THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

Bilateral and Multilateral Processing of Card Transactions in Europe

Authorisation

ISO 8583 Interchange Messages

Version 3.2 AES

Date: 08/07/2019

Notice

This Specification has been prepared by the Participants of the Berlin Group. Permission is hereby granted to use the document solely for the purpose of implementing the Specification subject to the following conditions: (i) that none of the participants of the Berlin Group nor any contributor to the Specification shall have any responsibility or liability whatsoever to any other party from the use or publication of the Specification; (ii) that one cannot rely on the accuracy or finality of the Specification; and (iii) that the willingness of the participants of the Berlin Group to provide the Specification does not in any way convey or imply any responsibility for any product or service developed in accordance with the Specification and the participants of the Berlin Group as well as the contributors to the Specification specifically disclaim any such responsibility to any party.

Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of the Berlin Group and any other contributors to the Specification are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Specification is provided "AS IS", "WHERE IS" and "WITH ALL FAULTS", and no participant in the Berlin Group makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights (whether or not the Participants of the Berlin Group have been advised, have reason to know, or are otherwise in fact aware of any information), and fitness for a particular purpose (including any errors and omissions in the Specification).**

To the extent permitted by applicable law, neither the Participants of the Berlin Group nor any contributor to the Specification shall be liable to any user of the Specification for any damages (other than direct actual out-of-pocket damages) under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, nor any damages arising out of third party claims (including claims of intellectual property infringement) arising out of the use of or inability to use the Specification, even if advised of the possibility of such damages.

Details of the Participants of the Berlin Group can be found at www.berlin-group.org.

Participation in the Berlin Group does not imply either endorsement of any of the solutions identified in the Feasibility Study, carried out by the Berlin Group, or a commitment to implement them.

The Specification, including technical data, may be subject to export or import regulations in different countries. Any user of the Specification agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import the Specification.

Contents

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.

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

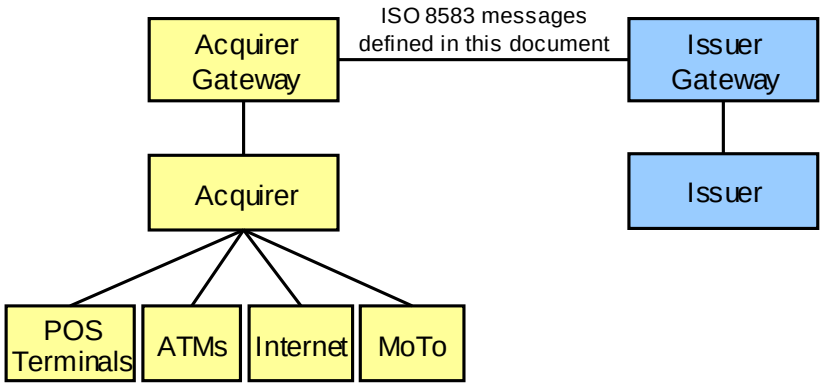

Figure 1: Infrastructure for bilateral and multilateral processing of card transactions in Europe

The focus of this document is on the specification of the ISO 8583 online messages, which are exchanged between acquirer gateways and issuer gateways in order to authorise card transactions in Europe.

An annex describes how a record in a BIN File for the definition of cards participating in bilateral or multilateral processing of transactions in Europe shall be structured.

2 Services Definitions and Support

The services defined in [ECSG] that are supported by this specification are described in Table 1. The service names and definitions given in Table 1 are in line with those in Part 2 of [ECSG]. The messages used to support the services are specified in sections 3 and 4.

Service Name and Description	Support
ATM Cash Withdrawal: A service which allows the cardholder to withdraw cash at an unattended cash dispensing device. Also called "ATM Cash Disbursement"	Authorisation with a specific Processing Code and Card Acceptor Business Code using Authorisation Request and Authorisation Request Response.
Balance Inquiry: A service which allows the cardholder to request information about their account balance.	Authorisation with a specific Processing Code and Inquiry Function Code and additional amounts in the response message using Inquiry Request and Inquiry Request Response. Surcharging is not supported for Balance Inquiry.
Cancellation: A service which allows the card acceptor to cancel a previously approved transaction. Cancellation should only occur before the transaction is cleared to the issuer. It is sometimes called "Manual Reversal".	Full Reversal with a specific Message Reason Code using Reversal Advice, Reversal Advice Repeat, and Reversal Advice Response.
Card Validity Check: A service that allows the validity of the card to be checked. This transaction is only for information and has no financial impact on the card account. It is sometimes called "Information request"	Authorisation with a specific Processing Code and Inquiry Function Code using Inquiry Request and Inquiry Request Response. Surcharging is not supported for Card Validity Check.
Cash Advance (attended): A service that allows the cardholder to withdraw cash in an attended environment, e.g. at a POS terminal or a bank counter. Also called Cash Disbursement.	Authorisation with a specific Processing Code and Card Acceptor Business Code using Authorisation Request and Authorisation Request Response.

Service Name and Description	Support
Combined Funds Request/Top-up This service allows a Card Acceptor to offer top-up services for Cardholders whose Issuer has a top-up contract/connection with the cardholder's mobile phone operator. The Card Acceptor in this case provides just the terminal for the entry of mobile phone data and initiates the Funds Request/top-up. The transaction management of the two subservices Funds Request and top up is performed by the Issuer/Issuer Gateway.	An Authorisation with a specific Processing Code and Card Acceptor BusinessCode using Authorisation Request and Authorisation Request Response. The mobile phone information for the top-up function is transported as private data. The Approval Code of the mobile operator on the top-up as such can additionally be transported in Authorisation Response Message. Specific Action Codes have been foreseen for informing the Card Acceptor and/or cardholder on specific reasons why the top-up function has not been performed successfully.
Deferred Payment: A combined service which enables the card acceptor to perform an authorisation for a temporary amount and a completion for the final amount within a limited time frame. Deferred Payment is only available in the unattended environment. Examples where this service is widely used are unattended petrol pumps and phone booths. This is also called "Outdoor Petrol" when used in the specific petrol sector.	**First step:** Authorisation of an initial amount using Pre-Authorisation Request and Authorisation Request Response. The acquirer may optionally request a validity period for the authorisation. If no validity period is present in the Pre-Authorisation Request, the validity period defined by the respective payment scheme applies. An issuer may approve a lesser amount or may reject the transaction if, for example, they do not accept the validity period. An acquirer may choose not to accept an approval for a lesser amount using a full Reversal. **Second (final) step:** There are two options for the acquirer gateway to perform the second step: • Partial reversal if the final amount is less than the authorised amount, using Reversal Advice, Reversal Advice Repeat, and Reversal Advice Response • Confirmation of the final amount, using Completion Advice, Completion Advice Repeat, and Authorisation Advice Response The issuer gateway must support both options.
Funds Request for Top-up A service requesting funds for loading of a prepaid mobile top-up account. The top-up of the account itself is not directly addressed. In contrast to a Payment transaction for Services, this service transports additionally mobile phone data.	An Authorisation with a specific Processing Code and Card Acceptor Business Code using Authorisation Request and Authorisation Request Response. Addtional mobile phone information e.g. for supporting dispute handling is transported as private data.

Service Name and Description	Support
No Show: A service which allows the card acceptor to charge the cardholder's account due to the fact that the cardholder has not arrived within the specified time and has not cancelled the guaranteed reservation within the specified period. It is used e.g. for hotel trade.	No Show may be performed without an online authorisation. If there was a Pre-Authorisation, No Show may be performed as the final step of the Pre-Authorisation Services (two options). If there was an authorisation of a Payment, No Show may be performed as a partial Reversal, if the amount to be charged is less than the authorised amount. It is scheme dependent, whether partial Reversals are allowed for Payments.
Original Credit: A service which allows the card acceptor to effect a credit to a cardholder' account. Unlike Refund, an Original Credit is not preceded by a card payment. This service is used for example for crediting winnings from gaming. Same kinematics as Refund.	If authorised online, Authorisation with a specific Processing Code using Authorisation Request and Authorisation Request Response. Surcharging and partial Reversals are not supported for Original Credit.
Payment: The basic service which allows the cardholder to pay for the purchase of goods and services from a card acceptor using their card.	Authorisation of an accurate amount using Authorisation Request and Authorisation Request Response. It is scheme dependent, whether partial Reversals are allowed for Payment.
Payment with Cashback: A service which allows the cardholder to obtain cash from the card acceptor in conjunction with a payment. Also called a Cashback transaction. . The cardholder receives the extra amount in cash along with the goods/services.	Authorisation of an accurate amount with a specific Processing Code and an additional amount field using Authorisation Request and Authorisation Request Response. An issuer has the possibility to approve the Payment amount but decline the Cashback amount. Partial Reversals are not supported for Payment with Cashback.
Payment with deferred Clearing: A feature where the acquirer postpones the clearing of the transaction. It is used for example for the payment of health expenses.	Pre-Authorisation indicating an extended validity period.

