FIS

HSM

Key Management and Key Exchange Process

Technology Services Australia

Empowering
the Financial World

FIS

Contents

Version	Author	Updates	Date
0.1	Marc Class	Initial Version	1st Oct, 2023
0.2	Marc Class	Grammer updates	19th Oct, 2023

©2023 FIS and/or its subsidiaries. All Rights Reserved.

1. Introduction

The purpose of this document is to describe the key management and key exchange process for FIS' Host Security Modules (HSM's). It will include the following areas:

- Definition of keys
- Key officers
- Key exchange process

2. Definition of Keys

- Local Master Key

  Local Master Key (LMK), is the highest-level hierarchical key for the HSM.

  The LMK is stored in three components on a Smart Card accessed by a PIN. These are duplicated at two different locations. The set of PINs for the Smart Cards are at two different locations.

  Access to both a set of Smart Cards and PINs is controlled by one organization being FIS.

  The LMK is used to encrypt the required application keys. Retirement of the LMK is not required as it never leaves the physical HSM.

- Transport Keys

  Zone Master Key (ZMK) is as an encryption key used for transporting encryption keys (e.g. Master Deviation Key) from one party to another.

  The ZMK is also known as a Zone Control Master Key (ZCMK).

  The ZMK can be generated by FIS to transport encryption keys between FIS and a client, card scheme (i.e. Visa, MasterCard, American Express) or vendor (i.e. PIN or embossing).

  Alternatively, the ZMK can be generated by a client, card scheme or vendor and exchanged with FIS. ZMK's are double length DES keys.

  The ZMK is generated in three components.

  Each component is sent to (if coming to FIS) or sent from (if being sent from FIS) by each of the three Key Officers.

  The ZMK is established as a cryptogram under an HSM's LMK key pair.

  The Transport key type used by FIS is a Double Length Triple DES 32 HEX Character Key type 000 or ZMK as defined by the Thales Variant LMK Scheme.

©2023 FIS and/or its subsidiaries. All Rights Reserved.

- Encryption Keys

The following keys can either be generated by FIS or by another party. If generated by another party, they need to be encrypted under the transport ZMK. Not all keys generated by FIS need to be exchanged with another party. For example, if FIS generates the CVK, it does not need to be exchanged with another party where FIS is responsible for the creation of embossing and authorization verification, although if a card scheme performs card verification during stand-in processing, the CVK would need to be exchanged between FIS and the card scheme.
Below is the encryption key types currently support by FIS:

- CVK – Card Verification Key. Key used for CVV, CVV2, CVC, CVC2, iCVV, 3CSC, 4CSC and 5CSC calculation during card embossing and verification during authorization verification.

- CAVV – Cardholder Authentication Verification Value. Key used during 3D Secure authentication transactions.

- PVK – PIN Verification Key. Key used for PIN PVV calculation during PIN generation and authorisation verification.

- PNK – PIN Key. Key used to calculate the cardholder PIN.

- MDK – Master Deviation Key. Key used to decrypt the chip card cryptogram.

- ZEK – Zone Encryption Key. Used to encrypt the Zone PIN Key which encrypts the PIN in the file sent to the embossing vendor if using offline PINs.

- ZMK – Zone Master Key (on BC10). Used to encrypt the Zone PIN Key which encrypts the PIN in the PIN mailer file.

- IWK – Issuer Working Key – Used to encrypt the PIN in authorizations.

- AUTHENTICATE – Used to verify the ARQC and to create the ARPC.

- SCRIPT MAC – Script Message Authentication Code. Used to generate the MAC required to send a PIU script to a chip card.

- PIN CHANGE – Key that encrypts the PIN block on an Offline PIN change message.

There are no Cryptos in the HSM itself. Keys are generated by the applicable application/s and managed as per individual processes (i.e. P1C (BASE Global), MasterCard, VISA, JCB, clients, embossing vendors, customer switches etc.)

©2023 FIS and/or its subsidiaries. All Rights Reserved.

