4 Encryption

4.1 Key Management with Chase/FDMS

PIN blocks passed from the [redacted] system to Chase/FDMS are encrypted within a Triple DES scheme. The keys are managed in the following manner:

- Chase/FDMS provides [redacted] with two or more double-length key parts, which – when loaded together – comprise the Key Exchange Key ('KEK'; also known as the Zone Master Key or 'ZMK' – see complete terminology description which follows).
- The ZMK key parts are entered into the Hardware Security Module, which returns the ZMK cryptogram. This cryptogram is loaded into OLS.Switch's database.
- According to Chase/FDMS's specification, the acquirer ([redacted] initiates a key exchange via a 0800 Network request with **ISO Field 70** set to **811** ('request new key'). Chase/FMDS replies via a 0810 with a copy of the new Zone PIN Key ('ZPK'; see terminology which follows) encrypted under the ZMK in **ISO Field 96** (see next section for complete breakdown of Field 96 contents).

4.1.1 Key Exchange (0800/0810)

Here is the 0800 New Key Request (as initiated by the acquirer):

Bit	Field Name	Type	Value/Mapping Notes
	Message Type	1AN	**0800**
	Primary Bit Map	64b	
1	Secondary Bit Map	64b	Required due to presence of Field 70 in request.
3	Processing Code	6BCD	Set to **900000**.
7	Transmission Date and Time	10BCD	
11	System Trace Audit Number	6BCD	
12	Local Time	6BCD	
13	Local Date	4BCD	
41	Card Acceptor Terminal ID	8AN	Proxy value for HSM is [redacted] (use same value for test and production). [Note that despite being an Alphanumeric field, FDMS specifically calls for value to right-justified and zero-filled on left.
42	Card Acceptor Merchant ID	15AN	Proxy value for HSM is [redacted] (use same value for test and production). [Note that despite being an Alphanumeric field, FDMS specifically calls for value to right-justified and zero-filled on left.
70	Network Management Info Code	3BCD	Place **811** (X '08 '11) in here to signify 'Request New Key.'

Here is the 0810 New Key Response (as formatted and transmitted by Chase/FDMS acting as the gateway):

Bit	Field Name	Type	Value/Mapping Notes
	Message Type	1AN	**0810**
	Primary Bit Map	64b	
1	Secondary Bit Map	64b	Required due to presence of Fields 70 and 96 in response.
3	Processing Code	6BCD	**900000**
7	Transmission Date and Time	10BCD	

Bit	Field Name	Type	Value/Mapping Notes
11	System Trace Audit Number	6BCD	
12	Local Time	6BCD	
13	Local Date	4BCD	
39	Response Code	2AN	
41	Card Acceptor Terminal ID	8AN	
42	Card Acceptor Merchant ID	15AN	
70	Network Management Info Code	3BCD	**811** is echoed by Chase/FDMS.
96	Key Management Data	18BCD [LLVAR]	• One byte prefix contains BCD LLVAR length identifier • First 16 bytes contain 32 Hex double-length ZPK under ZMK • Last two bytes contain four hex check digit sequence

In this scheme, OLS.Switch decides when to initiate key exchanges. To meet network audit standards and ensure synchronicity, exchanges ought to be initiated in the following circumstances:

- Upon OLS.Switch application start-up.
- Upon re-establishment of the physical or application-to-application level connection after a rupture between OLS.Switch running at [redacted] and the Chase/FDMS system.
- Upon a set schedule at least once per calendar day. With Triple DES, any rate of change above and beyond once every 24 hours invites excessive occurrences of an encryption 'race condition.' This condition refers to the small gap between when the gateway establishes its new key and when the acquirer does the same upon receiving the 0810 New Key Response. Financial transactions from acquirers that cross paths with the 0810 will fail with a key block/synchronicity error.
- Upon reaching a set number of consecutive encryption errors returned by Chase/FDMS. For example, receiving 50 consecutive errors would indicate a synchronicity issue more fundamental than a 'race condition' is afoot.

4.1.2 Performing a Key Exchange with the Hardware Security Module ('HSM')

The HSM employed by [redacted] is manufactured by RACAL (a division of Thales; hereafter, referred to as "Thales"). This section covers the message exchange between OLS.Switch and the Thales box required to execute the key exchange.

NOTE: Key terminology tends to be platform-specific. In describing the encryption actions in this section, we'll employ Thales terminology; the applicable terms are as follows:

- **Local Master Key ("LMK")**: The base level key comprised of key components generated by [redacted] The LMK is used to create cryptograms of all other keys.
- **Base Derivation Key ("BDK")**: The key used jointly by the PIN Pads and OLS.Switch to create and transport DUKPT-enabled PIN blocks.

