THE Berlin GROUP

A EUROPEAN INITIATIVE
WORKING FOR CARD PAYMENTS IN EUROPE

Bilateral and Multilateral Processing of Card Transactions in Europe

Security Features

Version 3.1

Date: 05/09/2012

Content

1 Introduction

The Berlin Group standard is a standard for the European area for bilateral/multilateral processing of card transactions.

The Berlin Group standard considers for this processing an exchange of authorisation and clearing data between gateways, where the role of an acquirer gateway and the role of an issuer gateway are distinguished. The acquirer gateway receives messages from acquirers that process card based transactions originating from ATMs, POS terminals, MoTo or the internet. The acquirer gateway communicates with the issuer gateway to receive online authorisation from the card issuer and to clear the transactions afterwards between the gateways. The ISO 8583 messages exchanged between acquirer gateway and issuer gateway for authorisation and clearing are specified in [BG A] and [BG CSI].

An overview on this infrastructure is given in the following diagram.

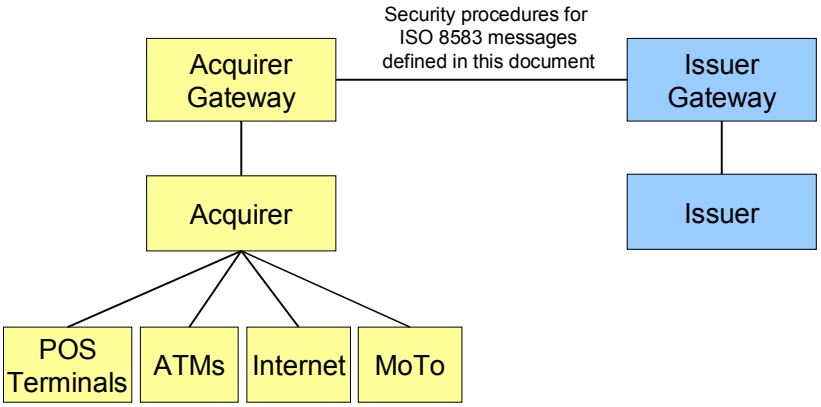

Figure 1: Infrastructure for bilateral and multilateral processing of card transactions in Europe

The focus of this document is solely on the specification of security procedures between the gateways mentioned above. This includes a definition of the BMP 53 of the respective transaction messages and necessary key management procedures.

2 Basic cryptographic mechanisms

Former versions of the Berlin Group specifications use Triple-DES (with double length keys, as specified in clause 4.2 of ISO 11568-2) as a basic cryptographic algorithm for all transactions (encryption and MAC-calculation). With version 3.1 Advanced Encryption Standard AES is introduced. The algorithm identifier in BMP 53 is used as an indicator (cf. chapter 4). Since the length of the PIN block in BMP 52 will exceed 8 bytes if AES is used for encryption, there will be a second indicator in BMP 3 (cf. chapter 4, note 7).

2.1 Padding

Padding will be performed by using the technique described as method 2 in chapter 5.1 of [ISO 9797-1]. For this chapter 2.1 the following applies:

- n = 64 in case of Triple DES
- n = 128 in case if AES

Method 2 of [ISO 9797-1] works as follows:

The data for which the MAC is to be calculated shall be appended with a single “1” bit. The resulting data shall then be appended with as few (possibly none) “0” bits as necessary to obtain a data string whose length (in bits) is an integer multiple of n.

The resulting data is divided into n-bit blocks. The bits which are padded to the original data, according to the above padding method, are only used for calculating and verifying the MAC. Consequently, the padding bits (if any) shall not be transmitted with the data. The verifier knows the padding bits have not been transmitted, and which padding method is in use.

2.2 Encryption

If the encryption algorithm is double length key Triple DES, then encryption will be performed according to [ISO 11568-2] in the encrypt-decrypt-encrypt mode. The key will be denoted as (K_L,K_R). K_L and K_R are of 8 byte length each.

