [DRV KRD 0949] {C-R}

**CI2- SAR-5.3.3.3n** (U//FOUO) The KMI shall enable an KOA Manager to obtain a sorted list of User Devices, including associated data items, that are currently held by a KOA to which that Manager is currently assigned. [DRV KRD 0949] {C-R}

### 5.3.3.4 (U) KOA Local Product Distribution

(U//FOUO) After a Product Requester has ordered a product for one or more KOAs, the KOA Managers of those KOAs can direct distribution of the product to devices owned by their accounts. This involves the following step, as illustrated by Figures 36 and 38:

- **Request to distribute product to device**. A KOA Manager of a specific KOA requests that a product, which has been ordered for that account by a Controlling Authority or Product Requester, be distributed to one or more devices in the account.

(U//FOUO) This step causes a device distribution profile to be established for the product associated with that KOA.

**CI2-SAR-5.3.3.4a** (U//FOUO) For each KOA, the KMI shall establish and maintain a separate Device Distribution Profile for each product for which a KOA Manager requests distribution to a User Device in the account. [DRV KRD 0424] {C-R}

**CI2-SAR-5.3.3.4b** (U//FOUO) A Device Distribution Profile for a product shall contain the following data items: [DRV KRD 0425] {C-R}

- (1) The product's Short Title (or some other KMI-unique identifier for the product).
- (2) A list of the User Devices (designated by KMI-unique Device Identifiers [KMI3001]) for which distribution orders are active for that product, with necessary information about each order, such as distribution routing and other items.
- [Additional data items are expected to be defined when a detailed design is done.]

**CI2-SAR-5.3.3.4c** (U//FOUO) For each KOA, the KMI shall enable each KOA Manager of the KOA to request distribution of any of the products, but only those products, for which Authorization has been granted to the KOA by a Controlling Authority or Product Requester (i.e., products for which the KOA is listed on the product's Account Distribution Profile). [DRV KRD 0425, 0946, 0949, 1034, 1720, 1722] {C-R}

**CI2-SAR-5.3.3.4d** (U//FOUO) For each KOA, the KMI shall enable each KOA Manager of the KOA to request distribution of a product to an individual User Device (i.e., to place the User Device on that KOA's Device Distribution Profile for that product). [DRV KRD 0425] {C-R}

**CI2-SAR-5.3.3.4e** (U//FOUO) For each KOA, the KMI shall enable each KOA Manager of the KOA to terminate distribution of a product to an individual User Device (i.e., remove a User Device from that KOA's Device Distribution Profile for that product). [DRV KRD 0425, 1034] {R}

**CI2-SAR-5.3.3.4f** (U//FOUO) The KMI shall record as a Mandatory Audit Event any request by a KOA Manager to place a User Device on a Device Distribution Profile, or to remove one from a profile. [DRV KRD 0990] {C-R}

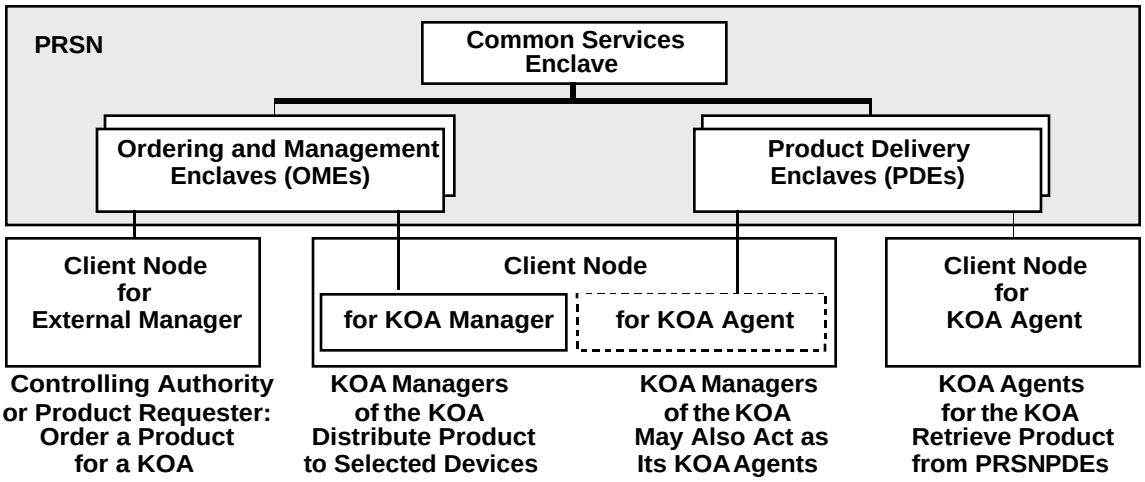
(U//FOUO) Each product has RuBAC Property values and can be distributed only to devices that have compatible RuBAC Attribute values.

**CI2-SAR-5.3.3.4g** (U//FOUO) The KMI shall enable a KOA Manager to request the distribution of a product to a User Device only if the product's RuBAC Property values are contained in both (1) the counterpart values of that device's Device Registration RuBAC Set and (2) the counterpart values of that device's Device Account RuBAC Set. [DRV KRD 0424, 0612, 1332] {C-R}

### 5.3.3.5 (U) KOA Agents: Designation and Removal

(U//FOUO) When products being distributed by a KOA have been generated and wrapped for distribution, they are placed in PDEs. Human users that have been enrolled as KOA Agents for that KOA access the PDEs, as illustrated in Figure 40, to retrieve the products for use in cryptographic devices that are assigned to the KOA.

**Figure 40. (U) KMI Product Distribution via KOA Agents**




UNCLASSIFIED//FOUO

**DEFINITION** (U//FOUO) KOA Agent. A User Identity of a Human User that is designated by a KOA to access PRSN PDEs for the purpose of retrieving wrapped products that have been requested for User Devices that are assigned to that KOA.

**CI2-SAR-5.3.3.5a** (U//FOUO) PRSN Common Services shall receive products items from PSNs and place them into PDEs to be retrieved by KOA Agents, in accordance with the distribution directions and designations of Controlling Authorities, Product Requesters, and KOA Managers. [DRV KRD 0949] {P-R}

(U//FOUO) A general device that is PDE-enabled can access a PRSN PDE to receive products that have been wrapped by a PSN according to the directions of the KOA Managers of the KOA to which the device is assigned. However, if a general device is not PDE-enabled, then some human user who is designated as a KOA Agent for that account needs to retrieve the products from a PDE so that they can be delivered to the device.

(U//FOUO) The KOA Agent role is not a management role; it is only a designation for a registered identity of a human user that has been associated with one or more KOAs. The process by which a person becomes a KOA Agent has two stages:

- (U//FOUO) **Stage 1: Registration as a Human User**. An identity is registered for the user as illustrated in Figure 39 (see "User Registration and Identification Service" of Volume 2). A human identity is registered by a Personnel Registration Manager, but the registration process is expected to differ depending on whether the identity is intended to be enrolled as a manager or only designated as a KOA Agent. The Registration Manager is likely to be associated with an Enrollment Manager in the first case, and with a KOA Manager in the second case. Also, the rigor with which the user's identity and eligibility are verified is expected to vary between the two cases, as is the amount and type of registration data that is gathered by the system. If an identity is first registered to become a manager, then no additional registration processing should be needed before also designating that identity as a KOA Agent. But if a human identity is first registered to become a KOA Agent, than it is expected that additional processing will be needed to upgrade the registration before enrolling the identity as a manager, including upgrading the identity's associated authentication material.

