DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY

ENTERPRISE SYSTEMS ENGINEERING

KEY MANAGEMENT SYSTEM BASELINE REQUIREMENTS

HEALTH SYSTEMS ENGINEERING & DESIGN (HSED)

V.1.6

Thomas H Sasse August 18, 2017

REVISION HISTORY

Date	Reason for Changes	Version	Author
07/14/17	Working Draft	1.0	Thomas Sasse
07/18/17	Working Draft	1.1	Thomas Sasse
07/24/17	Working Draft	1.2	Thomas Sasse
07/26/17	HSE&D Peer Review	1.3	Michael Cochran
07/27/17	Working Draft/Additions Per HSE&D Peer Review	1.3	Thomas Sasse
07/27/17	HSE&D Peer Review	1.4	Complete
08/08/17	KMIP additions	1.5	Thomas Sasse
08/18/17	Edits and Additions	1.6	RFI Review Team

Table of Contents

Security Requirements

The requirement to encrypt Data-AT-Rest to “render unsecured protected Health Information unusable, unreadable, or undecipherable to unauthorized individuals,” is per NIST Special Publication 800-111 and HIPAA. The HIPAA Security rule requires “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” to avoid breach of confidential information. This protection prevents attackers from gaining access to unprivileged information by bypassing normal access control mechanisms. The NIST Guidelines cover and define Full Disk Encryption (FDE), Virtual Disk Encryption and Volume Encryption as well as File/Folder Encryption.

NIST Controls and enhancements

NIST Control			
System and Communications Protection	SC-28	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including; for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related to: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7	Applies to Moderate and HIGH
Control Enhancements			
System and Communications Protection	SC-28 (1)	Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for	Applies to Moderate and HIGH

		media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related to: AC-19, SC-12	
System and Communications Protection	SC-28	Removing organizational information from online information system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.	Applies to Moderate and HIGH

Overview of Key Management Systems

The minimum functionality of a KMS is to logically maintain a key's set of attributes, such as operations that can be performed by the key, validity period of the key and associations of the key with other entities.

Keys within a system are in general used for different purposes. In order to ensure a key is only used for the purpose for which it was intended, it has bound with it a set of attributes defining how it may be used.

The term key in this document conveys a more comprehensive meaning than the popular use of the term which simply refers to its cryptographic binary value. To avoid confusion here the term Key Value is used to describe the cryptographic binary value, and the term Key Profile is used to describe an object which contains the Key Value and a set of attributes. Depending on the key's purpose, the attributes contained within a Key Profile will vary.

1. What is a KMS

A Key Management System is a system to securely generate, store, distribute and delete cryptographic Key Values and attributes. A KMS is part of a larger system that requires cryptographic Key Values. A Key Management System is typically a software based system making use of hardware based cryptographic processor for secure operations, and consists of several baseline elements:

- A database for storage of the Key Values and attributes
- Services to the systems needing Key Values – typically in the form of an API
- An HSM (Hardware Security Module, (***The Physical Appliance***)) to ensure the physical security and integrity of the Key Values and attributes, and also provide a resource for the mathematically intensive nature of Key Value generation.
- Procedures – or more accurate man/machine interface supporting procedures

Except for the requirements for security and procedural support, a Key Management System is much like any other management system e.g. a LINUX Satellite Server. At the heart of the system lies a Database storing the Data and an API giving access to that Data and the services associated with it.

General Key Management System Requirements

In order to protect an asset and manage Key Values in a robust way there are certain principles that must be applied to the design of a key management system. There are certain requirements for key management that are general enough to be listed as requirements for all KMSs. The requirements stated in this document lay down a baseline for interoperability (*KMIP*) and mutual trust between business entities that need to share and/or use cryptographic information. *KMIP (Key Management Interoperability Protocol)*

2. Overall requirements for a KMS

[R-1] The KMS shall be able to maintain Key Profiles during the entire lifetime for a specific Key Profile i.e. from definition, generation and storing, exchanging and using to expiration.

