SP 800-152
Profile of SP 800-130 for the Federal Government

September 10, 2012

Elaine Barker (Presenter)
Dennis Branstad
Miles Smid

Purposes of the Profile

- Provide requirements for Federal Govt. CKMS, based on the SP 800-130 CKMS Framework
- Specify algorithms, key types, metadata
- Specify requirements for procurement, installation, configuration, operation and use
- Specify systems, subsystems, devices, components, security interfaces, facilities, security functions
- Support a range of security protections – low, moderate and high, as specified in SP 800-53
- Serve as a basis for agencies to augment the profile with additional requirements, if necessary
- Serve as a model for other public and private sectors

Scope

- Specifies requirements for secure key mgmt. in Federal systems; not how to do, but what must be done
- Supports a wide-variety of applications
- Sensitive information, not classified information
- Applicable to the Federal govt. and its contractors; other sectors may use this as a foundation for their own sector profiles

Differences Between the Framework and the Profile

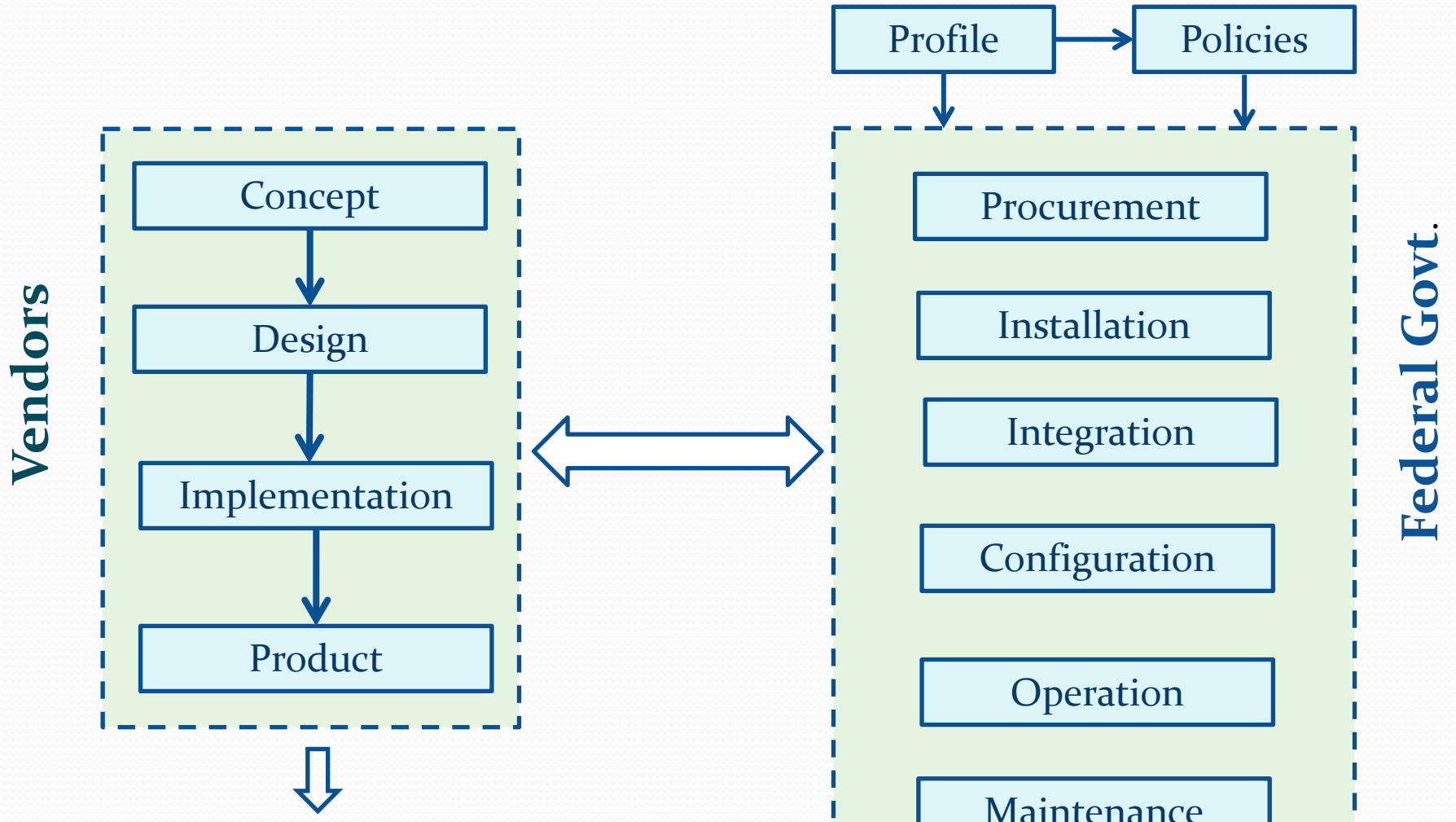
Framework

- Identifies topics to consider when designing a CKMS (product)
- Requires documentation about what is or is not in the CKMS (product) design
- Requires that all Framework requirements be addressed (e.g., documenting whether or not a topic area is applicable to the CKMS design)

Profile

- Specifies what must be in the design and provides requirements for the management and use of the CKMS
- Requirements are on the specifics of the CKMS (product) design and implementation, the various testing required and the environment in which the CKMS operates
- Requires that all Framework and Profile requirements be met.

CKMS Development and Operation



Framework: What does the product do?

Plans

1. Coordinate among the Federal agencies to determine reasonable base and augmented requirements
2. Compare the profile against CKMS used by the govt.
3. Investigate methods for determining compliance
4. Create an initial draft from
   - The table provided for public comment
   - Public comments received
   - Comments received during the workshop
   - Results of steps 1-3
5. Post for public comment

Questions for Reviewers

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 must 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?

Initial Requirements

- Provided in three sets:
  - Base requirements: the minimum for all Federal CKMS
  - Augmented requirements: For CKMS with higher security needs
  - Desirable CKMS features: nice-to-have someday
- Interoperability for base and augmented reqs. indicated (in parens.)

