The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **SPECIAL PUBLICATION 800-152**

Title: **A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)**

Publication Date: **10/30/2015**

- Final Publication: *Link to publication DOI -or-*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf
  DOI URL: http://dx.doi.org/10.6028/NIST.SP.800-152
  (the DOI URL is actually the same link as to the 1st one (nvlpubs.nist.gov))
- Related Information on CSRC NISTIR page:
  http://csrc.nist.gov/publications/PubsSPs.html#800-152
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

Requirements and Desirable Features of U.S. Federal Cryptographic Key Management Systems

NIST is developing a NIST Special Publication 800-152 entitled "A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)" for use by Federal agencies and contractors when designing, implementing, procuring, installing, configuring, and operating a CKMS. This Profile will be based on the NIST Special Publication 800-130 entitled "A Framework for Designing Cryptographic Key Management Systems." The Framework covers topics that should be considered by a product or system designer when designing a CKMS and specifies requirements for the design and its documentation. The Profile, however, will cover not only a CKMS design, but also its procurement, installation, management, and operation throughout its lifetime. Requirements will, therefore, be placed not only on a CKMS product or system, but also on people (procurement officials, installers, managers, and operators) while performing specific tasks involving the CKMS.

A draft Framework was published by NIST for comment in June 2010 and again in April 2012. The attached table of proposed Profile requirements was drafted for public comment and for discussion by participants of the CKM Workshop scheduled for September 10-11. Details of the workshop are available at http://www.nist.gov/itl/csd/ct/ckm_workshop_2012.cfm.

An initial attempt at defining Profile requirements is presented below in tabular form. Public-comment reviewers and workshop participants are invited to comment on these tables and are requested to provide answers to the following questions:

1) What topics are fundamental to the design and operation of a CKMS?
2) Are the topics, requirements, and desirable features proposed in the table appropriate?
3) What requirements should be satisfied in every Federal CKMS system?
4) What are cost-effective security augmentations to a Federal CKMS?
5) What attributes need default values for establishing interoperability among CKMS?
6) What attributes should be considered "nice-to-have" in the future?
7) What requirements for interoperability among CKMS, communications, secure computer applications, and user-CKMS interfaces are desirable and cost effective?

The Profile Table for a U.S> Federal Government CKMS

Profile CKMS topics, requirements and features are presented in the following table, and should be used as follows:

1) Obtain a copy of the Framework to review a topic and its CKMS design requirement(s). The section numbers in column 1 correspond with those of the CKMS Framework.

2) The section topics in column 2 are taken from the Framework and discussed there. The Framework requirements (denoted as FR:x.y, where x is the section, and y is a section topic requirement) relate to that topic as discussed in the Framework.

3) Column 3 contains the base requirements for implementation in all Federal CKMS. Interoperability requirements are shown in parentheses.

4) The augmented requirements in column 4 are those required for implementation in Federal CKMS having higher security needs. Those specific to an Agency may appear in the procurement documents of an agency or Federal contractor. Interoperability requirements are shown in parentheses.

5) The future features in column 5 are desirable features or "nice-to-haves"; for example, for those CKMS where such features are required and affordable.

6) The Requirements Table will be modified, based on public comments and workshop discussions. These requirements will then be integrated into the Profile and issued for public comment.

