TECHNICAL REPORT

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

VOLUME 2: (U) SYSTEM SECURITY POLICY AND RELATED REQUIREMENTS

VERSION 2.2
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

30 September 2005

(This Page Left Blank Intentionally)

KEY MANAGEMENT INFRASTRUCTURE

30 September 2005
Version 2.2
DRAFT

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

Volume 2: (U) System Security Policy and Related Requirements

(U) This document states security policy and specifies related security services and requirements for the Department of Defense Key Management Infrastructure.

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

Not releasable to the Defense Technical Information Center per DoD Instruction 3200.12.

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption 3.

(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 1.4.

Date	Version	Description of Changes
2 Aug 2002	0.00	Working draft established.
18 Oct 2002	0.10	Working draft with updates from various sources.
21 Oct 2002	0.20	Ready for delivery as First Draft per TTO schedule.
3 Dec 2002	0.40	Ready for delivery as Second Draft.
14 Jan 2003	0.41	Issued to transfer requirements to KMI 2200.
21 Jan 2003	0.50	First "near-final" version to begin review/approval/signout.
24 Mar 2003	0.54	"Final Draft" for requirements scrub and approval review.
5 Jun 2003	0.60	Updated for DoDD 8500.1 / DoDI 8500.2 IA controls.
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". Released non-draft 4/12/05
15 Apr 2005	2.0	Updated draft for community release.
7 Jul 2005	2.1	Updated draft for community release, incorporates 12 change proposals approved since April release.
30 Sept 2005	2.2	Updated draft for community release; 3-volume SDRS incorporates 13 change proposals approved since July release. Blue text indicates changes since version 2.1.

FOR OFFICIAL USE ONLY

(U) TABLE OF CONTENTS

(U) TABLE OF FIGURES

(U) TABLE OF TABLES

1 (U) INTRODUCTION

(U//FOUO) This document is Volume 2 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 (KMI). All parts—computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine—that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users.

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. The policies stated in this volume are intended to apply not only to Capability Increment 2 (CI-2), but also to later CIs and to the resulting long-term, target KMI.

(U//FOUO) This volume states overall security objectives, states policies for achieving the objectives, and states related security requirements that apply broadly to system components. However, the policies and requirements stated here are intended to be independent of all but the most basic and necessary architectural concepts. Although the policies and requirements provide a framework for design, implementation, and operation, they are not intended to imply either security mechanisms to be implemented or strength of mechanisms, except where those are specifically mentioned.

1.2 (U) KMI Security Objectives

(U//FOUO) The basic security objectives of the KMI are 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 against denial of service to authorized users.

- (U//FOUO) **System Integrity.** Protect all system elements to ensure their continued and correct operation.

- (U//FOUO) **User Authentication.** Verify the identities of system entities before permitting them to access system resources.

- (U//FOUO) **User Accountability.** Enable 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 managers to (1) configure KMI security characteristics, (2) ensure that the system meets applicable portions of this *Policy*, and (3) enable interoperation with the EKMS and external systems. (See "Relationship to Existing Key Management Systems and External Support Systems" section of Volume 1.)

DEFINITION (U//FOUO) External System. An information system (other than the EKMS) separate from the KMI, to which the KMI sends requests for data needed to support KMI operations, and from which the KMI receives requested data.

1.3 (U) Terminology and Capitalization

(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 3, 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 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 site facility that houses these things.

DEFINITION (U//FOUO) Component. A set of System Resources that (1) forms a physical or logical part of the system, (2) has specified functions and interfaces, and (3) is treated, by policies or requirement statements, as existing independently of the other parts.

(U//FOUO) In this document, the interpretation of the term "component" depends on the context. The term is used at more than one level of abstraction, and components may be nested.

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.

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 system functions.

1.4 (U) Office of Primary Responsibility

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

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

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

1.5 (U) Affected Organizations

(U//FOUO) Policies stated here apply to the entire KMI and require compliance by organizations and programs that develop, acquire, transport, install, test, operate, use, maintain, or dispose of KMI equipment, information, and other resources, and to facilities that house and support these activities. The affected organizations include the following:

- (U//FOUO) **Department of Defense (DoD).** The Office of the Secretary of Defense, the Military Departments, the Office of Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organization entities within DoD.

- (U//FOUO) **Other organizations.** Organizations authorized to use the KMI or exchange information with it, such as Federal civilian agencies; U.S. state and local government agencies; U.S. Allies as obligated by international agreements; other foreign governments; and commercial, public, or private organizations engaged in official or approved activities.

- (U//FOUO) **DoD contractors.** Contractors involved with KMI implementation, operation, use, and maintenance activities.

1.6 (U) Requirement Statements

(U) Requirement statements in this volume have a label of the form “**CI2-SEC-1.2.3a**”, where “**SEC**” identifies the requirement as a security policy 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 Policies and Requirements

(U) The key words **must**, **must not**, **should**, **should not**, **may**, and **optional** are to be interpreted as follows when they appear in a policy statement (i.e., a statement with the prefix "**POLICY**"):

- (U) **Must.** This word means that the statement is an absolute mandate.

- (U) **Must not.** This phrase means that the statement is an absolute prohibition.

- (U) **Should.** This word means that there may exist valid reasons in particular circumstances to ignore the statement, but the full implications must be understood and carefully weighed before choosing a different course.

- (U) **Should not.** This phrase means that there may exist valid reasons in particular circumstances to implement or accept the behavior described in the statement, but the full implications must first be understood and carefully weighed.

- (U) **May** or **Optional.** These words means that compliance with the statement is optional.

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

- (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. System-Wide Security Policies.** States KMI-wide policies that derive from DoD-wide policies, including establishing a policy basis for certification and accreditation of the KMI.
- (U) **3. Security Service Policies.** States policies and associated requirements for security services to be provided throughout the KMI.
- (U) **4. Functional Area Security Policies.** States policies and associated requirements for security services to be provided in some specific functional areas of the KMI.
- (U) **5. Security Implementation Policies.** States policies and associated requirements for security disciplines that are used to implement the services specified by Sections 3 and 4.
- (U) **6. Glossary of Acronyms**. (See additional definitions of terms in [KMI2211]).
- (U) **7. Glossary of Terms**. Terms for which this volume has DEFINITION statements.
- (U) **8. References**.
- (U) **Appendix A**. **Identity and Eligibility Proofing for Users**. Invites discussion of how to specify the documentation required as evidence.
- (U) **Appendix B**. **Accountability with Shared Identities**. Discusses ways to design authentication procedures to enable a user to access the KMI in a shared identity

(This Page Left Blank Intentionally)

2. (U) SYSTEM-WIDE SECURITY POLICIES

(U//FOUO) This section states KMI-wide policies that derive from DoD-wide security policies.

2.1 (U) Information Assurance Controls

POLICY (U) **General Policy on Information Assurance.** The KMI must meet the requirements of DoD Directive 8500.1, *Information Assurance* [DoDD8500.1].

(U//FOUO) DoD Directive 8500.1 is primary among those dealing with security features and assurances of information systems. The directive is supplemented by the following instruction:

- (U) DoD Instruction 8500.2, *Information Assurance (IA) Implementation* [DoDI8500.2].

(U//FOUO) Enclosure 4 of the instruction specifies protection for each DoD information system according to (1) the system's mission assurance category (MAC) and (2) the system's confidentiality level. On each of those two dimensions, the instruction defines three levels. The combinations of mission assurance category and confidentiality level establish nine baseline IA levels. For each level, the instruction specifies a set of IA controls. Each control is an "objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Control are assignable and thus accountable." [DoDI8500.2]

(U//FOUO) This volume and Volume 3 quote all of the controls, including both those that are applicable to the KMI and those that are not. Each control is presented with its original alphanumeric label and title and, in parentheses, the security service that DoDI 8500.2 intends the control to support, as shown in the following example:

> **CONTROL** (U//FOUO) **ECWM-1 Warning Message (Confidentiality)**. "All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing." [DoDI8500.2]

(U//FOUO) A control that is expected to be implemented by non-technical means has the notation "[NT]" immediately following its label. Otherwise, this *Specification* includes requirement statements to implement the control if it is applicable.

2.1.1 (U) Security Architecture

POLICY (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 incorporate the defense-in-depth security principles of the *Information Assurance Technical Framework* (IATF) [IATF].

(U//FOUO) Defense in depth is the "DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among [information technology] assets; and the selection of IA solutions based on their relative level of robustness." [DoDD8500.1] The IATF adopts defense in depth as the fundamental strategy for protecting computer systems and their interconnecting networks, and the DoD has adopted the IATF as "a common reference guide for selecting and applying adequate and appropriate IA and IA-enabled technology in accordance with the architectural principles of defense in depth." [DoDI8500.2]

> **CI2-SEC-2.1.1a** (U//FOUO) The KMI shall conform to the security architecture specified in *System Security Architecture and Related Requirements for KMI CI-2* [KMI2200V3]. [DRV KRD 2122] {Z}

(U//FOUO) The *Security Architecture* achieves defense in depth in several ways. It specifies role-based, rule-based, and approval-based access controls for authorizations that are assigned to functional roles played by users; it allocates security functions to system nodes and their components; and it specifies how the nodes and their components are contained within sets of nested security perimeters.

2.1.1.1 (U) User Roles

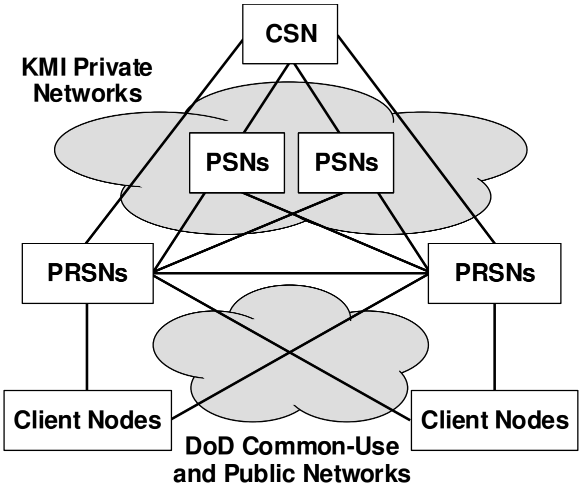
(U//FOUO) The roles played by users in the KMI are specified in Volume 1 and also listed in Volume 3. This section only describes the main types of roles. Registered identities of human users may be assigned to a non-management role or to management roles. The management roles have special authorizations that enable managers to direct, control, or regulate some set of system resources and thus operate or administer the KMI.

(U//FOUO) KMI management roles can be categorized as internal or external. Internal management roles are performed by people who are members of the central organization that controls the KMI. External management roles are performed by people that typically are members of KMI customer organizations. KMI management roles also can be categorized as operational or administrative. Operational management roles directly involve the ordering and distribution of products and services or supervise those functions. Administrative management roles do not directly involve products and services, but these roles involve housekeeping tasks that need to be done to support operational managers and other authorized users.

2.1.1.2 (U) Functional Nodes

(U//FOUO) Figure 1 illustrates that the KMI includes four basic types of nodes: Client Nodes, Primary Services Nodes (PRSNs), Product Source Nodes (PSNs), and the Central Services Node (CSN). KMI is a client-server system in which users employ client nodes to communicate across Government and public common-use networks and access centralized and regional server complexes composed of PRSNs, PSNs, and the CSN.

Figure 1. (U) KMI Nodal Architecture



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

PRODUCT SOURCE NODES (PSNs)
Cryptographic material generation.
Product packaging. Product vault.
Rekey. Conversion of seed key.

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

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

UNCLASSIFIED//FOUO

DEFINITION (U//FOUO) Node. A collection of related Components that is 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.

DEFINITION (U//FOUO) Client Node – The most general, abstract and high level way to refer to any version of a KMI component that will allow KMI Human users to communicate over a network to a PRSN and/or perform localized KMI functions.

(U//FOUO) Client Nodes enable users to request and use 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.

DEFINITION (U//FOUO) Client Host – The key management computing platform, with multiple configurations, that either connects to an AKP to form the KMI equivalent of an LMD/KP or operates without an AKP to provide reduced access to KMI services.

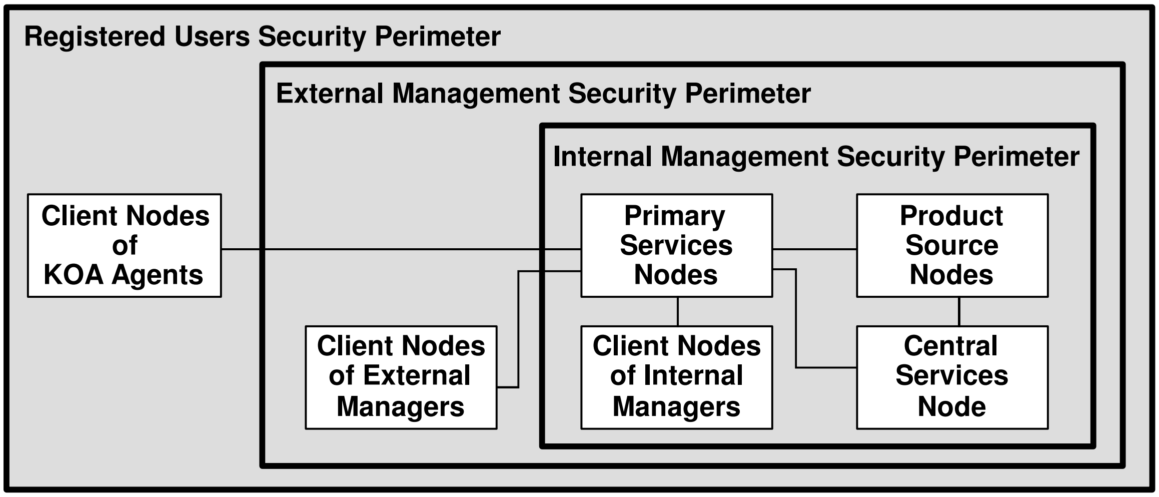
DEFINITION (U//FOUO) Management Client (MGC) – The specific configuration of a Client Host which operates in conjunction with an AKP to perform management of products and services for the KMI – KMI equivalent of an LMD/KP.

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

2.1.1.3 (U) Security Perimeters

(U//FOUO) The CI-2 security architecture is based on a layered series of security perimeters that enclose components that require protection. Figure 2 illustrates the two main, outer perimeters. The core nodes, including the client nodes for internal managers, are contained in the Internal Management Security Perimeter and are subject to essentially all of the protections that are specified in this volume. Outside that perimeter, but inside the External Management Security Perimeter, there are clients that serve the slightly less powerful, external management roles. Outside that perimeter, but inside the Registered Users Security Perimeter, there are clients that serve the single non-management role called KOA Agent (see "KMI Operating Accounts" section in Volume 3). Some of the nodes that serve KOA Agents are treated as being part of mission systems of the organizations that operate the nodes, and such nodes are subject to the protection requirements of those systems. However, an organization that operates such a node must still protect the node in accordance with KMI policy and architecture.

Figure 2. (U) KMI Security Perimeters


Registered Users Security Perimeter
External Management Security Perimeter
Internal Management Security Perimeter
Client Nodes of KOA Agents
Primary Services Nodes
Product Source Nodes
Client Nodes of External Managers
Client Nodes of Internal Managers
Central Services Node

UNCLASSIFIED//FOUO

(U//FOUO) CI-2 separates components that perform different functions and that serve different security domains. The separation is achieved through definition of (1) modular security enclaves that lie inside the domains and (2) modular security zones that are subdivisions of the enclaves.

DEFINITION (U//FOUO) Security Domain. A set of System Entities and System Resources that operate under a common security policy, including operating at the same security level. [KMI2200V3]

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. [KMI2200V3]

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. [KMI2200V3]

(U//FOUO) Descriptions and specifications of the various nodes, domains, enclaves, and zones for CI-2 are provided in Volume 3.

2.1.2 (U) Mission Assurance Categories

POLICY (U//FOUO) **General Policy on Mission Assurance Categories.** Core Nodes shall comply with DoD Instruction 5200.2 [DoDI8500.2] by (1) implementing the IA controls for Mission Assurance Category (MAC) II at a minimum and (2) implementing the controls for MAC I where practicable.

(U//FOUO) Systems in MAC I require high integrity and high availability; systems in MAC II require high integrity and medium availability; and systems in MAC III require basic integrity and availability.

(U) Mission assurance category. "Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity." [DoDI8500.2]

(U) Mission Assurance Category I (MAC I). "Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures." [DoDI8500.2]

(U) Mission Assurance Category II (MAC II). "Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance." [DoDI8500.2]

> (U) Mission Assurance Category III (MAC III). "Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices." [DoDI8500.2]

(U//FOUO) Enclosure 4 of [DoDI8500.2] states the same number of IA controls for both MAC I and MAC II; each have 32 controls for integrity and 38 for availability. All but six of the controls (CODB, COPS, COSP, VIIR, CODP, COED) are identical for both categories. All controls for both categories have been included in this *Specification*, and the six differences are noted in appropriate sections.

(U//FOUO) In CI-2, functions of core nodes require a high level of system integrity and, therefore, many if not all independent components of Core Nodes need to be treated as being in either MAC I or MAC II.

> **CI2-SEC-2.1.2a** (U//FOUO) For each Independent Component of a Core Node, the KMI system design shall specify a mission assurance category defined by DoD Instruction 8500.2, *Information Assurance (IA) Implementation* [DoDI8500.2]. [KRD NEW] {Z}

(U//FOUO) However, not all client nodes need the highest levels of assurance; some clients are expected to be assigned to MAC I, others to MAC II, and possibly still others to MAC III.

> **CI2-SEC-2.1.2b** (U//FOUO) The KMI shall be able to support concurrent Access by Users through Client Nodes that operate in all three of the mission assurance categories defined by DoD Instruction 8500.2, *Information Assurance (IA) Implementation* [DoDI8500.2], but where each Client Node is in just one category. [KRD NEW] {R}

2.1.3 (U) Confidentiality Levels

POLICY (U//FOUO) **General Policy on Confidentiality Levels.** Components of Core Nodes shall implement the IA controls defined by [DoD8500.2] for the "Sensitive" Confidentiality Level at a minimum, and shall implement the controls for the "Classified" Confidentiality Level where applicable.

(U//FOUO) Confidentiality levels are determined by whether a system processes (1) classified, (2) sensitive, or (3) public information.

> (U) Confidentiality Level. "Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless)." [DoDI8500.2]

(U//FOUO) All core nodes are assumed to process sensitive information, and some also process classified information. Depending on how the definitions of the confidentiality levels are interpreted for KMI, some DOCs might be said to process only public information.

> **CI2-SEC-2.1.3a** (U//FOUO) The KMI shall be able to support Client Nodes at each of the three confidentiality levels defined by DoD Instruction 8500.2, *Information Assurance (IA) Implementation* [DoDI8500.2]. [KRD NEW] {R}

(U//FOUO) Enclosure 4 of DoD Instruction 8500.2 states 45 confidentiality IA Controls for classified systems, and lists 34 confidentiality IA Controls for sensitive systems. All controls for both levels have been included in either this volume or Volume 3, and the differences between the controls for classified versus sensitive systems are noted in appropriate sections.

2.2 (U) Certification and Accreditation

(U//FOUO) To ensure that the KMI operates with an acceptable level of risk, this *Policy* imposes a certification and accreditation process. An accreditation is a formal declaration by a system's Designated Approving Authority (DAA) that the system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is normally preceded by and based on a certification, a technical evaluation of the system's security features and safeguards, usually including testing, that establishes the extent to which a system's design and implementation meet specified security requirements.

POLICY (U//FOUO) **General Policy on Accreditation.** Before KMI CI-2 begins operation, it must gain approval to operate through a formal process that satisfies the *DoD Information Technology Security Certification and Accreditation Process* [DITSCAP]. [DRV KRD 2037]

(U//FOUO) DoD Instruction 5200.40 specifies the DITSCAP as the DoD's standard process for identifying information security requirements, providing security solutions, managing information system security activities, and certifying and accrediting both classified and unclassified systems. The *System Security Authorization Agreement* (SSAA) is the document used to support certification under the DITSCAP.

POLICY (U//FOUO) **General Policy on Certification.** Before KMI CI-2 is accredited for operational use, its security safeguards must be certified as having satisfied applicable requirements.

(U//FOUO) The following subsections outline a technical and management structure for certification and accreditation of the KMI within the DITSCAP framework.

2.2.1 (U) Site-Level and System-Level Accreditation

POLICY (U//FOUO) **Site-Level Accreditation.** Each of the sites that together comprise the KMI must be individually certified and accredited to operate.

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 system functions are performed.

POLICY(U//FOUO) **System-Level Accreditation.** The KMI system as a whole must be accredited to operate, where the system-level accreditation is based, at least in part, on the set of equipment type certification actions and Site-level accreditation actions.

(U//FOUO) The KMI is a computer network. For purposes of accreditation, a network can be treated as either an interconnection of accredited systems (which themselves may be networks) or as a unified whole. Each approach has advantages, and this *Policy* treats the KMI both as a unified system and as a collection of separate sites.

2.2.2 (U) Accreditation Authorities

(U//FOUO) The Director of NSA appoints a DAA to act as one of the system-level accreditors of the KMI and to be responsible for accreditation of KMI sites operated by the NSA. Additional system-level DAAs are appointed by other DoD organizations that have a major role in the operation of the KMI and the systems with which the KMI interoperates. The system-level DAAs are collectively responsible for accrediting the KMI as a whole, and they approve KMI security standards and provide the authority to ensure enforcement of those standards.

POLICY (U//FOUO) **System-Level Accreditation Authority.** The KMI system-level DAAs must have collective authority to deny or discontinue KMI access by any Site that unacceptably increases risk to any other Site.

(U//FOUO) Various organizations appoint certifying officials for equipment types and DAAs for sites, but the system-level DAAs are collectively responsible for ensuring that all certifying officials and site DAAs are properly qualified. All certifying officials and DAAs need to be responsive to the issue of community-wide risk.

(U//FOUO) Accreditation of a KMI site is a collective responsibility of the system-level DAAs and the organization that operates and maintains the site. Site DAAs are expected to be appointed at organizational levels appropriate to their management environment.

POLICY (U//FOUO) **Site-Level Accreditation Authority.** Each Site DAA must have authority to deny or discontinue KMI access by a User of that Site if the User unacceptably increases risk to any other Site or User.

2.2.3 (U) Certification and Accreditation Processes

POLICY (U//FOUO) **Certification and Accreditation Processes:** Certification and accreditation processes at both the KMI system level and the Site level must be collectively approved by the system-level DAAs.

(U//FOUO) The KMI CI-2 SSAA is expected to provide detailed information concerning KMI certification and accreditation processes and set standards and procedures (primarily based on the

DoD-wide policies) for site-level certification activities and accreditation actions. In each capability increment, these actions are expected to take place on an on-going basis as the system is deployed. For system-level accreditation, the SSAA is expected to state criteria by which (1) an initial KMI operating configuration consisting of some subset of individually accredited sites receives system-level accreditation and (2) the accreditation is maintained as other sites are added to the configuration or are removed from it. A system-level accreditation action is expected prior to beginning operation of CI-2, and again when each subsequent capability increment is fielded.

> **CONTROL** [NT] (U//FOUO) **DCSD-1 IA Documentation (Availability)**. "All appointments to required IA roles (e.g., [Designated Approving Authority] and [Information Assurance Manager]/[Information Assurance Officer]) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and [Information Technology]-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response)." [DoDI8500.2]

> **CONTROL** [NT] (U//FOUO) **DCIT-1 IA for IT Services (Integrity)**. "Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities." [DoDI8500.2]

> **CONTROL** [NT] (U//FOUO) **DCDS-1 Dedicated IA Services (Integrity)**. "Acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD [Service or Agency] CIO." [DoDI8500.2]

(U//FOUO) The "outsourcing" parts of the DCIT-1 and DCDS-1 controls do not apply to CI-2 because this *System Description and Requirements Specification* [KMI2200] does not incorporate any outsourced components.

> **CONTROL** [NT] (U//FOUO) **VIVM-1 Vulnerability Management (Availability)**."A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities." [DoDI8500.2]

> **CONTROL** [NT] (U//FOUO) **DCAR-1 Procedural Review (Availability)**. "An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations." [DoDI8500.2]

2.2.4 (U) Type Certification

POLICY (U//FOUO) **Certification of Equipment Types.** KMI equipment elements or assemblies, categorized by type—i.e., grouped by similar functional characteristics and environmental assumptions—must be certified in accordance with specific security requirements appropriate for each type, independent of the Site in which equipment is installed.

> **DEFINITION** (U//FOUO) Equipment Type. A item of standalone equipment—or an assembly of such items intended to be installed and operated as a unit—of which one or more essentially identical replicas are installed in various facilities of the system.

(U//FOUO) This *Policy* applies to all equipment items—hardware, firmware, software, and combinations thereof—that perform a KMI function, and to equipment documentation. However, equipment types differ in functional characteristics and environmental needs and are subject to different technical and administrative requirements.

POLICY (U//FOUO) **Type Certification Process.** Certification of a KMI equipment type must be performed using either (1) a specific organization's implementation of the NISCAP or DITSCAP or (2) an equivalent process that has been approved by the KMI system-level DAAs.

2.2.5 (U) Site Accreditation

POLICY (U//FOUO) **Accreditation of DoD and Intelligence Community KMI Sites.** Accreditation of a Site must be performed using the DITSCAP or or an equivalent process, as approved in a memorandum of agreement between the system-level DAAs and the Site's DAA.

(U//FOUO) When DoD organizations use the DITSCAP or an equivalent, KMI-approved process, and follow the guidance of this *Policy* and the *Certification and Accreditation Plan for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)*, then all DoD KMI sites can be expected to receive equivalent levels of protection. However, site-level DAAs will accredit according to the regulations of their local operational and organizational environment. Also, individual sites differ in specific functional and environmental characteristics and consequently are subject to different technical and administrative requirements.

POLICY (U//FOUO) **Accreditation of Non-DoD KMI Sites.** Accreditation of a Site operated or controlled by a non-DoD organization must be performed through a process that (1) considers the Site's mission, environment, and architecture while assessing the impact of operation of that Site on the KMI as a whole and (2) is approved in a memorandum of agreement between the KMI system-level DAAs and the Site's DAA.

(U//FOUO) The community of KMI users is broader than just the DoD, and this *Policy* provides for cases where KMI sites are accredited according to rules other than the DITSCAP. For example, a non-DoD U.S. Government organization may be authorized to register KMI users at its own site. In that case, even if the Government organization that operates the site accredits it using equivalent local procedures rather than DoD procedures, the site is still subject to the direct policy authority of the U.S. Government. However, there might also be cases where the U.S. Government does not control the site.

2.2.6 (U) Non-KMI Systems

POLICY (U//FOUO) **Interconnection with Non-KMI Systems.** All interconnections of the KMI with other (i.e., non-KMI) systems must comply with the requirements of DoD Directive 8500.1, *Information Assurance* [DoDD8500.1], to ensure that the security of the KMI is not undermined by vulnerabilities of the connected systems.

(U//FOUO) The KMI interoperates with non-KMI systems. For example, to deliver cryptographic products and services electronically, the KMI connects (as described in the "Nodal Structures" section of the Volume 3) to DoD common-use communication networks that have their own connection approval criteria. In that case, this *Policy* cannot mandate accreditation requirements for the non-KMI system, but the interconnection needs to be documented, reviewed, and approved in the following cases:

- (U//FOUO) **DoD systems at the same level**. Interconnections with DoD systems at the same classification level need to be managed to minimize community risk.

- (U//FOUO) **DoD systems at different levels**. Interconnections with DoD systems at a different classification level need to be consistent with the Secret and Below Interoperability (SABI) process [ASDC3I97] using criteria approved by the DoD CIO and, where appropriate, formally coordinated with the Intelligence Community CIO.

- (U//FOUO) **Non-DoD systems**. Interconnections with non-DoD systems, including Intelligence Community and foreign systems, need to be in accordance with approved DoD criteria and be coordinated with the Intelligence Community CIO, as appropriate.

(U//FOUO) The following control and requirements address these interconnections:

CONTROL [NT] (U//FOUO) **EBCR-1 Connection Rules (Availability)**. "The DoD information system [i.e., the KMI] is compliant with established DoD connection rules and approval processes." [DoDI8500.2]

CI2-SEC-2.2.6a [NT] When a Site connects to and interoperates with a non-KMI information system, the reciprocal security safeguards to be implemented and the criteria by which the interconnection is approved to operate shall be documented in a memorandum of agreement between the KMI system-level DAAs and the other system's DAA before the connection is made. [KRD NEW] {C-P-R-S-T}

CI2-SEC-2.2.6b (U//FOUO) The KMI shall implement technical and procedural controls on interoperation with non-KMI systems, to ensure that Users can identify and limit interoperation to only systems that are authorized by DoD policy and have mechanisms that provide levels of security evaluated as adequate for KMI interoperation. [DRV KRD 0832] {C-P-R-S-T}

CONTROL [NT] (U//FOUO) **DCID-1 Interconnection Documentation (Integrity)**. "For AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. For enclaves, a list of all hosted AIS applications, interconnected

> outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements." [DoDI8500.2]

(U//FOUO) The "outsourced IT-based processes" part of the DCID-1 control does not apply to CI-2 because the *System Description and Requirements Specification* [KMI2200] does not incorporate any outsourced components.

(U//FOUO) See the "External Databases" section of this volume for additional policy and requirements that apply when the KMI depends on external databases as authoritative sources or repositories of KMI information.

(U//FOUO) See the "Extend Trust and Outside Users" section of this volume for additional policy and requirements that apply when the KMI interacts with non-KMI key management systems and with KMI users that are outside the policy authority of the KMI.

2.3 (U) Security Environment

(U//FOUO) KMI site accreditation decisions take into account a number of factors that affect the level of risk at the site. Among those factors are the following:

2.3.1 (U) Threat Assessment

(U//FOUO) The KMI's general threat environment is described in KMI 2204, *Threat Assessment for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)*, [KMI2204]. Other documented threat assessments may also apply.

2.3.2 (U) Information Sensitivity

(U//FOUO) The KMI handles both externally provided information and internally generated information:

- (U//FOUO) **Externally generated information.**
  - (U//FOUO) Information provided to the KMI by registered users. This mainly consists of registration data, product ordering data, and product distribution instructions.
  - (U//FOUO) Information provided to the KMI by other system entities. This includes data from external directories and repositories.

- (U//FOUO) **Internally generated information.**
  - (U//FOUO) Information provided by the KMI to registered users. This mainly consists of products and supporting documentation and reports.
  - (U//FOUO) Information maintained by the KMI for it's own internal use. This mainly consists of inventory, tracking, and controlling data.

(U//FOUO) The type and strength of protection needed for an information item depends on the information's sensitivity, i.e., the degree to which disclosure, alteration, destruction, or loss of the information would adversely affect the mission or other interests or business of the information's owner and users.

POLICY (U//FOUO) **General Policy on Protection of Externally Generated Information.** Information provided to the KMI by Users and other System Entities must be protected so as to satisfy both the protection requirements of the providers and also any requirements imposed by Managers in accordance with the KMI security architecture and applicable policies.

(U//FOUO) The KMI needs to know the sensitivity level of any data accepted from an outside source and, where applicable, must be authorized by the data owner's before handling the data.

CI2-SEC-2.3.2a [NT] (U//FOUO) The KMI shall ascertain the protection requirements of the information owner when the KMI accepts information from an external source. [DRV KRD 0969, 1779] {P-R-S}

(U//FOUO) Information provided by external entities, including ordering information and distribution instructions, is usually unclassified, but some might need to be classified. However, the components of the CSN and PRSNs that are specified in Volume 3 operate at no higher security level than U.S. Secret.

CI2-SEC-2.3.2b [NT] (U//FOUO) The KMI shall not accept externally generated, plaintext information that is classified higher than U.S.-Secret (i.e., any externally generated key management information that is classified higher than U.S.-Secret needs to be handled by means other than the Components that are specified in the *Security Architecture and Related Requirements for KMI CI-2* [KMI2200V3].) [KRD NEW] {P-R-S}

(U//FOUO) External providers usually request only that the KMI protect their information against disclosure. In many cases, however, the KMI has its own requirements for protecting that information against disclosure, modification, destruction, or loss when the information is processed and stored in the KMI. Therefore, other policies and associated requirements for protecting externally generated information are stated in the "Security Services" and "Security Implementation" sections of this volume, and in the other volumes of this *Specification*.

POLICY (U//FOUO) **General Policy on Protection of Internally Generated Information.** Information that is generated by the KMI to give to Users, or to be maintained for internal use, must be protected as determined by Managers in accordance with the KMI security architecture and applicable policies.

(U//FOUO) Material that is generated, managed, or accounted for through the KMI ranges in classification from Unclassified through Top Secret. Internally generated information includes COMSEC material:

DEFINITION (U//FOUO) COMSEC Material. "Item(s) designed to secure or authenticate information. COMSEC material includes, but is not limited to: key, products, equipment, modules, devices, documents, hardware, firmware, or software that embodies or describes cryptographic logic, and other items that perform COMSEC functions." [NSTISSI4005F]

(U//FOUO) "Keying material and COMSEC software encrypted via NSA approved means, are considered UNCLASSIFIED//FOUO unless the systems security doctrine directs otherwise." [NSTISSI4005F] Therefore, products are encrypted before storage or distribution.

CI2-SEC-2.3.2c (U//FOUO) The KMI shall encrypt COMSEC material that it generates in electronic form, as soon after generation as is practical, and before storage in the KMI or distribution to Registered Users. [DRV KRD 0563, 1088, 1089] {A-P}

3. (U) SECURITY SERVICE POLICIES

(U//FOUO) This section states policies and requirements for security services provided throughout the KMI. These policies and requirements are intended to operate in concert with those stated in Sections 4 and 5 to establish an integrated security infrastructure.

POLICY (U//FOUO) **General Policy on Security Services.** Components of the KMI system must provide security services to System Resources to maintain levels of information confidentiality and integrity, and product and service availability, commensurate with each Component's mission assurance category, information sensitivity, and need to interoperate with other Components, other systems, and System Entities. [DoDD8500.1]

> **DEFINITION** (U//FOUO) Security Service. A processing or communication service that is provided by a system to give a specific kind of protection to System Resources [RFC2828].

This section defines each security service independently of underlying security mechanisms, states the purpose or objective of the service, states policies and requirements to ensure that the objectives are achieved, and states capabilities needed to manage the service.

3.1 (U) Registered Users

(U//FOUO) This *Policy* defines the types of system entities that are permitted to access KMI system resources. The KMI provides its products, services, and other resources to authorized users, and does not intentionally provide any of its resources to other entities. Although the KMI cannot prevent unauthorized entities in its environment from attempting to access its resources, the KMI blocks such unauthorized access as much as possible. All authorized users must first be registered in the KMI before they can receive products or services from the system.

> **DEFINITION** (U//FOUO) Registered User (abbreviated as User). A System Entity that is authorized to receive KMI's products and services or otherwise access System Resources.

(U//FOUO) CI-2 recognizes three types of registered users:

> **DEFINITION** (U//FOUO) Human User. A human being that is registered as a User.

> **DEFINITION** (U//FOUO) User Device. A cryptographic device—a specific hardware unit with specific firmware or software running on it—that is registered as a User.

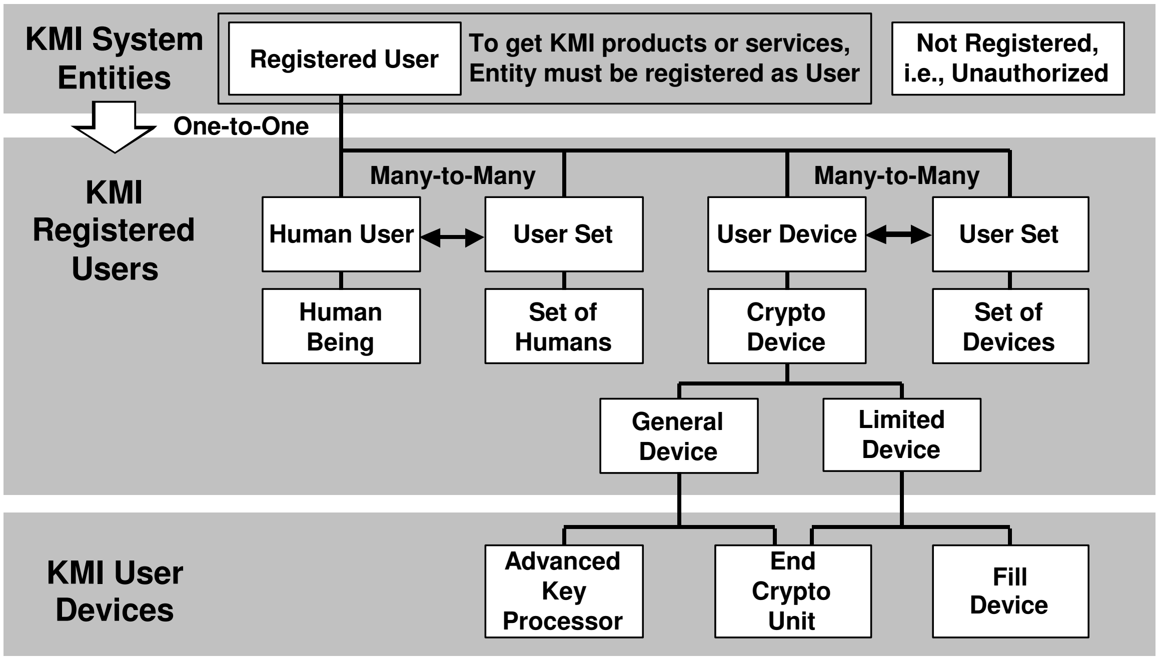
> **DEFINITION** (U//FOUO) User Set. A set that consists either (1) entirely of Human Users or (2) entirely of User Devices, and is registered to act as a single User. (KMI prohibits mixed sets of persons and processes, because such situations might cause security policies and related requirements to be interpreted in conflicting ways.)

3.1.1 (U) Human Users

(U//FOUO) A human user may be assigned to one or more roles that are defined in KMI's role-based access control system. The permissions associated with a role determine the system resources that the KMI permits the user to access when playing that role. (See "Access Control

Service" section of this volume, and also see "Access Control Processes" section of Volume 3.) Figure 3 illustrates that a human user may belong to one or more user sets, and a user set may contain one or more human users.

Figure 3. (U) KMI Registered Users



UNCLASSIFIED//FOUO

3.1.2 (U) User Devices

(U//FOUO) Figure 3 also illustrates that, like a human user, a user device may belong to more than one user set, and a user set may contain more than one user device. However, user devices are not assigned to roles; instead, the products and services that the KMI provides to a user device depends on the device's characteristics, including its basic functional type and its registration type.

(U//FOUO) CI-2 provides products and services to three basic functional types of user devices:

- **DEFINITION** (U//FOUO) End Cryptographic Unit (ECU). A device that (1) performs cryptographic functions, (2) may be part of a larger system for which the device provides security services, and (3), from the viewpoint of a supporting security infrastructure such as the KMI, is the lowest identifiable component with which a management transaction can be conducted [NSAECU].

- **DEFINITION** (U//FOUO) Advanced Key Processor (AKP). A cryptographic device that provides key processing capabilities for an MGC and is configurable to include a mission-appropriate subset of the following functions: key generation, wrapping, unwrapping, and storage; digital signature creation and verification; and interactions with Fill Devices.

- **DEFINITION** (U//FOUO) Fill Device. A COMSEC device used to transfer or store key in electronic form or to insert key into a crypto-equipment [CNSSI4009] (including into ECUs as defined in this section).

(U//FOUO) Figure 3 illustrates that CI-2 supports two forms of device identity, which differ in how widely their registration is known:

DEFINITION (U//FOUO) Limited Device. A User Device that has a User Identity 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.

(U//FOUO) A limited user device is known only locally; its registration information is held only by one, locally managed Client Node. Products destined for that device may be either locally or centrally generated, but to be delivered to the device, they need to wrapped by that local Client Node's AKP.

(U//FOUO) A User Device could need to be supported locally by two or more KOAs. In that case, the device could be separately registered as a Local Device in each of those KOAs (i.e., be registered at the respective management Client Node of each of the KOA's) and thus have two or more identities that have only local significance. (See "User Identities" section of this volume.)

DEFINITION (U//FOUO) General Device. A User Device that has a User Identity for which the registration has significance across the entire KMI (i.e., it is registered at a PRSN) and for which a product can be generated and wrapped by a PSN for distribution to that specific device. (Volume 1 uses the synonym KMI-Aware Device.)

(U//FOUO) A general user device is known globally in the KMI; its registration information is centrally managed by the PRSNs. However, the KOA to which a general device is currently assigned can also treat the device as though it were a limited device. When a general device is assigned or transferred to a KOA (see "KOA Device Assignment" section of Volume 3), that action also effectively registers the device as a local device at the Client Node that supports the KOA, so that the client can distribute locally wrapped products to the device. (See "Local Device Registration Management" section of Volume 1 for further details.)

(U//FOUO) Figure 3 also illustrates the following properties of user devices:

- **ECUs**. An ECU may (1) if properly equipped, be registered as a general device, or (2) be registered only as a limited device.
- **AKPs**. An AKP is always registered as a general device.
- **Fill Devices**. A fill device is registered only as a limited device; PSNs do not wrap products for fill devices.

(U//FOUO) This volume primarily discusses the registration of general devices, although many of the requirements stated here apply to both general and limited devices. Further information about other characteristics that distinguish different types of user devices, is provided in the "Key Fill" section of Volume 1.

3.1.3 (U) Client Support for Registered Users

(U//FOUO) To obtain products and services or otherwise access KMI resources in CI-2, almost all human users, and some user devices, employ Client Nodes to interact with a PRSN. (A few humans who act as administrative managers can directly access native interfaces of computer platforms that are components of KMI nodes, i.e., without using a client as an intermediary; see “Administrative Security for Platforms and Applications” section.) This section briefly describes how Clients support users; further details are provided primarily by the “System Architecture” section of Volume 1, especially the “Primary Services Nodes” and “Client Nodes” sections.

(U//FOUO) A human user accesses the KMI by operating a Client Node and connecting to a PRSN. A person acting in a management role connects an MGC to an Ordering and Management Enclave (OME) of a PRSN; a person acting in a non-management role (i.e., as a KOA Agent; see “KMI Operating Accounts” section of Volume 3) connects a DOC to a Product Delivery Enclave (PDE). (OMEs and PDEs are described in the “Nodal Structures” section of Volume 3.)

(U//FOUO) Clients operated by human users are expected to be computer platforms equipped with software (including a Web browser) and security features needed for KMI functions. The human user is registered with identity authentication material which supports KMI access control mechanisms. When a human user connects a client to a PRSN and logs in to establish a session, the PRSN provides the client with web pages that enable the user to play a role to which the user has been assigned and to request products and services in accordance with permissions that have been granted to that role.

(U//FOUO) User devices retrieve KMI products and services through a Client Node, which connects to a PDE of a PRSN. However, unlike clients that serve human users and communicate with a PRSN through a web protocol, clients that serve user devices communicate with a PRSN only through a strictly formatted transaction protocol. In some cases, the client that serves a user device is separate from the device and is operated by a KOA Agent. In other cases, the user device itself is equipped with the client functionality needed to connect to a PDE, and that functionality can operate without concurrent human direction. In the latter cases, the device is said to be PDE-enabled:

> **DEFINITION** (U//FOUO) PDE-Enabled Device. A User Device that is a General Device and also is equipped to be able to connect as a Client Node to a PRSN PDE to obtain KMI products and services.

(U//FOUO) Table 1 shows the combinations of device types that are supported in CI-2. If a user device is intended to be PDE-enabled, the device needs to have (1) a centrally registered identity (i.e., it needs to be a General Device), (2) material to authenticate its identity to the PDE, and (3) network connectivity between it and the PDE. Both U.S. and non-U.S. devices may be PDE-enabled.

Table 1. (U) KMI Registration Types for User Devices

	PDE-Enabled Device	Not Enabled for PDE Access
General Device	Products wrapped by PSN for device are distributed through PDE, and device <u>can</u> connect to a PDE to get them.	Products wrapped by PSN for device are distributed through PDE, but device <u>cannot</u> connect to a PDE to get them.
Limited Device	[By definition, this case is not supported in KMI CI-2]	Products wrapped by AKP for device are distributed through Client Node. Device <u>cannot</u> connect to a PDE to get them.

