ACME Cryptographic Key

Management Procedures

Information Security Department

March 1, 2016

ACME Cryptographic KeyManagement Procedures

Information Security Department

Table of Contents

[Confidentiality & Non-Disclosure 5](#_Toc273005807)

[Contact Details 5](#_Toc273005808)

[Document Information 6](#_Toc273005809)

[Version History 6](#_Toc273005810)

[Location 6](#_Toc273005811)

[Glossary of Terms 7](#_Toc273005812)

[1.0 Executive Summary 8](#_Toc273005813)

[2.0 ACME Key Management Lifecycle 8](#_Toc273005814)

[2.1.1 Stage 1 – [G] Generate 8](#_Toc273005815)

[2.1.2 Stage 2 – [E] Exchange 8](#_Toc273005816)

[2.1.3 Stage 3 – [C] Combine 8](#_Toc273005817)

[2.1.4 Stage 4 – [V] Validate 9](#_Toc273005818)

[2.1.5 Stage 5 – [A] Activate 9](#_Toc273005819)

[2.1.6 Stage 6 – [D] Destroy 9](#_Toc273005820)

[3.0 Compliance Regulations 9](#_Toc273005821)

[3.1 Interac Cryptographic Requirements 9](#_Toc273005822)

[3.1.1 Cryptographic Algorithm 9](#_Toc273005823)

[3.1.1.1 Triple DES Summary 9](#_Toc273005824)

[3.1.1.2 Triple DES Algorithm 10](#_Toc273005825)

[3.1.1.3 Triple DES Key Properties 10](#_Toc273005826)

[3.1.2 Key Length 11](#_Toc273005827)

[3.1.3 Key Integrity 11](#_Toc273005828)

[3.1.4 Key Change Frequency 11](#_Toc273005829)

[3.2 PCI-DSS Cryptographic Requirements 11](#_Toc273005830)

[3.2.1 Key Change Frequency 11](#_Toc273005831)

[3.2.2 Generation of Strong Cryptographic Keys 11](#_Toc273005832)

[3.2.3 Secure Cryptographic Key Distribution 12](#_Toc273005833)

[3.2.4 Secure Cryptographic Key Storage 12](#_Toc273005834)

[3.2.5 Periodic Cryptographic Key Changes 12](#_Toc273005835)

[3.2.6 Revocation of Keys 12](#_Toc273005836)

[3.2.7 Dual Custody and Split Knowledge 12](#_Toc273005837)

[3.2.8 Unauthorized Substitution 12](#_Toc273005838)

[3.2.9 Key Custodian Requirements 12](#_Toc273005839)

[4.0 ACME Production Cryptographic Standard 12](#_Toc273005840)

[4.1 Cryptographic Key Types 13](#_Toc273005841)

[4.2 Key/Group Naming Convention 13](#_Toc273005842)

[4.2.1 Field Length Limitation 13](#_Toc273005843)

[4.2.2 Key Naming Convention 14](#_Toc273005844)

[4.2.3 Group Naming Convention 14](#_Toc273005845)

[4.3 Key Management Activities 14](#_Toc273005846)

[4.3.1 HSM Console Laptop 14](#_Toc273005847)

[4.3.2 Key Generation 15](#_Toc273005848)

[4.3.2.1 MFK 15](#_Toc273005849)

[4.3.2.2 KEK and Other Keys 16](#_Toc273005850)

[4.3.3 Key Conveyance 17](#_Toc273005851)

[4.3.3.1 Conveyance of KEK 17](#_Toc273005852)

[4.3.3.2 Conveyance by KEK 18](#_Toc273005853)

[4.3.3.3 Conveyance by Clear Key Components 18](#_Toc273005854)

[4.3.3.4 Exporting Keys – Postilion 18](#_Toc273005855)

[4.3.4 Key Loading 19](#_Toc273005856)

[4.3.4.1 HSM 19](#_Toc273005857)

[4.3.4.2 Postilion 20](#_Toc273005858)

[4.3.4.3 ATM **Error! Bookmark not defined.**](#_Toc273005859)

[4.3.5 Key Substitution 20](#_Toc273005860)

[4.3.5.1 Tampered Conveyed or Stored Key Envelopes 20](#_Toc273005861)

[4.3.5.2 Keys that were delivered to an incorrect address 21](#_Toc273005862)

[4.3.5.3 Key Components that were shipped together 21](#_Toc273005863)

[4.3.5.4 Production Keys that were Conveyed via Electronic Mail 22](#_Toc273005864)

[4.3.6 Replacing Compromised & Subsidiary Keys 22](#_Toc273005865)

[4.3.6.1 MFK 22](#_Toc273005866)

[4.3.6.2 KEK 22](#_Toc273005867)

[4.3.7 Key Destruction 23](#_Toc273005868)

[4.3.7.1 MFK / KEK / TMK 23](#_Toc273005869)

[4.3.7.2 Postilion 23](#_Toc273005870)

[4.3.7.3 A98 Comvelopes 23](#_Toc273005871)

[4.3.8 Key Ceremony (Sessions) 23](#_Toc273005872)

[4.3.9 Key Storage 23](#_Toc273005873)

[4.3.10 Activity Log 23](#_Toc273005874)

[4.3.11 Key Renewals 24](#_Toc273005875)

[4.3.12 Key Revocation (Revoking Old/Inactive Keys) 24](#_Toc273005876)

[4.3.12.1 ATM Key Removal 24](#_Toc273005877)

[4.3.13 Test Keys 24](#_Toc273005878)

[5.0 Key Map (Key Acronym Cross Reference) 24](#_Toc273005879)

[5.1 Postilion Key Types 26](#_Toc273005880)

# Confidentiality & Non-Disclosure

This document contains information that is confidential and proprietary to ACME Management Inc. (ACME), and as such remains the property the respective party. Information contained herein may be the subject of patents, patent applications and otherwise comprise valuable intellectual property. It may be used only for the specific purpose for which it is supplied, namely the evaluation of switching service solutions, ATM solutions, transaction services, business opportunities or corporate relationships of mutual interest, and negotiating in good faith toward specific contract terms. Such information shall not be disclosed outside of the company, or party, to which it is directed, and shall not be duplicated, used or disclosed, in whole or in part, for any purpose without the prior written consent of ACME.