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 1, FR:1.1	**Framework and Profile Requirements**	**Base Requirements for CKMS Design and Implementation**	**Augmented Requirements for CKMS Design and Implementation**	**Features to consider for Future CKMS implementations**
Section 2.1, FR:2.1	**Cryptographic algorithms and key sizes**	**NIST-approved algorithms and key sizes per SP 800-131A**		**Multi-algorithm capability**
Section 2.1, FR:2.2	**Security strength of algorithms**	**112 bits of security minimum (112)**	**128 bits of security minimum (128)**	**Scalable security strength capability**
Not covered in the Framework	**Key and metadata sensitivity**	**Low, Moderate or High (Low)**	**Moderate or High (Moderate)**	**Multi-Level Security: Low, Moderate, and High**
Section 3.1	**Key Mgmt. for Networks, Applications, and Users**	**CKM for low, moderate or high confidentiality and integrity for selected applications (Low)**	**CKM for moderate or high confidentiality and integrity for selected applications (Moderate)**	**Multi-domain CKM supported, multi-level policy negotiation, enforce policy negotiated for application**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 3.2 **FR:3.4**	**Conformance to Standards**	**Conform to applicable NIST security Standards and Recommendations.**		**All CKMS services use applicable Federal, National, and International security and interoperability standards**
Section 3.3 **FR:3.10**	**Ease of Use**	**Simple user interfaces; easily managed, monitored ,and audited security services and functions; prevention or detection of user errors; easy recovery from a security breach**		**User-CKMS and CKMS-CKMS Interfaces use the same commands and parameters for the same services throughout all security domains**
Section 4 **FR:4.4** **FR:4.5**	**Security Policies: Required security policies**	**CKMS Security Policy and Cryptographic Module Security Policy**	**Base + Information Security Policy, Domain Security Policy**	**Supports Multiple Domain Security Policies; a CKMS can negotiate a new security policy for an application, based on policies from more than one security domain**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 4.6, FR:4.6	**Accountability**	**Required for all roles except the user role**	**Required for all roles**	**Personal Accountability for all activities within the CKMS while preserving anonymity and personal privacy**
		Identify entities (e.g., devices, users), verify entity authorization, detect unauthorized access, report requests for unauthorized access, and restrict CKMS use to authorized entities performing authorized activities		
Section 4.7 **FR:4.7**	**Anonymity, Unlinkability and Unobservability**	**Optional**	**CKMS assures that keys cannot be linked to an authorized entity when viewed from outside CKMS**	**Provided for entities using keys and metadata in accordance with a Domain Security Policy**
Section 4.8, FR:4.14	**Laws, Rules and Regulations: Intended use**	**US Federal Agency and Contractor facilities in US**	**Base + US Federal Facilities in Canada, Western Europe, Australia, and New Zealand.**	**Global US Federal Facilities**
Section 4.9	**Security Domains**	**Support the CKMS Security Policy that is based on one security domain policy**		**Support the CKMS security policy and multiple domain policies**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 4.9.3 **FR:4.18**	**Obtaining Assurances**	**Manual evaluation of security policies**		**Automated assistance of security policy evaluation**
Section 4.9.7 **FR:4.21**	**Multi-Level Security Domains**	**Optional**		**Supports multi-level security domains**
Section 4.9.8, FR:4.24	**Upgrading and downgrading**	**Optional**	**Only with security administrator approval**	**Automated support of administrative negotiation of a security level**
Section 5, FR:5.1	**Roles and Responsibilities: Required roles**	**System Administrator, Cryptographic Officer, Key Owner, Audit Administrator, Key Custodian, System User**		**System Authority, Domain Authority, Registration Agent, Key Recovery Agent, CKMS Operator**
Section 5.1 **FR:5.2**	**Roles and Responsibilities: Role separation**	**Audit Administrator can assume no additional role other than a System User**		
