Interface specification

for securing files with

FLAM®

Hybrid method with a random key per FLAMFILE® and a static symmetric transport key (AES) protected by a hardware security module (HSM)

Version 1.00

06.05.2015

Table of content

Table of figures

Table of tables

Version history

Version	Status	Date	Editor	Changes
00.90	In Progress	04.10.2011	F. Reichbott	- Document creation (Adoption of DES Spec)
00.92	In Progress	27.10.2011	F. Reichbott	Adjustment: ENC-Zero KTV only 4 Bytes, due to ICSF!
00.93	In Progress	02.11.2011	F. Reichbott	New function code for FKEY cipher change (RENW)
00.94	In Progress	15.01.2015	F. Reichbott	Fixed order of ICV creation, Adjusted descriptions
01.00	Approved	06.05.2015	F. Reichbott T. Eckert	Review and English translation

1 Introduction

This document describes how the cryptographic protection of files for storing with an entity (archive, logs, ...) and for transmission between entities (file transfer) is supposed to work through the FLAM® Key Management EXIT (FKME). For this purpose, a hybrid technique is specified which allows to generate a random key (FKEY) per FLAMFILE® using a Hardware Security Module (HSM) and to securely exchange this file-specific key using a FLAM® master key (FMKY) from the HSM. To ensure the secure transmission of the FLAM® key, the FLAM® Key Management CONTEXT (FKMC) in the user header of every FLAMFILE® is used. Established methods of key management are used for the provision of the FMKY. The following figure illustrates the relationships.

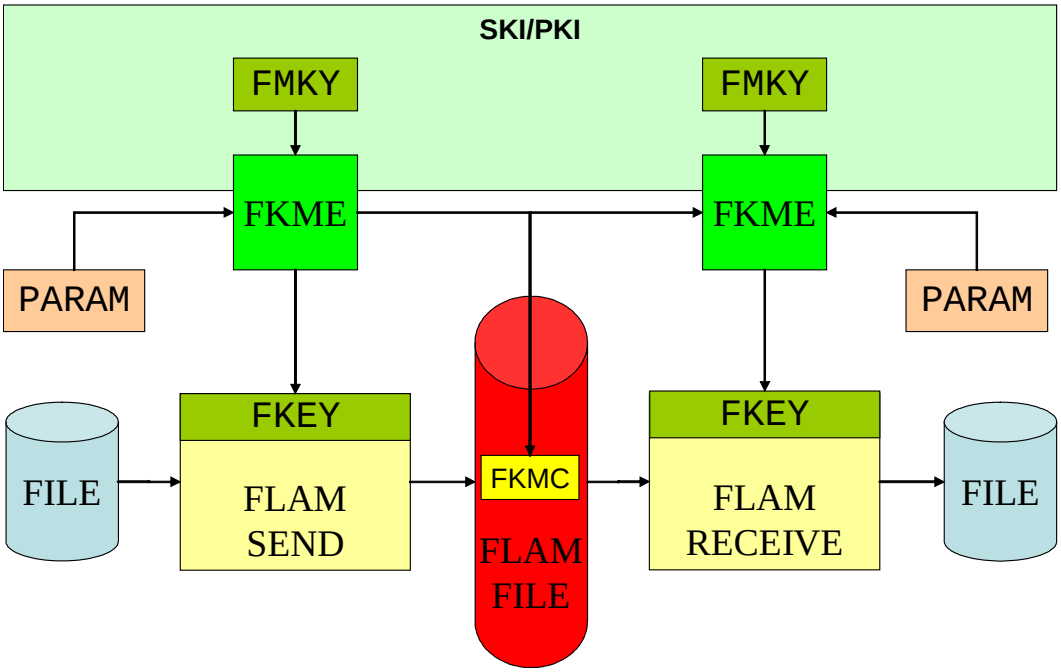

Figure 1 Overview

This specification is intended to fulfill, among other things, the requirements of the "Payment Card Industry Data Security Standard" (PCI DSS) and other requirements catalogs through FLAM®. In this respect, secure storage and archiving of files, the exchange of these files between parties as well as securing logs, dumps, database backups and other files that occur in the transaction processing plays a role. There are also other applications where confidentiality and integrity of files must be ensured.

2 System model

FLAM® with AES (as of version 4.0) realizes integrity protection and confidentiality through a 64-byte passphrase that is used for the derivation of four 128-bit AES keys on each of the three logical layers of a FLAMFILE® using a one-way hash function. They are used for the encryption of the user data (segment) and the calculation of Message Authentication Codes (MACs) for the respective components on each level (segment, member, file) of the FLAMFILE®.