The usage of the encryption algorithm AES is according to [FIPS 197]. The block length is therefore 16 bytes (128 bits) and supported key lengths are 128 bits, 192 bits and 256 bits. Keys are denoted as K.

2.3 HASH-Function

As hash-functions the algorithms SHA-256 or SHA-512 are used as specified in [SHA-512]. This function generates a value of fixed length h (256 / 512 bit or 32 / 64 bytes) over every input message M up to the length of 2^{64}-1 bits. It will be written as:

h := SHA-256 (M) or

h := SHA-512 (M)

2.4 MAC calculation

2.4.1 Authorisation Messages

The MAC is computed over the complete message without the MAC field; from and including the MTID through and including the last data element present in the message without the MAC field.

2.4.1.1 Triple-DES based

The MAC calculation is performed according to MAC algorithm 3 of [ISO9797-1].

2.4.1.2 AES based

The MAC calculation is performed according to chapter 6.2 in [NIST SP 38B]. The length of the MAC will be 8 bytes, the most significant bytes of the final encryption (see step 6 in chapter 6.2 of [NIST SP 38B], commonly referred to as 'CMAC').

2.4.2 Clearing Messages

A clearing file is structured as following:

- One ISO message header (first message)
- At least one ISO message presentment, charge back, reversal, rejection, fee collection, retrieval, or reconciliation acknowledgement
- One ISO message reconciliation (second last message) (is not present, if retrieval requests or reconciliation acknowledgements are the only transaction messages in the file)
- One ISO message trailer (last message)

During transmission clearing files are protected by a MAC located in BMP 128 in the ISO message trailer. The MAC is computed over a hash value h. h is the result of applying the hash-function over the complete clearing file excluding the ISO message trailer; from and including the MTID of the ISO message header through and including the last data element present in the ISO message preceding the trailer message. Padding is not necessary if SHA-256 or SHA-512 are used as the hash length is then a multiple of 16 bytes.

2.4.2.1 Triple-DES and SHA 256

The MAC calculation is performed according to MAC algorithm 3 of [ISO9797-1] which works as follows:

Assume a double length Triple DES key is denoted as in section 2.2 as (K_L,K_R) and enc(K)[X] denotes a single DES encryption of X. Process the four 8-byte blocks of the (32 bytes) hash value h = X1, X2, X3, X4 with the (Single-)DES in CBC mode using the left MAC key block K_L:

$H_i := enc(K_L)[X_i \text{ XOR } H_{i-1}]$, for i = 1, 2, 3, 4

with initial value

H_0 := ('00' || '00' || '00' || '00' || '00' || '00' || '00' || '00').

Compute the 8 byte block H_5 in the following way (according to [ISO9797-1] algorithm 3):

$H_5 := enc(K_L)[dec(K_R)[H_4]]$

The MAC is then equal to H_5. This calculation is also known as CBC Retail-MAC.

2.4.2.2 AES[1] and SHA 512

The MAC calculation is performed according to the specification in [NIST SP 38B]. Assume a key K of 128 bit and $enc_{AES\text{-}128}$ (K, X) denotes a AES-128 encryption of 16 byte value X with the key K. The output of the hash operation SHA-512 will be the 64 byte value h = X1, X2, X3, X4 (Xi of 16 byte length) as follows:

1. According to the specification in chapter 6.1 of [NIST SP 38B] a sub-key K1 is calculated from K[2]
2. X4 := X4 XOR K1
3. $H_i := enc_{AES\text{-}128}$ (K, $[X_i \text{ XOR } H_{i-1}]$, for i = 1, 2, 3, 4 with
   H_0 := ('00' || '00' || '00' || '00' || … || '00' || '00' || '00') a 16 byte initial vector.
4. The 8 most significant bytes of H_4 are taken as MAC.

[1] This chapter describes the case of AES using key with 128 bit length.

[2] The standard [NIST SP 38B] calculates two sub keys K1 and K2, depending if padding is necessary or not.. Since no padding is necessary in the above case only K1 is used.