Section 6.1, FR:6.1	**Key Types**	**At least one key type for performing a cryptographic function on data**	**At least two key types: one operates on data while the other operates on keys and/or metadata**	**All Key types needed to support multiple security domains as per policies**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.2.1, FR:6.2	**Metadata Elements: Selection and how associated with the key**	**Support of elements as specified in design** **(Application-dependent)** **Cryptographic or trusted-process association with the key**	**Key label, key identifier, key owner identifier, crypto.alg. using the key, schemes or modes of operation, parameters, key type, applications for the key, parent key, key sensitivity, access control list, date-times/usage count, and revocation reason.** **(All Application-dependent)** **Cryptographic association with the key**	**Security domain ID for each element supported**
Section 6.2.1	**Metadata Elements: Secret and private key protections**	**Confidentiality and integrity protection; integrity verified when received**	**Base+ source authentication**	**Integrity is verified before loading into crypto module prior to use**
Section 6.2.1	**Metadata Elements: Public key protection**	**Integrity verified when received**		**Integrity is verified before loading into crypto module prior to use**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.2.1,	**Metadata Elements: Metadata protection**	**Confidentiality protection if sensitive; integrity verified when received**	**Base+ source authentication**	**Integrity is verified before loading into crypto module prior to use**
Section 6.2.1, FR:6.10	**Metadata Elements: Time source**	**NIST time source; verified daily**	**NIST time source; verified hourly**	**NIST time source; verified as per domain policy**
Section 6.2.1, FR:6.12	**Metadata Elements: Time stamp**	**Capability for using an approved time-stamping authority; use for activate key, deactivate key revoke key, destroy a key, and recover a key.**	**Base+ generate or establish a key, derive or update a key, destroy metadata, backup and archive a key and its metadata, recover a key's metadata, manually enter and output a plaintext key or key split from a crypto-module, validate domain parameters and public key, validate a key pair, and validate the possession of a private key**	**Capability for providing a Time Stamp for: Suspend and reactivate a key, renew a public key, associate a key with its metadata, modify metadata, delete metadata, list metadata, store operational key and its metadata, validate certification path, validate a symmetric key, perform a function using a key, and manage the trust anchor store**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.2.2, FR:6.13	**Required Key and Metadata Information: Random number generation**	**Any NIST-approved RNG per SP 800-131A**	**SP 800-90 RBG**	
Section 6.2.2 FR:6.13	**Required Key and Metadata Information: Disclosure and modification protections**	**Cryptographic when outside a cryptomodule**		
Section 6.2.2 FR:6.13	**Required Key and Metadata Information: Assurances**	**Obtain key and domain parameter assurances using approved methods**		
Section 6.3, FR:6.15	**Key Lifecycle States and Transitions: Required states**	**Active, revoked and compromised**	**Base+ destroyed**	**Pre-activated, deactivated, suspended, reactivated after suspension**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.4, FR:6.17	**Key and Metadata Management Functions**	**Generate key, deactivate key, register owner, revoke key, associate a key with its metadata, list key metadata, destroy key and metadata, establish a key, validate keys and domain parameters (as appropriate), recover key and metadata, and perform a cryptographic function using a key**	**Base+ backup key and metadata,**	**Activate key, renew a key, modify metadata, archive key and metadata, suspend and re-activate a key, establish key and metadata for a negotiated new security domain**
Section 6.4.1 **FR:6.19**	**Generate Key**	**Use NIST-approved methods**		
Section 6.4.5	**Revoke Key**	**Required, with reason for revocation**		
Section 6.4.9	**Destroy a key**	**Use approved methods**		