In order to use the cleartext FLAM® key (FKEY) securely within a HSM-based cryptographic infrastructure, two requirements must be met:

1. The cleartext FKEY may exist in system memory (RAM) only for a brief period of time.

2. The FKEY may be used only for one single FLAMFILE® so that extracting its value from system memory by an attacker does not affect another FLAMFILE®.

In consequence, the FKEY only exists where the file's cleartext data also exists which is all that an attacker can get by obtaining the respective FKEY. Especially, he would not get access to other FLAMFILEs®. The provision of the FKEY occurs through the FLAM® Key Management EXIT (FKME), which is supported **since version 4.1 of FLAM®** for the integration of various cryptographic infrastructures.

The FKEY must consist of 64 bytes of randomness which must be generated by the respective HSM (or soft token). After that, the HSM (or soft token) provides a structure protected by the hardware (FLAM Key Management CONTEXT (FKMC)) for the user header of the FLAMFILE®. This allows the respective personalized HSM (or soft token) to restore the FKEY in its cleartext form for reading.

To protect the FKMC, a static, symmetrical master key is used for FLAM® (FMKY), which is used by the sender to encrypt the FKEY and used by the receiver to decrypt it. In order to not risk the HSMs security, the cleartext FKEY looks like 64 bytes of normal data from the HSM's point of view.

For the different use cases (ENCIPHER and DECIPHER), directed key relationships can be created through established Static Key Management Systems (SKMS) which conform to all requirements of PCI DSS. These allow to prove the origin of a FLAMFILE® distinctively. Intermediaries, "Kopfstellen" (central payment gateways) and other ownership transitions can be conducted safely through rekeying of the data (IDATXLAT and ODATXLAT). For this, only the FKEY needs to be rekeyed by the HSM and the user header of the FLAMFILE® must be exchanged. The actual data remains encrypted during this process at all times. The FKEY remains protected by the HSM throughout. This process for secure rekeying of a FLAMFILE® makes sure that the data needs to exist in cleartext only on its creation and extraction. This circumstance is illustrated in the following example of a generating office (GS) for card production and a personalization system of the card producer:

- Secure storage of the generated data within the generating office
  `FLAM(COMP, FMKY.GS2GS.ENCIPHER.ggvv)`

- Transfer of the card data to the producer
  `FLAM(CHNG, FMKY.GS2GS.IDATXLAT.ggvv, FMKY.GS2PS.ODATXLAT.ggvv)`

- Reception and secure storage at the producer
  `FLAM(CHNG, FMKY.GS2PS.IDATXLAT.ggvv, FMKY.PS2PS.ODATXLAT.ggvv)`

- Decryption of the stored data for production
  `FLAM(DECO, FMKY.PS2PS.DECIPHER.ggvv)`

Furthermore, rekeying allows to transition from one generation and version to another of the same or a different FMKY. It is also possible to migrate between different cipher suites if this migration path is supported by the EXIT. For the latter, there is a separate function code (RENW) to separate the rekeying (change of access permissions) from the migration of the cipher.

The generation and exchange of the FMKY between entities should be carried out according to the established procedures for static key management (at least two-tiered (2 or 3 clear key components + FMKY as cryptogram)). This is not part of this interface specification. The requirements applying to static key management in the respective environment (VISA, ZKA, BSI, …) must be met. This document assumes that the static FMKY is available through the HSM. The keys, like any static key, should be replaced frequently and should be replaceable ad-hoc. Therefore, for every key, there is a generation (GG) and a version (VV).

3 Specification FLAM Key Management CONTEXT (FKMC)

3.1 Input requirements of FLAM®

The context field (FKMC) must not exceed 512 bytes on all platforms and must have a constant length for the successful rekeying of FLAMFILES®. There are no requirements regarding the contents, except that the first 50 bytes are logged as information and the last 4 bytes must contain a test value for the FKEY which may not depend on the respective encryption.

Note: If more than 512 bytes are needed, a new version of FLAM with larger buffers is required.

