



National Security Agency/Central Support Service



INFORMATION ASSURANCE DIRECTORATE

CGS Key Management Capability

Version 1.1.1

Key Management is a service and process that provides, controls, and maintains the cryptographic keys, key material, and certificates required to support a wide range of operational missions. This Capability governs the key lifecycle, which includes key registration, ordering, generation, distribution, usage, expiration, revocation, and destruction. In addition, Key Management includes the functions of compromise management, accounting, handling, audit, and storage.

07/30/2012



CGS Key Management Capability

Version 1.1.1



Table of Contents

1	Revisions.....	2
2	Capability Definition.....	3
3	Capability Gold Standard Guidance	3
4	Environment Pre-Conditions	8
5	Capability Post-Conditions	8
6	Organizational Implementation Considerations	9
7	Capability Interrelationships	10
7.1	Required Interrelationships	10
7.2	Core Interrelationships.....	11
7.3	Supporting Interrelationships.....	11
8	Security Controls.....	12
9	Directives, Policies, and Standards	13
10	Cost Considerations	17
11	Guidance Statements.....	18



CGS Key Management Capability

Version 1.1.1



1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



CGS Key Management Capability



Version 1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Key Management is a service and process that provides, controls, and maintains the cryptographic keys, key material, and certificates required to support a wide range of operational missions. This Capability governs the key lifecycle, which includes key registration, ordering, generation, distribution, usage, expiration, revocation, and destruction. In addition, Key Management includes the functions of compromise management, accounting, handling, audit, and storage.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Key Management Capability encompasses the people, processes, technology, and products involved in the lifecycle of a cryptographic key. This lifecycle includes the registration, ordering, generation, distribution, usage, expiration, revocation, and destruction of keys, key material, and certificates. To ensure proper protection of keys, the Key Management Capability also oversees the functions of compromise management, accounting, handling, audit, and storage. These additional functions are used in every step of the key lifecycle.

Key Management includes remote keying for cryptographic devices, where possible. This is a procedure by which keys are electronically sent to remote cryptographic devices. This process shall be automated where possible, which means that the rekeying can be accomplished without specific actions by an operator at the receiving device. Not all devices will be capable of remote management, particularly legacy systems. All new systems shall be designed to allow for remote management. Remote management functions will work in coordination with other Capabilities (see Communication Protection, Access Management, Credential Management) to ensure that remote management occurs in a secure manner.



CGS Key Management Capability



Version 1.1.1

All keys used to protect classified materials shall be obtained from a source approved by the National Security Agency (NSA). Key Management infrastructures shall allow for interoperability with other Community partners. All key specifications, including key length and cryptographic algorithms, are set according to NSA policy for Type-1 keys. Type-1 algorithms and systems are approved by NSA for encrypting and decrypting classified and sensitive national security information. For other keys types, compliance with NSA, National Institute of Standards and Technology (NIST), Department of Defense (DoD) or commercial standards is recommended.

Interoperability and mission needs may create circumstances that require the use of keys that are not produced in coordination with NSA, such as when working with Organizations such as the North Atlantic Treaty Organization (NATO). In situations such as these, non-NSA sources may be used to obtain key material and certificates, such as a commercial entity or another government Organization. The processes used shall be in alignment with Gold Standard practices and Community policies and approved by NSA.

Certification Authorities (CAs) are a means of ensuring a trust relationship between parties that are unknown to each other. CAs act as trusted third parties that issue digital certificates and verify the identity of the digital certificate holders. If each party has a certificate that has been signed by a trusted CA, the two parties can each trust the identity of the other to the degree that the CA is trusted. CAs operate by cryptographically binding a public key with an attribute or identifier. CAs shall perform their operations in coordination with the Credential Management, Identity Management, and Attribute Management Capabilities. CAs shall be used as necessary to fulfill mission needs. This may mean the establishment of an internal CA or the use of an external CA.

All new systems and devices that use keys shall use electronic keys. Electronic keys can be transferred by electronic means and allow for a greater degree of control in contrast to physical keys. Physical keys may still be required for use in legacy systems. Where possible, legacy systems using physical keys shall be transitioned to new systems that use electronic keys.