- (U//FOUO) **Stage 2: Designation as a KOA Agent**. A KOA Manager designates the registered human identity as a KOA Agent for a specific KOA.

(U//FOUO) A human user identity might have more than one KMI-unique user identifier (see "User Identifier Registration Section" of Volume 2). To make the KOA Manager's job easier, the KMI permits the manager to use any of those identifiers for designating or removing the identity as a KOA Agent. The KMI also automatically designates the identities of KOA Managers to be KOA Agents for their own KOAs, and permits an identity to be designated as a KOA Agent for more than one KOA.

**CI2-SAR-5.3.3.5b** (U//FOUO) The KMI shall enable each KOA Manager of a KOA to designate the User Identities of one or more Human Users to be KOA Agents to retrieve products from PDEs on behalf of that KOA. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.5c** (U//FOUO) The KMI shall enable each KOA Manager of a KOA to remove the KOA Agent designation from one or more KOA Agents in that KOA. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.5d** (U//FOUO) The KMI shall enable a KOA Manager of a KOA to designate or remove a User Identity of a Human User as a KOA Agent by entering or selecting any one of the KMI-Unique User Identifiers of that User Identity. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.5e** (U//FOUO) A User Identity of a Human User shall be permitted to be designated as a KOA Agent by one or more KOAs. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.5f** (U//FOUO) The KMI shall automatically designate the User Identities of the KOA Managers of a KOA to be KOA Agents for that KOA. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.5g** (U//FOUO) The KMI shall record as a Mandatory Audit Event any request by a KOA Manager to designate a User Identity as a KOA Agent or to remove that designation from a User Identity. [DRV KRD 0071, 0876, 0990] {R}

(U//FOUO) KMI customer organizations might want to establish a process for vetting and preapproving KOA Agents before assigning them to KOAs, in the same way that KOA Managers are enrolled by Enrollment Managers before being assigned to KOAs, but this *Security Architecture* does not specify system functions to implement or support such a process.

### 5.3.3.6 (U) KOA Agents: Login at PDE

(U//FOUO) The designation of a human user identity as a KOA Agent for some KOA results in that identity being placed on the KMI-wide list of all KOA Agents .

**DEFINITION** (U//FOUO) KOA Agents List. The list of all the registered User Identities that are currently designated as KOA Agents.

(U//FOUO) This *Requirements Specification* [KMI2200] does not specify how to implement the KOA Agents List, but any implementation approach will necessarily involve replicating the list data between independent components of the system. For example, an obvious choice of a component in which to maintain the list is the PRSN Common Private Zone. However, the requirements stated in the “PRSN Service Redundancy and Data Replication” section imply that data from the list must be replicated between PRSNs, and the requirement to check the list for each PDE login implies that data from the list must be replicated from Common Services to all PDEs within a PRSN.

**CI2-SAR-5.3.3.6a** (U//FOUO) The KMI shall maintain a KOA Agents List consisting of all User Identities that are currently designated as a KOA Agent by one or more KOAs. [DRV KRD 0949] {R}

**CI2-SAR-5.3.3.6b** (U//FOUO) The KMI shall permit a User Identity to log in at a PDE as a KOA Agent only if that User Identity is currently listed on the KOA Agents List. [DRV KRD 0949] {R}

(U//FOUO) To make the KOA Agent's job easier, the KMI permits a KOA Agent to use any of its user identifiers to log in at a PDE as long as the identifier has authentication material for the authentication method used by the PDE. Each PDE uses only one authentication method for KOA Agents, and each KMI-unique user identifier is associated with only one type of authentication method (i.e., may have only one type of authentication material). However, not all identifiers of an identity need be authenticated with the same method, so that a KOA agent that has two identifiers, each with a different type of authentication material, might be able to access two different types of PDEs.

**CI2-SAR-5.3.3.6c** (U//FOUO) The KMI shall enable a User Identity to use each of its User Identifiers to log in as a KOA Agent at any PDE for which the identifier has valid Authentication Material of the type required by the PDE. [DRV KRD 0949] {R}

(U//FOUO) This *Requirements Specification* [KMI2200] does not specify how to implement the login process for KOA Agents, but any implementation approach would involve replicating data between independent components of the system. The requirements stated in the "PRSN Service Redundancy and Data Replication" section imply that data must be replicated between PRSNs, and the data must be replicated from Common Services to the PDEs within a PRSN. To avoid having each login request result in passing both (1) a verification request from a PDE to Common Services through a PDE Guard and (2) a response in the opposite direction, it would be desirable for Common Services to prestock each PDE with all data needed to authenticate the identities of any KOA Agents that are eligible to access that PDE. Each PDE needs the KMI-unique user identifiers for those eligible Agents and any associated data to operate the PDE's authentication mechanism (e.g., password files, and trust anchors to validate credentials).

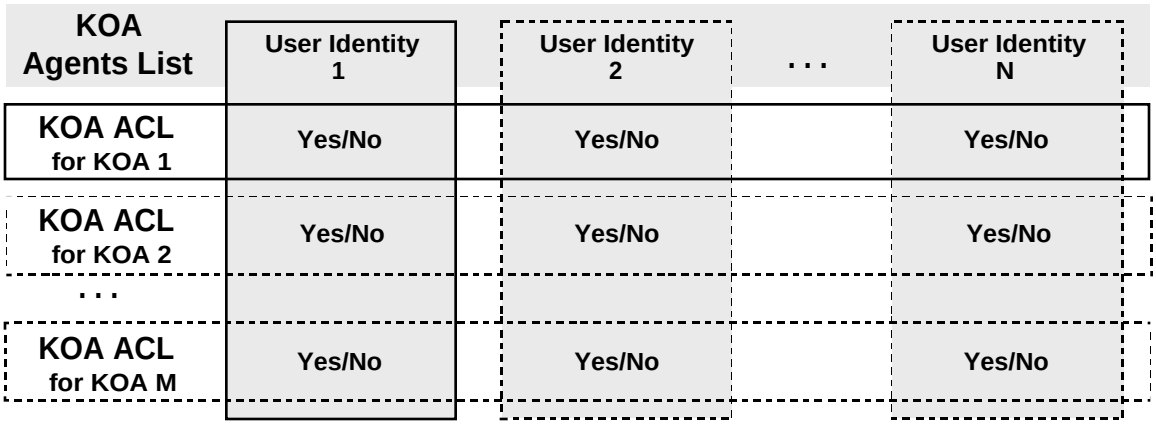
### 5.3.3.7 (U) KOA Agents: Retrieval of Products

(U//FOUO) The designation of a user identity as a KOA Agent for a KOA also results in that identity being added to an access control list for that specific KOA.

**DEFINITION** (U//FOUO) KOA Access Control List. An approval-based Access Control list for a specific KOA, that names the User Identities that are permitted to access PDEs to obtain products that are distributed by that KOA.

(U//FOUO) That is, besides the consolidated KOA Agents List, which lists all current KOA Agents for all KOAs, the KMI maintains a set of KOA-specific lists that each name the KOA Agents for a single KOA. As illustrated in Figure 41, the combination of these lists is logically equivalent to an access control matrix with M rows that each represent a KOA, and N columns that each represent a user identity.

