Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Cryptographic Management Standard

Document Name: Cryptographic Management Standard	Effective Date: October 15th, 2018
	Last Revised Date: March 10, 2025
Document ID: IS.019	

Table of Contents

1. PURPOSE

1.1. This ***standard*** establishes requirements for cryptography and ***encryption*** techniques for the Commonwealth. Cryptographic ***controls*** will be used to protect confidentiality (e.g., ***encryption***), authenticity and integrity (e.g., digital signatures or message authentication codes).

2. AUTHORITY

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security, (EOTSS), possess the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of ***information, information systems***, ***assets***, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, ***agencies***, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), by any form of contractual arrangement, are required to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***standard***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***standard*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

4.3. Additional ***information*** regarding this ***standard*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/*policies*.

4.4. In the event of any conflict between the provisions contained in this ***standard*** and the provisions set forth in any of the Enterprise Information Security Policies, the provisions in the Enterprise Information Security Policies will govern.

4.5. Definitions of terms in bold may be found in the *IS.Glossary of Terms* at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance

5.3.2. Identify and explain in detail the ***risks*** created due to the non-compliance

5.3.3. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level

5.3.4. Specify the time-frame required to implement the ***controls*** and mitigate the identified ***risks***. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact information for both the ***risk owner*** and the ***control owner*** designated by the agency to accept and manage the ***risks*** associated with the non-compliance and implement the ***controls*** that will effectively mitigate the identified ***risks***.

6. STANDARD STATEMENTS

6.1. Cryptographic Key Management

6.1.1. Commonwealth Agencies and Offices must ensure that secure methods for ***key*** management are in place to support the integrity of cryptographic ***controls***.

6.1.1.1. ***Encryption keys*** must be stored separately from the ***data*** they ***encrypt***.

6.1.1.2. ***Encryption keys*** must be protected during transit and in storage.

6.1.1.3. Access to ***encryption keys*** must be restricted to authorized ***personnel***.

6.1.1.4. Self-decrypting archives, private ***keys*** and symmetric ***key*** stores must be protected with a passphrase.

6.1.1.5. In cases where a passphrase is required, passphrases must comply with the secure passphrase practices defined in *IS.014 Access Management Standard*.

6.1.1.6. A salting mechanism must be implemented for ***data*** stored using a cryptographic hash.

6.1.1.7. Static salt values must be at least sixteen bytes in length.

6.1.1.8. ***Information Systems*** that implement ***encryption*** must have a documented process for regenerating ***encryption keys*** should they become exposed.

6.1.2. ***Key*** Management Life Cycle

6.1.2.1. ***Key*** **Generation:** Commonwealth Agencies and Offices must ensure that all ***keys*** will be generated within a FIPS 140 or FIPS 202 - validated cryptographic module or obtained from another source approved by the Commonwealth for the protection of ***information***.

6.1.2.1.1. If password-derived ***keys*** are to be used, compliance with the password complexity requirements in *IS.003 Access Management Standard* is required.

6.1.2.1.2. If password-based encryption is not used, then random number generation must be used.

6.1.2.2. ***Key*** **Distribution:** Commonwealth Agencies and Offices must ensure that ***keys*** generated as defined in section 6.1.2.1 will be distributed

manually (manual ***key*** transport) or using an electronic ***key*** transport protocol (electronic ***key*** transport).

6.1.2.2.1. ***Keys*** must not be shared or distributed beyond those specific entities or devices requiring the use of the ***key*** for approved purposes.

6.1.2.2.2. ***Keys*** must not be delivered in the clear over an electronic communications channel.

6.1.2.2.3. ***Keys*** delivered in-person must be delivered to the intended recipient, or if delivered to a proxy recipient must be delivered in a tamper-evident container.

6.1.2.2.4. Utilities to load or enter ***keys*** or components of a ***key*** over an unprotected channel must not display or transmit the ***data*** entered in the clear.

6.1.2.2.5. Symmetric ***keys*** and the ***data encrypted*** by that ***key*** must not be transmitted together unless the ***encryption key*** is protected via a secondary ***encryption***, e.g., public ***key encryption***.

6.1.2.2.6. If sending a symmetric ***key*** to a person through email, the email must be ***encrypted*** with the recipient's public ***key***.

6.1.2.2.7. Distribution of ***keys*** to backup and archive functions must be through ***encrypted*** channels.

6.1.2.2.8. ***Keys*** used only for the storage of ***information*** (i.e., ***data*** or keying material) must not be distributed except for backup or to other authorized entities that may require access to the ***information*** protected by the ***keys***.

6.1.2.3. ***Key* Storage:** Commonwealth Agencies and Offices must ensure that ***keys*** that are stored must always be protected against compromise and tampering. ***Key*** storage refers specifically to "active ***keys***" used in the Commonwealth.