[R-2] The KMS shall provide services to relevant systems having the need for use of a specific Key Profile. These services will provide a mechanism for users of the KMS to generate exchange and retrieve keys along with user profiles to define level of access.

[R-3] The KMS shall have any secret or critical function (such as generating or unwrapping/wrapping Key Values) performed within a Hardware Security Module or equivalent secure component.

[R-4] The KMS shall be able to recover all Key Profiles within the KMS in case of failure in the KMS itself or in the H SM utilized.

2.1 Requirements for KMS/HSM

The KMS relies on an HSM to supply certain capabilities the following section.

[R-5] The actual implementation of such a support is not mandated, but the minimum requirements for an HSM shall encompass support for:

[R-5a] Key Value generation

[R-5b] Key Value exchange

[R-5c] Key Profile separation (logically split key attributes)

[R-5d] Key Value export and import

[R-5e] Secure storage of Key Value

[R-5f] RNG testing shall be performed periodically to verify that is continues to operate correctly according to FIPS 140-2, any errors shall be reported to the KMS.

[R-6a] Services offered by the HSM, in addition to the requirements stated in this document shall not enable the HSM requirements of the KMS to be circumvented, for example the KMS requires Key Profile separation, and the HSM must not offer additional or legacy services to enable the key separation to be overridden.

[R-6b] The HSM shall be certified on a level corresponding to at least FIPS 140-2.

2.2 Requirement for Access and Audit

[R-7] The KMS shall be able to limit access to each Key Value and the functions possible for a Key Value to those with a defined need.

[R-8] No person must have access to a clear text value of any Key Value within the KMS.

[R-9] The KMS shall be able to manage and track any changes to the Key Profiles.

[R-10] The changes shall be tracked in a way that the information concerning the changes can be trusted.

[R-11a] The changes may be tracked in a way that they can be compared with information of the intended use of the Key Values and functions within the Key Management System.

[R-11b] Periodically an audit shall be done to review the changes tracked in order to verify that all of them are correct. The system shall provide an audit process.

2.3 Requirements for Supporting Cryptographic Algorithms and their Modes

[R-12] The KMS shall be capable of supporting Key Values for the following algorithms:

[R12a] TDEA – Triple Digital Encryption Algorithm ECB & CBC as described in FIPS PUB 81.

[R-12b] RSA – Rivest Shamir Adleman

While it is envisaged that various symmetric and asymmetric cryptographic algorithms could be supported, this document only outlines the requirements for the last two mentioned examples.

2.4 Requirements for Key Profile

[R-13] The KMS shall support a standard structure representing the attributes of a Key Value. The structure will be known as a Key Profile and act as a prototype for a Key Value.

The attributes making up a Key Profile can be grouped into three sections. The first contains those attributes used to identify a Key Profile (Owner, Source/Sender, Destination/Receiver, Name, etc.). The second is made up of those attributes that define the "context, environment, usage, type, etc." of a Key Profile. The final section contains those attributes that make up a version of a key (value, expiration/activation dates, version identification, integrity checks, etc.).

[R-14] A Profile is a unique set of attributes and shall be uniquely identified. Many Key Profiles can be based on a single source Profile if they share the same "context, environment, usage, type, etc." (i.e. multiple versions of a Key Value would share the same Profile).

[R-15] The presence of individual attributes or parts of a Key Profile shall be classified as mandatory or optional.

[R-16] A Key Value shall not be used for cryptographic purposes unless all mandatory attributes are present in a Key Profile.

A Key Value may be associated with more than one Key Profile although this requirement is not expected to be needed within the same KMS system. An example of this is the Transport Key used by the Issuer may have the usage of Wrap and Encrypt, and for the Enabler the same Key Value is to be loaded into a different Key Profile which may have a usage of Unwrap and Decrypt. These two different methods therefore use different KMSs with the correct Key Profile loaded into each. If the Issuer and Enabler were being carried out by the same actor they would probably not use a Transport Key.

2.5 Requirements for Key Generation

[R-18] The KMS shall be able to generate Key Values compliant to the cryptographic algorithms supported by the KMS.