**Figure 41. (U) KMI Access Control for KOA Agents**




**UNCLASSIFIED//FOUO**

**CI2-SAR-5.3.3.7a** (U//FOUO) The KMI shall enable a User Identity that has successfully logged in to a PDE as a KOA Agent to retrieve any product that is held by the PDE for distribution by a KOA that has that User Identity on its KOA Access Control List (i.e., by a KOA for which that Identity is a designated KOA Agent). [DRV KRD 0949] {R}

(U//FOUO) This *Requirements Specification* [KMI2200] does not specify how to implement the KOA Access Control Lists, but any implementation approach would involve replicating the list data between independent components. For example, an obvious choice of a component to maintain the lists is the PRSN Common Private Zone. However, the requirements stated in the "PRSN Service Redundancy and Data Replication" section imply that data must be replicated between PRSNs, and the need to check lists before allowing a KOA Agent to retrieve products from a PDE implies that data must be replicated from the Common Services Enclave to the PDEs within a PRSN.

## 5.4 (U) Alternative Mechanisms for Access Controls

(U//FOUO) Some basic types of mechanisms for implementing access control in an automated information system are access control lists, capability lists, and access control matrices.

**DEFINITION** (U//FOUO) Access Control List. A mechanism that implements access control for a System Resource by enumerating the System Entities that are permitted to access the resource and, either implicitly or explicitly, the access modes granted to each entity.

**DEFINITION** (U//FOUO) Capability List. A mechanism that implements access control for a System Entity by enumerating the System Resources that the entity is permitted to access and, either implicitly or explicitly, the access modes granted for each resource.

**DEFINITION** (U//FOUO) Access Control Matrix. A rectangular array of cells with one row per subject and one column per object. The entry in a cell indicates the mode of access that

the subject is permitted to exercise on the object. (Each column is equivalent to an access control list, and each row to a capability list.)

(U//FOUO) If only these three types of mechanisms were used to implement KMI role-based, rule-based, and approval-based access control, then several different lists or matrices would need to be made available to many different KMI components and probably would prove difficult and expensive to maintain, distribute, and protect. Replacing such lists and matrices, at least in part, by a mechanism involving capability tokens could reduce the complexity of maintaining, distributing, and protecting access control data.

**DEFINITION** (U//FOUO) Capability Token. A token, usually an unforgeable data object, that gives the bearer or holder the right to access a System Resource. Possession of the token is accepted by a system as proof that the holder has been authorized to access the resource that is named or indicated by the token.

(U//FOUO) Attribute certificates, which are specified in X.509, are one possible form that could be used for capability tokens.

**DEFINITION** (U//FOUO) Attribute certificate. A digital certificate that binds a set of descriptive data items other than a public key—such as Authorizations for an Access Control process—either directly to a subject name or to the identifier of another certificate that is a public-key certificate.

# 6 (U) DISTRIBUTED, MULTI-DOMAIN SUBSYSTEMS

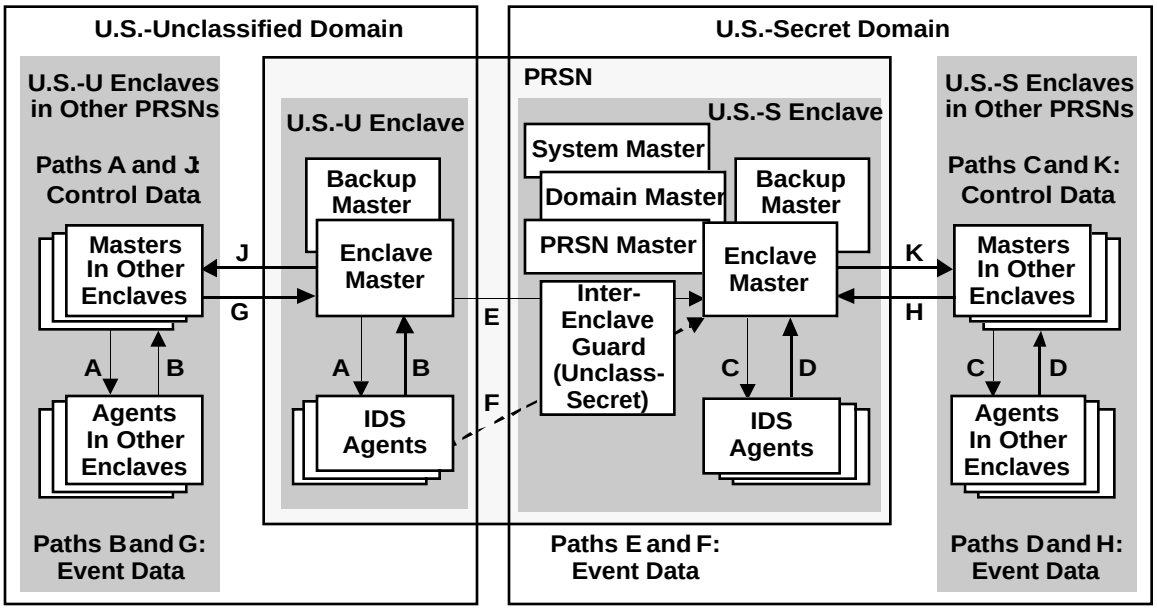
(U/FOUO) Some system-wide security functions, such as the audit service and ASWR, need to be implemented as internodal subsystems. That is, such functions are expected to be implemented by a set of components that are parts of different nodes but also cooperate as parts of the same subsystem.

**DEFINITION** (U//FOUO) Subsystem. A collection of related Components that together perform or deliver a particular KMI function or service. [KMI2020]

(U//FOUO) However, the multiple domains, enclaves, and zones that are specified for PRSNs in this *Security Architecture* cause complications for implementing data flows between subsystem components. As an example, this section presents a model for data flows in an intrusion detection system (IDS) that provides part of the ASWR service that is specified in Volume 2. The data flows needed for other types of KMI-wide services would be similar.

(U//FOUO) The subsystem model presented here assumes that IDS functions need to be distributed across PRSNs and across the enclaves within PRSNs, as illustrated in Figure 42. (Figure 42 is intended only to illustrate the concepts discussed in this section, and is not intended to correspond exactly with the PRSN components shown in figures in other sections, such as Figures 17 and 18.)

**Figure 42. (U) KMI Multi-Domain Subsystem**




UNCLASSIFIED//FOUO

(U//FOUO) The following requirements are basic for any such distributed subsystem of the KMI:

**CI2-SAR-6a** (U//FOUO) Within a Core Node, the Components of a functional Subsystem should be integrated across Security Domains to the extent that is technically possible, but the Components within a domain should be able to operate independently of other domains. [KRD 1180, 1824] {P-R-S}

**CI2-SAR-6b** (U//FOUO) Within a Security Domain, the Components of a functional Subsystem should be integrated across Nodes to the extent that is technically possible, but the Subsystem's functions within a Core Node should be able to operate independently of other Nodes. [KRD 1180, 1824] {P-R-S}

(U//FOUO) When data is replicated between domains, database synchronization and integrity checks are needed. For example, when user registration data is replicated, the KMI needs to compare the replicated User Core Data from one domain to that of another domain and, if duplicates or discrepancies are detected, either update the user's data in one of the domains, or revoke associated identities, identifiers, and credentials and notify an authorized User Registration Manager and SSO according to established procedures.