3.2 The data structure in version 002

The following table is an overview of the data structure. Used abbreviations and their meaning:

Lg = Length in bytes

CHR = Character in the character set of the creating machine
POV = BCD-encoded, right-aligned and padded with 0
BIN = Binary

Field	Description	Content	Lg	Format
1	Info data	`FKMC V002 L144 AES3 KL32 EZ04 ICBC SHA2`	50	CHR
2	Generation and version of the FMKY	`GGVV`	2	BIN
3	KTV for the FMKY	`RRRRRRRR`	4	BIN
4*	Creation time (GMT) of the FLAMFILE®	`YYYYMMDDHHMMSSss`	8	POV
5*	Random number for dynamization (if needed: prevention of replay attacks)	`RRRRRRRRRRRRRRR`	8	BIN
6**	Encrypted FKEY	`RRR…RRR`	64	BIN
7*	HASH of 4, 5 and the cleartext FKEY	`RRRRRRRRRRRRRRR`	8	BIN

Table 1 FLAM® Key Management CONTEXT (FKMC)

*) The fields are set at creation time of the FLAMFILE(*) and not changed later.

**) The cleartext FKEY is also generated at creation time and remains the same. Only its ciphered version changes depending on the FMKY.

3.2.1 Explanation of the data fields

3.2.1.1 Field 1: Info data

The info data is contained within the first 50 bytes of the context field, providing information about the EXIT itself. The following mandatory details must be provided in uppercase and separated by whitespace characters.

1. **Identifier for the FKMC** = FKMC
   4 bytes long constant for checking and detecting the character set (EBCDIC or ASCII).

2. **Version of the EXIT** = V002
   The version of the EXIT is defined as the constant V002. This information is used to differentiate between other implementations.

3. **Length of the EXIT** = L144
   The length of the context field of this EXIT is 144 bytes. The length may vary depending the version and is used for plausibility checking.

4. **Algorithm for the FMKY** = AES3
   This field defines the algorithm used to encrypt the FKEY using the FMKY. In version 002 this should usually be a 256 bit key. When using a HSM, it may occur that the application using it (the FKME itself) does not know the length of the master key. In this case, AES3 should be used.

   a. 256 Bit = AES3

   b. 196 Bit = AES2

   c. 128 Bit = AES1

5. **Key length of the FMKY** = KL32
   The length of the FMKY is defined by one of the keywords below. Using 256 bit keys is recommended.

   a. 256 Bit = KL32

   b. 196 Bit = KL24

   c. 128 Bit = KL16

6. **Verification algorithm for the FMKY** = EZ04
   Defines the algorithm used for calculation of the Key-Test-Values (KTV) for the

FMKY, which is realized by the method Enc-Zeros. Only the four high-order bytes are stored, however, which matches the VISA Key-Test-Procedure.

7. **Cipher mode for the FKEY** = ICBC
   The seventh field specifies the mode of encryption of the FKEY. ICBC stands for Cipher-Block-Chaining (CBC) with an initialization vector.

8. **One-way hash algorithm** = SHA2
   The algorithm used to hash the timestamp, random number and the cleartext FLAM® key is SHA-256.

9. **Further information**
   Further application-specific information (e.g. the implementation of the EXIT (IBMCCA, IBMDKMS, PKCS11, ATALLA, THALES, …)) may be defined. If no information is present, the remaining 10 bytes are padded with whitespace.

To verify the implementation of the EXIT against the info data, in version 002, the first 40 bytes are compared with the following constant (note the whitespace at the end):

„FKMC V002 L144 AES3 KL32 EZ04 ICBC SHA2 “

It is important that the character set used for the comparison must not play a role. The determination of the character set should be performed on the first byte of info data, which must be ‚C6’hex in EBCDIC and ‚46’hex in ASCII for a capital ‚F’. Since the first 50 bytes of FLAM are logged as comment of the FLAMFILE, the system-specific character set must be used when writing. When reading, FLAM recognizes the character set (ASCII or EBCDIC) for logging.

3.2.1.2 Field 2: Generation and version of the FMKY

This field is set to the generation (gg) and version (vv) of the FMKY when sending. It is used to select the correct FLAM master key (FMKY) when receiving the FLAMFILE®. Determination of generation and version when sending and their usage when receiving depends on the implementation of the EXIT. In general, a fully-qualified label for the key and the matching generation and version should be passed to the EXIT when sending. When receiving, it is then sufficient if the label contains placeholders for generation and version.

3.2.1.3 Field 3: KTV for the FMKY

The Key-Test-Value (KTV) for the FMKY is the result of encrypting 16 bytes of zeros with AES using the FMKY. However, only the 4 high-order (leftmost) bytes are stored. This algorithm was chosen because it is supported by most HSMs, matches the security requirements, can also be generated by the sender by encrypting 16 data bytes and can be implemented using AES as base algorithm.

