UNIVERSITY
OF
CALIFORNIA

*UCOP*
*ITS*
*Systemwide CISO Office*
*Systemwide IT Policy*

# UC Encryption Key and Certificate Management Standard



**Revision History**

| Date: | By: | Contact Information: | Description: |
|---|---|---|---|
| 06/21/18 | Robert Smith | robert.smith@ucop.edu | Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC. |
| | | | |
| | | | |
| | | | |

# Contents

## 1 Background and Purpose

The purpose of this Standard is to establish requirements for selecting cryptographic keys, managing keys, assigning key strength and using and managing digital certificates.

Encryption can be an effective protection control when it is necessary to possess Institutional Information classified at Protection Level 3 or higher.

Encryption is not a substitute for other information protection controls, such as access control, authentication or authorization. Institutional Information encryption must be used in conjunction with other controls.

Mistakes in selecting keys, implementing the encryption/decryption process and managing keys and other secrets are common causes of data exposure. Using vetted, automated tools and processes is the best practice.

## 2 Scope

This Standard applies to all IT Resources, physical or virtual, that store, transmit or process Institutional Information classified at Protection Level 3 or higher and use encryption keys or digital certificates. Please refer to UC's Institutional Information and IT Resource Classification Standard for more information.

## 3 Key Terms and Definitions

In this Standard, encryption is used to refer to both the process of encrypting and the process of decrypting information. The term encryption key therefore refers to the keys needed for encryption and those needed for decryption.

## 4 Requirements for Encryption Keys and Digital Certificates

IT Workforce Members must use industry-approved strong algorithms for encryption and/or digital signing processes. The following subsections detail requirements that also ensure an adequate level of protection.

> **Note**: IT Resources that are connected to or store Institutional Information classified at Protection Level 3 or higher may also be subject to specific encryption requirements provided by regulation or contract.

### 4.1 Protecting keys

Workforce Members must protect private encryption keys to prevent their unauthorized disclosure and subsequent fraudulent use.

All private keys protecting Institutional Information and IT Resources are classified at Protection Level 4.

### 4.2 Private keys

- Workforce Members handling private keys must:
  - Physically and logically secure them.
  - Store keys in/on:
    - An encrypted key store or in an otherwise encrypted form.
    - A security token.
    - An Encryption keyring.
  - Not share the key with anyone other than those expressly authorized.
  - Never store the key(s) on the same IT Resource as the Institutional Information being protected at rest (e.g., encrypted storage).
  - Never reuse the key(s) to encrypt another set of unrelated or separate Institutional Information.
- Workforce Members handling private keys protecting Institutional Information classified at Protection Level 4 must record access so the use of the keys is auditable.
- Workforce Members handling private keys must follow the UC Institutional Information Disposal Standard when retiring keys.
- Workforce Members handling private keys protecting Institutional Information classified at Protection Level 4 should use a privileged access management tool.

### 4.3 Generating strong keys

- Workforce Members generating private keys must:
  - Select a key size of AES 128 bit or greater, or the minimum specified by the encryption method, whichever is greater when symmetric key encryption is employed.
  - Generate keys on the IT Resource itself or, if transmission of a private key is required, distribute keys manually using a public key transport mechanism or using a previously distributed or agreed-upon key-encrypting key.
  - Use a random key generation mechanism.

### 4.4 Emergency access to keys

- Unit Information Security Leads (UISLs) must have auditable procedures in place to provide access to private keys in the event of an emergency and/or the passphrase holder being unavailable.

### 4.5 Changing private keys and the private key lifecycle

- UISLs must:
  - Have a process to approve key changes, record dispositions and change keys when a Workforce Member with access to a private key(s) separates or changes roles.
  - Have a process to change keys as part of the response to an Information Security Incident.
  - For private keys protecting Institutional Information classified at Protection Level 3 or higher, change keys at least once annually.
- Private keys shall be revoked and/or deleted when they are no longer needed to perform a business function.