## 6.1 (U) Intrusion Detection Subsystem

(U//FOUO) As defined in Volume 2, ASWR has three aspects: (1) sensing includes recognizing, identifying, and categorizing attacks and other threat actions; (2) warning includes communicating to a responsible official an alert concerning an attack or other threat action, in time for the official to make a decision and respond with effective counteractions; and (3) response includes initiating a counteraction to an attack or other threat action. The definition of ASWR could be construed broadly to include many different KMI security functions. Here, ASWR is limited to services provided by intrusion detection systems; other, closely related security services, such as audit, are treated separately.

(U//FOUO) Although all KMI nodes need intrusion detection services, this section discusses only PRSNs. Platforms within a PRSN comprise a computer network; there is a set of host (i.e., end system) computers together with an infrastructure (a subnetwork or internetwork) through which the hosts can communicate with each other and with Nodes. In this context, an intrusion detection system (IDS), or subsystem in this case, is an ASWR system that supports the defense of the components against malicious traffic that originates either externally or internally. An IDS may also have features that actively respond in some way to perceived attacks.

### 6.1.1 (U) IDS Types

(U) Many types of IDS products are available, but the two basic types are host-based (HIDS) and network-based (NIDS). In a HIDS, the system components—the sensors and analyzers—are placed on the hosts that they protect. In a NIDS, the sensors are placed on infrastructure components, and the analyzers are placed either on subnetwork platforms or separate hosts.

(U) The two basic IDS methods for detecting attacks are signature detection and anomaly detection. A signature-based IDS scans network traffic to detect packets and streams of packets that have content matching the patterns of known attacks. An IDS of this type has a library of attack patterns, and the library needs to be updated whenever new kinds of attacks become known. Usually, the IDS vendor supplies standard updates, and the IDS operator can add custom

updates. An anomaly-based IDS monitors network traffic to detect deviations from normal (i.e., expected) behavior, which is defined by a profile that has been established in advance. A profile is a set of statistical values and relationships concerning packet frequencies, types, and contents. In commercial offerings, a profile may be established automatically by monitoring traffic for some period of time or manually by defining rules, or both. Both signature- and anomaly-based IDSs typically look at all the fields in the IP header and some of the fields in the TCP header (particularly Source Port and Destination Port). They may or may not look higher into the protocol stack, depending on how they are designed and configured and how much processing power they have available. A signature-based IDS does not "learn" new attack patterns and cannot detect any attack that is not in the library. An anomaly-based IDS may be able to detect a new attack if the attack creates traffic that deviates sufficiently from the established profile.

### 6.1.2 (U) IDS Capabilities In PRSNs

(U//FOUO) Figure 42 illustrates that an IDS typically consists of a number of agents (e.g., sensors), some of which are host-based and some of which are network-based, and one or more management stations called masters, that monitor and control agents, or that monitor and control other masters in a hierarchical arrangement. It is desirable that IDS components in CI-2 PRSNs provide the following capabilities; these capabilities would take CI-2 in the direction of the target system, in which it is intended that all event data be sent to the CSN to be fused and analyzed.

#### 6.1.2.1 (U) Capabilities in Each Enclave of Each PRSN

(U//FOUO) In Figure 42, the subsystem of IDS components in an Unclassified or Secret enclave has the following capabilities:

- (U//FOUO) **Agent per platform**. Each computer platform in each zone—Public, Buffer, and Private—of an enclave has an IDS agent that is responsible for detecting attack events that occur on the platform.

- (U//FOUO) **Master for enclave**. The Private Zone of the enclave has an master ("Enclave Master") that (1) is responsible for controlling agents in the enclave (path A and C) and (2) receives, fuses, and analyzes event data sent to it by agents in the enclave (path B and D).

- (U//FOUO) **Enclave-wide control.** An authorized Manager can use the Enclave Master to operate the IDS subsystem of the enclave independently of the operation of IDS components in any other enclave or node. This implies that backup service for the master needs to be provided by redundant equipment in the same enclave, rather than depending on a master in another enclave.

- (U//FOUO) **Enclave-wide analysis**. An authorized Manager can use the Enclave Master to view all detected attacks that are directed against any platforms in the enclave.

(U//FOUO) These capabilities imply that control messages sent by the Enclave Master in the Private Zone to agents in the Buffer Zone and Public Zone, and event reporting messages received by the master from those agents, need to be permitted to pass through BPSs that separate and protect the zones.

#### 6.1.2.2 (U) Capabilities in Each PRSN

(U//FOUO) In Figure 42, the subsystem of IDS components in each PRSN has the following capabilities:

- (U//FOUO) **Master for PRSN**. The Enclave Master in the Unclassified enclave relays event data from that enclave to the Enclave Master in the Secret enclave (a.k.a. "PRSN Master") (Path E), or else agents in the Unclassified enclave send event data directly to the PRSN Master (Path F). (Alternatively, the PRSN Master might be located in the Secret enclave but be an additional master, separate from the Enclave Master.)

- (U//FOUO) **PRSN-wide analysis**. The PRSN Master receives, fuses, and analyzes event data sent to it from both the Secret and Unclassified enclaves. An authorized Manager can use the PRSN Master to view all detected attacks that are directed against any platforms in the PRSN.

(U//FOUO) These capabilities imply that event reporting messages received by the PRSN Master in the Secret Enclave from the Enclave Master or agents in the Unclassified Enclave, need to be permitted to pass through an inter-enclave guard.

#### 6.1.2.3 (U) Capabilities in Each Security Domain

(U//FOUO) The subsystem of IDS components in each security domain—Unclassified or Secret—has the following capabilities:

- (U//FOUO) **Master for domain**. One enclave of each domain has a master ("Domain Master") that (1) is responsible for controlling all masters in the domain (path J and K) and (2) receives, fuses, and analyzes event data from that domain that is sent to it by all Enclave Masters in that domain (path G and H). (The Domain Master might be an Enclave Master or a PRSN Master, or it might be an additional master that is separate from those.)

- (U//FOUO) **Domain-wide control**. An authorized Manager can use the Domain Master to operate the IDS subsystem of the domain independently of the operation of components in the other domain.

- (U//FOUO) **Domain-wide analysis**. An authorized Manager can use the Domain Master to view all detected attacks that are directed against any platforms in any enclaves of the domain.

(U//FOUO) These capabilities imply that control messages sent by the Domain Master to the Enclave Masters in other enclaves of the domain, and event reporting messages received by the Domain Master from those other masters, need to be permitted to pass through BPSs.

#### 6.1.2.4 (U) Capabilities in System of PRSNs

(U//FOUO) The subsystem of IDS components in the set of all PRSNs has the following capabilities:

- (U//FOUO) **Master for system**. One enclave of the Secret domain has a master ("System Master") that receives, fuses, and analyzes event data from both domains that is sent to it by the Enclave Masters in all Secret enclaves (path G and H). (The System Master might be an Enclave Master, PRSN Master, or Domain Master, or it might be an additional master that is separate from those.)

- (U//FOUO) **System-wide analysis**. An authorized Manager can use the System Master to view all detected attacks that are directed against platforms in any PRSN in the system.

(U//FOUO) These capabilities imply that event reporting messages, that are received by the System Master from Enclave Masters in the Secret domain, need to be permitted to pass through BPS-VPN.