The recipient, by retention or use of this document agrees to the above terms and will protect the document from loss, theft and compromise.

## Contact Details

|  |  |
| --- | --- |
| ACME Management Inc.  123 Middle Drive  Nowhere, XY 00000  Telephone: (123) 456-7890  Put URL Here |  |
| Warn Yu  Information Security Director  (123) 456-7890  Put Email Here |  |
|  |  |

# Document Information

## Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue [2.4]** | **Date** | **Changes** | **Init** |
| 0.1 | April 14, 2010 | Created Base document | WHY |
| 0.2 | April 15, 2010 | Added Key Management Content and Merged other Documents | WHY |
| 0.3 | April 16, 2010 | Defined document structure for efficient information flow | WHY |
| 0.4 | April 18, 2010 | Added cryptography content | WHY |
| 0.5 | April 22, 2010 | Added key map data | WHY |
| 0.6 | June 24, 2010 | Added key management content | WHY |
| 0.7 | June 25, 2010 | Added key management content | WHY |
| 0.8 | June 28, 2010 | Added key Management content | WHY |
| 0.9 | June 29, 2010 | Added key Management content | WHY |
| 1.0 | June 30, 2010 | Added key Management content | WHY |
| 1.1 | July 6, 2010 | Modified Document Formatting | WHY |
| 1.2 | July 12, 2010 | Added ATM Key loading instructions | WHY |
| 1.3 | August 6, 2010 | Added A98 Comvelope Destruction Procedures | WHY |
| 1.4 | August 17, 2010 | Changed document sensitivity description | WHY |
| 1.5 | August 18, 2010 | Modified Key Map | WHY |
| 1.6 | August 23, 2010 | Updated KEK/KEY generation checklist | WHY |
| 1.7 | August 23, 2010 | Added Exporting Keys under Postilion | WHY |
| 1.8 | August 23, 2010 | Added Postilion Key Types definition | WHY |
| 1.9 | September 23, 2010 | Defined Key and Group naming convention for Postilion | WHY |
| 2.0 | November 01, 2010 | Defined PGK Key | WHY |
| 2.1 | June 11, 2012 | Added Postilion PAN Encryption Key Procedures | WHY |
| 2.2 | November 30, 2012 | Added 64bit clarity (32 HEX Characters) | WHY |
| 2.3 | May 1, 2014 | Minor revisions | WHY |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Location

This document can be found in these locations:

|  |  |
| --- | --- |
| **Type** | **Location** |
| Word (\*.doc) | [Internal URL] |
| Adobe Acrobat (\*.pdf) |  |

## Glossary of Terms

Throughout this document the following definitions will apply:

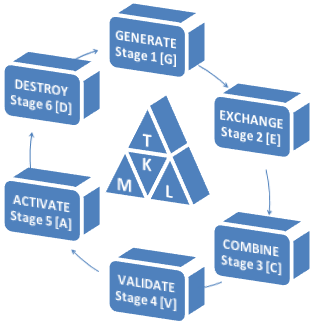
|  |  |  |  |
| --- | --- | --- | --- |
| HSM | Hardware Security Module | MFK | Master File Key |
| DES | Data Encryption Standard | 3DES | Triple DES |
| KEK | Key Exchange Key | PVK | PIN Verification Key |
| EMV | Euro pay/MasterCard/Visa | IMK | Issuer Master Key |
| LMK | Local Master Key | ZMK | Zone Master Key |
| PCI | Payment Card Industry | PCI-DSS | PCI Data Security Standard |
| KCV | Key Check Value | PCI-SSC | PCI Security Standards Council |
| cCVC | Chip Card Verification Key | FMPK | Final Master Personalization Key |
| MDK | Master Derivation Key | PEK | PIN Encryption Key |
| MAK | Message Authentication Key | BDK | Base Derivation Key |
| PGK | PIN Generation Key | CVC | Card Verification Key |
| PGP | Pretty Good Privacy | NIST | National Institute of Standards and Technology |
| DEK | Data Encryption Key | CIA | Confidentiality Integrity Availability |
| TKML | ACME Key Management Lifecycle | TMK | Terminal Master Key |
| UI | User Interface | GUI | Graphical User Interface |
| IV | Initialization Vector | DEA | Data Encryption Algorithm |
| OS | Operating System | PAN | Primary Account Number |
| CA | Certificate Authority |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

This document outlines the process for all cryptographic key management operations with respect to industry security best practices and compliance regulations. The intent of this document is to provide a detailed, clear-cut understanding, as well to define the processes for all cryptographic key management and related activities, for the ACME production environment.

# ACME Key Management Lifecycle

The key management lifecycle at ACME is based on six (6) stages, better explained as “GECVAD”.



### Stage 1 – [G] Generate

Stage 1 is where the key management lifecycle begins. At this stage cryptographic key components are created on the HSM, while exercising split knowledge, by predetermined key custodians and security coordinators. After all required components have been created; they are stored in vaults, secured with dual control.

### Stage 2 – [E] Exchange

At this stage, both ACME and client will exchange the key components they have generated. Key exchanges are done securely, using separate channels, and varying exchange intervals.

### Stage 3 – [C] Combine

The combine stage is where key components that have been successfully exchanged in stage 2 are retrieved from dual custody storage, and then combined on the HSM using split knowledge. The key cryptogram, which is a result of the combined key components, is recorded along with its integrity value then stored for future use.

### Stage 4 – [V] Validate

Validation is where the Key Check Value (KCV), also known as the integrity value, which was captured in stage 3 is validated against the client KCV value. If both values match this means that all key components were entered correctly and in the right order by both ACME and client.