When a new system is being developed or deployed for use that requires Type 1 key, a Key Management Plan (KMP) is developed that defines the capabilities of cryptographic devices. Operational Security Doctrine and other policies cover the use, support, and interoperability of all Type 1 cryptographic keys. Systems that already exist shall acknowledge and agree to the rules that are defined in the existing policies. Long-term



CGS Key Management Capability



Version 1.1.1

support (established during account registration) for a key generation agreement is based on these policies.

Throughout the entire Key Management process, every user or non-human entity that interacts with a key, certificates, or key device shall have the authorization to do so. Key Management operates in coordination with other Capabilities (see Access Management, Physical and Environmental Protections) to ensure proper controls are in place, restricting access based on Enterprise policy. Activity logs shall be maintained to ensure accountability for unauthorized actions. Key Management is implemented through the following process:

Registration

Registration has to take place before any Key Management functions can occur. Registration is the process by which an Enterprise establishes a formal relationship with its supplier of certificates or keys. During registration, each account (relationship) is mapped to a controlling party (e.g., Controlling Authority, Command Authority) within the supplier's hierarchy.

Ordering

Keys can be ordered only from a supplier with whom the requester is registered. The controlling party whom the requester is mapped to is accountable for the key ordering. The key request will specify the types of keys required (specification), how many, where they should be delivered, and the key duration. These details will be determined by the type of equipment that will use the keys, the needs of the mission, and the risk tolerance (see Risk Mitigation).

Generation

All cryptographic keys used to protect classified information shall be generated in accordance with NSA policies and use NSA-approved devices. Keys that are generated on an ad hoc basis (e.g., Secure Sockets Layer [SSL]/Transport Layer Security [TLS] keys) shall follow the relevant commercial standard, and also meet NSA implementation requirements.

Distribution

All symmetric keys and asymmetric private keys shall be delivered in encrypted form when possible. These keys shall be protected at the same level as or higher level than the data they will be used to protect. When possible, key material or keys shall be delivered directly from the supplier to the device that will use it, without requiring human



CGS Key Management Capability



Version 1.1.1

intervention. Only the device using the key or key material shall be able to decrypt it, where possible. Automated source authentication and integrity checking shall occur before any keys are used, when possible (see Communication Protection). For systems where these automated checks are not possible, the process for authentication and integrity checking shall be provided by policy.

Asymmetric public keys shall also have source authentication and integrity checks applied to them prior to use, when possible. In a hierarchical implementation, the path that may proceed through a number of intermediate steps shall provide validation to ensure informed trust decisions can be made. Although public keys do not need to be kept confidential themselves, they may have sensitive information associated with them, such as personally identifiable information (PII). In these situations, the key distribution function will work in coordination with other Capabilities to maintain confidentiality of all sensitive information (see Access Management and Data Protection).

For all types of keys and key material distribution, a manager oversees any transfers that take place and verifies that they did, indeed, occur. Key distribution systems shall maintain high availability to accomplish their tasks.

Usage

NSA-approved dedicated cryptographic hardware (e.g., a hardware security module) shall be used for the protection of keys and key material (see Data Protection, System Protection). Systems and devices that use keys are designed to use activation data so that a user can supply the appropriate data and activate the key without ever having direct access to the key.

Devices that use the keys directly shall have constrained user interfaces to prevent keys from being used for unauthorized purposes (see Access Management). Devices that store keys shall monitor the expiration dates of their keys and provide either user notification when the expiration date is near, or the device will automatically request a new key from its appropriate supplier. Devices shall not use keys past their expiration date.

When mission need requires the use of keys outside a secure environment, the key shall be able to be destroyed (access to the key is removed) if necessary to preserve confidentiality. All users who interact with keys shall be trained in their appropriate use, handling, and destruction, including procedures for keeping track of expiration dates. All



CGS Key Management Capability



Version 1.1.1

keys shall be subject to access control (see Access Management, Digital Policy Management) and accountability procedures.

For archival purposes, appropriate contingencies shall be established to obtain sensitive data while maintaining confidentiality requirements (see Contingency Planning). Methods include establishing a protected data archive and instituting a method for key recovery.

Expiration

All keys shall have an expiration date that limits their life. This lifespan will vary depending on the key's use, what mission it supports, and risk tolerance (see Risk Mitigation). When possible and depending on mission needs, keys shall be automatically disabled when they reach their expiration date. Replacing expired keys shall be automated where possible to prevent any service lapse while waiting for the new key to arrive.

