ACME

Enterprise Key Management Policy

Version 2.0

Table of Contents

[Executive Summary 3](#_Toc199842194)

[Enterprise Key Management Policy and Standards 4](#_Toc199842195)

[Overview and General Policies 4](#_Toc199842196)

[Generation of strong keys 4](#_Toc199842197)

[Secure Key Distribution 4](#_Toc199842198)

[Periodic Changing of Keys and Cryptoperiods 4](#_Toc199842199)

[Destruction of Old Keys 5](#_Toc199842200)

[Prevention of Unauthorized Substitution of Keys 5](#_Toc199842201)

[Replacement of Known or Suspected Compromised Keys 5](#_Toc199842202)

[Revocation of Old or Invalid Keys 5](#_Toc199842203)

[Auditing 6](#_Toc199842204)

[Enterprise Key Management Roles 6](#_Toc199842205)

[Key Management Governing Body 6](#_Toc199842206)

[Key Owner 6](#_Toc199842207)

[Key Administrator 6](#_Toc199842208)

[Key Manager 7](#_Toc199842209)

[Key Components Holder 7](#_Toc199842210)

[Key Auditor 7](#_Toc199842211)

[Split Knowledge and Dual Control 8](#_Toc199842212)

[Authorized 2 of 4 Dual Control Configurations 8](#_Toc199842213)

[International Standards 8](#_Toc199842214)

[Appendix A: Key Custodian Acceptance Form 9](#_Toc199842215)

[Appendix B: Key Types Glossary 10](#_Toc199842216)

[Appendix C: References 12](#_Toc199842217)

# Executive Summary

This document is to be used as a guideline for deploying strategic Key Management systems within the ACME enterprise. It defines the Enterprise Key Management Policy which should govern systems which consume, generate or otherwise utilize secret keys for encryption.

The purpose of this document is to attain compliance for section 3.6 of PCI-DSS 1.1. Section 3.6 is described as:

**3.6** Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

**3.6.1** Generation of strong keys

**3.6.2** Secure key distribution

**3.6.3** Secure key storage

**3.6.4** Periodic changing of keys

• As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically

• At least annually.

**3.6.5** Destruction of old keys

**3.6.6** Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)

**3.6.7** Prevention of unauthorized substitution of keys

**3.6.8** Replacement of known or suspected compromised keys

**3.6.9** Revocation of old or invalid keys

**3.6.10** Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

The overall goal of PCI compliance for ACME is set at September 1st, 2007. By September 1st, ACME will have all outstanding PCI items in a compliant status so that a formal audit will be successful.

The sections outlined in the Enterprise Key Management Standard break down each section of the PCI-DSS 3.6 so that compliance with the standard may be achieved.

# Enterprise Key Management Policy and Standards

## Overview and General Policies

Public asymmetric keys are unrestricted by definition, therefore their confidentiality is not necessary; however, the integrity and authenticity of public asymmetric keys must be established, maintained, and verifiable. Public key certificates bind the user’s identity to the public key via the Certificate Authority’s signature on the certificate, and therefore ensure the integrity and authenticity of the certificate contents, including the public key it contains.

Key synchronization is the ability to verify that the same key (e.g., symmetric or asymmetric private key) is securely stored in one or more locations without compromising the security of the keys or the systems.

A cryptographic key should be used for only one purpose. For example, a given symmetric key may be used for the encryption of data or the encryption of keys (key wrapping) or the creation of a Message Authentication Code or the generation of random numbers, but should not be used for more than one of these functions. A public/private key pair may be used for signing and verifying digital signatures or establishing keys, but not both.

## Generation of strong keys

Key generation should use only approved algorithms (e.g., X9 standards) for random or pseudo-random number generation and random prime number generation

These approved algorithms can be found in the *ACME System Development & Maintenance Standard* document.

## Secure Key Distribution

Private asymmetric keys and symmetric keys shall only exist in the following secure forms:

* As cleartext inside the protected memory of a tamper-resistant security module
* As ciphertext outside the protected memory of a tamper-resistant security module
* As two or more key fragments (e.g., key components, k-of-n key shares), either in cleartext or ciphertext, managed using dual control with split knowledge.

These three forms ensure that the confidentiality of private asymmetric and symmetric keys is absolute; no one must ever know these keys.

