State of Maine
Department of Administrative and Financial Services
Office of Information Technology

System and Communications Protection Procedures for Encryption Mechanisms (SC- 12, 13, and17)

Table of Contents

1.0. Purpose

The System and Communications Protection Procedures for Encryption Mechanisms detail State of Maine (SOM) procedures to leverage multiple layers of security measures to protect the organization's assets. The security controls detailed in this document align with select SC controls detailed in National Institute of Standards and Technology (NIST) Special Publication 800-53.

2.0. Scope

2.1. These procedures apply to all SOM personnel, both employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1. Executive Branch Agency information assets, irrespective of location; and

2.1.2. Information assets from other State government branches that use Executive Branch managed services.

3.0. Conflict

If these procedures conflict with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Procedures

4.1. SC Controls Cross References:

4.1.1. The following controls for the System and Communications Protection Policy and Procedures (SC) are published in separate policy and procedure documents:

4.1.1.1. System and Communications Protection Policy and Procedures[1] (SC-1, 7, 8);

4.1.1.2. System and Communications Protection Procedures for Defense in Depth (SC-2, 4, 5, 20, 21, 22, 23, 28, 32, 39) (under development); and

4.1.1.3. System and Communications Protection Procedures for Specific Technologies (SC-6, 10, 15, 18, 19, 40) (under development).

4.2. Cryptographic Key Establishment and Management (SC-12)

4.2.1. The Office of Information Technology (OIT) Computing Infrastructure & Services and OIT Enterprise Data Services use Entrust Certificate Authority (CA) (see Definitions) for external facing applications (see Definitions). Entrust or OIT public key infrastructure (PKI) (see Definitions) certificates are used for internal facing applications. OIT cryptographic key management is established in the Identification and Authorization (IA) policy, 8.4.8[2] (Intranet only) and is Federal Information Processing Standards (FIPS) 140-2 compliant or stronger.

4.2.1.1. OIT Computing Infrastructure & Services and OIT Enterprise Data Services maintain strict access control that uses the principle of

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemCommunicationsProtectionPolicy.pdf

[2] https://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

least privilege (see Definitions) for administrators. This ensures the availability of cryptographic keys in the event of loss of keys, such as forgotten passphrases.

4.2.1.2. OIT Information Asset Owners use product-specific features and internal administrative monitoring to guard against modification, substitution, and destruction of cryptographic keys. Private keys (see Definitions) are also protected against unauthorized disclosure.

4.2.1.3. Encryption key storage is managed by each Asset Owner, through either dedicated hardware or software modules.

4.2.1.3.1. Backups and recoveries are handled by Computing Infrastructure & Services and/or Enterprise Data Services. Backups are performed nightly, and daily reports of any failures are immediately addressed.

4.2.1.3.2. Access to Encryption Keys is limited only to authorized personnel.

4.2.1.3.3. Encryption keys are properly stored, separately from data.

4.2.2. **Cryptographic Key Establishment and Management, Symmetric Keys (SC-12(2)):** OIT Computing Infrastructure & Services produce, control, and distribute symmetric cryptographic keys using Microsoft Windows server root CA[3] and the public certificate authority Entrust for encryption and decryption. These dedicated hardware and software modules are approved by the National Security Agency (NSA), a government organization, and are FIPS-compliant.

4.2.3. **Cryptographic Key Establishment and Management, Asymmetric Keys (SC-12(3)):** Asymmetric key cryptography (see Definitions) is not used by OIT.

4.3. **Cryptographic Protection (SC-13)**

4.3.1. OIT Client Technologies enforces the protection of information systems and data storage as outlined in the Identification and Authorization (IA) policy, 8.4.8,[4] (Intranet only) in accordance with NIST Special Publication 800-53 and is FIPS 140-2 compliant.

4.3.2. Sensitive and restricted data: OIT uses external or removable storage devices that are encrypted to the AES-256 standard.

4.3.3. OIT has adopted the Federal Homeland Security Traffic Light Protocol (TLP)[5] (see Definitions) as the taxonomy of organizing data into categories so that data may be used and protected efficiently and to determine the appropriate

[3] https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment-overview

[4] https://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

[5] https://www.cisa.gov/tlp

level of risk management needed for unencrypted transmission (see Definitions) to a party not served by the OIT internal network (see the Data Exchange Policy). [6]

4.3.4. Laptop storage devices: OIT uses Trellix (formerly McAfee) encryption for internal/fixed storage devices.

4.3.4.1. External or removable storage devices are encrypted upon agency/department request. These external storage devices include SOM-issued and SOM-owned media devices such as secured digital (SD) cards, digital video disks (DVDs), media players (MPs) (see Definitions), and flash drives used to conduct SOM business.

4.3.4.2. Lookout (see Definitions) and Microsoft Intune (see Definitions) encrypt all SOM Android phones/tablets and iPhone/iPad mobile phones/tablets. See the Media Protection Policy (MP-1)[7] (Intranet only).