3.2.1.4 Field 4: Creation time of the FLAMFILE®

Based on the requirements, the point in time of creation of the FLAMFILE® must be recorded cryptographically secure. This happens by including it in the HASH calculation and the generation of the IV for CBC mode encryption. As indicated in the table above, the format consists of:

- YYYY - Year
- MM - Month
- DD - Day
- HH - Hour
- MM - Minute
- SS - Second
- ss - Millisecond

It is desirable to use a reliable time source for these 8 bytes. The time zone is Greenwich Mean Time (GMT) in order to allow international conversions.

3.2.1.5 Field 5: Random number for dynamization

The 8 bytes long random number serves as attribute for dynamization of a FLAMFILE® and is used for HASH calculation and IV generation.

3.2.1.6 Field 6: Encrypted FKEY

In version 002, the 64 bytes long random FKEY (4 blocks) is AES-encrypted in CBC mode using the FMKY. The IV is the result of concatenating fields 5 and 4. (Attention: the order differs from the hash calculation. The ICV must be constructed explicitly, i.e. one cannot simply use the address of field 4 with field 5 following.) The result is a ciphertext for the FKEY of 64 bytes which is put into the context structure in binary form by the EXIT.

3.2.1.7 Field 7: Hash of field 4, field 5 and the clear FKEY

Calculation of the hash value occurs by using the SHA-256 algorithm on the following 80 bytes:

- 8 bytes of field 4: Creation time of the FLAMFILE®
- 8 bytes of field 5: Random number for dynamization
- 64 bytes random FKEY in cleartext

Only the 8 high-order (leftmost) bytes of the hash value are stored in the context structure. It is calculated when the key is generated. The verification should only happen when the key is used. In other words, verification is only done when the cleartext key is necessary. This is not the case when a FLAMFILE® is rekeyed.

4 Specification FLAM® Key Management EXIT (FKME)

The FLAM® Key Management EXIT (FKME) is a function that is called by FLAM® when corresponding parameters (PARAM) for an EXIT are passed to FLAM®. It allows the inclusion of an arbitrary cryptographic infrastructure to enable implementing session key procedures with FLAM®.

4.1 The function interface

The following table provides an abstract overview of the parameters of the interface. Used abbreviations:

INT = 32 Bit (4 Byte) in two's complement
STR = Array of bytes

Para	Name	Comment	Direction	Type	Length
1	Fuco	Function code	INPUT	INT	4 bytes
2	RetCo	Return code	OUTPUT	INT	4 bytes
3	ParLen	Length of input parameters	INPUT	INT	4 bytes
4	Param	Input parameters	INPUT	STR	variable
5	DatLen	Length of the data (FKMC)	COMP:INPUT/OUTPUT DECO:INPUT CHNG:INPUT=OUTPUT RENW:INPUT	INT	4 bytes
6	Data	Data (FKMC)	COMP:OUTPUT DECO:INPUT CHNG:INPUT/OUTPUT RENW:INPUT	STR	variable
7	KeyLen	COMP/DECO: Length of the key (FKEY) RENEW: Length of the new context field (FKMC)	COMP:INPUT/OUTPUT DECO:INPUT/OUTPUT CHNG: not used RENW:INPUT/OUTPUT	INT	4 bytes
8	Key	COMP/DECO: Key (FKEY) RENEW: New context field (FKMC)	COMP:OUTPUT DECO:OUTPUT CHNG: not used RENW:OUTPUT	STR	variable
9	MsgLen	Length of the message	INPUT/OUTPUT	INT	4 bytes

Para	Name	Comment	Direction	Type	Length
10	Message	Message	OUTPUT	STR	variable

Table 2 FLAM® Key Management EXIT (FKME)

All parameters are passed as pointers (Call by Reference). FLAM® loads the FKME dynamically at runtime as module with a single function. The name of the module and (if applicable) the name of the function can be passed to FLAM® as parameters. The input lengths always specify the length of the data passed in the next parameter. The output lengths will be set to the length of the required memory after function execution.

4.1.1 Explanation of the parameters

4.1.1.1 Para 1: Function code

The function code is used to select the method for the EXIT. The following methods are defined:

- **0 – Decompression/Decryption**
  The input parameters and the context field (FKMC) from the user header are passed to the EXIT which returns the cleartext key (FKEY) to FLAM.

- **1 – Compression/Encryption**
  The input parameters are passed to the EXIT which then randomly generates the 64 bytes FKEY and returns it together with the context field (FKMC). FLAM stores the context field inside the user header and uses the generated key for creating the FLAMFILE®.

- **2 – Change/Rekeying**
  The input parameters and the context field (FKMC) from the user header are passed to the EXIT which calculates and returns the new context field (FKMC) to the program. The program then creates a new FLAMFILE® with a modified user header. The memory block must be large enough to be able to hold the newly generated context field.