### 6.1.3 (U) Implementation Issues

(U//FOUO) The stated capabilities raise the following questions when evaluating COTS IDS components for use in the multi-domain architecture of PRSNs:

- (U//FOUO) What data needs to pass through a multilevel BPS, i.e., through an inter-domain guard?
- (U//FOUO) What data needs to pass through the single-level BPSs, such as the BPS-BUFs and BPS-VPN illustrated in Figure 17?
- (U//FOUO) What protocols are used for those communications?

(U//FOUO) This discussion assumes that data may move rather freely through an inter-enclave guard from low to high, e.g., from an Unclassified enclave to a Secret enclave, but data that is downgraded from high to low needs to be minimized because of the difficulty of assuring that such data is properly reclassified.

(U//FOUO) In the IDS model presented here, event data moves from the Unclassified domain to the Secret domain, but not in the reverse direction. However, even when data is sent from the Unclassified domain to the Secret domain, there may be problems with how it is moved. If an application component on a platform in a Private Zone sends data through an inter-enclave guard to a counterpart component in another Private Zone, the application data might be carried over a Transport Layer protocol. That protocol could be either a best-effort, datagram protocol such as User Datagram Protocol (UDP) or a reliable protocol such as TCP. UDP could easily be upgraded through a guard, but TCP's acknowledgement packets could not easily be downgraded through a guard. TCP would need to be proxied, and it might be necessary to implement proxies for each side of the guard. The proxy on the Unclassified side would terminate TCP connections there and pass the application data through the guard on some one-way protocol to the proxy on the Secret side. To achieve acceptable, TCP-like reliability from end to end, the proxies would need to be implemented on the guard platform.

(U//FOUO) Within each domain, event data also needs to pass through a BPS-BUF from a Public Zone to a Buffer Zone, through a BPS-PRI from a Buffer Zone to a Private Zone, and through a BPS-VPN pair from one enclave to another. Since no downgrading takes place, passing TCP packets directly through these BPSs is less of a problem than in BPS-IEG, but

carefully filtering of the traffic is still needed. A separate implementation question is whether a COTS IDS supports the relay of event data from one master to another.

(U//FOUO) In the IDS model presented here, control messages do not pass through the inter-enclave guard at all. A master in the Secret domain that could fully control agents and masters in the Unclassified domain probably would cause unacceptable volumes of control data to be downgraded through guards. It might be feasible to downgrade some limited set of control commands, but this should be analyzed further. Also, it would be easier for a master in the Unclassified domain to send control commands to agents and masters in the Secret domain, but this does not seem to be advantageous. If no data was sent from the Secret domain to the Unclassified domain, the master in the Unclassified domain would have to operate "blind"; and if the more vulnerable Unclassified domain could be compromised, the master there might be used to disable the IDS in the more sensitive Secret domain.

(U//FOUO) Control messages do need to pass through BPS-BUF, BPS-PRI, and BPS-VPN components. Again, there is the question of how these messages are moved. Using TCP for control messages would not seem to present any greater problem in these cases than using TCP for event reporting, but carefully filtering of the traffic is still needed.

(U//FOUO) There is a more basic question of why TCP should be used at all for either event reporting or control messages, rather than using Simple Network Management Protocol (SNMP). SNMP assumes that monitoring and control capability is needed most when network service is least reliable. Therefore, SNMP avoids TCP and instead uses UDP, and applications of SNMP are designed with the assumption that some packets may be lost. IDS components might be more robust if they were designed the same way.

## 6.2 (U) Audit Subsystem

(U//FOUO) A subsystem to implement the requirements stated in the "Audit Service" section of Volume 2 would be similar to the IDS subsystem shown in Figure 42. However, the data flows in Figure 42 that carry control messages—paths A, C, J, and K—would be eliminated; to ensure the integrity of the audit process, the ability to control mechanisms that generate audit records on a KMI computer platform needs to be limited to the platform's local Audit Data Manager. Also, the audit data that is reported from one component to another needs to receive data integrity service of high robustness. Otherwise, the audit subsystem needs capabilities similar to those of the IDS subsystem.

## 6.3 (U) Compromise Reports and Revocation Requests

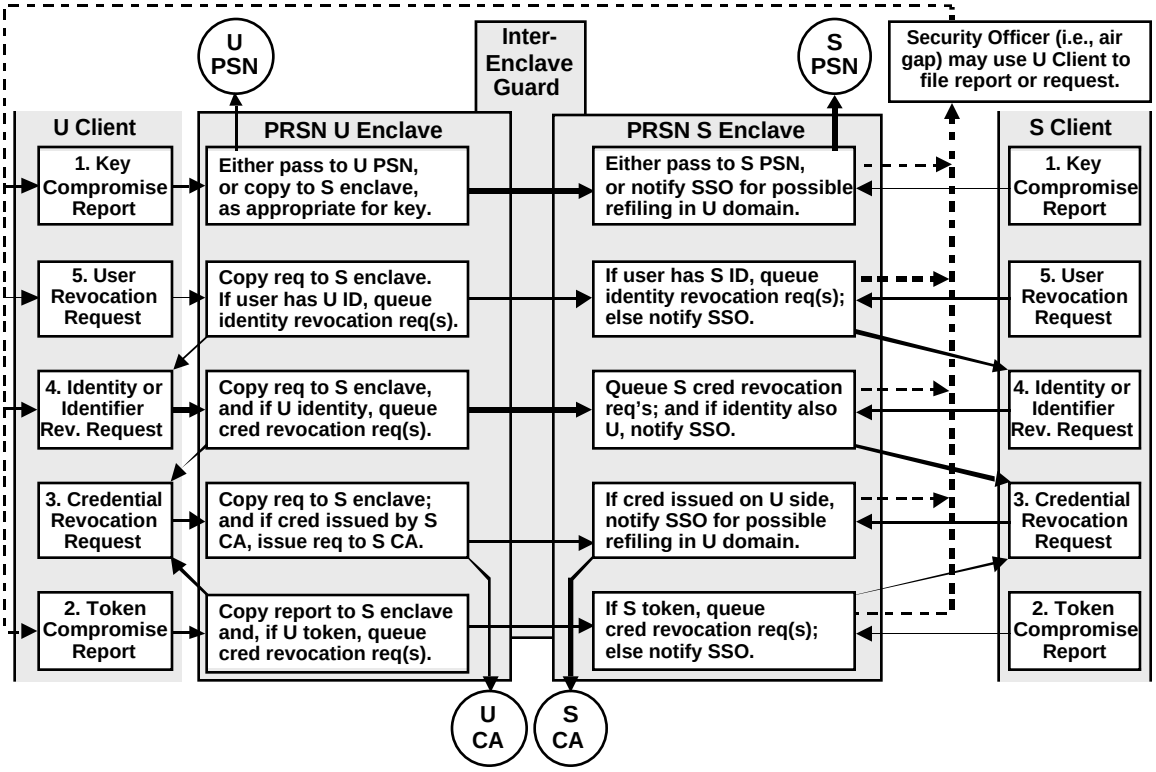
(U//FOUO) Another function that may involve interdomain data flow through a guard, from the Unclassified enclave of a PRSN to the Secret enclave, is the handling of compromise reports and revocation requests. A PRSN needs to enable a user at a Client Node to connect to either the Unclassified or Secret enclave of a PRSN and make the following reports and requests, regardless of the domain in which the subject item was issued or intended to be used:

- (U//FOUO) Report the compromise (loss, theft, or exposed) of a key (lost, stolen, or exposed).