Revocation

Keys or certificates shall, from time to time, need to be revoked (superseded) prior to their expiration date. This need could arise for a number of reasons including technology changes or data leaks. There shall be an authenticated manner in which to request revocation. This will ensure that the source requesting the revocation is authorized to do so. When a key is revoked, all relevant parties who may interact with that key shall be notified as soon as possible by the appropriate authoritative source.

When a public-key certificate needs to be revoked, the CA who signed it shall issue a digitally signed notification of the revocation, typically a Certificate Revocation List (CRL). Public-key enabled software shall check the validity of a certificate before using it, referring to the most recent revocation notification available. For revocation of other types of keys or key material, the office that authorized use of the key or key material shall issue a notification (e.g., a supersession message).

Destruction

Procedures shall be in place to destroy a key at any point in the lifecycle should there be a security compromise. All equipment using cryptographic keys shall incorporate anti-tamper mechanisms to detect when it has been compromised and automatically zeroize any keys it is storing. There shall be alternate means with which to destroy the applicable keys when automated key destruction means are not available, such as when the automated destruction function fails, no tampering has occurred, or when a hard copy exists. Part of the training that all key users receive includes proper key destruction procedures so that no residual key data remains, based on mission needs.



CGS Key Management Capability



Version 1.1.1

Compromise management, accounting, audit, handling, and storage are functions that occur across all steps of the Key Management lifecycle. Compromise management establishes measures to recover from unintended disclosure of keys. These measures shall be automated wherever possible. When there is a compromise, in addition to destroying keys, the Enterprise using the keys and the supplier of them shall be notified so that the key can be revoked.

Accounting and audit are closely related. All of the actions involving a key generate a trail of information that can be monitored by the audit function. Comprehensive audits are performed throughout the key lifecycle (see Enterprise Audit Management). Users are held accountable for unauthorized key-related actions.

Effective Key Management uses a variety of personnel requiring specialized training depending on the functions they perform during the Key Management lifecycle. Individuals need to be trained on proper use of equipment, Key Management processes and procedures, and governance and policies. These personnel shall be required to undergo periodic retraining in accordance with Community policy.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Policy is in place that determines protection requirements for different types of data and assets.
2. Data, System, Communications, and Physical and Environmental protections are in place to provide protection for the Key Management systems and the keying material.
3. Policy exists that determines where keys will be employed.
4. Key Management products are available for all users of end cryptographic units (ECU).

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.



CGS Key Management Capability



Version 1.1.1

1. The Capability ensures effective use of a Key Management infrastructure (both physical and electronic) in which keys are distributed in a manner that enables the systems to effectively use them.
2. The Capability provides the asymmetric and symmetric keys to be used by the requester.
3. Authoritative sources from which to receive a key will be identified.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization uses key devices that support remote Key Management and uses electronic keys, where possible. The Organization will review cryptographic equipment usage and document a formal plan for phasing out legacy equipment that does not support these functionalities, where viable. New devices all support remote management and use electronic keys.

The Organization will register with a key supplier before it can order keys or key material. When ordering keys, the Organization will specify the types of keys required (specification), how many, where they should be delivered, and the key duration. All of these details will be determined by the devices using the keys and their mission.

The Organization's use of cryptographic keys will be dictated by mission need and device capabilities. The Organization will generate and use keys only in accordance with established policy. The duplication or archiving of keys for the purpose of accessing encrypted material past the key's useful life is not recommended. Instead, the Organization will use a method such as duplicating encrypted information and storing that as a secure archive, when achievable.

The Organization will use devices that enable delivery of keys directly from suppliers, where possible. Where this is not possible, keys will remain encrypted such that only the final destination device will be able to decrypt them. Prior to use, all keys will be checked to ensure their integrity, and the authenticity of their source will be verified.



CGS Key Management Capability



Version 1.1.1

The Organization will ensure that all keys are always protected (see Data Protection, System Protection). The Organization will use devices that feature tamper detection and zeroization and will use devices that monitor key expiration dates. When the date approaches, the device will either alert the user or order a new key automatically.

The Organization will use devices that allow lists of revoked keys to be obtained by them from authorized sources. These sources will be determined by the Organization. The Organization will establish policies and procedures governing what steps to take in the event that keys, key material, or key devices are compromised. Established procedures for key destruction, as defined in the Gold Standard definition, depending on the key type will be followed.