Initial Requirements

- Posted in tabular form at http://csrc.nist.gov/publications/drafts/800-152/draft-sp-800-152.pdf

Framework Section (FR:x.y)	Topic/ Feature	Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Section 1 **FR:1.1 - Meet all "shall" requirements**	**Framework and Profile Requirements**	**Meet all Framework and Base Profile Requirements**	**Meet all Framework and Augmented Profile Requirements**	
…	…	…	…	…

Initial Profile Requirements

Framework Section (FR:x.y)	Topic/Feature
Section 1 **FR:1.1 - Meet all "shall" requirements**	**Framework and Profile Requirements** ★
Section 2.1 **FR:2.1 - Specify algorithms and key sizes**	**Cryptographic algorithms and key sizes** ★
Section 2.1 **FR:2.2 - Specify security strengths**	**Security strength of algorithms** ★
Not covered in the Framework	**Key and metadata sensitivity** ★

Previous

Next

Framework and Profile Requirements

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Meet all Framework and Base Profile Requirements	**Meet all Framework and Augmented Profile Requirements**	

Return

Cryptographic Algorithms and Key Sizes

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
NIST-approved algorithms and key sizes per SP 800-131A		**Multi-algorithm capability**

Return

Algorithm Security Strengths

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
112 bits of security minimum (112)	128 bits of security minimum (128)	Scalable security strength capability

Return

Key and Metadata Sensitivity

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Low, Moderate or High (Low)	Moderate or High (Moderate)	Multi-Level Security: Low, Moderate, and High

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 3.1	Key Mgmt. for Networks, Applications, and Users
Section 3.2 FR:3.4 - Specify Federal, natl. and international standards	Conformance to Standards
Section 3.3 FR:3.10 - Specify human error-prevention or failsafe features	Ease of Use

Key Mgmt. for Networks, Applications and Users

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Conformance to Standards

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Conform to applicable NIST security Standards and Recommendations.		**All CKMS services use applicable Federal, National, and International security and interoperability standards**

Return

Ease of Use

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 4 **FR:4.4 - Specify security policies that support the CKMS Security Policy** **FR:4.5 - Specify policies describing the conditions for key and metadata sharing**	**Security Policies: Required security policies**
Section 4.6 **FR:4.6 - Specify how accountability is enforced**	**Accountability**