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.5	Crypto. Key and/or Metadata Security: Key and metadata storage outside a cryptomodule	Store secret and private keys and sensitive metadata outside a crypto module encrypted and with an integrity code; verify integrity after retrieval from storage	Base + authenticate and verify authorization of entity retrieving keys and metadata from storage	
Section 6.6FR:6.79 FR:6.82	Crypto. Key and/or Metadata Security: During key establishment	Any NIST-approved scheme (SP 800-56A key agreement: C(2,0) EC (curve P-256); SP 800-56B key transport: KTS-OAEP)	Any NIST – approved scheme (SP 800-56A key agreement: C(1, 2, ECC CDH) with curve P-256 SP 800-56B key transport: KTS-KEM-KWS	SP 800-56A key agreement: C(2,2) DH and MQV; SP 800-56B key agreement: KAS2
Section 6.6.3, FR:6.84	Key Confirmation	Optional	Required	
Section 6.6.4, FR:6.86 Also Section 7, FR:7.2	Key Establishment Protocols	Any NIST-approved or allowed protocol (common protocol required for interoperability)		Automated domain policy negotiation protocol (to be developed)
Section 6.7.1, FR:6.89	Restricting Access to Key and Metadata Management Functions	Single-factor authentication on security-relevant functions	Multi-factor authentication on security-relevant functions	Personal authentication and function authorization