3 Message Key Derivation

Upon a basic Master Key (MK), which has to be exchanged by other means (see chapter 5) prior to the first transaction, message-individual keys are used for encryption and MAC-calculation (application specific).

The time period of a session is defined as the transmission period of exactly one ISO message. Thus, for *every* online ISO message and every clearing message a different key is used. This is also valid for corresponding request and response messages.

3.1 Triple-DES based

Let MK_{MAC} and MK_{ENC} be application specific Master Keys of 16 byte (128 bits) length for MAC building and encryption/decryption (of the PIN block) respectively. Different Master Keys are used for authorisation and clearing messages. The Master Keys must only be used inside a HSM.

The session keys SK_{MAC} and SK_{ENC} each of 16 byte length are then generated dynamically following the formula

$$SK_{MAC} = PA([d*(MK_{MAC}) RND1_{MAC}] || [d*(MK_{MAC}) RND2_{MAC}])$$

$$SK_{ENC} = PA([d*(MK_{ENC}) RND1_{PAC}] || [d*(MK_{ENC}) RND2_{PAC}])$$

where RND = RND1||RND2 is a random number of 16 byte length, concatenated by two blocks RND1 and RND2 of 8 byte length each, generated for each session. Here, PA is a byte wise parity adjustment and $d*MK_{XXX}(..)$ is the notation for the decryption with Triple DES in ECB-Mode with a Master Key MK_{XXX} of 16 byte length of the argument (..). The argument here is the random block RND1, resp. RND2. The random numbers will be different for a MAC calculation (RND_{MAC}) and for encryption (RND_{PAC}).

3.2 AES based according to [EMV_B2_4.3]

Let MK be a master key of length k. The length k is either 128 bits, 192 bit or 256 bit depending on which AES variant according to [FIPS 197] is used. Let RND be a 16 byte random number, denoted as $r_0 || r_1 || r_2 || \ldots || r_{15}$. Let

$$V1 = r_0 || r_1 || 'F0' || r_3 || \ldots || r_{15}$$

$$V2 = r_0 || r_1 || '0F' || r_3 || \ldots || r_{15}$$

be two variants of RND.

A session key KS will be derived according to chapter A1.3.1 of [EMV_B2_4.3] in one of the following ways:

$$KS = enc_{AES\text{-}128} (MK, RND)$$

KS = 192 most significant bits of {enc_{AES192} (MK, V1) || $enc_{AES-192}$ (MK, V2)}

KS = $enc_{AES-256}$ (MK, V1) || $enc_{AES-256}$ (MK, V2)

These derivations have to be performed respectively for a KS of 128, 192 and 256 bit.

Comment: a 256 bit key is derived using a random of 128 bit (16 bytes random) reducing the key space to 2^{128} instead of 2^{256}. However, since the AES algorithm is used for the derivation, the value of the key remains unpredictable i.e. it is currently not possible to determine which values of the key will be in the reduced key space without knowing the value of the master key. Hence an exhaustive search would currently still need to check all 2^{256} values. The same analysis holds for a 192 bit key.

4 Specification of BMP 53

BMP 53 in authorisation and clearing messages according to [BG A] and [BG CSI] shall have the following structure. All values in BMP 53 are binary coded.

Position	Length in bytes	Content	Value(s) (hexadecimal)	Remarks
1	1	PIN block format	'00' or '01' or '02' or '03' or '04' or 'FF'	'00': ISO PIN format 0 '01': ISO PIN format 1 '02': ISO PIN format x[3] using AES-128 for encryption '03': ISO PIN format x using AES-192 for encryption '04': ISO PIN format x using AES-256 for encryption the acquirer is allowed to choose the PIN block format, the issuer must support all formats 'FF': Filler for network management messages or messages without PIN block (no BMP 52), e.g. clearing messages '03'...'FE': RFU

[3] This will be the ISO format for PIN blocks not using Triple-DES as encryption algorithm. The actual ISO standard [ISO9564-1] is currently (05/09/2012) under review.
In addition, BMP 3 has to be adjusted to note that the length of BMP 52 will exceed 8 bytes. See Note 7 at the end of this chapter!