[R-19] The generated Key Values shall be cryptographically sound according to the nature of the algorithm. This requirement encompasses the algorithms defined in this document:

2.6.1 [R-20] TDEA:

[R-20a] Shall be 128/256 bit key, comprising of 112 bit Key Value plus odd parity

[R-20b] Weak or semi-weak Key Values shall not be allowed

[R-20c] Shall be generated using either a True Random Number Generator or a Pseudo Random Number Generator. The Random Number Generator that is used shall be designed to pass the statistical tests specified in FIPS 140-2

2.5.2 [R-21] RSA:

The General KMS requirement here is to support generation of RSA-keys, however actual specific requirements to the RSA key generation can and probably will be obtained from the requirements for the Application KMSs.

[R-21a] The KMS should be able to generate and manage RSA keys with a Public Key modulus lengths greater than or equal to 512 bits

[R-2 1b] The RSA key shall be generated to meet the requirements specified in the Key Profile defined for each application

2.6 Requirements for Key Revocation

[R-22] Where revocation services are employed the following requirements shall be maintained:

[R-22a] Maintaining a list of revoked key values and all associated profiles

[R-22b] Report list of revoked key values & profiles

[R-22c] Distribution of revocation lists or other mechanisms to verify current or recent validity of keys

2.7 Requirements for Storing Keys

[R-23] All Key Values, based on their longevity, shall be stored in a way that they are protected from exposure and unauthorized modification; the associated key profiles shall also be protected from unauthorized modification. A procedural policy is required to define what is modifiable with what level of authorization.

[R-24] Along with the actual Key Value other information shall be stored. This information represents necessary properties of the Key Value. Other than the properties than can be found in the corresponding Key Profile, a Key Value has properties that are directly related to the actual value. The information stored shall include at least:

[R-24a] Unique ID of the specific Key Value.

[R-24b] The intended usage of the Key Value.

[R-24c] The ID of the Key Profile.

[R-24d] Information on how the Key Value is encrypted, i.e. an identification of the Key Profile encrypting the Key Value.

[R-24e] Expiration date.

[R-24f] Indicator for whether a Key Value is for test or live-environment.

[R-24g] Key Check Value, which makes it possible to exchange information about a given Key Value without exposure of the actual Key Value.

2.8 Requirements for Key Exchanging

2.8.1 General Principle for Exchanging Keys

[R-25] The KMS shall be able to exchange both the Profile of the key and the Key Value itself.

[R-26] It may be possible to exchange a number of Transport Keys (TK) between physically separated Key Management Systems, which have the need to exchange Key Profiles.

[R-27] At least the first Key Profile exchanged between two such systems shall be done in a manner that shall provide mutual authentication1 between the two entities.

[R-28] The key exchange may be done in manner that provides secrecy of the Key Value.

Transport Keys can be exchanged using various methods VPN or LAN-connections.

2.8.2 Exchanging Key Profiles

[R-29] The KMS shall support the following to enable Exchanging Key Profiles:

[R-29a] The KMS shall be able to store, organize and retrieve the information relating to the Profile used for a specific Key Value.

1 Mutual Authentication in this context can be achieved procedurally or cryptographically. The intention of this requirement is to ensure the key value & attributes are shared with the correct party and not an impostor.

[R-29b] The exchange of Key Values between KMSs shall utilize Key Profiles.

[R-29c] The KMS shall support a method to ensure the integrity of a Key Profile. This integrity must be maintained during profile storage or exchange, even if the exchange is performed in multiple transmissions.

2.8.3 Exchanging TDEA keys

[R-30] The KMS shall be able to support a secure exchange of TDEA Keys with another KMS.

[R-31] A Key shall be exchanged as components or in encrypted format as mutually agreed upon between sender and receiver. If exchanged as components, the Key Value shall be exchanged as a number of components, bigger than one, with each component written to a separate medium and each should be sent independently.

[R-32] In case a Key Profile is imported into the KMS, the KMS shall be able to check for odd parity of the Key Value. When the Key Value does not have odd parity the KMS shall not accept the Key Profile.