Service Name and Description	**Support**
Payment with Increased Amount: A feature which allows the cardholder to increase the amount to pay by adding an extra amount, for example where a gratuity (tip) is added. There are two different cases: • The customer increases the amount of a payment prior to authorisation • The authorisation is processed prior to increasing the payment amount, e.g. adding a gratuity on the receipt	Only the first case is applicable to authorisation. In this case a Payment is processed where gratuity is included in the amount in BMP 4 (=transaction amount + gratuity). It is recommended that the gratuity amount is delivered in BMP 54. Note, that the clearing message shall reflect the different amounts contained in the authorisation message. In the second case a Payment is processed where BMP 4 only contains the transaction amount (excluding the gratuity amount). The gratuity amount will be notified as part of the clearing process. Partial Reversals are not supported for Payment with Increased Amount.
Remote Payments: e-Payment: A Remote Payment where goods, services, etc. are purchased over electronic systems such as the Internet and other computer networks. The cardholder may be authenticated by the issuer. MOTO: A Remote Payment following a mail order or telephone order	Authorisation with Authorisation Request containing specific attributes in BMP 22 and containing a BMP 62.

Service Name and Description	Support
Pre-Authorisation Services: A service composed of the 3 steps • **Pre-Authorisation**, • **Update Pre-Authorisation** (optional and potentially with several occurrences), and • **Payment Completion** A **Pre-Authorisation** allows the card acceptor to reserve an amount for a specified period of time to ensure that sufficient funds are available to complete a subsequent payment. The Pre-Authorisation is used only to reserve the amount since neither the final amount nor the final date and time of the actual payment are known (e.g. car rental, hotel, video rental, etc.). Pre-Authorisation is also called "Reservation". The **Update Pre-Authorisation** allows the card acceptor to update the estimated amount and/or the validity period of the previous Pre-Authorisation or the previous Update Pre-Authorisation. Also called a supplementary authorisation or "update reservation". The **Payment Completion** allows the card acceptor to finalise a payment following a Pre-Authorisation or Update Pre-Authorisation Request.	**First step (Pre-Authorisation) and optional subsequent steps (Update Pre-Authorisation):** Authorisation of an estimated amount valid for a specified period of time, using Pre-Authorisation Request (first step), optionally Update Pre-Authorisation Request (subsequent steps), and Authorisation Request Response. An issuer may approve a lesser amount or may reject the transaction if, for example, they do not accept the validity period. An acquirer may choose not to accept an approval for a lesser amount using a full Reversal. At any time before the validity period expires an acquirer may generate an Update Pre-Authorisation Request which, if approved, supersedes the most recent (Update) Pre-Authorisation. The Update Pre-Authorisation Request must contain an amount and may contain a validity period. The amount replaces the previous amount. If present, the validity period replaces the previous validity period. If the Update Pre-Authorisation Request does not contain a validity period the expiry date remains unchanged. Only the last (Update) Pre-Authorisation can be reversed for technical reasons, e.g. time out. **Final step (Payment Completion):** There are two options for the acquirer gateway to perform the final step: • Partial Reversal if the final amount is less than the most recently authorised amount, using Reversal Advice, Reversal Advice Repeat, and Reversal Advice Response • Confirmation of the final amount, using Completion Advice, Completion Advice Repeat, and Authorisation Advice Response The issuer gateway must support both options. Depending on the rules of the scheme under which the transaction is taking place, there may be no need to send an online Payment Completion providing a clearing message is sent before the validity period of the last (Update) Pre-Authorisation expires.

Service Name and Description	Support
Quasi Cash Payment: A service which allows the cardholder to obtain items which are directly convertible to cash. For example these can be gaming chips.	Authorisation with a specific Processing Code using Authorisation Request and Authorisation Request Response.
Recurring Payment: A service where the cardholder authorises an acceptor to charge the cardholder's account on a recurring basis.	Authorisation of all recurrent transactions with a specific Function Code using Recurring Authorisation Request and Authorisation Request Response. Every recurrent transaction shall use the same Retrieval Reference Number as used in the original authorisation. The original authorisation should be as secure as possible (possibly, but not necessarily card present). All subsequent authorisations may be card not present
Refund: A service which allows the card acceptor to reimburse the cardholder partially or totally. Unlike Cancellation, Refund is not necessarily linked to any previous transaction**.**	If authorised online, Authorisation with a specific Processing Code using Authorisation Request and Authorisation Request Response. Surcharging and partial Reversals are not supported for Refund.
Unsolicited Available Funds): A feature which allows the card issuer to provide account balance information in the authorisation response message.	Under the following conditions balance information may optionally be returned: • Insufficient funds (Action Code 116) • Transaction would exceed limits (Action Code 121) • Balance information on an approved transaction.

Table 1: Services supported by the specified messages

The following services and additional features defined in [ECSG] are not supported by this specification:

- Card Funds Transfer,
- Cash Deposit,
- e-purse - Loading/Unloading,
- Instalment Payment,
- Payment or cash withdrawal with dynamic currency conversion,
- Payment with purchasing or corporate card data,
- Payment with cumulative amount,
- Payment with Loyalty information.

3 Message Types and Message Flows

This section defines which message types and message flows must be supported by acquirer gateways and issuer gateways.

3.1 Supported Messages

The following Table 2 contains the supported messages, their message type identifier (MTID) according to [ISO 8583:1993] and the party that is supposed to send or receive the respective message type:

MTID	Message Type	Sender	Recipient
1100	Authorisation Request	Acquirer Gateway	Issuer Gateway
1110	Authorisation Request Response	Issuer Gateway	Acquirer Gateway
1120	Authorisation Advice	Acquirer Gateway	Issuer Gateway
1121	Authorisation Advice Repeat	Acquirer Gateway	Issuer Gateway
1130	Authorisation Advice Response	Issuer Gateway	Acquirer Gateway
1420	Reversal Advice	Acquirer Gateway	Issuer Gateway
1421	Reversal Advice Repeat	Acquirer Gateway	Issuer Gateway
1430	Reversal Advice Response	Issuer Gateway	Acquirer Gateway
1804	Network Management Request	Acquirer Gateway or Issuer Gateway	Issuer Gateway or Acquirer Gateway
1814	Network Management Request Response	Issuer Gateway or Acquirer Gateway	Acquirer Gateway or Issuer Gateway

Table 2: Messages supported by acquirer gateways and issuer gateways

3.2 Message Use

The following Table 3 describes how the Function Codes (FC) are used in requests and advices to identify the specific use of the message for the different services:

MTID	FC	Message Use	Services
1100	100	Authorisation Request	Payment, Payment with Cashback, ATM Cash Withdrawal, Cash Advance, Quasi Cash Payment, Original Credit, Refund, Funds Request for Top-Up, Combined Funds Request/Top-up
1100	101	Pre-Authorisation Request	Deferred Payment, Pre-Authorisation Services
1100	103	Update Pre-Authorisation Request	Pre-Authorisation Services
1100	108	Inquiry Request	Card Validity Check, Balance Inquiry
1100	181	Recurring Authorisation Request	Recurring Payment
1120 / 1121	180	Completion Advice / Completion Advice Repeat	Deferred Payment, Pre-Authorisation Services, eventually No Show
1420 / 1421	400	Reversal Advice / Reversal Advice Repeat	Cancellation, full Reversal
1420 / 1421	401	Reversal Advice / Reversal Advice Repeat	Partial Reversal, optionally Deferred Payment, optionally Pre-Authorisation Services

Table 3: Function Codes indicating the use of messages

3.3 General Rules

Only the acquirer gateways establish data communications and - after having successfully established data communications - initiate the communication on application level by sending a Sign-on Request.