Position	Length in bytes	Content	Value(s) (hexadecimal)	Remarks
2	1	Algorithm Identifier	'00', '01', '02'	'00': **no l**onger valid and shall **not** be used. '01': used in production phase: derivation of double length triple-DES session keys according to chapter **3.1** '02': identifies MAC calculation for clearing files by using double length key and the algorithm according to ISO 9797-1, algorithm 3 (see section 2.4.2.1) with SHA-256 as hash-function '03': AES based key derivation as described in chapter **3.2** '04': AES based CMAC calculation for clearing files according to [NIST SP 38B]; see 2.4.2.2 with SHA 512 '05'…'FF': RFU
3	2	Key ID of the Master Key(s)	'0000' - 'FFFF'	Binary coded; Key ID is used to identify and distinguish the communication pairs;
4	1	Key Version of Master Key(s)	'0x' or '1x' or '2x' or '3x' or '4x' or '5x' or '6x'	'0x': test key authorisation / network management '1x': production key authorisation / network management '2x': disaster backup key authorisation / network management '3x': test key clearing '4x': production key clearing '5x': disaster backup key clearing '6x': disaster backup test key authorisation / network management '7x' – 'Fx': RFU x denotes the last digit of the year, in which the key is introduced;

Position	Length in bytes	Content	Value(s) (hexadecimal)	Remarks
5	16	RND_{MAC}		16 byte Binary Random number (cf. chapter **3**)
6	16	RND_{PAC}		16 byte Binary Random number (cf. chapter **3**), only present if (and only if) BMP 52 is present in the respective message

Note 1:

It has to be pointed out that the value of the algorithm identifier in position 2, byte 2 of the above BMP 53 determines the structure of this BMP beginning with byte 3.

Note 2:

The Key IDs in position 3 of BMP 53 are chosen according to a table provided by Bank-Verlag. A Key ID identifies uniquely a pair of communication partners.

Note 3:

Each year a new Master Key is introduced which is valid from April 1st of this year until March 31st the following year.

For example the keys used in the time between April 1st 200**8** and March 31st 2009 the variable x in position 4 of BMP 53 has the value **8**. The test key for authorisation messages has the Key Version '08', while the production key for clearing has the Key Version '48'.

Note 4:

It is necessary to handle more than one Master Key within an HSM, so that the key change to the disaster backup keys (for authorisation and clearing) can be performed without loss of service in the case that the HSM itself is not compromised.

Note 5:

The last position (position no. 6; RND_{PAC} for session encryption key) is missing for messages that do not contain BMP 52 (see [BG A] and [BG CSI]).

Note 6:

To achieve the maximum entropy the 16 byte Random numbers in position 5 and 6 must be chosen out of the **full** range of **all** possible values. So each random number must be in the

range '00…00' to 'FF…FF' where **every** value in this range must be generated with equally distributed probability.

Note 7:

The ISO PIN block format is addressed in position 1 of BMP 53. The PIN block is formatted as described in the respective ISO standard (see [ISO9564-1][4]) and transmitted in BMP 52.

If according to position 1 of BMP 53 format x[5] is used, having a length of more than 8 bytes, the fifth half byte of BMP 3 MUST be set to '2'. This means, if 'n' is used for the digits in BMP 3 according to [BG A] the format will be

'nn nn **2**n'

if PIN block format x is used.

[4] This standard introduces a PIN block format for AES encryption but this is NOT published at 05/09/2012. The version of this document at hand has to be updated as soon as the standard is available.

[5] x will be fixed after the standard has been published. Within this document format x describes the AES PIN block format which has a length of more than 8 bytes.

5 Key Management

Each pair of communication partners has to exchange Master Keys for the key derivation according to chapter **3** in advance of the first transaction.