### Stage 5 – [A] Activate

At this stage keys that have been combined in stage 3 and then successfully validated in stage 4 are activated for use by both ACME and client.

### Stage 6 – [D] Destroy

After the activation stage is complete, keys are then marked for destruction two (2) weeks after they have been activated then stored under dual custody until this date has been expired. The Security Coordinator then schedules all relevant key custodians for the destruction of such keys, to be done under supervision. Key components are recorded in the key destruction log then destroyed using a cross-cut paper shredder. At the end of the key destruction session, the Security Coordinator collects all shredded pieces of paper and places it in a locked paper recycling bin, stored in a secure zone of the building. Recycling bin is then securely emptied once weekly by trusted third-party paper recycling specialists.

# Compliance Regulations

The ACME Transaction Switching Environment is governed by various compliance regulations that exist mainly in the public domain, some of which include but not limiting to INTERAC/PCI-DSS/VISA, just to name a few. These guidelines incorporate Information Security best practices such as those published by NIST, and others not mentioned in this document. All these regulations and guidelines have something in common, which is simply put as “exercise proper due diligence” when considering Information Security Controls and Information Security Management.

## Interac Cryptographic Requirements

All cryptographic keys must be created and managed as follows:

### Cryptographic Algorithm

All Cryptographic keys must be generated using, at minimum, the Triple DES (3DES) encipher algorithm.

#### Triple DES Summary

The Triple Data Encryption Algorithm (TDEA) block cipher, commonly known as Triple DES (3DES), applies the Data Encryption Standard (DES) three (3) times to each data block. This is due to the fact that DES, originally, was becoming problematically short. Triple DES on the other hand was designed to provide a simple method of increasing the key size of DES to protect against brute force attacks, without designing a new block cipher algorithm.

#### Triple DES Algorithm

Triple DES uses a key bundle which is comprised of three (3) DES keys, K1, K2, and K3, each limited to 56 bits, excluding parity bits.

**3DES Encryption explained**

The 3DES encryption algorithm is: **‘ciphertext = EK3(DK2(EK1(plaintext)))’**

1. DES encrypt with K1
2. DES decrypt with K2
3. Then DES encrypt with K3

**3DES Decryption explained**

The 3DES decryption algorithm is: **‘plaintext = DK1(EK2(DK3(plaintext)))’**

1. Decrypt with K3
2. Encrypt with K2
3. Decrypt with K1

*Note: The Triple DES decryption process is the opposite, reverse, of the encryption process.*

Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using key option 2, and provides backward compatibility with DES with key option 3.

#### Triple DES Key Properties

**Odd Key Parity**

A single-length DES key is 8 bytes long, and is generally represented as 16 hexadecimal characters. Only 56 of the total 64 bits (or 32 HEX Characters) are used by the DES algorithm. The last significant bit of each byte is not used in the DES algorithm and is considered the parity bit. By convention, DES keys are odd parity (that is, the number of 1’s in each byte is odd). The following hexadecimal numbers are odd parity: 01, 02, 04, 07, 08, 0B …Thus, the odd parity null DES key is hexadecimal 0101010101010101.

**Key Check Value (Checksum)**

When conveying keys it is important for the KCV to be checked before and after it is conveyed. Checking must be done without accessing the clear values of the key itself.

Checking is accomplished by generating a key checksum. By convention, the checksum is the encryption of 8 bytes of zeroes with the key.

**‘Checksum = E(0…0)KEY’**

When conveying keys, or key components, the KCV must be included for the whole key or a component of the key.

The KCV is not a key and therefore it does not require the same level of protection as actual keys.

### Key Length

All cryptographic keys must be generated, at minimum, as Double Length (64bit length) keys. This means that key components must also be 3DES Double Length.

### Key Integrity

It is highly recommended that a minimum of two (2) 64bit length Double Length key components be combined to form a single 64bit length Double Length cryptographic key.

### Key Change Frequency

The Interac Security Regulation guidelines requires that all Cryptographic keys must be changed (refreshed) at these required intervals, or at the usage ACME, defined below.

|  |  |
| --- | --- |
| **Key Type** | **Key Change Frequency / Usage ACME** |
| MFK (LMK) | Every Five (10) years for TDES |
| KEK (ZMK) | Every Two (2) years for DES and (5) years for TDES |
| ATM Working Keys | Every Two Hundred (200) Transactions or Twenty Four (24) hours. |
| Financial Institution Working Keys | Every Two Thousand (2000) Transactions or Twenty Four (24) hours. |
| PAN Encryption KEY | Annually |

## PCI-DSS Cryptographic Requirements

*At the time of writing this document, PCI-DSS version 3 was used as a source of reference. As such, quoted requirements will most likely change in upcoming releases; at that time this document will require updating to reflect the new version of the published requirements.*

The following cryptographic key management guidelines, below, are those specifically required by PCI DSS.

### Key Change Frequency

The PCI Data Security Standard requires that all Cryptographic keys must be changed (refreshed) at these required intervals, or at the usage ACME, defined below.

|  |  |
| --- | --- |
| **Key Type** | **Key Change Frequency** |
| PAN Encryption KEY | Annually |
| File Encryption KEYS (PGP) | Annually |

### Generation of Strong Cryptographic Keys

All cryptographic keys must be created using strong cryptographic algorithms. Also the “secret” (something you know factor/Passphrase) used must be of substantial length while utilizing a random stream of varying alphabetic characters/numbers/and symbols, where possible.

AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz0123456789~`@#$%^&\*()/-\_=+\|]}[{‘”;:/?.>,<

### Secure Cryptographic Key Distribution

All Cryptographic keys must be distributed securely. Whenever possible, use a key exchange key to encrypt cryptographic keys when exchanged.

### Secure Cryptographic Key Storage

All Cryptographic keys must be store securely. It is highly recommended that all cryptographic keys be stored in dual custody vaults, or a vault per key custodian.