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.7.2, FR:6.94	**Restricting Cryptographic Module Entry and Output of Plaintext Keys**	**Encryption or key splitting optional for secret and private keys - i.e., plaintext entry and output allowed.**	**Encryption or key splitting required for secret and private keys.**	
Section 6.7.4, FR:6.97	**Multi-party Control**	**Optional**	**Multi-party control on CA and/or KDC keys**	**Domain administrators for multi-domain services**
Section 6.7.5, FR:6.99	**Key Splitting**	**Optional**		
Section 6.8.1, (no specific FR) and Section 6.8.3, FR:6.107	**Key Compromise: Recovery**	**Change compromised key to the compromised state; key revocation and rekey of all keys affected by a compromise; audit logging of the revocation and rekey processes;**		
Section 6.8.2, FR:6.106 and Section 6.8.3, FR:6.107	**Metadata Compromise: Replacement of sensitive metadata**	**Metadata revocation and replace both key and metadata**	**Base + audit of compromise;**	
Section 6.8.4, FR:6.108	**Cryptographic Module Compromise: Recovery**	**FIPS 140-2 Level 2 tamper evidence**	**FIPS 140-2 Level 3 tamper evidence and protection**	**FIPS 140-2, Level 4 tamper evidence and protection**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 6.8.5, FR:6.113	**Computer System Compromise Recovery**	**Detect, report and analyze the problem; install system upgrades and perform system tests**	**Base + take compromised part of CKMS offline to repair and test**	**Automated detection and reporting of errors and return to known secure state**
Section 6.8.6, FR6:115 b)	**Network Security Controls and Compromise Recovery**	**Block unauthorized protocols ; install security patches and upgrades**	**Base + firewalls on networked computers**	**SCAP security status checking and perform recommended remediation**
Section 6.8.7, FR:6.117	**Personnel Security Compromise Recovery**	**Enforce personal accountability; minimize consequences of any role compromise; provide role separation and role backup**	**Base + annual audit of personnel security logs and whenever personnel security compromise is suspected; annual review of potential compromise consequences**	**Automated annual security training of all personnel with signed policy acceptance by each person**
Section 6.8.8, FR:6.118	**Physical Security Compromise Recovery**	**Controlled physical access to CKMS devices; Recovery procedures**	**Base + two-factor physical access control.**	

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 7, FR:7.1	**Interoperability and Transitioning**	**As required for supported applications; use an interoperable default; make and use transition plans, as needed**		**Protocols for establishing equivalence of security domains; key management interoperability for multi-domain transactions**
Section 7, FR:7.2	**Interoperability and Transitioning: Symmetric encryption using block ciphers**	**Any NIST-approved symmetric algorithms per SP 800-131A (AES-128)**		
	Block cipher modes	**SP 800-38 (Encryption only: CBC; Message authentication only: CMAC; Authenticated encryption: CCM; Key wrapping: CCM)**		
	Hash algorithm	**Any FIPS-approved hash function per SP 800-131A (SHA-256)**		
	Hash-based message authentication	**FIPS 198 (HMAC-SHA-1)**		
	Key Agreement	**SP 800-56A (C(2e,0s) EC with curve P-256; concatenation KDF with SHA-256)**	**SP 800-56A (C(1e, 2s, ECC CDH) with curve P-256; concatenation KDF with SHA-256)**	

