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.
7/31/2019	Robert Smith	robert.smith@ucop.edu	Adjusted 4.3 so that it applies appropriately to all ciphers – removing the specific reference to AES and 128 bits. 4.8 removed the names of specific algorithms (AES and RSA). Fixed minor formatting and errors.
8/21/2019	Robert Smith	robert.smith@ucop.edu	Updated to match standard formatting.
10/3/2019	Robert Smith	robert.smith@ucop.edu	Approved by ITLC.
2/10/2020	Robert Smith	robert.smith@ucop.edu	Technical edit, corrected section 5 to clearly show these are references and not requirements of this standard.

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.

For more information about definitions, consult the IT Policy Glossary.

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:

- o Physically and logically secure them.
- o Store keys in/on:
  - ▪ An encrypted key store or in an otherwise encrypted form.
  - ▪ A security token.
  - ▪ An Encryption keyring.
- o Not share the key with anyone other than those expressly authorized.
- o Never store the key(s) on the same IT Resource as the Institutional Information being protected at rest (e.g., encrypted storage).
- o 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:
  - o Select a key size using the minimum specified by the encryption method or greater when symmetric key encryption is employed.
  - o 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.
  - o 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:
  - o 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.
  - o Have a process to change keys as part of the response to an Information Security Incident.
  - o For private keys protecting Institutional Information classified at Protection Level 3 or higher, change keys at least once annually.
- ● Private keys must be revoked and/or deleted when they are no longer needed to perform a business function.
- ● Private keys must not be re-issued or reused.

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:
  o An encryption method based on the Risk Assessment;
  o Symmetric - using the minimum recommended key strength or higher; or
  o Asymmetric/Public-Private key pair - using the minimum recommended key strength 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:
  o Use digital certificates signed by a CISO-approved certificate authority (CA).
  o Select a key size of 2048 bits or greater.
  o Select an expiration of not more than three (3) years for IT Resources accessing Institutional Information classified at Protection Level 3.
  o Select an expiration of not more than one (1) year for IT Resources accessing Institutional Information classified at Protection Level 4.
  o 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.)
  o 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:
  - o   Protect access to these certificates with multifactor authentication.
  - o   Restrict access to the smallest group possible.

4.12   Self-signed certificates

- Workforce Members handling self-signed certificates must:
  - o   Not use them for any production purpose on a public network.
  - o   Not use them for the testing of IT Resources processing, storing or transmitting Institutional Information classified at Protection Level 3 or higher.
- IT resources with factory-installed self-signed certificates can only be used on protected private networks.

5   References

UC Policy

Business and Finance Bulletin IS-3 – Electronic Information Security

External Resources

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

ISO 27002:2013 - Cross Reference

Section	Description
10.1.2	Cryptographic algorithms, key lengths and usage practices should be selected according to best practices.
10.1.2	All cryptographic keys should be protected against modification and loss.
10.1.2	Equipment used to generate, store and archive keys should be protected.
10.1.2	A key management system should be based on an agreed set of standards, procedures, and secure methods for the following: • generating keys for different cryptographic systems and different applications; • issuing and obtaining public key certificates; • distributing keys to intended individuals or groups; including how to activate; • storing keys, including how authorized users obtain access;

Section	Description
	• changing or updating keys; • dealing with compromised keys; • revoking keys; • recovering keys; • backing up or archiving keys; • destroying keys; • logging and auditing of key management related activities.
10.1.2	Activation and deactivation for keys should be defined.
10.1.2	The authenticity of public keys should be considered.

Other External Resources:

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