3. Key Officers

The purpose of a Key Officer is:

- Generation of the three LMK components. Each component is stored on a Smart Card which can only be assessed by the authorised Key Officer using a four digit PIN.

- Generation of the three ZMK components where FIS is responsible for the exchange of Keys with another party.

- Authorising the HSM when keys need to be generated or translated. Key Officers 1 and 2 only.

- Recipient of ZMK components received from another party (e.g. client).

- Sender of the ZMK components to other party (e.g. client) for FIS generated ZMK's.

- Receiver and sender for encrypted key components (e.g. PVK). The keys for exchange are encrypted under the ZMK and passed to one or more key custodians. Some keys are in two parts (e.g. CVK) and others are in one part (e.g. MDK). For two part keys usually only Key Officers 1 and 2 are involved and Key Officer 1 for one part keys.

The primary FIS Key Officers responsible for key parts are as follows:

- Key officer 1 / Backup key officer/s 1 (component 1)
- Key officer 2 / Backup key officer/s 2 (component 2)
- Key officer 3 / Backup key officer/s 3 (component 3)

All Custodians are required to sign a Key Custodian Acknowledgement accepting their roles / duties as a custodian.

©2023 FIS and/or its subsidiaries. All Rights Reserved.

4. Key Exchange Process

The Key Exchange Process can be broken down into the following stages:

1) First each party exchanges a “Transport Key” in components. (ie ZCMK aka ZMK)
2) The components are formed into a Key (Encrypted under the LMK)
3) Once the Transport Key/s have been exchanged – subsequent keys can then be encrypted under the Transport key and safely and easily be exchanged between the parties.

FIS to Other Party

- For transport keys:
  - The three FIS Key Officers will generate the three ZMK components.
  -
  - Each component will be placed in a tamper proof envelope, sealed and signed by the FIS Key Officer.
  -
  - Each component will be sent to a component custodian at the other party.
  -
  - Each component will be sent via a different courier provider on different days to ensure that not one courier provider has all three components, and to ensure the three components arrive at different times to avoid all three components arriving at the other party's mail centre together.
  -
  - Upon receipt, each of the other party component custodians will be required to acknowledge receipt of their key components via email.

- For encryption keys:

  - The process is the same as above with the only difference being that FIS Key Officer 3 and the other party's component custodian 2 and 3 may not get involved as encryption keys are usually in one or two parts.
  - FIS will enter the encrypted keys within the relevant parameter table (e.g. BC10).

©2023 FIS and/or its subsidiaries. All Rights Reserved.

Other Party to FIS

- For transport keys:
  - The three other party Key Officers to generate the three ZMK components.
  -
  - Each component needs to be placed in a tamper proof envelope, sealed and signed by the other party's Key Officer.
  -
  - Each component is to be sent to the nominated FIS Key Officer.
  -
  - Each component needs to be sent via a different courier provider on different days to ensure that not one courier provider has all three components, and to ensure the three components arrive at FIS at different times.
  -
  - Upon receipt, the nominated FIS Key Officer will be required to acknowledge receipt of their key components via email.

- For encryption keys:

  - These keys will provide encryption of data or validation of items such as CVV, Cryptograms. These will be exchanged under the transport key to the primary Custodian, and in a key ceremony requiring 2 custodians will be imported into the System where they will be stored encrypted under the HSM Local Master Key.

©2023 FIS and/or its subsidiaries. All Rights Reserved.

3rd Party Retaining Responsibility for Key Custodianship to Other Party

This is where, for example a client is the custodian of the key(s) that are exchanged with an embossing vendor.

- For transport keys:

The three third party Key Officers will generate the three ZMK components.

Each component will be placed in a tamper proof envelope, sealed and signed by the 3rd part Key Officer.

Each component will be sent to a component custodian at the other party.

Each component will be sent via a different courier provider on different days to ensure that not one courier provider has all three components, and to ensure the three components arrive at different times to avoid all three components arriving at the other party's mail centre together. Alternatively, the third party custodians may elect to personally transfer the keys to the other part.