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 7 (contd.) **FR:7.2**	**Key Transport**	**SP 800-56B** **(KTS-OAEP; concatenation KDF with SHA-256)**	**SP 800-56B** **(KTS-KEM-KWS; concatenation KDF with SHA-256)**	
	Key Derivation (from a pre-shared key)	**SP 800-108** **(HMAC in counter mode with SHA-1)**		
	Digital Signature	**Any NIST-approved digital signature algorithm per SP 800-131A** **(ECDSA with curve P-256)**		**ECDSA with curve P-364**
Section 8	**Security Controls**	**Enforce CKMS Policy Sanctions**	**Base + multi-person control of critical system functions**	**Enforce Domain Policy Sanctions**
Section 8.1	**Physical Security Controls**	**Physical protection; access control for CKMS devices, keys and metadata.**	**Base + access control to CKMS facilities.**	
Section 8.1 **FR:8.2**	**Physical Security Controls: Protection of crypto. devices and components**	**FIPS 140-2, Level 2 physical protections in crypto modules.**	**FIPS 140-2, Level 3 physical protections in crypto modules.**	**FIPS 140-2, Level 4 physical protection in cryptomodules**
		Physical protection of computer systems and communication end-points.		

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 8.2.1, FR:8.3 and FR:8.5	**Operating System Security**	**Specification of requirements for secure operation. The following hardening features of FR:8.5: a) removal of all non-essential software programs & utilities; d) limiting user accounts to only those needed for essential operations; f) replacing default passwords and keys; g-i) disabling non-required services and data ports**	**Base + use of operating systems that provide protections to sensitive keys and metadata while resident in the computer for all multi-user components. All hardening principles of FR 8.5 are required unless specifically exempted by the CKMS owner.**	**Automated negotiation of Trusted System features to be used for a transaction**
Section 8.2.2, FR:8.6	**Individual CKMS Device Security**	**Implement and support the security controls as specified by each device's design**	**Provide security features a) to f) in Section 8.2.2 unless specifically exempted by the system-owning authority.**	**Configurable by system administration with approval of the system authority; dynamically configurable, based on domain security policy(ies)**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 8.2.3, FR:8.8	**Malware Protection**	**Implement and support time and event-driven malware scanning[1]. Update software when available.**	**Base + rootkit detection software. Software integrity verified upon installation and periodically.**	**Configurable malware monitoring**
Section 8.2.4, FR:8.10	**Auditing and Remote Monitoring**	**Auditing of specified security-related events. Report events to audit administrator. Audit capability and audit log protected from unauthorized modification.**	**Base + SCAP compatible**	
Section 8.3, FR:8.15	**Network Security Control Mechanisms**	**Section 8.3 items a) through f), as selected**	**All items in Section 8.3 items a) through f) required, unless exempted by owning authority Mechanisms in physically secure locations. Configured by authorized entities.**	

[1] Daily scan for Virus, Spyware, and other Malware. Scan of portable data storage media before it is opened for CKMS access. Scan of software modules and data files for Malware before they become accessible. Weekly checks for new updates of the Malware protection software. Weekly update and use of the known-Malware databases and system repair updates.

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 8.4, FR:8.19	**Cryptographic Module Controls**	**FIPS 140-2 Level 2 or above**	**FIPS 140-2 Level 3 or above**	**FIPS 140-2 Level 4**
Not covered in the Framework	**Control Selection Process**	**Compliance with FIPS 199, FIPS 200, and SP 800-53**		**Configurable by system administrator with approval of the system authority; dynamically configurable, based on domain security policy(ies)**
Section 9, FR:9.1, FR:9.2, FR:9.3, FR:9.4, FR:9.5, FR:9.6, and FR:9.7.	**Testing and System Assurances: By vendor, third-party, and system, procurement authority for scalability, functionality, security, and interoperability**	**Vendor and third-party testing; procurement acceptance testing; functional, and security testing; interoperability testing; self testing during operation. All must provide acceptable test results**		**Functional and operational testing of multi-domain policy negotiation and enforcement**
Not covered in Framework	**Ease-of-Use Testing**	**Demonstrate operation and use of CKMS for all users; demonstrate correct operation and failures of system with responses**	**Base + built-in demo of system operation**	**Third-party evaluation of usability prior to procurement.**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 9.7 **FR:9.8**	**Limitations of Testing: E.g., cannot test for all potential failures nor unexpected failures**	**Test CKMS operations within the expected environment[2] prior to procurement.**		**Automatically test periodically for negotiation of equivalent, compatible, and incompatible policies**
Section 9.8.1 **FR:9.11**	**Configuration Management**	**CKMS under device-level configuration management during implementation, procurement, installation, operation, maintenance, and disassembly. Record make, model and version for all devices of the CKMS.**		**Automated Configuration Management throughout CKMS lifetime; automatically track and record CKMS device IDs and locations.**
Section 9.8.2	**Secure Delivery**	**Verification that the procured products are those actually delivered. Unrequested delivery is detected. Tracking and verification of successful delivery in the expected time period.**	**Base + detection and/or prevention of tampering of CKM system, devices, or components during delivery**	