- (U//FOUO) Report the compromise (loss, theft, or PIN exposure) of a cryptographic hardware token.
- (U//FOUO) Request the revocation of a credential.
- (U//FOUO) Request the revocation of an identity or identifier (i.e., revocation of all certificates associated with that identity or containing that identifier), or
- (U//FOUO) Request the revocation of a user (i.e., revocation of all identities, by naming one), regardless of the domain in which the item was issued or intended to be used.

(U//FOUO) Figure 43 illustrates that the action taken by the PRSN depends on the domain in which the report or request is originated.

**Figure 43. (U) KMI Handling of Compromise Reports and Revocation Requests**




**UNCLASSIFIED//FOUO**

(U//FOUO) If a compromise report or revocation request is received from a Client Node in the Unclassified domain, the Private Zone of the Unclassified enclave takes the following actions:

1. (U//FOUO) For each key compromise report, pass the report to the Unclassified PSN or send the report to the Secret enclave, as appropriate for the key.

2. For each token compromise report, copy the report to Secret enclave for information purposes, and for action in case the token was issued for use in the Secret domain; also, if the token was issued for the Unclassified domain, queue one revocation request for each credential on the token.

3. For each credential revocation request, copy the request to the Secret enclave for information purposes; also, if the credential was issued by an Unclassified PSN, send the request to the PSN.

4. For each identity revocation request, copy the request to Secret enclave; also, queue one revocation request for each Unclassified credential issued for that identity.

5. For each user revocation request, copy request to Secret enclave; also, queue one revocation request for each Unclassified identity that has been registered for the user.

(U//FOUO) If a compromise report or revocation request is received from a Client Node in the Secret domain, the Private Zone of the Secret enclave takes the following actions:

1. For each key compromise report, pass the report to the Secret PSN or notify the cognizant SSO to refile the report through a Client Node in the Unclassified domain (i.e., such reports are not downgraded through an inter-enclave guard), as appropriate for the key.

2. For each token compromise report, if the token was issued in the Secret domain, queue one revocation request for each credential on the token; or else notify the cognizant SSO to refile the report through a Client Node in the Unclassified domain (i.e., such reports are not downgraded through an inter-enclave guard).

3. For each credential revocation request, send request to Secret PSN if credential was issued by Secret PSN; or else notify the cognizant SSO to refile the request through a Client Node in the Unclassified domain (i.e., such reports are not downgraded through an inter-enclave guard).

4. For each identity revocation request, queue one revocation request for each Secret credential issued for that identity; if identity has also been registered in the Unclassified domain, notify the cognizant SSO to refile the request through a Client Node in the Unclassified domain (i.e., such reports are not downgraded through an inter-enclave guard).

5. For each user revocation request, queue one revocation request for each Secret identity that has been registered for the user, and notify the cognizant SSO to refile the request through a Client Node in the Unclassified domain (i.e., such reports are not downgraded an inter-enclave guard).

(U) The stated requirements and capabilities have the following implications:

- (U//FOUO) The CI-2 PRSN needs to replicate token content data from the Unclassified domain to the Secret domain during token and credential issuance processes.

- (U//FOUO) Some delay is tolerable for processing a report or request pertaining to an Unclassified item when the report or request is made on the Secret side of a PRSN.

- (U//FOUO) Additional, unstated processing occurs to maintain a Secret replica of Unclassified databases for identity registration, token registration, outstanding certificates, and other configuration information.

# 7 (U) GLOSSARY OF ACRONYMS

| | |
|---|---|
| (U) **AKP** | Advanced Key Processor |
| (U) **ASWR** | attack sensing, warning, and response |
| (U) **BPS** | boundary protection suite |
| (U) **CA** | (X.509) certification authority |
| (U) **CCEB** | Combined Communications-Electronics Board (referring to Australia, Canada, New Zealand, the United Kingdom, and the U.S.) |
| (U) **CI-2** | Capability Increment 2 |
| (U) **CNSS** | (U.S.) Committee on National Security Systems (formerly NSTISSC) |
| (U) **COTS** | commercial off-the-shelf |
| (U) **CRL** | (X.509) certificate revocation list |
| (U) **CSN** | Central Services Node |
| (U) **DEERS** | (U.S.) Defense Enrollment Eligibility Reporting System |
| (U) **DITSCAP** | DoD Information Technology Security Certification and Accreditation Process [DITSCAP] |
| (U) **DN** | (X.500) Distinguished Name |
| (U) **DoD** | (U.S.) Department of Defense |
| (U) **DoDD** | DoD Directive |
| (U) **DoDI** | DoD Instruction |
| (U) **DRV** | derived from |
| (U) **ECU** | end cryyptographic unit |
| (U) **EDI-PI** | Electronic Data Interchange Person Identifier |
| (U) **EKMS** | Electronic Key Management System |
| (U) **FNBDT** | Future Narrow-Band Data Terminal |
| (U) **FOUO** | For Official Use Only |
| (U) **GOTS** | Government off-the-shelf (i.e., developed under Government auspices) |
| (U) **HAIPE** | High-Assurance Internet Protocol Encryptor |
| (U) **HIDS** | host-based IDS |
| (U) **HTTP** | Hypertext Transfer Protocol |
| (U) **IA** | information assurance |
| (U) **IATF** | Information Assurance Technical Framework |
| (U) **IDS** | intrusion detection system |
| (U) **IEG** | inter-enclave guard |
| (U) **IP** | Internet Protocol |
| (U) **IT** | information technology |
| (U) **IZG** | inter-zone guard |
| (U) **KEK** | key-encryption key |
| (U) **KLIF** | key loading and initialization facility |
| (U) **KME** | Key Management Entity |
| (U) **KMI** | Key Management Infrastructure |
| (U) **KMS** | key management system |
| (U) **KOA** | KMI operating account |
| (U) **KPC** | KMI Protected Channel |
| (U) **KRD** | KMI Requirements Database |
| (U) **MPMSS** | mission planning/management/support system |

| | |
|---|---|
| (U) **NATO** | North Atlantic Treaty Organization |
| (U) **NIDS** | network-based IDS |
| (U) **NIPRNET** | (DoD) Non-Classified Internet Protocol Router Network |
| (U) **NSA** | (U.S.) National Security Agency |
| (U) **NSTISSI** | (U.S.) National Security Telecommunications and Information Systems Security Instruction |
| (U) **NT** | non-technical (see “Requirement Statements” section) |
| (U) **OCSP** | On-Line Certificate Status Protocol |
| (U) **OME** | Ordering and Management Enclave |
| (U) **PDE** | Product Distribution Enclave |
| (U) **PKI** | public-key infrastructure |
| (U) **PRSN** | Primary Services Node |
| (U) **PSN** | Product Source Node |
| (U) **PSTN** | public switched telephone network |
| (U) **RuBAC** | rule-based access control |
| (U) **SIPRNET** | Secret Internet Protocol Router Network |
| (U) **SSL** | Secure Sockets Layer (protocol) |
| (U) **SSO** | system security officer |
| (U) **TCP** | Transmission Control Protocol |
| (U) **TLS** | Transport Layer Security (protocol) |
| (U) **UDP** | User Datagram Protocol |
| (U) **VPN** | virtual private network |

# 8 (U) GLOSSARY OF TERMS

(U//FOUO) This glossary lists the terms for which this volume has DEFINITION statements.