If the currency of a transaction is different from Euro the acquirer shall convert the transaction amount(s) to Euro. The rules to determine the conversion rate are outside the scope of this specification.

The flows of messages between acquirer gateway and issuer gateway are described in the following sections.

For all messages exchanged between gateways the following rules apply:

- If a gateway receives from another gateway a message, which cannot be recognized (MTID not supported, identifying message fields missing, too many data fields corrupted) or if a gateway receives a message with wrong MAC, the receiver shall not respond to the message.

- A gateway has to respond to all request and repeat messages, which have been sent by another gateway, can be recognized, and contain a correct MAC.

  If a request or repeat message received by a gateway from another gateway can be recognized and contains a correct MAC but has an invalid syntax or format according to the following rules:

  - Message fields not defined for the MTID are not allowed,

  - Data fields and data elements which are mandatory must be present,

  - Message fields, which are present (whether mandatory, conditional or optional) must be coded according to the rules described below,

  the receiver of the message must respond to the sender of the message with a response message containing the Action Code "Format error" (904).

- In the following cases a gateway shall not process a response message it receives from another gateway:

  - The response message cannot be matched to any request message sent before (in the time out interval) to the sender of the response message.

  - The response message has an invalid syntax or format according to the following rules:

    - Message fields not defined for the MTID are not allowed.

    - Data fields and data elements which are mandatory must be present,

    - Message fields, which are present (whether mandatory, conditional or optional), must be coded according to the rules described below.

- Reversal Advices and Authorisation Advices are handled by the gateways according to the store and forward principle:
  - After receiving an Advice or an Advice Repeat, which can be recognized as such, the gateway responds with the appropriate Advice Response to the sender.
  - Irrespective of the communication with the sender of the Advice or Advice Repeat, the gateway tries to forward the Advice or Advice Repeat to the next recipient until it is successful or the maximum number of repetitions or the time limit for repetitions is reached.
  - This is true for both, acquirer gateways and issuer gateways.

3.4 Authorisation and Reversal Message Flow

The normal message flow for an authorisation is shown in Figure 2. It consists of the following steps:

1. An acquirer gateway sends an Authorisation Request (MTID 1100) to the issuer gateway.

2. The issuer gateway receives the valid Authorisation Request from the acquirer gateway and responds with an Authorisation Request Response (MTID 1110) to the acquirer gateway.

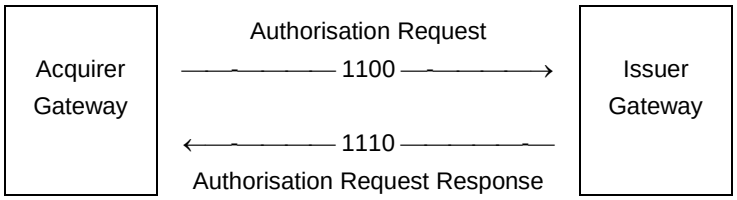

Figure 2: Normal message flow for an authorisation

If after having sent an Authorisation Request the acquirer gateway does not receive the Authorisation Request Response within a pre-set time frame (time out of the Authorisation Request Response) the acquirer gateway must initiate a reversal message flow with Message Reason Code "Timeout waiting for response" (4021) to the issuer gateway.

The time out limit for Authorisation Request Responses is a parameter to be set by the acquirer gateway according to the rules agreed between the acquirer gateway and the respective issuer gateway. It must not exceed 16 seconds.

Not processing the Authorisation Request Response for any of the reasons described in section 3.3 will cause a time out of the Authorisation Request Response at the acquirer gateway. As a consequence the acquirer gateway will initiate a reversal flow.

If the acquirer gateway receives the Authorisation Request Response in time, with valid syntax, format and MAC, but is unable to forward the Authorisation Request Response to the acquirer, the acquirer gateway initiates a reversal message flow to the issuer gateway with Message Reason Code "Unable to deliver message to point of service" (4013).

After having successfully received and forwarded an Authorisation Request Response the acquirer gateway initiates a reversal message flow to the issuer gateway, only if this is required by the acquirer. This may be necessary because of communication problems in the acquirer network or because the transaction cannot be completed on the acquirer side or because the transaction is only partially completed on the acquirer side or because a Cancellation has been initiated at Point of Service (POS). In this case the Message Reason Code to be used will be set by the acquirer.

The normal message flow for a Reversal initiated by the acquirer is shown in Figure 3. It consists of the following steps:

1. The acquirer gateway sends a Reversal Advice (MTID 1420) to the issuer gateway.

2. The issuer gateway receives the advice from the acquirer gateway and answers this message by sending a Reversal Advice Response (MTID 1430) to the acquirer gateway.

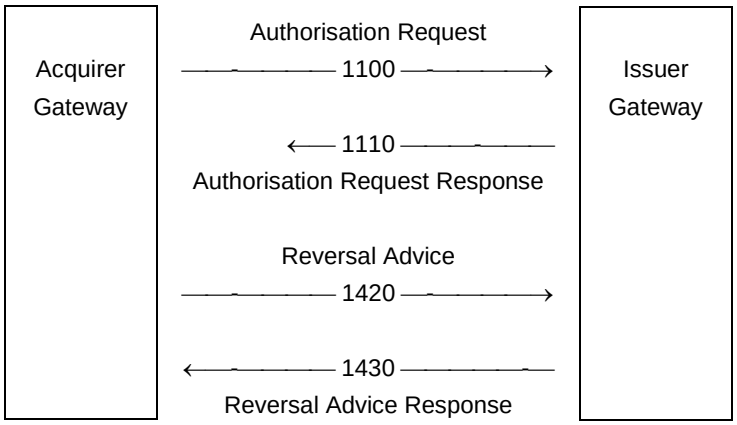

Figure 3: Normal message flow for a reversal

If after having sent a Reversal Advice the acquirer gateway does not receive the Reversal Advice Response within a pre-set time frame (time out of the Reversal Advice Response) the acquirer gateway must send a Reversal Advice Repeat (MTID 1421) to the issuer gateway.

The time out limit for Reversal Advice Responses is a parameter to be set by the acquirer gateway according to the rules agreed between the acquirer gateway and the respective issuer gateway. It must not exceed 16 seconds.

Not processing the Reversal Advice Response for any of the reasons described in section 3.3 will cause a time out of the Reversal Advice Response at the acquirer gateway. As a consequence the acquirer gateway will send a Reversal Advice Repeat to the issuer gateway.

The acquirer gateway repeats the Reversal Advice Repeat until it receives a valid Reversal Advice Response or until the maximum number of repetitions is reached or until the time limit for repetitions is reached.

The intervals for resending Reversal Advice Repeats and the number of repetitions are to be defined by the acquirer gateways according to the rules agreed between the acquirer gateway and the respective issuer gateway. The minimum length of the intervals for resending Reversal Advice Repeats is 1 minute. The maximum number of repetitions of a Reversal Advice Repeat is 10.

If the issuer gateway receives a Reversal Advice or Reversal Advice Repeat without having received the initial Authorisation Request it may respond with Action Code "Not able to trace back to original transaction" (914).

The time limit for Reversal Advices and repetitions of Reversal Advice Repeats is two days. If the issuer gateway receives a Reversal Advice or Reversal Advice Repeat later than two days after the initial Authorisation Request it may respond with Action Code "Not able to trace back to original transaction" (914).