[2] Number of users, number of keys, temperature, communications and electrical service.

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 9.8.3 **FR:9.13**	**Development and Maintenance Environment Security**	**Implement physical security, separation of duties, computer security controls, network security controls, controls for ensuring the trustworthiness of implementation tools and the resulting hardware, software, and maintenance data as specified by the design.**	**Base + Personnel security3. Multi-person control of critical security parameters (e.g., CA certificates and keys) when implementing high-level security CKMS. Cryptographic security control of the integrity of software and critical data.**	
Section 9.8.4	**Flaw Remediation Capabilities**	**Implement capabilities for detecting[4] and expeditiously reporting potential and detected flaws[5] to developers and managers. Implement and use capabilities for installing authorized fixes quickly and then testing for adequacy as specified by the design.**		**Automated initiation of flaw detection and reporting, based on dynamic risk monitoring**
Section 10	**Disaster Recovery**	**24 hour recovery from backup of the CKMS**	**12 hour recovery from backup of the CKMS**	**Fifteen Minute recovery from backup of the CKMS**

[3] Clearances and background checks, where appropriate, for developers, testers, and maintainers.
[4] E.g., known-answer tests, error detection codes, anomaly detection and functional testing.
[5] E.g., status-report messages.

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 10.1 **FR: 10.1**	**Facility Damage**	**Provide, maintain, and test environmental, fire, and physical protection and procedures for recovering from disasters at primary, backup and archive facilities as specified in the design; test yearly; examine procedures every five years.**	**Base + Test at least every 6 months to determine that these mechanisms and procedures work as expected. Backup facility operational within 12 hours. Potentially compromised keys revoked and replaced within 12 hours. Examine procedures every two years.**	**CKMS automatically transfers to backup upon detection of electrical, water, or facility failure or significant physical damage. Verify monthly that backup capability works properly. Verify that compromised keys are revoked and replaced as per domain policy**
Section 10.2 **FR:10.2**	**Utility Service Outage**	**Provide and maintain computer-facility industry-recommended electrical, water, sanitary, heating, cooling and air filtering requirements for the primary and all backup and archive facilities as specified in the design**	**Provide and maintain industry recommended high-availability utility services, including electrical, water, sanitary, heating, cooling and air filtering requirements for the primary and all backup and archive facilities**	**CKMS automatically transfers to backup upon detection of utility services damage. Verify monthly that backup capability works properly.**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 10.3 **FR:10.3**	**Communication and Computation Outage**	**Provide computation and communication redundancy needed to recover within 24 hours.**	**Provide computation and communication redundancy needed to recover within 12 hours**	**Provide automatic switch-over to backup computation and communications within 15 minutes**
Section 10.4 **FR:10.4**	**System Hardware Failure**	**Provide backup and recovery from hardware failures upon detection. Perform initial and yearly tests of redundant systems**	**Base + Repair or replace failed hardware within 12 hours. Perform periodic tests of redundant hardware at least once per month**	**Maintain backup of each CKMS sub-system for the primary and backup facilities. Return to secure state within 15 minutes**
Section 10.5 **FR:10.5** **FR:10.6** **FR:10.7**	**System Software Failure**	**Verify software integrity after loading into memory and before use. Follow CKMS security policy for backup and recovery from software failures. Immediately backup and verifiy software after returning the CKMS to a secure state. Test software after repair and before use.**	**Base + verify correctness of the security-critical software using known-answer tests. Perform daily backups.**	**Verify correct operation of CKMS software by performing supported key management functions in both the primary and backup facilities and verifying that the results are identical**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 10.6 **FR:10.10**	**Cryptographic Module Failure**	**Repair or replace failed modules and verify that authorized personnel perform these repairs and replacements self tests**		**Automatically switch CKMS processing to a backup capability upon detection and verification of a cryptographic module failure.**
Section 10.7 **FR:10.11** **FR:10.12**	**Corruption of Keys and Metadata**	**Use mechanisms to detect corrupted stored and transmitted keys and metadata, report corruption to the system administrator, and restore or replace the corrupted keys and metadata. Report to all affected users.**	**Base + train and then test personnel every six months in performing recovery and replacement processes.**	**Automatically report detected security-critical CKMS failures to all potentially affected users and initiate recovery and repair procedures.**
Section 11.1 **FR:11.2** **FR:11.2**	**Full Security Assessment**	**Full CKMS assessment before initial operation and after major system change or major compromise**		**Security assessment of CKMS modifications after adding new security domain support. Periodic security assessments.**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 11.1.1 **FR:11.3**	**Review of Third-Party Validations**	**CAVP and CMVP validation of crypto. algorithms and modules.**	**Base + NIAP/CC validation of non-crypto and hardware.**	**CKMS and its sub-systems and devices validated by a third party for implementation of its design and for conformance to SP 800-130 and SP 800-152.**
Section 11.1.2 **FR:11.5**	**Architectural Review of System Design**	**Perform an architectural review of CKMS design, implementation, installation, and configuration prior to initial deployment and after a major system redesign using a team having the required skill set.**		
Section 11.1.3 **FR:11.7**	**Functional and Security Testing**	**CKMS- designer and owner-specified functional and security tests before initial operation performed by the vendor, the owner, and a trusted third party (trusted by the Fed. Govt.); perform CKMS usability testing**	**Base + annual functional and security verification tests.**	**Automatically test all CKMS services for security and functionality that are intended to interact with other security domains and report results to security domain administrators**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 11.1.4 **FR:11.9**	**Penetration Testing**	**Perform penetration testing of CKMS and report the results to CKMS administrator.**	**Base + test CKMS sub-systems and devices before deployment and annually thereafter -see 9.6.**	**Perform automated penetration testing during policy negotiation among multiple CKMS in different domains.**
Section 11.2	**Periodic Security Review**	**Bi-annual reviews**	**Annual reviews**	**Automated periodic monitoring of security-critical processes. Automated security testing after two or more CKMS negotiate a new security policy for data from different security domains**
Section 11.3 **FR:11.14** **FR:11.15**	**Incremental Security Assessment**	**Assess the security of the component whenever a change is made in that component. Perform functional and security testing of the affected component before making the change operational.**	**Perform an incremental assessment of the CKMS whenever a change is made. Perform full functional and security testing before making the change operational.**	**Automatically perform random security tests for critical CKMS functions and report failures to affected domain security administrators**

Frame-work Section (FR:x.y)	Topic/Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 11.4 **FR:11.16**	**Security Maintenance**	**Perform an incremental security assessment before and after changes are made; report reasons for the change, discovered security defects, results of the assessment, and the corrective actions taken**	**Base + perform security state verification following any routine or emergency maintenance on a CKMS or its devices**	**Automatically perform security verification on policy enforcing CKMS after a new policy is negotiated between two mutually suspicious but cooperating entities in different security domains**
Section 12	**Crypto Technology Review**	**Compare CKMS design and implementations with latest CKMS technology and new products every two years**		**Review CKMS-relevant technology in all countries participating in security policy enforcement with United States-based CKMS**