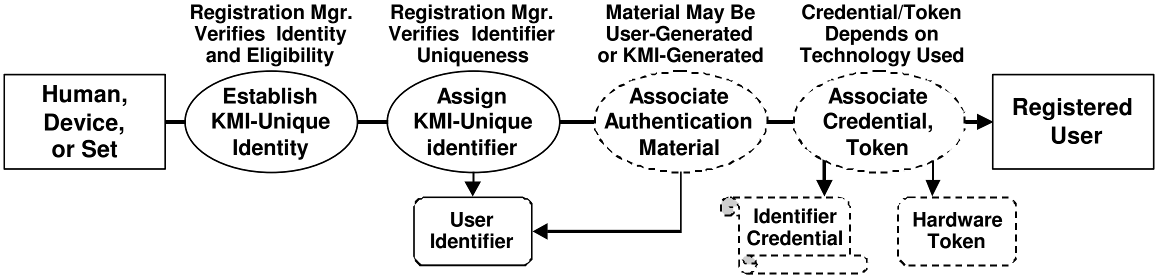
UNCLASSIFIED//FOUO

3.2 (U) User Registration and Identification Service

POLICY (U//FOUO) **General Policy on User Registration.** The KMI must use assured means to register a User prior to authorizing the User to request or receive any product or service.

(U//FOUO) This section specifies KMI's basic process for registering users. This registration process, which is illustrated in Figure 4, is used to register humans, devices, sets of humans, and sets of device, in accordance with the *KMI Policy for Registration of Users* [NSAKMIRU].

Figure 4. (U) KMI User Registration Process


Registration Mgr. Verifies Identity and Eligibility
Registration Mgr. Verifies Identifier Uniqueness
Material May Be User-Generated or KMI-Generated
Credential/Token Depends on Technology Used
Human, Device, or Set
Establish KMI-Unique Identity
Assign KMI-Unique identifier
Associate Authentication Material
Associate Credential, Token
Registered User
User Identifier
Identifier Credential
Hardware Token

UNCLASSIFIED//FOUO

DEFINITION (U//FOUO) <u>User registration</u>. The process that (1) initializes a User Identity in the KMI for a System Entity that is authorized to access the KMI, (2) associates a User Identifier with the identity, (3) may also associate Authentication Material with the identifier, and (4), depending on the authentication mechanism being used, may also associate an Identifier Credential with the identifier (see "Identifier Credentials" section).

(U//FOUO) The "Access Control" section of Volume 3 of this *Specification* also uses the term "registration" for two other KMI processes. One process is performed in association with enrolling a human user as a manager and ensures that the basic registration for that person was done with sufficient security assurance for someone who will act as a manager. The other process establishes KOAs in the system. Both of these other processes are separate from the basic user registration process that is described in this section.

(U//FOUO) The user registration process involves the concepts of "user identity" and "user identifier", and may involve "authentication material", a "user credential", and "hardware token". These concepts are defined in this section and the "Identity Authentication Service" section.

(U//FOUO) The *KMI Policy for Registration of Users* [NSAKMIRU] will provide details of KMI requirements for assignment of user identifiers that are used to access the KMI and for security features and assurances of their associated authentication material and credentials, whether issued by the KMI or by other systems. That policy may, therefore, incorporate other specific policies and standards as needed, such as the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] or the *United States Government Type 1 Certificate Policy* [UST1CP].

3.2.1 (U) Identity Registration

POLICY (U//FOUO) **General Policy on User Identification.** Whenever a Registered User accesses the KMI, the User must identify itself in a way that enables the KMI to associate with the User Identity all the actions of the User, so that a specific person—either that User in the case of a User Person, or the User Sponsor in the case of a User Device or User Set—can be held accountable for those actions.

(U//FOUO) Control of access to KMI resources is based on identities that have been established in the system. The requirements stated in this volume mainly deal with identities of users, but some cases involve identities of other components. The following general requirement to support identities for users is implemented by more detailed requirements in following subsections:

> **CI2-SEC-3.2.1a** (U//FOUO) The KMI shall enable each Registered User to have one or more User Identities, each of which is associated with one or more User Identifiers; and each User Identifier may be associated with one or more types and items of Authentication Material. [DRV KRD 1577, 1605] {R}

3.2.1.1 (U) User Identities

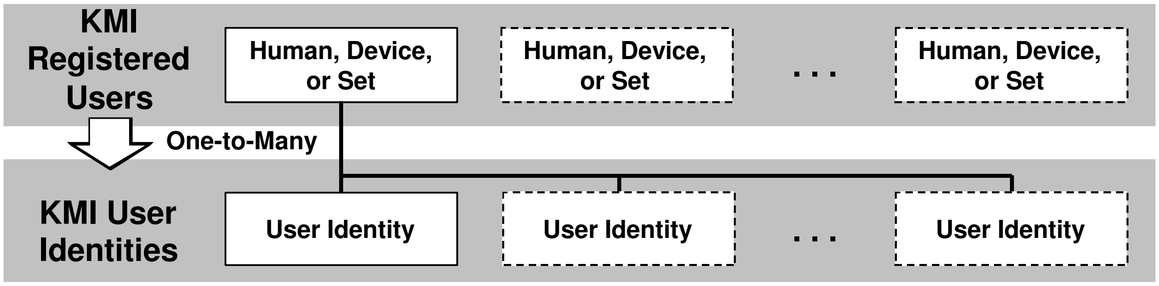
(U//FOUO) Control of access to KMI resources by users is based on identities that have been established through the basic registration process by the actions of User Registration Managers.

> **DEFINITION** (U//FOUO) User Identity. The collective aspect of a set of attribute values (i.e., characteristics) by which a specific individuality of a Registered User is recognized or known by the KMI and which are sufficient to distinguish the identity from (1) any other identities of that same User and also from (2) identities of other Users.

(U//FOUO) This *Specification* also defines the term "User Identifier" (see "User Identifier Registration" section in this Volume). User Identifier refers to a different concept than User Identity; in brief, a User Identifier is a name of a User Identity.

(U//FOUO) Figure 5 illustrates that a registered user may have one or more user identities.

Figure 5. (U) KMI User Identities



UNCLASSIFIED//FOUO

(U//FOUO) The following three cases are functionally different in the KMI:

- (U//FOUO) **One user has two identities.** If two user identities are registered for one user, it means that the user has two independent justifications for KMI access, such as belonging to two Government organizations that operate independently of each other. Thus, a user device is expected to need only one KMI identity, but some human users are expected to need more than one. For example, a law enforcement officer in the Department of Justice might also be a reserve military office in the Department of Defense.

- (U//FOUO) **One identity has two identifiers.** If two identifiers are registered for one identity, it means that the identity is concurrently known by two different names or titles. Each user device is expected to have only a one KMI identifier, but some human users are expected to need more than one. (See “User Identifier Registration” section.)

- (U//FOUO) **One identity is assigned to two roles.** Each user device is expected to be assigned to at most one KMI role; but some human users are expected to be assigned to more than one. (See “Access Control Service” section.)

(U//FOUO) User identities are established in the system by the user registration process.

CI2-SEC-3.2.1.1a (U//FOUO) When registering the first User Identity for a User, the KMI shall determine whether the User is (1) a Human User, (2) a User Device, or (3) a User Set. [DRV KRD 0355, 1587] {C-R}

CI2-SEC-3.2.1.1b (U//FOUO) The KMI shall enable a User Registration Manager, and only a User Registration Manager, to register a User Identity. [DRV KRD 1574] {R}

CI2-SEC-3.2.1.1c (U//FOUO) The KMI shall enable a Personnel Registration Manager to register a User Identity for a Human User. [DRV KRD 1587] {R}

CI2-SEC-3.2.1.1d (U//FOUO) The KMI shall enable a Device Registration Manager to register a User Identity for a User Device. [DRV KRD 0355, 1587] {C-R}

(U//FOUO) Except for the difference expressed in the two foregoing requirement statements, the role-based access control permissions (see “Role-Based Access Control Section” in Volume 3) granted to a Personnel Registration Manager are essentially identical to those granted to a Device Registration Manager. Thus, other requirement statements and descriptive text refers to both roles collectively as "User Registration Manager".

CI2-SEC-3.2.1.1e (U//FOUO) The KMI shall be able to register a User Identity for a User Set that either (1) contains only Human Users or (2) contains only User Devices, but shall not be able to register a set that contains both humans and devices. [DRV KRD 0865] {R}

(U//FOUO) This *Policy* prohibits mixed user sets of humans and devices because such situations might cause security policies and related requirements to be interpreted in conflicting ways.

CI2-SEC-3.2.1.1f (U//FOUO) The KMI shall be able to register additional User Identities of the same type (i.e., human, device, or set) for a Registered User that already has a User Identity. [DRV KRD 1605] {R}

CI2-SEC-3.2.1.1g (U//FOUO) The KMI shall prevent any User that is acting as a User Registration Manager from registering a User Identity for itself. [DRV KRD 1560] {R}

CI2-SEC-3.2.1.1h (U//FOUO) The KMI shall record for Audit, as specified in the *KMI Policy for the Registered Users* [NSAKMIRU], data about each registration of a User Identity. [DRV KRD 1597] {C-R}

3.2.1.2 (U) Component Identities

(U//FOUO) In some cases, the KMI architecture requires a component to control access to its resources by other components. Some such inter-component access controls might be implemented implicitly by fixed physical connections or other means through which communication paths are provided, but other inter-component access controls could be implemented more explicitly. Since "devices" and "sets of devices" are types of users, any component identity could be registered like other KMI user identities.

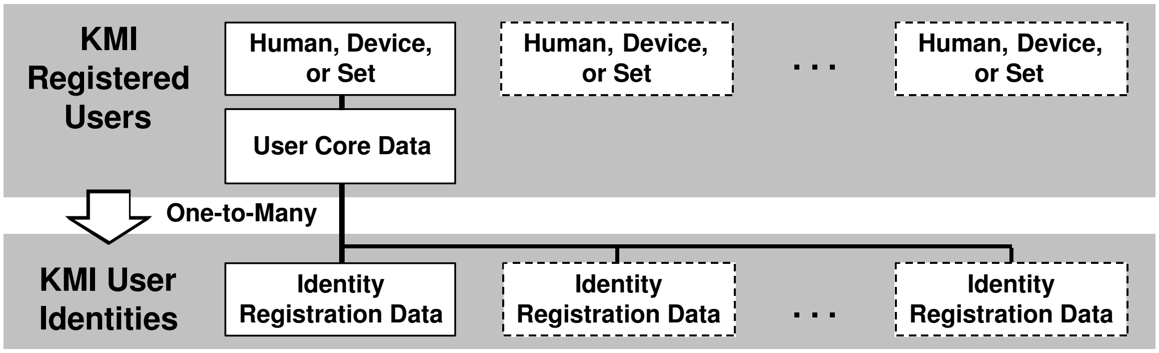
DEFINITION (U//FOUO) Component Identity. A special case of User Identity; the collective aspect of a set of attribute values (i.e., characteristics) by which a Component is recognized or known by other Components and which is sufficient to distinguish that Component (1) from all other identities of that same Component and also (2) from all identities of all other Components.

CI2-SEC-3.2.1.2a (U//FOUO) The KMI shall protect each registered Component Identity from unauthorized modification by protecting the Registration Data and other data associated with the identity. [DRV KRD 1027] {A-P-R-S-T}

3.2.2 (U) User Registration Data

(U//FOUO) As illustrated in Figure 6, the user registration process records data for each registered user and for each identity of a registered user, and retains that data on a long-term basis to deter fraudulent acts and to support compromise recovery.

Figure 6. (U) KMI User Registration Data



UNCLASSIFIED//FOUO

> **DEFINITION** (U//FOUO) User Registration Data. The set of attribute values acquired by, and stored and maintained in, the KMI to establish and describe a Registered User.

(U//FOUO) The KMI records core registration data for each registered user, and records identity-specific registration data for each user identity. (As is noted in several places in this “User Registration and Identification Service” section, the requirements stated in this *Specification* for handling user registration data are intended to be supplemented by additional details stated in the *KMI Policy for Registered Users* [NSAKMIRU].)

> **DEFINITION** (U//FOUO) User Core Data. A subset of the User Registration Data, that (1) distinguishes a Registered User from all other Registered Users, (2) has the same values for all User Identities of the User, and (3) includes some attributes that have values that remain constant over the life of the User. [DRV KRD 1588]

> **DEFINITION** (U//FOUO) Identity Registration Data. A subset of the User Registration Data that describes a specific User Identity.

(U//FOUO) The KMI can recognize each registered user independently of how many identities are registered for the user, because a user’s identities all have the same core data values. However, a KMI implementation needs to assign to each user a value that can be used to anchor the association of the user’s core data with identity-specific data and other information.

> **DEFINITION** (U//FOUO) KMI User Number (KU#). A KMI-unique value that the KMI assigns to a Registered User and that is used in the system’s internal database as an index, label, or abbreviated name for associating data elements pertaining to that User.

(U//FOUO) This *Specification* calls the anchor value a “number” to prevent confusion with the term “user identifier” (see “User Identifiers Registration” below), but a variety of implementations is possible. For example, KU#s might be sequential integers that are internally assigned but are mapped to other, externally assigned identifiers, such as a person’s Electronic Data Interchange Person Identifier (EDI-PI) or a device’s serial number [KMI3001] or an X.500 Distinguished Name (DN). Alternatively, the KU# space might be constructed as a composite of external identifier spaces, perhaps by adding a common, KMI-unique prefix to each type of external identifier.

CI2-SEC-3.2.2a (U//FOUO) When registering the first User Identity for a User, the KMI shall assign to that User a permanent, unique KU#. [DRV KRD 1588] {C-R}

CI2-SEC-3.2.2b (U//FOUO) When registering the first User Identity for a User, the KMI shall record the User Core Data. [DRV KRD 1588] {C-R}

CI2-SEC-3.2.2c (U//FOUO) When registering a User Identity for a Human User or User Device (that has not already acquired a KMI-unique external User Identifier through previous registration of another User Identity), the KMI shall associate a permanent, KMI-unique, external User Identifier with that User Identity. [KRD 1590] {R}

CI2-SEC-3.2.2d (U//FOUO) When registering a User Identity for a User Device, the KMI shall ascertain and record the device's serial number as defined by the *Electronic Serial Number Standard* [KMI3001]. [DRV KRD 1588] {C-R}

CI2-SEC-3.2.2e (U//FOUO) When registering a User Identity for a User Set, the KMI shall associate with that User Identity a permanent, KMI-unique, external User Identifier that is separate from the User Identifiers of the members of the set. [DRV KRD 1590] {R}

CI2-SEC-3.2.2f (U//FOUO) The User Core Data shall include at least the following attributes: [DRV KRD 1588] {C-R}

- (1) The User's KU#. [DRV KRD 1588]
- (2) Designation of the User as either a person, set of persons, device, or set of devices.
- (3) If the User is a Human User:
    - The person's KMI-unique external User Identifier. [DRV KRD 1590]
    - The person's citizenship or national affiliation. [KRD 1594]
- (4) If the User is a General Device:
    - The device's KMI-unique external User Identifier. [DRV KRD 1590]
    - The device's serial number [KMI3001].
    - Additional items specified in the *Security Architecture* [KMI2200V3].
- (5) If the User is a User Set:
    - The set's KMI-unique external User Identifier. [DRV KRD 1590]
- [Additional data items are expected to be defined when a Component-level design is done.]

CI2-SEC-3.2.2g (U//FOUO) When registering a User Identity, the KMI shall record Identity Registration data, which is in addition to the User Core Data. [DRV KRD 1588] {C-R}

(U//FOUO) The following requirement uses three terms that are not defined until later sections of this volume: User Identifier, Token Holder, and KT#. These are also defined in the Glossary sections.

CI2-SEC-3.2.2h (U//FOUO) The Identity Registration Data for a User Identity shall include at least the following attributes: [DRV KRD 1589] {C-R}

- (1) The organizational authority (i.e., a DoD Service or Agency, or another Department of Government) under which the User Identity is registered. [DRV KRD 1593]
- (2) If the User Identity is for a User Device or User Set:
    - The User Device Sponsor or User Set Sponsor of the Identity. [DRV KRD 1582]

- (3) The User Identifiers that have been assigned to the User Identity.
- (4) If the User acts in that identity as a Token Holder:
  - The KT#(s) of the token(s) assigned to the User Identity. [DRV KRD 1686]
- (5) The User Identity of the User Registration Manager that most recently verified the authenticity and eligibility of the registered User Identity.
- (6) If the User is a User Device:
  - Additional items specified in the *Security Architecture* [KMI2200V3].

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

CI2-SEC-3.2.2i (U//FOUO) When recording User Registration Data, the KMI shall be able to record different types of attributes for different types of Users and different types of User Identities. [DRV KRD 1589] {C-R}

CI2-SEC-3.2.2j (U//FOUO) User Registration Data elements that the KMI holds in common with any External System with which the KMI interoperates, shall share compatible formats and allowable values for DoD personnel registrations. [DRV KRD 0353] {R}

(U//FOUO) For example, although the following control does not apply to CI-2 because KMI does not assign e-mail addresses, CI-2 might record registration data that includes e-mail addresses assigned by naming authorities outside the KMI:

CONTROL (U//FOUO) **ECAD-1 Affiliation Display (Confidentiality)**. [Not applicable to CI-2.] "To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation 'ctr' and all foreign nationals are identified by the inclusion of their two character country code in:" [DoDI8500.2]

- "DoD user e-mail addresses
  (e.g., john.smith.ctr@army.mil or john.smith.uk@army.mil)."
- "DoD user e-mail display names
  (e.g., John Smith, Contractor <john.smith.ctr@army.mil>
  or John Smith, United Kingdom <john.smith.uk@army.mil>)."
- "Automated signature blocks
  (e.g., John Smith, Contractor, J-6K, Joint Staff
  or John Doe, Australia, LNO, Combatant Command)."

"Contractors who are also foreign nationals are identified as both (e.g., john.smith.ctr.uk@army.mil). Country codes and guidance regarding their use are in FIPS 10-4."

3.2.3 (U) Uniqueness of Users and User Identities

POLICY (U//FOUO) To ensure individual accountability, the KMI must prevent any System Entity from becoming registered as two different Users.

(U//FOUO) User accountability is the property of a system 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 needs to be able to identify a registered user uniquely when the user accesses the system, regardless of how many identities the user has. Any customer organization that authorizes registration of KMI users will normally need to ensure user accountability for its own purposes and, therefore, is expected support that policy. However, an organization may need to register an entity as two different KMI users to protect the interests of either the organization or the entity. If so, then the KMI, when performing operations such as compromise recovery, will not be able to associate all system activities of that entity.

CI2-SEC-3.2.3a (U//FOUO) When registering the first User Identity for a User, the KMI shall (1) compare the User Core Data to that of all other Registered Users to ensure that the new User Identity is not already registered; and, if a probable duplicate is detected, the KMI shall (2) record the event for audit, (3) stop the registration process and not record the duplicative data, (4) notify the User Registration Manager, and (5) notify an Incident Response Manager. [DRV KRD 0295, 0401] {C-R}

CI2-SEC-3.2.3b (U//FOUO) When registering the first User Identity for a User, the KMI shall associate the Identity Registration Data with User Core Data. [DRV KRD 1595] {C-R}

CI2-SEC-3.2.3c (U//FOUO) When registering an additional User Identity for a User, the KMI shall associate the new Identity Registration Data with that User's existing User Core Data. [DRV KRD 1595] {C-R}

CI2-SEC-3.2.3d (U//FOUO) When registering an additional User Identity for a User, the KMI shall (1) compare the new Identity Registration Data to that User's existing User Identities; and, if a probable duplicate identity is detected, the KMI shall (2) notify the User Registration Manager and enable that Manager, at the Manager's discretion, to stop the registration process and not record the duplicative data, (3) notify an Incident Response Manager, and (4) record the event for Audit. [DRV KRD 0295, 0401, 2000, 2001] {C-R}

3.2.4 (U) User Identity Authenticity and Eligibility

POLICY (U//FOUO) **Identity Authenticity and Eligibility.** When a User Identity is registered, the KMI must verify the identity's authenticity—i.e., that the User (1) has the right to claim the identity being registered and (2) has been authorized to do so—and its eligibility—i.e., that the identity (3) is qualified to be registered and (4) needs to be registered. [DRV KRD 0923]

POLICY (U//FOUO) **Identity Evidence.** A person who applies to register a User Identity of their own—or a person who applies to register an identity for a device, for a set of persons, or for a set of devices—must present a form of evidence that has been approved by the KMI system-level DAAs for verifying authenticity and eligibility; and the cognizant User Registration Manager must not accept any other form of evidence.

(U//FOUO) Appendix A of this volume proposes a partial, draft specification of forms of evidence for identity authenticity.

CI2-SEC-3.2.4a (U//FOUO) For each registered User Identity, the KMI shall record and maintain Identity Registration Data elements that (1) describe the evidence, as specified in the *KMI Policy for Registration of Users* [NSAKMIRU], that was presented and examined to verify authenticity and eligibility and (2) ensure accountability for approval of the evidence. [DRV KRD 0923, 1593] {R}

(U//FOUO) For example, if a state driver's license is presented to verify an identity, the KMI would record that fact along with the license's issuer, date of issue, and date of expiration; and the KMI also would record the date and time of verification, the identity of the verifying official, and an authenticated acknowledgement by the verifying official.

CI2-SEC-3.2.4b (U//FOUO) When the KMI registers a User Identity, the KMI shall prompt the associated User Registration Manager to verify and record evidence, as specified in the *KMI Policy for Registration of Users* [NSAKMIRU], for the identity's authenticity and eligibility. [DRV KRD 0923, 1593] {C-R}

3.2.5 (U) User Identity States

(U//FOUO) An identity need not become active immediately upon entry of identity registration data, and an active identity can be become inactive.

DEFINITION (U//FOUO) Identity Registration State. A User Identity that has been registered for accessing the KMI and also is currently authorized to do so, is in the Active State. A User Identity that has been registered for accessing the KMI but is not currently authorized to do so, is in the Inactive State.

CI2-SEC-3.2.5a (U//FOUO) The KMI shall enable an authorized User Registration Manager to enter Identity Registration Data to establish a new User Identity in the Inactive State. [DRV KRD 0395] {C-R}

CI2-SEC-3.2.5b (U//FOUO) The KMI shall enable an authorized User Registration Manager to enter Identity Registration Data to establish a new User Identity in the Active State. [DRV KRD 0395] {C-R}

CI2-SEC-3.2.5c (U//FOUO) The KMI shall enable an authorized Manager to change the User Identity Registration State of an existing User Identity from Active to Inactive. [DRV KRD 1203] {C-R}

CI2-SEC-3.2.5d (U//FOUO) If a User Identity is in the Inactive State, the KMI shall not permit a User to access the KMI by invoking that identity. [DRV KRD 1203] {C-R}

CI2-SEC-3.2.5e (U//FOUO) If a User Identity is in the Inactive State, the KMI shall not perform actions to issue products or provide services in association with that identity, except to revoke products previously issued or services previously performed. [DRV KRD 1203] {C-R}

CI2-SEC-3.2.5f (U//FOUO) When a Manager changes the Identity Registration State of a User Identity from Active to Inactive, the KMI shall require the Manager to record the reason for the change and to designate the reason as either routine or for cause; and if the change is for cause, the KMI shall require the Manager to record the reason in a text block and shall permanently include the text in the User Identity's Registration Data. [DRV KRD 1355] {C-R}

CI2-SEC-3.2.5g (U//FOUO) When the Identity Registration State of a User Identity changes, the KMI shall archive the Identity Registration Data. [DRV KRD 0930] {R}

CI2-SEC-3.2.5h (U//FOUO) The KMI shall enable an authorized Manager to change the User Identity Registration State of a User Identity from Inactive to Active. [DRV KRD 1356] {C-R}

CI2-SEC-3.2.5i (U//FOUO) When the KMI receives a request to reactivate a User Identity that has previously had its Identity Registration State changed from Active to Inactive for cause, the KMI shall perform the following actions in order: [KRD 1356] {C-R}

(1) The KMI shall notify the cognizant User Registration Manager and display the recorded reason for the previous revocation.
(3) The KMI shall require the User Registration Manager to acknowledge reading the reason.
(4) The KMI shall enable the User Registration Manager to accept or reject the request, or to postpone a decision for a period not to exceed one week.
(5) The KMI shall present postponed requests weekly, for a maximum of four weeks.
(6) Upon the fifth presentation of the request, the KMI shall require the User Registration Manager to either approve or reject the request, or else the KMI shall automatically reject the request.
(7) The KMI shall enable the User Registration Manager to append comments to the Identity Registration Data.

CI2-SEC-3.2.5j (U//FOUO) When a Manager changes the Identity Registration State of a User Identity from Inactive to Active, the KMI shall require the Manager to record the reason for the change. [DRV KRD 1356] {C-R}

CI2-SEC-3.2.5l (U//FOUO) The KMI shall record for Audit any change in the Identity Registration State of a User Identity. [DRV KRD 1355, 1356] {C-R}

3.2.6 (U) User Identity Reverification

POLICY (U//FOUO) **Identity Reverification.** The KMI must periodically reverify the authenticity and eligibility of each active User Identity that is registered in the system, in the same manner as if the identity were being newly registered, in accordance with applicable policies and product doctrine.

CI2-SEC-3.2.6a (U//FOUO) For each User Identity, the KMI shall periodically prompt a User Registration Manager to examine and reverify evidence, as specified in the *KMI Policy for Registration of Users* [NSAKMIRU], for the User Identity's authenticity and eligibility; and if that is not done within a specified time interval, the KMI shall set the Identity Registration State to Inactive. [DRV KRD 0925] {C-R}

CI2-SEC-3.2.6b (U//FOUO) The KMI shall enable a Security Configuration Manager to configure the periodicity of reverification of User Identity authenticity and eligibility. [DRV KRD 0925] {R-S}

CI2-SEC-3.2.6c (U//FOUO) The KMI shall enable a Security Configuration Manager to set the time interval within which a User Registration Manager must complete reverification of a User Identity. [DRV KRD 0925] {R-S}

(U//FOUO) Related requirements are stated in the "Manager Reverification and Confirmation" section of Volume 3.

3.2.7 (U) User Identifier Registration

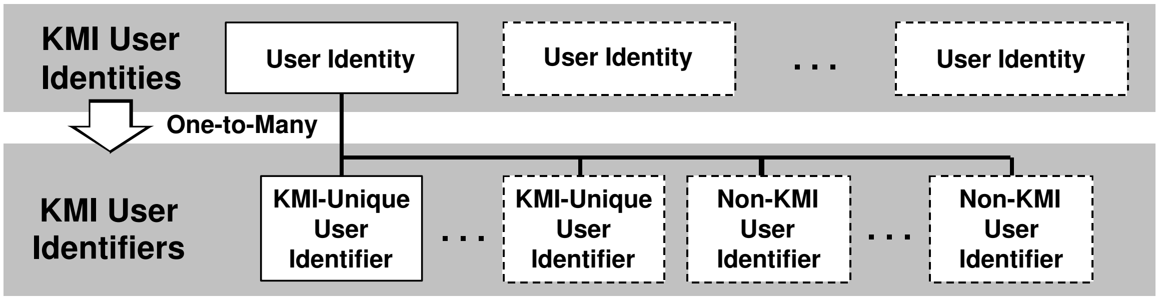
POLICY (U//FOUO) **Presentation of Identifier.** When a Registered User attempts to access the KMI, the entity must first present, either explicitly or implicitly, a registered KMI-Unique User Identifier.

(U//FOUO) Individual accountability of users depends on the uniqueness of user identifiers.

DEFINITION (U) User Identifier. A name that can be unambiguously represented by a printable, non-blank character string.

(U//FOUO) Figure 7 illustrates that a user identity has at least one KMI-unique identifier, and may have non-KMI identifiers.

Figure 7. (U) KMI User Identifiers



UNCLASSIFIED//FOUO

DEFINITION (U//FOUO) KMI-Unique User Identifier. A User Identifier that (1) can be used to access the KMI, (2) takes a form specified in the *KMI Policy for Registration of Users* [NSAKMIRU], and (3) is unique among all current and past User Identities (i.e., is associated with one and only one User Identity and thus enables the KMI to distinguish that Identity and its User from all other System Entities).

(U//FOUO) A KMI-Unique User Identifier is not the same as KU#. A KU# is assigned to a User, and each User has only one KU#. A KMI-Unique User Identifier is assigned to an Identity of a User, so that each User could have more than one KMI-Unique User Identifier. The KU#s are used only internally, but the KMI-Unique User Identifiers are typically known, and often used for other purposes, outside the KMI.

(U//FOUO) Although the form of KMI-unique user identifiers has not yet been specified, one possible form is the X.500 DN, because many users who will act as KOA Agents are expected to already have been assigned a DN by the DoD Public-Key Infrastructure (PKI) or some other system. Therefore, DNs are used for the examples in this volume. A user identity may have more than one KMI-unique identifier; this feature is needed to support aliasing, renaming, and other procedures. The KMI also may need to register identifiers for purposes other than KMI access.

DEFINITION (U//FOUO) Non-KMI User Identifier. A User Identifier that (1) cannot be used to access the KMI as a Registered User and (2) either takes the same form as a KMI-Unique User Identifier or takes some other form.

(U//FOUO) For example, an identity could have an X.500 DN that is used to access the KMI, but also have an RFC 822 mailbox name that is used as an administrative point of contact with KMI managers.

CI2-SEC-3.2.7a (U//FOUO) When registering a User Identity, the KMI shall establish at least one KMI-Unique User Identifier for the identity. [DRV KRD 0354, 1578, 1586] {C-R}

CI2-SEC-3.2.7b (U//FOUO) The KMI shall enable a User Registration Manager, and only a User Registration Manager, to register KMI-Unique User Identifiers. [DRV KRD 1716] {C-R}

CI2-SEC-3.2.7c (U//FOUO) When registering a KMI-Unique User Identifier, the KMI shall (1) check whether the User Identifier is already assigned to another User Identity that belongs to either the same or any other Registered User (past or present); and, if a probable duplicate identifier is detected, the KMI shall (2) stop the registration process and not record the duplicative data, (3) notify the User Registration Manager, (4) notify an Incident Response Manager, and (5) record the event for Audit. [DRV KRD 0262, 0295, 0401, 0650] {C-R}

CI2-SEC-3.2.7d (U//FOUO) The KMI shall be able to register additional KMI-Unique User Identifiers for a User Identity that already has one or more. [DRV KRD 1577] {C-R}

CI2-SEC-3.2.7e (U//FOUO) The KMI shall be able to record one or more non-KMI identifiers for a User Identity, but the KMI shall not require such a non-KMI identifier to be unique across the KMI. [DRV KRD 1577] {C-R}

CI2-SEC-3.2.7f (U//FOUO) The KMI shall enable a User Registration Manager, and only a User Registration Manager, to record non-KMI User Identifiers. [DRV KRD 1716] {C-R}

(U//FOUO) Requirements to enable registration of User Sets are stated later, in the "Registration of Set Identities" section.

CI2-SEC-3.2.7g (U//FOUO) The KMI shall record for Audit the registration of each User Identifier, as specified in the *KMI Policy for Registration of Users* [NSAKMIRU]. [DRV KRD 1597] {C-R}

3.2.8 (U) User Identifier Authorities

POLICY (U//FOUO) **Authoritative Assignment of Identifiers.** The KMI may associate a User Identifier with a User Identity only if the identifier has been assigned to that identity by an entity that the KMI system-level accreditors recognize as authoritative for the identifier's name space.

(U//FOUO) The systems that are authoritative for user identifiers are expected to implement and enforce administrative security measures to ensure proper association of the identifiers with user identities. Some of those systems are expected to be part of the KMI, and others (e.g., the DoD PKI) are not. In any case, those measures are not defined in this *Specification*. From a technical viewpoint, the KMI is only responsible for ensuring that identifiers are unique across the KMI. That is, if someone tries to register an identifier for a KMI identity and that identifier is already registered for a different KMI identity, then the KMI will detect the duplication and not permit the second registration.

> **CI2-SEC-3.2.8a** (U//FOUO) The KMI shall record information regarding the naming authority by which a User Identifier has been assigned to a User Identity. [DRV KRD 0259, 0509, 0650, 1593] {C-R}

(U//FOUO) Identifiers used for KMI access need to be unique across the KMI, but the KMI is not expected to control all the name spaces from which identifiers are assigned. In the DoD PKI, for example, a DN is assigned by a naming authority in the user's organization, regardless of whether the DN is used for KMI access or for some other system [DoDGDS]. Some non-DoD users are expected to access the KMI with DNs assigned by a DoD naming authority, but other users are expected to have DNs assigned by non-DoD authorities. Also, although an affiliation should exist between a KMI user and any organization indicated by an identifier, assuring that association is not the direct responsibility of the KMI. Procedures for coordinating among all naming authorities—DoD, non-DoD U.S. Government, and non-Government—to assign DNs that are globally unique, for assuring organization affiliations indicated by identifiers, and for otherwise managing the name spaces are the responsibility of the naming authorities.

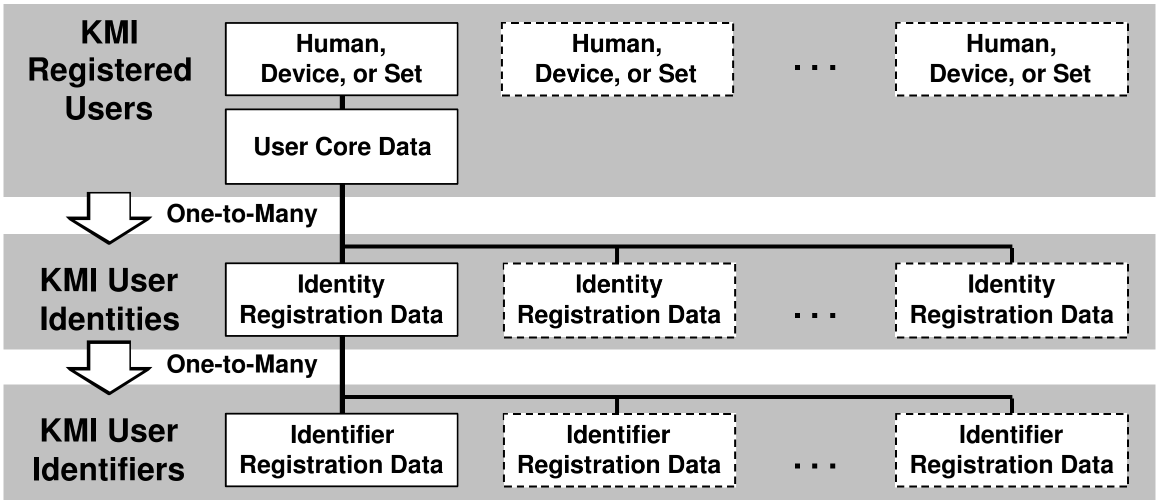
3.2.9 (U) User Identifier Registration Data

(U//FOUO) As illustrated in Figure 8, the KMI records data for each identifier of a user identity.

> **DEFINITION** (U//FOUO) <u>KMI Identifier Registration Data</u>. A subset of the Identity Registration Data that describes a specific User Identifier.

> **CI2-SEC-3.2.9a** (U//FOUO) When registering a User Identifier for a User Identity, the KMI shall record Identifier Registration Data. [DRV KRD 1588] {C-R}

Figure 8. (U) KMI User Registration Data



UNCLASSIFIED//FOUO

CI2-SEC-3.2.9b (U//FOUO) The Identifier Registration Data for a User Identifier shall include at least the following data elements: [DRV KRD 1588] {C-R}

– (1) The naming authority by which the identifier is assigned. [DRV KRD 0259, 0650, 1593]

– (2) A list of Identifier Credentials issued for the identifier by the KMI, if any. [DRV KRD 1718]

– [Additional data elements are expected to be defined when a Component-level design is done.]

CI2-SEC-3.2.9c (U//FOUO) When recording Identifier Registration Data, the KMI shall be able to record different types of data items for different type of User Identifiers. [DRV KRD 1589] {C-R}

CI2-SEC-3.2.9d (U//FOUO) The KMI shall ensure that Identifier Registration Data elements held in common with an External System with which the KMI interoperates, shall share formats and allowable values for DoD personnel registrations. [DRV KRD 0353] {C-R}

3.2.10 (U) User Identifier States

(U//FOUO) Once an identifier has been registered for an identity, the registration data is retained on a long-term basis to support compromise recovery. However, an identifier can become inactive for various reasons, similar to the way the registration state of an identity can change (see “User Identity State” section).

DEFINITION (U//FOUO) Identifier Registration State. A KMI-Unique User Identifier that has been registered for accessing the KMI and also is currently authorized to do so, is in the Active State. A KMI-Unique User Identifier that has been registered for accessing the KMI but is not currently authorized to do so, is in the Inactive State.

CI2-SEC-3.2.10a (U//FOUO) The KMI shall enable an authorized Manager to change the Identifier Registration State of a KMI-Unique User Identifier from Active to Inactive. [DRV KRD 1203] {C-R}

(U//FOUO) In the preceding requirement, "authorized" implies that KMI supports a role-based permission to perform that action. (See "Role-Based Access Control" section of Volume 3.) The permission to change the activity state of a user identifier is primarily intended to be assigned to Enrollment Managers for use in controlling managers; but the permission might also be assigned to other managers, depending on how CI-2 operational procedures evolve.

CI2-SEC-3.2.10b (U//FOUO) If a KMI-Unique User Identifier is in the Inactive State, the KMI shall not permit a Registered User to access the KMI by invoking that User Identifier. [KRD 1203] {C-R}

CI2-SEC-3.2.10d (U//FOUO) When the Identifier Registration State of a KMI-Unique User Identifier changes, the KMI shall archive the Identifier Registration Data. [KRD 0930] {C-R}

CI2-SEC-3.2.10d (U//FOUO) When the registration state of a KMI-Unique User Identifier changes, the KMI shall archive the Identifier Registration Data. [KRD 0930] {C-R}

CI2-SEC-3.2.10e (U//FOUO) The KMI shall record for Audit any change in the Identifier Registration State of a KMI-Unique User Identifier. [KRD 1355, 1356] {C-R}

CI2-SEC-3.2.10f (U//FOUO) When a Manager changes the Identifier Registration State of a KMI-Unique User Identifier, the KMI shall require the Manager to record the reason for the change. [DRV KRD 1356] {C-R}

CI2-SEC-3.2.10g (U//FOUO) The KMI shall enable an authorized Manager to change the Identifier Registration State of a KMI-Unique User Identifier from Inactive to Active. [DRV KRD 0935, 1356] {C-R}

3.2.11 (U) User Identity and Identifier Management

POLICY (U//FOUO) **Identity Management.** The KMI must manage and safeguard User identification mechanisms and their implementations so as to protect the confidentiality and integrity of Identity Registration Data.

CI2-SEC-3.2.11a [NT] (U//FOUO) The KMI shall ensure that Identity Registration Data stored in the system accurately describes all Registered Users, User Identities, and User Identifiers, and completely and consistently records the values of the associated attributes. [DRV KRD 0369, 0927] {R}

CI2-SEC-3.2.11b (U//FOUO) The KMI shall enable an authorized Manager to access Core Data, Identity Registration Data, and Identifier Registration Data. [DRV KRD 0927] {C-R}

CI2-SEC-3.2.11c (U//FOUO) The KMI may enable a Registered User to enter or update, in limited cases, some descriptive elements of the User's own Identity Registration Data and Identifier Registration Data. [KRD NEW] {R}

CI2-SEC-3.2.11d (U//FOUO) The KMI shall enable an authorized Manager to modify or delete elements of the User Registration Data for a User—including User Core Data, Identity Registration Data, and Identifier Registration Data—that is stored in the system, as permitted by the permissions of each specific Management Role. [DRV KRD 1575] {C-R}

CI2-SEC-3.2.11e (U//FOUO) The KMI shall prevent any User that is acting as a User Registration Manager from modifying or deleting any of its own User Registration Data that is stored in the system. [DRV KRD 1560] {R}

CI2-SEC-3.2.11f (U//FOUO) The KMI shall archive Identity Registration Data associated with a User Identity before modifying or deleting that data. [DRV KRD 1575] {C-R}

CI2-SEC-3.2.11g (U//FOUO) The KMI shall record for Audit all actions that attempt to modify or delete stored User Registration Data. [DRV KRD 0930, 1476] {C-R}

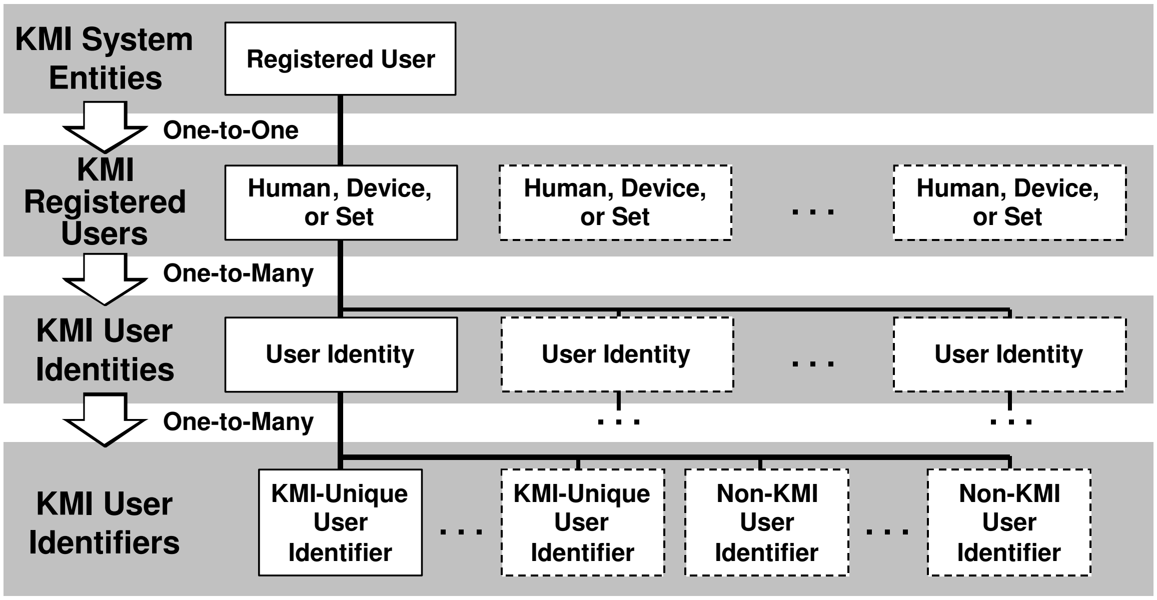
CI2-SEC-3.2.11h (U//FOUO) The on-line KMI shall retain essential identity-specific User Registration Data elements for a User Identity—i.e., KMI shall not delete all knowledge of the identity from the on-line system—as long as the associated User Core Data is still held in the on-line operational system. [KRD NEW] {C-R}

CI2- SEC-3.2.11i (U//FOUO) The KMI shall archive User Registration Data for Users that do not have an active User Identity for a period of time that is configurable by an authorized Archive Manager; and, after verifying that the data has been successfully written to Archive media, the KMI shall remove the data from the on-line operational database. [DRV KRD 2096] {R}

CI2-SEC-3.2.11j (U//FOUO) The on-line KMI shall retain essential User Core Data elements for a Registered User—i.e., KMI shall not delete all knowledge of the User from the on-line system—for a configurable number of years after all the User Identities of that User have become inactive. [KRD NEW] {R}

(U//FOUO) Figure 9 illustrates basic relationships among the concepts of Registered User, User Identity, and User Identifier. The Identity Registration Data that the KMI maintains for those relationships can be used to answer queries from Managers in special situations, such as compromise recovery.

Figure 9. (U) KMI Users, Identities, and Identifiers



UNCLASSIFIED//FOUO

CI2-SEC-3.2.11k (U//FOUO) The KMI shall enable an authorized Manager that has knowledge of a User—i.e., has knowledge of (1) distinguishing User Core Data values, (2) a KMI-Unique User Identifier, or (3) other User Registration Data values that distinguish that User from all others—to display (a) all User Identities and User Identifiers that have been registered for that User, (b) any User Device Sponsor or User Set Sponsor of that User (if the User is a User Device or User Set), (c) all User Devices and User Sets for which the User is a User Sponsor, and (d) all User Sets that contain that User. [DRV KRD 2024] {C-R}

3.2.12 (U) Singular Identities and Set Identities

(U//FOUO) The KMI supports two basic types of identities—singular and set.