The message flow for a Reversal with Reversal Advice Repeats after time outs for the Reversal Advice Responses is shown in Figure 4:

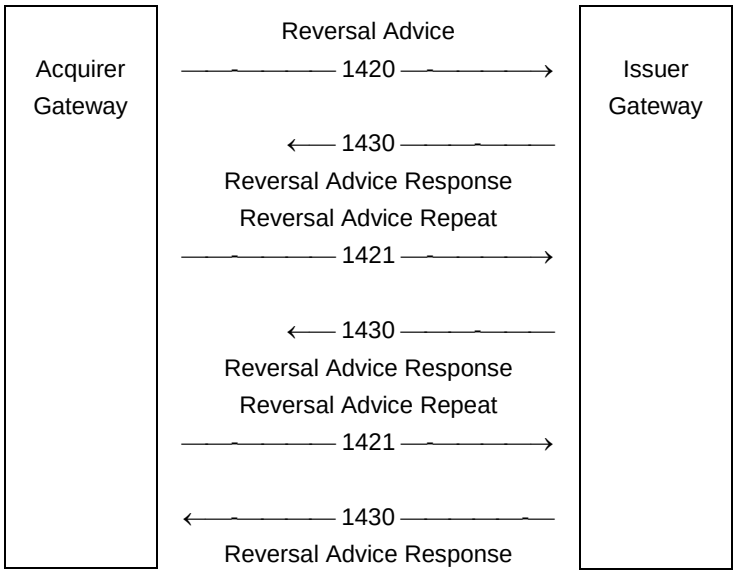

Figure 4: Message flow for a Reversal with Reversal Advice Repeats

3.5 Authorisation and Authorisation Advice Message Flow

The Authorisation and Authorisation Advice message flow may be used by the acquirer gateway to process a Deferred Payment transaction or Pre-Authorisation Services.

The normal message flow for an authorisation consists of the following steps (see Figure 2):

1. An acquirer gateway sends an Authorisation Request (MTID 1100) to the issuer gateway.

2. The issuer gateway receives the valid Authorisation Request from the acquirer gateway and responds with an Authorisation Request Response (MTID 1110) to the acquirer gateway.

For Pre-Authorisation Services the authorisation message flow will be repeated for each Update Pre-Authorisation.

In the case of a Deferred Payment or Pre-Authorisation Services using the completion option, the transaction is finalised with the message flow for an authorisation advice shown in Figure 5. It consists of the following steps:

1. An acquirer gateway sends an Authorisation Advice (MTID 1120) to the issuer gateway.

2. The issuer gateway receives the valid Authorisation Advice from the acquirer gateway and responds with an Authorisation Advice Response (MTID 1130) to the acquirer gateway.

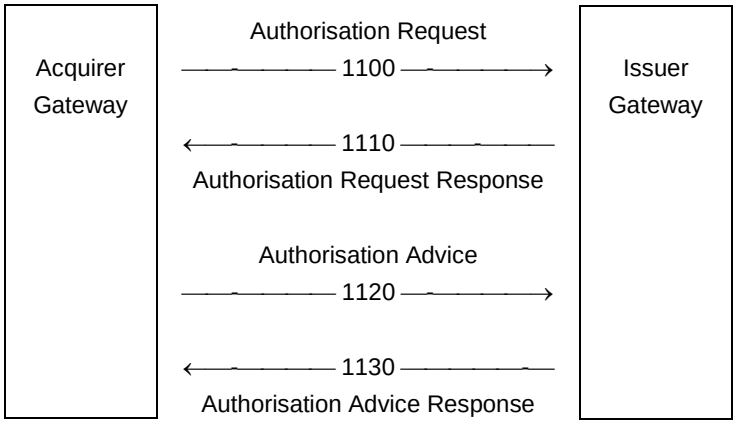

Figure 5: Normal message flow for an authorisation advice

If after having sent an Authorisation Advice the acquirer gateway does not receive the Authorisation Advice Response within a pre-set time frame (time out of the Authorisation Advice Response) the acquirer gateway must send an Authorisation Advice Repeat (MTID 1121) to the issuer gateway.

The time out limit for Authorisation Advice Responses is a parameter to be set by the acquirer gateway according to the rules agreed between the acquirer gateway and the respective issuer gateway. It must not exceed 16 seconds.

Not processing the Authorisation Advice Response for any of the reasons described in section 3.3 will cause a time out of the Authorisation Advice Response at the acquirer gateway. As a consequence the acquirer gateway will send an Authorisation Advice Repeat to the issuer gateway.

The acquirer gateway repeats the Authorisation Advice Repeat until it receives a valid Authorisation Advice Response or until the maximum number of repetitions is reached or until the time limit for repetitions is reached.

The intervals for resending Authorisation Advice Repeats and the number of repetitions are to be defined by the acquirer gateways according to the rules agreed between the acquirer gateway and the respective issuer gateway. The minimum length of the intervals for resending Authorisation Advice Repeats is 1 minute. The maximum number of repetitions of an Authorisation Advice Repeat is 10.

The message flow for an authorisation advice with Authorisation Advice Repeats after time outs for the Authorisation Advice Responses is shown in Figure 6:

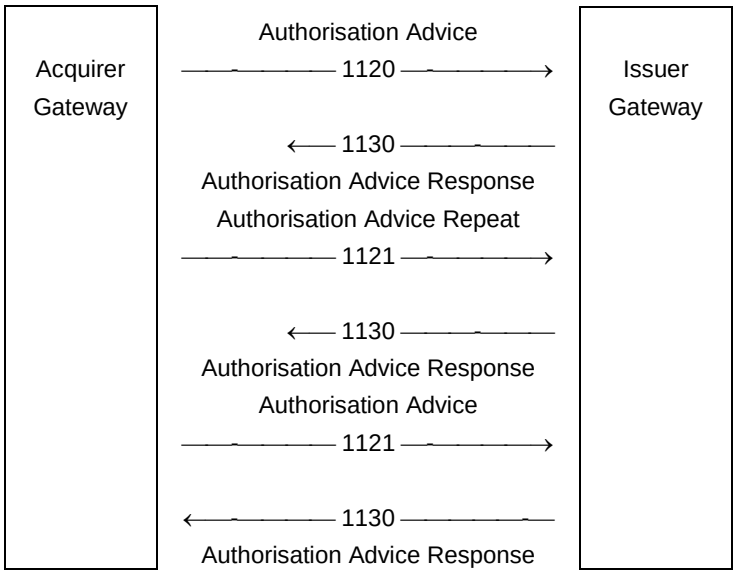

Figure 6: Message flow for an authorisation advice with Authorisation Advice Repeats

3.6 Network Management Message Flow

Network management messages are used to test, to establish, or to terminate communication at the application level.

The following Table 6 describes how the Function Codes (FC) and Messages Reason Codes (MRC) are used in a Network Management Request to identify the specific purpose of the Network Management Request (MTID 1804) and the respective Network Management Response (MTID 1814):

MTID	**Network Management Request**		**Purpose of the Network Management Message**
	FC	**MRC**	
1804	831	8600	Echo-Test Request sent by acquirer gateway
1814			Echo-Test Response sent by issuer gateway
1804	801		Sign-on Request sent by acquirer gateway
1814			Sign-on Response sent by issuer gateway
1804	802		Sign-off Request sent by acquirer gateway
1814			Sign-off Response sent by issuer gateway
1804	831	8601	Echo-Test Request sent by issuer gateway
1814			Echo-Test Response sent by acquirer gateway
1804	801		Sign-on Request sent by issuer gateway
1814			Sign-on Response sent by acquirer gateway
1804	802		Sign-off Request sent by issuer gateway
1814			Sign-off Response sent by acquirer gateway

Table 4: Function Codes and Message Reason Codes used in Network Management Messages

Network Management Messages for Echo-Test shall be supported by all gateways.

Network Management Messages for Sign-on/Sign-off shall be used if supported by both communicating gateways.

3.6.1 Echo-Test

At any time any gateway (called the **sending gateway**) may send an Echo-Test Request to any other gateway (called the **receiving gateway**).

Echo-Test Requests are used by the sending gateway to detect, whether communication at the application level is still established with the receiving gateway.

Any gateway receiving a valid Echo-Test Request shall respond with an Echo-Test Response.