6.1.2.3.1. ***Keys*** must never be written down. Passwords or PINs used to access recovery ***keys*** must never be written down.

6.1.2.3.2. ***Keys*** that are stored in a ***software*** container (e.g., file, password manager, or other form of password keeper) must be ***encrypted***.

6.1.2.3.3. The ***key*** storage must only be accessible by an authorized person or an approved recovery agent.

6.1.2.4. ***Key* Backup/Escrow:** Commonwealth Agencies and Offices must ensure that backup ***keys*** are stored on independent secure storage media. ***Keys*** backed up by a Certificate Authority will be held in escrow.

6.1.2.4.1. ***Keys*** that are backed up/escrowed in a device ***key*** store must be ***encrypted***.

6.1.2.4.2. Backup/escrow copies of password-based ***encryption keys*** must never be written down.

6.1.2.4.3. ***Keys*** that are backed up/escrowed in a software container (e.g., file or another ***key*** store) must be ***encrypted***.

6.1.2.5. ***Key* Archive:** If keying material needs to be recoverable (e.g., after the end of its ***crypto period***), the keying material will either be archived, or the system will be designed to allow reconstruction (i.e., re-derivation) of the keying material from archived ***information***.

6.1.2.5.1. An archive of keying material will provide both integrity and access control in order to protect the archived material from unauthorized modification, deletion, and insertion.

6.1.2.5.2. When keying material is entered into the archive, it must be time-stamped so that the date-of-entry can be determined.

6.1.2.5.3. This date itself must be cryptographically protected so that it cannot be changed without detection.

6.1.2.6. ***Key* Usage:** Commonwealth Agencies and Offices must ensure that a single ***key*** will be used for only one purpose (e.g., ***encryption***, authentication, ***key*** wrapping, random number generation or digital signatures).

6.1.2.6.1. For asymmetric ***key*** pairs, each ***key*** of the pair will have its own ***crypto period***.

6.1.2.6.2. Symmetric ***keys*** will not be used to provide protection after the end of the ***originator usage period***. The recipient usage period may extend beyond the originator usage period.

6.1.2.7. ***Key* Renewal:** If a ***key*** makes it through the entire period of time it is valid without the need for revocation, Commonwealth Agencies and Offices must ensure that it will be renewed. One of the ***key*** renewal processes specified below must be used, depending on the ***user*** and the requirements of the certificate authority (CA).

6.1.2.7.1. Individuals do not have to prove their identity again to get a new certificate. If the certificate is in good standing and it is being renewed with the same CA, the old ***key*** can be used to sign the request for the new ***key***.

6.1.2.7.2. A new ***key*** is created by modifying the existing ***key***.

6.1.2.8. ***Key* Revocation:** Commonwealth Agencies and Offices must ensure that ***key*** revocation must be accomplished using a notification indicating that the continued use of the keying material is no longer recommended.

6.1.2.8.1. ***Keys*** for cryptographic systems will be evaluated when they have reached the end of their ***crypto period*** by the ***Data Steward*** or delegate and changed.

6.1.2.8.2. ***Keys*** will be revoked and replaced in the event of the compromise of cryptographic ***keys***.

6.1.2.8.3. ***Keys*** which belong to terminated or separated employees will be deactivated on the date of or prior to the date of termination or separation. Commonwealth Agencies and Offices will maintain a list of separated employees. This list will be reviewed annually to ensure that ***keys*** that were managed by separated employees and contractors have been revoked.

6.1.2.9. ***Key* Recovery:** Because ***key*** archival and recovery create circumstances under which an individual's private ***key*** is accessible to others, ***risks*** to confidentiality and ***data*** integrity are a concern and Commonwealth Agencies and Offices must ensure that they are mitigated by implementing industry leading best practices. The following is a list of important considerations when implementing ***key*** archival and recovery.

6.1.2.9.1. Defining ***key*** recovery ***policies*** and ***procedures***.

6.1.2.9.2. Using role-based administration.

6.1.2.9.3. Protecting ***key*** recovery agent ***keys***.

6.1.2.9.4. Auditing ***key*** recovery operations.

6.1.2.10. ***Key* Suspension:** A suspension is a temporary state where the ***key*** itself cannot be used for any cryptographic operation for a period of time but may go back into a state of active usage.

6.1.2.10.1. If a ***key*** is suspended, Commonwealth Agencies and Offices must ensure that its usage for cryptographic functions is not allowed.

6.1.2.10.2. Privileges may also be suspended from the ***application*** with which the ***key*** is associated.

6.1.2.10.3. Logging must be performed when a ***key*** goes into a suspended state or leaves a suspended state.

6.1.2.11. ***Key* Disposal:** ***Key*** disposal is the removal of a ***key*** permanently (from the ***user***, backup, escrow, and archives) as well as all traces of its use, e.g., any material ***encrypted*** by that ***key***.