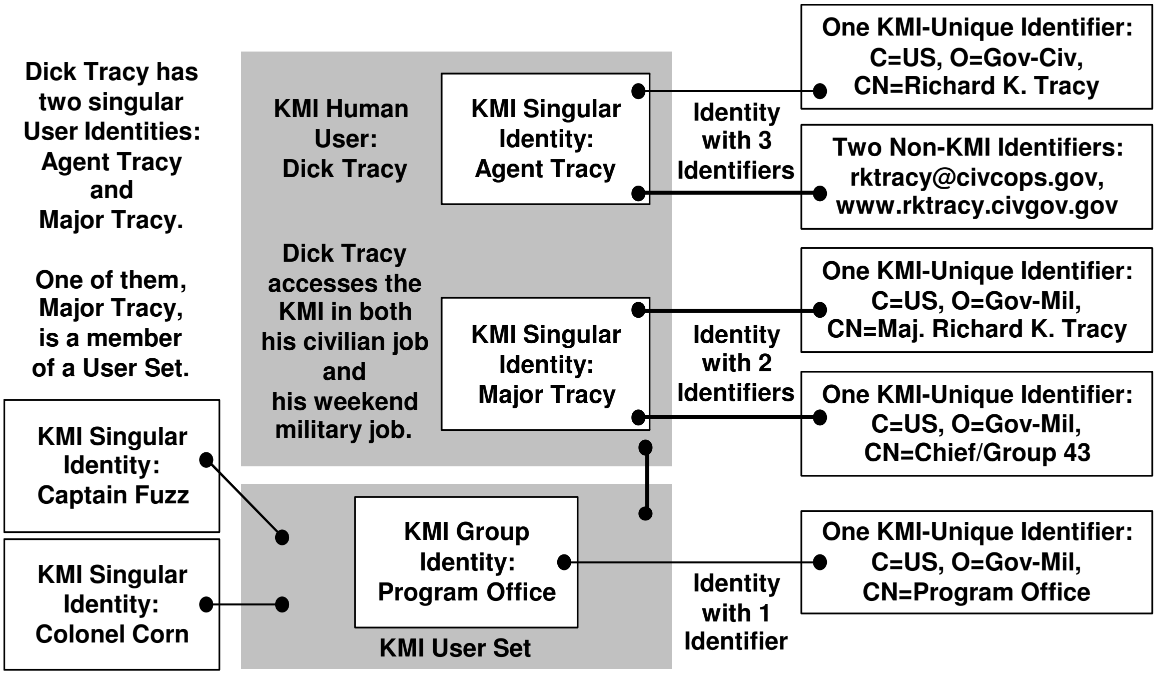
DEFINITION (U//FOUO) Singular Identity. A User Identity that is registered for exactly one, specific Human User or User Device.

(U//FOUO) To support long-term compromise recovery both for the KMI and for external systems operated by KMI customer organizations, a singular identity is never reassigned to a different user. However, situations can exist in which individual users share some common purpose and use a set identity.

DEFINITION (U//FOUO) Set Identity. A User Identity that is registered for a User Set composed either (1) entirely of Human Users or (2) entirely of User Devices.

(U//FOUO) Although set identities are not currently intended to be used in operating KMI CI-2, their use is anticipated for identity credentials that KMI is expected to issue for other applications and systems planned for the Global Information Grid. Figure 10 illustrates a fictitious human user ("Dick Tracy") who has two singular identities ("Agent Tracy" and "Major Tracy"), one of which ("Major Tracy") also is a member of a user set ("Program Office").

Figure 10. (U) KMI User Identification Example


Dick Tracy has two singular User Identities: Agent Tracy and Major Tracy.
One of them, Major Tracy, is a member of a User Set.
KMI Singular Identity: Captain Fuzz
KMI Singular Identity: Colonel Corn
KMI Human User: Dick Tracy
Dick Tracy accesses the KMI in both his civilian job and his weekend military job.
KMI Singular Identity: Agent Tracy
KMI Singular Identity: Major Tracy
KMI Group Identity: Program Office
KMI User Set
Identity with 3 Identifiers
Identity with 2 Identifiers
Identity with 1 Identifier
One KMI-Unique Identifier: C=US, O=Gov-Civ, CN=Richard K. Tracy
Two Non-KMI Identifiers: rktracy@civcops.gov, www.rktracy.civgov.gov
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Maj. Richard K. Tracy
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Chief/Group 43
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Program Office

UNCLASSIFIED//FOUO

(U//FOUO) A KMI user set usually is some type of organizational unit. However, this *Policy* avoids the term "organizational identity" because that would conflict with "organizational" as used in the Defense Message System (DMS) (see "Singular-Set versus Individual-Organizational" section below).

(U//FOUO) The KMI treats a set identity much like a singular identity, but the types differ in their security risks. Therefore, rather than allowing a registered identity to be used as either a singular identity or a set identity, the KMI requires the person who registers an identity to declare which usage is intended, so that the KMI can properly manage the associated risks.

3.2.12.1 (U) Registration of Singular Identities

(U//FOUO) In-person registration of singular identities for human users provides the foundation of accountability not only for humans, but also for devices and sets.

POLICY (U//FOUO) **Personal Registration of Human Users.** To register a User Identity for a Human User, that person must appear before a User Registration Manager, either when first applying or when being granted possession of related Authentication Material.

CI2-SEC-3.2.12.1a (U//FOUO) When registering a User Identity for a Human User or a User Device, the KMI shall establish the Identity as a Singular Identity. [DRV 1587] {C-R}

CI2-SEC-3.2.12.1b (U//FOUO) The KMI shall record the date of the most recent in-person registration appearance for each Human User. [DRV KRD 1591] {R}

(U//FOUO) When a registered user is a user device or a user set, that user must have a sponsor.

DEFINITION (U//FOUO) User Sponsor. A Human User, represented in the KMI by a User Identity, who officially represents the KMI customer organization that is accountable for use of a User Identity of a User Device or User Set.

POLICY (U//FOUO) **Sponsored Registration of User Devices.** To register a User Identity for a User Device, the device must be sponsored by a KOA that will initially be accountable for use of the device identity and has been authorized to register User Devices on behalf of a Government organization that is served by that KOA. (That is, each User Device must be sponsored for registration by a KOA Manager who acts on behalf of a specific KOA.)

(U//FOUO) Accountability for a User Device should be based on accountability for a specific Human User, and the logical candidate to name is a KOA Manager in the KOA to which the device is assigned at registration time. However, when a registered device is transferred from one KOA to another, that manager normally does not transfer with it, and the persons serving as KOA Managers in a particular KOA are frequently replaced by other persons as part of normal duty rotation and personnel reassignment processes in DoD organizations. (See "KMI Operating Accounts" section of Volume 3 for more information.) Therefore, this *Policy* designates, as the device's sponsor, the Primary KOA Manager of whatever KOA currently holds the user device.

DEFINITION (U//FOUO) User Device Sponsor. The Primary KOA Manager of the KOA that is currently accountable for use of a User Device; i.e., the KOA to which a User Device is currently assigned. (See "KOA Device Assignment" section of Volume 3 for more information.)

CI2-SEC-3.2.12.1c [NT] (U//FOUO) The KMI shall enable a Human User Primary KOA Manager to be the User Device Sponsor for the initial registration of a User Identity for a User Device if and only if that KOA is authorized to have its Primary KOA Manager sponsor device registrations. [DRV KRD 1582, 1592] {C-R}

CI2-SEC-3.2.12.1d }**CI2-SEC-3.2.12.1d** (U//FOUO) When registering a User Identity for a User Device, the KMI shall associate the requesting User Device Sponsor with the new identity (i.e., include the KOA Identifier in the Identity Registration Data). [DRV KRD 1582, 1592, 1719] {C-R}

(See information about KOA Identifiers in the "KOA Registration and Associated Data" section of Volume 3.)

3.2.12.2 (U) Registration of Set Identities

POLICY (U//FOUO) **Sponsored Registration of User Sets.** To register a User Identity for a User Set, the set must be sponsored by a previously registered User Identity that belongs to a Human User who will be accountable for use of the Set Identity and who has been authorized to register User Sets on behalf of a Government organization that is served by the KMI.

(U//FOUO) Accountability for user sets is based on accountability for individual persons.

DEFINITION (U//FOUO) User Set Sponsor. A Human User, represented in the KMI by a User Identity, who (1) requests that a new User Identity be registered for a User Set and then (2) continues to officially represent the KMI customer organization that is accountable for use of the new identity.

CI2-SEC-3.2.12.2a (U//FOUO) The KMI shall enable a Human User to sponsor a User Set if and only if the person's User Identity has authorization to sponsor User Sets. [DRV KRD 1582, 1592] {R}

CI2-SEC-3.2.12.2b (U//FOUO) When registering a User Identity for a User Set, the KMI shall associate the requesting User Set Sponsor with the Set Identity (i.e., include the sponsor's User Identity in the Identity Registration Data for the set). [DRV KRD 1582, 1592, 1719] {R}

CI2-SEC-3.2.12.2c (U//FOUO) The KMI shall enable a Personnel Registration Manager, and only such a Manager, to register a User Identity for a User Set consisting of Human Users. [KRD 1587] {R}

CI2-SEC-3.2.12.2d (U//FOUO) The KMI shall enable a Device Registration Manager, and only such a Manager, to register a User Identity for a User Set consisting of User Devices. [KRD 0355, 1587] {R}

3.2.12.3 (U) Singular-Set versus Individual-Organizational

(U//FOUO) The "singular-set" dichotomy defined in this *Policy* for KMI identity types is different than the "individual-organizational" dichotomy defined by the Defense Message System for message types (and, by extension, for X.500 DNs of DMS users). A DMS organizational message is one for which (1) the originator is acting as a point of organizational responsibility (but may have either a singular identity or a group identity in KMI), (2) the recipient is doing likewise, and (3) the message is formally approved as officially representing the originator [MJCS20-89]. A DMS individual message is a one that is not organizational.

(U//FOUO) Table 2 gives examples for the four cases that could occur if KMI identities were established for DMS users:

Table 2. (U) KMI Singular-Set versus Individual-Organizational

		DMS Message Type Sent By User	
		Individual	**Organizational**
User's KMI Identity Type	**Singular**	Example: A DoD employee sends an informal query.	Example: A DoD commander issues an order.
	Set	Example: A DoD program office team replies to an informal query.	Example: A DoD program office issues a formal standard.

UNCLASSIFIED//FOUO

3.2.13 (U) Group Identities and Shared Identities

(U//FOUO) This *Specification* proposes that KMI support the following two types of set identities:

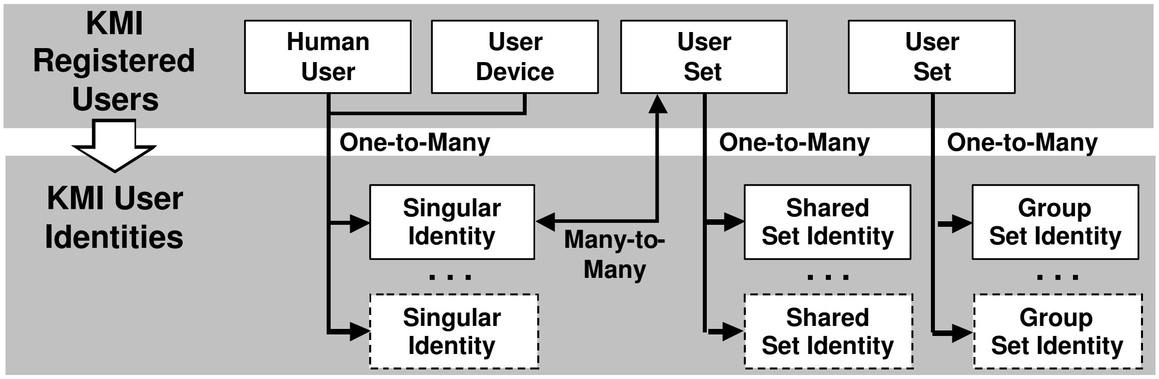
> **DEFINITION** (U//FOUO) Group Identity. A User Identity that is registered for a User Set for which the KMI does not maintain a record of the members of the set (i.e., the KMI does not have knowledge of the Human Users, or User Devices, that belong to the set). [KRD 365, 366. 1584]

> **DEFINITION** (U//FOUO) Shared Identity. A User Identity that is registered for a User Set in which each member of the set is authorized to assume that identity individually, and for which the KMI maintains a record of members of the set. [KRD 365, 366]

(U//FOUO) These two types of set identity are similar in that (1) a human user must sponsor registration of the set and (2) the set's membership can change over time and consist of zero, one, or more users. However, the two types differ in how they are intended to be used, in the degree to which accountability for their use can be maintained, and in how responsibility is assigned for maintaining accountability. The requirement for group identities in KMI is well-established. However, the requirement for set identities is not well-established, and consideration is being given to removing the Shared Identity concept from this *Specification*.

(U//FOUO) Figure 11 illustrates relationships between the three types of registered users—human, devices, and sets—and the three types of user identities—singular, group, and shared.

Figure 11. (U) KMI Singular, Group, and Shared Identities



UNCLASSIFIED//FOUO

- (U//FOUO) Figure 11 illustrates that each human or device may have one or more singular identities, and that each set may have either one or more group identities or one or more shared identities.

- (U//FOUO) Figure 11 illustrates that the relationship between (1) singular identities and (2) user sets that have one or more shared identities is many-to-many; that is, a singular identity may be associated with one or more user sets, and a user set may be associated with one or more one singular identities.

3.2.13.1 (U) Registration of Group and Shared Identities

(U//FOUO) The KMI supports group identities for situations where the KMI does not need to ensure individual accountability within the set, and supports shared identities for situations where the KMI must ensure individual accountability within the set.

CI2-SEC-3.2.13.1a (U//FOUO) When registering a User Identity for a User Set, the KMI shall require the User Registration Manager to declare the identity to be either (1) a Group Identity or (2) a Shared Identity. [DRV KRD 0365, 0366, 1584, 1587] {R}

CI2-SEC-3.2.13.1b (U//FOUO) The KMI shall be able to associate a specified Shared Identity with a specified Singular Identity of either a Human User or a User Device (depending on whether the Shared Identity consists of Human Users or User Devices), thus indicating that the Human User or User Device that has the Singular Identity is a member of the User Set that is authorized to use the Shared Identity to access the KMI. [DRV KRD 0365, 0366] {R}

CI2-SEC-3.2.13.1c (U//FOUO) The KMI shall be able to associate a Singular Identity with zero, one, or more Shared Identities for which the Singular Identity is a member of the User Set that is authorized to use those Shared Identities to access the KMI. [DRV KRD 0365, 0366] {R}

CI2-SEC-3.2.13.1d (U//FOUO) When a Singular Identity is associated with one or more Shared Identities, the KMI shall continue to maintain the separate Singular Identity in addition to the Shared Identities. [DRV KRD 0365, 0366] {R}

CI2-SEC-3.2.13.1e (U//FOUO) The KMI shall be able to associate a Shared Identity with zero, one, or more Singular Identities that are members of the User Set that is authorized to use that Shared Identity to access the KMI. [DRV KRD 0365, 0366] {R}

CI2-SEC-3.2.13.1f (U//FOUO) The KMI shall be able to remove a specified Singular Identity from the User Set that is authorized to use a specified Shared Identity to access the KMI; but the KMI shall retain knowledge (to support compromise recovery operations) that the Singular Identity has been a member of the set. [DRV KRD 0365, 0366] {R}

CI2-SEC-3.2.13.1g (U//FOUO) If a Singular Identity of a Human User or User Device is in the Inactive State, the KMI shall not permit the User to access the KMI through any Set Identity with which that Singular Identity is associated. [DRV KRD 0365] {R}

3.2.13.2 (U) Intended Use of Group Identities and Shared Identities

(U//FOUO) Table 3 summarizes accountability responsibilities for the two types of set identities when those identities are used to access the KMI versus non-KMI systems.

Table 3. (U) KMI Accountability Responsibilities for Set Identities

		KMI Responsibility	**Sponsor Responsibility**
When Used To Access the KMI	**Accountability for Set as a Whole**	Group or Shared Identity KMI can and does maintain accountability for actions of set as a whole.	
	Accountability for Individual Members	Group Identity KMI is unable to maintain accountability for actions of individual members.	Sponsor must maintain accountability for individual members, per KMI policy.
		Shared Identity KMI maintains accountability for actions of each set member that uses the identity.	

UNCLASSIFIED//FOUO

- (U//FOUO) **Accountability for Group identities**. The KMI does not maintain knowledge of the individual humans or devices that are members of a group identity, and thus cannot maintain accountability for those individuals when a group identity is used to access the KMI. For access to the KMI, a group identity is appropriate for assignment to the KOA Agent role, but usually not to a manager role. (See “Access Control Service” section for additional information.)

- (U//FOUO) **Accountability for Shared identities**. The KMI can maintain individual accountability for users of a shared identity when the identity is used to access the KMI. Therefore, a shared identity is appropriate for assignment to any role.

3.2.13.3 (U) Non-Convertibility Between Group and Shared Identities

(U//FOUO) Conversion of a shared identity to a group identity or vice versa is not needed. No shared identity need be converted to a group identity, because a shared identity can be used by a non-KMI system as though the identity were a group identity. A group identity could not be converted to a shared identity without asserting individual accountability for members of the underlying user set, and this would be impossible for past actions already associated with the group identity. (For further explanation, see Appendix B, which discusses approaches to implementing individual accountability for using shared identities.)

3.2.14 (U) Summary of KMI Identity Types

(U//FOUO) Table 4 summarizes the identity types and subtypes proposed for KMI. Two contrasting cases of special interest in the table are (1) a singular identity consisting of one human user and (2) a set identity that contains persons but has N=1. Although the latter seems more complex, it actually can simplify the management of identities in some situations; and it a need for this type of identity has been expressed by KMI customer organizations.

Table 4. (U) KMI Identity Types

	Singular Identity	**Set Identity**
Purpose	Represents a registered Human User or User Device.	Represents an automated function performed by one or more Registered Users.
Number of Performers	Exactly one performer, and always the same performer.	May have from 0 to N, and the actual performers that comprise the N members may change. – Group Identity, KMI does not know members. – Shared Identity, KMI knows the set members.
Case 1: Person(s)	Represents a specific person. – Could be called a “personal” identity.	Represents a human function, which is performed collectively by the set members. – If N>1, could be called a “team” Identity. – If N=1, could be called a “position” Identity.
Case 2: Device(s)	Represents a specific device. – If hardware, could be called a “device” Identity. – If software, could be called an “application” Identity.	Represents an automated function, which is performed collectively by the set members. – If devices are hardware, could be called a “cluster” Identity. – If devices are software, could be called a “service” Identity.

UNCLASSIFIED//FOUO

(U//FOUO) For example, suppose a DoD customer organization has a job called Supervisor, and suppose that Joe Doe is a registered user and has an identity with the KMI-unique identifier “Mr. Joe Doe”. If Joe Doe is assigned to the Supervisor position, then a second identity, with the

KMI-unique identifier “Supervisor”, could be registered for him. However, when Joe Doe leaves the position and John Smith takes his place, a new identity must be registered for John Smith, because the existing “Supervisor” identity is permanently associated with Joe Doe and cannot be reassigned. John’s new identity would need a new KMI-unique name, because the KMI-unique identifier “Supervisor” is permanently associated with Joe Doe’s identity. Instead, a set identity named “Supervisor” could be registered independent of either Joe or John, and the “Joe Doe” identity could be assigned to that user set. When Joe leaves the position and John takes his place, Joe’s identity could be removed from the set and the “John Smith” identity could be added. The permissions and other associations that were established for “Supervisor” when Joe filled the position would not need to be reestablished for John. (In some DoD PKI discussions, a public-key certificate issued to identify this kind of user set has been called a “role certificate”, but this *Policy* avoids that use of “role” because it conflicts with how the term in used in KMI role-based access control that is specified in Volume 3.)

3.3 (U) Identity Authentication Service

POLICY (U//FOUO) **General Policy on User Identity Authentication.** When a System Entity presents a registered User Identifier in an attempt to access the KMI as a Registered User, the KMI must authenticate the claimed User Identity before providing the entity with any product or service or permitting the entity to perform any other action in the KMI.

DEFINITION (U//FOUO) User Authentication. A security service that verifies a User Identity that is claimed by or for a System Entity that attempts to access the KMI.

(U//FOUO) User authentication involves two steps. (1) The first step is identification, which consists of presenting an identifier that is claimed to be bound to the entity. This enables the entity to be recognized as a registered user or system component, and to be distinguished from other such entities. (2) The second step is verification, which consists of presenting information that proves the truth of the claimed identity.

(U//FOUO) KMI user authentication services provide a basis for access control and other security services and, when complemented by audit services, ensures accountability. Therefore, the KMI needs to employ robust user identity authentication mechanisms and protect their implementations and associated information. Managers need to be able to direct and control the establishment and maintenance of authentication material, identifier credentials, and authentication tokens. The specific policies and associated requirements for implementing user authentication service are as follows:

CI2-SEC-3.3a (U//FOUO) When a System Entity attempts to access the KMI without presenting a KMI-Unique User Identifier, the KMI shall treat the entity as not registered. [DRV 0865, 0947] {R}

(U//FOUO) The foregoing requirement refers to interactions with an entity prior to when the KMI invokes an authentication dialogue, or where no dialogue is used. In the case of a PRSN, the “PRSN Public Zones” section of Volume 3 contains requirements to minimize such interactions. The “Training and Awareness” section of this volume contains requirements to warn unregistered entities against attempting access to the KMI.

CI2-SEC-3.3b (U//FOUO) When a System Entity attempts to access the KMI by presenting a KMI-Unique User Identifier—i.e., claims the User Identity of a Registered User—the KMI shall authenticate the Identifier before permitting the entity to access the system as a Registered User. [DRV KRD 0341, 0846, 0865, 0942, 0947, 1549] {C-R}

CI2-SEC-3.3c (U//FOUO) The KMI shall record for Audit all authentication failures when a System Entity attempts to access any System Resource by presenting a KMI-Unique User Identifier of a Registered User. [DRV KRD 0844, 0866, 0867] {C-R}

(U//FOUO) The KMI needs to authenticate the identity not only of user entities that access KMI components but also of components themselves when they access other components. The definitions of “System Entity” and “Registered User” (see “User Entities” section) are sufficiently general to cover such intra-system, inter-component authentication.

CI2-SEC-3.3d (U//FOUO) Each Independent Component shall cryptographically authenticate the identity of other, remote Components before permitting them to access its local System Resources. [DRV KRD 0846, 1549] {Z}

3.3.1 (U) Choice of Authentication Technology

(U//FOUO) This *Specification* is written to be largely independent of specific authentication technologies, so as to facilitate evolution to new technologies. However, the primary authentication technologies for CI-2 initially are expected to be asymmetric cryptography, in which a system entity proves its identity by using a private key, and identifier-password pairs.

CI2-SEC-3.3.1a (U//FOUO) The KMI shall support the following technologies for authentication of User Identifiers: [DRV KRD 1992] {Z}

- Asymmetric cryptography using FIREFLY Credentials.
- Asymmetric cryptography using X.509 certificates, including being able to specify which Certificate Policies within those certificates are acceptable, and to specify whether Certificate Policy Mapping is acceptable or not.
- Identifier-password pairs, both persistent and one-time.
- Other technologies that become approved for KMI use, such a biometric (when draft DoDI 8550.dd, *DoD Biometrics*, is finalized and issued).
- Combinations of two of the above.

(U//FOUO) One reason for CI-2 accepting (1) X.509 certificates issued by KMI-approved, non-U.S. certification authorities and (2) identifier-password pairs issued by the KMI, is that CI-2 needs to support non-U.S. users who act as KOA Agents and access PDEs to retrieve wrapped products but who have no other means of authentication.

(U//FOUO) In some cases, KMI might need to require a second (i.e., additional, supplemental) form of identity authentication before permitting a user to act in certain roles during a session, or might need to support multiple forms that are configurable to meet operational requirements.

CI2-SEC-3.3.1b (U//FOUO) The Preliminary Design for CI-2 shall specify for Government approval (1) which situations require only a single, fixed form of authentication, (2) which situations, if any, require a second, i.e., additional, form of authentication, and (3) which situations require alternate, configurable forms. [DRV 1553] {Z}

CI2-SEC-3.3.1c (U//FOUO) For Access Control situations that require alternate, configurable forms of authentication, the KMI shall enable a Security Configuration Manager to select from the available methods to configure the types of authentication that are acceptable for each applicable Role [DRV KRD 1553, 1992] {Z}

CI2-SEC-3.3.1d (U//FOUO) To authenticate a User Identity or Component Identity for a Manager or for any other Access that affects the life cycle of Type 1 products and services, the KMI shall use high-assurance procedures and mechanisms, such as those based on Type 1 products. [DRV KRD 1063] {Z}

3.3.2 (U) Identity Authentication Material

POLICY (U//FOUO) **Protection of Identity Authentication Material.** If Authentication Material is associated with a User Identity, the KMI must not provide knowledge or control of that information to any System Entity other than the User or the User Sponsor.

DEFINITION (U//FOUO) Authentication Material. A unit of information that a Registered User employs to prove a claimed User Identity when accessing the system.

(U//FOUO) All human users need an identifier and some form of associated authentication material to authenticate themselves to the system, and so do user devices that access the KMI by acting as a client node. User devices that receive products indirectly and do not directly access a PRSN need an identifier but not authentication material.

CI2-SEC-3.3.2a (U//FOUO) The KMI shall be able to associate a User Identifier with one or more of the following types of Authentication Material: [1554, 1992] {Z}

- Private keys involving Type 1 or Type 2 products or Type 3 or Type 4 algorithms.
- Passwords.
- Material that may be defined for other authentication technologies that become approved for KMI use.

(U//FOUO) Authentication material for a user identifier may be generated by the user, by the KMI, or by some other system, depending on the type of authentication mechanism. For example, for an identifier-password mechanism, a password could be chosen by either the KMI or the user. For a mechanism using X.509 public-key certificates, a key pair could be generated by either the user or the PKI.

CI2-SEC-3.3.2b (U//FOUO) The KMI shall protect from unauthorized Access any Authentication Material it handles and also other security-sensitive information and mechanisms associated with authentication of identities. [DRV KRD 0868, 1993] {Z}

CI2-SEC-3.3.2c (U//FOUO) The KMI shall enable only authorized System Security Officers to access stored Authentication Material and other security-sensitive information and mechanisms associated with authentication of identities. [DRV KRD 0937] {Z}

CI2-SEC-3.3.2d (U//FOUO) The KMI shall ensure that only the Registered User with which Authentication Material is associated, can invoke the use of that material. [KRD 0826] {Z}

(U//FOUO) If a user or a non-KMI system generates authentication material, the KMI would implement the foregoing requirement by administratively verifying that the non-KMI system implements that requirement with sufficient assurance to meet KMI's security needs.

CI2-SEC-3.3.2e (U//FOUO) The KMI shall ensure that any transfer of a shared secret (e.g., passwords) during the User Identity registration process, or for use in such a process (e.g., a one-time password), is protected using measures commensurate with the sensitivity of the Roles that the User is authorized to play. [KRD 0309] {R}

(U//FOUO) CI-2 is expected to use password-based authentication in at least two cases. First, some users that access the KMI to retrieve products (see "KMI Operating Accounts" section of Volume 3) might not be able to use authentication technology based on asymmetric cryptography and will need to use passwords. Second, most commercial off-the-shelf (COTS) platforms do not incorporate authentication based on asymmetric cryptography, and so CI-2 needs to use authentication mechanisms that are native to those platforms (see "Administrative Security for Platforms and Applications" section). Most platforms support only passwords.

CONTROL (U//FOUO) **IAIA-2 Individual Identification and Authentication (Confidentiality)**. For passwords, in Components that process classified information, "DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement these measures to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Multiple forms of certification of individual identification such as a documentary evidence or a combination of documents and biometrics are presented to the registration authority. Additionally, to the extent capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse, and processes are in place to validate that passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **IAIA-1 Individual Identification and Authentication (Confidentiality)**. Also for passwords, in Components that process sensitive information, "DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission." [DoDI8500.2]

(U//FOUO) The following requirements establish a basis for implementing the IAIA controls; and additional requirements related to the controls are stated in other sections of this volume.

CI2-SEC-3.3.2f (U//FOUO) The KMI design shall not include unencrypted password files. [KRD 0939] {Z}

CI2-SEC-3.3.2g (U//FOUO) For Registered Users that authenticate using an identifier-password mechanism, password usage shall comply with Federal Information Processing Standards Publication 112, *Password Usage* [FIPS112], and the *DoD Password Management Guideline* [CSCSTD002]; and the KRD shall be able to generate such passwords for issuance to KOA Agents that retrieve products using KPC-Protected Distribution (see the "KPC-Protected Product Distribution" section of Volume 1). [DRV KRD 1544] {Z}

CI2-SEC-3.3.2h (U//FOUO) Any password used in the KMI for authentication a User Identity shall be, at a minimum, a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a password is updated. [DRV KRD 2147] {Z}

CI2-SEC-3.3.2i (U//FOUO) The KMI shall enforce automatic expiration of passwords and prevent password reuse. [DRV KRD 2148] {Z}

3.3.3 (U) Establishment of Identity Authentication Material

POLICY (U//FOUO) The KMI must use assured means to establish Authentication Material for each User Identifier that is to be used to Access the KMI.

CI2-SEC-3.3.3a (U//FOUO) The KMI shall be able to associate one or more units of Authentication Material with each KMI-Unique User Identifier that is registered for accessing the KMI. [KRD 1549] {C-R}

CI2-SEC-3.3.3b (U//FOUO) In cases where the KMI generates Authentication Material for a User Identifier of a Singular Identity of a Human User, the KMI shall securely deliver the material to that person through verifiable participation of the person. [DRV KRD 1321] {R}

CI2-SEC-3.3.3c (U//FOUO) In cases where the KMI generates Authentication Material for a User Identifier of a Singular Identity of a User Device, the KMI shall securely deliver the material either to the device, through verifiable participation of that device, or to a KOA

Manager of the KOA that is the User Device Sponsor, through verifiable participation of that person . [DRV KRD 1321] {C-R}

CI2-SEC-3.3.3d (U//FOUO) In cases where the KMI generates Authentication Material for a User Identifier of a Group Identity, the KMI shall securely deliver the material to the User Sponsor of the User Set, through verifiable participation of the person who is the Sponsor. [DRV KRD 1321, 1322] {R}

CI2-SEC-3.3.3e (U//FOUO) In cases where the KMI generates Authentication Material for a User Identifier of a Shared Identity of a User Set of Human Users, the KMI shall securely deliver separate Authentication Material to each person in the set, either to the member person or to the set's User Sponsor, through verifiable participation of the receiving person. [DRV KRD 1321, 1322] {R}

CI2-SEC-3.3.3f (U//FOUO) In cases where the KMI generates Authentication Material for a User Identifier of a Shared Identity of a User Set of User Devices, the KMI shall securely deliver separate Authentication Material to each device in the set, either to the device through verifiable participation of the receiving device, or to the set's User Sponsor through verifiable participation of the receiving person [DRV 1321, 1322, 1323] {R}

CI2-SEC-3.3.3g (U//FOUO) If a Registered User generates its own Authentication Material for a User Identifier, the KMI shall verify that the Human User—or, in the case of a User Device or User Set, shall verify that either the device or the User Sponsor—has control of the material at the time when it is associated with the identifier. [DRV KRD 1038] {R}

(U//FOUO) If a user generates its own authentication material (e.g., a private signature key) but an associated identifier credential (e.g., X.509 public-key certificate) is issued by a non-KMI system (e.g., DoD PKI), the KMI would need to administratively verify that the non-KMI system implements that foregoing requirement with sufficient assurance to satisfy KMI policy.

CI2-SEC-3.3.3h (U//FOUO) For each User Identifier, the KMI shall obtain from each Human User—or, in the case of a User Device or a User Set, from the User Sponsor—an authenticated confirmation that the User or User Sponsor has accepted responsibility for the User Identifier and any associated Authentication Material. [DRV KRD 0370] {C-R}

CI2-SEC-3.3.3i (U//FOUO) The KMI shall store and maintain information to prove that each Human User—or, in the case of a User Device or a User Set, each User Sponsor— agreed (1) to protect the confidentiality of any Authentication Material used to access the KMI and (2) to notify a designated Manager if that material is lost or compromised. [DRV KRD 0370, 0924] {C-R}

CI2-SEC-3.3.3j (U//FOUO) The KMI shall enable an authorized Security Configuration Manager to set time limits on the validity of Authentication Material used to access a Component. [DRV KRD 0926] {Z}

CI2-SEC-3.3.3k (U//FOUO) The KMI shall enforce set time limits on the validity of Authentication Material used to access a Component. [DRV KRD 0926] {Z}

CI2-SEC-3.3.3l (U//FOUO) The KMI shall enable an authorized Manager to revoke any Authentication Material—i.e., invalidate the material or break the binding between the material and an associated User Identifier—that either is held by the KMI (e.g., a password) or for which the KMI issued an Identifier Credential. [DRV KRD 0782, 0897, 1203] {Z}

CI2-SEC-3.3.3m (U//FOUO) The KMI shall be able to revoke Authentication Material both for authentication technologies using asymmetric encryption and also for other authentication technologies. [DRV KRD 0950, 1016, 1203] {Z}

CI2-SEC-3.3.3n (U//FOUO) The KMI shall be able to notify affected Users about the compromise or revocation of Authentication Material. [DRV KRD 0940] {Z}

3.3.4 (U) Identifier Credentials

POLICY (U//FOUO) The KMI must ensure that any Identifier Credential issued or accepted by the KMI accurately presents the User Identifier and other descriptive information pertaining to the indicated User Identity. [DRV KRD 0368].

(U//FOUO) In cases where the KMI accepts credentials issued by a non-KMI system, the KMI would implement the foregoing policy statement by administratively verifying that the non-KMI system issues credentials with sufficient assurance to meet KMI's security needs.

DEFINITION (U//FOUO) Credential. Information, passed from one System Entity to another, used to establish the sending entity's access rights [CNSSI4009].

DEFINITION (U//FOUO) Identifier Credential. A data object that is a portable, secure representation of the association between a User Identifier and some Authentication Material, and that can be presented for use in proving a claimed User Identity to which that User Identifier has been assigned.

(U//FOUO) For example an authentication mechanism based on asymmetric encryption, a PKI certification authority issues public-key certificates. However, not all authentication technologies involve credentials; credentials are not used for identifier-password authentication.

CI2-SEC-3.3.4a (U//FOUO) The KMI shall be able to accept X.509 public-key certificates as Identifier Credentials wherever required by this *Specification* [KMI2000], and shall handle those Credentials as specified by the applicable certificate policies (e.g., [DoDX509CP, UST1CP]). [DRV KRD 1061, 1702] {R}

CI2-SEC-3.3.4b (U//FOUO) The KMI shall be able to accept FIREFLY Credentials as Identifier Credentials whenever required by this *Specification* [KMI2000], and shall handle those Credentials in accordance with [REFTBD13]. [KRD NEW] {R}

CI2-SEC-3.3.4c (U//FOUO) The KMI shall be able to accept Identifier Credentials that are defined for additional authentication technologies that become approved for KMI use, such a biometric methods. [1554, 1992] {Z}

CONTROL (U//FOUO) **IATS-2 Token and Certificate Standards (Integrity)**. For Registered Users that authenticate using asymmetric cryptography, "Identification and authentication is accomplished using the DoD PKI Medium or High Assurance certificate and hardware security token (when available) or an NSA-certified product." [DoDI8500.2]

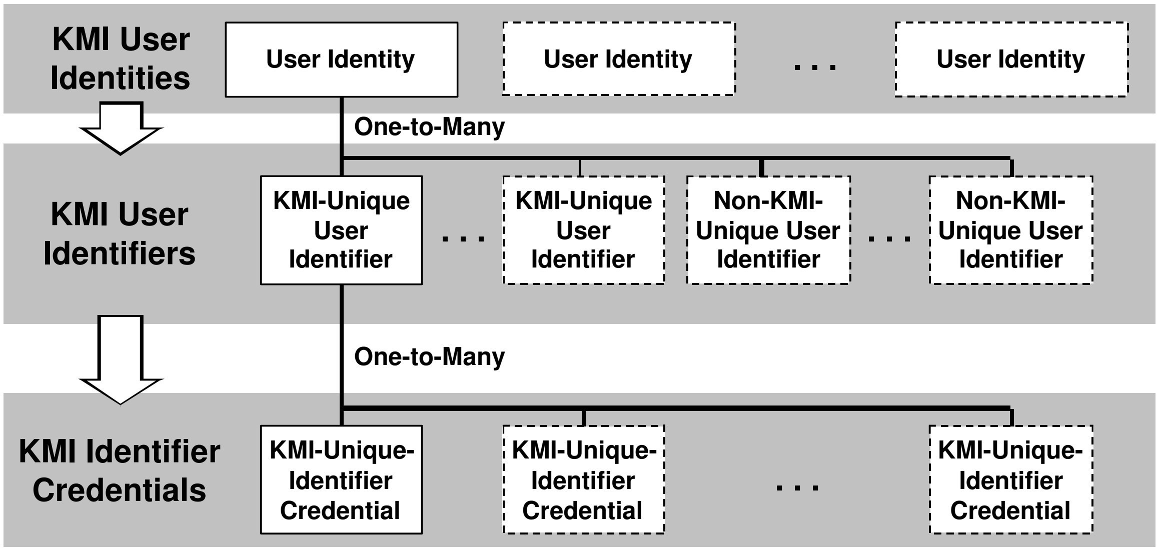
(U//FOUO) Medium and High levels of assurance are defined in the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP]. This *Specification* interprets the IATS-2 control as requiring a Medium Assurance "or better" certificate.

CI2-SEC-3.3.4d (U//FOUO) When using a public-key Identifier Credential to authenticate the User Identity of a Registered User, the KMI shall use procedures and mechanisms that at a minimum meet the requirements of the policy that is asserted by or otherwise associated with the Credential (e.g., [DoDX509CP]). [DRV KRD 0188, 1702] {C-R}

CI2-SEC-3.3.4e (U//FOUO) When using a public-key Identifier Credential to authenticate the User Identity of either (1) a Registered User acting in a Management Role (except for the Role of Personnel Registration Manager) or (2) a Component of a Core Node, the KMI shall use procedures and mechanisms that at a minimum meet the requirements of the applicable policy for Managers [USGT1CP]. [DRV KRD 0308, 1061, 1606, 1608] {C-R}

(U//FOUO) Figure 12 illustrates that a KMI-unique identifier (e.g., an X.500 DN) may be associated with one or more identifier credentials (e.g., X.500 public-key certificates).

Figure 12. (U) KMI Identifier Credentials

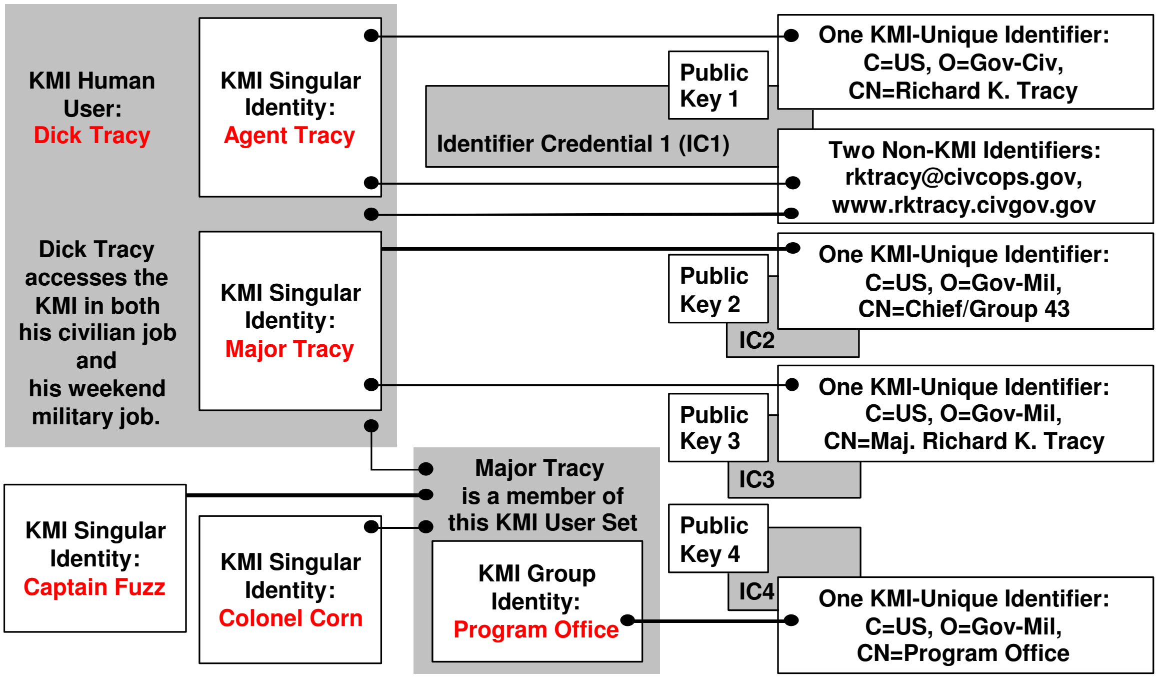

KMI User Identities
User Identity
User Identity
. . .
User Identity
One-to-Many
KMI User Identifiers
KMI-Unique User Identifier
. . .
KMI-Unique User Identifier
Non-KMI-Unique User Identifier
. . .
Non-KMI-Unique User Identifier
One-to-Many
KMI Identifier Credentials
KMI-Unique-Identifier Credential
KMI-Unique-Identifier Credential
. . .
KMI-Unique-Identifier Credential

UNCLASSIFIED//FOUO

(U//FOUO) Figure 13 further illustrates the example of the fictitious human user Dick Tracy, which was begun in Figure 10. The figure shows four identifier credentials. The DNs and other identifiers shown in the figure are all fictitious examples:

- IC1 (i.e., Identifier Credential 1) binds Public Key 1 to the KMI-unique user identifier “C=US, O=Gov-Civ, CN=Richard K. Tracy”.
- IC2 binds Public Key 2 to “C=US, O=Gov-Mil, CN=Chief/Group 43”.
- IC3 binds Public Key 3 to “C=US, O=Gov-Mil, CN=Maj. Richard K. Tracy”.
- IC4 binds Public Key 4 to “C=US, O=Gov-Mil, CN=Chief/Group 43”, an identifier of the “Program Office” identity of a User Set to which the “Major Tracy” identity belongs.

Figure 13. (U) KMI User Authentication Example


KMI Human User: Dick Tracy
KMI Singular Identity: Agent Tracy
Dick Tracy accesses the KMI in both his civilian job and his weekend military job.
KMI Singular Identity: Major Tracy
Public Key 1
Identifier Credential 1 (IC1)
One KMI-Unique Identifier: C=US, O=Gov-Civ, CN=Richard K. Tracy
Two Non-KMI Identifiers: rktracy@civcops.gov, www.rktracy.civgov.gov
Public Key 2
IC2
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Chief/Group 43
Public Key 3
IC3
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Maj. Richard K. Tracy
Major Tracy is a member of this KMI User Set
KMI Singular Identity: Captain Fuzz
KMI Singular Identity: Colonel Corn
KMI Group Identity: Program Office
Public Key 4
IC4
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Program Office

UNCLASSIFIED//FOUO

(U//FOUO) IC1 also binds Public Key 1 to two non-KMI identifiers, the RFC 822 mailbox name “rktracy@civcops.gov” and the Uniform Resource Locator “www.rktracycivgov.gov”, which would be carried in a Subject Alternative Name extension of an X.509 certificate. These two identifiers are not used for KMI access; they are bound in the credential by the PKI for some other application.

3.3.5 (U) Handling of Identifier Credentials

(U//FOUO) Identifier credentials in CI-2 are initially expected to take the forms of (1) FIREFLY credentials and (2) X.509 public-key certificates. Other forms of credentials to support additional identification technologies, such as biometrics, have not yet been specified for KMI. The KMI uses identifier credentials to authenticate the identities of users for playing both management and non-management roles, but requires the stronger credentials for the management roles.