The Organization will perform audits of its Key Management system through its implementation of the Enterprise Audit Management Capability. The frequency of these audits will follow guidelines established by the Organization's policies. The Organization will keep an up-to-date inventory of all keying materials and devices. This will be conducted in coordination with the Hardware Device Inventory and Software Inventory Capabilities.

The Organization will ensure all of its users are properly trained in key handling procedures. This can be accomplished either through internal training programs or through agreements with other Organizations that will provide the necessary training for them. This training will include security awareness considerations and key emergency destruction procedures.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.



CGS Key Management Capability



Version 1.1.1

- Digital Policy Management—The Key Management Capability relies on the Digital Policy Management Capability to translate key management policies into machine-readable form.
- Risk Mitigation—The Key Management Capability relies on the Risk Mitigation Capability to determine the strength of the cryptographic mechanism used and the type and size of keys to produce, based on the acceptable risk level. The Key Management Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Key Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Key Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness—The Key Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Key Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Key Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Physical and Environmental Protections—The Key Management Capability relies on the Physical and Environmental Protections Capability to provide physical protection to keys and key material. This includes the protection of the systems and devices used for the management of electronic keys and for legacy physical keys themselves.



CGS Key Management Capability



Version 1.1.1

- Data Protection—The Key Management Capability relies on the Data Protection Capability to provide protection mechanisms for the data assets used for key management.
- Contingency Planning—The Key Management Capability relies on the Contingency Planning Capability to establish mechanisms by which to recover information protected by lost, destroyed, or expired keys.
- Access Management—The Key Management Capability relies on the Access Management Capability to control access to keys and key material.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
SC-12 <i>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</i>	Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system. Enhancement/s: (1) The organization maintains availability of information in the event of the loss of cryptographic keys by users. (2) The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST-approved, NSA-approved] key management technology and processes. (3) The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes. (4) The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material. (5) The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.
SC-17 <i>PUBLIC KEY</i>	Control: The organization issues public key certificates under an



CGS Key Management Capability



Version 1.1.1

INFRASTRUCTURE CERTIFICATES	appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. Enhancement/s: None Specified.
------------------------------------	---

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Key Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 8500.01E Summary: Information Assurance (IA), 23 April 2007, Unclassified	Summary: This directive establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare. It is DoD policy that: ... Interoperability and integration of IA solutions within or supporting DoD shall be achieved through adherence to an architecture that will enable the evolution to network-centric warfare by remaining consistent with the Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance Architecture Framework, and a defense-in-depth approach. This combination produces layers of technical and nontechnical solutions that provide appropriate



CGS Key Management Capability



Version 1.1.1

	<p>levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, including robust Key Management and Incident Detection and Response.</p>
<p>DoDI 8523.01, Communications Security (COMSEC), 22 April 2008, Unclassified</p>	<p>Summary: The ability to maintain the confidentiality, integrity, and availability of DoD classified information and unclassified information that has not been approved for public release during transmission is of paramount importance for an effective DoD security posture. Therefore, it is DoD policy that: Transmission of DoD information shall be protected through the (use of) COMSEC measures and procedures ... COMSEC equipment shall be compatible with DoD-approved key management systems....</p>
<p>NSA/CSS Policy 3-9, Cryptographic Modernization Initiative Requirements for Type 1 Cryptographic Products, 28 March 2003, Classified</p>	<p>Summary: Defines the Cryptographic Modernization Initiative (CMI) requirements that program managers must include for the design of NSA-certified, Type 1 cryptographic solutions to ensure assured security robustness, cryptographic algorithm support, interoperability, releasability, programmability, and End Cryptographic Unit (ECU) management and Key Management Infrastructure (KMI) compatibility.</p>
<p>Information Assurance Security Requirements Directive (IASRD), September 2009, Classified</p>	<p>Summary: This directive is the current replacement for the Unified INFOSEC Criteria (UIC) and the Functional Security Requirements Specifications (FSRS). The Information Assurance Security Requirements Directive (IASRD) lists the requirements and rationale for the development of high-assurance cryptographic products and systems. The IASRD is official guidance for any new program or cryptographic system undergoing NSA certification.</p>
<p>Committee for National Security Systems (CNSS)</p>	
<p>CNSSP 15, National Information Assurance Policy on the Use of Public Standards for the Secure</p>	<p>Summary: This policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS). This policy establishes the use of a secure sharing suite</p>