### Periodic Cryptographic Key Changes

All Cryptographic keys must be changed at least annually.

### Revocation of Keys

All Cryptographic keys must be revoked when:

* Expired (out of date)
* Compromised
* Known
* Deemed unusable

After the key has been revoked, it must be destroyed as defined in the Key Destruction section of the document.

### Dual Custody and Split Knowledge

All cryptographic keys must be stored under dual custody, meaning that no single person should have access to, or gain the ability to compromise an entire key. Split knowledge must also exist when handling cryptographic keys, meaning that an individual shout not, at any time, have knowledge of a whole key.

### Unauthorized Substitution

All Cryptographic keys must be secured in a way that prevents unauthorized substitution. Access to cryptographic keys must be provided based on a need-to-know. All access to key custodian vaults must be witnessed by the Security Coordinator and recorded in the vault access log. The Security Coordinator is required to sign the log book, per vault access.

### Key Custodian Requirements

All key custodians must sign a formal key custodians agreement, witnessed by the Security Coordinator, as formal acceptance of their key custodian responsibility defined in the key custodians agreement.

# ACME Production Cryptographic Standard

Cryptographic keys are an integral part of the ACME Transaction Processing Environment and as such require many stringent processes to ensure the CIA of each key. Below are usage guidelines for how Cryptographic keys are identified and handled within the ACME Transaction Processing Environment.

## Cryptographic Key Types

The table below provide a summarized definition of the various key types used in the ACME transaction processing switch environment.

|  |  |
| --- | --- |
| **Key Name** | **Key Definition** |
| MFK(LMK) | Master File Key (Local Master Key) – This is the Master key used to encrypt all keys under storage |
| KEK(ZMK) | Key Exchange Key (Zone Master Key) – Used to encrypt all keys that are transferred between security domains (from storage under one MFK to another) |
| PVK | PIN Verification Key – Used to create PIN Offsets |
| PBK | PIN Block Encryption Key |
| CVC | Card Verification Key – Reside in magnetic stripe on the back side of a card |
| CVK | Card Verification Key – Used to Calculate the CVC |
| cCVC | (EMV) Chip Card Verification Key – Track 2 equivalent data in the chip |
| FMPK | (EMV) Final Master Personalization Key – Used to secure a chip after personalization |
| IMKAC (CAK) | (EMV Application Key) Issuer Master Key – Application Cryptogram Key |
| IMKSMC (ECK) | (EMV Application Key) Issuer Master Key – Secure Messaging Confidentiality, Encryption, PIN Encryption Key for Issuer Script Processing |
| IMKSMI (EMK) | (EMV Application Key) Issuer Master Key – Secure Messaging Integrity, MAC Key for Issuer Script Processing |
| IMKAS | (Multos Application Management Key) – Issuer Master Key – Application Signature |
| IMKCS | (Multos Application Management Key) – Issuer Master Key – Certificate Signature |
| IMKKE | (Multos Application Management Key) – Issuer Master Key – Key Transformation Unit |
| IMKCU | (Multos Application Management Key) – Issuer Master Key – Card Unblock Certificates |

## Key/Group Naming Convention

Below is a definition of how cryptographic keys and key groups should be named, from the point in time the key and or key group is created.

### Field Length Limitation

Postilion presently supports a maximum of 55 characters for key and group names, however within the ACME Production environment this field was further restricted to 20 characters.

### Key Naming Convention

The standard for naming cryptographic keys within the ACME Production environment, are as follows:

NNNNNNNNN\_KKKKKK\_000

Where “NNNNNNNNN” are the 9 characters limitation reserved for defining an Issuer ID, “KKKKKK” are the 6 characters limitation reserved for key acronyms (these would be industry recognized key acronyms), and “000” are the 3 digits reserved identifying key indexes.

### Group Naming Convention

The standard for naming key groups within the ACME Production environment, are as follows:

NNNNNNNNN\_KKKKKK

Where “NNNNNNNNN” are the 9 characters limitation for defining an Issuer ID, and “KKKKKK” are the 6 characters limitation reserved for key acronyms (these would be industry recognized key acronyms).

## Key Management Activities

This section of the Key Management Procedures defines all procedural steps associated with ACME Key Management Lifecycle (TKML).

### HSM Console Laptop

The HSM Console Laptops are configured by the Security Officer according to a specific build document for HSM Console Laptops. All configurations are validated by an IS staff.

Maintenance of these laptops is done, periodically, by the Security Officer.

Before a production HSM laptop is used for any Key Management Activity, the following must be completed.

1. Retrieve:
   1. The PRIMARY HSM Console Laptop from the vault.
   2. Laptop power adapter.
   3. HSM Console Cable.
2. **‘Physically Inspect’** ALL hardware to identify ANY compromise/modifications.

*Note: If physical modifications/compromise is identified on any hardware, it MUST be replaced.*

1. Turning on Laptop:
   1. Connect power adapter to AC outlet and Laptop.
   2. Power on the Laptop.
   3. Login to the operating system.
2. If Laptop:
   1. Is suspected of compromise.
   2. OS looks suspicious.
   3. OS is infected with malicious software (not limited to Spyware/Viruses/Worms/Root kits)

*Note: If any of the above is TRUE the Laptop MUST NOT be used. The entire machine MUST be rebuilt from SCRATCH.*

1. Connect HSM Console cable to HSM and Laptop.
2. Launch HSM Console Application.

*Note: Alternatively, the BACKUP HSM Console Laptop that is located in the same vault as the PRIMARY HSM Console Laptop can be used in any event the PRIMARY is deemed unusable, as defined above.*

**Checklist to be used for ‘ALL’ HSM Console Laptops**

[HSM Console Laptop Checklist](https://policy.directcash.net/docview/?docid=356)

### Key Generation

Below are procedural guides on how to generate cryptographic key components.