[R-33] In both cases, certain information other than the actual Key Value shall be transferred along with the Key Value. This information shall encompass at least:

[R-33a] ID of the specific Key Profile uniquely identifying the Key Profile to both sender and receiver;

[R-3 3b] Indicator for whether the Key Value is a test or a live key;

[R-33c] Key Check value making it possible to verify that Key Value after installation has the same value at both sender and receiver;

[R-33c1] If exchanged in the clear each component shall have a Key Check Value attached;

[R-33c2] For both clear and encrypted Key Values the final (combined) Key Value shall have a Key Check Value attached;

[R-33d] For Encrypted Key Values only, a unique identification of the Transport Key (TK) used to encrypt the exchanged Key Value. The ID shall be unique to both sender and receiver, and based on Name/Owner/Version or OID.

2.8.4 Exchanging RSA keys

[R-34] RSA Key Profiles shall be exchanged in the following manner:

[R-34a] Public Key Values shall be exchanged using a method providing authenticity and integrity.

[R-34b] Private Key Values shall be exchanged using a method providing authenticity, integrity and secrecy.

[R-35] For both Public and Private Key Profiles certain information other than the key itself will be transferred along the Key Value. This shall at least encompass:

[R-35a] ID of the specific Key Profile uniquely identifying the key to both sender and receiver;

[R-35b] Indicator for whether the Key Value is a test or a live key;

[R-35c] Integrity check such as a Key Check Value making it possible to verify that Key Value after installation has the same value at both sender and receiver;

[R-35d] For Private Key Values, a unique identification of the Transport Key (TK) used to encrypt the Private Key Value during transport.

2.9 Requirements for Importing and Exporting Keys

[R-36] The KMS shall support and use mechanisms to prevent Key Value import/export unless explicitly authorized.

2.10 Requirements for Key Separation

[R-37] The KMS shall support and use methods to make it impossible to use a Key Value for another usage or purpose other than the intended usage as indicated by the associated Key Profile.

2.11 Requirements for the Date Checking

[R-38] The KMS shall prohibit the usage of Key Values outside the Key Profile's valid date range.

2.12 Requirements for Expiration and Deletion

[R-39] The KMS shall support and use processes to have a Key Profile expired and archived.

2.13 Requirements for HA (High Availability) and DR (Disaster Recovery)

[R-40] The KMS shall support Multi-Site, Client failover Clustered

[R-41] The KMS shall support Replication between Multi-Site instances Clustered

[R-42] The KMS shall support Mirror Disk, Dual power and Dual NICs

[R-43] The KMS shall run on VA Server Class standard hardware

[R-44] The KMS shall have processes to recover from backup (DR)

2.14 Requirements for Contingency Applications

[R-45] The KMS shall have processes to allow for key transfers to contingency systems located outside of a data center during a WAN outage.

2.15 Requirements for KMS Administration

[R-46] The KMS shall have a user interface to manage the key profiles generated by the systems being managed.

[R-47] Centrally manage keys, Oracle Wallets, Java Keystores, and credential files.

[R-48] Securely share keys across authorized endpoints in an enterprise

[R-49] Manage key lifecycle stages including creation, rotation, and expiration

[R-50] Be optimized for Transparent Data Encryption (TDE) master keys

[R-51] Easily enroll and provisions endpoints

[R-52] Automate endpoint enrollment using protected RESTful interfaces

[R-53] Support primary and standby for availability and disaster recovery

[R-54] Schedule automatic backup to a remote location

[R-55] Support prior database versions without requiring database patching

[R-56] Support Linux, Windows, Solaris, AIX, and HP-UX(IA) endpoint platform

[R-57] Support Hardware Security Module (HSM) Integration

[R-58] Support the OASIS KMIP standard

2.16 Requirements for Third Party Encryption Technology

[R-47] The KMS shall have processes in place to accept third party the key profiles and manage them. e.g. Microsoft PCKS#11(MS SQL), Oracle KMIP and Intersystems KMIP.