> **CI2-SEC-3.3.5a** (U//FOUO) When issuing an Identifier Credential, the KMI shall record Identifier Registration Information to associate the credential with KMI-Unique User Identifier for which the Credential is issued. [DRV KRD 1718] {P-R}

CI2-SEC-3.3.5b (U//FOUO) The KMI shall validate X.509 Credentials (i.e., X.509 public-key certificates) by using the procedures and mechanisms specified in *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [RFC3280], the *X.509 Certificate Policy for the U.S. Department of Defense* [D0DX509CP], and the policy for Type 1 certificates [USGT1CP], as applicable. [DRV KRD 0752, 1608] {Z}

CI2-SEC-3.3.5c (U//FOUO) The KMI shall validate FIREFLY Credentials by using the procedures and mechanisms specified in *EKMS Firefly Specification*. [EKMS322]. [DRV KRD 0134, 0752] {Z}

CI2-SEC-3.3.5d (U//FOUO) The KMI shall check the most currently available revocation information before acting on any request that is authenticated using an Identifier Credential. [DRV KRD 1741] {Z}

3.3.6 (U) Authentication of a Group Identity

(U//FOUO) For authentication purposes, the KMI treats a group identity nearly like a singular identity, associating authentication material with identifiers of the identity.

CONTROL (U//FOUO) **IAGA-1 Group Identification and Authentication (Confidentiality)**. "Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA)." [DoDI8500.2]

(U//FOUO) This *Specification* interprets the first sentence of the IAGA control to mean that a DoD information system must maintain some degree of individual user accountability, even when users share a group identity that has a single authenticator. This *Specification* permits the following three modes, each of which supports a different degree of individual accountability, for managing the authentication material for a group identity:

- (U//FOUO) **Mode 1: Single identifier with single unit of authentication material**. The set's sponsor registers only one identifier for the identity, and the KMI associates the identifier with only one unit of authentication material.

(U//FOUO) Using mode 1 can ensure that only one member of the group uses the identity at a time. For example, a private key can be held in an authentication token that the sponsor controls through physical, personnel, and administrative security means (see "Authentication Tokens" section). Thus, mode 1 can locally support some degree of individual accountability.

- (U//FOUO) **Mode 2: Single identifier with multiple units of authentication material.** The set's sponsor registers only one identifier for the identity, but the KMI associates the identifier with multiple units of authentication material that are different from each other.

(U//FOUO) Mode 2 can be used in at least two ways.

1. (U//FOUO) Use of the identity can be restricted to one member of the user set at a time, as in mode 1, while the sponsor also holds one or more additional, secondary tokens as backups for use in case a member of the set loses, damages, or compromises the primary token.
2. (U//FOUO) The identity can be used by multiple set members at the same time, each of which holds one of the units of authentication material. For example, each member can have a personal token that holds a different private key.

(U//FOUO) Either way, the set's sponsor controls usage by physical, personnel, and administrative security means; and thus mode 2 can locally support some degree of individual accountability.

- (U//FOUO) **Mode 3: Multiple identifiers, separately authenticated**. The set's sponsor registers multiple identifiers for the identity, and the KMI associates each identifier with its own unit of authentication material, i.e., a unit that is different for each identifier.

(U//FOUO) Mode 3 can be used in the same ways as mode 2. In addition, management of individual accountability is somewhat enhanced by the separate identifiers. However, the knowledge of the association between an identifier of the group and the actual identity of the person or device that is currently using that identifier is maintained only by the sponsor, and is not known by the KMI. (See "Intended Use of Group Identities and Shared Identities" section.)

3.3.7 (U) Authentication of a Shared Identity

(U//FOUO) Authentication of a shared identity must support individual accountability. Appendix A describes potential ways to design authentication procedures to enable users to access the KMI in a shared identity. However, this *Specification* supports only the following mode:

- (U//FOUO) **Single identifier with multiple units of authentication material**. As in mode 2 for group identities, the set's sponsor registers only one identifier for the identity, and the KMI associates the identifier with multiple units of authentication material that are different from each other. However, the sponsor does not hold authentication material for the set members. Instead, each member holds and protects its own unit of authentication material, and the KMI maintains the association between that information and the set.

(U//FOUO) Each set member that uses the shared identity presents the same identifier to the KMI, but each uses different authentication material with the identifier. When the material is a private key, the KMI issues a separate X.509 public-key certificate for each user, but all the certificates have the same KMI-unique X.500 DN in the Subject field. Thus, the KMI needs a way to learn which key should be used for the verification step of the authentication service. A brute force method is to try each certificate in which the subject is the shared identifier. Another method is to require each set member to present the correct certificate along with the identifier, as is sometimes recommended in Internet standards and done in commercial software.

(U//FOUO) To establish individual accountability within the shared identity, the KMI needs a method for learning the singular identity of a user of the shared identifier. Several methods are possible. Given the correct certificate, the KMI can use the issuer DN and serial number stated in the certificate to learn, by querying the certificate issuer, which human user holds the private key. Alternatively, the holder's singular identifier could be included in the certificate in a Subject Alternative Name extension.

3.3.8 (U) Hardware Tokens

(U//FOUO) The KMI needs to ensure individual accountability for authentication material that is used for access to the KMI. Therefore, this *Policy* needs to address the use of hardware tokens.

> **DEFINITION** (U//FOUO) Hardware Token. A Registered User's individual cryptographic device, that carries the User's Authentication Material and associated Identifier Credentials, cryptographic algorithms, and keying material.

(U//FOUO) A typical hardware token consists of an integrated circuit computer and operating system, packaged and embedded in a carrier, usually in the form of a "smartcard".

> **CI2-SEC-3.3.8a** (U//FOUO) The KMI shall enable a User Registration Manager, and only a User Registration Manager, to register supported Hardware Tokens for Registered Users. [DRV KRD 0240] {R}

3.3.8.1 (U) KMI Token Holder

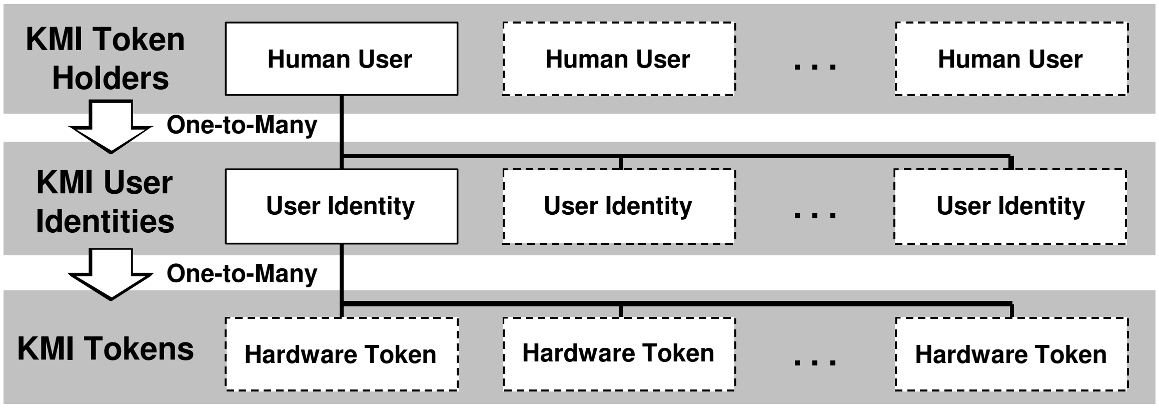
(U//FOUO) To ensure individual user accountability for the security-sensitive material carried by hardware tokens, each token is assigned to the control of a single human user.

> **DEFINITION** (U//FOUO) Token Holder. The Human User who is assigned to be accountable for the use of Authentication Material and other security-sensitive material that is carried by a Hardware Token.

> **CI2-SEC-3.3.8.1a** (U//FOUO) When the KMI issues a Hardware Token to a Registered User, the KMI shall assign a specific User Identity of a Human User to be the Token Holder. [DRV KRD 1580, 1581] {R}

(U//FOUO) Figure 14 illustrates that (1) each hardware token may have only one holder, but (2) a person may be the holder of one or more tokens.

Figure 14. (U) KMI Hardware Token Holders



UNCLASSIFIED//FOUO

(U//FOUO) Table 5 describes who is permitted to be the holder of a hardware token in various situations. The choice depends on the authentication material carried by the token. For example, if a token carries authentication material for an identity of a human user, then individual accountability can be maintained only if that person is also the token holder.

Table 5. (U) KMI Rules for Assigning Token Holder

This table determines who is named to be the Token Holder when the first unit of Authentication Material is placed on a Hardware Token, i.e., when the token is initialized.

If the Authentication Material is for an identity of this type ...	**1 Human User (i.e., Singular Identity)**	**2 User Device (i.e., Singular Identity)**	**3 User Set of Devices that has Group ID**	**4 User Set of Persons that has Group ID**	**5 User Set (of Persons) that has Shared ID**
... then assign this person as the Token Holder	Token holder is that Human User.	Token holder is Human User who sponsors the device.	Token holder is Human User who sponsors the set of devices.	Token holder is either (1) the Human User who sponsors the set or (2) a set member who is selected by the sponsor.	Token holder is a set member.

UNCLASSIFIED//FOUO

(U//FOUO) Table 5 is implemented by the following requirement:

CI2-SEC-3.3.8.1b (U//FOUO) When the first unit of Authentication Material is placed or generated on a Hardware Token, the Token Holder shall be assigned as follows: [DRV 1580, 1581] {R}

– (1) If the material is for an identity of a Human User, the Holder is that User Identity.

– (2) If the material is for an identity of a User Device or a Group Identity for devices, the Holder is the User Sponsor of the device or group.

– (3) If the material is for an identity of a Group Identity for humans, the Holder is either the User Sponsor of the group or a group member selected by the sponsor.

– (4) If the material is for an identity of Shared Identity for humans, the Holder is a member of the User Set.

(U//FOUO) If a hardware token is able to carry more than one unit of authentication material, then it might carry material for more than one identity. However, individual accountability can be maintained only if certain combinations of identities are prohibited. Table 6 describes the situations in which a token may carry more than one unit of authentication material.

(U//FOUO) Table 6 is implemented by the following requirements. The requirements permit a token to carry material for a person and sets of persons, or for a device and sets of devices, but not for both. The latter simplification was made because there is no apparent need for supporting the complexity that would result from mixing persons and devices on one token.

CI2-SEC-3.3.8.1c (U//FOUO) A Hardware Token that is used to authenticate a User Identity to the KMI shall not be permitted to carry Authentication Material for User Identities of two different Human Users (i.e., carry material for an identity of a person and also carry material for an identity of a second person). [KRD NEW] {R}

CI2-SEC-3.3.8.1d (U//FOUO) A Hardware Token that is used to authenticate a User Identity to the KMI shall not be permitted to carry Authentication Material for User Identities of two different User Devices (i.e., carry material for an identity of a device and also carry material for an identity of a second device) unless the Human User who is the Token Holder is the User Sponsor of both of the device identities. [KRD NEW] {R}

CI2-SEC-3.3.8.1e (U//FOUO) A Hardware Token that is used to authenticate a User Identity to the KMI shall not be permitted to carry both (1) Authentication Material of a User Identity of a Human User and (2) Authentication Material of a User Identity of a User Device. [KRD NEW] {R}

Table 6. (U) KMI Rules for Additional Authentication Token Content

Given a Hardware Token that already holds Authentication Material, this table determines whether or not the KMI permits an additional unit of authentication material to be placed on the token.

Choose leftmost column that applies to the authentication material that is already on the token. **Then choose the row for the information that is being added.**	**1** **Human User (i.e., Singular Identity)** Implies that the person is the token holder.	**2** **User Device (i.e., Singular Identity)** Implies that the token holder is the sponsor.	**3** **User Set of Devices with Group ID** Implies that the token holder is the sponsor.	**4** **User Set of Humans that has Group ID** Implies holder is sponsor or a set member**.**	**5** **User Set of Humans that has Shared ID** Implies that the token holder is a set member**.**
Human User	OK if holder is the same as the added person. Else, this case not supported.	This case is not supported.	This case is not supported.	OK if holder is the same as the added person. Else, this case not supported	OK if holder is the same as the added person. Else, this case not supported
User Device	This case is not supported.	OK if both have the same sponsor. Else, this case not supported	OK if both have the same sponsor. Else, this case not supported	This case is not supported.	This case is not supported.
User Set of Devices that has Group ID	This case is not supported.	OK if both have the same sponsor. Else, this case not supported	OK if both have the same sponsor. Else, this case not supported	This case is not supported.	This case is not supported.
User Set of Humans that has Group ID	OK if sponsor of the new set approves. Else, this case not supported	This case is not supported.	This case is not supported..	OK if sponsor of the new set approves. Else, this case not supported.	OK if sponsor of the new set approves. Else, this case not supported.
User Set of Humans that has Shared ID	OK if holder is a member of the added set Else, this case not supported	This case is not supported.	This case is not supported..	OK if holder is a member of the added set. Else, this case not supported.	OK if holder is a member of the added set. Else, this case not supported

UNCLASSIFIED//FOUO

3.3.8.2 (U) Hardware Token Identification

(U//FOUO) The KMI needs to be able to uniquely identify any tokens that it issues.

CI2-SEC-3.3.8.2a The KMI shall be capable of reading unique identification information from a Hardware Token, including the manufacturer and serial number. [KRD 1670] {C}

DEFINITION (U//FOUO) KMI Token Number (KT#). A KMI-unique value that the KMI associates with a Hardware token.

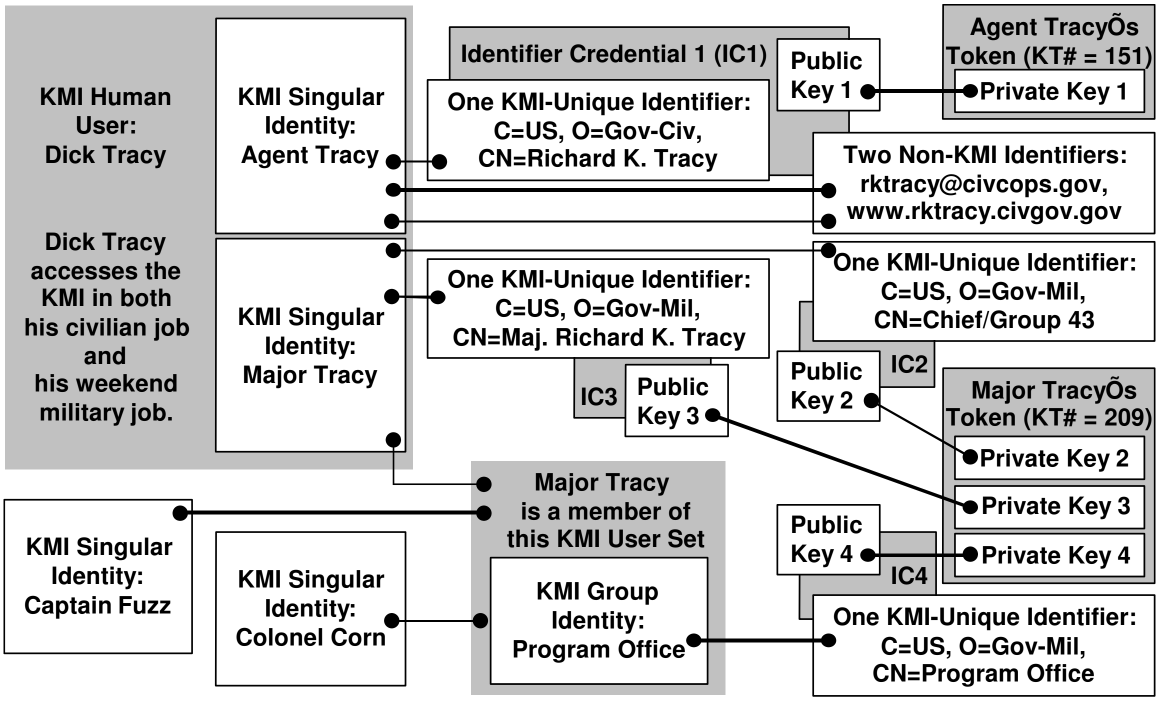
CI2-SEC-3.2.8.2b (U//FOUO) When the KMI issues a Hardware Token to a User Identity, the KMI shall associate the KT# of the token with that User Identity. [DRV KRD 1686] {R}

(U//FOUO) Depending on how the KMI is implemented, the KT# might only be used internally by KMI processes, or it might be known or used by some KMI users or by some non-KMI systems. In that case, an authorized KMI manager would control the KT# name space. However, implementation may require the KT# to be a composite of a common, KMI-assigned prefix and a manufacturer- or vendor-controlled internal or external serial number.

(U//FOUO) Figure 15 continues the example, which was begun in Figure 10, of the fictitious human user Dick Tracy. Figure 15 illustrates how a single hardware token (the one with KT# 209) may carry authentication material for multiple singular identities of a human user, and also for one or more group or shared identities of user sets to which an identity of the person belongs. However, when a token carries more than one unit of authentication material, care must be taken to maintain individual accountability.

(U//FOUO) In Figure 15, Dick Tracy has two hardware tokens. The token with KT# 151 carries authentication material (private key 1) for a KMI-unique identifier of the Agent Tracy identity. The second token, the one with KT# 209, carries authentication material (private key 2 and private key 3) for two KMI-unique identifiers of the Major Tracy identity. The second token also carries authentication material (private key 4) for a KMI-unique identifier of the "Program Office" identity of a user set to which Dick Tracy belongs.

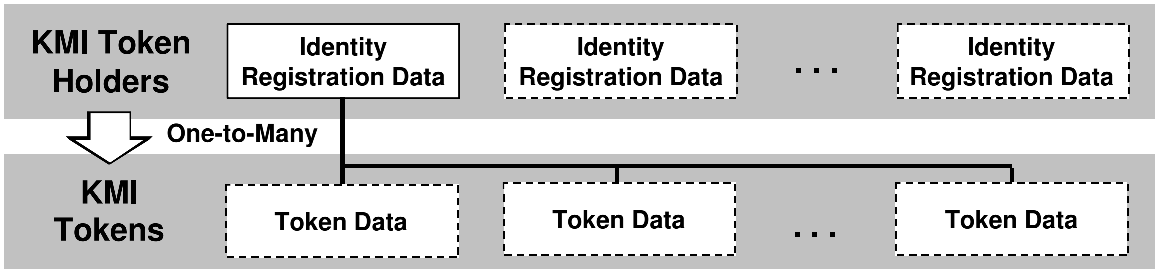
Figure 15. (U) KMI Hardware Token Example


KMI Human User: Dick Tracy
Dick Tracy accesses the KMI in both his civilian job and his weekend military job.
KMI Singular Identity: Agent Tracy
KMI Singular Identity: Major Tracy
Identifier Credential 1 (IC1)
One KMI-Unique Identifier: C=US, O=Gov-Civ, CN=Richard K. Tracy
Public Key 1
Agent TracyÕs Token (KT# = 151)
Private Key 1
Two Non-KMI Identifiers: rktracy@civcops.gov, www.rktracy.civgov.gov
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Chief/Group 43
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Maj. Richard K. Tracy
IC3
Public Key 3
Public Key 2
IC2
Major TracyÕs Token (KT# = 209)
Private Key 2
Private Key 3
Private Key 4
Major Tracy is a member of this KMI User Set
KMI Singular Identity: Captain Fuzz
KMI Singular Identity: Colonel Corn
KMI Group Identity: Program Office
Public Key 4
IC4
One KMI-Unique Identifier: C=US, O=Gov-Mil, CN=Program Office

3.3.9 (U) Hardware Token Data

(U//FOUO) Figure 16 illustrates that the KMI records data for each hardware token issued by the KMI.

Figure 16. (U) KMI Token Data


KMI Token Holders
Identity Registration Data
Identity Registration Data
. . .
Identity Registration Data
One-to-Many
KMI Tokens
Token Data
Token Data
. . .
Token Data

UNCLASSIFIED//FOUO

DEFINITION (U//FOUO) Token Data. The set of attribute values acquired by, and stored in, the system for the purpose of establishing and describing a Hardware Token.

CI2-SEC-3.3.9a The KMI shall be able to collect and record Token Data for Hardware Tokens it issues. [DRV KRD 1671] {C-R}

CI2-SEC-3.3.9b (U//FOUO) When the KMI associates Authentication Material or other security-sensitive information with a KMI-Unique User Identifier, and that information is to be carried by a Hardware Token that is issued by the KMI, then the KMI shall (1) ensure that the token's access protection mechanism is initialized, (2) shall determine the KT# of the token, and (3) shall record and retain that KT# and other associated Token Data. [DRV KRD 1670, 1675] {C-R}

CI2-SEC-3.3.9c (U//FOUO) When the KMI issues a Hardware Token to a Registered User, the KMI shall associate the token's KT# with the selected User Identity of the Human User who is to be the Token Holder. [DRV KRD 1580, 1686] {R}

CI2-SEC-3.3.9d (U//FOUO) The KMI shall provide the capability to identify all Identifier Credentials that are associated with a Hardware Token. [DRV KRD 1581, 1681] {R}

CI2-SEC-3.3.9e (U//FOUO) Token Data shall include at least the following attributes:

- The KT# of the token. [DRV KRD 1686] {R}
- The Token Holder's User Identity to which the token is issued. [DRV KRD 1580, 1686].
- Information that associates the token with Authentication Material, Identifier Credentials, and other security-sensitive information items that are placed on the token by the KMI. [DRV KRD 1672]
- The identification (e.g., issuer name and serial number) of all Identifier Credentials for which matching Authentication Material is held on the token. [DRV KRD 1681]
- [Additional data items are expected to be defined when a Component-level design is done.]

CI2-SEC-3.3.9f (U//FOUO) When recording Token Data, the KMI shall be able to record different types of attributes for different types of Hardware Tokens supported by the KMI. [DRV KRD 1589] {C-R}

CI2-SEC-3.3.9g [NT] (U//FOUO) The KMI shall ensure that all Token Data elements held in common with an External System with which the KMI interoperates share formats and allowable values for DoD personnel registrations. [DRV KRD 0243] {R}

3.3.10 (U) Protection of Hardware Tokens

POLICY (U//FOUO) The KMI must limit the potential for unauthorized use of Hardware Tokens, including when they are reported lost or compromised.

CI2-SEC-3.3.10a (U//FOUO) the KMI shall enable only authorized Managers to access stored Token Data. [KRD NEW] {R}

CI2-SEC-3.3.10b [NT] (U//FOUO) The KMI shall ensure that Hardware Tokens accepted by Components have mechanisms to protect the tokens from being used by a System Entity that physically possesses a token but is not authorized to use that token's computing capabilities or data content, such as the Authentication Material held on the token. [DRV KRD 0900] {X}

(U//FOUO) Self-protection of a hardware token could involve a password, biometrics, or other mechanism of sufficient robustness to control activation of, or access to, token functions. For example, a token might require a personal identification number (PIN) to be entered through a keypad on the token before authentication material held on the token can be used.

CI2-SEC-3.3.10c [NT] The KMI shall record for Audit each System Action that initializes or changes a Hardware Token's PIN or password. [DRV KRD 1698] {C}

CI2-SEC-3.3.10d (U//FOUO) The KMI shall support compromise management of Hardware Tokens it issues. [DRV KRD 1677] {R}

3.3.11 (U) Limits on Authentication Attempts

POLICY (U//FOUO) The KMI must limit the potential for unauthorized or incorrect attempts to access the KMI.

CONTROL (U//FOUO) **ECLO-2 Logon (Confidentiality)**. For Components that process classified information, "Successive logon attempts are controlled using one or more of the following:" [DoDI8500.2]

– "Access is denied after multiple unsuccessful logon attempts."
– "The number of access attempts in a given period is limited."
– "A time-delay control system is employed."

"If the system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon."

CONTROL (U//FOUO) **ECLO-1 Logon (Confidentiality)**. For Components that process sensitive information, "Successive logon attempts are controlled using one or more of the following:" [DoDI8500.2]

– "Access is denied after multiple unsuccessful logon attempts."
– "The number of access attempts in a given period is limited."
– "A time-delay control system is employed."

"If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon sessions."

(U//FOUO) This and other sections of this *Security Policy* state requirements that implement the ECLO controls.

CI2-SEC-3.3.11a (U//FOUO) In each Component that authenticates User Identities claimed by System Entities attempting to access the KMI as Registered Users, the KMI shall enable a Security Configuration Manager to set limits on the maximum number of consecutive unsuccessful authentication attempts permitted with a KMI-Unique User Identifier. [DRV KRD 0933] {Z}

CI2-SEC-3.3.11b (U//FOUO) Each Component that authenticates User Identities presented by System Entities attempting to access the KMI as Registered Users shall enforce set limits on the number of consecutive unsuccessful authentication attempts by a KMI-Unique User Identifier. [DRV KRD 0933] {Z}

CI2-SEC-3.3.11c (U//FOUO) When a KMI-Unique User Identifier exceeds a Component's set limit on the maximum number of consecutive unsuccessful authentication attempts, the KMI shall change the identifier's Registration State to Inactive. [DRV KRD 0934] {Z}

(U//FOUO) See "User Identifier States" section for information regarding changing the registration state of a user identifier from inactive to active.

3.4 (U) Data Origin Authentication Service

POLICY (U//FOUO) **General Policy on Data Origin Authentication**. When the KMI receives information, the KMI must authenticate the identity of the source so as to ensure that Components process and take action only on authentic inputs.

DEFINITION (U) Data Origin Authentication Service. A Security Service that verifies, to an entity that uses the service, the identity that is claimed to be the original source of data received by the entity.

(U//FOUO) KMI data origin authentication service protects against a false identity being claimed by a source of information that is handled in the KMI. This service is provided to any system entity that receives or holds the data. Unlike peer entity authentication service (see "Peer Entity Authentication Service" section), this service is independent of any communication association between the originator and recipient, and the data may have been originated at any time in the past. Also, this service depends on data integrity service because, if a received data unit has been changed, there can be no verification that the identity of the original source of the data is as claimed.

CI2-SEC-3.4a (U//FOUO) Components shall verify the origin and the integrity of data that they receive before using the data as input to any Security-Sensitive Function. [DRV KRD 1545, 1904] {Z}

CI2-SEC-3.4b (U//FOUO) The KMI shall provide data origin authentication service that enables Users to verify the source of products that are provided by the KMI. [DRV KRD 0941] {A-C-P-R-S}

CI2-SEC-3.4c (U//FOUO) The KMI shall provide data origin authentication service needed to support the creation and secure use of Audit Trails. [DRV KRD 1559] {Z}

3.5 (U) Peer-Entity Authentication Service

POLICY (U//FOUO) **General Policy on Peer-Entity Authentication.** When a Component communicates or otherwise interacts with other System Entities, the Component must authenticate the identity of those entities so as to ensure that the interaction is authentic.

DEFINITION (U) Peer-Entity Authentication Service. A Security Service that verifies an identity claimed by or for a System Entity in a Communication Association.

(U) This service is used at the establishment of, or at times during, a communication association to confirm the identity of one entity to another. Unlike data origin authentication service, this service requires that an association exists between the entities; and the corroboration provided by the service is valid only at the current time that the service is invoked.

(U//FOUO) In the KMI, peer-entity authentication services protect against a system entity masquerading as, or being mistaken for, another entity. In some cases, peer-entity authentication is achieved implicitly, perhaps based on fixed physical connections; in other cases, an explicit service is needed. (See use of this authentication service in a “Protected Channel” in “Internal Communication Services” section.)

CI2-SEC-3.5a (U//FOUO) The KMI shall provide peer-entity authentication service needed by Components and other System Entities to verify identities in KMI interactions. [DRV KRD 0862] {Z}

CI2-SEC-3.5b (U//FOUO) Each Independent Component shall uniquely identify and authenticate other Independent Components before permitting them to access its System Resources. [DRV KRD 0862] {Z}

(U//FOUO) The preceding requirement covers a wide range of situations and could be implemented by a wide range of mechanisms. For example, components that communicate via a switched network shared with others might authenticate each other with a cryptographic protocol; components that communicate via a dedicated link might authenticate each other by sharing a key that is used to encrypt the link; and components that are physically adjacent and directly connected within a common, protected environment could be implicitly authenticated to each other.

3.6 (U) Non-Repudiation Service

POLICY (U//FOUO) **General Policy on Non-Repudiation.** The KMI must implement non-repudiation services as required by law or by Government regulation.

(U//FOUO) Non-repudiation services protect against false denial of involvement in a communication or other interaction. There are two basic kinds of non-repudiation service:

> **DEFINITION** (U) Non-Repudiation with Proof of Origin. A security service that provides the recipient of data with evidence that can be retained and that proves the origin of the data, and thus protects the recipient against any subsequent attempt by the originator to falsely deny sending the data. (This service can be viewed as a stronger version of a data origin authentication service, because it can verify identity to a third party.)

> **DEFINITION** (U) Non-Repudiation with Proof of Receipt. A security service that provides the originator of data with evidence that can be retained and that proves the data was received as addressed, and thus protects the originator against a subsequent attempt by the recipient to falsely deny receiving the data.

(U) These services cannot prevent an entity from repudiating a communication. Instead, they provide evidence that can be stored and later presented to a third party to resolve disputes that arise if and when a communication is repudiated.

(U//FOUO) KMI customers may use KMI-issued credentials and other products to support non-repudiation services that the customers themselves implement, but CI-2 does not offer externally available non-repudiation services that are usable by customers. Instead, the KMI implements non-repudiation services only where they are needed to support its own internal operations.

> **CI2-SEC-3.6a** (U//FOUO) For a System Entity receiving data from a Component, the KMI shall provide, in instances specified elsewhere in the *System Description and Requirements Specification* [KMI2200], a service ("non-repudiation with proof of origin") that provides evidence that can be stored and later presented to a third party to enable the receiving entity to prove that the Component sent the data. [DRV KRD 0945] {P-R-S}

> **CI2-SEC-3.6b** (U//FOUO) For a System Entity sending data to a Component, the KMI shall provide, in instances specified elsewhere in the *System Description and Requirements Specification* [KMI2200], a service ("non-repudiation with proof of receipt") that provides evidence that can be stored and later presented to a third party to enable the sending entity to prove that the Component received the data. [DRV KRD 0944] {P-R-S}

3.7 (U) Access Control Service

POLICY (U//FOUO) **General Policy on Access Control.** The KMI must regulate access to its System Resources so that they are used only as authorized by applicable policies and doctrine, in accordance with the principle of "need to know".

> **DEFINITION** (U) Access. The ability and the means to communicate with, or otherwise interact with, a system's resources in order to either (1) handle data held by the system or (2) control system Components and their functions.

> **DEFINITION** (U) Handle. Perform processing operations on data, such as receive and transmit, collect and disseminate, create and delete, store and retrieve, read and write, and compare.

(U//FOUO) The KMI needs to restrict each system entity's access to only those system resources and actions for which the entity has been granted authorization.

> **DEFINITION** (U) Access Control. A service that protects against unauthorized Access to System Resources (including protecting against use of a System Resource in an unauthorized manner by a User that is authorized to use the resource in some other manner).

(U//FOUO) Access control processes for CI-2 are designed to satisfy the following general requirements:

> **CI2-SEC-3.7a** (U//FOUO) The KMI shall provide mechanisms and procedures to implement Access Controls for the hardware, software, information databases, operational and administrative functionality, and other System Resources of the KMI. [DRV KRD 1793] {Z}

> **CI2-SEC-3.7b** (U//FOUO) The KMI shall implement Access Control processes that limit Access to both externally and internally generated information in accordance with the need-to-know principle. [DRV KRD 1645] {Z}

(U//FOUO) The "Information Sensitivity" section states general policies and requirements for protecting externally and internally generated information.

> **CI2-SEC-3.7c** (U//FOUO) Each Independent Component shall incorporate Access Control processes to control the Access that other System Entities—whether part of KMI or not—have to its System Resources. [KRD 0592, 0846, 1546] {Z}

(U//FOUO) The foregoing requirement recognizes that some components need to control access to their resources not only by entities that are outside the KMI but also by entities inside the system, including by other components. Some inter-component access controls might be provided implicitly through the means by which communication paths are implemented, but others might be provided explicitly by registering remote components as user devices (see "Component Identities" section).

(U//FOUO) KMI grants several different types of access rights to registered users. In discussing access rights, this *Policy* uses the general term "authorization".

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

(U//FOUO) To manage authorizations, Volume 3 specifies three kinds of access control processes: role-based, rule-based, and approval-based. In specifying these processes, the *Architecture* uses additional terms to indicate that access rights are specifically associated with one type of process. For example, a "permission" is an authorization controlled by the role-based process (see "User Roles and Permissions" section of Volume 3).

CI2-SEC-3.7d The KMI shall record for Audit each request, assignment, receipt, modification, deletion, or rejection of an Authorization for a Registered User, User Identity, Role, or Component. [KRD 0071, 0876, 0844] {Z}

(U//FOUO) Role-based, rule-based, and approval-based access control processes are specified in the "Access Control" section of Volume 3. Also, the following applies to all KMI components accessed by human users.

CONTROL (U//FOUO) **PESL-1 Screen Lock (Integrity)**. "Unless there is an overriding technical or operational problem, a workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded)." [DoDI8500.2]

CI2-SEC-3.7e (U//FOUO) Each KMI workstation shall, after a configurable period of inactivity specified by an authorized Security Configuration Manager or upon user action, either (1) shut down completely or (2A) place an unclassified pattern onto its display, totally hiding what was previously visible there, and (2B) lock itself so that regaining access requires a user to have possession of a unique token or authentication information equivalent to that used for initial authentication. [KRD NEW] {Z}

3.8 (U) Information Confidentiality Service

POLICY (U//FOUO) **General Policy on Information Confidentiality.** The KMI must safeguard the information it handles so that the information is disclosed only to authorized System Entities to be used only for its intended purpose. (See related policies in "Information Protection Requirements" section.)

DEFINITION (U) Information Confidentiality Service. A security service that protects information from being disclosed or made available to unauthorized System Entities.

(U//FOUO) KMI confidentiality services protect information from disclosure to unauthorized persons or other system entities. The services directly protect information handled by the KMI, and also indirectly protect information that is protected through use of KMI products and services. (Also see confidentiality services specified by “Protected Channels” and “Rule-Based Access Control” sections of Volume 3.)

(U//FOUO) This service and the one defined in the next section, “Information Integrity Service”, are usually stated in terms of “data” rather than “information”. (Information is facts and ideas, which can be represented, i.e., encoded, as various forms of data. Data is information in a specific physical representation, usually a sequence of symbols that have meaning, especially a representation of information that can be processed or produced by a computer.) However, this *Policy* uses the term “information” to retain full generality and avoid implying any specific architecture or implementation.

(U//FOUO) The specific policies and associated requirements for information confidentiality service are as follows:

3.8.1 (U) Sensitivity to Disclosure

POLICY (U//FOUO) **Sensitivity to Disclosure.** The KMI must provide confidentiality services to information it handles, commensurate with the sensitivity of the information to unauthorized disclosure.

DEFINITION (U//FOUO) Sensitive Information. “Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code, “The Privacy Act” ... , but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of Title 15, United States Code, “The Computer Security Act of 1987” ... .) This includes information in routine DoD payroll, finance, logistics, and personnel management systems.” [DoDD 8500.1]

CI2-SEC-3.8.1a (U//FOUO) The KMI shall employ means to identify the confidentiality requirements of information that it handles. [DRV KRD 0840] {Z}

(U//FOUO) Related requirements are stated in the “Marking and Labeling” section.

(U//FOUO) When a KMI authentication process has verified the identity of a registered user that is attempting to access the system, and the user is either (1) a person or (2) a user set consisting of persons, the KMI needs to provide the user with notice of rights to personal privacy.

CI2-SEC-3.8.1b (U//FOUO) Prior to prompting Users for information covered by Section 552a of Title 5, United States Code (“The Privacy Act of 1974”), as amended, the KMI shall display an appropriate warning notice as required by the DoD Privacy Program [DoDD5400.11]. [DRV KRD 1543] {Z}

3.8.2 (U) Protection Against Disclosure

POLICY (U//FOUO) **Disclosure of Information.** The KMI must ensure that the information it handles is disclosed only to Registered Users that have authorization and a need to know.

CONTROL (U//FOUO) **ECAN-1 Access for Need-to-Know (Confidentiality)**. "Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access:" [DoDI8500.2]

1. "**Open access** to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction."
2. "**Controlled access** to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction."
3. "**Restricted access** to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions."

(U//FOUO) Several sections of this *Security Policy* and of Volume 3 state requirements that implement the ECAN-1 control. The general requirements for protection against unauthorized disclosure are as follows:

CI2-SEC-3.8.2a (U//FOUO) All information handled by the KMI, both classified and unclassified, that is sensitive to disclosure shall be protected by a confidentiality service of strength commensurate with (1) the sensitivity of the information to disclosure and (2) handling instructions associated with the information. [DRV KRD 0841] {Z}

CI2-SEC-3.8.2b (U//FOUO) All information handled by the KMI, both classified and unclassified, shall be protected by confidentiality services using security mechanisms that are appropriate for, and certified for, protection (1) at the information's level of sensitivity and (2) in the environment in which the information is handled. [DRV KRD 0860] {Z}

(U//FOUO) See "Security Robustness and Security Assurance" section and "Communications Security" section for additional requirements pertaining to confidentiality service and the mechanisms and equipment used to implement it.

CI2-SEC-3.8.2c (U//FOUO) The KMI shall be able to provide required confidentiality service to information that is (1) stored in Components, (2) transferred between Components, (3) transferred between the KMI and its Registered Users, or (4) released to a communication network. [DRV KRD 0842] {Z}

(U//FOUO) See "Protected Channels" section of Volume 3 for additional, detailed requirements pertaining to confidentiality service for KMI information transfers.

CI2-SEC-3.8.2d (U//FOUO) The KMI shall provide confidentiality protection for software if disclosure of the software would reveal classified information. [DRV KRD 0804] {Z}

CI2-SEC-3.8.2e (U//FOUO) Components that relay information that is sensitive to disclosure shall provide the information with confidentiality service that protects against disclosure to local Administrative Managers of the Components. [DRV KRD 0871] {Z}

CI2-SEC-3.8.2f (U//FOUO) The KMI shall ensure that keying material used to provide confidentiality service for KMI information is protected to at least the sensitivity level of the information being protected. [DRV KRD 0105, 1060] {Z}

CI2-SEC-3.8.2g (U//FOUO) When a Registered User accesses the KMI by invoking a User Identity and a Role to which the Identity is assigned, the KMI shall disclose information to the User only if authorized by the User Identity's attributes, the Role's Permissions, and other Authorizations associated with the assignment. [DRV KRD 0959] {C-R-S}

CI2-SEC-3.8.2h (U//FOUO) When a Registered User accesses the KMI by invoking a User Identity, the KMI shall disclose information to the User only if the access level of the User Identity dominates the sensitivity level of the information. [DRV KRD 0959] {C-R-S}

CI2-SEC-3.8.2i (U//FOUO) When the KMI is accessed by a System Entity that has not been authenticated as a Registered User, the KMI shall not disclose information to the entity unless the information has previously been designated for release to the public. [KRD 0931] {R}

(U//FOUO) The ECCR-3 control is not applicable to CI-2 because KMI does not handle Sources and Methods Intelligence.

CONTROL (U//FOUO) **ECCR-3 Encryption for Confidentiality (Data at Rest) (Confidentiality)**. [Not applicable to CI-2.] "If a <u>classified</u> enclave contains SAMI [Sources and Methods Intelligence] and is accessed by individuals lacking an appropriate clearance for SAMI, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave." [DoDI8500.2]

(U//FOUO) The ECCR-2 and ECCR-1 controls are not applicable to the KMI because the KMI owns all the information it contains.

CONTROL (U//FOUO) **ECCR-2 Encryption for Confidentiality (Data at Rest) (Confidentiality)**. [Not applicable to CI-2.] "If required by the information owner, NIST-certified cryptography is used to encrypt stored <u>classified</u> non-SAMI information." [DoDI8500.2]

CONTROL (U//FOUO) **ECCR-1 Encryption for Confidentiality (Data at Rest) (Confidentiality)**. [Not applicable to CI-2.] "If required by the information owner, NIST-certified cryptography is used to encrypt stored <u>sensitive</u> information." [DoDI8500.2]

(U//FOUO) The KMI uses NSA-approved cryptography for all internal functions, and the following requirements are applicable to all CI-2 components:

CI2-SEC-3.8.2j [NT] (U//FOUO) Cryptographic algorithms that are used by the KMI to provide information confidentiality service for Sensitive or classified information must be approved by NSA, and each specific application of such algorithms for that purpose within the KMI design must also be approved by NSA. [DRV KRD 2154] {Z}

CI2-SEC-3.8.2k [NT] (U//FOUO) Cryptographic equipment that is used by the KMI to provide information confidentiality service for Sensitive or classified information must be approved by NSA, and each specific application of such equipment for that purpose within the KMI design must also be approved by NSA. [DRV KRD 2155] {Z}

3.8.3 (U) Sanitization

POLICY (U//FOUO) **Sanitization of Information.** The KMI must be able to sanitize any Component upon command of an authorized Registered User.

CONTROL (U//FOUO) **ECRC-1 Resource Control (Confidentiality)**. "All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object." [DoDI8500.2]

(U//FOUO) The general requirements for information sanitization are as follows

CI2-SEC-3.8.3a (U//FOUO) The KMI shall provide means to destroy (i.e., delete, make unreadable)—(1) upon command from an authorized Manager, (2) in the event of a predefined condition specified by an authorized Manager, or (3) in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]—all classified information or other information (including cryptographic material) that is held in a Component and is sensitive to disclosure. [DRV KRD 0884, 0886, 0963] {Z}

CI2-SEC-3.8.3b (U//FOUO) The KMI shall provide means to securely destroy— in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]—all classified information or other information that is held in a Component's internal memory, external memory, magnetic media, or other storage media and is sensitive to disclosure. [DRV KRD 0810] {Z}

CI2-SEC-3.8.3c (U//FOUO) The KMI shall provide means to destroy KMI cryptographic material—i.e., material stored in a Component or otherwise held for use by the KMI—within a configurable interval of time after the end of the cryptographic period, as configured by an authorized Manager. [KRD 0965, 1994, 1995] {Z}

(U//FOUO) See "Zeroization and Data Destruction" section of Volume 1 for additional, more specific requirements regarding destruction of KMI products.

3.9 (U) Information Integrity Service

POLICY (U//FOUO) **General Policy on Information Integrity**. The KMI must safeguard the information it handles so that the information retains its content integrity.

DEFINITION (U) Information integrity. The property that ensures that information has not been changed, destroyed, or lost in an unauthorized or accidental manner. (This property is concerned with the constancy of data values, i.e., information content that is encoded in data, and not with how accurately the information was recorded or how trustworthy the information source was.)

DEFINITION (U) Information Integrity Service. A security service that protects against unauthorized changes to information—including both intentional and accidental change and destruction—by ensuring that such changes are detectable.

(U//FOUO) KMI information integrity services protect information from unauthorized change or destruction. The services directly protect information handled by the KMI, and also indirectly protect information that is protected by KMI products and services. (Also see integrity service specified by "Protected Channels" section of Volume 3.)

(U) Regardless of what causes a change in data, an integrity service can only detect the change and report it to an appropriate authority; changes cannot be totally prevented unless the system is perfect (error-free) and no malicious user has access. However, a system that offers data integrity service might also attempt to correct and recover from changes.

(U) **Relationship between information integrity and authentication services**: Although data integrity service is defined separately from data origin authentication service and peer entity authentication service, it is closely related to them. Authentication services depend, by definition, on companion data integrity services. Data origin authentication service provides verification that the identity of the original source of a received data unit is as claimed; there can be no such verification if the data unit has been altered. Peer entity authentication service provides verification that the identity of a peer entity in a current association is as claimed; there can be no such verification if the claimed identity has been altered.

(U//FOUO) The specific policies and associated requirements for information integrity service are as follows:

3.9.1 (U) Protection Against Modification

POLICY (U//FOUO) **Sensitivity to Modification.** The KMI must provide integrity services to information it handles, commensurate with the sensitivity of the information to modification, destruction, or loss.

POLICY (U//FOUO) **Authorization for Modification.** The KMI must ensure that the information it handles can be modified only by Users that have Authorizations to do so.