- **3 – Renew/FKEY cipher change**
  Through this function code, a cipher change for the FKEY (change of the encryption Algorithm used to encrypt FLAM® key) can be performed if it is supported by the respective EXIT.

- **0xFFFFFFFF – Information**
  Prompts the EXIT to output information about itself into the message field.

4.1.1.2 Para 2: Return code

The return code is used for program control of FLAM. If the return code equals 0 after the call to the EXIT, the call was successful, and FLAM continues execution as expected. If it equals 4, the amount of memory provided to the EXIT was insufficient. This leads to another call with sufficient memory for platforms with dynamic memory management. On other platforms, this error, like all other error codes larger than 0, result in an abort of FLAM. The reason for such an abort can be communicated to the outside by the EXIT only through the message field. It is always output when the length of the message is not equal to 0. This allows the EXIT to communicate warnings even if the return code is 0. If everything was ok, this fact, the function (COMP, CHNG, DECO, RENW), the timestamp and the random number are logged through the message field.

4.1.1.3 Para 3: Length of input parameters

The length of the input parameters depends on the method and the implementation of the EXIT. It is determined by FLAM® when called and passed to the EXIT.

4.1.1.4 Para 4: Input parameters in version 002

The input parameters depend on the method and the implementation of the EXIT. Basically, they should include the following information depending on the method:

- **Encryption**
    - If necessary, the method if several are supported
    - If necessary, identification data and authentication data for the HSM
    - Referencing data for the FLAM-Master-Key (FMKY)
        - Key label, generation and version *or*
        - Key label and key label template
- **Decryption**
    - If necessary, identification data and authentication data for the HSM
    - Referencing data for the FLAM-Master-Key (FMKY)
        - Key label template
- **Rekeying**
    - If necessary, identification data and authentication data for the HSM

  - Referencing data for the FLAM-Master-Key (FMKY) incoming
    - Key label template
  - Referencing data for the FLAM-Master-Key (FMKY) outgoing
    - Key label, generation and version *or*
    - Key label and key label template

- **FKEY cipher change**
  - A new version of the output FKMC to transition from an old cipher (TDES) to a newer cipher (AES3)
  - If necessary, identification data and authentication data for the HSM
  - Referencing data for the FLAM-Master-Key (FMKY) incoming
    - Key label template
  - Referencing data for the FLAM-Master-Key (FMKY) outgoing
    - Key label, generation and version *or*
    - Key label and key label template

When calling FLAM, the maximum buffer size for input parameters currently is 256 bytes.

4.1.1.5 Para 5: Length of context data (FKMC) in version 002

The length of the context data (FKMC) is 144 bytes. The size of the buffer is lower than the 512 bytes that are provided by FLAM. Hence, there should always be enough memory available for the context field. On the output side, the EXIT must set this parameter to 144 and the field must be checked to be equal to 144 if a context field is passed by FLAM® (decryption or rekeying).

4.1.1.6 Para 6: Context data (FKMC) in version 002

The context field (FKMC) is provided or accepted by the EXIT through this field. Its specification can be found in section 3.2.

4.1.1.7 Para 7: Key (FKEY) length in version 002

If returned by the EXIT (encryption or decryption), the length of the random cleartext key is always 64 bytes, which are provided by FLAM® on the input side.

On RENW, this parameter is used to specify the available length for the new context structure. The EXIT returns the right length.

4.1.1.8 Para 8: Key (FKEY) in version 002

The EXIT provides the 64 bytes long key (random number) to FLAM® for encryption and decryption through this parameter.

On RENW, the parameter is used to return the new context structure.

4.1.1.9 Para 9: Message length

FLAM® provides a message buffer of size 128 bytes. It can be used by the EXIT to let FLAM® log error messages or other information.

4.1.1.10 Para 10: Message

Contains the message which is output if the length does not equal 0. If the function code is ‚FFFFFFFFFF'hex, the EXIT returns its info data through this parameter.

4.2 Proceedings in version 002

4.2.1 Encryption of a FLAMFILE®

FLAM® calls the EXIT with the following parameters and the EXIT returns the following values upon success:

Para	Input values	Output values
Fuco	1	=
RetCo	0	0
ParLen	>0	=
Param	Parameter for the EXIT	=
DatLen	512	144
Data	undefined	FKMC as per 3.2
KeyLen	64	64
Key	undefined	64 bytes of random data
MsgLen	128	Length of the OK message
Message	undefined	OK message

Table 3 Parameters for encryption

Below, the encryption procedure (Fuco=1) is set out in bullet points.