Required Security Policies

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Accountability

<table>
<tr><th>Base Requirements (Interoperability)</th><th>Augmented Requirements (Interoperability)</th><th>Desirable CKMS Features for the Future</th></tr>
<tr><td>Required for all roles except the user role</td><td>Required for all roles</td><td rowspan="2">Personal Accountability for all activities within the CKMS while preserving anonymity and personal privacy</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 4.7 **FR:4.7 – Specify anonymity, unlinkability and unobservability policies supported and enforced**	**Anonymity, Unlinkability and Unobservability**
Section 4.8 **FR:4.14 – Specify countries and legal restrictions**	**Laws, Rules and Regulations: Intended use**
Section 4.9	**Security Domains**

Previous

Next

Anonymity, Unlinkability, Unobservability

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Laws, Rules and Regulations: Intended Use

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
US Federal Agency and Contractor facilities in US	Base + US Federal Facilities in Canada, Western Europe, Australia, and New Zealand.	Global US Federal Facilities

Return

Security Domains

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Support the CKMS Security Policy that is based on one security domain policy		**Support the CKMS security policy and multiple domain policies**

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 4.9.3 **FR:4.18 – Specify reqs. For reviewing and verifying policies of other domains**	**Obtaining Assurances**
Section 4.9.7 **FR:4.21 – Are multi-level security domains supported?**	**Multi-Level Security Domains**
Section 4.9.8 **FR:4.24 – Is upgrading or downgrading permitted?**	**Upgrading and downgrading**

Previous

Next

Obtaining Assurances

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Manual evaluation of security policies		Automated assistance of security policy evaluation

Return

Multi-level Security Domains

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Optional		Supports multi-level security domains

Return

Upgrading and Downgrading

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Optional	Only with security administrator approval	Automated support of administrative negotiation of a security level

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 5 **FR:5.1 – Specify roles, responsibilities and how roles are assigned**	**Roles and Responsibilities: Required roles** ★
Section 5.1 **FR:5.2 – Specify key and metadata mgmt. functions for each role**	**Roles and Responsibilities: Role separation**

Required Roles and Responsibilities

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
System Administrator, Cryptographic Officer, Key Owner, Audit Administrator, Key Custodian, System User		System Authority, Domain Authority, Registration Agent, Key Recovery Agent, CKMS Operator

Return

Roles and Responsibilities:
Role Separation

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Audit Administrator can assume no additional role other than a System User		

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.1 **FR:6.1 – Specify and define key types used**	**Key Types**
Section 6.2.1 **FR:6.2 – Specify metadata elements for a trusted assoc. , circumstances for creating and associating with a key, and method of association**	**Metadata Elements: Selection and how associated with the key**
Section 6.2.1	**Metadata Elements: Secret and private key protections**

Previous

Next

Key Types

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Metadata Element Selection and Assoc. with Keys

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Metadata Elements: Secret and Private Key Protections

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Confidentiality and integrity protection; integrity verified when received	Base+ source authentication	Integrity is verified before loading into crypto module prior to use

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.2.1	Metadata Elements: Public key protection
Section 6.2.1,	Metadata Elements: Metadata protection
Section 6.2.1 FR:6.10 – Specify the authoritative time source	Metadata Elements: Time source
Section 6.2.1 FR:6.12 – Specify dates, times and functions requiring a TTP time stamp	Metadata Elements: Time stamp

Previous

Next

Metadata Elements: Public Key Protection

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Integrity verified when received		Integrity is verified before loading into crypto module prior to use

Return

Metadata Elements: Metadata Protection

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Confidentiality protection if sensitive; integrity verified when received	Base+ source authentication	Integrity is verified before loading into crypto module prior to use

Return

Metadata Elements: Time Source

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
NIST time source; verified daily	NIST time source; verified hourly	NIST time source; verified as per domain policy

Return

Metadata Elements: Time Stamp

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.2.2 **FR:6.13 – Specify key and metadata information**	**Required Key and Metadata Information: Random number generation**
Section 6.2.2 **FR:6.13 - Specify key and metadata information**	**Required Key and Metadata Information: Disclosure and modification protections**
	Required Key and Metadata Information: Assurances
Section 6.3 **FR:6.15 – Specify possible key states**	**Key Lifecycle States and Transitions: Required states**

Required Key and Metadata Info: RNGs

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Any NIST-approved RNG per SP 800-131A	SP 800-90 RBG	

Return

Required Key and Metadata Info: Disclosure and Modification Protections

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Cryptographic when outside a cryptomodule		