CONTROL (U//FOUO) **ECCD-2 Changes to Data (Integrity)**. For Components in MAC I and MAC II, and for Components that process classified information, "Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. Access and changes to the data are recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users are notified of time and date of the last change in data content." [DoDI8500.2]

(U//FOUO) Some requirements to implement the ECCD control are stated in the "Access Control" section of the *Security Architecture* [KMI23200V3]; the general requirements for protection against unauthorized modification of information are as follows:

CI2-SEC-3.9.1a (U//FOUO) All information handled by the KMI, both classified and unclassified, that is sensitive to modification shall be protected by Information Integrity Service of strength commensurate with (1) the sensitivity of the information to modification and (2) handling instructions associated with the information. [DRV KRD 0860] {Z}

CI2-SEC-3.9.1b (U//FOUO) All information handled by the KMI, both classified and unclassified, shall be protected by Information Integrity Service using security mechanisms appropriate for, and certified for, protection (1) at the information's level of sensitivity and (2) in the environment in which the information is handled. [DRV KRD 0860] {Z}

(U//FOUO) See "Security Robustness and Security Assurance" section and "Communications Security" section for additional requirements pertaining to integrity service and the mechanisms and equipment used to implement it.

CI2-SEC-3.9.1c (U//FOUO) The KMI shall be able to provide required integrity service to information that is (1) stored in Components, (2) being transferred between Components, (3) exchanged between the KMI and its Registered Users, or (4) released to a communication network. [DRV KRD 0931, 1779] {Z}

(U//FOUO) See "Protected Channels" section of Volume 3 for additional, detailed requirements pertaining to integrity service for KMI information transfers.

CI2-SEC-3.9.1d (U//FOUO) When a Registered User accesses the system by invoking a User Identity and a Role to which that identity has been assigned, the KMI shall permit the User to create, modify, or destroy information only if authorized by the User Identity's attributes, the Role's Permissions, and other Authorizations associated with the assignment. [DRV KRD 0860, 1289] {P-R-S}

CI2-SEC-3.9.1e (U//FOUO) The KMI shall preserve the integrity of information security mechanisms (e.g., labels, hash values, and digital signatures) that have been applied by sources from which the KMI receives information, and that are intended for use by Registered Users that consume the information. [DRV KRD 0968] {Z}

CI2-SEC-3.9.1f [NT] (U//FOUO) Cryptographic algorithms that are used by the KMI to provide Information Integrity Service for Sensitive or classified information must be approved by NSA, and each specific application of such algorithms for that purpose within the KMI design must also be approved by NSA. [DRV KRD 2154] {Z}

CI2-SEC-3.9.1g [NT] (U//FOUO) Cryptographic equipment that is used by the KMI to provide Information Integrity Service for Sensitive or classified information must be approved by NSA, and each specific application of such equipment for that purpose within the KMI design must also be approved by NSA. [DRV KRD 2155] {Z}

3.9.2 (U) Prevention and Detection

POLICY (U//FOUO) **Prevention and Detection of Information Modification.** The KMI must employ safeguards to detect and minimize inadvertent modification, destruction, or loss of information that is handled by the system, and to detect and, where possible, prevent malicious modification or destruction.

CI2-SEC-3.9.2a (U//FOUO) The KMI shall protect all sensitive information against any change or loss caused by an unauthorized action of a Registered User or other System Entity. [DRV KRD 1556] {Z}

CI2-SEC-3.9.2b (U//FOUO) The KMI shall protect all sensitive information against any change or loss caused by an authorized but unintentional (i.e., inadvertent or accidental) action of a Registered User or other System Entity. [DRV KRD 1556] {Z}

CI2-SEC-3.9.2c (U//FOUO) The KMI shall protect all sensitive information against any change or loss due to a natural occurrence, such as an electrical discharge, fire, flood, earthquake, or windstorm. [DRV KRD 1556] {Z}

CI2-SEC-3.9.2d (U//FOUO) The KMI shall be able to detect any unauthorized change or destruction, either intentional or accidental, of sensitive information. [DRV KRD 1557] {Z}

CI2-SEC-3.9.2e (U//FOUO) The KMI shall record for Audit any detected unauthorized change or destruction, either intentional or accidental, of sensitive information. [DRV KRD 1557] {Z}

CI2-SEC-3.9.2f (U//FOUO) The KMI shall record as a Mandatory Audit Event each failure of an Information Integrity test performed by an application Component. [KRD 0420, 0560] {Z}

3.9.3 (U) Restoration of Information

POLICY (U//FOUO) **Restoration of Information.** The KMI must employ means to restore information that has been changed or destroyed in an unauthorized manner.

(U//FOUO) The KMI needs to be able to create a backup copy of information stored in system components (i.e., make a reserve copy that is stored separately from the original), and to use that copy to recover from loss or failure of components or other unauthorized modification or destruction of the information.

CONTROL [NT] (U//FOUO) **CODB-3 Data Backup Procedures (Availability)**. For Components in MAC I, “Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation[DoDI8500.2]"

CONTROL [NT] (U//FOUO) **CODB-2 Data Back-up Procedures (Availability)**. For Components in MAC II, "Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level." [DoDI8500.2]

(U//FOUO) This and other sections of this *Security Policy* state requirements that implement the CODB controls. The general requirements for restoration of information are as follows:

CI2-SEC-3.9.3a (U//FOUO) Each Independent Component shall enable a Backup Manager (1) to cause the Component to create—either periodically according to schedules in KMI contingency plans, or on demand—a backup copy of operationally necessary information held by the Component and (2) to maintain the backup copy for use if the original information becomes damaged or destroyed. [DRV KRD 0099, 1105] {Z}

CI2-SEC-3.9.3b (U//FOUO) Each Independent Component shall provide means to create full backup copies of operationally necessary information and also incremental backups. [DRV KRD 1881] {Z}

CI2-SEC-3.9.3c (U//FOUO) Each Independent Component shall automate information backup operations and make them transparent to (i.e., hidden from, not evident to) Users. [DRV KRD 1175, 1891] {Z}

CI2-SEC-3.9.3d (U//FOUO) Each Independent Component shall enable a Backup Manager to restore information from a backup copy. [DRV KRD 1892] {Z}

CI2-SEC-3.9.3e (U//FOUO) The KMI shall provide Information Integrity Service for backup copies of KMI information. [DRV KRD 1893] {Z}

CI2-SEC-3.9.3f (U//FOUO) Each Independent Component shall enable a Backup Manager to use backup copies to complete the restoration of information held by the Component, within four hours of initiating restoration operations. [DRV KRD 0100, 1106, 1165, 1354, 1892] {Z}

CI2-SEC-3.9.3g (U//FOUO) During restoration of KMI information from a backup copy, the KMI shall ensure that the information is restored in its entirety from the most recent backup copy, unless a Backup Manager directs that an older copy should be used. [DRV KRD 1894] {Z}

CI2-SEC-3.9.3h (U//FOUO) During restoration of KMI information from a backup copy, the KMI shall verify the integrity of the backup copy. [DRV KRD 1894] {Z}

CI2-SEC-3.9.3i (U//FOUO) Each Component that supports backup and recovery shall include appropriate drivers for the storage and back-up mechanisms it uses. [DRV KRD 2110] {Z}

(U//FOUO) The following control is implemented by function-specific requirements that are stated in Volume 1:

CONTROL (U//FOUO) **ECDC-1 Data Change Controls (Integrity)**. "Transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction roll-back and transaction journaling, or technical equivalents." [DoDI8500.2]

3.10 (U) System Integrity and Availability Service

POLICY (U//FOUO) **General Policy on System Integrity**. The KMI must safeguard system Components at all times so that they continue to perform their functions as intended, in an unimpaired manner and free from unauthorized change.

DEFINITION (U//FOUO) System Integrity. The quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

DEFINITION (U//FOUO) System Integrity Service. A security service that protects system Components in a verifiable manner against unauthorized change throughout their lifetime.

(U//FOUO) KMI system integrity service protects functionality against unauthorized change, either malicious or accidental, throughout the KMI's life cycle; and all other security services described in this *Policy* depend on system integrity for their proper functioning. Unauthorized change includes any unauthorized introduction, modification, manipulation, tampering, removal, or destruction of a KMI component during development, distribution, implementation, or operation of the system. Changes include those made by designers, developers, maintainers, vendors, administrators, users, adversaries, and all other entities that have access to KMI system resources.

(U//FOUO) KMI system availability services are a subset of system integrity services, and they protect system resources against anything malicious or accidental that could cause unauthorized denial of KMI products and services.

DEFINITION (U) Availability Service. A security service that ensures that a system is accessible and usable upon demand by an authorized User.

DEFINITION (U) Denial of Service. The intentional or unintentional prevention of authorized access to System Resources or delaying of time-critical operations.

(U//FOUO) System integrity service has both static and dynamic aspects. This section addresses the dynamic aspects; static aspects are addressed in the "Configuration Control" section. This section focuses on integrity of security services and availability of system services. Policies and requirements in the "Information Protection Requirements" section and "Attack Sensing, Warning, and Response Service" section also support dynamic aspects of system integrity.

CI2-SEC-3.10a (U//FOUO) The KMI shall be designed to protect the System Integrity of both the configuration and operation of its Components. [DRV KRD 0835] {Z}

CI2-SEC-3.10b (U//FOUO) Each Computer Platform shall be able to check the System Integrity of its software and data configuration during the operation of that platform, in order to detect unauthorized changes in the configuration. [DRV KRD 1019] {Z}

CI2-SEC-3.10c (U//FOUO) Each Computer Platform of a Node, or Independent Component of a Node, that has a Monitoring Zone shall be able to report the results of its System Integrity check to a Monitoring Zone. [DRV KRD 1019] {Z}

(U//FOUO) Volume 3 describes the Monitoring Zones.

CI2-SEC-3.10d (U//FOUO) The KMI shall provide alternate (i.e., backup) means to permit performance of critical system functions despite damage to System Resources. [DRV KRD 0062] {Z}

CI2-SEC-3.10e (U//FOUO) KMI mechanisms used (1) to detect loss of System Integrity or (2) to restore System Integrity shall not degrade system security. [DRV KRD 1297] {Z}

3.10.1 (U) Integrity of Security Services

(U//FOUO) KMI security services and their implementing mechanisms need to be in operation at all times, and any failure of those services or mechanisms needs to be reported to appropriate managers.

CONTROL (U//FOUO) **DCSS-2 System State Changes (Integrity)**. “System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. Tests are provided and periodically run to ensure the integrity of the system state.” [DoDI8500.2]

(U//FOUO) Integrity for security services in general, and the DCSS-2 control in particular, are implemented by the following requirements:

CI2-SEC-3.10.1a (U//FOUO) Each Independent Component shall be placed in an initial secure state following either power-up or error recovery, in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC], and shall be placed in a secure state prior to transition to an off state when the operator initiates such a transition. [DRV KRD 0856, 2123] {Z}

CI2-SEC-3.10.1b (U//FOUO) Each Component shall implement tamper protection mechanisms consistent with (1) the Site where it will operate, (2) the value of the keys and data processed by the Component, (3) the functionality of the Component, (4) the threat to the Component, and (5) the highest classification level of key material or other data that will be handled by the Component. [DRV KRD 0913] {Z}

CI2-SEC-3.10.1c (U//FOUO) The KMI shall periodically scan Component configurations to ensure that security services are still in place. [DRV KRD 1839] {Z}

CI2-SEC-3.10.1d (U//FOUO The KMI shall enable a Security Configuration Manager to set the periodicity of security configuration scans of Components. [DRV KRD 1840] {Z}

CI2-SEC-3.10.1e (U//FOUO) The KMI shall verify that security monitoring actions are performed by authorized Administrative Managers on a periodic basis as specified by a Security Configuration Manager. [KRD 0974] {Z}

CI2-SEC-3.10.1f (U//FOUO) The KMI shall notify an Incident Response Manager if KMI security monitoring actions are not performed by Administrative Managers within specified timeframes. [KRD 0975] {Z}

CI2-SEC-3.10.1g (U//FOUO) The KMI shall notify an Incident Response Manager of any detected security failure or violation of security policy. [DRV KRD 0155, 0978] {Z}

CI2-SEC-3.10.1h (U//FOUO) KMI Nodes—the CSN, PSNs, PRSNs, and Clients—and the EKMS Translator, and their Independent Components, that perform Security-Sensitive functions shall meet the requirements of the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]. [DRV KRD 2124] {Z}

3.10.2 (U) Availability of System Services

(U//FOUO) KMI system resources need to be protected at all times against unauthorized actions and adverse events and conditions that could render the system unable to serve authorized users, by either loss or degradation of operational availability. The general requirements for availability are as follows:

CI2-SEC-3.10.2a (U//FOUO) The KMI shall be designed to maintain continuity of operations (i.e., continue mission-essential functions without unacceptable interruption) in accordance with DoD Directive *Defense Continuity Program (DCP)*, 8 September 2004. [DRV KRD 1154] {Z}

CI2-SEC-3.10.2b (U//FOUO) The KMI shall be designed to resist and continue to operate in the event of denial-of-service attacks and other actions, events, and conditions that could deny service to Registered Users. [DRV KRD 0127] {Z}

CI2-SEC-3.10.2c (U//FOUO) KMI system functions that have real-time response requirements shall automatically and securely switch to backup Components in the event of failure of their primary Components. [DRV KRD 0127, 1297] {Z}

(U//FOUO) This volume does not state requirements to implement the following non-technical controls, which support system availability:

CONTROL [NT] (U//FOUO) **COMS-2 Maintenance Support (Availability)**. "Maintenance support for key IT assets is available to respond 24-by-7 immediately upon failure." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **COPS-3 Power Supply (Availability)**. For Components in MAC I, "Electrical systems are configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **COPS-2 Power Supply (Availability)**. For Components in MAC II, "Electrical systems are configured to allow continuous or uninterrupted power to key IT assets. This may include an uninterrupted power supply coupled with emergency generators."

CONTROL [NT] (U//FOUO) **COSP-2 Spares and Parts (Availability)**. For Components in MAC I, "Maintenance spares and spare parts for key IT assets are available 24 x 7 immediately upon failure." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **COSP-1 Spares and Parts (Availability)**. For Components in MAC II, "Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **COSW-1 Backup Copies of Critical SW (Availability)**. "Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software." [DoDI8500.2]

3.10.3 (U) Detection of Failure Conditions

(U//FOUO) The KMI needs to be able to detect system failures, including loss of secure state. The requirements for detection of failures are as follows:

CI2-SEC-3.10.3a (U//FOUO) Each Component shall be able to detect hardware and software errors when handling data, in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]. [DRV KRD 0859] {Z}

CI2-SEC-3.10.3b (U//FOUO) Each Component shall perform self-tests (1) at startup, (2) periodically during operation, (3) prior to resuming operation after a failure, and (4) upon command of an authorized Administrative Manager. [DRV KRD 1882] {Z}

CI2-SEC-3.10.3c (U//FOUO) KMI self-tests shall validate that all Components are operating within specified parameter values. [DRV KRD 1887] {Z}

CI2-SEC-3.10.3d (U//FOUO) KMI self-tests shall validate that all security mechanisms and services are operating as specified. [DRV KRD 1886] {Z}

CI2-SEC-3.10.3e (U//FOUO) KMI self-tests shall validate the correct operation of security mechanisms on (1) a periodic basis and (2) in certain pre-determined circumstances, in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]. [DRV KRD 0833, 0971] {Z}

CI2-SEC-3.10.3f (U//FOUO) KMI self-tests shall periodically verify that all KMI security-sensitive functions are operating correctly, in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]. [DRV KRD 0883] {Z}

CI2-SEC-3.10.3g (U//FOUO) The KMI shall enable a Security Configuration Manager to specify the periodicity of self-tests in each Component. [DRV KRD 1883] {Z}

CI2-SEC-3.10.3h (U//FOUO) The maximum time between self-tests of a Component shall be 24 hours. [DRV KRD 1884] {Z}

CI2-SEC-3.10.3i (U//FOUO) The KMI shall enable a Security Configuration Manager to select start times for periodic tests within the bounds determined by other requirements when it is impractical for start times to be fully automated. [DRV KRD 0972] {Z}

CI2-SEC-3.10.3j (U//FOUO) KMI self-tests, once initiated, shall execute to completion without interruption, unless interrupted by higher-priority security conditions. [DRV KRD 1888] {Z}

CI2-SEC-3.10.3k (U//FOUO) The KMI shall summarize and report the results of a self-test to an authorized Administrative Manager either (1) upon command or (2) in the event of a failure of the test. [DRV KRD 1885] {Z}

CI2-SEC-3.10.3l (U//FOUO) The KMI shall enable a Security Configuration Manager to set parameters, consistent with other security requirements, for a self-test to declare a failure. [DRV KRD 1558] {Z}

CI2-SEC-3.10.3m (U//FOUO) The KMI shall determine the nature and source of system failures and prepare a report for authorized Operational and Administrative Managers. [DRV KRD 1890] {Z}

CI2-SEC-3.10.3n (U//FOUO) The KMI shall determine the nature and source of security-sensitive system failures (i.e., failures that could change the security state of a Component or could violate a security policy) and prepare a report for authorized Administrative Managers. [DRV KRD 0988] {Z}

CI2-SEC-3.10.3o (U//FOUO) The KMI shall record for Audit each detected failure of a system Component or failure of a System Integrity test. [DRV KRD 0420, 0560] {Z}

3.10.4 (U) Detection of Denial of Service

(U//FOUO) The KMI needs to be able to detect actions, events, and conditions that affect the system and its interfaces in ways that could deny service to authorized users. The requirements for detection of denial of service are as follows:

CI2-SEC-3.10.4a (U//FOUO) The KMI shall attempt to detect and report to authorized Administrative Managers any unauthorized actions, events, or conditions that could deny service to Registered Users. [DRV KRD 0153] {Z}

CI2-SEC-3.10.4b (U//FOUO) The KMI must capture, maintain, and analyze information on workload capacity, and also forecast future workload, for the purpose of anticipating both authorized (i.e., crisis) and unauthorized (i.e., flooding) service demands that could overload the system and deny service to Registered Users. [DRV KRD 1107] {P-R-S}

CI2-SEC-3.10.4c (U//FOUO) The KMI shall notify an Incident Response Manager of any shutdown of an Independent Component or other major Component of a PRSN, PSN, CSN, or Translator and shall identify a shutdown as unauthorized or unexpected in cases where such identification is possible. [DRV KRD 1799] {Z}

CI2-SEC-3.10.4d (U//FOUO) The KMI shall perform self-tests to determine the cause of any security-related denial of service and prepare a report for an Incident Response Manager. [DRV KRD 1885] {Z}

CI2-SEC-3.10.4e (U//FOUO) All Nodes and Independent Components of Nodes shall incorporate means, including intrusion detection systems and boundary protection systems, to detect and react to denial-of-service attacks, and shall support denial-of-service contingency plans. [DRV KRD 0153] {Z}

(U//FOUO) Intrusion detection is discussed in this volume in the “Attack Sensing, Warning, and Response Service” section, and boundary protection is discussed in Volume 3 in the “Perimeter Defense” section.

3.10.5 (U) Fail-Safe Security Behavior

(U//FOUO) The KMI needs to minimize the extent to which a failure of any component affects the security of the overall system. The general requirements for fail-safe behavior are as follows:

CI2-SEC-3.10.5a (U//FOUO) Component failures shall result in the KMI entering a defined and restricted secure state rather than an indeterminate or insecure state. [DRV KRD 0977] {Z}

CI2-SEC-3.10.5b (U//FOUO) The KMI shall ensure that any Component failure or discontinuity within a Component does not cause a violation of the security policy, in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]. [KRD 0857] {Z}

CI2-SEC-3.10.5c (U//FOUO) In the event of detection of a failure of a security mechanism, the KMI shall handle the condition in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]. [KRD 0978] {Z}

CI2-SEC-3.10.5d (U//FOUO) Each newly developed Independent Component shall be designed in accordance with the Fail Safe Design Analysis process [NSAC02-00], as is applicable to the Component. [DRV KRD 0858] {Z}

3.10.6 (U) Degraded Operation

(U//FOUO) KMI managers need to be informed of any detected loss of secure state, and to be able to inhibit system operation until a secure state has been restored. The requirements for degraded operation are as follows:

CI2-SEC-3.10.6a (U//FOUO) If the KMI detects a failure of a security mechanism or security service that might cause certain operations to result in a violation of security policy, the KMI shall be able to automatically disable those operations. [REV KRD 1341] {Z}

CI2-SEC-3.10.6b (U//FOUO) The KMI (1) shall enable an authorized Administrative Manager to override, under two-person integrity, the automatic restriction or disabling of operations where such override will not result in a security violation, in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC] and in accordance with any other security requirements that are applicable to the KMI, and (2) shall record as a Mandatory Audit Event any such override. [DRV KRD 0979] {Z}

CI2-SEC-3.10.6c (U//FOUO) If the KMI detects a failure of a security mechanism or service, or detects a loss of secure state, the KMI shall notify Incident Response Manager and other appropriate Administrative Managers of the event, if security conditions allow such notification without additional compromise. [DRV KRD 1342] {Z}

CI2-SEC-3.10.6d (U//FOUO) If the KMI detects (1) a failure of a security mechanism or service, (2) a loss of secure state, or (3) a denial of KMI service, the KMI shall enable authorized Administrative Managers to restrict operations (including excising portions of the system) in order to contain the effect of the failure, loss, or denial while allowing continued KMI operation at a degraded level, so long as the restrictions do not rely on security mechanisms that are not functioning properly. [DRV KRD 0983] {Z}

3.10.7 (U) Restoration of System Integrity

(U//FOUO) KMI managers need to be able to restore system integrity after a system failure or system damage. The requirements for restoration of system integrity are as follows:

CI2-SEC-3.10.7a (U//FOUO) The KMI shall enable authorized Administrative Managers to restore the operational integrity of the overall system in case of failure, damage, or complete loss or destruction of one or more Nodes, Components, or Sites. [DRV KRD 1300] {Z}

CI2-SEC-3.10.7b (U//FOUO) The KMI shall enable authorized Administrative Managers to restore the operational integrity of the overall system (i.e., the KMI) following failure, damage, or complete loss or destruction of another (i.e., non-KMI) key management system or other External System that interoperates with the KMI. [DRV KRD 1115] {Z}

CI2-SEC-3.10.7c (U//FOUO) The KMI shall enable authorized Administrative Managers to restore the operational integrity of a failed Node, Component, or Site following repair of that part of the system. [DRV KRD 1354] {Z}

CI2-SEC-3.10.7d (U//FOUO) To the maximum extent possible, system functions for restoring operational integrity shall be transparent to (i.e., hidden from, not evident to) Users. [DRV KRD 1297] {Z}

CI2-SEC-3.10.7e (U//FOUO) The KMI shall enable authorized Administrative Managers to use backed-up data to assist in system recovery. [KRD 1106] {Z}

CI2-SEC-3.10.7f (U//FOUO) A Component shall not be returned to a fully operational, mission-capable state until its Audit capability is restored. [KRD 0118] {Z}

CI2-SEC-3.10.7g (U//FOUO) A Component shall not be returned to a fully operational mission-capable state until its ASWR capability is restored. [DRV KRD 1845] {Z}

(U//FOUO) This volume does not state requirements to implement the COBR-1 control, which supports restoration of system integrity:

CONTROL [NT] (U//FOUO) **COBR-1 Protection of Backup and Restoration Assets (Availability)**. "Procedures are in place [to] assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software." [DoDI8500.2]

3.10.8 (U) Restoration of Secure State

(U//FOUO) KMI managers need to be able to restore system security services after a loss of secure state.

CONTROL (U//FOUO) **COTR-1 Trusted Recovery (Availability)**. "Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place." [DoDI8500.2]

(U//FOUO) The requirements to implement the COTR-1 control are as follows:

CI2-SEC-3.10.8a (U//FOUO) The KMI shall enable authorized administrative Managers to restore the overall system to a secure state from an insecure state that was caused by failure, damage, complete loss or destruction, or compromise of one more Nodes, Components, or Sites. [DRV KRD 0984] {Z}

CI2-SEC-3.10.8b (U//FOUO) The KMI shall enable authorized Administrative Managers to restore the overall system (i.e., the KMI) to a secure state from an insecure state that was caused by compromise of another (i.e., non-KMI) key management system or other External System that interoperates with the KMI. [REV KRD 1115] {Z}

CI2-SEC-3.10.8c (U//FOUO) The KMI shall enable authorized Administrative Managers to restore a Node, Component, or Site to a secure state from an insecure state after a compromise of that part of the system. [REV KRD 0066] {Z}

CI2-SEC-3.10.8d (U//FOUO) Prior to resuming operation of any functionality after restoration of secure state from an insecure state, the KMI shall perform and successfully pass self-tests in accordance with the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC], and shall notify an authorized SSO of the results of the tests. [DRV KRD 0985] {Z}

CI2-SEC-3.10.8e (U//FOUO) The KMI shall implement processes for recovery from security compromise and make the processes available to Operational and Administrative Managers, and to KOA Agents, as appropriate for each type of User. [KRD 0830] {Z}

CI2-SEC-3.10.8f (U//FOUO) The KMI shall provide means to support rapid recovery from compromises of KMI internal keys. [DRV KRD 0285] {Z}

3.10.9 (U) Restoration of System Availability

(U//FOUO) KMI managers need to be able to restore availability of products and services that have been denied to users in an unauthorized manner.

CONTROL [NT] (U//FOUO) **COAS-2 Alternate Site Designation (Availability)**. "An alternate site is identified that permits the restoration of all mission or business essential functions." [DoDI8500.2] [See KRD 0061, 0109]

CONTROL (U//FOUO) **COEB-2 Enclave Boundary Defense (Availability)**. "Enclave boundary defense at the alternate site [as mentioned in COAS-2] must be configured identically to that of the primary site." [DoDI8500.2] (See Volume 3 regarding Boundary Protection Suites for enclaves.)

(U//FOUO) The general requirements for restoration of system availability are as follows:

CI2-SEC-3.10.9a [NT] (U//FOUO) KMI contingency plans shall ensure continued support for Registered Users while inoperative Nodes, Components, and Sites are repaired or replaced. [DRV KRD 1300] {Z}

CI2-SEC-3.10.9b (U//FOUO) The KMI shall enable authorized Managers to restore availability of system products and services for Registered Users after failure, damage, complete loss or destruction, or compromise of one or more Nodes, Components, or Sites. [DRV KRD 1300] {Z}

CI2-SEC-3.10.9c [NT] (U//FOUO) The KMI shall use techniques such as local, regional, and remote backup capabilities to provide continuous support for missions of Registered Users. [DRV KRD 0061] {P-R-S}

CI2-SEC-3.10.9d (U//FOUO) Each Site shall be able to act as a backup for other, equivalent Sites; and Sites that are in MAC I shall have automated cutover capabilities that can ensure uninterrupted service to Registered Users. [DRV KRD 0109] {P-R-S}

3.10.10 (U) Contingency Planning

POLICY (U//FOUO) **Policy on Contingency Planning.** The KMI must have in place and periodically test contingency plans for the system to perform its functions in abnormal operating conditions and to restore its functions in the event of system failures.

(U//FOUO) Successful implementation requires that each KMI site and each independent KMI component have a contingency plan to provide for continuation of service. Persons responsible for operation and administration of sites plan how to perform their mission and recover from the loss of existing component support, whether the loss is due to the inability of the specific component to function or a general system failure. To be effective, site contingency plans, which might involve backup systems, need to be carefully developed, thoroughly tested, and continuously maintained. The level of detail and the complexity of the plans need to be consistent with the value and criticality of the site's components and functions.

(U//FOUO) This *Specification* does not include requirements to implement the following non-technical controls, which support contingency planning:

CONTROL [NT] (U//FOUO) **COEF-2 Identification of Essential Functions (Availability)**. "Mission and business-essential functions are identified for priority restoration planning along with all assets supporting mission or business-essential functions (e.g., computer-based services, data and applications, communications, physical infrastructure)." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **VIIR-2 Incident Response Planning (Availability)**. For Components in MAC I, "An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least every 6 months." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **VIIR-1 Incident Response Planning (Availability)**. For Components in MAC II, "An incident response plan exists that identifies the responsible [Computer Network Defense] Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **CODP-3 Disaster and Recovery Planning (Availability)**. For Components in MAC I, "A disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.) [DoDI8500.2]"

CONTROL [NT] (U//FOUO) **CODP-2 Disaster and Recovery Planning (Availability).** For Components in MAC II, "A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.) [DoDI8500.2]"

CONTROL [NT] (U//FOUO) **COED-2 Scheduled Exercises and Drills (Availability)**. For Components in MAC I, "The continuity of operations or disaster recovery plans or significant portions are exercised semi-annually." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **COED-1 Scheduled Exercises and Drills (Availability)**. For Components in MAC II, "The continuity of operations or disaster recovery plans are exercised annually." [DoDI8500.2]

3.11 (U) Audit Service

POLICY (U//FOUO) **General Policy on Audit**. The KMI must record audit trail data concerning Security Sensitive Events and Security Sensitive Functions, and must periodically analyze the data.

CONTROL (U//FOUO) **ECAT-2 Audit Trail, Monitoring, Analysis and Reporting (Integrity)**. For Components in MAC I and MAC II, and for Components that process classified information, "An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **ECAT-1** [NT] **Audit Trail, Monitoring, Analysis and Reporting (Integrity)**. For Components that process sensitive information, "Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures." [DoDI8500.2]

(U//FOUO) Both MAC I and MAC II require ECAT-2, and all components of Core Nodes are in either MAC I or MAC II. Therefore, ECAT-1 applies only to client nodes that are in MAC III.

(U//FOUO) This volume uses the following definitions to interpret the ECAT controls and to state requirements for audit service [NCSCTG1, NCSCTG4]:

DEFINITION (U) Security-Sensitive Event. An event that attempts to change the security state of a Component or attempts to violate the KMI *Security Policy*.

DEFINITION (U) Security-Sensitive Function. A system function that must operate correctly in order to ensure adherence to the KMI *Security Policy*.

DEFINITION (U) Audit. A security service that performs an independent review and examination of records of system activities to find security violations.

DEFINITION (U//FOUO) Audit Event. A System Event that has been determined to have sufficient security relevance to require that data be recorded for audit purposes.

DEFINITION (U//FOUO) Audit Trail. A chronological set of data records describing Audit Events that is sufficient to enable reconstruction and examination, from inception to final result, of the sequence of environments and states surrounding or leading to an event of interest.

DEFINITION (U//FOUO) Mandatory Audit Event. An Audit Event that a Component always records in the Audit Trail.

DEFINITION (U//FOUO) Discretionary Audit Event. An Audit Event that a Component records in the Audit Trail unless an authorized Manager directs that it should not be recorded.

(U//FOUO) KMI audit service, when complemented by authentication services, provides a basis for (1) establishing individual accountability, (2) detecting security violations, and, if violations should occur, (3) investigating them to determine cause, scope of harm, and responsibility.

3.11.1 (U) Audit Trail Creation

(U//FOUO) This section states basic requirements for creating an audit trail that apply to system components in general.

CI2-SEC-3.11.1a [NT] (U//FOUO) KMI Component-level specifications shall identify all Audit Events within the system. [DRV KRD 0990] {Z}

CI2-SEC-3.11.1b (U//FOUO) The KMI shall produce Audit Trails that record system events that have been identified as Audit Events. [DRV KRD 0990] {Z}

CI2-SEC-3.11.1c (U//FOUO) Each Independent Component shall be able to create an Audit Trail that records Audit Events. [DRV KRD 0120, 0990] {Z}

CI2-SEC-3.11.1d (U//FOUO) The KMI shall ensure that only authorized Audit processes can collect data for, or write to, an Audit Trail. [DRV KRD 1805] {Z}

CI2-SEC-3.11.1e (U//FOUO) Each Component shall activate its Audit processes—(1) at startup and (2) immediately after any restoration operation—before activating KMI production processes. [DRV KRD 0069, 0118] {Z}f

CI2-SEC-3.11.1f (U//FOUO) Audit Trail collection and recording processes shall remain active and available in all KMI operational states. [KRD 0069, 0991] {Z}

CI2-SEC-3.11.1g (U//FOUO) The KMI shall automate Audit Trail collection, making it transparent to (i.e., hidden from, not evident to) Users. [DRV KRD 1175] {Z}

3.11.2 (U) Audit Trail Content, General

(U//FOUO) This section states general requirements for the information that needs to be recorded in an audit trail.

CI2-SEC-3.11.2a (U//FOUO) Audit processes shall support both Mandatory Audit Events and Discretionary Audit Events. [DRV KRD 1002] {Z}

CI2-SEC-3.11.2b (U//FOUO) Each Component shall record all Mandatory Audit Events at all times. [DRV KRD 1003] {Z}

CI2-SEC-3.11.2c (U//FOUO) The KMI shall treat all Audit Events as Mandatory Audit Events, except those designated as Discretionary Audit Events. [DRV KRD 1008] {Z}

CI2-SEC-3.11.2d [NT] (U//FOUO) The KMI design shall specifically identify the Audit Events that are Discretionary Audit Events. [DRV KRD 1009.] {Z}

CI2-SEC-3.11.2e (U//FOUO) A Component or Computer Platform shall enable an authorized Audit Data Manager, and only an Audit Data Manager, to turn on and turn off the recording of Discretionary Audit Events. [DRV KRD 1004, 1006] {Z}

CI2-SEC-3.11.2f (U//FOUO) The KMI shall record as a Mandatory Audit Event each action of an Audit Data Manager that turns on or off the recording of Discretionary Audit Events. [DRV KRD 1007] {Z}

CI2-SEC-3.11.2r (U//FOUO) The KMI shall treat as a Mandatory Audit Event each action of a System Security Officer that involves a Security-Sensitive Function. [KRD 1007] {Z}

CI2-SEC-3.11.2g (U//FOUO) The KMI shall record for Audit each Discretionary Audit Event unless an authorized Audit Data Manager directs that it should not be recorded. [DRV KRD 1005, 1013] {Z}

CI2-SEC-3.11.2h (U//FOUO) The KMI shall ensure that the User Identity of any responsible User and the User Identities of any other involved Users are bound to each Audit Event record in the Audit Trail. [DRV KRD 0684, 1014] {Z}

CI2-SEC-3.11.2i (U//FOUO) In an Audit Trail record concerning an action by a Shared Identity, the KMI shall include the Singular Identity that was using the Shared Identity for the action. [DRV KRD 1014] {Z}

CI2-SEC-3.11.2j (U//FOUO) The KMI shall ensure that the identity of the recording Component and the identities of any other involved Components are bound to each event that is recorded in the Audit Trail. [DRV KRD 1014] {Z}

CI2-SEC-3.11.2k (U//FOUO) The KMI shall be able to identify the Component or process, as appropriate, that is source of each record in the Audit Trail. [DRV KRD 1559] {Z}

CI2-SEC-3.11.2m (U//FOUO) The KMI shall include the time of occurrence in each Audit Event record in the Audit Trail. [DRV KRD 1010] {Z}

(U//FOUO) In CI-2, the time reference used to record the time of occurrence in an audit record is expected to be provided by a clock on the computer platform that supports the component performing the recording function.

CI2-SEC-3.11.2n (U//FOUO) The KMI shall enable only an authorized Security Configuration Manager to change the time reference that a Component uses to record the time of occurrence for an Audit Event. [DRV KRD 1011] {Z}

CI2-SEC-3.11.2o (U//FOUO) The Audit Trail shall contain information that indicates the sequence in which recorded Audit Events occurred. [DRV KRD 1012] {Z}

CI2-SEC-3.11.2p (U//FOUO) The Audit Trail shall not contain Authentication Material (e.g., passwords or private keys) in any form that requires the KMI to provide continuing confidentiality service for the Audit Trail. [DRV KRD 1812] {Z}

CI2-SEC-3.11.2q (U//FOUO) The Audit Trail shall not contain cryptographic material in any form that requires the KMI to provide continuing confidentiality service for the Audit Trail. [DRV KRD 1814] {Z}

3.11.3 (U) Audit Trail Content, Specific

(U//FOUO) The requirements stated in this section are primarily guidelines that apply to many parts of the KMI. These requirements are implemented by more specific statements in other sections of [KMI2200], but also have been retained here as a summary of intent.

CI2-SEC-3.11.3a(U//FOUO) The KMI shall record, as Mandatory Audit Events, suspicious actions of both Operational Managers and Administrative Managers. (Criteria for identifying such actions shall be proposed by the contractor and approved by the Government.) [DRV KRD 1978] {Z}

CI2-SEC-3.11.3b (U//FOUO) The KMI shall record, as Mandatory Audit Events, suspicious interactions on communication networks, including both internal networks that connect Core Nodes and external networks that connect Client Nodes to PRSNs. (Criteria for identifying such interactions shall be proposed by the contractor and approved by the Government.) [DRV KRD 0942, 1979] {Z}

CI2-SEC-3.11.3c (U//FOUO) If CI-2 provides, supports, or uses services or products of a PKI, then the KMI shall, at a minimum, record as Mandatory Audit Events any applicable events and data specified by the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] or the *United States Government Type 1 Certificate Policy* [UST1CP], as applicable. [DRV KRD 0843, 1809] {Z}

(U//FOUO) The KMI shall record the following information (as applicable) for each event that is recorded for audit:

CI2-SEC-3.11.3f (U//FOUO) For each Audit Event, the KMI shall record the date and time when the event occurred. [DRV KRD 0572, 0684, 1010, 2130, 2131, 3132] {Z}

CI2-SEC-3.11.3g (U//FOUO) For each Audit Event that involves transaction processing, the KMI shall record the unique transaction number that is associated with the event. [DRV KRD 684] {Z}

CONTROL (U//FOUO) **ECAR-1 Audit Record Content (Confidentiality)**. For systems that process publicly released information, “Audit records include:” [DoDI8500.2]

- “User ID.”
- “Successful and unsuccessful attempts to access security files.”
- “Date and time of the event.”
- “Type of event.”

CI2-SEC-3.11.3h (U//FOUO) For Components that process sensitive unclassified information, Audit Trail records shall include the following data items (where applicable) for each audit event: [DRV KRD 2130] {Z}

- User Identity of any responsible User, and User Identities of any other involved Users. [DRV KRD 1014]
- Successful and unsuccessful attempts to access security-sensitive data.
- Date and time of the event. [DRV KRD 1010]
- Type of event.

CONTROL (U//FOUO) **ECAR-2 Audit Record Content (Confidentiality)**. For systems that process sensitive information, "Audit records include:" [DoDI8500.2]

- "User ID."
- "Successful and unsuccessful attempts to access security files."
- "Date and time of the event."
- "Type of event."
- "Success or failure of event."
- "Successful and unsuccessful logons."
- "Denial of access resulting from excessive number of logon attempts."
- "Blocking or blacklisting a user ID, terminal or access port, and the reason for the action."
- "Activities that might modify, bypass, or negate safeguards controlled by the system."

CI2-SEC-3.11.3i (U//FOUO) For Components that process Sensitive information, Audit Trail records shall include the following data items (where applicable) for each Audit Event: [DRV KRD 2131] {Z}

- User Identity of any responsible User, and User Identities of any other involved Users. [DRV KRD 1014]
- Successful and unsuccessful attempts to access security-sensitive data.
- Date and time of the event. [DRV KRD 1010]
- Type of event.
- Success or failure of event.
- Successful and unsuccessful logons.
- Denial of access resulting from excessive number of logon attempts.
- Blocking or blacklisting a user ID, terminal or access port and the reason for the action.
- Activities that might modify, bypass, or negate safeguards controlled by the system.

CONTROL (U//FOUO) **ECAR-3 Audit Record Content (Integrity)**. For systems that process classified information, "Audit records include:" [DoDI8500.2]

- "User ID."
- "Successful and unsuccessful attempts to access security files."
- "Date and time of the event."
- "Type of event."
- "Success or failure of event."
- "Successful and unsuccessful logons."
- "Denial of access resulting from excessive number of logon attempts."
- "Blocking or blacklisting a user ID, terminal or access port, and the reason for the action."

- “Activities that might modify, bypass, or negate safeguards controlled by the system.”
- “Data required to audit the possible use of covert channel mechanisms.”
- “Privileged activities and other system-level access.”
- “Starting and ending time for access to the system.”
- “Security relevant actions associated with periods processing or the changing of security labels or categories of information.”

CI2-SEC-3.11.3j (U//FOUO) For Components that process classified information, Audit Trail records shall include the following data items (where applicable) for each Audit Event: [DRV KRD 2132] {Z}

- User Identity of any responsible User, and User Identities of any other involved Users. [DRV KRD 1014]
- Successful and unsuccessful attempts to access security-sensitive data.
- Date and time of the event. [DRV KRD 1010]
- Type of event.
- Success or failure of event.
- Successful and unsuccessful logons.
- Denial of access resulting from excessive number of logon attempts.
- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action.
- Activities that might modify, bypass, or negate safeguards controlled by the system.
- Data required to audit the possible use of covert channel mechanisms.
- Privileged activities and other system-level access.
- Starting and ending time for access to the system.
- Security-sensitive actions associated with periods processing or the changing of security labels or categories of information.

3.11.4 (U) Audit Trail Protection

(U//FOUO) This section specifies how KMI audit processes and audit trails must be protected.

CONTROL (U//FOUO) **ECTP-1 Audit Trail Protection (Integrity)**. “The contents of audit trails are protected against unauthorized access, modification or deletion.” [DoDI8500.2]

CONTROL [NT] (U//FOUO) **ECTB-1 Audit Trail Backup (Integrity)**. For Components that process classified information, “The audit records are backed up not less than weekly onto a different system or media than the system being audited.” [DoDI8500.2]

(U//FOUO) The requirements for protecting KMI audit trails and the processes that produce them are as follows:

CI2-SEC-3.11.4a (U//FOUO) The KMI shall protect all Audit processes and Audit Trail records against unauthorized Access. [DRV KRD 0992, 1815] {Z}

CI2-SEC-3.11.4b (U//FOUO) The KMI shall ensure that only Audit Data Managers and authorized Audit processes can access Audit Trail records. [DRV KRD 0993, 1806, 1980] {Z}

CI2-SEC-3.11.4c (U//FOUO) If CI-2 provides, supports, or uses services or products of a PKI, the KMI shall, at a minimum, protect Audit processes and Audit Trail records, including backup copies as specified by the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] or the *United States Government Type 1 Certificate Policy* [UST1CP], as applicable. [DRV KRD 1797, 1804] {Z}

CI2-SEC-3.11.4d (U//FOUO) Audit processes shall run independently and shall not in any way be under the control of any User except an authorized Audit Data Manager. [DRV KRD 1798] {Z}

CI2-SEC-3.11.4e (U//FOUO) The KMI shall include means to detect a failure of an Audit data collection or recording process and, when a failure has been detected, shall prevent exercise of KMI functions that require auditing except for those associated with certificate revocation. [DRV KRD 0117] {Z}

3.11.5 (U) On-Line Audit Trail

(U//FOUO) This section states requirements regarding the balance between audit records that are maintained on-line and those that are transferred to archive media.