#### MFK

Before an MFK is generated the Security Coordinator must formally schedule a key ceremony or in the event of an emergency, immediately gather all relevant vault and key custodians.

1. Key Custodians will:
   1. Unlock safe.
   2. Sign the vault access log book and state the reason for opening each vault.
   3. Retrieve their lock boxes, where HSM brass keys and HSM Console Laptop Vault keys are stored.
   4. Unlock Vault where HSM Console Laptops are stored, then sign the vault access log book and state the reason for opening this vault.
   5. Unlock HSM by removing the protective face plate.
2. Security Coordinator will follow HSM Console Laptop procedures.
3. Key Custodians will retrieve their individual HSM administration credentials then log in to the HSM, respectively.
4. Key Custodian MFK Part 1 will:
   1. Retrieve Blank cryptographic worksheet then label as ‘MFK Part 1’
   2. Generate their MFK key component (3DES Double Length).
   3. Record the HSM output values on their cryptographic worksheet.
   4. Clear the screen of any key values.
   5. Sign and date their cryptographic worksheet.
   6. Place worksheet in an envelope, seal and label ‘MFK Part 1’, then print the date.
5. Key Custodian MFK Part 2 will:
   1. Retrieve Blank cryptographic worksheet then label as ‘MFK Part 2’
   2. Generate their MFK key component (3DES Double Length).
   3. Record the HSM output values on their cryptographic worksheet.
   4. Clear the screen of any key values.
   5. Sign and date their cryptographic worksheet.
   6. Place worksheet in an envelope, seal and label ‘MFK Part 2’, then print the date.
6. Key Custodian MFK Part 3 will:
   1. Retrieve Blank cryptographic worksheet then label as ‘MFK Part 3’
   2. Generate their MFK key component (3DES Double Length).
   3. Record the HSM output values on their cryptographic worksheet.
   4. Clear the screen of any key values.
   5. Sign and date their cryptographic worksheet.
   6. Place worksheet in an envelope, seal and label ‘MFK Part 3’, then print the date.
7. Key Custodians will ‘Logout’ of the HSM.
8. Security Coordinator will:
   1. Remove HSM Console cable.
   2. Power down HSM Console Laptop then Place in it respective vault.
9. Key Custodians will:
   1. Secure HSM front panel (faceplate).
   2. Secure the HSM Console Laptop Vault.
   3. Secure all keys in their respective lock boxes.
   4. Secure the Key Custodians Vault.

**Checklist to be used for ‘ALL’ MFK key generation**

[MFK Generation Checklist](https://policy.directcash.net/docview/?docid=355)

#### KEK and Other Keys

Before a KEK is generated the Security Coordinator must formally schedule a key ceremony or in the event of an emergency, immediately gather all relevant vault and key custodians.

1. Key Custodians will:
   1. Unlock safe.
   2. Sign the vault access log book and state the reason for opening each vault.
   3. Retrieve their lock boxes, where HSM brass keys and HSM Console Laptop Vault keys are stored.
   4. Unlock Vault where HSM Console Laptops are stored, then sign the vault access log book and state the reason for opening this vault.
   5. Unlock HSM by removing the protective face plate.
2. Security Coordinator will follow HSM Console Laptop procedures.
3. Key Custodians will retrieve their individual HSM administration credentials then log in to the HSM, respectively.
4. Key Custodian KEK Part 1 will:
   1. Retrieve Blank cryptographic worksheet then label as ‘KEK Part 1’
   2. Generate their KEK key component (3DES Double Length).
   3. Record the HSM output values on their cryptographic worksheet.
   4. Clear the screen of any key values.
   5. Sign and date their cryptographic worksheet.
   6. Place worksheet in an envelope, seal and label ‘KEK Part 1’, then print the date.
5. Key Custodian KEK Part 2 will:
   1. Retrieve Blank cryptographic worksheet then label as ‘KEK Part 2’
   2. Generate their KEK key component (3DES Double Length).
   3. Record the HSM output values on their cryptographic worksheet.
   4. Clear the screen of any key values.
   5. Sign and date their cryptographic worksheet.
   6. Place worksheet in an envelope, seal and label ‘KEK Part 2’, then print the date.
6. Key Custodian KEK Part 3 will:
   1. Retrieve Blank cryptographic worksheet then label as ‘KEK Part 3’
   2. Generate their KEK key component (3DES Double Length).
   3. Record the HSM output values on their cryptographic worksheet.
   4. Clear the screen of any key values.
   5. Sign and date their cryptographic worksheet.
   6. Place worksheet in an envelope, seal and label ‘KEK Part 3’, then print the date.
7. Key Custodians will ‘Logout’ of the HSM.
8. Security Coordinator will:
   1. Remove HSM Console cable.
   2. Power down HSM Console Laptop then Place in it respective vault.
9. Key Custodians will:
   1. Secure HSM front panel (faceplate).
   2. Secure the HSM Console Laptop Vault.
   3. Secure all keys in their respective lock boxes.
   4. Secure the Key Custodians Vault.

**Checklist to be used for ‘ALL’ key generation, except for MFK**

[KEK & Other KEY Generation Checklist](https://policy.directcash.net/docview/?docid=354)

### Key Conveyance

All keys/key components must be conveyed as defined below.

**Checklist to be used for ‘ALL’ Key conveyance**

[Key Conveyance Checklist](https://policy.directcash.net/docview/?docid=353)

#### Conveyance of KEK



**KEK Conveyance Summary**

The creation of a KEK, between two organizations, is done mutually. In the above example, both TFTI and the Client contribute to the makeup of a KEK by creating and exchanging, clear 3DES Double Length, key components and their corresponding KCV. Both Organizations will then combine both KEK components, with TFTI’s KEK\_1 always being component 1 or the left side key component, to form a symmetric KEK. The KCV of the whole KEK is then compared by both organizations, if the KCV is the same on both ends this means the KEK was combined correctly.