The normal message flow for network management in order to test the communication at the application level is shown in Figure 7. It consists of the following steps:

1. The sending gateway sends an Echo-Test Request (MTID 1804, Function Code 831) to the receiving gateway.

2. The receiving gateway receives the valid Echo-Test Request from the sending gateway and responds with an Echo-Test Response (MTID 1814) with Action Code "Accepted" (800) to the sending gateway.

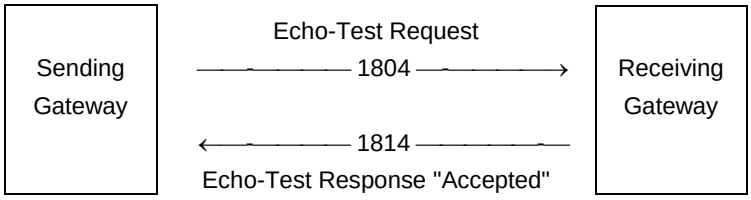

Figure 7: Normal message flow to test communication at the application level

If the sending gateway receives a valid Echo-Test Response of the receiving gateway with Action Code "Accepted" (800) within a pre-set time frame (time out of the Echo-Test Response), communication on application level is still established.

The time out limit for Echo-Test Responses is a parameter to be set by the gateways. It must not exceed 30 seconds and must not be less than 15 seconds.

If the sending gateway does not receive the Echo-Test Response within the time out limit for the Echo-Test Response, the sending gateway may send another Echo-Test Request.

Note:

> If the sending gateway is not able to process the Echo-Test Response for any of the reasons described in section 3.3 this will also cause a time out of the Echo-Test Response at the sending gateway.

If the sending gateway does not receive a valid Echo-Test Response after an appropriate number of Echo-Test Requests, or if the sending gateway receives an Echo-Test Response

containing an Action Code other than "Accepted", manual procedures shall be initiated by the sending gateway in order to get in contact with the receiving gateway directly.

3.6.2 Sign-on

An acquirer gateway and an issuer gateway may agree to use Sign-on to establish communication at the application level. If one of these gateways wants to establish communication at the application level, this gateway (called the **sending gateway**) sends a Sign-on Request to the other gateway (called the **receiving gateway**).

The normal message flow for network management in order to establish the communication at the application level is shown in Figure 8. It consists of the following steps:

1. The sending gateway sends a Sign-on Request (MTID 1804, Function Code 801) to the receiving gateway.

2. The receiving gateway receives the valid Sign-on Request from the sending gateway and responds with a Sign-on Response (MTID 1814) with Action Code "Accepted" (800) to the sending gateway.

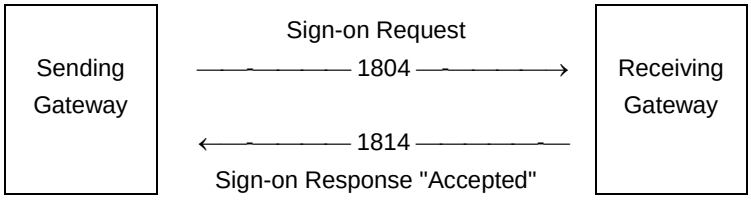

Figure 8: Normal message flow to establish communication at the application level

If the sending gateway receives a valid Sign-on Response of the receiving gateway with Action Code "Accepted" (800) within a pre-set time frame (time out of the Sign-on Response), communication on application level is successfully established.

The time out limit for Sign-on Responses is a parameter to be set by the gateways. It must not exceed 30 seconds and must not be less than 15 seconds.

Note:

If the sending gateway is not able to process the Sign-on Response for any of the reasons described in section 3.3 this will also cause a time out of the Sign-on Response at the sending gateway.

If the sending gateway does not receive the Sign-on Response within the time out limit for the Sign-on Response, the sending gateway may send another Sign-on Request.

After sending a Sign-on Request, the sending gateway shall neither send other messages than repetitions of the Sign-on Request to the receiving gateway nor start processing messages originating from the receiving gateway before a valid Sign-on Response with Action Code "Accepted" (800) originating from the receiving gateway arrives.

If the sending gateway does not receive a valid Sign-on Response after an appropriate number of Sign-on Requests, or if the sending gateway receives a valid Sign-on Response containing another Action Code than "Accepted", manual procedures shall be initiated by the sending gateway in order to get in contact with the receiving gateway directly and to establish communication at the application level.

3.6.3 Sign-off

An acquirer gateway and an issuer gateway may agree to use Sign-off to terminate communication at the application level. If one of these gateways wants to terminate communication at the application level, this gateway (called **sending gateway**) has to send a Sign-off Request to the other gateway (called **receiving gateway**).

The normal message flow for the termination of communication at the application level is shown in Figure 9. It consists of the following steps:

1. The sending gateway sends a Sign-off Request (MTID 1804, Function Code 802) to the receiving gateway.

2. The receiving gateway receives the valid Sign-off Request from the sending gateway and responds with a Sign-off Response (MTID 1814) with Action Code "Accepted" (800) to the sending gateway.

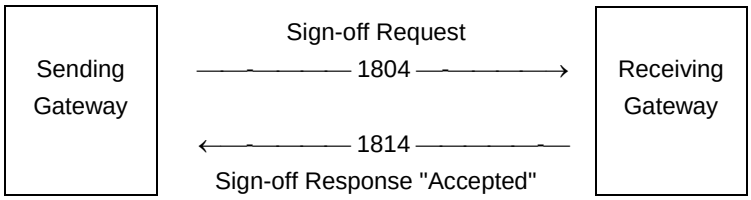

Figure 9: Normal message flow to terminate communication at the application level

If the sending gateway receives a valid Sign-off Response of the receiving gateway with Action Code "Accepted" (800) within a pre-set time frame (time out of the Sign-off Response), communication on application level is successfully terminated and the sending gateway may stop processing messages originating from the receiving gateway.

The time out limit for Sign-off Responses is a parameter to be set by the gateways. It must not exceed 30 seconds and must not be less than 15 seconds.

Note:

If the sending gateway is not able to process the Sign-off Response for any of the reasons described in section 3.3 this will also cause a time out of the Sign-off Response at the sending gateway.

If the sending gateway does not receive the Sign-off Response within the time out limit for the Sign-off Response, the sending gateway may send another Sign-off Request.

After sending a Sign-off Request, the sending gateway shall continue processing messages originating from the receiving gateway until the sending gateway receives a valid Sign-off Response with Action Code "Accepted" (800) originating from the receiving gateway. In particular:

- If the sending gateway is an issuer gateway, it shall wait for a valid Sign-off Response with Action Code "Accepted" originating from the receiving acquirer gateway before communication may be terminated at application level. That is, the issuer gateway shall continue processing and responding to the request/repeat/advice messages originating from the receiving acquirer gateway until a valid Sign-off Response with Action Code "Accepted" originating from of the receiving acquirer gateway arrives,

- If the sending gateway is an acquirer gateway, it shall wait for a valid Sign-off Response with Action Code "Accepted" originating from the receiving issuer gateway before communication may be terminated at application level. That is, the acquirer gateway shall continue processing response messages originating from the receiving issuer gateway until a valid Sign-off Response with Action Code "Accepted" originating from of the receiving issuer gateway arrives.

But if the sending gateway is an acquirer gateway, it shall stop sending other messages than repetitions of the Sign-off Request to the receiving issuer gateway after sending a Sign-off Request to the issuer gateway.

If the sending gateway does not receive a valid Sign-off Response after an appropriate number of Sign-off Requests, or if the sending gateway receives a valid Sign-off Response containing another Action Code than "Accepted", manual procedures shall be initiated by the sending gateway in order to get in contact with the respective receiving gateway directly and to terminate communication at the application level.

4 Message Structure

This section describes the structure of the ISO 8583 messages supported by acquirer and issuer gateways.