CI2-SEC-3.11.5a (U//FOUO) The KMI shall (1) move on-line Audit Trail records from Components that record or hold them to Archive media and (2) delete the records from the Components, only as directed by an authorized Audit Data Manager. [DRV KRD 1802] {Z}

CI2-SEC-3.11.5b (U//FOUO) The KMI shall maintain the most recent Audit Trail records on-line until (1) they are moved onto Archive media by direction of an authorized Audit Data Manager, (2) they have been on-line for a specified maximum time period, or (3) a specified maximum quantity of records has been collected on-line. [DRV KRD 1000] {Z}

CI2-SEC-3.11.5c (U//FOUO) The KMI shall enable an authorized Audit Data Manager to direct that Audit Trail records be moved onto Archive media. [DRV KRD 1802] {Z}

CI2-SEC-3.11.5d (U//FOUO) The KMI shall move on-line Audit Trail records onto Archive media when they have been on-line for a specified maximum time period. [DRV KRD 1800] {Z}

CI2-SEC-3.11.5e (U//FOUO) The KMI shall enable an authorized Audit Data Manager to configure the maximum time period that Audit Trail records are required to be maintained on-line. [DRV KRD 1800] {Z}

CI2-SEC-3.11.5f (U//FOUO) The KMI shall move on-line Audit Trail records onto Archive media when a specified maximum quantity of records has been collected on-line. [DRV KRD 1800] {Z}

CI2-SEC-3.11.5g (U//FOUO) The KMI shall enable an authorized Audit Data Manager to configure the maximum quantity of Audit Trail records to be maintained on-line. [DRV KRD 1800] {Z}

CI2-SEC-3.11.5h (U//FOUO) The KMI shall not delete (i.e., purge) on-line Audit Trail records until an authorized Audit Data Manager has verified that the records have been archived successfully. [DRV KRD 1800] {Z}

CI2-SEC-3.11.5i (U//FOUO) The KMI shall not delete (i.e., purge) any on-line Audit Trail records until the records have been on-line for a specified minimum time period, even if the records have already been archived. [DRV KRD 1801] {Z}

CI2-SEC-3.11.5j (U//FOUO) The KMI shall enable an authorized Audit Data Manager to configure the minimum time period for Audit Trail records to be maintained on-line. [DRV KRD 1801] {Z}

CI2-SEC-3.11.5k (U//FOUO) The KMI shall support retention of Audit Trail records on-line for the time periods specified by applicable policy and doctrine. [DRV KRD 0072] {Z}

CI2-SEC-3.11.5l (U//FOUO) The KMI shall employ means, including a degraded mode of system operation if necessary, to ensure that Audit Trail records are not lost or discarded due to lack of on-line storage capacity or inability to archive them. [DRV KRD 0103, 0119] {Z}

CI2-SEC-3.11.5m (U//FOUO) The KMI shall alert an Audit Data Manager when a Component’s Audit Trail storage is filled to a configurable percentage of its capacity, and shall require the Manager to acknowledge the alert before permitting the Manager to take other actions. [DRV KRD 2014] {Z}

3.11.6 (U) Audit Trail Archive

(U//FOUO) This section specifies how audit records are maintained in archive media.

CONTROL [NT] (U//FOUO) **ECRR-1 Audit Record Retention (Confidentiality)**. “If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year.” [DoDI8500.2]

(U//FOUO) The requirements for archiving audit trails are as follows:

CI2-SEC-3.11.6a (U//FOUO) The KMI shall Archive all Audit Trail records. [DRV KRD 0104] {Z}

CI2-SEC-3.11.6b (U//FOUO) The KMI shall protect Audit Trail records that have been archived, or are intended to be, against undetected modification. [DRV KRD 0103, 0994, 0995, 0996] {Z}

CI2-SEC-3.11.6c (U//FOUO) If CI-2 provides, supports, or uses services or products of a PKI, the KMI shall, at a minimum, archive Audit Trail records and protect the archives as specified by the *DoD X.509 Certificate Policy* [DoDX509CP], or the policy for Type 1 certificates [USGT1CP], as appropriate. [DRV KRD 1803] {Z}

CI2-SEC-3.11.6d (U//FOUO) The KMI shall store archived Audit Trail records on separate physical media than other archived data. [KRD NEW] {Z}

CI2-SEC-3.11.6g [NT] (U//FOUO) The KMI shall store archived Audit Trail records in a separate physical storage location than other archived data. [KRD NEW] {C-P-R-S-T}

CI2-SEC-3.11.6e [NT] (U//FOUO) The KMI shall support retention of Audit Trail records on Archive media for the time periods specified by applicable policy and doctrine. [DRV KRD 0072] {C-P-R-S-T}

CI2-SEC-3.11.6f [NT] (U//FOUO) The KMI shall provide a centralized Archive facility that retains Audit Trail records for 30 years and makes the records available to authorized Audit Trail Managers. [DRV KRD 2011] {S}

3.11.7 (U) Audit Trail Analysis

(U//FOUO) This section specifies how audit trail records need to be analyzed both (1) periodically to detect security violations and (2) upon request to assess damage caused by a violation.

CONTROL (U//FOUO) **ECRG-1 Audit Reduction and Report Generation (Integrity)**. "Tools are available for the review of audit records and for report generation from audit records." [DoDI8500.2]

(U//FOUO) The requirements for analyzing audit trails are as follows:

CI2-SEC-3.11.7a (U//FOUO) The KMI shall provide automated data reduction and analysis tools to assist authorized Managers in analyzing Audit Trail records. [DRV KRD 0998] {C-P-R-S}

CI2-SEC-3.11.7b (U//FOUO) If CI-2 provides, supports, or uses services or products of a PKI, the KMI shall, at a minimum, meet audit reduction requirements as specified by *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] or the *United States Government Type 1 Certificate Policy* [UST1CP], as applicable. [DRV KRD 1820] {C-P-R-S}

CI2-SEC-3.11.7c (U//FOUO) The KMI shall enable an authorized Audit Data Manager to establish and make available to authorized Managers, an ongoing, automatic analysis of selected Audit Trail records. [DRV KRD 1015, 1821] {P-R-S}

CI2-SEC-3.11.7d (U//FOUO) KMI audit analysis processes shall enable an authorized Audit Data Manager to request selected Audit Trail records for analysis. [DRV KRD 1822] {C-P-R-S}

CI2-SEC-3.11.7e (U//FOUO) The KMI shall enable an authorized Audit Data Manager or authorized Audit analysis process to retrieve and analyze archived Audit Trail records. [DRV KRD 0997] {S}

CI2-SEC-3.11.7f (U//FOUO) The KMI shall provide means to analyze Audit Trail records produced by an individual Component or Computer Platform. [DRV KRD 1816] {Z}

CI2-SEC-3.11.7g (U//FOUO) The KMI shall provide means within each Security Enclave to analyze the Audit Trail records produced by the Components in that enclave. [DRV KRD 1816] {P-R-S}

CI2-SEC-3.11.7h (U//FOUO) The KMI shall provide means within a Node to analyze the Audit Trail records produced by the Components in that Node. [DRV KRD 1816] {C-P-R-S}

CI2-SEC-3.11.7i (U//FOUO) The KMI shall be able to centrally analyze Audit Trail records produced by any individual networked Component regardless of the Component's location. [DRV KRD 1817] {R-S}

CI2-SEC-3.11.7j (U//FOUO) The KMI shall provide means to analyze Audit Trail records produced by multiple Components in a manner that facilitates detection and characterization of attacks that span multiple Components. [DRV KRD 0999] {R-S}

CI2-SEC-3.11.7k (U//FOUO) The KMI shall provide means to collect Audit Trail records from all Components into a central Component for the purpose of analysis. [DRV KRD 0120, 1818] {R-S}

CI2-SEC-3.11.7l (U//FOUO) Non-networked Components shall be able to transfer their Audit Trail records to networked Components, and networked Components shall be able to transfer Audit Trail records to a central Component. [DRV KRD 1818] {Z}

CI2-SEC-3.11.7m (U//FOUO) The KMI shall be able to (1) analyze a consolidated set of Audit Trail records that have been collected from multiple Components and Computer Platforms and (2) provide a consolidated analysis report. [DRV KRD 1819] {R-S}

3.12 (U) Attack Sensing, Warning, and Response Service

POLICY (U//FOUO) **General Policy on Attack Sensing, Warning, and Response (ASWR).** The KMI must attempt to detect Threat Actions and, if and when Threat Actions are detected, provide warning of them and respond to them with counteractions.

DEFINITION (U) Threat Action. An intentional act, an unintentional or accidental act, or a natural event that has the potential to violate KMI security policy, cause the KMI to behave in an unauthorized manner, or otherwise interrupt proper operation of the KMI.

DEFINITION (U) Attack. An intentional Threat Action, i.e., an act by which an intelligent System Entity attempts to evade security measures and violate security policy.

DEFINITION (U) Sensing. Recognizing, identifying, and categorizing attacks and other Threat Actions.

DEFINITION (U) Warning. 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.

DEFINITION (U) Response. Initiating a counteraction to an attack or other Threat Action.

(U//FOUO) ASWR services, in cooperation with audit services, protect against security breaches by detecting and reacting to indications of threat actions against the KMI, including both insider and outsider attacks. Each node, security enclave, and computer platform protects itself with an independent ASWR capability. Additional information about the placement of ASWR capabilities in nodes, enclaves, zones, and platforms—and particularly in Monitoring Zones of PRSNs—is provided in the "Nodal Structures" section of Volume 3.

(U//FOUO) The basic requirements for KMI ASWR service are as follows:

CI2-SEC-3.12a (U//FOUO) The KMI shall incorporate processes and procedures for sensing, providing warning of, and responding to Threat Actions. [DRV KRD 1823, 1826, 1016] {Z}

CI2-SEC-3.12b (U//FOUO) ASWR processes and procedures shall integrate with, and provide information to, DoD standard systems for network monitoring and defense, including Computer Network Defense (CND) Centers. [DRV KRD 0128] {R-S}

3.12.1 (U) ASWR Methods

(U//FOUO) ASWR services need to be built into the geographically distributed architecture of the KMI system, which depends on computer networks.

DEFINITION (U) Computer Network. A collection of host computers together with the communication infrastructure (a Subnetwork) through which the Hosts can exchange data.

DEFINITION (U) Host. A computer that is attached to a communication Subnetwork and can use services provided by the Subnetwork to exchange data with other attached systems.

DEFINITION (U) Subnetwork. A system of packet relays and connecting links that implement a communication service to interconnect attached computers that subscribe to the service.

(U//FOUO) ASWR processes need to include the type commonly called an intrusion detection system (IDS), that defends system components against threat actions carried by network data traffic. The two basic categories of IDS are host-based and network-based. In a host-based IDS, the IDS components—the traffic sensors and analyzers—run directly on one or more of the hosts that they are intended to protect. In a network-based IDS, the sensors are placed on subnetwork components, and analysis components run either on subnetwork processors or hosts. This terminology—host-based and subnetwork-based—can be used for ASWR processes in general, not just those that defend against communication-based threat actions.

CONTROL (U//FOUO) **ECID-1 Host Based IDS (Integrity)**. "Host-based intrusion detection systems are deployed for major applications and [network-based intrusion detection systems are deployed] for network management assets, such as routers, switches, and domain name servers (DNS)." [DoDI8500.2]

CONTROL (U//FOUO) **EBVC-1 VPN Controls (Availability)**. "All VPN traffic is visible to network intrusion detection systems (IDS)." [DoDI8500.2]

(U//FOUO) This *Specification* interprets EBVC-1 to mean that at each point where a VPN terminates in a "security enclave" (as defined in Volume 3), the data that emerges from the VPN into the enclave must be subject to IDS protections that are specified in this section and further implemented in the "Boundary Protection Suites and Guards" section in Volume 3. CI-2 uses KMI Protected Channels (KPCs) (see "Communications Services" section) to implement virtual private networks (VPNs) between KMI components. In most cases, a VPN implements end-to-end encryption to provide confidentiality service for the protected data along an entire VPN transmission path. Therefore, the clear text content of traffic carried by a KMI VPN must not be available to an IDS at any midpoint in a VPN transmission path.

(U//FOUO) Two basic methods are used by IDSs to detect threat actions: 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 threat actions, particular attacks. An signature-based IDS has a library of threat actions, and the library needs to be updated whenever new kinds of threat actions become known. Usually, the IDS vendor supplies these updates, and the IDS user can add patterns to the library, too. An anomaly-based IDS monitors network traffic to detect deviations from "normal" or "expected" behavior, where that behavior 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. A profile may be established automatically by monitoring traffic for some period of time, or manually by stating desired values. This terminology—signature-based and anomaly-based—also can be used for ASWR processes in general, not just those that defend against communication-based threat actions.

3.12.2 (U) Sensing Threat Actions

(U//FOUO) This section states requirements for sensing events that might be threat actions:

CI2-SEC-3.12.2a (U//FOUO) The KMI shall incorporate appropriate ASWR sensors throughout the entire KMI—specifically, in all Nodes, Security Enclaves, and Computer Platforms—as is appropriate for the security architecture of each Component and the threats to each Component. [DRV KRD 1823] {Z}

CI2-SEC-3.12.2b (U//FOUO) ASWR processes shall address both Host-based and Subnetwork-based Threat Actions. [DRV KRD 1828] {Z}

CI2-SEC-3.12.2c (U//FOUO) ASWR processes shall protect Components against Threat Actions at all protocol layers of KMI Computer Networks. [KRD DRV KRD 0902] {C-P-R-S-T}

CI2-SEC-3.12.2d (U//FOUO) ASWR sensors and processes shall continually monitor for Threat Actions by comparing system inputs, events, and conditions against parameters established by ASWR Managers to define Threat Actions. [DRV KRD 1831] {Z}

CI2-SEC-3.12.2e (U//FOUO) ASWR processes shall report when system events and conditions match established threat-definition parameters. [DRV KRD 1834] {Z}

CI2-SEC-3.12.2f (U//FOUO) ASWR processes that are signature-based shall incorporate libraries of patterns of Threat Actions. [DRV KRD 1831] {C-P-R-S-T}

CI2-SEC-3.12.2g (U//FOUO) ASWR sensors shall compare system inputs, events, and conditions against threat definition parameters, including libraries of patterns of Threat Actions. [DRV KRD 1831] {Z}

CI2-SEC-3.12.2h (U//FOUO) ASWR processes shall report when system events and conditions match threat definition parameters, including entries in libraries of patterns of Threat Actions. [DRV KRD 1834] {Z}

CI2-SEC-3.12.2i (U//FOUO) The KMI shall enable an ASWR Manager to configure and update threat definition parameters, including libraries of patterns of Threat Actions. [DRV KRD 1834] {Z}

CI2-SEC-3.12.2j (U//FOUO) ASWR processes shall be able to rapidly and incrementally receive and deploy updates to libraries of Threat Actions, in order to deal with new kinds of Threat Actions. [DRV KRD 1834] {C-P-R-S-T}

CI2-SEC-3.12.2k (U//FOUO) ASWR processes shall enable an ASWR Manager to tailor libraries or create custom libraries of Threat Actions, in order to deal with KMI-unique threat problems. [DRV KRD 1834] {C-P-R-S-T}

CI2-SEC-3.12.2l (U//FOUO) The KMI shall record for Audit changes to ASWR threat-definition parameters, including libraries of patterns of Threat Actions. [DRV KRD 1977] {Z}

3.12.3 (U) ASWR Assurance and Protection

(U//FOUO) This section states requirements for assurance and protection of ASWR processes, particularly those that traditionally have been called IDSs.

CI2-SEC-3.12.3a (U//FOUO) ASWR processes shall be invoked at Component startup and shall be shut down only at Component shutdown. [DRV KRD 1841] {Z}

CI2-SEC-3.12.3b (U//FOUO) ASWR processes shall remain active and available in all KMI operational states. [DRV KRD 1842] {Z}

CI2-SEC-3.12.3c (U//FOUO) ASWR processes and related data shall be protected against unauthorized modification and use. [DRV KRD 1843] {Z}

CI2-SEC-3.12.3d (U//FOUO) ASWR processes shall operate under the control of an ASWR Manager, and only a Security Configuration Manager shall be able to disable them. [DRV KRD 1844] {Z}

CI2-SEC-3.12.3e (U//FOUO) ASWR processes shall include NSA-approved intrusion detection capabilities. [DRV KRD 0129] {Z}

CI2-SEC-3.12.3f (U//FOUO) Intrusion detection processes shall be approved by the National Information Assurance Partnership (NIAP) against the following protection profiles: [DRV KRD 1555] {Z}

– *Intrusion Detection System Analyzer Protection Profile* [PF11].
– *Intrusion Detection System Sensor Protection Profile* [PF12].
– *Intrusion Detection System Scanner Protection Profile* [PF13].
– *Intrusion Detection System* [PF16].

3.12.4 (U) Providing Warning of Threat Actions

(U//FOUO) This section states requirements for providing notification and warning of events that might be Threat Actions:

CI2-SEC-3.12.4a (U//FOUO) ASWR processes shall provide warning to an Incident Response Manager of any detected event or condition that might indicate a Threat Action against the KMI by any System Entity. [DRV KRD 1826, 1975, 1976] {Z}

CI2-SEC-3.12.4b (U//FOUO) ASWR processes shall provide warning to an Incident Response Manager of detected attempts to violate the KMI security policy. [DRV KRD 1017] {Z}

CI2-SEC-3.12.4c (U//FOUO) ASWR processes shall be able to categorize actual or suspected Threat Actions into multiple warning levels (defined by severity, frequency, and other factors). [DRV KRD 1835] {Z}

CI2-SEC-3.12.4d (U//FOUO) The KMI shall enable an ASWR Manager to configure the reporting required for each warning level that is defined for Threat Actions. [DRV KRD 1833, 1835] {Z}

CI2-SEC-3.12.4e (U//FOUO) ASWR processes shall provide warning to an Incident Response Manager of Threat Actions that exceed a warning level configured by an ASWR Manager. [DRV KRD 1833, 1835] {Z}

CI2-SEC-3.12.4f (U//FOUO) The KMI shall enable an ASWR Manager to configure a timeframe within which a Threat Action must be reported. [DRV KRD 1833, 1837] {Z}

CI2-SEC-3.12.4g (U//FOUO) The KMI shall enable an ASWR Manager to configure certain warning levels as requiring immediate (i.e., real-time) warning. [DRV KRD 1832] {Z}

CI2-SEC-3.12.4h (U//FOUO) ASWR processes shall report Threat Actions within a timeframe specified by an ASWR Manager. [KRD 1838] {Z}

CI2-SEC-3.12.4i (U//FOUO) The KMI shall immediately provide warning to an Incident Response Manager when ASWR processes detect Threat Actions that have been designated as requiring such immediate notification. [DRV KRD 1833] {Z}

CI2-SEC-3.12.4j (U//FOUO) Immediate warnings of Threat Actions shall be both visible and audible, and shall require explicit acknowledgement by the notified Incident Response Manager. [DRV KRD 1833] {Z}

CI2-SEC-3.12.4k (U//FOUO) ASWR processes shall enable an ASWR Manager to notify National attack sensing and warning centers of detected Threat Actions against the KMI, including being able to generate and send authenticated notifications. [DRV KRD 0155] {R-S}

3.12.5 (U) Responding to Threat Actions

(U//FOUO) This section states requirements for managers to be able to initiate counteractions in response to threat actions against the KMI.

CI2-SEC-3.12.5a (U//FOUO) The KMI shall enable Incident Response Managers to initiate KMI reactions to detected attempts to violate KMI security policy. [DRV KRD 1016] {C-P-R-S-T}

CI2-SEC-3.12.5b (U//FOUO) The KMI shall enable Administrative Managers to alter the KMI configuration or operations appropriately when warned of attempts to violate KMI security policy. [DRV KRD 0154, 1016] {Z}

CI2-SEC-3.12.5c (U//FOUO) ASWR processes shall enable Incident Response Managers to control both host and subnetwork Components of the KMI for the purpose of responding to Threat Actions. [DRV KRD 1829] {Z}

CI2-SEC-3.12.5d (U//FOUO) ASWR processes shall enable Incident Response Managers to specify in advance the KMI response to each type of detected Threat Action. [DRV KRD 1836] {Z}

CI2-SEC-3.12.5e [NT] (U//FOUO) The KMI shall provide means (i.e., countermeasure) to provide an applicable response to each type of Threat Action that can be detected. [DRV KRD 1981] {Z}

3.12.6 (U) ASWR Management and Architecture

(U//FOUO) This section states requirements for management of ASWR processes. The requirements in this section are primarily guidelines that apply to many parts of the KMI. These requirements are implemented by more specific statements in other sections of [KMI2200], but also have been retained here as a summary of intent.

CI2-SEC-3.12.6a (U//FOUO) ASWR processes shall provide user-friendly interfaces that enable authorized ASWR Managers to monitor and control ASWR processes in both host and subnetwork Components. [DRV KRD 1829] {Z}

CI2-SEC-3.12.6b (U//FOUO) ASWR processes shall enable ASWR Managers to input and update information regarding Threat Actions and related events and conditions against which the ASWR processes will react. These inputs may be made locally, or may be accomplished using remote updates from authenticated, authorized remote sources over KPCs. [DRV KRD 1830] {C-P-R-S-T}

CI2-SEC-3.12.6c (U//FOUO) The KMI shall support hierarchical reporting and storage structures for aggregation, correlation, and management of information in support of ASWR service. [DRV KRD 1824] {Z}

CI2-SEC-3.12.6d (U//FOUO) The KMI shall enable ASWR Managers to sort information received from ASWR sensors on the basis of parameters of interest within that information (e.g., dates, type of Threat Action, criticality of Threat Action, identity of affected Component, source of the information, etc.). [KRD 2004] {Z}

CI2-SEC-3.12.6e (U//FOUO) The KMI shall provide ASWR management capabilities on a dedicated Computer Platform in networked Sites that house Core Nodes. [DRV KRD 1825] {P-R-S}

CI2-SEC-3.12.6f (U//FOUO) The KMI shall provide ASWR management capabilities on a dedicated Computer Platform in each Security Enclave. [DRV KRD 1825] {P-R-S}

CI2-SEC-3.12.6g (U//FOUO) ASWR information shall be collected from each Computer Platform in a Security Enclave of a Core Node, onto the enclave's ASWR management platform. [DRV KRD 1824] {P-R-S}

CI2-SEC-3.12.6h (U//FOUO) The KMI shall provide KPCs, with confidentiality service, for information flows between Computer Platforms that are dedicated to ASWR management. [DRV KRD 1827] {P-R-S}

3.13 (U) Security Configuration Service

POLICY (U//FOUO) **General Policy on Security Configuration**. The KMI must be able to adapt its security posture to defined variations in its mission environments and external interfaces.

(U//FOUO) KMI security configuration services adapt the KMI to satisfy the requirements of mission environments and external interfaces that change over time. The specific requirements that implement security configuration service are as follows:

3.13.1 (U) Mechanism Parameters

(U//FOUO) The characteristics of KMI security services need to be adaptable to meet defined variations in the threat environment, such as the DoD INFOCON levels [CJCS].

CI2-SEC-3.13.1a (U//FOUO) The KMI shall enable Security Configuration Managers, and only Security Configuration Managers, to control and configure security resources and security settings, both for the system as a whole and for specific Nodes, Components, and Computer Platforms. [DRV KRD 1781] {Z}

(U//FOUO) The characteristics of KMI security services must be adaptable to enable interoperation with external systems, to exchange products, services, or related information.

3.13.2 (U) Technical Protection Policies

(U//FOUO) It is desirable for the KMI to be able to manage multiple, concurrent technical protection policies for applying security services to various tasks, products, services, user communities, and environments.

DEFINITION (U//FOUO) Technical Protection Policy. A set of security requirements that apply to a specific KMI task area (e.g., product ordering, generation, or distribution) or other focus of attention.

(U//FOUO) The KMI is expected to perform basic tasks independently of the method of KMI implementation, and the relevant technical protection policies are expected to apply to whatever implementation is selected.

CI2-SEC-3.13.2a (U//FOUO) [Not applicable to CI-2.] The KMI shall provide a capability for authorized Users to develop, construct, and compose technical protection policies. [KRD 1028] {X}

CI2-SEC-3.13.2b (U//FOUO) [Not applicable to CI-2.] The KMI shall provide means to assert multiple, concurrent, technical protection policies. [DRV KRD 1032] {X}

CI2-SEC-3.13.2c (U//FOUO) [Not applicable to CI-2.] The KMI shall provide means to map between technical protection policies. [DRV KRD 1032] {X}

CI2-SEC-3.13.2d (U//FOUO) [Not applicable to CI-2.] The KMI shall provide means to enforce multiple, concurrent, technical protection policies. [KRD 1032] {X}

CI2-SEC-3.13.2e (U//FOUO) [Not applicable to CI-2.] The KMI shall provide means to verify compliance with technical protection policies. [KRD 1030] {X}

4. (U) FUNCTIONAL AREA SECURITY POLICIES

(U//FOUO) This section states policies and some of the associated requirements for security services in specific functional areas of the KMI. It is expected that the KMI will perform these functions regardless of how the system is implemented, and that the policies and requirements will apply to whatever implementation is selected. These security services are intended to operate in concert with those described in Sections 3 and 5.

4.1 (U) Communication Services

POLICY (U//FOUO) **General Policy on Communications**. A KMI Communication Association must use a Protected Channel if the association transfers information through a medium that does not provide equivalent protection.

(U//FOUO) The geographical distribution of the DoD and other U.S. Government organizations that provide and use KMI products and services requires the KMI to be a distributed system, i.e., a system in which an integrated set of related logical computing tasks are dispersed across separate but cooperating system components. This distribution requires the KMI to protect communications between its components, and between the components and their users.

> **DEFINITION** (U) Communication Association. A cooperative relationship among Components or other System Entities, for the purpose of transferring information between them.

> **DEFINITION** (U) Communication Channel. An information transfer path implemented between Components or other System Entities.

> **DEFINITION** (U//FOUO) KMI Protected Channel (KPC). A KMI Communication Channel that provides (1) Information Integrity Service; (2) either Data Origin Authentication Service or Peer Entity Authentication Service, as is appropriate to the mode of communication; and (3), optionally, Information Confidentiality Service.

(U//FOUO) The type of authentication service provided by a KPC depends on the mode of communication. For example, data origin authentication is usually appropriate for store-and-forward messages, while peer entity authentication is usually appropriate for file transfers. Whether or not a KPC provides information confidentiality service depends on the sensitivity of the communication association being carried, but the service is generally desirable for all protected channels. (Also see “Information Protection Requirements” section.)

(U//FOUO) KPCs are implemented mainly by requirements in the “Protected Channels” section of Volume 3. KPCs are used in the CI-2 security architecture to implement the following controls for information that is transmitted through a network:

> **CONTROL** (U//FOUO) **ECTM-2 Transmission Integrity Controls (Integrity)**. “Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all

transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels)." [DoDI8500.2]

CONTROL (U//FOUO) **ECCT-2 Encryption for Confidentiality (Data in Transit) (Confidentiality)**. "Classified data transmitted through a network that is cleared to a lower level than the data being transmitted are separately encrypted using NSA-approved cryptography (See also DCSR-3 in "Security Robustness and Security Assurance" section.) [DoDI8500.2]"

CONTROL (U//FOUO) **ECCT-1 Encryption for Confidentiality (Data in Transit) (Confidentiality)**. "Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2)." [DoDI8500.2]

CONTROL (U//FOUO) **ECNK-1 Encryption for Need-To-Know (Confidentiality)**. For Components that process classified information or sensitive information, "Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality – data in transit)." [DoDI8500.2]

(U//FOUO) The following control is not applicable to CI-2 because the KMI does not handle Sources and Methods Intelligence:

CONTROL (U//FOUO) **ECNK-2 Encryption for Need-To-Know (Confidentiality)**. [Not applicable to CI-2.] For Components that process classified information, "SAMI [Sources and Methods Intelligence] information in transit through a network at the same classification level is encrypted using NSA-approved cryptography. This is to separate it for need-to-know reasons. This is in addition to ECCT [in this section]." [DoDI8500.2]

CONTROL (U//FOUO) **ECWN-1 Wireless Computing and Networking (Availability)**. "Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. (See also ECCT [in this section]). Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users." [DoDI8500.2]

CI2-SEC-4.1a [NT] (U//FOUO) The KMI shall not implement wireless communications for either (1) connections between Components inside any Core Node or (2) connections between Core Nodes. [DRV KRD 2145] {C-P-R-S-T}

(U//FOUO) Regarding implementation of wireless communications, this *Specification* states no requirements for either (1) non-core client nodes or (2) non-KMI networks that carry KMI communications.

4.2 (U) Product Ordering

POLICY (U//FOUO) **General Policy on Product Ordering**. The KMI ordering process must ensure that only Registered Users acting within proper Authorizations and Constraints can order KMI products, services, and related information.

(U//FOUO) Product ordering is the process by which Users request products, services, and related information resources from the KMI. The security requirements that are specific to product ordering are stated in Volume 1.

4.3 (U) Product Generation

POLICY (U//FOUO) **General Policy on Product Generation**. The KMI generation process, although intended to uniformly serve a broad range of products, must satisfy the special requirements of individual product classes in accordance with applicable, product-specific doctrine.

(U//FOUO) Product generation is the process by which the KMI creates the products and prepares the services that are delivered to consuming users. The security requirements that are specific to product generation are stated in Volume 1.

4.4 (U) Product Handling

POLICY (U//FOUO) **General Policy on Product Handling**. KMI product handling methods, although intended to uniformly serve a broad range of KMI products, must satisfy the special requirements of individual product classes in accordance with applicable, product-specific doctrine.

(U//FOUO) Product handling refers generally to the processing and storage of KMI cryptographic products and related information within the KMI system. The security requirements that are specific to product handling are stated in Volume 1.

4.4.1 (U) Product Handling Restrictions

POLICY (U//FOUO) The KMI must enforce handling restrictions that are required for KMI products and services.

> **DEFINITION** (U) Handling Restriction. A type of Access Control other than the rule-based protections of mandatory access control and the identity-based protections of discretionary access control, and is usually procedural in nature.

(U//FOUO) Some KMI products are subject to special controls and procedures. For example, two-person integrity imposes “continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements” [CNSSI4009]. Some KMI authorizations may be defined in association with handling restrictions, and constraints on roles and permissions may be used to implement some forms of handling restrictions.

(U//FOUO) The security requirements that are specific to handling restrictions are stated in Volume 1.

4.4.2 (U) Product Expiration and Destruction

POLICY (U//FOUO) The KMI must ensure that all cryptographic products are destroyed upon expiration.

(U//FOUO) The security requirements that are specific to product expiration and destruction are stated in Volume 1.

4.4.3 (U) Product Tagging

POLICY (U//FOUO) To prevent misuse of cryptographic products, the KMI must bind descriptive data to the products it produces.

(U//FOUO) Product tagging helps to ensure that key material is used correctly and only for its intended purposes. The security requirements that are specific to product tagging are stated in Volume 1.

4.5 (U) Product Distribution

POLICY (U//FOUO) **General Policy on Product Distribution**. The KMI distribution process must protect KMI products and related information resources in accordance with applicable, product-specific doctrine.

(U//FOUO) Product distribution is the process by which KMI products and related information resources are delivered to Users. The security requirements that are specific to product distribution are stated in Volume 1.

4.6 (U) Product Tracking and Accounting

(U//FOUO) In addition to collecting audit information (see “Audit Service” section), the KMI needs to collect “tracking” information about its key management operations and “accounting” information about the custody of certain products.

POLICY (U//FOUO) **General Policy on Product Tracking**. The KMI must be able to maintain information on the status of orders for products and services and the status of the products that result.

(U//FOUO) Product tracking is the process of collecting, recording, and managing information that describes the processing status of orders received from Users for products and services, including the delivery status of the results of those orders. Tracking data is retained only temporarily.

POLICY (U//FOUO) **General Policy on Product Accounting**. The KMI must be able to maintain information on the custody of KMI products that are potentially subject to exposure or to a transformation that could potentially lead to exposure.

(U//FOUO) Accounting (also called COMSEC accounting) is the process of collecting, recording, and managing information that describes the status and custody of designated key management products during each product's lifecycle. Accounting data is retained indefinitely. In CI-2, many products are handled mainly in encrypted form, and that enables accounting to be simplified or eliminated, replaced by "tracking". In some cases, products are not handled entirely in encrypted form, and those cases require tracking to be supplemented by accounting.

(U//FOUO) The security requirements that are specific to tracking and accounting functions are stated in Volume 1.

4.7 (U) External Databases

POLICY (U//FOUO) **General Policy on External Directories, Repositories and Other Databases.** The KMI should conform to the security standards of non-KMI directories, repositories, and other databases used as sources of information for producing KMI products and services, but such conformance must not degrade the security required for the KMI by this *Policy*.

(U//FOUO) The KMI accesses or depends on external databases as authoritative sources of some of the information needed to produce products and services. The requirements for such interaction with external directories, repositories, or other databases are stated in the "Relationship to Existing Key Management Systems and External Support Systems" section of Volume 1 and in the "PRSN External System Enclaves" section of Volume 3.

4.8 (U//FOUO) Extend Trust and Outside Users

POLICY (U//FOUO) **General Policy on Extend Trust**. The KMI must interact with non-KMI key management systems and Outside Users in a manner that does not degrade the security that is otherwise required for the KMI by this *Policy*.

> **DEFINITION** (U) KMI Extend Trust. A term that refers to situations in which the KMI interacts with non-KMI key management systems that are External Systems and are not subject to the authority of this *Policy*.

(U//FOUO) The KMI needs to interact with non-KMI key management systems (KMSs) to support the missions of KMI users. However, such interoperation in CI-2 is limited to supporting certification validation by cross-certifying with, or otherwise recognizing, non-KMI PKI systems such as commercial certification authorities (CAs), both foreign and domestic; allied and coalition partner CAs, both military and civil; and various bridge CAs, including the U.S. Government Federal Bridge Certification Authority.

CI2-SEC-4.8a (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall be able to interoperate with selected non-KMI KMSs by exchanging products and services. [DRV KRD 1023] {R-S}

CI2-SEC-4.8b [NT] (U//FOUO) The KMI shall be able to interoperate for the purpose of certificate validation with U.S. Federal PKIs (including the Federal Bridge Certification Authority); U.S. state PKIs; and PKIs supporting the intelligence community, the medical community, allies, and coalition military forces. [DRV KRD 0484] {R-S}

CI2-SEC-4.8c [NT] (U//FOUO) The KMI shall be able to interoperate for the purpose of certificate validation with allied national PKIs to the extent permitted by the designs of those systems. [DRV KRD 0493] {R-S}

CI2-SEC-4.8d [NT] (U//FOUO) The KMI shall be able to interoperate for the purpose of certificate validation with DoD-approved commercial PKIs. [DRV KRD 0501] {R-S}

CI2-SEC-4.8e (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall interoperate with non-KMI KMSs without diminishing the security assurance level of the KMI, despite the fact that those systems may operate at levels of assurance less than that of the KMI. [DRV KRD 1065] {R-S}

CI2-SEC-4.8f [NT] (U//FOUO) The KMI shall be able to interoperate with non-KMI PKI CAs only after approval by an authorized Manager. [DRV KRD 1444] {P-S}

CI2-SEC-4.8g [NT] (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall provide means for an authorized Manager to approve interaction of the KMI with a non-KMI KMS. [DRV KRD 1444] {P-R-S}

(U//FOUO) Other specific policies and associated requirements that the KMI shall meet to support Extend Trust functions are as follows:

4.8.1 (U) Outside Users

(U//FOUO) In some cases, rather than supporting interoperability indirectly through a non-KMI KMS, the KMI might support interoperability directly by registering users of the other system as outside users.

DEFINITION (U) Outside User. A Registered User that is not directly subject, or not fully subject, to U.S. Government authority for enforcing this *Security Policy*.

(U//FOUO) For example, the KMI might register military personnel of an allied or coalition nation, or employees of an international or private humanitarian organization. Because such persons are not subject to the authority of the U.S. Government, they are not directly subject to the authority of this *Policy*, even though they are registered through a formal agreement between the U.S. Government and the other nation or organization.

CI2-SEC-4.8.1a (U//FOUO) The KMI shall be able to provide products and services for Users outside the authority of this *Policy* that are authorized to access the KMI in connection with Department of Defense or other Federal Government business. [DRV KRD 0504] {R-S}

CI2-SEC-4.8.1b [NT] (U//FOUO) The KMI shall require a System Entity that is not fully subject to the authority of this *Policy* to be registered as an Outside User before providing that entity with a product or service. [DRV KRD 1572] {R}

CI2-SEC-4.8.1c (U//FOUO) The KMI shall be able to register Outside Users, including Users from the international community (i.e., non-U.S. Users). [DRV KRD 1571] {R}

CI2-SEC-4.8.1d If a Registered User, or a User Identity of a User, is outside the KMI's policy authority, the KMI shall include that fact in the User Registration Data. [DRV KRD 1571] {R}

CI2-SEC-4.8.1e (U//FOUO) The KMI shall provide means for an authorized Manager to authorize Outside Users to access the KMI. [DRV KRD 1571] {R}

CI2-SEC-4.8.1f (U//FOUO) The KMI shall be able to (1) associate Identity Authentication Material with Outside Users, including Users from the international community (i.e., non-U.S. Users) and (2) issue appropriate Identifier Credentials to those Users, including KMI Management Credentials if authorized. [DRV KRD 1571] {R}

4.8.2 (U) "Least Privilege" for Actions Outside the KMI's Policy Authority

POLICY (U//FOUO) The KMI must restrict interactions with non-KMI KMSs and Outside Users to the least authorizations and functionality that can adequately support interoperability needed for mission requirements of Regressed Users.

CI2-SEC-4.8.2a [NT] (U//FOUO) The KMI shall minimize the extent to which it relies on proper behavior of Outside Users. [DRV KRD 1065] {P-R-S}

CI2-SEC-4.8.2b [NT] (U//FOUO) The KMI shall require a Registered User to have specific Authorization before the User can take any system action that involves or results in interaction of the KMI with an Outside User. [DRV KRD 0832, 1067] {P-R-S}

CI2-SEC-4.8.2c [NT] (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall restrict its communications with non-KMI KMSs to those communications required to effect the interactions approved by authorized Managers. [DRV KRD 1068] {P-R-S}

CI2-SEC-4.8.2d [NT] (U//FOUO) The KMI shall restrict the products, services, and access that it provides to or accepts from non-KMI System Entities to those that are authorized by a Manager and are consistent with the level of assurance and Authorizations of the entities. [DRV KRD 1067] {P-R-S}

4.8.3 (U) Control of Import and Export Functions

POLICY (U//FOUO) The KMI must ensure that material and services delivered to, or received from, a non-KMI KMS or an Outside User have been authorized for release or acceptance.

(U//FOUO) The KMI sometimes needs to export cryptographic products and related information and services to non-KMI KMSs. The related information might include compromise reports, accounting and audit records, operation manuals, and policy descriptions. Also, the KMI sometimes needs to import such material from non-KMI KMSs, either for KMI internal consumption or to pass on to KMI users.

POLICY (U//FOUO) The KMI shall comply with CNSSP 14, *National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Authorized U.S. Activities that are Not a Part of the Federal Government* [CNSSP14].

POLICY (U//FOUO) The KMI shall comply with NTISSP 8, *National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Foreign Governments* [NSTISSP8].

CI2-SEC-4.8.3a (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall provide means to import products and related material from, and export them to, non-KMI KMSs—such as those of the commercial sector, the Federal Government, and allies—while providing appropriate security services for those interactions. [DRV KRD 1064] {S}

CI2-SEC-4.8.3b (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall be able to produce and export products and related material for use by allies. [DRV KRD 0497] {S}

CI2-SEC-4.8.3c (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall provide means for an authorized Manager to designate which products and other material can be exported to or imported from a non-KMI KMS. [DRV KRD 1051] {S}

CI2-SEC-4.8.3d (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall be able to import products and related material from a non-KMI KMS if directed by an authorized Manager. [DRV KRD 1359] {S}

CI2-SEC-4.8.3e (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall use material imported from non-KMI KMSs only for purposes approved by authorized Managers. [DRV KRD 1369] {S}

CI2-SEC-4.8.3f (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall enable an authorized Manager to establish a control list to restrict the distribution of material imported from a non-KMI KMS. [DRV KRD 1069] {S}

CI2-SEC-4.8.3g (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall use security mechanisms of high robustness to authenticate the identity of a non-KMI KMS when exchanging material with such a system. [KRD NEW] {S}

CI2-SEC-4.8.3h (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall use cryptographic means to authenticate a non-KMI KMS prior to exchanging material with that system. [DRV KRD 1049, 1779] {S}

CI2-SEC-4.8.3i (U//FOUO) The KMI shall authenticate material imported from a non-KMI Federal Government PKI prior to accepting, acting on, or further disseminating the material and shall enable such PKIs to authenticate material exported to them by the KMI. [DRV KRD 1443, 1779] {S}

CI2-SEC-4.8.3j (U//FOUO) The KMI shall record for Audit all interactions with Outside Users—including but not limited to product and service requests and product import and export actions—and include in each such audit record the identities of Regressed Users that are involved, especially the identities of Managers that authorize the interactions. [KRD NEW] {R-S}

4.8.4 (U) Protection of Imported and Exported Material

POLICY (U//FOUO) Material that the KMI exchanges with (i.e., either exports to, or imports from) Outside Users, should be protected according to requirements determined by the originators.

(U//FOUO) When the KMI exports products and other material, the KMI can no longer directly apply security measures and enforce policy to protect the material. Instead, the KMI must depend on a non-KMI system or a KMI outside user to protect the material in accordance with an applicable memorandum of agreement. (See “Non-KMI Systems” section.) On the other hand, when the KMI imports material, the KMI itself must protect the material, and the applicable agreement might require the KMI to use means that are different than it uses to protect its own, internally generated material. (See “Information Protection Requirements” section.) Importing and exporting material may require need-to-know controls.

(U//FOUO) The “[Not applicable to CI-2 ...]” note that appears on some of statements that follow is explained in the “Requirements Statements” subsection of Section 1 in this volume.

CI2-SEC-4.8.4a (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall use security mechanisms of high robustness to provide Information Confidentiality and Information Integrity Services for material exchanged with a non-KMI KMS. [KRD NEW] {S}

CI2-SEC-4.8.4b (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall verify the data integrity of all products imported from non-KMI KMSs. [KRD 1360] {R-S}

CI2-SEC-4.8.4c (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] When the KMI handles material that it has imported from a non-KMI KMS, or received from an Outside User, the KMI shall protect the material at least to the sensitivity level that has been specified by the originator. [DRV KRD 1052] {R-S}

CI2-SEC-4.8.4d (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] When the KMI handles material that it has imported from a non-KMI KMS, or received from an Outside User, the KMI shall protect the material to a level at least in accordance with the degree of trust that the KMI has assigned to that system or User. [DRV KRD 1052] {R-S}

CI2-SEC-4.8.4e (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] When interacting with a non-KMI KMS, the KMI shall enable only authorized Managers to learn the identity of that system. [KRD NEW] {R-S}

4.8.5 (U) Identification and Tracking of Imported Material

POLICY (U//FOUO) The KMI must verify and protect the identity of the origin of material that is imported from non-KMI KMSs, and must track such material.

(U//FOUO) Considerations of need-to-know and operations security also make necessary the policy and requirements in this section.

CI2-SEC-4.8.5a (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall track material that is imported from non-KMI KMSs. [KRD NEW] {R}

CI2-SEC-4.8.5b (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall use cryptographic means to bind information to imported material that enables authorized Users to learn and authenticate the material's origins, and shall maintain the binding throughout each product's life cycle. [DRV KRD 0440, 1050, 1368] {R-S}

CI2-SEC-4.8.5c (U//FOUO) [Not applicable to CI-2 except for PKI interoperation, as specified in other requirements.] The KMI shall enable only authorized User and Managers of imported material to learn the origin of imported material. [KRD NEW] {R}

4.9 (U) Archive Service

POLICY (U//FOUO) **General Policy on Archive Service**. The KMI must maintain long-term data archives to support long-duration security services and long periods of use of KMI products and services.

DEFINITION Archive. (1.) *Noun*: A collection of data that is stored for a relatively long period of time for historical and other purposes, such as to support non-repudiation service or audit service. (2.) *Verb*: To store data in such a way.

(U//FOUO) Some KMI products and services are used for long-term protection of customer resources. To support this, the KMI needs to retain information for long periods of time.

(U//FOUO) For example, a digital signature may need to be verified a very long time after the signing occurs. If the required public key certificates and other verification material are no longer available from the usual public-key infrastructure sources, such as public directories and on-line certification authority (CA) services, then the KMI must provide the material from data archived by certification authorities.

(U//FOUO) The security requirements that are specific to archive service are stated in Volume 1.

(This Page Left Blank Intentionally)

5. (U) SECURITY IMPLEMENTATION POLICIES

(U//FOUO) This section states policies and associated requirements for security disciplines that are used to implement the services specified by Sections 3 and 4. This section references basic National and DoD policies that apply to KMI implementation.

POLICY (U//FOUO) **General Policy on Security Implementation.** The mix of safeguards selected for the KMI must meet the minimum requirements of DoD Instruction 8500.2, *Information Assurance (IA) Implementation* [DoDI8500.2]. The requirements may be met through automated or manual means, but must be met in a cost-effective and integrated manner. An analysis must be performed to identify additional needs over and above the set of minimum requirements.