- Check of buffer lengths
- Determination of identification and authentication data for the HSM from the parameter field

- Determination of the label, generation and version for the key from the parameter field
- Initialization of the context structure with the information data
- Setting the generation and version in the context field
- Calculation of the KTV for the FMKY based on the label and entering it into the context field
- Determination of the timestamp and setting it in the context field
- Generation of the random number and setting it in the context field
- Construction of the IV from timestamp and random number
- Generation of the 64 bytes long key as return value to FLAM®
- Calculation of the SHA-256 over the timestamp, the random number and the cleartext key and setting it in the context field
- CBC encryption of the key using the IV and the FMKY, putting the result into the context field
- Setting the buffer lengths, ok message and the return code
- Return from the EXIT

4.2.2 Rekeying of a FLAMFILE®

The program calls the EXIT with the following parameters. On successful execution, the EXIT returns the following values:

Para	**Input values**	**Output values**
Fuco	2	=
RetCo	0	0
ParLen	>0	=
Param	Parameter for the EXIT	=
DatLen	144	144
Data	FKMC as per 3.2	FKMC as per 3.2
KeyLen	undefined	=
Key	undefined	=
MsgLen	128	Length of the OK message
Message	undefined	OK message

Table 4 Parameters for rekeying

Below, the rekeying procedure (Fuco=2) is set out in bullet points.

- Check of buffer lengths
- Determination of identification and authentication data for the HSM from the parameter field
- Determination of the input template for the input key from the parameter field
- Determination of the output label, output generation and output version for the output key from the parameter field
- Determination of the input version and input generation from the context field
- Determination of the fully qualified input label from template, generation and version
- Verification of the KTV through the input label
- Setting the output generation and version in the context field
- Calculation of the KTV for the output FMKY based on output label and setting it the context field
- Construction of the IV from timestamp and random number
- Rekeying of the 64 bytes long key from the input FMKY to the output FMKY using the IV; replacement of the ciphered key in the context field
- Setting the buffer lengths, ok message and the return code
- Return from the EXIT

Decryption of a FLAMFILE®

FLAM® calls the EXIT with the following parameters. On successful execution, the EXIT returns the following values:

Para	Input values	Output values
Fuco	0	=
RetCo	0	0
ParLen	>0	=
Param	Parameters for the EXIT	=
DatLen	144	=
Data	FKMC as per 3.2	=
KeyLen	64	64
Key	undefined	64 bytes decrypted random data from FKMC
MsgLen	128	Length of the OK message
Message	undefined	OK message

Table 5 Parameters for decryption

Below, the decryption procedure (Fuco=0) is set out in bullet points.

- Check of buffer lengths
- Determination of identification and authentication data for the HSM from the parameter field
- Determination of the input template for the static key from the parameter field
- Determination of the version and generation from the context field
- Determination of the fully qualified label from template, generation and version
- Verification of the KTV through the label
- Construction of the IV from timestamp and random number
- CBC decryption of the 64 bytes long key using the IV and the FMKY, returning the result to FLAM® through the key parameter
- Calculation of the SHA-256 over the timestamp, the random number and the cleartext key and comparison with the value from the context field
- Setting the buffer lengths, ok message and the return code
- Return from the EXIT

4.2.3 FKEY cipher change for a FLAMFILE®

FLAM® calls the EXIT with the following parameters. On successful execution, the EXIT returns the following values:

Para	Input values	Output values
Fuco	3	=
RetCo	0	0
ParLen	>0	=
Param	Parameter for the EXIT	=
DatLen	144	=
Data	FKMC as per 3.2	=
KeyLen	512	???
Key	undefined	New FKMC
MsgLen	128	Length of the OK message
Message	undefined	OK message

Table 6 Parameters for decryption

At this point, the process is not explicitly described, since the novel FKMC and thus the associated new methods are not fixed. If an exit supports the RENW, then it must implement a separate function for each cipher transition, which is to be marked for the EXIT by the first parameter.

5 Appendix

5.1 FLAM implementation recommendations

The following subsections provide some recommendations for the implementation of EXITs which should be followed, as far as the utilized HSM architecture permits.

5.1.1 Handling of generation and version

When sending, the generation and version is determined from the key label by applying a template. For the template, the following wildcard characters are defined:

- Generation ,++'
- Version ,**'

All other characters must match with the corresponding label. Alternatively, they can be replaced by ,%' so that the position of generation and version in the label can be determined by the EXIT.