CGS Key Management Capability



Version 1.1.1

<p>Sharing of Information Among National Security Systems, 29 March 2010, Unclassified</p>	<p>using a standard suite of protocols and cryptographic algorithms. The cryptographic protocols describe how to implement the cryptographic algorithms to achieve interoperability. The use of standardized protocols is the most efficient way to achieve interoperability.</p>
<p>CNSSI 4009, National Information Assurance (IA) Glossary, 26 April 2010, Unclassified</p>	<p>Summary: This instruction resolves the differences between the definitions of terms used by the DoD, Intelligence Community (IC), and civil agencies (National Institute of Standards and Technology [NIST] Glossary) to enable all three to use the same glossary.</p>
<p>Other Federal (OMB, NIST, ...)</p>	
<p>Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, 10 November 2009, Unclassified</p>	<p>Summary: This document outlines a common framework for identity, credential, and access management (ICAM) within the Federal Government and provides supporting implementation guidance for program managers, leadership, and stakeholders planning to execute a segment architecture for ICAM management programs. It includes courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of ICAM. Federal Identity, Credential, and Access Management (FICAM) mentions Key Management as one of three cryptography services.</p>
<p>NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005, Unclassified</p>	<p>Summary: This special publication is intended to help system administrators adequately protect sensitive but unclassified data against serious threats on the Internet. This sensitive data needs to be protected commensurate with the risk and harm that would result from the loss, misuse, or unauthorized access to or modification of this data. The guide provides information on the selection and use of Transport Layer Security (TLS), which provides a mechanism to protect sensitive data during electronic dissemination across the internet.</p>
<p>NIST SP 800-57, Recommendation for Key Management – Part 1: General (Revised), March 2007, Unclassified</p>	<p>Summary: This special publication provides basic Key Management guidance. It is intended to advise developers and system administrators of “best practices” associated with Key Management. Some of the topics this document discusses include security services provided by</p>



CGS Key Management Capability



Version 1.1.1

	cryptographic mechanisms, cryptographic algorithms, and classifications of key types according to their functions, key lifecycle, and management issues.
NIST SP 800-57, Recommendation for Key Management – Part 2: Best Practices for Key Management Organization, March 2007, Unclassified	Summary: This special publication provides guidance on policy and security planning requirements for U.S. government agencies and is intended primarily to address the needs of system owners and managers. This document provides context, principles, and implementation guidelines to assist in implementation and management of institutional Key Management systems.
NIST SP 800-57, Recommendation for Key Management – Part 3: Application-Specific Key Management Guidance, December 2009, Unclassified	Summary: This special publication is intended to help system administrators and system installers adequately secure applications based on product availability and organizational needs and to support Organization decisions about future procurements. The guide also provides information for end users regarding application options left under their control in normal use of the application.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Key Management Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
KMI-3002, Symmetric Key Format Standard DRAFT 0.76, September 2007,	Summary: This standard defines a symmetric key format that will be used for all new symmetric keys delivered by the Key Management Infrastructure (KMI) for National Security



CGS Key Management Capability



Version 1.1.1

Classified	Systems that use Type 1 symmetric keys.
KMI-3006, Key Packaging Standard, January 2005, Classified	Summary: This standard describes the critical concepts that must be understood to correctly plan for and apply key packaging in the KMI. Key packaging adds data to a key such as key name, classification, and other attributes that must be associated with the key so that it can be appropriately delivered to and used by the End Cryptographic Unit (ECU).
KMI-3300, Over-The-Network-Keying (OTNK) Specification, December 2009, Classified	Summary: This specification specifies requirements that ECUs and Information Assurance Components (IACs) must meet to receive KMI products and services via Over-The-Network-Keying (OTNK).
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
FIPS 140-2, Security Requirements for Cryptographic Modules, 3 December 2002, Unclassified	Summary: This document establishes the requirements and standards for cryptography modules that include both hardware and software components.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:



CGS Key Management Capability



Version 1.1.1

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation—This Capability requires the use of highly specialized tools and equipment (hardware and software), which may need to be custom built.
2. Necessary training—The Enterprise must make sure everyone knows how to use key devices if they are going to interact with them.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Key Management Capability.