(U//FOUO) KMI security services are accomplished through the continuous employment of safeguards consisting of a combination of personnel security, physical security, emanations security, computer security, communications security, and other disciplines. Enforcement of security policy depends on correct implementation and operation of mechanisms that provide the required security services. The policies and requirements in this section are intended to operate in concert with those described in Sections 3 and 4 to establish an integrated security infrastructure. Also, the "best security practices" implementation approach stated in the following control is followed throughout both this volume and Volume 3.

CONTROL (U//FOUO) **DCBP-1 Best Security Practices (Integrity)**. "The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics." [DoDI8500.2]

(U//FOUO) The specific policies and requirements that the KMI shall meet to implement security services are as follows:

5.1 (U) Implementation Methodology

POLICY (U//FOUO) **Development Methodologies.** KMI implementation activities must use development methodologies and development environments—including, where appropriate, protected facilities and cleared developers—that are approved by the Designated Approving Authorities for the development of Components that perform Security-Sensitive Functions.

(U//FOUO) The specific requirements with regard to implementation methodology are as follows. (Some of these are not strictly security requirements, but they are included here because they must be balanced against requirements in the "Computer Security" section.)

CI2-SEC-5.1a [NT] (U//FOUO) Computer Platform requirements for newly developed Components shall be satisfied, to the maximum extent practicable, by using COTS and GOTS products. [DRV KRD 0217] {Z}

CONTROL [NT] (U//FOUO) **DCSQ-1 Software Quality (Integrity)**. "Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives." [DoDI8500.2]

CI2-SEC-5.1b [NT] (U//FOUO) All newly developed KMI software shall be developed in accordance with software development practices that are specified for the KMI by NSA. [DRV KRD 1374] {Z}

CI2-SEC-5.1c [NT] (U//FOUO) All newly developed Components shall be compliant with applicable DoD DII COE standards [DISACOE]. [DRV KRD 0205, 1377] {C-P-R-S-T}

CI2-SEC-5.1d [NT] (U//FOUO) The KMI shall ensure that custom software contained in Components was developed in a secure development environment by appropriately-cleared U.S. citizens using development tools that are highly robust (see definition in [DoDI8500.2]). [DRV KRD 2080] {Z}

5.2 (U) Computer Security

POLICY (U) **General Policy on Technical Computer Security**. The KMI must comply with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products* [NSTISSP11], as interpreted for DoD by DoD Instruction 5200.2 [DoDI5200.2]. [REV KRD 970]

(U) An IA product is a "Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control or non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks." An IA-enabled product is a "Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities." [DoDI5200.2]

(U//FOUO) NSTISSP 11 requires that acquisition of all COTS IA and IA-enabled IT products for use on systems handling national security information shall be limited to products that have been evaluated and validated, as appropriate, in accordance with one of the following:

- (U//FOUO) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement
- (U//FOUO) The National Security Agency/National Institute of Standards and Technology National Information Assurance Partnership
- (U//FOUO) The NIST Federal Information Processing Standard validation program

(U//FOUO) For each category of information technology product or system that is the subject of an evaluation under NSTISSP 11, security requirement statements from the *Common Criteria* [IS15408] are used to construct a protection profile.

DEFINITION (U) Protection Profile. An implementation-independent set of security assessment requirements for a category of information technology products or systems, and their associated administrator and user guidance documentation, that meet specific consumer needs. [IS15408-1]

(U//FOUO) The specific requirements that the KMI shall meet to implement computer security are as follows:

5.2.1 (U) DoD and KMI Implementation of NSTISSP 11

(U//FOUO) Regardless of the MAC or Confidentiality Level of KMI components, all incorporated IA products, and IA-enabled IT products that require use of the product's IA capabilities, need to comply with the evaluation and validation requirements of [NSTISSP11].

> **CONTROL** (U//FOUO) **DCAS-1 Acquisition Standards (Confidentiality)**. "The acquisition of all IA and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA and IA-enabled COTS IT products is limited to products that have been evaluated or validated through . . . the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation."

(U//FOUO) DoD Instruction 8500.2 also states the following:

> (U) "At the enterprise level, implementation-independent specifications for IA and IA-enabled IT products are provided in the form of protection profiles. Protection profiles are developed in accordance with the Common Criteria (reference (j)) within the NIAP framework. Regardless of the mission assurance category or confidentiality level of the DoD information system, all incorporated IA products, and IA-enabled IT products that require use of the product's IA capabilities, acquired under contracts executed after July 1, 2002, shall comply with the evaluation and validation requirements of NSTISSP No. 11 (reference (ah)), with the following qualifications:" [DoDI8500l.2 para E3.2.5]
>
> (U) "If an approved U.S. Government protection profile exists for a particular technology area and there are validated products available for use that match the protection profile description, then acquisition is restricted to those products; or to products that vendors, prior to purchase, submit for evaluation and validation to a security target written against the approved protection profile." [DoDI8500.2 para E3.2.5.1]
>
> (U) "If an approved U.S. Government protection profile exists for a particular technology area, but no validated products that conform to the protection profile are available for use, the acquiring organization must require, prior to purchase, that vendors submit their products for evaluation and validation by a NIAP EVP or CCRA laboratory to a security target written against the approved protection profile or acquire other U.S.-recognized products that have been evaluated under the sponsorship of other signatories to the CCRA." [DoDI8500.2 para E3.2.5.2]
>
> (U) "If no U.S. Government protection profile exists for a particular technology area and the acquiring organization chooses not to acquire products that have been evaluated by the NIAP CCEVS or CCRA laboratories, then the acquiring organization must require, prior to

purchase, that vendors provide a security target that describes the security attributes of their products, and that vendors submit their products for evaluation and validation at a DAA-approved [Evaluation Assurance Level (EAL)].” [DoDI8500.2 para E3.2.5.3]

(U//FOUO) The DCAS-1 control and DoD policy are implemented by these requirements and those that follow in the “Assurance Levels” and “Specific Protection Profiles” sections:

CI2-SEC-5.2.1b [NT] (U//FOUO) All Components used in the KMI, including those that perform security functions, shall have been evaluated and validated as required by Section E3.2.5 of DoD Instruction 8500.2 [DoDI8500.2] with Protection Profiles that have been approved by NSA, except for GOTS products developed to NSA-approved security criteria (such as the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]). [DRV KRD 1527] {Z}

CI2-SEC-5.2.1c [NT] (U//FOUO) Freely distributed IT equipment shall be subject to the same Protection Profile requirements as equipment acquired from vendors, except that NSA shall play the role of the vendor with regard to providing a profile and submitting it for evaluation and validation. (Also see DCPD-1 in [DoDI8500.2].) [DRV KRD 0970, 1423, 1527] {Z}

5.2.2 (U) Security Robustness and Security Assurance

(U//FOUO) Some system security assurance requirements (such as requirements for documentation, testing, and change control) are included in other sections of this *Specification*. However, specific assurance requirements for each KMI capability increment are intended to be specified in a *KMI Certification and Accreditation Plan* and in protection profiles. The profiles are expected to include any statements regarding the required strength of security mechanisms.

CONTROL (U//FOUO) **DCSR-3 Specified Robustness – High (Confidentiality)**. “Only high-robustness GOTS or COTS IA and IA-enabled IT products are used to protect classified information when the information transits networks that are at a lower classification level than the information being transported. High-robustness products have been evaluated by NSA or in accordance with NSA-approved processes. COTS IA and IA-enabled IT products used for access control, data separation or privacy on classified systems already protected by approved high-robustness products at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.” [DoDI8500.2]

CI2-SEC-5.2.2a (U//FOUO) Components that process classified information shall employ protection mechanisms that satisfy the requirements for “high robustness” as defined in [DoDI8500.2]. [DRV KRD 1538] {Z}

CI2-SEC-5.2.2d (U//FOUO) Within each Components that processes classified information (and is therefore already protected by high-robustness mechanisms), products used by the Component for Access Control, data separation, or personal privacy shall satisfy the requirements for at least basic robustness as defined in [DoDI8500.2]. [DRV KRD 2121] {Z}

CONTROL (U//FOUO)**DCSR-2 Specified Robustness - Medium (Confidentiality**). "At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF. COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required." [DoDI8500.2]

CI2-SEC-5.2.2b (U//FOUO) Components that meet the criteria of a national security system and process only unclassified information that has no effect on Type 1 products shall employ protection mechanisms that satisfy the requirements for at least "medium robustness" as defined in [DoDI8500.2]. [DRV KRD 1539] {Z}

(U//FOUO) For the parts of the DCSR-3 and DCSR-2 controls that address network transit, see the policy and requirements stated in the "Communication Services" section of this *Security Policy* and in the "Protected Channels" section of Volume 3

CONTROL (U//FOUO) **DCSR-1 Specified Robustness – Basic (Confidentiality**). "At a minimum, basic-robustness COTS IA and IA-enabled products are used to protect publicly released information from malicious tampering or destruction and ensure its availability. The basic-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Basic Robustness published under the IATF." [DoDI8500.2]

CI2-SEC-5.2.2c (U//FOUO) Components that process sensitive information subject to Public Law 100-235 as codified in Title 15, U.S.C. 278g-3 shall employ protection mechanisms that satisfy the requirements for at least "basic robustness" as defined in [DoDI8500.2]. [DRV KRD 1540] {Z}

(U//FOUO) The following requirements are intended to provide security assurance for the KMI, i.e., to provide grounds for having confidence that the KMI operates such that the system security policy is enforced:

CI2-SEC-5.2.2e (U//FOUO) To the extent that the KMI implements Components at multiple assurance levels, the KMI shall ensure that transactions are serviced by Components at the appropriate assurance level or higher. [DRV KRD 1029] {Z

CI2-SEC-5.2.2f [NT] (U//FOUO) Each security-critical Component (except for GOTS products developed to NSA-approved security criteria, such as the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC] and any product that can impact the security of Type 1 operations) that processes Sensitive information shall have been evaluated as meeting the requirements of a U.S. Government-approved Protection Profile for medium robustness (i.e., at EAL4+) or better. [DRV KRD 1090] {C-P-R-S-T}

CI2-SEC-5.2.2g [NT] (U//FOUO) Each security-critical Component (except for GOTS products developed to NSA-approved security criteria, such as the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]) that processes classified information or can affect the security of classified information or Type 1 operations shall have been evaluated as meeting the requirements of a U.S. Government-approved Protection Profile for high robustness (i.e., at EAL6+) or better. [DRV KRD 1091] {C-P-R-S-T}

CI2-SEC-5.2.2h [NT] (U//FOUO) Each security-critical Component (except for GOTS products developed to NSA-approved security criteria, such as the Unified INFOSEC Criteria as tailored for application to CI-2 [NSAUIC]) that processes or can affect the security of information that must be handled with two-person integrity shall have been evaluated as meeting the requirements of a U.S. Government-approved Protection Profile at EAL6+ or better. [DRV KRD 1092] {C-P-R-S-T}

CI2-SEC-5.2.2i (U//FOUO) If CI-2 supports or uses products of the DoD PKI, then the KMI shall meet any applicable assurance requirements of the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP]. [DRV KRD 0208] {Z}

CI2-SEC-5.2.2j (U//FOUO) In cases where CI-2 uses X.509 public-key certificates to authenticate the identity of Managers, the KMI shall meet the assurance requirements of the *United States Government Type 1 Certificate Policy* [UST1CP]. [KRD NEW, 0208] {Z}

5.2.3 (U) Specific Protection Profiles

(U//FOUO) The following are some of the protection profiles that apply to KMI components. Although these requirement statements say “NIAP-approved”, there are additional statements in a previous subsection of this volume that require the profiles to be “NSA-approved”.

CI2-SEC-5.2.3a [NT] (U//FOUO) Cryptographic Hardware Tokens used to access the KMI in the Role of KOA Agent, but not as a Manager, shall have been NIAP-approved against the *DoD Public Key Infrastructure Target Class 4 Token Protection Profile* [PF1]. [DRV KRD 0970, 1528] {X}

CI2-SEC-5.2.3b [NT] (U//FOUO) Cryptographic Hardware Tokens used to access the KMI as a Manager shall have been NIAP-approved against *Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness* [PF14]). [DRV KRD 0970] {X}

CI2-SEC-5.2.3d [NT] (U//FOUO) Directories included in Components shall have been NIAP-approved against the *U.S Department of Defense Directory Protection Profile for Medium Robustness Environments* [PF3]. [DRV KRD 0970, 1530] {P-R-S}

CI2-SEC-5.2.3f [NT] (U//FOUO) Components that provide virtual private network services shall have been NIAP-approved against the *A Goal VPN Protection Profile for Protecting Sensitive Information* [PF7]. [DRV KRD 0970, 1532] {P-R-S-T}

CI2-SEC-5.2.3g [NT] (U//FOUO) Component operating systems shall have been NIAP-approved against the protection profile for *Single Level Operating Systems in Environments Requiring Medium Robustness* [PF8]. [DRV KRD 0970, 1533] {C-P-R-S-T}

CI2-SEC-5.2.3h [NT] (U//FOUO) Firewalls included in Components shall have been NIAP-approved against one of the following Protection Profiles as appropriate: [DRV KRD 0970, 1991] {C_P-R-S-T}

– *Traffic Filtering Firewall Protection Profile for Medium Robustness* [PF9].
– *U.S. Department of Defense Application Firewall for Medium Robustness* [PF10].
– *U.S. Government Firewall Protection Profile for Medium Robustness Environments* [PF15].

5.2.4 (U) Administrative Security for Platforms and Applications

POLICY (U//FOUO) **General Policy on Administrative Computer Security**. The KMI must ensure secure administration of functional control of Computer Platforms that support Components.

(U//FOUO) The following statements establish minimum requirements for secure administration of KMI platforms. Most COTS platforms currently do not incorporate KMI's PKI-based authentication mechanisms and role-based access control mechanisms. In some cases, therefore, KMI needs to use other mechanisms, such as identifier-password pairs, that are native to the platforms. Such names and passwords qualify as "user identifiers" and "authentication material" defined in this volume, but KMI does not register the names and maintain authentication data for them in the same way as for PKI-based identifiers.

CI2-SEC-5.2.4a (U//FOUO) The KMI shall use automated Access Control measures to ensure that only authorized Administrative Managers can access operating system functions that are used to administer Computer Platforms. [DRV KRD 1782] {Z}

CI2-SEC-5.2.4b (U//FOUO) If administrative access to a Computer Platform cannot be controlled by identity authentication based on asymmetric encryption and role-based Access Control, then mechanisms incorporated in (i.e., native to) the platform shall be used. [DRV KRD 1782] {Z}

CI2-SEC-5.2.4c (U//FOUO) The KMI shall authenticate the identity of Administrative Managers of Computer Platforms prior to permitting them to perform platform-level actions. [DRV KRD 1782] {Z}

CI2-SEC-5.2.4d [NT] (U//FOUO) The KMI shall ensure that only authorized Administrative Managers have administrative access to operating systems and hardware of Computer Platforms. [DRV KRD 1782] {Z}

CI2-SEC-5.2.4e [NT] (U//FOUO) The KMI shall enable only authorized Administrative Managers to activate (i.e., start up, boot up), configure, and deactivate (i.e., shut down) Computer Platforms. [DRV KRD 1889] {C-P-R-S-T}

(U//FOUO) Some computer platforms are administered locally, through direct physical access, but other platforms are expected to be administered remotely, through communication channels. The instances of remote access need to use KPCs that provide security services as strong as the physical and procedural protections for local access. The following requirement is related to DoDI 8500.2 control "EBRP-1 Remote Access for Privileged Functions" and to associated KMI requirements that are stated in the "Client Nodes Serving Managers" section of Volume 3:

> **CI2-SEC-5.2.4f** (U//FOUO) Remote access to a Computer Platform for administrative purposes shall be permitted only via a KPC that provides appropriate security services, including strong information integrity and strong authentication of the identities of Administrative Managers. [DRV KRD 2127] {Z}

(U//FOUO) This *Specification* interprets the following control as applying to accounts that are implemented by mechanisms that are part of computer platforms:

> **CONTROL** (U//FOUO) **IAAC-1 Account Control (Confidentiality)**. "A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated." [DoDI8500.2]

(U//FOUO) The IAAC-1 control is implemented by the following requirements and by requirements in other sections of this volume and Volume 3.

> **CI2-SEC-5.2.4g** (U//FOUO) The KMI shall enable only an authorized Platform Account Manager to establish platform-level accounts that are authorized to perform administrative or operational functions. [DRV KRD 1788, 1789] {Z}

> **CI2-SEC-5.2.4h** (U//FOUO) The KMI shall limit Platform Account Managers to the permissions assigned to their administrative Role and the Authorizations assigned to their platform-level account. [DRV KRD 0407, 1552] {Z}

> **CI2-SEC-5.2.4i** (U//FOUO) The KMI shall prevent a Human User from being assigned to both the Platform Account Manager role and the Audit Data Manager role for the same Computer Platform. [DRV KRD 1790] {Z}

5.3 (U) Personnel Security

(U//FOUO) Secure system implementation requires assurance that registered users are appropriately trustworthy.

> **CONTROL** [NT] (U//FOUO) **PRRB-1 Security Rules of Behavior or Acceptable Use Policy (Availability)**. "A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access." [DoDI8500.2]

5.3.1 (U) Clearance and Authorization

POLICY (U//FOUO) **General Policy on Personnel Assurance**. The KMI must ensure that its Registered Users have security clearance and Authorizations commensurate with their assigned Roles and Privileges.

CONTROL [NT] (U//FOUO) **PRNK-1 Access to Need-to-Know Information (Confidentiality)**. "Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PRAS-2 Access to Information (Confidentiality)**. "Individuals requiring access to classified information are processed for access authorization in accordance with DoD personnel security policies." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PRAS1-Access to Information (Confidentiality)**. "Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies." [DoDI8500.2]

(U//FOUO) The requirements for personnel assurance are as follows:

CI2-SEC-5.3.1a [NT] (U//FOUO) KMI personnel security practices shall comply where applicable with DoD Regulation 5200.2, *DoD Personnel Security Program Regulation*, [DoDR5200.2]. [KRD NEW] {C-P-R-S}

CI2-SEC-5.3.1b [NT] (U//FOUO) Access to the KMI by foreign nationals shall require (1) approval by a DoD Service or Agency Head in accordance with Section 4.9 of DoD Directive 8500.1, *Information Assurance* [DoDD8500.1], and (2) approval by an authorized Administrative Manager. [KRD NEW] {C-R}

CI2-SEC-5.3.1c [NT] (U//FOUO) KMI personnel security practices shall comply where applicable with the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] or the *United States Government Type 1 Certificate Policy* [UST1CP]. [DRV KRD 1702] {C-R}

(U//FOUO) Technical controls to implement the following controls for maintenance personnel are not stated in [KMI2200]:

CONTROL [NT] (U//FOUO) **PRMP-2 Maintenance Personnel (Confidentiality)**. For Components that process classified information, "Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented. Except as authorized by the DAA, personnel who perform maintenance on classified DoD information systems are cleared to the highest level of information on the system. Cleared personnel who perform maintenance on a classified DoD information systems require an escort unless they have authorized access to the computing facility and the DoD information system. If uncleared or lower-cleared personnel are employed, a fully cleared and technically qualified escort monitors and records all activities in a maintenance log. The level of detail required in the maintenance log is determined by the [Information Assurance Manager]. All maintenance personnel comply with DAA requirements for U.S. citizenship, which are explicit for all classified systems." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PRMP-1 Maintenance Personnel (Confidentiality)**. For Components that process sensitive information, "Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented." [DoDI8500.2]

5.3.2 (U) Training and Awareness

POLICY (U//FOUO) **General Policy on Personnel Security Training and Awareness**. The KMI must ensure that its Registered Users have been appropriately instructed in KMI security practices before they access the system.

(U//FOUO) KMI users need to be appropriately knowledgeable of security risks and proper procedures for mitigating those risks. The specific requirements that the KMI shall meet to implement security training and awareness are as follows:

CONTROL [NT] (U//FOUO) **PRTN-1 Information Assurance Trainin**g **(Confidentiality)**. "A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA-related plans such as incident response, configuration management and COOP or disaster recovery." [DoDI8500.2]

(U//FOUO) The KMI issues a security warning to every system entity that attempts to access the system, regardless of whether the entity is a registered user or not.

CONTROL (U//FOUO) **ECWM-1 Warning Message (Confidentiality)**. "All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing." [DoDI8500.2]

CI2-SEC-5.3.2a (U//FOUO) Security awareness for unregistered System Entities that attempt to access the KMI shall be established by the displaying officially approved versions of warning banners of each of the following types, according to what is appropriate for the type of access attempted (i.e., web-based or transaction-based): {C-P-R-S-T }

– (1) DoD security warning banner. [KRD 1541]
– (2) DoD "Government use only" warning banner. [KRD 1542]
– (3) DoD "Privacy Act Notice" warning banner. [KRD 1543]

(U//FOUO) The text for warning banners usually is determined by the organization that is responsible for operating the equipment that posts the banner, and the text may change from time to time to conform with changes in laws and regulations. The following text is only an example:

> "WARNING! This is a U.S. Department of Defense computer system intended for use only by U.S. Government personnel and authorized affiliates. Unauthorized attempts to upload or change information on this site, or otherwise cause damage, are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act, as amended and codified at 18 U.S.C. 1030a. For site security purposes and to ensure that this service remains available to all legitimate users, this Federal Government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage. Use of this site constitutes consent to this monitoring."

(U//FOUO) KOA Agents need security training material that is understandable and provides complete coverage of topics relevant to using the KMI securely.

> **CI2-SEC-5.3.2b** [NT] (U//FOUO) Security awareness and training for KOA Agents shall include (1) the warnings provided to unregistered System Entities that attempt to access the KMI and also include (2) additional information that is provided as part of the KMI registration and re-registration processes, explains the KOA Agent's role in maintaining KMI security, explains the User-visible security functions of the KMI and how to use them. [DRV KRD 1541, 1542, 1543] {C-R}

(U//FOUO) KMI managers need security training material that is understandable and provides complete coverage of topics relevant to securely operating and administering the KMI.

> **CI2-SEC-5.3.2c** [NT] (U//FOUO) Security awareness and training for Managers shall (1) be in addition to that for KOA Agents and (2) provide detailed, accurate information about how to manage the KMI in a secure manner and how to make effective use of KMI protection functions. [DRV KRD 1541. 1542. 1543] {C-R}

5.4 (U) Physical Security

POLICY (U//FOUO) **General Policy on Physical Security.** Components must be protected against physical modification and destruction throughout their life cycle by security controls commensurate with the requirements for information confidentiality and integrity and with the requirements for system integrity and availability.

(U//FOUO) KMI components operate in environments that vary from well-protected and benign to potentially very dangerous (e.g., tactical), and that need physical protection appropriate for each case. The specific requirements for physical security are as follows:

> **CI2-SEC-5.4a** [NT] (U//FOUO) Physical security for Sites and Components shall comply with DoD 5200.8, *Security of DoD Installations and Resources* [DoDD5200.8], and related guidance, as implemented by the regulations of organizations that operate and maintain the Sites and Components. {Z}

> **CI2-SEC-5.4b** [NT] (U//FOUO) Components that access two-person integrity keys used to protect KMI functions shall be located in Sites that meet the requirements of NSTISSI 4005, *Safeguarding Communications Security (COMSEC) Facilities and Material* [NSTISSI4005]

and for which the design of the facilities support two-person integrity. [DRV KRD 1071] {C-P-R-S}

CI2-SEC-5.4c [NT] (U//FOUO) KMI physical security practices shall comply where applicable with the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] or the *United States Government Type 1 Certificate Policy* [UST1CP]. [DRV KRD 1702] {C-R}

CI2-SEC-5.4d [NT] (U//FOUO) Components shall be designed to minimize the degree to which additional physical security requirements are placed on the Sites where such Components are operated. [DRV KRD 0838] {Z}

CI2-SEC-5.4e (U//FOUO) Components that are identified as performing security-relevant functions—i.e., functions for which correct operation is necessary to ensure adherence to, or detect potential violations of, this *Security Policy* and the *Security Architecture* [KMI22200V3]—shall incorporate, or be provided with, appropriate tamper-evident protective measures. [DRV KRD 1073] {Z}

(U//FOUO) Technical requirements to implement the following controls on physical security are not stated in [KMI2200].

CONTROL [NT] (U//FOUO) **PECF-2 Access to Computing Facilities (Confidentiality)**. "Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PECF-1 Access to Computing Facilities (Confidentiality)**. "Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEPF-2 Physical Protection of Facilities (Confidentiality)**. "Every physical access point to facilities housing workstations that process or display classified information is guarded or alarmed [24 hours per day, 7 days per week]. Intrusion alarms are monitored. Two (2) forms of identification are required to gain access to the facility (e.g., ID badge, key card, cipher PIN, biometrics). A visitor log is maintained." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEPF-1 Physical Protection of Facilities (Confidentiality)**. "Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PECS-2 Clearing and Sanitizing (Confidentiality)**. "All documents, equipment, and machine-readable media containing classified data are cleared and sanitized before being released outside its security domain according to DoD 5200.1-R." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PECS-1 Clearing and Sanitizing (Confidentiality)**. "All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD(C3I) Memorandum, dated June 4, 2001, subject: 'Disposition of Unclassified DoD Computer Hard Drives.' [DoDI8500.2]"

CONTROL [NT] U//FOUO) **PEDD-1 Destruction (Confidentiality)**. For Components that process classified information, "All documents, machine-readable media, and equipment are destroyed using procedures that comply with DoD policy (e.g., DoD 5200.1-R)." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEDI-1 Data Interception (Confidentiality)**. "Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEEL-2 Emergency Lighting (Availability)**. "An automatic emergency lighting system is installed that covers all areas necessary to maintain mission or business essential functions, to include emergency exits and evacuation routes." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEFD-2 Fire Detection (Availability)**. "A servicing fire department receives an automatic notification of any activation of the smoke detection or fire suppression system[DoDI8500.2]"

CONTROL [NT] (U//FOUO) **PEFI-1 Fire Inspection (Availability)**. "Computing facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEFS-2 Fire Suppression System (Availability)**. "A fully automatic fire suppression system is installed that automatically activates when it detects heat, smoke, or particles." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEHC-2 Humidity Controls (Availability)**. "Automatic humidity controls are installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation [DoDI8500.2]"

CONTROL [NT] (U//FOUO) **PEMS-1 Master Power Switch (Availability)**. "A master power switch or emergency cut-off switch to IT equipment is present. It is located near the main entrance of the IT area and it is labeled and protected by a cover to prevent accidental shut-off." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEPS-1 Physical Security Testing (Confidentiality)**. "A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PESP-1 Workplace Security Procedures (Confidentiality)**. "Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PESS-1 Storage (Confidentiality)**. "Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PETC-2 Temperature Controls (Availability)**. "Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PETN-1 Environmental Control Training (Availability)**. "Employees receive initial and periodic training in the operation of environmental controls." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEVR-1 Voltage Regulators (Availability)**. "Automatic voltage control is implemented for key IT assets." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **PEVC-1 Visitor Control to Computing Facilities (Confidentiality)**. "Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility." [DoDI8500.2]

5.5 (U) Marking and Labeling

POLICY (U//FOUO) **General Policy on Marking.** The KMI must safeguard information at all times so that information is marked to accurately reflect its sensitivity, as required by applicable security policy.

(U//FOUO) Procedures for coordinating marking among all parties that provide data to the KMI—DoD, non-DoD U.S. Government, and non-Government—in order to ensure proper handling in the KMI, are outside the scope of this *Policy*. However, such coordination is needed.

CONTROL (U//FOUO) **ECML-1 Marking and Labeling (Confidentiality)**. "Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents such as DoD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions." [DoDI8500.2]

CONTROL (U//FOUO) **ECLC-1 Audit of Security Label Changes (Confidentiality)**. "The [KMI] system automatically records [for Audit] the creation, deletion, or modification of confidentiality or integrity labels, if required by the information owner." [DoDI8500.2]

(U//FOUO) The specific requirements for marking are as follows:

CI2-SEC-5.5a (U//FOUO) The KMI shall comply with the marking and labeling requirements of DoD 5200.1-R for all stored, processed, transmitted, or displayed data that is classified or Sensitive. [DRV KRD 2140] {Z}

CI2-SEC-5.5b (U//FOUO) All classified data being stored or processed in, or exchanged between Components shall be labeled, either explicitly or implicitly, with its classification (i.e., hierarchical sensitivity level and non-hierarchical compartments) and with any additional handling restrictions. [DRV KRD 0840] {Z}

CI2-SEC-5.5c (U//FOUO) All portable data storage media—including printed, magnetic, and electronic—that receive output from a Component operating in system-high security mode shall be labeled with the system-high level of the Component, as required by security policy applicable to the media. [DRV KRD 0819] {Z}

CI2-SEC-5.5d (U//FOUO) The KMI shall, when necessary, add a security label to information received from External Systems so that the security label can be interpreted by Users. [DRV KRD 0969] {Z}

CI2-SEC-5.5e (U//FOUO) The KMI shall record for Audit the creation, deletion, or modification of confidentiality or integrity labels. [DRV KRD 2137] {Z}

5.6 (U) Communications Security

POLICY (U//FOUO) **General Policy on Communication Security**. All KMI communications must be properly protected against passive and active wiretapping by methods and equipment approved by the National Security Agency.

CONTROL [NT] (U//FOUO) **ECCM-1 COMSEC (Confidentiality)**. For Components that process classified information, "COMSEC activities comply with DoD Directive C-5200.5." [DoDI8500.2]

CI2-SEC-5.6a (U//FOUO) Components that perform COMSEC functions shall comply with DoD Directive 5200.5, *Communications Security* [DoDD5200.5], and with related implementation guidance. [KRD NEW] {Z}

CI2-SEC-5.6b [NT] (U//FOUO) COMSEC equipment and COMSEC materials used to protect classified KMI information shall be acquired only through NSA as the centralized COMSEC acquisition authority, or through NSA designated agents. [KRD NEW] {Z}

CI2-SEC-5.6c [NT] (U//FOUO) Cryptographic equipment shall be approved by NSA before the equipment is used to protect KMI classified information that is transmitted through otherwise unprotected channels. [KRD NEW] {Z}

5.7 (U) Emanations Security

POLICY (U//FOUO) **General Policy on Emanations Security.** Components must be protected throughout their life cycle with emanations controls commensurate with KMI policy and requirements for information confidentiality, in accordance with NSTISSP No. 300, *National Policy on Control of Compromising Emanations*, 3 October 1988.

CONTROL (U//FOUO) **ECTC-1 Tempest Controls (Confidentiality)**. "Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19." [DoDI8500.2]

(U//FOUO) The requirements for KMI emanations security are as follows:

CI2-SEC-5.7a (U//FOUO) Components shall incorporate countermeasures for compromising emanations, in accordance with the following: [DRV KRD 1093] {Z}
– DoD Directive C-5200.19, *Control of Compromising Emanations* [DoDD5200.19].
– NSTISSI No. 7000, *TEMPEST Countermeasures for Facilities* [NSTISSI7000].
– NSTISSI No. 7001, *NONSTOP Countermeasures* [NSTISSI7001].
– NSTISSAM TEMPEST/2-95, *RED/BLACK Installation Guidance* [NSTISAM2-95].

5.8 (U) Cryptographic Security

(U//FOUO) This section addresses only basic key management requirements for the cryptography used by the KMI to implement the security services described in this volume and the security architecture described in Volume 3. Additional requirements for that cryptography are stated in the "Assurance Levels" section.

(U//FOUO) Requirements for cryptographic security that pertains to specific functions of requesting, generating, producing, and distributing products and services are stated in Volume 1.

POLICY (U//FOUO) **General Policy on Encryption Key Management.** The KMI must employ key management techniques that are commensurate with the sensitivity and criticality of use of the material in the KMI, and that mitigate operational threats, promote operational effectiveness, and minimize operational losses, impacts, and costs.

(U//FOUO) This section addresses the management of cryptographic keys and related material that are used by the KMI system itself to provide security services.

CONTROL (U//FOUO) **IAKM-3 Key Management (Integrity)**. For Components that process classified information, "Symmetric and asymmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes." [DoDI8500.2]

CONTROL (U//FOUO) **IAKM-2 Key Management (Integrity)**. For Components in MAC I or MAC II, "Symmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Medium or High Assurance certificates and hardware security tokens that protect the user's private key." [DoDI8500.2]

(U//FOUO) Where these controls are applicable to the KMI, they are implemented by requirements stated in this volume and in Volumes 1 and 3. The general requirements for key management are as follows:

CI2-SEC-5.8a [NT] (U//FOUO) The KMI shall comply with NSTISSP No. 3, *National Policy For Granting Access To U.S. Classified Cryptographic Information*, 19 December 1988. [KRD NEW] {A-P-S}

CI2-SEC-5.8b [NT] (U//FOUO) The KMI shall comply with NSTISSI No. 4001, *Controlled Cryptographic Items*, July 1996. [KRD NEW] {A-P-S}

CI2-SEC-5.8c [NT] (U//FOUO) The KMI shall comply with NTISSI No.4004, *Routine Destruction and Emergency Protection of COMSEC Material*, 11 March 1987. [KRD NEW] {A-P-S}

CI2-SEC-5.8d [NT] (U//FOUO) The KMI shall comply with NSTISSI 4005, *Safeguarding Communications Security (COMSEC) Facilities and Material* [NSTISSI4005]. [KRD NEW] {Z}

CI2-SEC-5.8f [NT] (U//FOUO) Components that use cryptographic mechanisms must be supported with a key management plan that defines the keying concept and procedures, and the interfaces to the supporting key management system. [KRD NEW] {Z}

CONTROL (U//FOUO) **DCNR-1 Non-Repudiation (Integrity)**. NIST FIPS 140-2 validated cryptography (e.g., DoD PKI Medium or High Assurance) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available." [DoDI8500.2]

CI2-SEC-5.8g (U//FOUO) Cryptographic modules that are used in Core Nodes with Sensitive unclassified key material shall at least meet the requirements of FIPS 140-2 level 3 [FIPS140]. [DRV KRD 1534] {P-R-S}

CI2-SEC-5.8h (U//FOUO) The KMI shall ensure that entry of activation data for cryptographic modules is protected from disclosure (e.g., the data should not be displayed while it is entered). [KRD 0899] {Z}

CI2-SEC-5.8i (U//FOUO) The KMI shall ensure that Registered Users, including System Security Officers, have no access to unencrypted private keys. [KRD 0938] {Z}

5.9 (U) Configuration Control

POLICY (U//FOUO) **General Policy on Configuration Control.** The KMI must have a configuration management system that controls changes to Components during the complete life cycle of the KMI, including design, development, operation, and maintenance.

(U//FOUO) *A Guide to Understanding Configuration Management in Trusted System* [NCSCTG6] provides an introduction to good practices for configuration management in systems that process classified or sensitive information.

DEFINITION (U) Configuration Management. The management of changes made to KMI hardware, firmware, software, documentation, test plans, test fixtures, and test documentation throughout the development and operational life of the system. [NCSCTG6]

DEFINITION (U//FOUO) Configuration Control. The process of controlling modifications to the KMI design, hardware, firmware, software, and documentation that provides sufficient assurance the system is protected against the introduction of unauthorized or improper modifications before, during, and after system implementation. [NCSCTG6]

(U//FOUO) The KMI needs configuration control to ensure system integrity. System integrity has both static and dynamic aspects. This section addresses static aspects (and the “System Integrity” section addresses dynamic aspects.) Changes in the configuration of KMI components are inevitable, but configuration management and control ensure that changes take place in an identifiable and deliberate way and do not adversely affect complete and correct implementation of KMI security policies.

CONTROL [NT] (U//FOUO) **DCPR-1 CM Process (Integrity)**. “A configuration management (CM) process is implemented that includes requirements for: (1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation; (2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems; (3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and (4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.” [DoDI8500.2]

CONTROL [NT] (U//FOUO) **DCCB-2 Control Board (Integrity)**. “All information systems are under the control of a chartered Configuration Control Board that meets regularly according to DCPR-1. The [Information Assurance Manager] is a member of the CCB.” [DoDI8500.2]

CONTROL [NT] (U//FOUO) **DCII-1 IA Impact Assessment (Integrity)**. “Changes to the [KMI] are assessed for [information assurance] and accreditation impact prior to implementation.” [DoDI8500.2] (See “Certification and Accreditation” and “Testing” sections.)

(U//FOUO) The specific requirements that the KMI shall meet to implement the general policy on configuration control are as follows:

5.9.1 (U) Basic Configuration Control

CI2-SEC-5.9.1a [NT] (U//FOUO) The KMI shall employ assured configuration control measures to protect its Components—including hardware, firmware, and software in all forms—and associated documentation, against unauthorized changes throughout the life of the system. [DRV KRD 1170] {Z}

CI2-SEC-5.9.1b [NT] (U//FOUO) The KMI shall enable authorized Administrative Managers, and only such Managers, to introduce, modify, or remove Components. [DRV KRD 1895] {Z}

CI2-SEC-5.9.1c [NT] (U//FOUO) The KMI shall attempt to detect and report to an Incident Response Manager any unauthorized introduction, modification, or removal of a Component during the system's development and implementation. [DRV KRD 1895] {P-R-S}

CI2-SEC-5.9.1d (U//FOUO) The KMI shall check system hardware, software, and data files—when the system is initialized, when the system is updated, and periodically during operation—for any unauthorized modification of the system configuration. [DRV KRD 1019] {Z}

(U//FOUO) These and other requirements in this volume (see "Audit" section) and in Volume 3 support implementation of the following ECND control:

CONTROL (U//FOUO) **ECND-2 Network Device Controls (Integrity)**. "An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested." [DoDI8500.2]

5.9.2 (U) Configuration Tracking

(U//FOUO) The following control and associated requirements address basic configuration management for hardware:

CONTROL [NT] (U//FOUO) **DCHW-1 HW Baseline (Availability)**. "A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original." [DoDI8500.2]

CI2-SEC-5.9.2a (U//FOUO) The KMI shall record and maintain configuration information about its Components. [DRV KRD 1382] {Z}

CI2-SEC-5.9.2c (U//FOUO) Independent Components shall be able to exchange information about their configurations. [DRV KRD 1383] {Z}

CI2-SEC-5.9.2d (U//FOUO) The KMI shall enable authorized Administrative Managers to query, view, analyze, chart, and report information concerning the configuration of Components. [DRV KRD 1384] {Z}

CI2-SEC-5.9.2e (U//FOUO) The KMI shall enable authorized Administrative Managers to remotely query Independent Components, via KPCs over internal and external networks, to obtain information about the installed hardware and software and other configuration characteristics of the Components. [DRV KRD 1382, 1383, 1384] {Z}

CI2-SEC-5.9.2f (U//FOUO) Independent Components shall be able to provide information about their installed hardware and software and other configuration characteristics, in response to authorized and authenticated requests that are received via KPCs, over internal and external networks, from remote Administrative Managers and management processes. [DRV KRD 1382, 1383, 1384] {Z}

5.9.3 (U) Control of Software

(U//FOUO) The following control and associated requirements address basic configuration management for software:

CONTROL [NT] (U//FOUO) **DCSW-1 SW Baseline (Availability)**. “A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.” [DoDI8500.2]

CI2-SEC-5.9.3a [NT] (U//FOUO) The KMI shall control the configuration of its software by using formal configuration management procedures. [DRV KRD 1170] {Z}

CI2-SEC-5.9.3h (U//FOUO) All KMI software resident on a system-high Component shall be protected at the system-high classification level. [DRV KRD 0816] {Z}

(U//FOUO) The following controls and requirements address specific aspects of configuration control for software:

CONTROL [NT] (U//FOUO) **ECSD-2 Software Development Change Controls (Integrity)**. “Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. Change controls include review and approval of application change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.” [DoDI8500.2]

CONTROL [NT] (U//FOUO) **ECPC-2 Production Code Change Controls (Integrity)**. “Application programmer privileges to change production code and data are limited and reviewed every 3 months.” [DoDI8500.2]

CI2-SEC-5.9.3g (U//FOUO) The KMI shall use technical security mechanisms to ensure that its software (1) has been obtained from authorized sources and (2) has not been modified prior to installation. [DRV KRD 0801, 0835, 1179, 2080] {Z}

CI2-SEC-5.9.3b (U//FOUO) The KMI shall protect its installed software against unauthorized modification. [DRV KRD 0802, 0835, 1179, 2080] {Z}

CI2-SEC-5.9.3c (U//FOUO) The KMI shall employ means to detect unauthorized attempts to modify its software. [DRV KRD 0803, 0835, 1179] {Z}

CI2-SEC-5.9.3d [NT] (U//FOUO) Upon receipt, but prior to use, the integrity of COTS software for use in KMI shall be protected by system developers and users, in accordance with approved doctrine. [DRV KRD 0801] {C-R-S-T}

CONTROL (U//FOUO) **DCPD-1 Public Domain Software Controls (Availability)**. "Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government." [DoDI8500.2]

CI2-SEC-5.9.3e [NT] (U//FOUO) Client Nodes shall be based on commercial or open-source offerings where possible, consistent with the other KMI security requirements; but, in accordance with control DCPD-1 in [DoDI8500.2], the KMI shall not use freeware or shareware unless it meets the following conditions: [DRV KRD 1423] {C-R-S-T}

- (1) The software is necessary for mission accomplishment and there are no alternative information technology solutions available.
- (2) The software has been assessed for information assurance impacts, and approved for use by the DAAs.
- (3) The assessment addresses the fact that such software is difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.

CONTROL [NT] (U//FOUO) **DCSL-1 System Library Management Controls (Integrity)**. "System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code." [DoDI8500.2]

CONTROL (U//FOUO) **DCMC-1 Mobile Code (Integrity)**. "The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements:" [DoDI8500.2]

1. "Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used."
2. "Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited."
3. "Category 2 mobile code, which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used."

4. "Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate)."
5. "Category 3 mobile code may be used."
6. "All DoD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited."
7. "The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments."

DEFINITION (U) Mobile Code. "Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient." [DoDD8500.1]

CI2-SEC-5.9.3f [NT] (U//FOUO) The KMI shall not load or use mobile code unless the usage is specifically approved by the DAAs, and then shall use mobile code only in the manner specified in [DoDD8500.1] and [DoDI8500.2]. [DRV KRD 0849, 0912] {C-P-R-S-T}

5.9.4 (U) Component Distribution and Installation

(U//FOUO) The following controls address deployment of CI-2 components:

CONTROL [NT] (U//FOUO) **DCCS-2 Configuration Specifications (Integrity)**. "A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a Departmental reference guide." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **ECSC-1 Security Configuration Compliance (Availability)**. "For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied." [DoDI8500.2]

(U//FOUO) The requirements for distributing and installing CI-2 components are as follows:

CI2-SEC-5.9.4a [NT] (U//FOUO) The KMI shall employ high-assurance methods to ensure that the Components that are delivered to and installed in Core Nodes are properly authorized. [DRV KRD 0981] {P-R-S}

CI2-SEC-5.9.4l [NT] (U//FOUO) For software in transit to distributed Components and Sites, the KMI shall provide high-grade, NSA-approved cryptographic confidentiality service for the software if its disclosure would reveal classified data (e.g., key lengths, plaintext key formats). [DRV KRD 2079] {A-P}

CI2-SEC-5.9.4m (U//FOUO) For Components that may be used in tactical deployments in which there is a risk of overrun, loss or capture or in Sites where provision of consistently high levels of physical security would be impractical, the KMI shall use NSA-approved cryptographic technical countermeasures to protect software stored in those Components if its disclosure would reveal classified data (e.g., key lengths, plaintext key formats). [DRV KRD 2078] {A}

CI2-SEC-5.9.4b (U//FOUO) The KMI shall verify the integrity of software and that software is from a valid source prior to changing the software configuration of the KMI. (When mechanisms other than digital signatures are used to protect software integrity, meeting this requirement may require significant use of procedural mechanisms.) [DRV KRD 1897] {Z}

CI2-SEC-5.9.4c (U//FOUO) When a software distribution is signed, the KMI shall verify the signature, and verify that the software is from an authorized source, prior to installing the software in a Component. [DRV KRD 1896] {Z}

CI2-SEC-5.9.4d [NT] (U//FOUO) The KMI shall ensure that any software installed in a Component is necessary to the functioning of that Component. [DRV KRD 0905] {C-R-S-T}

CI2-SEC-5.9.4e [NT] (U//FOUO) The KMI shall ensure that all parts and features of a COTS software Component that are not needed for specified KMI functions shall either not be installed or shall be turned off during installation. [DRV KRD 1378] {C-R-S-T}

CI2-SEC-5.9.4f [NT] (U//FOUO) The KMI shall ensure that software for unused network services is removed from all Components to the extent feasible, or is otherwise rendered not executable. [DRV KRD 0904] {C-P-R-S-T}

CI2-SEC-5.9.4g [NT] (U//FOUO) The KMI shall ensure that all unused network ports are turned off in communication Components. [DRV KRD 0903] {C-P-R-S-T}

CI2-SEC-5.9.4h (U//FOUO) The KMI shall be able to securely upgrade software in remote Components from a central site. [DRV KRD 1101] {Z}

CI2-SEC-5.9.4i [NT] (U//FOUO) The KMI shall ensure that distribution of software to remote Components is provided Information Confidentiality and Information Integrity Services, in accordance with approved doctrine. [DRV KRD 1379] {A-C}

CI2-SEC-5.9.4j (U//FOUO) Components shall be able to receive new, upgraded, or replacement algorithms via properly authenticated and protected downloads. [DRV KRD 1380] {Z}

CI2-SEC-5.9.4k (U//FOUO) When performing automated updates of software or firmware, the KMI shall destroy or dispose of software and firmware in accordance with approved policy, upon user confirmation that the new software or firmware has been installed and is working properly. [DRV KRD 0805] {Z}

5.9.5 (U) Detection of Malicious Logic

(U//FOUO) The KMI needs to attempt to detect and remove malicious logic.