Access Control List. A mechanism that implements access control for a System Resource by enumerating the System Entities that are permitted to access the resource and, either implicitly or explicitly, the access modes granted to each entity.

Access Control Matrix. A rectangular array of cells with one row per subject and one column per object. The entry in a cell indicates the access mode that the subject is permitted to exercise on the object. (Each column is equivalent to an access control list, and each row to a capability list.)

Account Distribution Profile. An approval-based Access Control list for a specific product that (1) names the KOAs to which PRSNs distribute the product and (2) states conditions of distribution (e.g., requires per-edition approval).

Administrative Manager. A Manager that performs housekeeping functions that support the work of operational managers and KOA Agents, but usually do not directly involve KMI products and services.

Attribute certificate. A digital certificate that binds a set of descriptive data items other than a public key—such as Authorizations for an Access Control process—either directly to a subject name or to the identifier of another certificate that is a public-key certificate.

Authorization (or Privilege). A right that is granted to a User or other System Entity to Access a System Resource for a specific purpose.

Boundary Protection Suite (BPS). A Component that (1) is a data communication gateway into a Security Enclave or Security Zone and (2) regulates data communication traffic to and from the enclave or zone.

Capability List. A mechanism that implements access control for a System Entity by enumerating the System Resources that the entity is permitted to access and, either implicitly or explicitly, the access modes granted for each resource.

Capability Token. A token, usually an unforgeable data object, that gives the bearer or holder the right to access a System Resource. Possession of the token is accepted by a system as proof that the holder has been authorized to access the resource that is named or indicated by the token.

Client Node (abbreviated as Client). A set of hardware and software with computing and cryptographic capabilities that enable a registered Human User or User Device to obtain products and services.

Command Authority. Individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges [CNSSI4009].

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 other parts.

Computer Platform. A combination of computer hardware and an operating system (consisting of software, firmware, or both) for that hardware, that supports automated KMI functions.

Constraint. A limitation, implemented by role-based Access Control, on a relationship or function of a User Identity, a Role, or a Permission. (In effect, a constraint is a form of security policy.)

Controlling Authority. Official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet. [CNSSI4009].

Core Nodes. The set of Nodes that includes (1) the CSN, (2) all PSNs, (3) all PRSNs, and (4) all Client Nodes that serve Managers playing Internal Management Roles (see "Management Roles" section).

Device Account RuBAC Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute values, (2) is associated with a User Device Identity in the context of the KOA to which the device is currently assigned, and (3) controls the distribution of products to the device within that KOA.

Device Convenience Label. A non-blank printable text string that is assigned to a User Device, is unique among the User Devices in the KOA to which the device is currently assigned, and can be used by the KOA Managers to assist in identifying and managing the device.

Device Registration RuBAC Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute values, (2) is associated with a User Device Identity, and (3) controls the distribution of products to the device in any KOA to which the device is assigned.

Device Serial Number. A centrally registered, electronically processed identifier that is assigned to a KMI User Device or other information assurance device for the purpose of remote management and is unique across all NSA equipment programs.

Enrollment. The KMI process that assigns a User Identity to a Management Role.

Enrollment Domain. A set of Managers (i.e., a set of assignments of User Identities to Management Roles) that includes (1) one or more Enrollment Managers and (2) any additional Managers of other types that have been placed into the domain.

Enrollment Domain Hierarchy. A subordination relationship among all Enrollment Domains, that is one-to-many and is transitive. (That is, if enrollment domain A is subordinate to domain B, and B is subordinate to C, then A is also subordinate to C. If A is subordinate to B, then B is said to be superior to A.)

External Management Role. A Role that is intended to be performed by a Manager that typically is a member of a KMI customer organization.

Guard. A BPS that (1) connects Components that operate in different Security Domains; (2) is trusted to prevent unauthorized disclosure of data from one domain to the other, if that service is required by the respective security levels of the Components; and (3) is trusted to protect the data integrity and system integrity of each domain against threats actions communicated from the other.

Independent Component. A Component that has a defined security perimeter at which, or within which, the Component is responsible for some set of Security Services.

Internal Management Role. A Role that is intended to be performed by a person who is a member of the central organization that controls the KMI.

Key Management Infrastructure. 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.

KMI Operating Account (KOA). A KMI business relationship that is established to manage (1) the set of User Devices that are under the control of a KMI customer organization and (2) the distribution of KMI products to those devices.

KOA Access Control List. An approval-based Access Control list for a specific KOA, that names the User Identities that are permitted to access PDEs to obtain products that are distributed by that KOA.

KOA Agent. A User Identity of a Human User that is designated by a KOA to access PRSN PDEs for the purpose of retrieving wrapped products that have been requested for User Devices that are assigned to that KOA.

KOA Agents List. The list of all the registered User Identities that are KOA Agents.

KOA Core Data. A subset of the KOA Registration Data that distinguishes a KOA from all other KOAs and relates it to other non-KMI systems and organizations.

KOA Identifier. A name that can be unambiguously represented by a printable, non-blank character string.

KOA Registration Data. The set of data values that is maintained by the KMI for managing a KOA.

Device Distribution Profile. An approval-based Access Control list for a specific product, that (1) names the User Devices in a specific KOA to which PRSNs distribute the product and (2) states conditions of distribution for each device.

Management Role. A Role that has Permissions that enable a Registered User to direct, control, or regulate some set of System Resources.

Manager. A Registered User that directs, controls, or regulates some set of System Resources.

Node. A collection of related Components that is (1) located on one or more Computer Platforms at a single Site.

Operational Manager. A Manager that performs functions directly involving the production of products and services, or that supervises such functions.

Peer System. An information system (other than the EKMS) that is external to the KMI and with which the KMI exchanges products and services that are needed to support KMI operations.

Permission. An positively-stated Authorization for Access that (1) can be associated with one or more Roles and (2) enables a User in a Role to access a specified set of System Resources by causing a specific set of System Actions to be performed on the resources.

Principal. A specific User Identity that is asserted and activated by a Registered User when accessing the system.

Principle of Least Privilege. The practice of granting to each System Entity the minimum Authorizations that the entity needs to do its legitimate work.
Principle of Positive Authorization. The practice of granting Access to System Resources only in a positive way.

Principle of Separation of Duties. The practice of dividing the functions of a system process among different System Entities, to prevent a single entity from subverting the process. (The "Role Separation Constraints" section specifies a general capability for separating roles, and the "Specifically Separated Roles" section identifies some required separations.)

Product Manager. Either a Controlling Authority or a Command Authority.
Resource Object. A specific System Resource that (1) can be accessed by a System Action and (2) can be protected by Access Control services.

Role. A job title in the KMI system that (1) has a specified set of functional responsibilities within the system, (2) can be granted one or more Permissions, and (3) can be assigned to one or more Users.