#### Conveyance by KEK



**Key Conveyance by KEK Summary**

With a common KEK in place, organizations can transmit cryptographic keys as key cryptograms. This means that clear keys with one hundred percent (100%) integrity are encrypted with 3DES Double Length Keys before they are conveyed between organizations.

#### Conveyance by Clear Key Components



**Key Conveyance by Clear Components Summary**

When a KEK is not in place to securely exchange cryptographic keys, it is recommended that a key be conveyed in at least three (3) key components. According to the diagram above, the way this will work is for either organizations, being ACME or a Client, to generate three (3) individual 3DES Double Length key components, while exercising Dual Custody and Split Knowledge, then package each key component along with its corresponding KCV into separate tamper evident envelopes. These components must then be shipped, using separate channels on different intervals, to the designated key custodians on the receiving end.

After ALL key components have been successfully conveyed, both organizations will combine all key components in the same order, then compare they whole key KCV.

#### Exporting Keys – Postilion

This section explains how to export a key using a KEK as its parent under the Postilion Hardware Security Module interface. It is assumed that a key has already been generated and combined, combined key encrypted under an LMK (MFK). Additionally these instructions assume that a KEK (Parent\_KEK), parent key for keys that are exported, has been added to the Postilion crypto table.

1. Log into Postilion Realtime Management Console and launch the ‘Hardware Security Module’ application.
2. Select ‘Edit > Add New…’, as this will launch a ‘New DEA1 Key’ form for adding new keys to Postilion.
3. Enter a key ‘Name’ (i.e. IMK\_AC/etc).
4. HSM Type should be ‘Thales RG7000’.
5. ‘Key Type’ should be the correspond value for your key name, found in the Postilion section of the Key Map table in this document.
6. Select a ‘PIN Block Format’, found in the Postilion Key Types section of this document.
7. Select an ‘IBM PIN Scheme’, found in the Postilion Key Types section of this document.
8. ‘Domain’ should be set to ‘Network’
9. ‘Use Variants’, should NOT be selected for key types that are to be exported. Variants should only be enabled for the Parent\_KEK in this scenario.
10. Set ‘Key Length’ to ‘Double’ and ‘Parity’ to ‘Odd’.
11. ‘Parent’ should be set to the Parent\_KEK.
12. ‘Key Under Storage Key – Part 1’ is the leftmost 16 characters of your double length key that is encrypted under an MFK, and ‘Part 2’ is the rightmost 16 characters of your key under the MFK.
13. Select ‘Save + Exit’.
14. Select the key Name you just added, and then click the ‘Export’ button.
15. Now double click on the key Name to open the ‘Modify DEA1 Key – […’ form.
16. The ‘Value under Parent’ is your key encrypted under the Parent\_KEK.

### Key Loading

The following procedures define the key loading process of cryptographic keys across various systems.

#### HSM

The following steps define the key injection process for the ACME production environment.

1. Key Custodians will:
   1. Unlock safe.
   2. Sign the vault access log book and state the reason for opening each vault.
   3. Retrieve their lock boxes, where HSM brass keys and HSM Console Laptop Vault keys are stored.
   4. Unlock Vault where HSM Console Laptops are stored, then sign the vault access log book and state the reason for opening this vault.
   5. Unlock HSM by removing the protective face plate.
2. Security Coordinator will follow HSM Console Laptop procedures.
3. Key Custodians will retrieve their individual HSM administration credentials then log in to the HSM, respectively.
4. Key Custodian 1 will:
   1. Enter their key component.
   2. Verify their KCV.
   3. Clear the screen of any key values.
   4. Secure store (put away) their key component.
5. Key Custodian 2 will:
   1. Enter their key component.
   2. Verify their KCV.
   3. Clear the screen of any key values.
   4. Secure store (put away) their key component.
6. Key Custodian 3 will:
   1. Enter their key component.
   2. Verify their KCV.
   3. Clear the screen of any key values.
   4. Secure store (put away) their key component.
7. Key Custodians will ‘Logout’ of the HSM.
8. Security Coordinator will:
   1. Remove HSM Console cable.
   2. Power down HSM Console Laptop then Place in it respective vault.
9. Key Custodians will:
   1. Secure HSM front panel (faceplate).
   2. Secure the HSM Console Laptop Vault.
   3. Secure all keys in their respective lock boxes.
   4. Secure the Key Custodians Vault.

#### Postilion

The following procedures outline the steps involved when loading keys into Postilion.

1. From the Postilion Realtime Management Console, launch ‘Hardware Security Module’ Configuration UI.
2. Add a new key (Edit-Add New...)
3. Enter key parameters:
   1. Name – key name
   2. HSM Type – Atalla NSP *(This value is universal throughout the environment)*
   3. Key Type – select preferred key type *(i.e. KEK/KVP/etc.)*
      1. PIN Block Format – Typically *‘ISO-0 (ANSI X9.8/VISA-1/ECI)’*
      2. PIN Verification Method – IBM
   4. Domain – NETWORK
   5. Use Variants [Yes] – ATALLA
   6. Key Length – Double
   7. Parity – Odd
   8. Key Under Storage Key – This is the key cryptogram which is the key under storage or an MFK
   9. Use Key Scheme [Yes]
4. Save + Exit

### Key Substitution

To identify and or prevent the substitution of cryptographic keys, the following procedures must be done for the relevant scenario, below.

#### Tampered Conveyed or Stored Key Envelopes

If a production key component envelope, that has been received or has been stored, becomes evident of tampering, the following procedure must be done.

1. Notify the Security Coordinator of tampering, and also provide the following information:
   1. Name of affected client(s)
   2. Name of sender and recipient
   3. Key Type
   4. Primary or Backup key
   5. Key Check Value
   6. Key creation date and by whom
2. Security Coordinator will execute the process for the affected key type in section *‘Replacing Compromised & Subsidiary Keys’*.
3. Key Coordinators will execute the process for the affected key type in section *‘Key Destruction’.*

#### Keys that were delivered to an incorrect address

If a key or key component was delivered to an incorrect address, the following procedure must be done.