Return

Required Key and Metasdata Protections: Assurances

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Obtain key and domain parameter assurances using approved methods		

Return

Key Lifecycle States and Transitions: Required States

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Active, revoked and compromised	Base+ destroyed	Pre-activated, deactivated, suspended, reactivated after suspension

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.4 FR:6.17 – Specify key and metadata functions to be supported	Key and Metadata Management Functions
Section 6.4.1 FR:6.19 – Specify the key-generation methods for each key type	Generate Key
Section 6.4.5	Revoke Key
Section 6.4.9	Destroy a key

Previous

Next

Key and Metadata Mgmt. Functions

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Generate Key

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Use NIST-approved methods		

Return

Revoke Key

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Required, with reason for revocation		

Destroy a Key

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Use approved methods		

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.5	**Crypto. Key and/or Metadata Security: Key and metadata storage outside a cryptomodule** ★
Section 6.6 **FR:6.79 – Specify how secret and private keys are kept secret during transport** **FR:6.82 – Specify key-agreement schemes supported**	**Crypto. Key and/or Metadata Security: During key establishment** ★
Section 6.6.3 **FR:6.84 – Specify key-confirmation methods used**	**Key Confirmation**

Previous

Next

Crypto. Key and/or Metadata Security: Key and Metadata Storage Outside a Cryptomodule

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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	

Return

Crypto. Key and/or Metadata Security: During Key Establishment

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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**

Return

Key Confirmation

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Optional	Required	

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.6.4 **FR:6.86 – Specify protocols for key establishment and storage** **Also Section 7** **FR:7.2 – Specify standards, protocols, interfaces supporting services, commands and data formats**	**Key Establishment Protocols**
Section 6.7.1 **FR:6.89 – How are key mgmt. functions restricted to authorized entities?**	**Restricting Access to Key and Metadata Management Functions**

Key Establishment Protocols

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Any NIST-approved or allowed protocol (common protocol required for interoperability)		Automated domain policy negotiation protocol (to be developed)

Return

Restricting Access to Key and Metadata Functions

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Single-factor authentication on security-relevant functions	Multi-factor authentication on security-relevant functions	Personal authentication and function authorization

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.7.2 **FR:6.94 – How are plaintext keys protected and controlled?**	**Restricting Cryptographic Module Entry and Output of Plaintext Keys**
Section 6.7.4 **FR:6.97 – Specify functions requiring multi-party control (specify *k* out of *n*)**	**Multi-party Control**
Section 6.7.5 **FR:6.99 – Specify keys using key-splitting techniques (specify *k* and *n*)**	**Key Splitting**

Restricting Cryptomodule Entry of Plaintext Keys

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.**	

Return

Multi-party Control

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Optional	Multi-party control on CA and/or KDC keys	Domain administrators for multi-domain services

Return

Key Splitting

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Optional		

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.8.1 (no specific FR) and Section 6.8.3 FR:6.107 – Specify key revocation and notification mechanisms	Key Compromise: Recovery
Section 6.8.2 FR:6.106 – Specify how metadata compromises are remedied Section 6.8.3 FR:6.107 -Specify key revocation and notification mechanisms	Metadata Compromise: Replacement of sensitive metadata

Previous

Next

Key Compromise: Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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		

Return

Metadata Compromise: Replacement of Sensitive Metadata

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Metadata revocation and replace both key and metadata	Base + audit of compromise	

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.8.4 **FR:6.108 – Describe how physical access to the cryptomodule is restricted**	**Cryptographic Module Compromise: Recovery**
Section 6.8.5 **FR:6.113 – Describe how unauthorized mods to the hardware, software and data are detected**	**Computer System Compromise Recovery**
Section 6.8.6 **FR6:115 b) – Describe mitigation techniques for recovering from compromise of network security control**	**Network Security Controls and Compromise Recovery**

Cryptomodule Compromise: Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Computer System Compromise Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Network Security Controls and Compromise Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Block unauthorized protocols ; install security patches and upgrades	Base + firewalls on networked computers	SCAP security status checking and perform recommended remediation

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 6.8.7 **FR:6.117 – Specify automated features for recovering from a compromise of personnel security**	**Personnel Security Compromise Recovery**
Section 6.8.8 **FR:6.118 – Specify how components and devices are protected from unauth. access**	**Physical Security Compromise Recovery**

