

# Bilateral and Multilateral Processing of Card Transactions in Europe

## Security Features

Version 3.0

Date: 25/02/2009

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
<b>2</b>	<b>Basic cryptographic mechanisms .....</b>	<b>3</b>
2.1	Padding .....	3
2.2	Encryption .....	3
2.3	HASH-Function .....	3
2.4	MAC calculation .....	4
2.4.1	Authorisation Messages .....	4
2.4.2	Clearing Messages .....	4
<b>3</b>	<b>Message Key Derivation .....</b>	<b>6</b>
<b>4</b>	<b>Specification of BMP 53 .....</b>	<b>7</b>
<b>5</b>	<b>Key Management .....</b>	<b>10</b>
<b>6</b>	<b>Check values .....</b>	<b>12</b>
<b>7</b>	<b>References .....</b>	<b>13</b>

## 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.

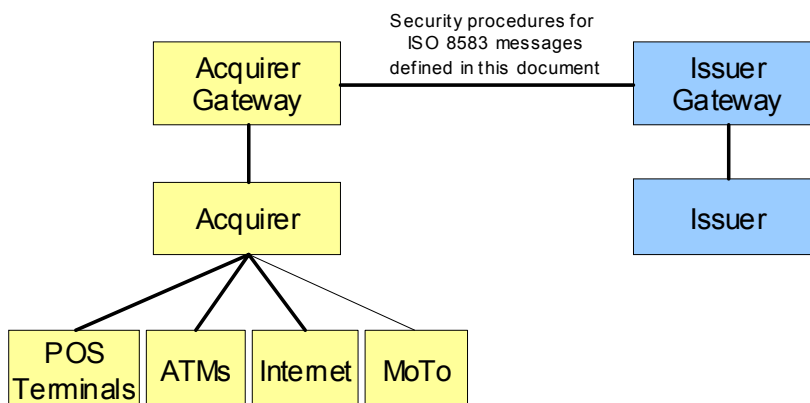


Figure 1: Infrastructure for bilateral and multilateral processing of card transactions in Europe

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

It was decided to 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). A migration to a new algorithm like Advanced Encryption Standard AES might be discussed later. For this reason there should be an algorithm identifier in BMP 53.

### 2.1 Padding

Padding will be performed by using the technique described as method 2 in chapter 5.1 of [ISO 9797-1]. 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 64.

The resulting data is divided into 64-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

Encryption algorithm will be double length key Triple DES 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.

### 2.3 HASH-Function

As a hash-function the algorithm SHA-256 is used as specified in [SHA-256]. This function generates a value of fixed length  $h$  (256 bit or 32 bytes) over every input message  $M$ . It will be written as:

$$h := \text{SHA-256}(M)$$

## 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.

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

### 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.

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  $e(K)[X]$  denotes a single DES encryption of  $X$ . Process the four 8-byte blocks of the (32 bytes) hash value  $h = X_1, X_2, X_3, X_4$  with the (Single-)DES in CBC mode using the left MAC key block  $K_L$ :

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

with initial value

$$H_0 := ('00' \parallel '00' \parallel '00' \parallel '00' \parallel '00' \parallel '00' \parallel '00' \parallel '00').$$

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

$$H_5 := e(K_L)[d(K_R)[H_4]]$$

The MAC is then equal to  $H_5$ .

### 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.

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 ( $RND_{PAC}$ ).

#### 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 'FF'	'00': ISO PIN format 0 '01': ISO PIN format 1 the acquirer is allowed to choose the PIN block format, the issuer must support both formats 'FF': Filler for network management messages or messages without PIN block (no BMP 52), e.g. clearing messages '02'...'FE': RFU
2	1	Algorithm Identifier	'00', '01', '02'	'00': used in pilot phase; '00' is <b>no</b> longer valid and shall <b>not</b> be used.  '01': used in production phase: derivation of double length triple-DES session keys according to chapter 3  '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) with SHA-256 as hash-function;  '03'...'FF': RFU
3	1	Key ID of the Master Key(s)	'00' - 'FF'	Binary coded; Key ID is used to identify and distinguish the communication pairs;

Position	Length in bytes	Content	Value(s) (hexadecimal)	Remarks
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;
5	16	RND <sub>MAC</sub>		16 byte Binary Random number (cf. chapter 3)
6	16	RND <sub>PAC</sub>		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 BV Zahlungssysteme. 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 1<sup>st</sup> of this year until March 31<sup>st</sup> the following year.

For example the keys used in the time between April 1<sup>st</sup> 2008 and March 31<sup>st</sup> 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.