### 4.6 Encryption key backup and escrow

- Workforce Members must backup the private key associated with any encryption at rest of Institutional Information.
- UISLs must place in escrow the private key associated with any encryption of Institutional Information using at least one CISO-approved role (e.g., a Workforce Member who is trained to handle private keys) or in a CISO-approved tool or process (e.g. key management software, a second key pair to provide access).
- Workforce Members handling Institutional Information classified at Availability Level 3 or higher must test key recovery or business continuity/disaster recovery of keys at least once annually.

### 4.7 Access to keys

- Workforce Members handling private keys must be limited to those who have a need-to-know based on job responsibilities.

### 4.8 Encryption methods

- UISLs must select the stronger of the following methods:
  - An encryption method based on the Risk Assessment;
  - Symmetric - AES (128 bits or higher); or
  - Asymmetric/Public-Private key pair - RSA (2048 bits or higher).

### 4.9 Compromised keys

- Workforce Members must change encryption keys immediately if the key becomes compromised or is discovered by any unauthorized person or party.
- Workforce Members must report any compromised key to the CISO.

### 4.10 Web server certificates

- Workforce Members handling web server certificates must:
  - Use digital certificates signed by a CISO-approved certificate authority (CA).
  - Select a key size of 2048 bits or greater.

- Select an expiration of not more than three (3) years for IT Resources accessing Institutional Information classified at Protection Level 3.
- Select an expiration of not more than one (1) year for IT Resources accessing Institutional Information classified at Protection Level 4.
- Use a new public-private key pair when the certificate is renewed. (The public key is sent as part of the CSR - Certificate Signing Request.)
- Not use wildcard digital certificates for top level domains or subdomains accessing Institutional Information classified at Protection Level 3 or higher.

### 4.11 Code signing certificates

- Workforce Members handling code signing certificates must:
  - Protect access to these certificates with multifactor authentication.
  - Restrict access to the smallest group possible.

### 4.12 Self-signed certificates

- Workforce Members handling self-signed certificates must:
  - Not use them for any production purpose.
  - Not use them for the testing of IT Resources processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher.
- Use factory-installed certificates on IT Resources that are on protected private networks.

## 5 References

**Standards**

ISO 27002:2013 - Cross Reference. These ISO 27002:2013 requirements are met by this Standard.

| **ISO 27002:2013 Section** | **Requirements** |
|---|---|
| 10.1.2 | A persistent encryption key backup method must be established. |
| 10.1.2 | A persistent encryption key recovery method must be established. |
| 10.1.2 | Persistent private encryption keys must be secured. |
| 10.1.2 | Private encryption keys must not be stored or posted in clear text for any purpose. |

| | |
|---|---|
| 10.1.2 | Private encryption keys must be physically secured with at least two approved Workforce Members assigned backup access. |
| 10.1.2 | Private encryption keys must not be stored with or on the IT Resource(s) the key is protecting. |
| 10.1.2 | Access to private encryption keys must be recorded and limited based on current job responsibilities. |
| 10.1.2 | Private encryption keys must not be shared. |
| 10.1.2 | Encryption keys must be securely generated using a method approved by the CISO and a record must be kept of the approved purpose for the key. |
| 10.1.2 | Encryption keys must have the expected maximum lifetime of the key and related metadata documented in the Risk Assessment or other document approved by the CISO. |
| 10.1.2 | Encryption keys must not be reused and must be securely destroyed after use. |
| 10.1.2 | Issuing a private encryption key to any third party must be approved by the CISO. |
| 10.1.2 | Encryption keys protecting Institutional Information classified at Level 3 or higher must be changed when:<br>● Workforce Members who had access to one or more keys separate from UC.<br>● After a compromise that could have allowed an unauthorized party to gain access to one or more keys.<br>● When one or more keys is lost or damaged. |



A Framework for Designing Cryptographic Key Management Systems NIST SP 800-130

Recommendation for Key Management NIST SP 800-57 Part 1 Rev 4

OWASP Key Management Cheat Sheet

UC Institutional Information Disposal Standard

UC Institutional Information and IT Resource Classification Standard

**UC Policy**

- BFB-IS-3 Information Security