Personnel Security Compromise Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Physical Security Compromise Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Controlled physical access to CKMS devices; Recovery procedures	**Base + two-factor physical access control.**	

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 7 **FR:7.1 – Specify how compatibility and interop. reqs. are satisfied across devices**	**Interoperability and Transitioning**
Section 7 **FR:7.2 – Specify standards, protocols, interfaces, supporting services, commands and data formats**	**Interoperability and Transitioning: Symmetric encryption using block ciphers**
	Block cipher modes ★
	Hash algorithm

Previous

Next

Interoperability and Transitioning

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Interoperability and Transitioning: Symmetric Encryption Using Block Ciphers

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Any NIST-approved symmetric algorithms per SP 800-131A **(AES-128)**		

Return

Block Cipher Modes

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
SP 800-38 **(Encryption only: CBC;** **Message authentication only: CMAC;** **Authenticated encryption: CCM;** **Key wrapping: CCM)**		

Return

Hash Algorithm

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Any FIPS-approved hash function per SP 800-131A (SHA-256)		

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 7 (contd.) FR:7.2 – Specify standards, protocols, interfaces, supporting services, commands and data formats	Hash-based message authentication
	Key Agreement ★
	Key Transport ★
	Key Derivation (from a pre-shared key) ★
	Digital Signature ★
Section 8	Security Controls
Section 8.1	Physical Security Controls

Hash-based Message Authentication

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
FIPS 198 (HMAC-SHA-1)		

Return

Key Agreement

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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)**	

Return

Key Transport

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
SP 800-56B **(KTS-OAEP; concatenation KDF with SHA-256)**	**SP 800-56B** **(KTS-KEM-KWS; concatenation KDF with SHA-256)**	

Return

Key Derivation: From a Pre-shared Key

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
SP 800-108 **(HMAC in counter mode with SHA-1)**		

Return

Digital Signatures

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Any NIST-approved digital signature algorithm per SP 800-131A **(ECDSA with curve P-256)**		**ECDSA with curve P-364**

Return

Security Controls

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Enforce CKMS Policy Sanctions	Base + multi-person control of critical system functions	Enforce Domain Policy Sanctions

Return

Physical Security Controls

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Physical protection; access control for CKMS devices, keys and metadata.	Base + access control to CKMS facilities.	

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 8.1 **FR:8.2 – Specify physical security controls for each device**	**Physical Security Controls: Protection of crypto. devices and components**
Section 8.2.1 **FR:8.3 – Specify secure operating system reqs.** **FR:8.5 – Specify the hardening features**	**Operating System Security**
Section 8.2.2 **FR:8.6 – Specify the security controls for each device**	**Individual CKMS Device Security**

Physical Security Controls: Protection of crypto. Devices and Components

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.		

Return

Operating System Security

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Individual CKMS Device Security

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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)

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 8.2.3 **FR:8.8 – Specify malware protection capabilities**	**Malware Protection**
Section 8.2.4 **FR:8.10 – Specify auditable events and indicate whether fixed or configurable**	**Auditing and Remote Monitoring**
Section 8.3 **FR:8.15 – Specify boundary-protection mechanisms**	**Network Security Control Mechanisms**

Malware Protection

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Implement and support time and event-driven malware scanning. Update software when available.	Base + rootkit detection software. Software integrity verified upon installation and periodically.	Configurable malware monitoring

Return

Auditing and Remote Monitoring

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Auditing of specified security-related events. Report events to audit administrator. Audit capability and audit log protected from unauthorized modification.	**Base + SCAP compatible**	

Return

Network Security Control Mechanisms

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.	

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 8.4 **FR:8.19 – Identify cryptomodules used and their security policies**	**Cryptographic Module Controls**
Not covered in the Framework	**Control Selection Process**
Section 9 **FR:9.1, FR:9.2, FR:9.3, FR:9.4, FR:9.5, FR:9.6, and FR:9.7 – Specify vendor, third-party, interop., self, scalability, functional and security testing performed**	**Testing and System Assurances: By vendor, third-party, and system, procurement authority for scalability, functionality, security, and interoperability**

Cryptographic Module Controls

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
FIPS 140-2 Level 2 or above	FIPS 140-2 Level 3 or above	FIPS 140-2 Level 4

Return

Control Selection Process

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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)

Return

Testing and System Assurances: By Vendor, 3rd Party, and system, Procurement Authority, for Scalability, Functionality, Security and Interoperability

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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**

Return

Frame-work Section (FR:x.y)	Topic/Feature
Not covered in Framework	Ease-of-Use Testing
Section 9.7 FR:9.8 – Specify environments for the CKMS	Limitations of Testing: E.g., cannot test for all potential failures nor unexpected failures
Section 9.8.1 FR:9.11 – Specify devices to be managed and protections to assure only auth. changes	Configuration Management
Section 9.8.2	Secure Delivery

Ease-of-Use Testing

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.