4.1 Notations

The attribute and format of message data elements are defined according to [ISO 8583:1993] and [ISO 13492] using the following abbreviations:

Abbreviation	Description
N	numeric digits
B	binary representation of data
A	alphabetical characters A through Z and a through z
P	pad character, space
An	alphabetical and numeric characters
Ans	alphabetical, numeric and special characters
Ansb	alphabetical, numeric, special characters and binary representation of data
Anp	alphabetical, numeric and space (pad) characters
LL	length of variable field that follows, coded in two numeric digits
LLL	length of variable field that follows, coded in three numeric digits
LLLL	length of variable field that follows, coded in four numeric digits
VAR	variable length field
3	fixed length of three characters (n, a, an, ans) or bytes (b)
..17	variable length up to maximum 17 characters (n, a, an, ans, z) or bytes (b)
Z	Track 2 code set as defined in ISO 7813

All fixed length numeric data elements are assumed to be right justified with leading zeros. All fixed length binary coded data elements are assumed to be left justified with trailing binary zeroes. All other fixed length data elements are left justified with trailing spaces.

The ASCII character set is used to code numeric digits, alphabetical characters and special characters.

Where a data element is composed of sub-fields:

- Sub-fields consist of a tag (n 3) and a length (n 3) and a value.
- Tags in the range 001 to 499 are reserved for definition by the Berlin Group specification, tags in the range 500 to 699 are reserved for definition by payment schemes, tags in the range 700 to 799 are reserved for bilateral/private definition, and tags in the range 800 to 999 are reserved for future use.
- Tags in the range 001 to 499 shall be unique within a data element.

- Tags in the range 500 to 699 shall be unique within a data element per payment scheme.
- The (maximum) length of the value fields shall be defined for the respective tag (in the respective data element).
- The format of the value fields shall be defined for the respective tag (in the respective data element).
- Sub-fields may appear in any order in a data element.
- Sub-fields with tags in the range 001 to 499 that are unknown to the receiver of a message shall be ignored.

The rules for the presence of a data element in a message are defined using the following abbreviations:

Abbreviation	**Description**
M	mandatory: data element must be present in a message and is set by the originator of the message
C	conditional: data element must be present in a message, if certain conditions are satisfied, and is set by the originator of the message
O	optional: data element is present at the discretion of the originator of the message; if present, the receiver of the message will process the data element
=	mirrored: data element must be present in a response message and must be set to the same value as contained in the respective request message; if the data element to be mirrored is optional or conditional in the respective request message, and if the respective request message does not contain the data element, the data element will not be contained in the response message
R	repeated: data element must be present in an advice and must be set to the same value as contained in the respective Authorisation Request; if the data element to be repeated is optional or conditional in the Authorisation Request, and if the respective Authorisation Request does not contain the data element, the data element will not be contained in the advice
-	data element is not present in a message

The abbreviation 142x stands for MTID 1420 and MTID 1421.

The abbreviation 112x stands for MTID 1120 and MTID 1121.

BMP is used as abbreviation for "bit map position".

BMP x is used as abbreviation for "data element at BMP x".

4.2 Transaction Messages

4.2.1 Overview

The following table gives an overview of the message structure of the transaction messages exchanged between acquirer gateway and issuer gateway:

1100 Authorisation Request

1110 Authorisation Request Response

1120 Authorisation Advice

1121 Authorisation Advice Repeat

1130 Authorisation Advice Response

1420 Reversal Advice

1421 Reversal Advice Repeat

1430 Reversal Advice Response

BMP	1100	1110	1120	1130	1420	1430	Name	Format	Attribute
	m	m	m	m	m	m	Message Type Identifier		n 4
	m	m	m	m	m	m	Primary Bit Map		b 8
1	c	c	c	c	c	c	Secondary Bit Map		b 8
2	m	=	r	=	r	=	Primary Account Number (PAN)	LLVAR	n..19
3	m	=	r	=	r	=	Processing Code		n 6
4	c	c	m	=	m	=	Amount, Transaction		n 12
6	c	c	c	=	c	=	Amount, Cardholder Billing		n 12
7	m	m	m	m	m	m	Date and Time, Transmission	MMDDhhmmss	n 10
10	c	=	c	=	r	=	Conversion Rate, Cardholder Billing		n 8
11	m	=	m	=	m	=	System Trace Audit Number (STAN)		n 6
12	m	=	m	=	m	=	Date and Time, Local Transaction	YYMMDDhhmmss	n 12
14	c	-	r	-	-	-	Date, Expiration	YYMM	n 4
22	m	-	-	-	-	-	POS Data Code		an 12
23	c	-	c	-	r	-	Card Sequence Number		n 3
24	m	-	m	-	m	-	Function Code		n 3
25	-	-	-	-	m	-	Message Reason Code		n 4
26	m	-	-	-	-	-	Card Acceptor Business Code		n 4
30	c	c	c	-	c	-	Amounts, Original		n 24
32	m	=	r	=	r	=	Acquiring Institution Identification Code	LLVAR	n..11
35	c	-	-	-	-	-	Track 2 Data	LLVAR	z..37
37	m	=	r	=	r	=	Retrieval Reference Number		anp 12
38	c	c	m	-	m	-	Approval Code		anp 6
39	-	m	-	m	-	m	Action Code		n 3
41	m	=	m	=	-	-	Card Acceptor Terminal Identification		ans 8
42	m	=	m	=	-	-	Card Acceptor Identification Code		ans 15

BMP	1100	1110	112x	1130	142x	1430	Name	Format	Attribute
43	m	-	m	-	r	-	Card Acceptor Name/Location	LLVAR	ans..56
48	m	-	r	-	r	-	Additional Data - Private	LLLVAR	ans..999
49	c	=	r	=	r	=	Currency Code, Transaction		n 3
51	c	=	r	=	r	=	Currency Code, Cardholder Billing		n 3
52	c	-	-	-	-	-	Personal Identification Number (PIN) Data		b 8
53	c	c	c	c	c	c	Security Related Control Information	LLVAR	b..48
54	c	c	c	-	c	-	Amounts, Additional	LLLVAR	ans..120
55	c	c	-	-	-	-	Integrated Circuit Card (ICC) System Related Data	LLLVAR	b..255
56	-	-	m	=	m	=	Original Data Elements	LLVAR	n..35
57	c	-	-	-	-	-	Authorisation Life Cycle Code		n 3
58	-	o	=	-	=	-	Authorising Agent Institution Identification Code	LLVAR	n..11
59	o	=	o	=	o	=	Acquirer Reference Data (Transport Data)	LLLVAR	ans..999
62	c	-	-	-	-	-	e-Payment and MOTO Data	LLLVAR	ansb..999
64	c	c	c	c	c	c	Message Authentication Code (MAC) Field		b 8
95	c	o	c	-	c	-	Card Issuer Reference Data	LLVAR	ans..99
111	c	c	c	c	c	c	Encryption Data	LLLLVAR	b..9999
128	c	c	c	c	c	c	Message Authentication Code (MAC) Field		b 8

The Advice Repeats are identical to the respective Advices with exception of the MTID and the values of BMP 53 and BMP 64 or BMP 128.

The messages belonging to the same transaction are uniquely identified as follows:

- System Trace Audit Number (STAN) in BMP 11 together with Date and Time, Local Transaction in BMP 12, and Acquiring Institution Identification Code in BMP 32 of the Authorisation Request must be unique.

- Authorisation Request and Authorisation Request Response must contain the same values in BMP 11, BMP 12 and BMP 32.

- Reversal Advice, Reversal Advice Repeat and Reversal Advice Response must contain in BMP 56 (Original Data Elements) the values of BMP 11, BMP 12 and BMP 32 defined in the respective Authorisation Request.

- In this way each message of a transaction can be uniquely identified by its MTID and the values of BMP 11, BMP 12 and BMP 32 defined for the transaction in the respective Authorisation Request.

Issuers should use the following message fields to match an Update Pre-Authorisation Request or a Completion Advice (Repeat) to the previous (Update) Pre-Authorisation Request:

- PAN in BMP 2,
- Acquiring Institution Identification Code in BMP 32,
- Approval Code in BMP 38,
- Retrieval Reference Number in BMP 37,
- Card Issuer Reference Data in BMP 95, if used by the issuer.

4.2.2 Data Element Description

In this section data elements contained in authorisation, advice or reversal messages are described in more detail where necessary.

Primary Bit Map

The Primary Bit Map is a series of 64 bits (8 bytes) used to identify the presence (denoted by 1) or the absence (denoted by 0) of the first 64 data elements, defined for a message in ISO 8583.