6.1.2.11.1. Commonwealth Agencies and Offices must ensure that a ***key*** is destroyed when the certificate is no longer valid.

6.1.2.11.2. If the ***key*** pair is used for digital signature purposes, Commonwealth Agencies and Offices must ensure that the private ***key*** portion is destroyed to prevent future signing activities with the ***key***.

6.1.2.11.3. If the ***key*** pair is used only for privacy purposes, Commonwealth Agencies and Offices must ensure that a copy of the private ***key*** will be archived because the private ***key*** might need to be used to decrypt archived ***data*** that was ***encrypted*** using it.

6.1.2.11.4. Depending on the sensitivity of the ***key*** in question, it may be necessary for Commonwealth Agencies and Offices to contact the individuals who use this certificate and trust the credentials it represents to inform them to no longer trust this certificate.

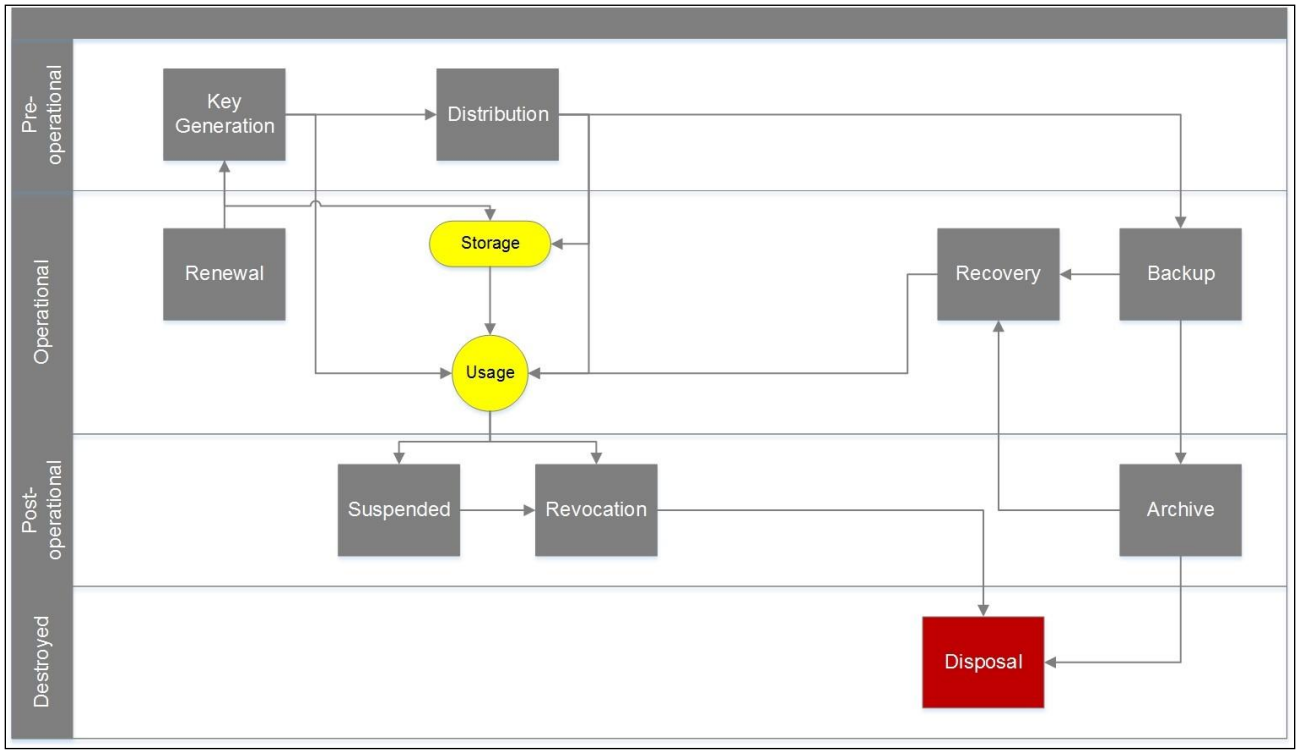

Figure 1: Key Management Life Cycle

6.2. Approved Cryptographic Techniques

6.2.1. Commonwealth Agencies and Offices must ensure that ***confidential information*** transmitted over an unsecured path will be ***encrypted*** with approved cryptographic techniques when appropriate.