DEFINITION (U) Malicious Logic. Hardware, software, or firmware that is intentionally included or inserted in a system for a harmful purpose.

(U//FOUO) The requirements for detecting malicious logic are as follows:

CI2-SEC-5.9.5a (U//FOUO) The KMI shall employ techniques to protect the system against the insertion of any form of malicious logic, including but not limited to computer viruses and worms, Trojan horse, and logic bombs. [DRV KRD 1020] {Z}

CI2-SEC-5.9.5b (U//FOUO) The KMI shall test for the presence of malicious logic when the system is initialized, when the system is updated, and periodically during operation, especially when data files are received. [DRV KRD 1020] {Z}

CI2-SEC-5.9.5c (U//FOUO) Nodes and Independent Components of Nodes that read portable electronic media shall be able to scan that data media for computer viruses using one or more DoD-approved commercial virus checking tools, in accordance with Annex G, *Computer Virus and Malicious Code Prevention,* of the *NSA/CSS Operational Information Systems and Networks Security Manual*. [NSA130-1]. [DRV KRD 1437] {C-P-R-S-T}

CONTROL (U//FOUO) **ECVP-1 Virus Protection (Availability**). "All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates." [DoDI8500.2]

(U//FOUO) The following requirements implement the ECVP control:

CI2-SEC-5.9.5d (U//FOUO) The KMI shall automatically update its malicious logic detection information (e.g. virus definitions) on a time period set by a Security Configuration Manager, and shall use the most recent version of this information when checking Components for malicious software. [DRV KRD 2143] {Z}

CI2-SEC-5.9.5e (U//FOUO) The KMI shall implement technical mechanisms to ensure that only malicious software detection information (e.g. virus definitions) obtained from authenticated, authorized sources is used for detecting malicious logic. [DRV KRD 2144] {Z}

5.10 (U) Testing

POLICY (U//FOUO) **General Policy on Testing.** The Security-Sensitive Functions of Components must be well-tested before deployment to ensure that they will satisfy security requirements when in operational use.

CONTROL [NT] (U//FOUO) **DCCT-1 Compliance Testing (Availability**). "A comprehensive set of procedures is implemented that tests all patches, upgrades, and new [automated information system] applications prior to deployment." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **ECMT-2 Conformance Monitoring and Testing (Confidentiality**). For Components that process classified information, "Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities." [DoDI8500.2]

CONTROL [NT] (U//FOUO) **ECMT-1 Conformance Monitoring and Testing (Confidentiality)**. For Components that process sensitive information, "Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD [Information Assurance Vulnerability Alert] or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities." [DoDI8500.2]

(U//FOUO) Successful implementation requires that KMI components be tested to ensure that security services are delivered as required and specified. The specific requirements for security testing are as follows:

CI2-SEC-5.10a [NT] (U//FOUO) Before operational deployment of Components, their Security-Sensitive Functions shall be tested and found to work as required by the system specifications and guidance documentation. [KRD NEW] {Z}

CI2-SEC-5.10b [NT] (U//FOUO) Before operational deployment of Components, their Security-Sensitive Functions shall be tested to assure that there are no obvious ways for an unauthorized entity to bypass or otherwise defeat the security protection mechanisms. [KRD NEW] {Z}

CI2-SEC-5.10c [NT] (U//FOUO) Before operational deployment of Components, their Security-Sensitive Functions shall be tested as specified in applicable Protection Profiles (see "Computer Security" section) and by the DITSCAP process (see "Certification and Accreditation" section) [DITSCAP]. [KRD NEW] {Z}

(This Page Left Blank Intentionally)

6. (U) GLOSSARY OF ACRONYMS

AKP	Advanced Key Processor
ASWR	Attack Sensing, Warning, and Response
CA	Certification Authority
CI-2	Capability Increment 2
COTS	Commercial Off-The-Shelf
CNSS	(U.S.) Committee on National Security Systems (formerly "NSTISSC")
CSN	Central Services Node
DAA	Designated Approving Authority
DEERS	(U.S.) Defense Enrollment Eligibility Reporting System
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	(U.S.) Defense Message System
DN	(X.500) Distinguished Name
DoD	(U.S.) Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
ECU	End Cryptographic Unit
EDI-PI	Electronic Data Interchange Person Identifier
EAL	Evaluation Assurance Level
FOUO	For Official Use Only
GOTS	Government Off-The-Shelf (i.e., developed under Government auspices)
IA	Information Assurance
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System
IT	Information Technology
KMI	(U.S. DoD) Key Management Infrastructure
KMS	Key Management System
KPC	KMI Protected Channel
KRD	KMI Requirements Database
KT#	KMI Token Number
KU#	KMI User Number
MAC	Mission Assurance Category [DoDI8500.2]
MPMSS	Mission Planning, Management, And Support System
NCSC	(U.S.) National Communications Security Committee
NIAP	(U.S.) National Information Assurance Partnership
NIST	(U.S.) National Institute of Standards and Technology
NSA	(U.S.) National Security Agency
NSTISSI	(U.S.) National Security Telecommunications and Information Systems Security Instruction
NSTISSP	(U.S.) National Security Telecommunications and Information Systems Security Instruction
NT	Non-Technical (see "Requirement Statements" section)
OCSP	On-Line Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public-Key Infrastructure

PRSN	Primary Services Node
PSN	Product Source Node
SAMI	Sources And Methods Intelligence
SSAA	System Security Authorization Agreement

7 (U) GLOSSARY OF TERMS

(U//FOUO) This glossary lists the terms for which this volume has DEFINITION statements.

(U//FOUO) Access. The ability and the means to communicate with, or otherwise interact with, a system's resources in order to either (1) handle data held by the system or (2) control system Components and their functions.

(U//FOUO) Access Control. A service that protects against unauthorized Access to System Resources (including protecting against use of a System Resource in an unauthorized manner by a User that is authorized to use the resource in some other manner).

(U//FOUO) Advanced Key Processor (AKP). A cryptographic device that performs all Type 1 cryptographic functions for a Client Host and contains (1) the interfaces to exchange information with a Client Host, (2) the interfaces to interact with fill devices and (3) the interfaces to connect a Client Host securely to the PRSN.

(U//FOUO) Archive. (1.) *Noun*: A collection of data that is stored for a relatively long period of time for historical and other purposes, such as to support non-repudiation service or audit service. (2.) *Verb*: To store data in such a way.

(U//FOUO) Attack. An intentional Threat Action, i.e., an act by which an intelligent System Entity attempts to evade security measures and violate security policy.

(U//FOUO) Authorization (or Privilege). A right that is granted to a System Entity to have Access to a System Resource for a specific purpose.

(U//FOUO) Audit. A security service that performs an independent review and examination of records of system activities to find security violations.

(U//FOUO) Audit Event. A system event that has been determined to have sufficient security relevance to require that data be recorded for audit purposes.

(U//FOUO) Audit Trail. A chronological set of data records describing system activities that is sufficient to enable reconstruction and examination, from inception to final result, of the sequence of environments and states surrounding or leading to an event of interest.

(U//FOUO) Authentication Material. A unit of information that a Registered User employs to prove a claimed User Identity when accessing the system.

(U//FOUO) Availability Service. A security service that ensures that a system is accessible and usable upon demand by an authorized User.

(U//FOUO) Client Host. The key management computing platform, with multiple configurations, that either connects to an AKP to form the KMI equivalent of an LMD/KP or operates without an AKP to provide reduced access to KMI services.

(U//FOUO) Client Node. The most general, abstract and high level way to refer to any version of a KMI component that will allow KMI Human users to communicate over a network to a PRSN and/or perform localized KMI functions.

(U//FOUO) Communication Association. A cooperative relationship among Components or other System Entities, for the purpose of transferring information between them.

(U//FOUO) Communication Channel. An information transfer path implemented between Components or other System Entities

(U//FOUO) Component. A set of System Resources that (1) forms a physical or logical part of the system, (2) has specified functions and interfaces, and (3) is treated, by policies or requirement statements, as existing independently of other parts.

(U//FOUO) Component Identity. A special case of User Identity; the collective aspect of a set of attribute values (i.e., characteristics) by which a Component is recognized or known by other Components and which is sufficient to distinguish that Component (1) from all other identities of that same Component and also (2) from all identities of all other Components and all Registered Users.

(U//FOUO) Computer Network. A collection of host computers together with the communication infrastructure (a “subnetwork”) through which the hosts can exchange data.

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

(U//FOUO) COMSEC Material. “Item(s) designed to secure or authenticate information. COMSEC material includes, but is not limited to: key, products, equipment, modules, devices, documents, hardware, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.” [NSTISSI4005F]

(U//FOUO) Configuration Control. The process of controlling modifications to the KMI design, hardware, firmware, software, and documentation that provides sufficient assurance the system is protected against the introduction of unauthorized or improper modifications before, during, and after system implementation. [NCSCTG6]

(U//FOUO) Configuration Management. The management of changes made to KMI hardware, firmware, software, documentation, test plans, test fixtures, and test documentation throughout the development and operational life of the system. [NCSCTG6]

(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.

(U//FOUO) Credential. Information, passed from one entity to another, used to establish the sending entity’s access rights [CNSSI4009].

(U//FOUO) Data Origin Authentication Service. A Security Service that verifies, to an entity that uses the service, the identity that is claimed to be the original source of data received by the entity.

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

(U//FOUO) Denial of Service. The intentional or unintentional prevention of authorized access to System Resources or delaying of time-critical operations.

(U//FOUO) Discretionary Audit Event. An Audit Event that a Component records in the Audit Trail unless an authorized Manager directs that it should not be recorded.

(U//FOUO) End Cryptographic Unit (ECU). A device that (1) performs cryptographic functions, (2) may be part of a larger system for which the device provides security services, and (3), from the viewpoint of a supporting security infrastructure such as the KMI, is the lowest identifiable component with which a management transaction can be conducted [NSAECU].

(U//FOUO) Equipment Type. A item of standalone equipment—or an assembly of such items intended to be installed and operated as a unit—of which one or more essentially identical replicas are installed in various facilities of the KMI.

(U//FOUO) External System. An information system (other than the EKMS) separate from the KMI, to which the KMI sends requests for data needed to support KMI operations, and from which the KMI receives requested data.

(U//FOUO) Fill Device. A COMSEC device used to transfer or store key in electronic form or to insert key into a crypto-equipment, including ECUs [CNSSI4009].

(U//FOUO) General Device. A User Device that has a User Identity for which the registration has significance across the entire KMI (i.e., it is registered at a PRSN) and for which a product can be generated and wrapped by a PSN for distribution to that specific device. (Volume 1 uses the synonym KMI-Aware Device.)

(U//FOUO) Group Identity. A User Identity that is registered for a User Set for which the KMI does not maintain a record of the members of the set (i.e., the KMI does not have knowledge of the Human Users, or User Devices, that belong to the set).

(U//FOUO) Handle. Perform processing operations on data, such as receive and transmit, collect and disseminate, create and delete, store and retrieve, read and write, and compare.

(U//FOUO) Handling Restriction. A type of Access Control other than the rule-based protections of mandatory access control and the identity-based protections of discretionary access control, and is usually procedural in nature.

(U//FOUO) Hardware Token. A Registered User's individual cryptographic device, that carries the user's Authentication Material and associated Identifier Credentials, cryptographic algorithms, and keying material.

(U//FOUO) Host. A computer that is attached to a communication subnetwork and can use services provided by the subnetwork to exchange data with other attached systems.

(U//FOUO) Human User. A human being that is registered to be a User.

(U//FOUO) Identifier Credential. A data object that is a portable, secure representation of the association between a User Identifier and some Authentication Material, and that can be presented for use in proving a claimed identity to which that User Identifier has been assigned.

(U//FOUO) Identifier Registration Data. A subset of the User Registration Data that describes a specific User Identifier.

(U//FOUO) Identifier Registration State. A KMI-Unique User Identifier that has been registered for accessing the KMI and also is currently authorized to do so, is in the Active State. A KMI-Unique User Identifier that has been registered for accessing the KMI but is not currently authorized to do so, is in the Inactive State.

(U//FOUO) Identity Registration Data. A subset of the User Registration Data that describes a specific User Identity.

(U//FOUO) Identity Registration State. A User Identity is in the Active State if the identity is currently authorized to be used to access the KMI. Otherwise, the identity is in the Inactive State.

(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.

(U//FOUO) Information Confidentiality Service. A security service that protects information from being disclosed or made available to unauthorized System Entities.

(U//FOUO) Information Integrity. The property that ensures that information has not been changed, destroyed, or lost in an unauthorized or accidental manner. (This property is concerned with the constancy of data values, i.e., information content that is encoded in data, and not with how accurately the information was recorded or how trustworthy the information source was.)

(U//FOUO) Information Integrity Service. A security service that protects against unauthorized changes to information—including both intentional and accidental change and destruction—by ensuring that such changes are detectable.

(U//FOUO) Identity Registration State. A User Identity is in the Active State if the identity is currently authorized to be used to access the KMI. Otherwise, the identity is in the Inactive State.

(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.

(U//FOUO) KMI Extend Trust. A term that refers to situations in which the KMI interacts with non-KMI key management systems, i.e., systems that are outside of KMI and are not subject to the authority of this *Policy*.

(U//FOUO) KMI Token Number (KT#). A KMI-unique value that the KMI associates with a Hardware token.

(U//FOUO) KMI-Unique User Identifier. A User Identifier that (1) can be used to access the KMI, (2) takes a form specified in the *KMI Policy for Registration of Users* [NSAKMIRU], and (3) is unique among all current and past User Identities (i.e., is associated with one and only one User Identity and thus enables the KMI to distinguish that Identity and its User from all other System Entities).

(U//FOUO) KMI User Number (KU#). A KMI-unique value that the KMI assigns to a Registered User and that is used in the system's internal database as an index, label, or abbreviated name for associating data elements pertaining to that user.

(U//FOUO) Limited Device. A User Device that has a User Identity 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.

(U//FOUO) Malicious Logic. Hardware, software, or firmware that is intentionally included or inserted in a system for a harmful purpose.

(U//FOUO) Management Client (MGC). The specific configuration of a Client Host which operates in conjunction with an AKP to perform management of products and services for the KMI – KMI equivalent of an LMD/KP.

(U//FOUO) Mandatory Audit Event. An Audit Event that a Component always records in the Audit Trail.

(U//FOUO) Mobile code. "Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient." [DoDD8500.1]

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

(U//FOUO) Non-KMI User Identifier. A User Identifier that (1) cannot be used to access the KMI as a user and (2) either takes the same form as a KMI-Unique User Identifier or takes some other form.

(U//FOUO) Non-Repudiation with Proof of Origin. A security service that provides the recipient of data with evidence that can be retained and that proves the origin of the data, and thus protects the recipient against any subsequent attempt by the originator to falsely deny sending the data.

(This service can be viewed as a stronger version of a data origin authentication service, because it can verify identity to a third party.)

(U//FOUO) (U) Non-Repudiation with Proof of receipt. A security service that provides the originator of data with evidence that can be retained and that proves the data was received as addressed, and thus protects the originator against a subsequent attempt by the recipient to falsely deny receiving the data.

(U//FOUO) Outside User. A Registered User that is not directly subject, or not fully subject, to U.S. Government authority for enforcing this *Security Policy*.

(U//FOUO) PDE-Enabled Device. A User Device that is a General Device and also is equipped to be able to connect as a Client Node to a PRSN PDE to obtain KMI products and services.

(U//FOUO) Peer-Entity Authentication Service. A Security Service that verifies an identity claimed by or for a System Entity in a Communication Association.

(U//FOUO) Protected Channel (KPC). A KMI communication channel that provides (1) information integrity service; (2) either information origin authentication service or peer entity authentication service, as is appropriate to the mode of communication; and (3), optionally, information confidentiality service.

(U//FOUO) Protection Profile. An implementation-independent set of security assessment requirements for a category of information technology products or systems, and their associated administrator and user guidance documentation, that meet specific consumer needs. [IS15408-1]

(U//FOUO) Registered User (abbreviated as User). A System Entity that is authorized to access the KMI by invoking an identity that has previously been established in the system.

(U//FOUO) Response. Initiating a counteraction to an attack or other Threat Action.

(U//FOUO) Security Domain. A set of System Entities and System Resources that operate under a common security policy, including operating at the same security level. [KMI2200V3]

(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. [KMI2200V3]

(U//FOUO) Security Service. A processing or communication service that is provided by a system to give a specific kind of protection to System Resources [RFC2828].

(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. [KMI2200V3]

(U//FOUO) Security-Sensitive Event. An event that attempts to change the security state of a KMI Component or attempts to violate the KMI *Security Policy*.

(U//FOUO) Security-Sensitive Function. A system function that must operate correctly in order to ensure adherence to the KMI *Security Policy*.

(U//FOUO) Sensing. Recognizing, identifying, and categorizing attacks and other Threat Actions.

(U//FOUO) Sensitive Information. "Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code, "The Privacy Act" ... , but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of Title 15, United States Code, "The Computer Security Act of 1987" ... .) This includes information in routine DoD payroll, finance, logistics, and personnel management systems." [DoDD 8500.1]

(U//FOUO) Set Identity. A User Identity that is registered for a User Set composed either (1) entirely of Human Users or (2) entirely of User Devices.

(U//FOUO) Shared Identity. A User Identity that is registered for a User Set in which each member of the set is authorized to assume that identity individually, and for which the KMI maintains a record of members of the set. [KRD 365, 366]

(U//FOUO) Singular Identity. A User Identity that is registered for exactly one, specific Human User or User Device.

(U//FOUO) Site. A facility—i.e., a physical space, room, or building together with its physical, personnel, administrative, and other safeguards—in which system functions are performed.

(U//FOUO) Subnetwork. A system of packet relays and connecting links that implement a communication service to interconnect attached computers that subscribe to the service.

(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 KMI's environment and that incorporates some specific set of capabilities.

(U//FOUO) System Integrity. The quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

(U//FOUO) System Integrity Service. A security service that protects system Components in a verifiable manner against unauthorized change throughout their lifetime.

(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 site facility that houses these things.

(U//FOUO) Technical Protection Policy. A set of security requirements that apply to a specific KMI task area (e.g., product ordering, generation, or distribution) or other focus of attention.

(U//FOUO) Token Data. The set of attribute values acquired by, and stored in, the system for the purpose of establishing and describing a Hardware Token.

(U//FOUO) Token Holder. The Human User who is assigned to be accountable for the use of Authentication Material and other security-sensitive material that is carried by a Hardware Token.

(U//FOUO) User. See Registered User.

(U//FOUO) User Authentication. A security service that verifies a User Identity that is claimed by or for a System Entity that attempts to access the KMI.

(U//FOUO) User Core Data. A subset of the User Registration Data, that (1) distinguishes a Registered User from all other Registered Users, (2) has the same values for all User Identities of the User, and (3) includes some attributes that have values that remain constant over the life of the User. [DRV KRD 1588]

(U//FOUO) User Device. An automated process—a specific hardware unit with specific software running on it—that is registered to act as a User, either a User that accesses the KMI directly or one that is receives KMI products and services indirectly.

(U//FOUO) User Device Sponsor. The Primary KOA Manager of the KOA that is currently accountable for use of a User Device; i.e., the KOA to which a User Device is currently assigned.

(U//FOUO) User Identifier. A name that can be unambiguously represented by a printable, non-blank character string.

(U//FOUO) User Identity. The collective aspect of a set of attribute values (i.e., characteristics) by which a specific individuality of a Registered User is recognized or known by the KMI and which are sufficient to distinguish the identity from (1) any other identities of that same user and also from (2) identities of other Registered Users.

(U//FOUO) User Number. See “KMI User Number”.

(U//FOUO) User Registration. The process that (1) initializes an identity in the KMI for a System Entity that is authorized to access the KMI, (2) associates an identifier with the identity, (3) may also associate authentication material with the identifier, and (4), depending on the authentication mechanism being used, may also issue or association an identifier credential (see “Identifier Credentials” section).

(U//FOUO) User Registration Data. The set of attribute values acquired by, and stored and maintained in, the KMI to establish and describe a Registered User.

(U//FOUO) User Set. A set that consists either (1) entirely of Human Users or (2) entirely of User Devices, and is registered to act as a single User.

(U//FOUO) User Set Sponsor. A Human User, represented in the KMI by a User Identity, who (1) requests that a new User Identity be registered for a User Set and then (2) continues to officially represent the KMI customer organization that is accountable for use of the new identity.

(U//FOUO) User Sponsor. A Human User, represented in the KMI by a User Identity, who (1) requests that a new User Identity be registered for a User Device or a User Set and (2) officially represents the KMI customer organization that is accountable for use of the new identity.

(U//FOUO) Warning. 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.

(This Page Left Blank Intentionally)

8. (U) REFERENCES

(U) Policies, standards, and specifications listed here should be replaced by the latest approved version, if there is a newer one.

(U) AF36-3026(I) Air Force Instruction 36-3026(I) (also Army Regulation 600-8-14; BUPERS Instruction 1750.10a, Change 1; Marine Corps Order P5512.11b, Change 1; Commandant Instruction M5512.1; Commissioned Corps Personnel Manual 29.2, Instructions 1 And 2), Personnel Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel, 14 July 1998

(U) ASDC3I97 Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, *Secret and Below Interoperability (SABI)*, 20 March 1997.

(U) CJCS Chairman of the Joint Chiefs of Staff, *Information Operations Condition*, CJCS Memorandum CM-510-9910, Mar 1999.

(U) CNSSI4009 Committee on National Security Systems, *National Information System Security (INFOSEC) Glossary*, CNSS Instruction No. 4009, May 2003.

(U) CNSSP14 ———, *National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Authorized U.S. Activities that are Not a Part of the Federal Government*, CNSSP No. 14, November 2002.

(U) CSCSTD002 DoD Computer Security Center, *DoD Password Management Guideline*, CSC-STD-002-85, 12 April 1985.

(U) DISACOE Defense Information Systems Agency, Global Information Grid Enterprise Services Organization, *Common Operating Environment (COE) Integration and Runtime Specification (I&RTS)*, Version 4.3, Oct 2003.

(U) DITSCAP DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, 30 December 1997. [This instruction is expected to be superseded by DoDI 8510.bb, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*.]

(U) DoDD5200.19 DoD Directive C-5200.19, *Control of Compromising Emanations*, 16 May 1995 (or as updated, if there is a later version).

(U) DoDD5200.5 DoD Directive C-5200.5, *Communications Security (COMSEC)*, 21 April 1990.

(U) DoDD5400.11 DoD Directive 5400.11, *DoD Privacy Program*, 13 Dec 1999.

(U) DoDD8500.1 DoD Directive 8500.1, *Information Assurance*, 24 October 2002.

(U) DoDD8550 DoD 8550.dd, *Biometric Technologies*, DRAFT, 2002.

(U) DoDGDS DoD, *Global Directory Service Naming Conventions*, Draft, version 0.7, 10 Apr 2002.

(U) DoDI8500.2 DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, 6 Feb 2003.

(U) DoDR5200.2 DoD Regulation 5200.2-R, *DoD Personnel Security Program Regulation*, January 1987.

(U) DoDR5200.8 DoD Regulation 5200.8, *Security of DoD Installations and Resources*, 25 April 1991.

(U) DoDX509CP ASD C3I, *X.509 Certificate Policy for the U.S. Department of Defense*, version 9.0, 9 Feb 2005.

(U) EKMS322 National Security Agency, *EKMS FIREFLY Specification*, EKMS 322 Revision B inc. SCN-1, 15 Apr 2002,

(U) FIPS112 U.S. Department of Commerce, *Password Usage*, Federal Information Processing Standards Publication (FIPS PUB) 112, 30 May 1985.

(U) FIPS140 National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2, 25 May 2001, as modified by subsequent Change Notices.

(U) HAIPE *Interoperability Specification for High Assurance Internet Protocol Encryptor (HAIPE) Devices*, Version 2.0 Charlie, 3 Jan 2003.

(U) IATF National Security Agency, *Information Assurance Technical Framework (IATF)*, Release 3.1, September 2002, or latest release.

(U) IS7498-2 International Standards Organization, *Information Processing Systems — Open Systems Interconnection Reference Model — Basic Reference Model — Part 2: Security Architecture*, IS 7498-2.

(U) IS15408-1 Common Criteria Implementation Board, *Common Criteria for Information Technology Security Evaluation*, ver. 2.1, CCIB-98-031, August 1999: Part 1: *Introduction and General Model*;

(U) IS15408-2 _____, Part 2: *Security Functional Requirements*.

(U) IS15408-3 _____, Part 3: *Security Assurance Requirements*.

(U) KMI1001 National Security Agency, *KMI 1001: A Concept for the KMI*, 16 June 1999

(U) KMI1011 _____, *KMI 1011: Roadmap for Key Management Capabilities for the Department of Defense*, draft version 0.4, 11 Feb 2002.

(U) KMI2200 _____, *System Description and Requirements Specification for Key Management Infrastructure (KMI) Capability Increment 2 (CI-2)*, KMI 2200, version 1.25 (“SRS F”), 28 February 2005, including the following:

(U) KMI2200V1 _____, _____, Volume 1: *Key Management Functions and Related Requirements*, version 1.25 (“SRS F”), 28 February 2005.

(U) KMI2200V3 _____, _____, Volume 3: *System Security Architecture and Related Requirements*, version 1.25 (“SRS F”), 28 February 2005.

(U) KMI2211 ———, *KMI Program Glossary*, KMI 2211, DRAFT, 2003.

(U) KMI3001 _____, *Electronic Serial Number Standard*, draft 0.71, 24 Oct 2003.

(U) MJCS20-89 Joint Chiefs of Staff, *Implementation of Multicommand Required Operational Capability (MROC) 3-88, the Defense Message System (DMS*), memorandum MJCS-20-89, 6 February 1989.

(U) NCSCTG1 National Computer Security Center, *A Guide to Understanding Audit in Trusted Systems*, NCSC-TG-001, 1 June 1988.

(U) NCSCTG4 _____, *Glossary of Computer Security Terms*, NCSC-TG-004, 21 October 1988.

(U) NCSCTG6 _____, *A Guide to Understanding Configuration Management in Trusted Systems*, NCSC-TG-006, 28 March 1988.

(U) NISCAP National Security Agency, *NSA/CSS Information System Certification and Accreditation Process (NISCAP) Guide*, version 2.0, 31 July 2002.

(U) NSA130-1 National Security Agency, *NSA/CSS Operational Information Systems and Networks Security Manual*, NSA/CSS Manual 130-1.

(U) NSAC02-00 _____, *Fail-safe Design & Analysis: Revised*, C Technical Report 02-00 27 Jan 2000, SECRET//REL TO USA, AUS, CAN, and GBR.

(U) NSAECU ———, *ECU Lifecycle Model*, Technical Report, version 0.4, 5 August 2003.

(U) NSAKMIEM ———, *KMI Policy for Enrollment of Managers*, [to be provided by the Government].

(U) NSAKMIRU ———, *KMI Policy for Registration of Users*, [to be provided by the Government].

(U) NSAUIC _____, *The Unified Information Security Criteria as Tailored for KMI CI-2*, [to be prepared by NSA]. (The UIC are expected to be tailored for CI-2 by separately listing a set of criteria for each type of Node or each major, distinct Component.)

(U) NSTISSI4005 NSTISSI No. 4005, *Safeguarding Communications Security (COMSEC) Facilities and Material*, August 1997

(U) NSTISSI4005F Annex F, *Safeguarding COMSEC Material in Electronic Form*, in NSTISSI No. 4005 [NSTISSI4005].

(U) NSTISSI7000 NSTISSI No. 7000, *TEMPEST Countermeasures for Facilities*, 29 November 1993.

(U) NSTISSI7001 NSTISSI No. 7001, *NONSTOP Countermeasures*, June 1994.

(U) NSTISAM2-95 NSTISSAM TEMPEST/2-95, *RED/BLACK Installation Guidance*, 12 December 1995

(U) NSTISSI4005F Annex F, *Safeguarding COMSEC Material in Electronic Form*, in NSTISSI No. 4005 [NSTISSI4005].

(U) NSTISSP8 National Security Telecommunications and Information Systems Security Committee (NSISSC), *National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Foreign Governments*, NSTISSP No. 8, 13 February 1997.

(U) NSTISSP11 _____, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, NSTISSP No. 11, January 2000.

(U) OASD2002 Office of the Assistant Secretary of Defense (OASD), *National Information Assurance Acquisition Policy*, policy memorandum of 6 Aug 2002.

(U) PF1 *DoD Public Key Infrastructure Target Class 4 Token Protection Profile*, version 1.01, 8 September 2000 (or as updated, if there is a later version).

(U) PF3 *U.S Department of Defense Directory Protection Profile for Medium Robustness Environments*, Version 2.0, 9 April 2003 (or as updated, if there is a later version).

(U) PF7 *A Goal VPN Protection Profile for Protecting Sensitive Information*, version 2, 10 July 2000 (or as updated, if there is a later version).

(U) PF8 *Single Level Operating Systems in Environments Requiring Medium Robustness*, version 1.22, 23 May 2001 (or as updated, if there is a later version).

(U) PF9 *Traffic Filtering Firewall Protection Profile for Medium Robustness*, version 1.4, 1 May 2000 (or as updated, if there is a later version.

(U) PF10 *U.S. Department of Defense Application Firewall for Medium Robustness*, version 1.0, 28 June 2000 (or as updated, if there is a later version.

(U) PF11 *Intrusion Detection System Analyzer Protection Profile*, version 1.1, 10 Dec 2001 (or as updated, if there is a later version).

(U) PF12 *Intrusion Detection System Sensor Protection Profile* version 1.1, 10 Dec 2001 (or as updated, if there is a later version).

(U) PF13 *Intrusion Detection System Scanner Protection Profile*, version 1.1, 10 Dec 2001 (or as updated, if there is a later version).

(U) PF14 *Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness)*, version 3.0, 29 mar 2002.

(U) PF15 *U.S. Government Firewall Protection Profile for Medium Robustness Environments*, version 1.0, 28 October 2003.

(U) PF16 *Intrusion Detection System*, version 1.4, 4 Feb 2002.

(U) REFTBD13 [TBD: Need reference that specifies rules for FIREFLY Credentials, similar to *X.509 Certificate Policy for the U.S. Department of Defense*.]

(U) RFC2828 R. Shirey, *Internet Security Glossary*, Request for Comment 2828, May 2000.

(U) RFC3280 R. Housley, W. Polk, W. Ford, and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Request for Comment 3280, Apr 2002.

(U) USGT1CP National Security Agency, *United States Government Type 1 Certificate Policy*, 28 Jul 2005.

(This Page Left Blank Intentionally)

Appendix A (U) Identity and Eligibility Proofing for Users

(U//FOUO) For each User Identity, a Registration Manager examines evidence to verify both authenticity—i.e., that the KMI User has the right to claim the identity being registered—and eligibility—i.e., that the identity is eligible for KMI registration. This appendix invites discussion of how to specify the documentation required as evidence.

(U//FOUO) For example, the *X.509 Certificate Policy for the U.S. Department of Defense* [DoDX509CP] requires an applicant for a Medium or High Assurance certificate to present at least one Federal Government official picture identification credential (such as a DoD identification card or passport), or two non-Federal official identification credentials, at least one of which must be a photo ID, such as a driver's license. The *Certificate Policy* permits other mechanisms of equivalent or greater assurance—such as comparison of biometric data to identities pre-verified to the standards of the *Certificate Policy*, and obtained via authenticated interaction with secured databases—to be used as an alternative to presentation of the credentials.

(U//FOUO) The requirements of the *Certificate Policy* are unnecessarily vague. It is possible to be more precise in specifying the acceptable credentials. To show this, Subsection A.1 presents a worked example of a U.S. Government requirement to provide evidence for verification of identity.

(U//FOUO) The *Certificate Policy* also specifies that requests for certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. Also, the certificate management authority is required to verify that information, in addition to the authenticity of the requesting representative, and to verify the representative's authorization to act for the organization. These requirements are even vaguer than for personal identity proofing. Further, for both persons and organizations, the *Certificate Policy* does not distinguish the need to verify identity from the need to verify eligibility. However, the worked example in Subsection A.1 does separately and precisely specify the evidence required to proof both identity and eligibility.

(U//FOUO) Subsection A.2 suggests KMI draft requirements, based on the example in subsection A.1, for evidence of identity and eligibility. In final form, the KMI policy and requirements might be a separate document or be included in an existing operational procedure.

A.1 Worked Example: Documents Required for Employment in the U.S.

(U//FOUO) The U.S. Immigration and Naturalization Service's Employment Eligibility Verification Form—Form I-9 (Rev. 11-21-91) N—requires U.S. employers to examine evidence of personal identity and employment eligibility of job applicants. Applicants are required to present original documents listed below, either one from Group A, or one from each of Group B and C:

(U//FOUO) **Group A.** Documents that establish both identity and employment eligibility:

1. U.S. Passport (expired or unexpired)

2. Certificate of U.S. Citizenship (INS Form N-560 or N-561).
3. Certificate of Naturalization (INS Form N-550 or N-570).
4. Unexpired foreign passport, with I-551 stamp or attached INS Form I-94 indicating unexpired employment authorization.
5. Alien Registration Receipt Card with photograph (INS Form I-151 or I-551).
6. Unexpired Temporary Resident Card (INS Form I-6689)
7. Unexpired Employment Authorization Card (INS Form I-688A).
8. Unexpired Reentry Permit (INS Form I-327)
9. Unexpired Refugee Travel Document (INS Form I-571)
10. Unexpired Employment Authorization document issued by the INS which contains a photograph (INS Form I-688B).

(U//FOUO) **Group B.** Documents that establish Identity:

1. Driver's license or ID Card issued by a state or outlying possession of the U.S., provided it contains a photograph or information such as name, date of birth, sex height, eye color, and address.
2. ID card issued by federal, state, or local government agencies or entities provided it contains a photograph or information such as name, date of birth, sex, height, eye color, and address.
3. School ID card with a photograph.
4. Voter's registration card.
5. U.S. Military card or draft record.
6. Military dependents ID card.
7. U.S. Coast Guard Merchant Mariner Card.
8. Native American tribal document.
9. Driver's license issued by a Canadian government authority.

(U//FOUO) For persons under age 18 who are unable to present one of B1 through B9:

10. School record or report card.
11. Clinic, doctor, or hospital record.
12. Day-care or nursery school record.

(U//FOUO) **Group C.** Documents that establish employment eligibility:

1. U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment).
2. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350).
3. Original or certificated copy of a birth certificate issued by a state, county municipal authority or outlying possession of the U.S. bearing an official seal.
4. Native American tribal document.
5. U.S. Citizen ID Card (INS Form I-197)
6. ID Card for use of Resident Citizen in the United States (INS Form I-179)
7. Unexpired employment authorization document issued by the INS (other than A1 through A10).

A.2 Proposed Evidence Required for Registration of KMI User Identities

(U//FOUO) This section proposes policy and requirements for documentary evidence for registering identities for KMI Human Users.

POLICY (U//FOUO) A User Registration Manager must examine and verify evidence of authenticity and eligibility before either registering a person as a User or registering an additional User Identity for a person that is already a Registered User.

REQUIREMENT (U//FOUO) As evidence for KMI identity registration, an applicant shall present one or more credentials as specified below:

A.2.1 (U) Registration for KMI Human Users

(U//FOUO) To register as a new Human User and establish the first User Identity for that user, a person presents a document from each of Groups 1A and 1C. To register an additional KMI identity, a person that is already registered as a Human User presents a document from each of Groups 1A, 1B, 1C.

Group 1A. (U//FOUO) Proof of New Identity for a KMI Human User. Only the documents listed here may be used to prove an identity to be registered for a Human User.

1. U.S. Passport (expired or unexpired).
2. Certificate of U.S. Citizenship (INS Form N-560 or N-561).
3. Certificate of Naturalization (INS Form N-550 or N-570).
4. Driver's license or age verification card issued by a state or outlying possession of the U.S., provided the document contains (1) a photograph of the subject and (2) descriptive information for the subject, such as full name, date of birth, sex, height, and residential address.
5. Employee or contractor ID card issued by a federal, state, or local government agency, provided the document contains (1) identification of the issuer, (2) a photograph of the subject, and (3) descriptive information for the subject, such as full name and employee identification number.
6. Directly collected biometric data—e.g., fingerprint, hand geometry measurement, retina scan—that is obtained via in-person interaction and that is verified by comparing it to securely obtained identity data that has been pre-verified to the standards of this policy and stored in a secured database.
7. [Are there other forms of evidence that are equally strong and acceptable? Are there other forms that will need to be accepted in order to handle the full range of KMI Human Users?]

(U//FOUO) **Group 1B.** Proof of Existing Identity for a KMI Human User. Only the documents listed here may be used to prove an already registered identity for a Human User. (These obviously should be identity documents that are issued by or in conjunction with KMI registration. Items 1 through 7 are those currently issued by [AF36-3026(I)]. In the future, this list should include the DoD Common Access Card.)

1. DD Form 2, Armed Forces of the United States Identification Card (Active) (manually-prepared card or machine-readable card).
2. DD Form 2, United States Uniformed Services Identification Card (Retired) (manually-prepared card or machine-readable card).
3. DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Reserve) or United States Uniformed Services Identification Card (Reserve Retired (manually-prepared card or machine-readable card).
4. DD Form 1173, Uniformed Services Identification and Privilege Card (manually-prepared card or machine-readable card).
5. DD Form 1173-1, Department of Defense Guard and Reserve Dependent Identification Card (manually-prepared card) or United States Uniformed Services Identification and Privilege Card (machine-readable card).
6. DD Form 489, Geneva Conventions Identity Card for Civilians Who Accompany the Armed Forces.
7. DD Form 1934, Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces.

(U//FOUO) **Group 1C.** Proof of Eligibility for a New Identity for a KMI Human User. Only the documents listed here may be used to prove eligibility for registration for a Human User.

1. DD Form 1172, Application For Uniformed Services Identification Card-DEERS Enrollment, signed by an authorized verifying official as required by [AF36-3026(I)]. (This form is expected to require modification to support KMI registration.)
2. [Processes other than DEERS/RAPIDS that are used to register KMI Human Users should be required to use a form equivalent to selected parts of DD Form 1172.]

Appendix B (U) Accountability with Shared Identities

(U//FOUO) This section provides a top-down analysis of potential ways to design authentication procedures to enable a user to access the KMI in a shared identity. However, of the six ways analyzed, this *Specification* supports only the one designated 2a.

(U//FOUO) The basic strategies that are possible are as follows:

1 (U//FOUO) **First access singular identity and then switch to shared identity**. A person or device first accesses the KMI by presenting and authenticating an identifier that is associated with a singular identity. Then the KMI enables the user to switch from the singular identity to a shared identity for which the user is authorized.

2 (U//FOUO) **Access shared identity without first accessing singular identity.** A person or device directly accesses the KMI in a shared identity without first establishing a session in a shared identity.

(U//FOUO) In case 1, the KMI establishes individual accountability by requiring the user to present a singular identifier. The KMI can then tie that singular identity to the ensuing session for the shared identity, either through audit records or another mechanism. There are two ways to authorize a person or device to switch to the shared identity:

1a (U//FOUO) **Shared identifier has no authentication material**. After singular authentication is successful, the KMI enables the person or device to switch from the singular identity to one of the shared identities for which the singular identity has been authorized, without going through a second authentication step. (Access to the shared identity could be controlled either through an access control list or through attribute certificates issued to singular identities.)

(U//FOUO) In KMI, a use for case 1a might be to cluster identities to simplify their assignment to roles. However, this *Specification* does not support case 1a, because case 2 offers alternatives that are simpler in terms of user interface and KMI mechanism (although perhaps not simpler in terms of managing identifier credentials).

1b (U//FOUO) **Shared identifier has authentication material.** After singular authentication is successful, the authenticated person or device then presents an identifier that is associated with a shared identity to which the user wants to switch.

(U//FOUO) This *Specification* does not support case 1b, because case 2 offers alternatives that are simpler in terms of user interface and KMI mechanism. Also, no need has been identified for case 1b either in KMI or in non-KMI systems.

(U//FOUO) There are four ways to authenticate a person or device that accesses KMI directly through a shared identity in case 2:

2a (U//FOUO) **Shared identifier, separate authentication material**.
2b (U//FOUO) **Shared identifier, shared authentication material**.
2c (U//FOUO) **Separate identifiers, separate authentication material**.
2d (U//FOUO) **Separate identifiers, shared authentication material**.

(U//FOUO) This *Specification* now supports case 2a, but not 2b, 2c, or 2d. The rationale for this is as follows:

2a (U//FOUO) **Shared identifier, separate authentication material**. Each person or device that uses the shared identity presents the same identifier to the KMI, but each uses different authentication material to prove its association with that identity.

(U//FOUO) In case 2a, when the authentication material is a private key, the KMI needs a way to determine which public key to use for the verification step of the authentication service. An implementation could try each certificate in which the subject is the shared identifier, but it is more efficient for the singular user to present the correct certificate along with the identifier, as is commonly done in commercial software.

(U//FOUO) Further, to establish individual accountability in case 2a, the KMI needs a way to determine the singular identity of the user. This could be done with the issuer DN and serial number of the certificate, with a Subject Alternative Name extension in the certificate, or with some other mechanism.

2b (U//FOUO) **Shared identifier, shared authentication material**. Each person or device that uses the shared identity presents the same identifier to the KMI, and each uses the same authentication material to prove its association with that identity.

(U//FOUO) This *Specification* does not support case 2b for authentication, because individual accountability cannot be assured. (When each singular user has the same private key, then any user in the set can masquerade as another user in the set by presenting the other user's certificate to the KMI or any other system.)

(U//FOUO) There are cases in non-KMI systems (and probably also in KMI) where multiple indistinguishable users need to hold the same private key for the same identifier. But such cases use the key pair to provide data confidentiality service and not authentication service. (For example, in the "Group-Individual" situation mentioned above for DMS, all members of a team may need to be able to decrypt queries directed to the group identifier.) Such cases involve increased risk that the private key might be compromised.

2c (U//FOUO) **Separate identifiers, separate authentication material**. Each person or device that uses the shared identity presents a different identifier to the KMI and uses different authentication material.

(U//FOUO) This *Specification* does not support case 2c for authentication because, even though implementation is relatively simpler than for case 2a, the result is the same as if separate singular identities were used.

2d (U//FOUO) **Separate identifiers, shared authentication material**. Each person or device that uses the shared identity presents a different identifier to the KMI, but each uses the same authentication material to prove its association with that identity.

(U//FOUO) This *Specification* does not support case 2d for authentication, because individual accountability cannot be assured. (When each singular user has the same private key, then any user in the set can masquerade as another user in the set by presenting the other user's certificate to the KMI or any other system.) As in case 2b, there are cases where multiple distinguishable users need to hold the same private key, but such cases confidentiality service and not authentication service. (For example, all members of a team may need to be able to decrypt any message directed to any individual team member.)

(This Page Left Blank Intentionally)