## Periodic Changing of Keys and Cryptoperiods

A cryptoperiod is the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system may remain in effect. ACME uses the following criteria to establish appropriate cryptoperiods:

* Amount of information protected by a given key that is available for cryptanalysis
* Amount of exposure if a single key is compromised
* Use of a particular algorithm to its estimated effective lifetime, and amount of time available for cryptanalytic attacks to be useful
* The strength of the cryptographic mechanisms (e.g., the algorithm, key length, mode of operation),
* The embodiment of the mechanisms (e.g., FIPS 140-2 Level 4 implementation, software implementation on a Microsoft Windows machine), the operating environment (e.g., secure limited access facility, open office environment, publicly accessible terminal)
* The volume of information flow or the number of transactions
* The security function (e.g., data encryption, digital signature, key production or
* derivation, key protection)
* The rekeying method (e.g., keyboard entry, rekeying using a key loading device where humans have no direct access to key information, remote rekeying within a PKI)
* The number of nodes in a network that share a common key
* The threat to the information (e.g., who the information is protected from, and what are their perceived technical capabilities and financial resources to mount an attack).

Unless otherwise noted; all keys should be changed or rotated at least on an annual basis.

See glossary in Appendix K for a definition of the different key types.

## Destruction of Old Keys

When there are no further requirements for retaining keying material or its association with an entity, the key should be de-registered (i.e., all records of the keying material and its associations should be destroyed), and all copies of the private or secret key should be destroyed. Any media on which the keying material was stored should be erased in a manner that removes all traces of the keying material so that it cannot be recovered by either physical or electronic means.

*Note: while it may be desirable to destroy all copies of a public key, in many cases it is not possible to guarantee that this is actually done. Retention of the public key is not a security problem.*

## Prevention of Unauthorized Substitution of Keys

Only authorized users and secured transport channels are allowed to generate new keys. Sensitive encryption keys must be secured such that an unauthorized substitution cannot occur.

These controls may include physical security of an offline key generation, dual control and split knowledge access requirements to perform re-keying functions and periodic auditing.

## Replacement of Known or Suspected Compromised Keys

If a key used to provide confidentiality protection, via encryption, is compromised, or is known by unauthorized parties the Key Owner must be immediately informed.

Unauthorized access to system keys may occur when:

* Audit logs reveal inappropriate use, such as exporting of system keys without proper authorization (which may be tracked through audit logs and change request tickets)
* Evidence of physical tampering with the system
* Security issues prompt an audit due to physical compromise of a key component (e.g. a key component is missing) by an internal or external third party

The Key Owner must then document the incident and perform the following tasks:

* Document the incident including; date and time of compromise, means of compromise, as well as data, systems, and users affected,
* Open a ticket for authorization, and follow the appropriate procedures to revoke the compromised key(s)
* Inform associated application and or data owners of the incident
* Authorize the Key Manager(s) to securely issue the new keys

## Revocation of Old or Invalid Keys

It may be necessary to remove keying material from use prior to the end of its normal cryptoperiod for reasons that include key compromise, removal of an entity form an organization, etc. This is accomplished by notifying all entities that may be using the revoked keying material that the material should no longer be used. The notification should include:

* A complete identification of the keying material
* The date and time of revocation
* The reason for revocation (e.g. key compromised)

## Auditing

Key management systems should be audited on a regular basis to ensure that the practices continue to effectively support the Key Management Policy. The protective mechanisms should be reassessed as to the level of security that they provide and are expected to provide in the future.

The actions of the personnel that use, operate and maintain the key management systems should be reviewed by the Key Auditor to verify that they continue to follow established security procedures.

Unless otherwise noted, audits should occur on at a minimum on a quarterly basis.

## Enterprise Key Management Roles

This section defines the enterprise Key Management roles required for deploying, operating, and maintaining a secure Key Management solution.

Each user authorized to perform a key management duty must read and sign the Key Custodian form (found in the appendix).

It is acceptable for users of key management roles to be responsible for multiple systems, i.e. a Key Manager may perform that role for multiple key management systems.

### Key Management Governing Body

The Key Management Governing Body is responsible for reviewing and authorizing the Key Owner role. This governing body is made up of ACME management and meets quarterly to review the assigned Key Owner roles and authorized users.

### Key Owner

The Key Owner is responsible for the overall security of the encryption keys. This role is responsible for authorizing Key Admins and Key Managers. The Key Owner is also responsible for working with the Data Owners during such events as key compromises or other sensitive situations which may impact the integrity or security of the sensitive data. The Key Owner’s duties include:

* Authorize creation of the Key Manager and Key Administrator Roles
* Authorize key generation and revocation events
* Liaise and communicate with Data Owners during key compromises or other sensitive events which may jeopardize the security and/or integrity of data or systems.