Example: ,TFMKY.%%%%%%%%.%%%%%%%%.DAT0++**' when sending

The template for receiving must not contain a ‚%' in order to enable completion of the name for the key.

Example: ,TFMKY.BV000000.GUD00000.DAT0++**' when receiving

When creating a FLAMFILE®, a complete label and a template for the EXIT is always passed to FLAM®. If a FLAMFILE® needs to be accessed later on, only a template is passed where only the generation and the version remain variable.

5.1.2 Passing the input parameters to the EXIT via FLAM / FLAMUP

The input parameters for the EXIT are passed as a parameter in the parameter list for FLAM® or FLAMUP. The parameters must be combined into a string. If it contains rounded brackets or single quotation marks, those must be escaped by doubling them. The necessary key label (if applicable) followed by the key templates should be supplied first. Then the optional identification data and authentication data may follow. All values a separated by a dot. Below, you can find one example for every use case without authentication information for the HSM:

- **Encryption**
  TFMKY.BV000000.GUD00000.DAT00601
  TFMKY.%%%%%%%%.%%%%%%%%.DAT0++**
- **Rekeying**
  TFMKY.BV000000.GUD00000.DAT0++**

```
TFMKY.GUD00000.GUD00000.DAT00601
TFMKY.%%%%%%%%.%%%%%%%%.DAT0++**
```

- **Decryption**
  ```
  TFMKY.GUD00000.GUD00000.DAT0++**
  ```

- **FKEY cipher change**
  ```
  TDESAES3
  TFMKY.GUD00000.GUD00000.DAT0++**
  TFMKY.GUD00AES.GUD00AES.DAT00901
  TFMKY.%%%%%%%%.%%%%%%%%.DAT0++**
  ```

5.1.3 The last 10 bytes of the info field of the FKMC

The first 40 bytes of the 50 bytes of the info field are specified in 3.2. The remaining 10 bytes are freely available to the EXIT. It is recommended that the EXIT stores an identifier for its implementation. The following identifiers are defined:

- LIMESSWM02
  Standard software implementation by Limes Datentechnik
  „FKMC V002 L144 AES3 KL32 EZ04 ICBC SHA2 LIMESSWM02“

- IBMCCCAxx
  IBM implementation against the SAPI of the CCA
  „FKMC V002 L144 AES3 KL32 EZ04 ICBC SHA2 IBMCCCA02 “

- IBMDKMSxx
  IBM implementation against the DKMS General Purpose API
  „FKMC V002 L144 AES3 KL16 EZ04 ICBC SHA2 IBMDKMS02 “

- GUDPKCSxx
  PKCS11 implementation of G+D
  „FKMC V002 L144 AES3 KL16 EZ04 ICBC SHA2 GUDPKCS02 “

- BVUTIMAxx
  UTIMACO implementation of the Bankverlag
  „FKMC V002 L144 AES3 KL16 EZ04 ICBC SHA2 BVUTIMA02 “

xx – A placeholder for the version of the implementation; should be 02, like in the examples.

The Limes Datentechnik reserves the following identifiers for its implementations:

- LIMESSWMxx - Standard software implementation
- LIMESCCAxx - Implementation for IBM47xx or ICSF
- LIMESP11xx - Implementation for PKCS#11

5.1.4 EBCDIC and ASCII conversion

Only the info field depends on character set. When creating a FLAMFILE®, the info field is filled depending on the platform of the sender. Hence, the recipient has to check which character set the info data is stored in and need to convert it, if necessary.

5.1.5 Result messages

5.1.5.1 Error messages of the Exit

The following messages should be consulted when the corresponding error occurs.

- FKME – The function code is not supported + additional error info
- FKME – The input parameter length is not correct + additional error info
- FMKE – The input parameter is not formatted correctly + additional error info
- FKME – The length of the data field is too short + additional error info
- FKME – The length of the data field is not correct + additional error info
- FKME – The data field is not formatted correctly + additional error info
- FKME – The length of the key field is too short + additional error info
- FKME – The length of the key field is not correct + additional error info
- FKME – The key field is not formatted correctly + additional error info
- FKME – The authentication failed + additional error info
- FKME – The cipher suite is not supported (The FKMC info field is not correct) + additional error info
- FKME – The determination of generation and version failed + additional error info
- FKME – The generation and version is not formatted correctly + additional error info
- FKME – The determination of the label for the FMKY failed + additional error info
- FKME – FMKY not found + additional error info
- FKME – The calculation of the key test pattern for FMKY failed + additional error info
- FKME – The verification of the key test pattern for FMKY failed + additional error info
- FKME – The determination of the time stamp failed + additional error info

- FKME – The verification of the time stamp failed + additional error info
- FKME – The generation of the random numbers failed + additional error info
- FKME – The calculation of the hash value (FKEY) failed + additional error info
- FKME – The verification of the hash value (FKEY) failed + additional error info
- FKME – The encryption of FKEY failed + additional error info
- FKME – The decryption of FKEY failed + additional error info
- FKME – The translate of FKEY failed + additional error info

All other message must start with ‘FKME - ‘ and may consist of other messages in English followed by corresponding error information from the respective subsystems or EXITs.