Upon receipt, each of the other party component custodians will be required to acknowledge receipt of their key components via email.

©2023 FIS and/or its subsidiaries. All Rights Reserved.

5. Key Generation, Export and Import Examples

Prerequisites:

For all of the following examples you will need:

- To be logged on to the HSM console.
- Have the necessary key custodians available.
- Have the necessary key components available.
- Have the necessary HSM Security Settings.
- NOTE! The following commands are for a Thales HSM only.

©2023 FIS and/or its subsidiaries. All Rights Reserved.

5.1 Generating a Transport Key / Zone Master Key

1) Authorise the HSM for component.{key}.console

2) Generate the Key components

```
Online-AUTH> GC
Enter LMK id: 00            (NOTE – this depends on the HSM)
Enter Key length: [1,2,3]: 2
Enter key type: 000         (Key type 000 ZMK)
Enter key scheme: U

Clear component: 2CE0 79A1 0E34 D637 6E7A 2980 809B 7A08
Encrypted component: U9993 9066 0692 8BBE 9939 084F 2426 FD1D
Key check value: 89B8D3


Online-AUTH>GC
Enter LMK id [0-1]: 0
Enter key length [1,2,3]: 2
Enter key type: 000
Enter key scheme: U

Clear component: 3E4C 8508 86E5 CD3D CD97 FEE3 DAFD BFA2
Encrypted component: U4CFF AD11 F825 6EB3 7CDC A409 2E11 B255
Key check value: 561C1D


Online-AUTH>GC

Enter LMK id [0-1]: 0
Enter key length [1,2,3]: 2
Enter key type: 000
Enter key scheme: U

Clear component: CE5E B585 52E6 7CEC 08AB 0ED3 04FB 9458
Encrypted component: UC908 82A3 848B FF24 EB0B E63A 637F C877
Key check value: 26C4AF
```

Record the **Clear Component** and KCV on the Form in Appendix A

Run the above command three times or as required per number of Key Custodians

©2023 FIS and/or its subsidiaries. All Rights Reserved.

5.2 Forming a Key from components

These steps are used to form a key or to import a partners Transport key

From the HSM console:

1) Authorise the HSM for component.{key}.console

2) Form the Key:

```
Online-AUTH> FK
Enter LMK id: 00
Enter key length[1,2,3]: 2
Enter key type: 000
Enter key scheme: U
Component type [X,H,E,S,T]: X   (Clear Text Component)
Enter number of components [1-9]: 3

Enter component 1: **** **** **** **** **** **** **** ****
Component 1 check value: 89B8D3 Continue? [Y/N]: y
                    (Check this value matches the Component 1 check value provided by the partner)

Enter component 2: **** **** **** **** **** **** **** ****
Component 2 check value: 561C1D Continue? [Y/N]: y

Enter component 3: **** **** **** **** **** **** **** ****
Component 3 check value: 26C4AF Continue? [Y/N]: y

Encrypted key: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
Key check value: 19A9A8
```

- Record the FINAL KCV on the Form in Appendix A

- The U"Encrypted key" is used to encrypt the keys being exchanged.

5.3 Exporting a key under a Transport Key

The purpose of this command is to translate a key from encryption under an LMK to encryption under a ZMK

1) Authorise the HSM for: export.{key}.console

For this example, we will export a Pin Verification Key (type 002) and Card Verification Key (type 402)

Keys used for Example:

ZMK / Transport Key - Key Type Code 000

- Encrypted key: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
- Key check value: 19A9A8

Pin Verification Key - Key Type Code 002

- Key under LMK: U828B 4A09 A507 946E A339 763E 5A21 6F11
- Key check value: 386312

Card Verification Key - Key Type Code 402

- Key under LMK: U2E7D 4C69 2B18 FB72 B8C0 B630 109A 3061
- Key check value: 0B9157