**Note 5:**

The last position (position no. 6; RND<sub>PAC</sub> 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:**

If the ISO PIN block format 1 is addressed in position 1 of BMP 53 the PIN block is filled with random numbers up to the length of 8 bytes after the PIN itself has been introduced. For example, for a 4 digit PIN 4711 the PIN block is as follows (noted in half bytes):

1	4	4	7	1	1	R	R	R	R	R	R	R	R	R	R
Byte 1		Byte 2		Byte 3		Byte 4		Byte 5		Byte 6		Byte 7		Byte 8	

- The first byte '14' indicates PIN block format 1 and a length of 4 digits for the PIN.
- The second and third byte contain the PIN digits.
- Bytes 4 to 8 must contain random values R in the range '0' ... 'F', where **every** value in this range must be generated with equally distributed probability.

## 5 Key Management

Each pair of communication partners has to exchange double length 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:

Key Name	Key Version	Description
BGMK-ENC	1x	Berlin Group Master Key for derivation of encryption session keys for authorisation messages according to chapter 3
BGMK-MAC	1x	Berlin Group Master Key for derivation of MAC session keys for authorisation messages according to chapter 3
BGMK-MAC	4x	Berlin Group Master Key for derivation of MAC session keys for clearing messages according to chapter 3
BGMK-ENC	2x	Backup key for BGMK-ENC
BGMK-MAC	2x	Backup key for BGMK-MAC for authorisation messages
BGMK-MAC	5x	Backup key for BGMK-MAC for clearing messages
BGMK-ENC	0x	Test key for Master Key for derivation of encryption session keys for authorisation messages according to chapter 3
BGMK-MAC	0x	Test key for Master Key for derivation of MAC session keys for authorisation messages according to chapter 3
BGMK-ENC	6x	Disaster Backup test key for test BGMK-ENC
BGMK-MAC	6x	Disaster Backup test key for test BGMK-MAC for authorisation messages
BGMK-MAC	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. A so called Key Encryption Keys (KEK) is used to encrypt Master Keys. Each pair of communication partners

(in the following called participants **A** and **B**) must exchange one KEK. The KEKs are double length keys for the Triple-DES encryption algorithm.

Key Encryption Keys are divided into three parts (combined by XOR to build the final KEK) so that

$$\text{KEK} = \text{KEK}_1 \text{ XOR } \text{KEK}_2 \text{ XOR } \text{KEK}_3.$$

Each  $\text{KEK}_i$  ( $i = 1,2,3$ ) is generated randomly by a security officer of one party (security officer of participant **A**). Each of the three key parts will be transported by registered mail in sealed envelopes to one (of three) key custodian of the second communication partner (participant **B**). The key custodians of **B** should inform the sending party **A** when they have received the key parts in envelopes not tampered with. Otherwise the procedure has to start again with a new KEK. A check value according to chapter 6 will be delivered with each  $\text{KEK}_i$  ( $i = 1,2,3$ ) and also for the final KEK. The lifetime of a KEK is 5 years.

Therefore a list of three key custodians within each organization has to be exchanged between the partners. When the list of key custodians (name, address, phone, fax, e-mail, picture, signed by a representative of the company) is exchanged the process described above is started.

When the secure deliverance of KEK is finished, the Master Keys can be transmitted in encrypted form, using Triple DES (or DES<sup>3</sup>, ECB mode) with the corresponding KEK. This key exchange can be performed online. The Master Keys are generated by participant **B** and transmitted to participant **A**. The encrypted Master Key could be printed or stored on an electronic medium like floppy disc and is send by registered mail to **A**. A full set of Master Keys (including production & backup and encryption, authorisation & clearing keys) is exchanged. A check value according to chapter 6 will be delivered for each Master Key.

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

In the future it might be possible to have different set of Master Keys with different activation and expiration dates. Additionally the security level of transactions could be improved if a different set of Master Keys e.g. for each different month within a single year is used.

## **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 encryption of 0-vector 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 3.0, 25/02/2009
- [BG CSI] Bilateral and Multilateral Processing of Card Transactions in Europe, Clearing and Settlement, Interface Specification, Version 3.0, 25/02/2009
- [ISO 8583:1993] ISO 8583, Financial transaction card originated messages - Interchange message specifications, 1993
- [ISO/IEC 9797-1] Information technology – Security techniques – Message Authentication Codes – Part 1: Mechanisms using a block cipher
- [ISO/IEC 11568-2] Banking – Key Management (Retail) – Part2: Symmetric Ciphers. Their Key Management and Life Cycle
- [SHA-256] NIST: FIPS Publication 180-2: Secure Hash Standard (SHS), August 2002 and Change Notice 1, February 2004.