- The Enterprise shall provide key management services and processes that provide, control, and maintain the cryptographic keys, key material, and certificates required to support a wide range of operational missions. Key management governs the key lifecycle, which includes key registration, ordering, generation, distribution, usage, expiration, revocation, and destruction and includes the functions of compromise management, accounting, handling, audit, and storage.
- Remote management (keying) shall be used by the Organization in a secure manner and shall be as automated as possible with the exception of legacy representation nodes (end-points, intermediary, switches, etc.).
- All keys used to protect classified materials shall be obtained from any source approved by NSA to support interoperability with other Community partners.



CGS Key Management Capability



Version 1.1.1

- CAs, acting as trusted third parties that issue digital certificates and verify the identity of the digital certificate holders, shall perform their operations in coordination with the credential management, identity management, and attribute management systems to fulfill mission needs.
- All new systems and devices that use keys shall use electronic keys that can be transferred by electronic means.
- Legacy systems using physical keys shall be transitioned to new systems that use electronic keys.
- For all systems that use cryptographic keys for protecting classified information, appropriately documented policies, including a KMP, Operational Security Doctrine, and other policies, shall cover the use, support, and interoperability of all cryptographic keys.
- The process of registering a user or non-human entity with the Enterprise shall occur before any Key Management functions can occur.
- During registration, each account shall be mapped to a controlling party within the supplier's (of certificates or keys) hierarchy.
- Keys and certificates shall be ordered only from a supplier with whom the requester is registered.
- The key request (order) shall specify the types, quantity, delivery location, and expiration date of the keys and certificates that are being ordered.
- All cryptographic keys used to protect classified information shall be generated in accordance with NSA policies and use NSA-approved devices or Community-established standards.
- Keys that are generated on an ad hoc basis (e.g., SSL/TLS keys) shall follow the relevant commercial standard, and also meet NSA implementation requirements.
- All symmetric keys and asymmetric private keys shall be delivered in encrypted form when possible and protected at the same level as or higher level than the data they will be used to protect.
- Key material or keys shall be delivered directly from the supplier without human intervention (when possible) to the device that will use it, when possible.
- Automated source authentication and integrity checking shall occur before any keys, including asymmetric public keys, are used, when possible. For systems where these automated checks are not possible, the process for authentication and integrity checking will be provided by policy.
- A manager shall oversee and verify the transfers of all keys and key material.
- NSA-approved dedicated cryptographic hardware (e.g., a hardware security module) shall be used for the protection of keys and key material. Systems and



CGS Key Management Capability



Version 1.1.1

devices that use keys are designed to use activation data so that a user can supply the appropriate data and activate the key without ever having direct access to the key.

- Devices that store keys shall monitor the expiration dates of their keys and provide user notification when the expiration date is near, or the device will automatically request a new key from its appropriate supplier.
- Keys shall not be used past their expiration date.
- Procedures shall be in place to destroy a key at any point in the lifecycle should there be a security compromise.
- All equipment using cryptographic keys shall incorporate anti-tamper mechanisms to detect when it has been compromised and automatically zeroize any keys it is storing.
- There must be alternate means with which to destroy the applicable keys when automated key destruction means are not available.
- Keys shall be able to be destroyed to preserve confidentiality for keys used outside a secure environment.
- For archival purposes, appropriate contingencies must be established to obtain sensitive data while maintaining confidentiality requirements (see Contingency Planning). Methods include establishing a protected data archive and instituting a method for key recovery.
- When possible and depending on mission needs, keys shall be automatically disabled when they reach their expiration date.
- The source that is requesting the revocation of a key shall be authenticated to ensure that the source requesting the revocation is authorized to do so.
- When a key is revoked, prior to the expiration date, all relevant parties who may interact with that key shall be notified as soon as possible by the appropriate authoritative source.
- When a public key certificate needs to be revoked, the CA who signed it shall issue a digitally signed notification of the revocation, typically a CRL.
- Public-key enabled software shall check the validity of a certificate before using it, referring to the most recent revocation notification available. For revocation of other types of keys or key material, the office that authorized use of the key or key material will issue a notification (e.g., a supersession message).
- Compromise management shall establish automated measures (wherever possible) to recover from unintended disclosure of keys.
- When there is a compromise, in addition to destroying keys, the Enterprise using the keys and the supplier of them must be notified so that the key can be revoked.



CGS Key Management Capability



Version 1.1.1

- Comprehensive audits shall be performed throughout the key lifecycle of all of the actions involving keys.
- Personnel shall be trained and periodically retrained on proper use of Key Management processes and procedures, equipment, governance, and policies, in accordance with Community policy.