4.4. **Public Key Infrastructure Certificates (SC-17)**

4.4.1. OIT Computing Infrastructure & Services uses a NIST-approved secured process for PKI CAs. This secured process ensures that only approved trust anchors (see Definitions) are used for its information system trust stores (see Definitions), as outlined in the Identification and Authorization (IA) policy, 8.4.8[8] (Intranet only).

4.4.2. Registration of PKI certificates is strictly controlled by administrators in OIT Computing Infrastructure & Services using the principle of least privilege.

4.4.3. Authenticity of Entrust-issued PKI certificates: Entrust validates the authenticity of SOM's ownership of PKI certificates being issued during the time of issuance.

5.0. Document Details

5.1. Initial Issue Date: April 28, 2023
5.2. Latest Revision Date: April 28, 2023
5.3. Point of Contact: Enterprise.Architect@Maine.Gov
5.4. Approved By: Chief Information Officer, OIT
5.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[9]
5.6. Waiver Process: Waiver Policy[10]
5.7. Distribution: Internet[11]

[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlProceduresForUsers.pdf
[8] https://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf
[9] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[11] https://www.maine.gov/oit/policies-standards

6.0. Review

This document will be reviewed annually, and when substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

7.0. Records Management

OIT major policies and procedures fall under Maine State Archives General Schedule 1, Administrative Records[12], series GS1.13a, Policies and Procedures – Major. They will be retained for 6 years after being superseded or withdrawn. Typically, these records are archival (permanent) value, and will be evaluated on a case-by-case basis by Maine State Archives staff. If deemed archival (permanent) value, then OIT should send these records to Maine State Archives for their historical/research collection.

8.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA),[13] certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as to security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the Maine State Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the State.

9.0. Definitions

9.1. Asymmetric Key Cryptography: A cryptographic system where users have a private key that is kept secret and used to generate a public key (which is freely provided to others). Users can digitally sign data with their private key and the resulting signature can be verified by anyone using the corresponding public key. Also known as a Public-key cryptography. Source: NIST.[14]

9.2. Certificate Authority: A trusted entity that issues and revokes public key certificates. Source: NIST.[15]

9.3. External Facing Applications: Applications that are open to the internet and provide content to public users, internal employees, and business partners.

9.4. Lookout: A data protection and cloud security platform.

9.5. Media Player (MP): Software that "plays" audio, video, or animation files on a computer. Windows Media Player is the default player from Microsoft, but iTunes, RealPlayer and other software are also widely used. iTunes and QuickTime Player

[12] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf
[13] https://legislature.maine.gov/statutes/1/title1sec402.html
[14] https://csrc.nist.gov/glossary/term/asymmetric_key_cryptography
[15] https://csrc.nist.gov/glossary/term/certificate_authority

are the default products for Mac devices.

9.6. Microsoft Intune: A cloud-based service that focuses on mobile device management and mobile application management for mobile phones, tablets, and laptops (part of Microsoft Endpoint Manager).

9.7. Principle of Least Privilege: A security principle where users are assigned the minimal access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.

9.8. Private Key: A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. Source: NIST.[16]

9.9. Public Key Infrastructure (PKI): The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates. Source: NIST.[17]

9.10. Traffic Light Protocol (TLP): The Federal Homeland Security Traffic Light Protocol is used by OIT for the classification of Personally Identifiable Information (PII) impact level. See the Data Classification Policy.[18]

9.11. Trust Anchor: The end-entity certificate used to validate the identity of an entity such as a website, business, or person.

9.12. Trust Store: A list of root, intermediate, and user certificates that are trusted by the operating system or application.

9.13. Unencrypted Transmission: A communication method that does not meet encryption requirements as outlined in the Transmission of Sensitive Information Standard. For example, confidential or sensitive data may be intercepted by a malicious user by monitoring plaintext data that is transmitted across an unencrypted network to gain unauthorized access. This method can jeopardize the confidentiality of the sensitive data.

10.0. Abbreviations

10.1. AES: Advanced Encryption Standard
10.2. CA: Certificate Authority
10.3. DVD: Digital Video Disks
10.4. FIPS: Federal Information Processing Standards
10.5. FOAA: Freedom of Access Act (Maine)
10.6. MP: Media Players (MP3 and MP4)

[16] https://csrc.nist.gov/glossary/term/private_key
[17] https://csrc.nist.gov/glossary/term/pki
[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

10.7. NIST: National Institute of Standards and Technology
10.8. NSA: National Security Agency
10.9. OIT: Office of Information Technology
10.10. PII: Personally Identifiable Information
10.11. PKI: Public Key Infrastructure
10.12. SC: System and Communications Protection Policy and Procedures
10.13. SD: Secured Digital Cards
10.14. SOM: State of Maine
10.15. TLP: Traffic Light Protocol