Example 1: Exporting Pin Verification Key

```
Online-AUTH>ke
Enter LMK id [0-1]: 0
Enter key type: 002 (PVK)
Enter key scheme: X (Double Length)
Enter ZMK: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
Enter key under LMK: U828B 4A09 A507 946E A339 763E 5A21 6F11

Key under ZMK: XA6F6 B84D B333 FEE9 A56C 5B16 7BB2 30B6
Key check value: 386312
```

Example 2: Exporting Card Verification Key

```
Online-AUTH>ke
Enter LMK id [0-1]: 0
Enter key type: 402 (CVK)
Enter key scheme: X
Enter ZMK: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
Enter key under LMK: U2E7D 4C69 2B18 FB72 B8C0 B630 109A 3061

Key under ZMK: X95E3 7670 09FC 2C9D 0983 925C 6FC2 659F
Key check value: 0B9157
```

©2023 FIS and/or its subsidiaries. All Rights Reserved.

5.4 Importing an Encrypted key

The purpose of this command is to import a key from encryption under a ZMK to encryption under an LMK.

1) Authorise the HSM for: command.ik.console

For this example, we will Import a Pin Verification Key (type 002) and Card Verification Key (type 402)

Keys used for Example:

ZMK / Transport Key - Key Type Code 000

- Encrypted key: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
- Key check value: 19A9A8

Pin Verification Key - Key Type Code 002

- Key under ZMK: XA6F6 B84D B333 FEE9 A56C 5B16 7BB2 30B6
- Key check value: 386312

Card Verification Key - Key Type Code 402

- Key under ZMK: X95E3 7670 09FC 2C9D 0983 925C 6FC2 659F
- Key check value: 0B9157

<u>Example 1:</u> Importing Pin Verification Key

```
Online-AUTH>ik
Enter LMK id [0-1]: 0
Enter key type: 002
Enter key scheme: u
Enter ZMK: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
Enter key: XA6F6 B84D B333 FEE9 A56C 5B16 7BB2 30B6

Encrypted key: U828B 4A09 A507 946E A339 763E 5A21 6F11
Key check value: 386312
```

<u>Example 2:</u> Importing Card Verification Key

```
Online-AUTH>ik
Enter LMK id [0-1]: 0
Enter key type: 402
Enter key scheme: u
Enter ZMK: U77B5 849C 973A BC0D 64DE 15D8 462B E03C
Enter key: X95E3 7670 09FC 2C9D 0983 925C 6FC2 659F

Encrypted key: U2E7D 4C69 2B18 FB72 B8C0 B630 109A 3061
Key check value: 0B9157
```

©2023 FIS and/or its subsidiaries. All Rights Reserved.

6. References

ID	Name	Link
Ref-1	FIS Key Management Process	https://meljira01.fnfis.com:8091/display/PM/HSM+Key+Management+Processes
Ref-2	Thales Payshield Console Guide	
Ref-3	Thales Host Programmers Guide	

©2023 FIS and/or its subsidiaries. All Rights Reserved.

Appendix A - Forms

A.1 Sample Key Exchange Form

Key Custodian Key
Exchange Form.xlsx

©2023 FIS and/or its subsidiaries. All Rights Reserved.

A.2 Confirmation of dispatch of Key Email

To:	Sender Custodian 1 email address
Subject:	Dispatch of Key Component 1 of 3

To Custodian 1

Key Details:

Please note that the following secure envelope has been sent via *Courier Name*

Envelope Seal Number: *xxxxxxxxxxxxxxx*

With Waybill Number: *xxxxxxxxxxxxxxxx*

Please confirm Receipt of envelope via email

Please confirm that envelope has not been tampered with

Regards

Custodian 1
Institution
Email address

©2023 FIS and/or its subsidiaries. All Rights Reserved.

A.3 Confirmation or Receipt of Key Email

To: Receiver Custodian 1 email address

Subject: Receipt of Key Component 1 of 3

To Custodian 1

Key Details:

Please note that the following secure envelope with seal number: *xxxxxxxxx* has been received untampered.

Regards

Custodian 1
Institution
Email address

©2023 FIS and/or its subsidiaries. All Rights Reserved.