### Key Administrator

The Key Administrator is responsible for setting up key management systems. This includes the following functional roles:

* Installation and setup of Key Management System
* Creation of the Key Manager/Security Officer role

*Note: Due to the sensitive nature of this role, no single individual should have sole access to a system which can create users who can export keys and generate initial key sets (see Split Knowledge / Dual Control sections).*

*In situations where the system does not have the capability to distinguish roles between a Key Administrator and Key Manager, these roles may be combined. However the functions must be carried out using dual control. This reduces the risk associated with a single user have the ability to export the master keys or perform other sensitive functions.*

### Key Manager

The Key Manager also known as the Security Officer, oversees the security, access, usage and handling of any encryption key or cryptographic device that resides in the location assigned to him/her, during its entire life cycle and to ensure that all such activities are in compliance with the ACME Key Management Policy. Some of he Key Manager’s responsibilities include:

* Create the user login and password
* Create the enabling key token (EKT)
* Create tokens
* Write device keys
* Enable the encryption-capable tape drives
* Tape drive enablement
* Create key sets and keys
* Import keys
* Export keys
* Key creation

*Note: Due to the sensitive nature of this role, no single individual should have sole access to a system which exports keys and generates initial key sets (see Split Knowledge / Dual Control sections).*

*In situations where the system does not have the capability to distinguish roles between a Key Administrator and Key Manager these roles may be combined, however the functions must be carried out using dual control. This reduces the risk associated with a single user have the ability to export the master keys or perform other sensitive functions.*

### Key Components Holder

Actual handling of keys in the component form (i.e. two or more full-length values) is done by a minimum of two trusted and trained individuals who will each be given access to a component of the key, under the supervision and guidance of the Key Manager. The Key Components Holder is to securely handle the encryption keys in the following manner:

* Keep the key component(s) secret and confidential, at all times, and not share a key component with anyone other then his/her designated backup.
* Follow the corresponding Key Component Holder Stand Operating Procedures guide in performing all key activities.
* Securely document all key activities performed.
* Inform the Key Owner or Key Manager of any known or suspected compromise or loss of a key component as soon as the event is known.

*Note: If dual control is in place, it may sufficient for the Key Manager and Key Components Holder roles to be fulfilled by the same personnel.*

### Key Auditor

The Key Auditor plays a security role to ensure that the Key Management Policy is being upheld. This includes the review of all administrative functions related to the creation and maintenance of all users of the Key Management solution. It all also includes any user or system usage of cryptographic keys.

*Note: There cannot be a ranking relationship between Key Mangers, Key Admins, Key Component Holders, or Key Auditors.*

## Split Knowledge and Dual Control

Due to this requirement, access to the Key Manager and Key Administrator roles must be secured using split knowledge and/or dual control procedures. This means that 2 of 4 authorized users are required in order to access the Key Management system as a Key Manger or Key Administrator.

The recommended scenario will consist of one set of Key Managers and Key Administrators, but in the event of a technology or geographic constraint (inability for key synchronization between physical sites or distance between physical sites); the policy may be implemented on a per location basis.

### Authorized 2 of 4 Dual Control Configurations

If the system provides the capability of generating dual control (dual authentication) methods, such that it may be configured to consume multiple user credentials in order to authenticate, this is the preferred method.

If the system does not have the inherent ability to enforce dual control, then a secured safe with dual key lock or dual PINs (meaning two keys or two PINs required in order to unlock it) may be utilized. All access requests must be securely logged and accessible to the Key Auditor.

Storing the key material in a single secured location is acceptable, so long as it does not pose an undue risk to business processes. For example, if the keys to system X and the keys to all the backups of system X are in the same place, this may pose a business risk as one fire may destroy all ability to run and restore system X.

The requirement for dual control stipulates that even if key materials are stored in the same place, control/access to these materials should be separated:

* The key materials for system X are stored in the key safe
* The key materials for system Y are stored in the same key safe
* The key safe is located in a security office with a physical (paper) ACL and log which is verified by a company security (physical security) officer each time access to the safe is granted
* Physical security officer (security guard) does not know combination to safe. He just has the sheet with images and names of those allowed access

When Key Managers (who have access to both X and Y materials via dual control) arrive to remove materials from the safe they must:

* Present him or herself to physical security officer (if necessary)
* Unlock safe using dual control
* Perform an inspection--all materials should have previously been identified and properly sealed in tamper evident envelopes
* Fill in a physical control log indicating time, date and materials removed and purpose
* Access log is signed by both Key Managers
* When materials are returned, the time and date are likewise noted in log and signed by both parties

A time limit should be in place to establish the amount of time these materials are allowed to be checked out at one time (the Key Managers should not be able to take them home or leave them overnight unsecured).

## International Standards

The ANSI X9 and ISO standards for symmetric key management have been established for over ten years, with revisions every five years per the ANSI procedures, or on an as-needed basis (e.g., X9 standards using single DES encryption have either been withdrawn or revised to triple DES encryption). Similarly, many ANSI X9 and ISO standards for asymmetric key management have been recently published or are in progress. In parallel to the X9 standards, auditing standards for certification authorities (CAs) relating to asymmetric key management have also been published.

# Appendix A: Key Custodian Acceptance Form

I accept and understand the responsibilities outlined in the Key Management Policy and Procedural documents supplied to me.