Return

Limitations of Testing

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Test CKMS operations within the expected environment prior to procurement.		Automatically test periodically for negotiation of equivalent, compatible, and incompatible policies

Return

Configuration Management

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.

Return

Secure Delivery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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**	

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 9.8.3 FR:9.13 – Specify security reqs. For the development and maintenance environment	Development and Maintenance Environment Security ★
Section 9.8.4	Flaw Remediation Capabilities
Section 10	Disaster Recovery
Section 10.1 FR: 10.1 – Specify environmental, fire and physical access control mechanisms and procedures for recovery from damage	Facility Damage

Previous

Next

Development and Maintenance Environment Security

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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 security. 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.	

Return

Flaw Remediation Capabilities

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
Implement capabilities for detecting and expeditiously reporting potential and detected flaws 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

Return

Disaster Recovery

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
24 hour recovery from backup of the CKMS	12 hour recovery from backup of the CKMS	Fifteen Minute recovery from backup of the CKMS

Return

Facility Damage

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 10.2 **FR:10.2 – Specify minimum electrical, water, sanitary, heating, cooling and air-filtering reqs.**	**Utility Service Outage**
Section 10.3 **FR:10.3 – Specify communication and computation redundancy available**	**Communication and Computation Outage**
Section 10.4 **FR:10.4 – Specify strategy for backup and recovery from hardware and device failures**	**System Hardware Failure**

Utility Service Outage

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.

Return

Communication and Computation Outage

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

System Hardware Failure

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 10.5 **FR:10.5 – Specify techniques used to verify software correctness** **FR:10.6 – Specify techniques to detect alterations or garbles in the software** **FR:10.7 – Specify strategy for backup and recovery from software failures**	**System Software Failure**
Section 10.6 **FR:10.10 – Specify strategy for repair or replacement of failed cryptomodules**	**Cryptographic Module Failure**

System Software Failure

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Cryptographic Module Failure

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.**

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 10.7 **FR:10.11 – Specify procedures for restoring or replacing corrupted keys and metadata** **FR:10.12 – Specify procedures for backing up and archiving keys and metadata**	**Corruption of Keys and Metadata**
Section 11.1 **FR:11.2 – Specify the circumstances for a full security reassessment**	**Full Security Assessment**
Section 11.1.1 **FR:11.3 Specify validation programs used**	**Review of Third-Party Validations**

Previous

Next

Corruption of Keys and Metadata

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.

Return

Full Security Assessment

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.**

Return

Review of Third-Party Validations

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 11.1.2 **FR:11.5 – Specify whether an architectural review is required**	**Architectural Review of System Design**
Section 11.1.3 **FR:11.7 – Specify required functional and security testing**	**Functional and Security Testing**
Section 11.1.4 **FR:11.9 – Specify penetration testing performed and the results**	**Penetration Testing**
Section 11.2	**Periodic Security Review**

Architectural Review of System Design

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.		

Return

Functional and Security Testing

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Penetration Testing

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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.

Return

Periodic Security Review

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Frame-work Section (FR:x.y)	Topic/Feature
Section 11.3 **FR:11.14 – Specify the circumstances for an incremental security assessment** **FR:11.15 – Specify the scope**	**Incremental Security Assessment**
Section 11.4 **FR:11.16 – List activities required to maintain security**	**Security Maintenance**
Section 12	**Crypto Technology Review**

Incremental Security Assessment

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Security Maintenance

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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

Return

Crypto. Technology Review

Base Requirements (Interoperability)	Augmented Requirements (Interoperability)	Desirable CKMS Features for the Future
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**

Return

Profile Status

- Initial requirements provided in table-form for public comment until October 10th
- Send comments to ckmsdesignframework@nist.gov with "Comments on SP 800-152 Profile Requirements" in the subject line.