Between each pair of communication partners the following Master Keys must be exchanged where the expansion ALG is either DES (for two key Triple-DES), AES-128, AES-192 or AES-256 (for AES with key length of 128 bit, 192 bit or 256 bit, respectively):

Key Name	Key Version	Description
BGMK-ENC-ALG	1x	Berlin Group Master Key for derivation of encryption session keys for authorisation messages according to chapter **3**
BGMK-MAC-ALG	1x	Berlin Group Master Key for derivation of MAC session keys for authorisation messages according to chapter **3**
BGMK-MAC-ALG	4x	Berlin Group Master Key for derivation of MAC session keys for clearing messages according to chapter **3**
BGMK-ENC-ALG	2x	Backup key for BGMK-ENC
BGMK-MAC-ALG	2x	Backup key for BGMK-MAC for authorisation messages
BGMK-MAC-ALG	5x	Backup key for BGMK-MAC for clearing messages
BGMK-ENC-ALG	0x	Test key for Master Key for derivation of encryption session keys for authorisation messages according to chapter **3**
BGMK-MAC-ALG	0x	Test key for Master Key for derivation of MAC session keys for authorisation messages according to chapter **3**
BGMK-ENC-ALG	6x	Disaster Backup test key for test BGMK-ENC
BGMK-MAC-ALG	6x	Disaster Backup test key for test BGMK-MAC for authorisation messages
BGMK-MAC-ALG	3x	Test key for Master Key for derivation of MAC session keys for clearing messages according to chapter **3**

The distribution of those Master Keys will take place in encrypted form. The systems and processes used for key distribution should comply with the requirements for securing encryption keys mentioned in [PCI PSR]. Especially the requirements in objective 3 (Keys are conveyed or transmitted in a secure manner) must be fulfilled. Sender and receiver of keys must agree on a detailed procedure.

A Zone Master Key is used as Key Encryption Key to encrypt Master Keys for secure transport between two communication partners. This Zone Master Key ZMK_AES is an AES key exchanged in components that are combined in XOR to build the final ZMK_AES. The Master Keys are encrypted under this ZMK_AES for transport in CBC mode with IV all zeroes. A Key Check value (KCV) is appended to each encrypted Master Key. This KCV is calculated as ECB encryption of 0-vector (of 16 bytes length) using the plaintext Master Key and taking the 3 rightmost significant bytes of the result in hexadecimal representation as check value, as described in section 6.

Each year a new set of Master Keys is introduced which is valid from April 1st of this year until March 31st the following year.

6 Check values

Check values will be used during key exchange to avoid wrong key input in HSMs. The check values will be calculated as ECB encryption of 0-vector (16 bytes in case of AES, 8 bytes in case of Triple-DES) using the transmitted key and taking the 3 most significant bytes of the result in hexadecimal representation as check value.

7 References

[BG A] Bilateral and Multilateral Processing of Card Transactions in Europe, Authorisation, ISO 8583 Interchange Messages, Version 3.1, 25/03/2011

[BG CSI] Bilateral and Multilateral Processing of Card Transactions in Europe, Clearing and Settlement, Interface Specification, Version 3.1, 25/03/2011

[ISO 8583:1993] ISO 8583, Financial transaction card originated messages - Interchange message specifications, 1993

[ISO/IEC 9797-1] ISO/IEC 9797-1:2011, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

[ISO/IEC 11568-2] Banking – Key Management (Retail) – Part2: Symmetric Ciphers. Their Key Management and Life Cycle

[FIPS 197] Federal Information Processing Standards Publication 197, November 26, 2001, Specification for the ADVANCED ENCRYPTION STANDARD (AES)

[NIST SP 38B] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[EMV_B2_4.3] EMV Integrated Circuit Card Specifications for Payment Systems Book 2, Security and Key Management, Version 4.3, November 2011

[SHA-512] NIST: FIPS 180-3, Secure Hash Standard, Federal Information Processing Standards Publication 180-3, U. S. Department of Commerce / N.I.S.T., October 2008

[PCI PSR] Payment Card Industry (PCI) PIN Security Requirements, Version 1.0 September 2011,

[ISO9564-1] ISO 9564-1:2011/DAM 1, Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINS in card-based systems, currently under review