6.2.2. Approved ***encryption*** algorithms and ***keys***:

Key Family	Recommended Algorithms	Acceptable Algorithms
Symmetric	AES	RC5, CAST, Twofish
Asymmetric	RSA, DSA	ECDSA, ECDH

Key Family	Algorithms	Minimum Key Length	Maximum Lifetime
Symmetric	AES	128-bit, 256 to be used if technically feasible	12 months
	RC5, , CAST, Twofish	128-bit, 256 to be used if technically feasible	12 months

Asymmetric, or public key	RSA	1024-bit (legacy implementation only) 2048 (new standard), 3072 recommended	12 months (1024) 36 months (2048)
	DSA (for verification only)	1024-bit finite field / 160-bit subgroup (deprecated — no longer recommended) 2048-bit finite field / 224-bit subgroup (legacy) 4096-bit finite field/ 256-bit subgroup is the new standard	12 months (2048) 36 months (4092)
	ECDSA (for signatures only)	256	12 months
	ECDH		12 months

6.2.2.1. Use approved ***encryption*** protocols (see above) for signing, ***encrypting***, and decrypting texts, emails, files directories, removable media, and whole disk partitions, especially while storing or exchanging ***confidential information.***

6.2.2.2. Use Transport Layer Security (version 1.2 or above) certificates issued by an approved and trusted Certificate Authority (CA) for ***information systems*** containing nonpublic ***information***.

6.2.2.3. Secure/Multipurpose Internet Mail Extension (S/MIME) for public ***key encryption*** and signing of MIME ***data***.

6.2.2.4. Secure Copy (SCP) or Secure File Transfer Protocol (SFTP) for file copy over Secure Shell (SSH v2). Use of FTP to transfer any ***confidential information*** is prohibited.

6.2.2.5. Secure Real Time Protocol (SRTP) for voice/multimedia traffic.

6.2.2.6. File compression ***software*** with the 256-bit AES ***encryption*** is acceptable for secure file transmission of ***confidential information*** via email within the Commonwealth.

6.2.2.7. Secure network access protocols, such as SSH v2, will be used in place of traditionally insecure protocols such as telnet, remote shell (rsh) and rlogin for login to a shell on a remote host or for executing commands on a remote host.

6.2.2.8. ***Encrypt*** remote access connections using approved ***encryption*** techniques (e.g., virtual private network (VPN)).

6.2.2.9. ***Confidential data*** transmissions over the Internet must employ end-to-end ***encryption*** mechanisms such as using HTTPS protocol and Transport Layer Security (TLS) v1.2, v1.3 or later, recommended.

6.2.2.10. Use current industry standard (e.g., WPA2, or WPA3) for wireless networks to implement strong ***encryption*** for authentication and transmission. The use of WEP as a security ***control*** is prohibited.

6.2.2.11. Internet facing ***Information Systems*** that implement TLS must obtain extended validation certificates (EV).

6.2.3. Certification Authorities

6.2.3.1. Commonwealth Agencies and Offices must ensure that the certificate must be configured to use 2048-bit or stronger RSA or 256-bit or stronger ECDSA private ***keys***.

6.2.3.2. Commonwealth Agencies and Offices must ensure that certificates must be signed using a SHA2 or SHA3 hashing algorithm when TLS 1.2 is being used.

6.2.3.3. Approved Commonwealth certificate authorities must be used for ***applications*** and services that require internal certificates.

6.2.3.4. Self-signed certificates are prohibited in a production environment, unless authorized by the Enterprise Security Office.

6.2.3.5. Commonwealth authorized certificate authorities must issue TLS 1.2 certificates with Fully Qualified Domain Name (FQDN).

6.2.3.6. ***Information systems*** must be configured to perform Path Validation (i.e., the certificate must be validated back to the trusted root Certificate Authority).

6.2.4. Commonwealth Agencies and Offices must ensure that ***encryption*** techniques will be reviewed on a semiannual basis or as required (e.g., deprecated ***encryption*** techniques are identified) to ensure the required levels of protection are identified, taking into account the type, strength and quality of the ***encryption*** algorithm required.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	18 v8	NIST CSF
6.1. Cryptographic Key Management	SC-12, SC-17, AC-3	- - CSC 3	PR.AC-1 PR.AC-3 PR.AC-4
6.2. Approved Cryptographic Techniques	IA-7, SC-8, SC-12, SC-13, SC-20, SC-28, AC-17, IA-2, IA-3	- CSC 3 - - CSC 4 CSC 3 CSC 12 CSC 6 -	PR.DS-1 PR.DS-6 PR.PT-2 PR.AC-4

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting
0.92	John Merto	01/02/2018	Corrections and formatting
0.95	Sean Vinck	5/7/2018	Corrections and Formatting
0.97	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	Annual Review; revised for NIST 800-53r5
1.4	Thomas E. McDermott	10/02/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony O'Neill	10/02/2023	Final Review
1.5	Thomas E. McDermott	12/3/2024	Corrections, Formatting, Updating and Annual Review
1.5	Anthony O'Neill	12/3/2024	Final Review
1.6	Thomas McDermott	2/10/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	2/12/2025	Correction and Formatting
1.6	Anthony O'Neill	3/10/2025	Final Review