Check the applicable role and list applicable systems:

|  |  |  |
| --- | --- | --- |
|  | **Role** | **Associated Systems** |
|  | Key Owner |  |
|  | Key Administrator |  |
|  | Key Manager |  |
|  | Key Components Holder |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizer’s Name and Role

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

# Appendix B: Key Types Glossary

The following are types of keys. Not all types are utilized by ACME, however it is important to understand each type and how they may be used properly.

1. **Signing key:** The cryptoperiod of a signing key should, in general, be shorter than the cryptoperiod of the corresponding signature verification key.
2. **Signature verification key:** The cryptoperiod of a signature verification key should, in general, be longer than the cryptoperiod of the corresponding signing key so that signed information could be verified at a later time than when it was signed.
3. **Secret authentication key:** The cryptoperiod of a secret authentication key depends on the sensitivity of the type of information it protects. For very sensitive information (e.g., information that one would not like to be compromised (unprotected) if the key used to protect other information were compromised), should have an authentication key that is unique to that protected information. Otherwise, suitable cryptoperiods may extend beyond a single use.
4. **Private authentication key:** A private authentication key would presumably be used multiple times. Its associated public key could be certified, for example, by a Certificate Authority or Attribute Authority. The cryptoperiod of the private authentication key and its associated public key would be the same, e.g., for the cryptoperiod of the certificate. An appropriate cryptoperiod for the key would be 1-2 years, depending on its use.
5. **Public authentication key:** The cryptoperiod would be the same as the associated private authentication key. See the discussion for the private authentication key.
6. **Long term data encryption key:** A long term data encryption key is used multiple times over an extended period of time. An encryption key that is used to encrypt large volumes of information over a short period of time (e.g., for a link encryption) should have a relatively short cryptoperiod (e.g., a day or a week). An encryption key used to encrypt less information could have a longer cryptoperiod.
7. **Short term data encryption key:** The cryptoperiod of a short term data encryption key is very short, e.g., a single message or a communication session.
8. **RNG key:** The cryptoperiod of a key used to create random numbers depends on the amount of its use, though it may be used for an extended period of time. Suitable cryptoperiods might be a month or a year or two.
9. **Key encrypting key used for key wrapping:** This key may be used multiple times over an extended period of time. A key of this type that is used to encrypt large numbers of keys over a short period of time should have a relatively short cryptoperiod (e.g., a day or a week). If a small number of keys are encrypted, the cryptoperiod of the key encrypting key could be longer.
10. **Master key used for key derivation:** A master key is used multiple times. Therefore, a suitable cryptoperiod depends on the considerations provided earlier in this section.
11. **Keys derived from a master key:** The cryptoperiod of a key derived from a master key is relatively short, e.g., a single use or a communication session or transaction.
12. **Key transport private key:** A key transport private key would presumably be used multiple times. The cryptoperiod of the key transport private key and its associated public key would be the same, e.g., for the cryptoperiod of the certificate. An appropriate cryptoperiod for the key would be 1-2 years.
13. **Key transport public key:** The cryptoperiod would be the same as the associated key transport private key. See the discussion for the key transport private key.
14. **Static key agreement private key:** A static key agreement private key would presumably be used multiple times. The cryptoperiod of the private key and its associated public key would be the same, e.g., for the cryptoperiod of the certificate. An appropriate cryptoperiod for the key would be 1-2 years.
15. **Static key agreement public key:** The cryptoperiod would be the same as the associated static key agreement private key. See the discussion for the static key agreement private key.
16. **Ephemeral key agreement private key:** The cryptoperiod of an ephemeral key agreement private key should be the duration of a single key agreement process.
17. **Ephemeral key agreement public key:** The cryptoperiod of an ephemeral key agreement public key should be the duration of a single key agreement process.
18. **Secret authorization key:** An authorization key may be used for an extended period of time, depending on the resources that are protected and the role of the entity authorized for access. Suitable cryptoperiods should be less than two years.
19. **Private authorization key:** A private authorization key may be used for an extended period of time, depending on the resources that are protected and the role of the entity authorized for access. The cryptoperiod of the private authorization key and its associated public key should be the same. Suitable cryptoperiods should be less than two years.
20. **Public authorization key:** The cryptoperiod of the public authorization key should be the same as the private authorization key: less than two years. Other keying material does not have well established cryptoperiods, per se.

* Domain parameters remain in effect until changed.
* An IV is associated with the information that it helps to protect, and is needed until the information and its protection are no longer needed.
* Shared secrets should be destroyed when no longer needed to derive keying material.
* Seeds should be destroyed immediately after use unless needed for validation (e.g., as one of the elliptic curve domain parameters).
* Intermediate results should be destroyed immediately after use.

# Appendix C: References

*ACME Key Administrator User Guide v2.03*