BMP 1: Secondary Bit Map

BMP 1 shall be present in a message if the message contains any fields from BMP 65 to BMP 128 (inclusive).

The Secondary Bit Map is a series of 64 bits (8 bytes) used to identify the presence (denoted by 1) or the absence (denoted by 0) of the data elements 65 through 128, defined for a message in ISO 8583.

BMP 2: Primary Account Number (PAN)

The Primary Account Number (PAN) is a series of digits used to identify a customer account or relationship. In case of data encryption in Dataset 3 of BMP 111 (see Table 10), the field contains only the BIN.

BMP 3: Processing Code

The Processing Code is a series of digits used to describe the effect of a transaction on the customer account and the account affected.

The Processing Codes used in the messages defined in this document are

00 00 00 for purchase of goods and services (Payments)

00 00 08 for a funds request for mobile top-up

01 00 00 for cash disbursement (ATM Cash Withdrawal and Cash Advance)

Note: BMP 26 is used to distinguish between ATM Cash Withdrawal and Cash Advance.

09 00 00 for purchase of goods and services (Payment) with Cashback

11 00 00 for Quasi Cash Payment

20 00 00 for Refund

28 00 00 for Original Credit

31 00 00 for Balance Inquiry

36 00 00 for Card Validity Check

90 00 08 Combined Funds Request/Top-Up

BMP 4: Amount, Transaction

- Authorisation Request:

  BMP 4 is **not** present in an Inquiry Request. In all other cases BMP 4 contains the value of the transaction in the transaction currency (indicated by the value of BMP 49).

  If the transaction is a Payment with Cashback, BMP 4 contains the total amount including the Payment amount and the Cashback amount. The Cashback amount is contained in BMP 54.

  If the transaction includes a Surcharge, BMP 4 contains the total amount including the transaction amount and the Surcharge amount. The Surcharge amount may be contained in BMP 54 depending on scheme rules.

  If the transaction is a Payment with Increased Amount (i.e. gratuity) where the additional amount is known at the time of authorisation, BMP 4 contains the total amount including the Payment amount and the additional amount (i.e. gratuity). It is recommended that the additional amount is contained in BMP 54.

- Authorisation Request Response:

  BMP 4 is **not** present in an Inquiry Request Response. In all other cases BMP 4 is filled as follows:

  - Approved transaction:

BMP 4 of the Authorisation Request Response contains the same transaction amount that was contained in BMP 4 of the Authorisation Request.

The Authorisation Request Response does not contain BMP 30.

If the transaction is a Payment with Cashback, BMP 4 contains the total amount including the Payment amount and the Cashback amount. The same Cashback amount that was contained in BMP 54 of the Authorisation Request is contained in BMP 54.

- Approved transaction for partial amount (Action Code 002, only in response to (Update) Pre-Authorisation Request):

  BMP 4 of the Authorisation Request Response contains the amount approved by the issuer which is less than the amount contained in BMP 4 of the (Update) Pre-Authorisation Request.

  BMP 30 of the Authorisation Request Response contains the original transaction amount contained in BMP 4 of the (Update) Pre-Authorisation Request.

- Approved transaction for Payment amount only (Action Code 080, only in response to Authorisation Request for Payment with Cashback):

  BMP 4 of the Authorisation Request Response contains the Payment amount approved by the issuer which is less than the amount contained in BMP 4 of the Authorisation Request (the difference being the Cashback amount in BMP 54 of the Authorisation Request).

  BMP 30 of the Authorisation Request Response contains the original transaction amount contained in BMP 4 of the Authorisation Request.

  The Cashback amount with value 0 is contained in BMP 54.

- Declined transaction:

  BMP 4 of the Authorisation Request Response contains the value 0.

  BMP 30 of the Authorisation Request Response contains the original transaction amount contained in BMP 4 of the Authorisation Request.

  If the transaction is a Payment with Cashback, the Cashback amount with value 0 is contained in BMP 54.

- Authorisation Advice:

  BMP 4 contains the final amount of the authorisation in the transaction currency (indicated by the value of BMP 49).

  If the transaction includes a Surcharge, BMP 4 contains the total amount including the transaction amount and the Surcharge amount. The Surcharge amount shall be contained in BMP 54 if (and only if) BMP 54 was present in the original Authorisation Request.

- Authorisation Advice Response:

  BMP 4 of the Authorisation Advice Response mirrors BMP 4 of the Authorisation Advice.

- Reversal Advice:

  BMP 4 of the Reversal Advice contains the amount to be reversed (= difference between approved or original transaction amount and final transaction amount) in the transaction currency.

  Partial Reversals are not allowed for

  - Payment with Cashback,
  - Payment with Increased Amount, and
  - Cancellations.

  - Full Reversal:

    BMP 4 of the Reversal Advice contains the approved amount, that is, the transaction amount contained in BMP 4 of the respective (most recent) Authorisation Request Response of the transaction to be reversed. Only if no or no correct Authorisation Request Response was received for the respective (most recent) Authorisation Request (indicated by the value 0 in BMP 38 of the Reversal Advice), BMP 4 of the Reversal Advice contains the transaction amount contained in BMP 4 of the respective (most recent) Authorisation Request.

    If the transaction is a Payment with Cashback, BMP 4 contains the total amount to be reversed which includes the Payment amount and the Cashback amount. The Cashback amount to be reversed is contained in BMP 54. This is the Cashback amount contained in BMP 54 of the respective (most recent) Authorisation Request Response of the transaction to be reversed. Only if no or no correct Authorisation Request Response was received for the respective (most recent) Authorisation Request (indicated by the value 0 in BMP 38 of the Reversal

Advice), BMP 54 of the Reversal Advice contains the Cashback amount contained in BMP 54 of the respective (most recent) Authorisation Request.

If the transaction is a Payment with Increased Amount, BMP 4 contains the total amount to be reversed which includes the Payment amount and the additional amount (i.e. gratuity). If the additional amount was present in BMP 54 of the Authorisation Request it must be present in BMP 54 of the Reversal Advice.

If the original transaction includes a Surcharge, BMP 4 contains the total amount to be reversed including the transaction amount to be reversed and the Surcharge amount to be reversed. The Surcharge amount to be reversed shall be contained in BMP 54 if (and only if) BMP 54 was present in the original Authorisation Request.

The Reversal Advice does not contain BMP 30.

- Partial Reversal:

  BMP 4 of the Reversal Advice contains the amount to be reversed in the transaction currency. The amount to be reversed shall be the difference between the approved amount (in BMP 4 of the (most recent) Authorisation Request Response of the transaction to be reversed) and the final transaction amount.

  If the original transaction includes a Surcharge, BMP 4 contains the amount to be reversed consisting of the transaction amount to be reversed and the Surcharge amount to be reversed. The Surcharge amount to be reversed shall be contained in BMP 54 if (and only if) BMP 54 was present in the original Authorisation Request.

  BMP 30 of the Reversal Advice contains the original approved transaction amount contained in BMP 4 of the Authorisation Request Response (which may be less than the transaction amount in BMP 4 of the Authorisation Request in the event of a partial approval or of a Payment with no Cashback approval).

- Reversal Advice Response:

  BMP 4 of the Reversal Advice Response mirrors BMP 4 of the Reversal Advice.

BMP 6: Amount, Cardholder Billing

BMP 6 is present, if and only if BMP 49 is present and the transaction currency is different from Euro. In this case the acquirer must convert the Amount, Transaction contained in BMP 4 to Euro.

The conversion rate used to compute Amount, Cardholder Billing from Amount, Transaction is contained in BMP 10.

Requirement:

> The conversion rate used to compute Amount, Cardholder Billing in the Reversal Advice must be the same as the conversion rate used to compute Amount, Cardholder Billing in the respective Authorisation Request.

BMP 7: Date and Time, Transmission

The gateway originating a request or advice or response message creates the Date and Time, Transmission. The content is the timestamp of the originating gateway in UTC (formerly known as GMT).