1. Notify the Security Coordinator of incorrect delivery location, and also provide the following:
   1. Name of affected client(s)
   2. Name of sender and recipient
   3. Key Type
   4. Primary or Backup key
2. Security Coordinator will contact Client’s Security Coordinator and advise the client:
   1. That key was delivered to incorrect address
   2. Verify delivery address
   3. New key/key component must be generated and resent
3. Should the compromised key component get re-routed to ACME, the Key Coordinators will execute the process for the affected key type in section *‘Key Destruction’*.

#### Key Components that were shipped together

If two or more key components were shipped together, by the same courier at the same time, the following procedure must be done.

1. Notify the Security Coordinator of the incident, and also provide the following:
   1. Name of affected client(s)
   2. Name of sender and recipient
   3. Key Type
   4. Primary or Backup Key
   5. Key Check Value, if available
2. Security Coordinator will contact Client’s Security Coordinator and advise the client:
   1. That the keys need to be shipped using different channels on different delivery intervals.
   2. The keys received will be destroyed.
   3. New key components must be generated and re-delivered.
3. Key Custodians will execute the process for the affected key type in section *‘Key Destruction’*.

#### Production Keys that were Conveyed via Electronic Mail

If a production key was delivered using electronic mail, the following procedure must be done.

1. Notify the Security Coordinator of the incident, and also provide the following:
   1. Name of affected client(s)
   2. Name of sender and recipient
   3. Key Type
   4. Primary or Backup Key
   5. Key Check Value, if available
2. Security Coordinator will contact Client’s Security Coordinator and advise the client:
   1. That delivery method is non-compliant, and therefore keys/key components must be delivered by courier using separate deliver channels on varying delivery intervals
   2. The keys received will be destroyed.
   3. That new key must be generated and shipped in a compliant manner.
3. Key Coordinators will execute the process for the affected key type in section *‘Key Destruction’*.

### Replacing Compromised & Subsidiary Keys

The procedures outline the requirements for when a key is compromised.

#### MFK

In the event it became known that an MFK has been compromised, the following procedure must be done IMMEDIATELY.

1. Declare an EMERGENCY Maintenance window.
2. Take ALL Transaction switches OFFLINE.
3. Generate NEW MFK.
4. Load new MFK on an HSM.
5. Translate ALL keys under storage of the compromised MFK to the new MFK.
6. Delete ALL keys under storage of the compromised MFK.
   1. Scrub DB table to prevent restoration of deleted keys.
7. Replace compromised MFK on ALL HSMs with new MFK.
8. Replace ALL keys under storage of the new MFK.
9. Bring ALL Transaction switches ONLINE.
10. Securely destroy the compromised MFK.

#### KEK

In the event a KEK has been compromised, the following procedure must be done IMMEDIATELY.

1. Disable the compromised KEK.
2. Notify the client of the compromised KEK.
3. Initiate EMERGENCY key generation of new KEK.
4. Combine and load new KEK.
5. Enable new KEK.
6. Initiate changing of ALL working keys.
7. Securely destroy the compromised KEK.

### Key Destruction

All cryptographic keys must be destroyed as follows.

#### MFK / KEK / TMK

The destruction of MFK, KEK, and TMK must be documented then securely destroyed using cross-cut shredding device. The destruction process must also be witnessed by a third party. Key Custodians and witness are required to sign and date the key destruction log.

#### Postilion

Keys that have been decommissioned / revoked / compromised must be removed from Postilion’s cryptographic key store. This process must be witnessed by a third party. Both the Switch Applications Engineer and witness need to sign and date the key destruction log.

#### A98 Comvelopes

A98 Comvelopes must be destroyed using a crosscut shredder, by incineration or equivalent methods of destruction. The destruction process MUST be witnessed by a third party, who is NOT a key custodian.

After the “Key Component” section of the comvelope, bottom half, has been destroyed the key custodian MUST sign and date the top half of the comvelope then have it signed by the person who witnessed the destruction of the bottom half.

The top half of the comvelope, signature portion, must be returned to ACME for its record keeping.

### Key Ceremony (Sessions)

All key ceremonies, including emergency key ceremonies, MUST be scheduled and supervised by the Primary or Backup Security Coordinator.

### Key Storage

ALL cryptographic keys and cryptographic key components must be stored under dual custody and split knowledge. This means that NO single individual should be allowed gain knowledge of a whole key. Key storage facility must be a fire rated vault that is stored in a secure facility which is controlled by at least two authentication factors, something you have (Proximity or Swipe Badge) and something you know (PIN). The facility must also be under constant surveillance.

### Activity Log

All production key management activities MUST be logged. The following is a list of logs that are used to track all key management activities within the ACME environment.

|  |  |
| --- | --- |
| **Log Title** | **Description** |
| Keys Received | Contain entries for all keys that were received from customers by receiving key custodian |
| Keys Sent | Contain entries for all keys that were sent to customers by sending custodian |

### Key Renewals

It is the responsibility of the Security Coordinator to effectively manage the TKML (GECVAD). An important part of this responsibility is the management of key expiry dates, standardized by the regulatory compliance bodies of governance that applies to ACME.

***Recommendation*** *– It has proven efficient in the past to query the following parameters in production against the Postilion crypto DEA1 table to identify addition of new keys and key change dates/times.*

***SELECT NAME****,* ***CREATED,UPDATED FROM REALTIME.CRYPTO\_DEA1\_KEYS WHERE KEY\_TYPE=0 with UR***

The table below provides a high level highlight of key rotation frequencies based on key types.

|  |  |
| --- | --- |
| **Key Type** | **Rotation Frequency** |
| MFK | TDES MFKs are required to be rotated once every 10 years. |
| Postilion PAN Encrypting key | Once every 5 years. |

### Key Revocation (Revoking Old/Inactive Keys)

It is required that ALL inactive keys be removed from the production environment. The efforts to identify such keys are directly linked to the identification of expired keys. As such both Key Renewals and Key Revocation are identified and executed as a single key maintenance process.