- **Zone Master Key ("ZMK")**: The key provide (in parts) by Chase/FDMS to [redacted] for entry in a key ceremony. When online "key exchanges" take place, the newly-received values are encrypted under the ZMK.
- **Zone PIN Key ("ZPK")**: The Triple DES key used to encrypt PIN blocks in the 0200 card-based transaction requests sent to the Chase/FDMS Debit/EBT gateway. New ZPKs are delivered to [redacted] at pre-determined intervals encrypted under the ZMK.

Therefore, using strict Thales parlance, a key exchange request is a request to "translate a ZPK from ZMK to LMK encryption." This topic is covered in Section 5.2 (page 2-32) of the reference document entitled "Host Security Module RG7000 Programmer's Manual" (reference number 1270A514 Issue 5).

Upon receiving the 0810 New Key Response from Chase/FDMS on a key exchange, OLS.Switch formats a command to the Hardware Security Module ("HSM") which essentially asks it to:

- Decrypt the new 'ZPK' Working Key (which was encrypted under the Chase/FDMS-provided 'ZMK').
- Re-encrypt the working key under [redacted] Master File Key ('LMK'), creating the working key cryptogram.
- Return the ZPK working key cryptogram for storage and subsequent usage by OLS.Switch.

Based upon a teleconference with Geobridge ([redacted] Thales distributor), the FA/FB exchange should be handled as follows (refer to pp. 2-32 – 2-33 in the vendor specification):

--- FA ---

Message header	OLS can use as it sees fit. Value is echoed back in FB. Note that the length is constant and must be configured in HSM by administrator. [**Value has been set to '4' by [redacted] administrator**.]
Command code	FA
ZMK	Use the "1A + 32H" option. Geobridge recommends that the administrator configure the device as being able to handle single- or double-length keys. When that configuration is used, the commands need to signal when a double-length key follows, which is what the '1A' does. For the ZMK, the '1A' value should be set to '**U**' indicating that the ZMK cryptogram created by [redacted] is a double-length DES key encrypted using the 'Variant' (a.k.a., 'Racal') key encryption scheme.
ZPK (encrypted under ZMK)	For reasons noted above, use the "1A + 32H" option. Chase/FDMS uses the ANSI X9.17 Key Encryption Scheme, so the '1A' value here should be set to '**X**' indicating that the ZPK under ZMK provided by Chase/FDMS in the 0810 New Key Response is a double-length DES key encrypted using the 'ANSI X9.17' key encryption scheme.
Atalla Variant	If Chase/FDMS uses an Atalla (or Atalla "look-alike") HSM, then the value should be set to '**1**'. If Chase/FDMS uses a Thales device, then do not include the field. [**FDMS has confirmed they use a Thales device**, so this field is omitted.]
END	That is the END of the required message (nothing on p. 2-32 from "Delimiter" through "Message trailer" is required).

--- FB ---

Message header	Echoed back from FA usage.
Response code	FB
Error Code	Only '00' should be accepted as an exchange that "worked." [**NOTE**: Legacy system shows '01' is also a working exchange and that ZPK parity error warning is advice only. Treat as error for now; need to validate in test/certification.]
ZPK (encrypted under LMK)	Response will be received in "1A + 32H" format ('U' followed by the ZPK cryptogram)
Check value	The device will be configured to send back the '6H' version of the value
END	That is the end of the required message (remainder of list only present if they were provided in the FA command request).

4.2 Translating PIN Blocks in Debit/EBT Messages

On PIN-enabled Debit/EBT transactions sent in from a [redacted] point-of-sale location, OLS.Switch must perform a PIN translation, transforming the incoming DUKPT PIN block from the Visa Gen2 request into a outgoing Triple DES-encrypted PIN block that makes use of the newly established ZPK working key (as obtained and stored in the methods described in Sections 4.1.1 – 4.1.2).

Using strict Thales parlance, this variant of a PIN translation request is a request to "translate a PIN from *BDK encryption to interchange key encryption." This topic is covered in Section 27.2 (page 2-185) of the reference document entitled "Host Security Module RG7000 Programmer's Manual" (reference number 1270A514 Issue 5).

Based upon a teleconference with Geobridge ([redacted] Thales distributor), the CI/CJ exchange should be handled as follows (refer to p. 2-185 in the vendor specification):

--- CI ---

Message header	Value is echoed back in CJ. Note that the length is constant and must be configured in HSM by administrator. [**Value has been set to '4' by [redacted] administrator**.]
Command code	CI
***BDK**	The Base Derivation Key "in play" for this transaction. Use the "32H" option (no '1A' prefix is required here). The first six positions of the KSN (see below) represent the "key name" of the BDK injected into the PIN Pad at the transaction origination point ([redacted] currently has about 8 – 12 BDKs in use throughout its terminal population).
ZPK	The ZPK Cryptogram obtained and stored in the methods described in Sections 4.1.1 – 4.1.2. Use the "1A + 32H" option, where the '1A' value should be set to '**U**'. [**NOTE**: Even though the ZPK under ZMK received from Chase/FDMS is a double-length DES key encrypted using the 'ANSI X9.17' key encryption scheme, the result of the FA/FB exchange (as described in that section) is to obtain the ZPK under LMK, a cryptogram value that uses the 'Variant' (a.k.a., 'Racal') key encryption scheme.]
KSN Descriptor	This value is a bit esoteric and refers directly to the make-up of the KSN which follows. So to understand the descriptor, it's first necessary to talk a bit about the KSN (the next field in the CI command layout).