Role Hierarchy. A subordination relationship, "≤", among Roles, where "A≤B" means that Role A is subordinate to Role B. The relationship is many-to-many and is a partial ordering of the set of all Roles. That is, for any three Roles A, B, and C, the following are always true: (1) A≤A; (2) if A≤B and B≤C, then A≤C; and (3) if A≤B and B≤A, then A and B must be the same Role.
RuBAC Access Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute values, (2) is associated with a Manager, and (3) determines the limits of the Manager's Permissions when accessing Resource Objects.

RuBAC Attribute. A characteristic of a System Entity, where the value of the characteristic is used in making Access Control decisions that enforce data confidentiality.

RuBAC Conferral Set. A set of RuBAC Attribute values that is (1) contained in the set of all KMI RuBAC Attribute Values; (2) is associated with an Enrollment Manager, Device Registration Manager, or KOA Registration Manager; and (3) constrains the attribute values that the Manager can assign.

RuBAC Property. A characteristic of a System Resource object, where the value of the characteristic is used to make Access Control decisions that enforce data confidentiality.

Security Domain. A set of KMI system entities that operate under a common security policy, including operating at the same security level.

Security Enclave. A set of Components that operate in the same Security Domain and share the protection of a common, continuous security perimeter.

Security Zone. A logically contiguous subdivision of a Security Enclave; that is, each Component in a Security Enclave is contained in one of the enclave's Security Zones. Each zone has a well-defined security perimeter, part of which may be formed by the perimeter of the enclave.

Session. A temporary mapping of a Principal to a Role or Roles (especially when a Client Node accesses a PRSN).

Short Title. An identifying combination of letters and numbers assigned to certain COMSEC materials to facilitate handling, accounting, and controlling. [CNSSI4009].

Site. A facility—i.e., a physical space, room, or building together with its physical, personnel, administrative, and other safeguards—in which (1) KMI functions are performed and (2) KMI Components might be housed.

Subsystem. A collection of related Components that together perform or deliver a particular KMI function or service. [KMI2020]

System Action. A specific function or behavior of the KMI that accesses and possibly affects one or more Resource Objects.

System Entity. An active element—i.e., either (1) a person or (2) set of persons, or (3) an automated device or (4) set of devices—that is part of either the KMI or the KMI's environment and that incorporates some specific set of capabilities.

System Resource. Information held in the system, or a service or product provided by the system; or a system capability (e.g., processing power or communication bandwidth); or an item of equipment (i.e., hardware, firmware, software, or documentation); or a facility that houses those things.

Top-Level Enrollment Manager. A KMI job position held by a Human User who has a User Identity that is initialized in the Role of Enrollment Manager as part of the KMI startup process, and is then able to enroll other User Identities in Management Roles. (An Enrollment Manager also has RuBAC management responsibilities, as described in the "Rule-Based Access Control" section.)

Type 1 [cryptographic device]. Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to [cryptographic devices], and not to information, key, services, or controls. Type 1 [cryptographic devices] contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation. [CNSSI4009]

# 9 (U) GLOSSARY OF TERMS

(U) ANSI — American National Standards Institute, *Role Based Access Control*, Secretariat, Information Technology Industry Council, BSR INCITS 359, DRAFT, 10 Nov 2003.

(U) CNSSI4009 — Committee on National Security Systems, *National Information System Security (INFOSEC) Glossary*, CNSS Instruction No. 4009, May 2003.

(U) CNSSI40xx — _____, Safeguarding COMSEC Material in Electronic Form, DRAFT CNSS Instruction 40xx, Rev 5.2, 3 Jul 2003 (or as updated, if there is a later version).

(U) DITSCAP — DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997.

(U) DoDX509CP — ASD C3I, X.509 Certificate Policy for the U.S. Department of Defense, version 5.2, 13 Nov 2000.

(U) DoDD5200.28 — DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), 21 March 1988.

(U) DoDD8500.1 — DoD Directive 8500.1, Information Assurance, 24 October 2002.

(U) DoDI8500.2 — DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 Feb 2003.

(U) EKMS103 — National Security Agency, *Security Policy for the Electronic Key Management System*, EKMS 103A, 22 Jan 1997.

(U) EKMS202 — _____, *Electronic Key Management System Security Requirements*, EKMS 202B, 16 Sep 1998.

(U) Ferraiolo — David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli, *Role-Based Access Control*, Artech House, Norwood, Massachusetts, 2003, ISBN 1-58053-370-1.

(U) FNBDT — [Interoperability specification for *Future Narrow-Band Data Terminal* is TBD]

(U) Gray — Jim Gray and Andreas Reuter, *Transaction Processing: Concepts and Techniques*, Morgan Kaufmann Publishers, Inc., 1993.

(U) HAIPIS — National Security Agency, *Interoperability Specification for High Assurance Internet Protocol Encryptor (HAIPE) Devices*, version 2.0 Charlie, 3 Jan 2003.

(U) IATF — _____, *Information Assurance Technical Framework*, Release 3.1, Sep 2002.

(U) IS15408-2 — Common Criteria Implementation Board, *Common Criteria for Information Technology Security Evaluation*, ver. 2.1, CCIB-98-031, August 1999: Part 2: *Security Functional Requirements*.

(U) KMI1001 — National Security Agency, *A Concept for the KMI*, KMI 1001, 10 Jun 1999.

(U) KMI1011 — _____, *Key Management Infrastructure Roadmap for the Department of Defense*, KMI 1011, DRAFT, 9 Jun 2000.

(U) KMI2020 _____, *Key Management Infrastructure (KMI) Target Architecture System Interface Description*, KMI 2020, DRAFT, 19 Jan 2000.

(U) KMI2200 _____, *System Description and Requirements Specification for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)*, KMI 2200, version 1.26 ("SRS F" plus changes), April 2005, including the following:

(U) KMI2200V1 _____, _____, Volume 1: *Key Management Functions and Related Requirements*, version 1.26 ("SRS F" plus changes), April 2005.

(U) KMI2200V2 _____, _____, Volume 2: *System Security Policy and Related Requirements*, version 1.26 ("SRS F" plus changes), April 2005.

(U) KMI2204 _____, *Threat Assessment Report for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)*, KMI 2204, version 1.0 ("Final Draft"), 30 Jan 2004.

(U) KMI2206 _____, Security Risk Analysis for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2), KMI 2206, DRAFT, 2003.

(U) KMI2211 _____, Glossary for the Key Management Infrastructure (KMI) Program, Capability Increment Two (CI-2), DRAFT.

(U) KMI2212 _____, Concept of Operations for the Key Management Infrastructure (KMI) Capability Increment Two (CI-2), DRAFT version 0.8, 3 Nov 2003.

(U) KMI3001 National Security Agency, *Electronic Serial Number Standard*, DRAFT version 0.71, 24 Oct 2003.

(U) NSAKMICP ———, *X.509 Certificate Policy for U.S. DoD KMI Trustees*, Technical Report, version 1.0, 17 Sep 2003.

(U) NSAKMIRU ———, *KMI Policy for Registration of Users*, [to be provided by the Government].

(U) NSAKMIEM ———, *KMI Policy for Enrollment of Managers*, [to be provided by the Government].

(U) REFTBD1 [TBD: Need to provide reference or explain Unified INFOSEC Criteria.]

(U) REFTBD7 [TBD: Need reference to specifications of KMI Management Token.]

(U) RFC3546 S. Blake-Wilson et al, *Transport Layer Security (TLS) Extensions*, Request for Comments 3546, The Internet Society, June 2003.