#### ATM Key Removal

It is required that ALL cryptographic keys must be removed from ATM devices as it is disconnected from the network.

ATMs devices must not be shipped with cryptographic keys.

### Test Keys

It is required for ALL test keys to be logged and maintained by the Security Coordinator in the *‘Test Cryptographic Keys’* log.

# Key Map (Key Acronym Cross Reference)

The table below maps key acronyms and modifier/variants between various HSM manufactures and the Postilion transaction switch. This diagram was made specifically for the ACME production environment.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Common Keys** | **Futurex** | | **Thales** | | **Atalla** | | **Postilion** | |
|  | **Key** | **Modifier** | **Key** | **Variant** | **Key** | **Variant** | **Key** | **Variant** |
| MFK |  | unknwn |  | unknwn |  | unknwn | n/a | n/a |
| KEK | KEK | 0 |  |  |  |  | KEK | ATALLA |
|  | PEK | 1 |  |  |  |  |  |  |
|  | DEK | 2 |  |  |  |  |  |  |
| CVC | MAK | 3 |  |  |  |  | KVC | ATALLA |
| CVV | MAK | 3 |  |  |  |  | KVC | ATALLA |
| CVK | MAK | 3 |  |  |  |  | KVC | ATALLA |
| cCVC | MAK | 3 |  |  |  |  | KVC | ATALLA |
| PBK | PVK | 4 |  |  |  |  | KWP | ATALLA |
| PVK | PVK | 4 |  |  |  |  | KVP | ATALLA |
|  | ATM Key | 5 |  |  |  |  |  |  |
|  | IV | 6 |  |  |  |  |  |  |
|  |  | 7 |  |  |  |  |  |  |
| IMKAC | BDK | 8 |  |  |  |  | CAK | ATALLA |
| IMKSMI | BDK | 8 |  |  |  |  | EMK | ATALLA |
| IMKSMC | BDK | 8 |  |  |  |  | ECK | ATALLA |
| IMKAS | BDK | 8 |  |  |  |  |  | ATALLA |
| IMKCS | BDK | 8 |  |  |  |  |  | ATALLA |
| IMKKE | BDK | 8 |  |  |  |  |  | ATALLA |
| IMKCU | BDK | 8 |  |  |  |  |  | ATALLA |
| FMPK | BDK | 8 |  |  |  |  | ECK | ATALLA |
|  | PGK | 9 |  |  |  |  |  |  |
|  |  | A |  |  |  |  |  |  |
|  |  | B |  |  |  |  |  |  |
|  |  | C |  |  |  |  |  |  |
|  | EMV | D |  |  |  |  |  |  |
|  |  | E |  |  |  |  |  |  |
|  |  | F |  |  |  |  |  |  |
|  |  | 10 |  |  |  |  |  |  |
|  |  | 11 |  |  |  |  |  |  |
|  |  | 12 |  |  |  |  |  |  |
|  |  | 13 |  |  |  |  |  |  |
|  |  | 14 |  |  |  |  |  |  |
|  |  | 15 |  |  |  |  |  |  |
|  |  | 16 |  |  |  |  |  |  |
|  |  | 17 |  |  |  |  |  |  |
|  |  | 18 |  |  |  |  |  |  |
|  |  | 19 |  |  |  |  |  |  |
|  |  | 1A |  |  |  |  |  |  |
|  |  | 1B |  |  |  |  |  |  |
|  |  | 1C |  |  |  |  |  |  |
|  |  | 1D |  |  |  |  |  |  |
|  |  | 1E |  |  |  |  |  |  |
|  |  | 1F |  |  |  |  |  |  |

## Postilion Key Types

The screenshot examples demonstrate how keys should be configured in the ‘Hardware Security Module’ of Postilion Real time Management Console.

The key type configuration is for keys that will be exported, therefore no Variants are specified. After the keys have been exported ‘ATALLA’ variants can be specified.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Postilion Key Type Configuration Parameters** | | | | | | | | |
| **Common Keys** | **HSM Type** | **Key Type** | **PIN Block Format** | **IBM PIN Scheme** | **Domain** | **Variants** | **Key Length** | **Parity** |
| KEK | Thales RG7000 | KEK | n/a | n/a | NETWORK | ATALLA | Double | Odd |
| PBK | Thales RG7000 | KWP | ISO-0 | n/a | NETWORK |  | Double | Odd |
| PVK | Thales RG7000 | KVP | VISA | n/a | n/a |  | n/a | Odd |
| CVK | Thales RG7000 | KVC | n/a | n/a | n/a |  | n/a | Odd |
| CVC | Thales RG7000 | KVC | n/a | n/a | n/a |  | n/a | Odd |
| cCVC | Thales RG7000 | KVC | n/a | n/a | n/a |  | n/a | Odd |
| CVV | Thales RG7000 | KVC | n/a | n/a | n/a |  | n/a | Odd |
| IMK\_AC | Thales RG7000 | CAK | n/a | n/a | n/a |  | n/a | n/a |
| IMK\_SMI | Thales RG7000 | EMK | n/a | n/a | n/a |  | n/a | Odd |
| IMK\_SMC | Thales RG7000 | ECK | n/a | n/a | n/a |  | n/a | Odd |
| IMK\_AS | Thales RG7000 | ECK | n/a | n/a | n/a |  | n/a | Odd |
| IMK\_CS | Thales RG7000 | ECK | n/a | n/a | n/a |  | n/a | Odd |
| IMK\_KE | Thales RG7000 | ECK | n/a | n/a | n/a |  | n/a | Odd |
| IMK\_CU | Thales RG7000 | ECK | n/a | n/a | n/a |  | n/a | Odd |
| FMPK | Thales RG7000 | ECK | n/a | n/a | n/a |  | n/a | Odd |