[redacted] has chosen a typical KSN implementation where the acquirer has chosen a 16-position scheme:

- **Positions 1 – 6:** The name of the BDK injected into this device
- **Positions 7 – 11:** The device ID
- **Positions 12 – 16:** The transaction counter

The 'rules' for a KSN construction are as follows (reading from left to right in the KSN):

1. The 'base derivation key identifier,' which is mandatory and five to nine (Hex) positions in length.
2. A 'sub-key identifier,' which Thales says is 'optional' but in practice is 'reserved for future use' (and therefore always set to zero).
3. A 'device identifier' (mandatory), which is two to five Hex digits in length.
4. A 'transaction counter' (mandatory) which essentially is the part "left over".

So, in the example here, you have a 6, 0, 5, 5 implementation.

With this information in hand, the KSN Descriptor (a three-position value) is better described as **XYZ**, where:

X = base derivation key identifier length

Y = sub-key identifier key length (will be zero)

Z = device identifier length

So, in this context, the '605' submitted in my example is better visualized. '605' says that the 16-digit KSN consists of a 6-position BDK ID, a 0-position sub-key, a 5-position device ID, **AND** (what's remaining basically) a 5-position transaction counter.

KSN

Using the layout from the descriptor, a typical KSN at [redacted] might be **091301000A8001D4** where: '091301' is the BDK name (see more information which follows); '000A8' is the device ID; and '001D4' is the transaction counter.

Here is some further information on BDK nomenclature at [redacted]

Currently, the following BDKs are 'in play' (i.e., present in the host system encryption database and injected into production PIN Pads) in [redacted] Debit/EBT environment:

```
011401   Naming model of this group is MMDDNN, where…
051601   [NN = Sequence Number of BDKs generated that day]
071101
071102
071103
091301
111601

110301   Naming model of this group is MMYYNN
120501   [This is the naming model currently in practice.]
120502

128123   Unknown naming model
```

This information is presented on an 'FYI' basis only, since – in practice – it only matters that the BDK name embedded in a particular KSN string find a match within the BDK cryptogram values loaded into OLS.Switch's encryption

	database. **If a match is not found in the encryption database**, then set the internalResultCode to APPLERR_INVBDK and end the transaction. If a match is found, then the corresponding BDK cryptogram value from the database is placed into the BDK field (as described above).
Source encrypted block	The PIN block plucked from the VG2 request (this is a 16H value; no '1A' indicator is required).
Destination PIN block format code	Set to '01' to signify ANSI format.
Account Number	Right-most 12 positions of the PAN excluding the check digit
END	That is the END of the required message.
--- CJ ---	
Message header	Echoed back from CI usage.
Response code	CJ
Error Code	Only '00' should be accepted as an exchange that "worked."
PIN length	Although this field is not used to build the 0200 message formatted for Chase/FDMS gateway, a value like '04' or '05' here are a pretty good indication that the translation occurred successfully.
Encrypted PIN	The PIN block that will be used to build the 0200 message formatted for Chase/FDMS gateway (this is a 16H value; no '1A' indicator is required).
Destination PIN block format code	Echoed back from the device as '01'.
END	That is the end of the required message (remainder of list only present if they were provided in the CI command request).

4.3 Doing HSM Health Checks

OLS.Switch also makes use of an HSM's native "diagnostic" or health check message to inquire and "keep alive" the status of the HSM connection during times of transaction inactivity. [NOTE: A typical HSM health-check setting might be "obtain diagnostics after five minutes of transaction inactivity." So – with the level of PIN-based transactions seen in production – the health check would probably never trigger. It can be useful in a test or QA environment though.]

This topic is covered in Section 21.5 (page 2-138) of the reference document entitled "Host Security Module RG7000 Programmer's Manual" (reference number 1270A514 Issue 5).

Based upon a teleconference with Geobridge ([redacted] Thales distributor), the NC/ND exchange should be handled as follows (refer to p. 2-138 in the vendor specification):

--- NC ---

Message header	OLS can use as it sees fit. Value is echoed back in ND. Note that the length is constant and must be configured in HSM by administrator. [**Value has been set to '4' by [redacted] administrator**.]
Command code	NC
END	Only the characters 'NC' are required.

--- ND ---

Message header	Echoed back from NC usage.
Response code	ND
Error Code	Only '00' should be accepted as an exchange that "worked."
LMK Check value	Format is '16H'
Firmware number	Format is '9A' ("xxxx-xxxx")