5.1.5.2 OK messages from the Exit

If execution of a function code does not result in an error, a so called OK message is generated for the purpose of logging. It consists of the function code, the timestamp and the random number.

„FKME – COMP successful + TSP(YYYYMMDDHHMMSSss) RND(RRRRRRRRRRRRRRR)“

„FKME – CHNG successful + TSP(YYYYMMDDHHMMSSss) RND(RRRRRRRRRRRRRRR)“

„FKME – DECO successful + TSP(YYYYMMDDHHMMSSss) RND(RRRRRRRRRRRRRRR)“

„FKME – RENW successful + TSP(YYYYMMDDHHMMSSss) RND(RRRRRRRRRRRRRRR)“

By logging timestamp and random number, monitoring and inspection are possible. Additionally, the standards set by VISA and MasterCard are met.

5.1.5.3 Information about the Exit itself

The first 50 bytes should match the info field of the FKMC, followed by other useful information about the respective implementation of the EXIT.

„FKME - FKMC V002 L144 AES3 KL32 EZ04 ICBC SHA2 LIMESSWM02 + additional info“

FKME – Default implementation with a fixed key (FLAMFIX02)

For a separate transmission of FKMC and FLAMFILE® (new feature in FLAM® version 4.?), a special case for this EXIT is specified. The EXIT contains a hard-coded value for the FMKY that is equal for every FLAM® installation. This enables every installation to read a FLAMFILE® that has been created using this EXIT, even though it is technically encrypted.

Due to the fact that the FMKY is not a secret, it is merely an obfuscation. If, however, the FKMC is transmitted separately from the FLAMFILE® via a second secure channel (e.g. TLS), the large FLAMFILE® can be transmitted through an unsecure channel like FTP, resulting in an organizational transmission protection. For this special implementation, the following definitions are made:

- Key value of the FMKY: fixed, not published
- Generation: 00
- Version: 00
- KTV: consequently also fixed
- Length of input parameters: 0
- Input parameters: none

This kind of EXIT is meant to be used in special use cases where there is a secure channel for small amounts of data and an insecure channel for large amounts of data. For this purpose, there will be functions for SPLIT and MERGE. The SPLIT function reads a complete FLAMFILE® containing an FKMC, creates a new FLAMFILE® without an FKMC and writes the FKMC to a separate file. The MERGE function takes both files and reassembles the complete FLAMFILE® with FKMC. In the incomplete FLAMFILE®, the last 4 bytes of the FKMC remain in the user header in order to avoid that an FKMC and a FLAMFILE® can be merged that don't fit together.

6 List of abbreviations

AES = Advanced Encryption Standard

BIN = Binary

CBC = Cipher Block Chaining

CHNG = Change

CHR = Character

COMP = Compression

DAT = Data

DECO = Decompression

DED = Decryption Encryption Decryption

DES = Data Encryption Standard

EDE = Encryption Decryption Encryption

EZ = Encrypted Zeros

FKEY = FLAM® Key

FKMC = FLAM® Key Management CONTEXT

FKME = FLAM® Key Management EXIT

FLAM® = Frankenstein Limes Access Method

FMKY = FLAM® Master Key

FUCO = Function code

GG = Generation

GS = Generating Entity

HSM = Hardware Security Module

ICBC = CBC with IV

INT = Integer

IV = Initialization Vector

KL = Key Length

KTV = Key Test Value

LG = Length

MAC = Message Authentication Code

MDC = Message Digest Cipher

MSG = Message

PAR = Parameter

PARAM = Parameter

PCI DSS = Payment Card Industry Data Security Standard

PIN = Personal Identification number

POV = BCD Encoding

PS = Personalization System

RAM = Random Access Memory

RETCO = Return code

SKMS = Static Key Management System

STR = String

TDES = Triple DES

VV = Version

ZKA = Zentraler Kredit Ausschuss (Central Credit Committee)