BMP 10: Conversion Rate, Cardholder Billing

BMP 10 is present, if and only if BMP 49 is present and the transaction currency is different from Euro.

In this case the acquirer must convert the Amount, Transaction contained in BMP 4 to Euro.

The Amount, Transaction (BMP 4) is multiplied by Conversion Rate, Cardholder Billing (BMP 10) to determine Amount, Cardholder Billing (BMP 6).

The leftmost digit of BMP 10 denotes the number of positions the decimal separator shall be moved from the right. Digits 2-8 of BMP 10 define the conversion rate without decimal separator. If digit 1 of BMP 10 has a value >= 7, it is assumed that the digit to the left of the decimal separator has the value 0. If digit 1 of BMP 10 has a value >= 8, it is assumed that the first (two) digit(s) to the right of the decimal separator has (have) the value 0.

Requirement:

> The conversion rate provided in the Reversal Advice must be the same as the conversion rate provided in the respective Authorisation Request.

BMP 11: System Trace Audit Number (STAN)

The STAN is a number used to identify a transaction uniquely together with the values of BMP 12 and 32 in the respective Authorisation Request (see section 4.2.1).

The STAN in BMP 11 together with Date and Time, Local Transaction in BMP 12, and Acquiring Institution Identification Code in BMP 32 shall be unique per two-message exchange, e.g. request/repeat and response.

The STAN shall remain unchanged for all messages within a two-message exchange.

The STAN shall never have the value 0.

BMP 12: Date and Time, Local Transaction

The local date and time at which the transaction takes place at the card acceptor location. For e-Payment and MOTO transactions this is the card acceptor's date and time. This data element is used to identify a transaction uniquely together with the values of BMP 11 and 32 in the respective Authorisation Request (see section 4.2.1).

The local date and time shall remain unchanged from card acceptor to issuer and shall be echoed in the responses.

Date and Time, Local Transaction in Reversal Advices should indicate the local date and time at which the reversal is generated. However, for reversals generated for technical reasons it is allowed to echo the Date and Time, Local Transaction of the original authorisation.

Date and Time, Local Transaction in Authorisation Advices and Update Pre-Authorisation Requests shall indicate the local date and time at which the advice or request is generated.

BMP 14: Date, Expiration

The year and month after which the card expires.

Date, Expiration must be present in the Authorisation Request, if the Track 2 Data in BMP 35 or BMP 111 is absent from the Authorisation Request. It may be absent from the Authorisation Request, if the Track 2 Data are present.

BMP 14 is present if the Date, Expiration is sent as plain text. In case of data encryption in Dataset 3 of BMP 111 (see Table 10), the field is not present.

BMP 22: POS Data Code

A series of 12 codes intended to identify terminal capability, terminal environment and presentation security data.

	Name	Description	Format
1	Card data input capability	Indicates the primary means of getting the information on the card into the terminal. 1 – Manual, no terminal 2 – Magnetic stripe read 5 – ICC 6 – Key entered 7 – Contactless	an1
2	Cardholder authentication capability	Indicates the primary means of verifying the cardholder at this terminal. 0 – No electronic identification 1 – PIN U – Secure e-Payment	an 1
3	Card capture capability	Indicates whether or not the terminal has the ability to capture a card. 0 – None 1 – Can capture	an 1
4	Operating environment	Indicates if the terminal is attended by the card acceptor and its location. 0 – No terminal used 1 – On premises of card acceptor - attended 2 – On premises of card acceptor - unattended 3 – Off premises of card acceptor - attended 4 – Off premises of card acceptor - unattended 5 – On premises of cardholder - unattended	an 1
5	Cardholder present	Indicates if the cardholder is present at the point of service. 0 – Cardholder present 2 – Cardholder not present, mail order 3 – Cardholder not present, telephone order 4 – Cardholder not present, standing authorisation 9 – Cardholder not present, e-Payment	an 1
6	Card present	Indicates if the card is present at the point of service or not. 0 - Card not present 1 - Card present	an 1
7	Card data input mode	Indicates method used to input the information from the card to the terminal. 1 – Manual, no terminal 2 – Magnetic stripe read 5 – ICC 6 – Key entered 7 – Contactless S – Magnetic stripe, fallback T – e-Payment U – MOTO	an1
8	Cardholder authentication method	Indicates the method for verifying the cardholder. 0 – Not authenticated 1 – PIN 5 – Manual signature verification 6 – Other manual verification (e.g. drivers license) U – Secure e-Payment	an 1
9	Cardholder authentication entity	Indicates the entity verifying the cardholder identity. 0 – Not authenticated 1 – ICC (for Offline-PIN) 3 – Authorising agent (for Online-PIN or e-Payment) 4 – By merchant (for signature)	an 1

	Name	Description	Format
10	Card data output capability	Indicates the ability of the terminal to update the card. 1 – None (for non EMV terminals) 3 – ICC (for EMV terminals)	an 1
11	Terminal output capability	Indicates the ability of the terminal to print/display messages. 0 – Unknown 1 – None 2 – Printing 3 – Display 4 – Printing and display	an 1
12	PIN capture capability	Indicates the length of PIN which the terminal is capable of capturing. 0 – No PIN capture capability 4-C – Four thru twelve digits	an 1

BMP 23: Card Sequence Number

A number distinguishing between separate cards with the same primary account number.

BMP 23 must be present in the Authorisation Request and Authorisation Advice, if the transaction is a chip based EMV transaction and the Card Sequence Number can be retrieved from the ICC from DO with tag '5F34' if the Card Sequence Number is sent as plain text.

BMP 23 shall also be present in the Update Pre-Authorisation Request and Authorisation Advice, if it was present in the first Pre-Authorisation Request and sent as plain text.

BMP 23 shall be present in the Reversal Advice, if it was present in the original Authorisation Request and sent in plain text.

In case of data encryption in Dataset 3 of BMP 111 (see Table 10), the field is not present.

BMP 24: Function Code

Code indicating the specific purpose of the message within its message class. The following Function Codes are used for the purposes of this specification:

100: Original authorisation - amount accurate

101: Original authorisation - amount estimated

103: Replacement authorisation - amount estimated

108: Inquiry

180: Completion of a previously approved authorisation

181: Recurring Payment

400: Full Reversal

401: Partial Reversal

BMP 25: Message Reason Code

Provides the receiver of the Reversal Advice with the reason of the Reversal as follows:

Code	Description
4000	Cancellation
4001	Unspecified Error
4002	System malfunction
4004	Completed partially
4005	Original amount incorrect
4007	Card acceptor device unable to complete transaction
4013	Unable to deliver message to point of service
4014	Suspected malfunction/card retained (ATM)
4015	Suspected malfunction/card returned (ATM)
4017	Suspected malfunction/no cash dispensed
4019	Timed-out taking card/card retained and no cash dispensed (ATM)
4021	Timeout waiting for response
4351	Card acceptor does not agree to partial approved amount

BMP 26: Card Acceptor Business Code

Code classifying the type of business being done by the card acceptor for this transaction according to ISO 18245:2003.

If the transaction is a cash disbursement, the following Card Acceptor Business Codes are to be used:

6011: Financial institution - Automated cash disbursements (ATM Cash Withdrawal)

6010: Financial institution - Manual cash disbursements (Cash Advance)

For POS transactions at petrol stations the following Card Acceptor Business Codes shall be used:

5541: Service stations

5542: Automated gasoline dispensers

For Funds Request for Top-Up or a Combined Funds Request/Top-Up the following Card Acceptor Business Code shall be used:

4814: Telco Service

BMP 30: Amounts, Original

The Amounts, Original data element consists of two data elements in fixed length format totalling 24 digits:

a) Original Amount, Transaction n 12

b) Original Amount, Reconciliation n 12, always set to 0

Original Authorisation Request and advice responses do not contain BMP 30.

The Update Pre-Authorisation Request always contains BMP 30, where the first 12 digits contain the approved transaction amount contained in BMP 4 of the most recent Authorisation Request Response.

The Authorisation Request Response contains BMP 30, if:

- The transaction is declined or
- The transaction is approved for a partial amount (Action Code 002) or
- The transaction is approved for Payment amount only (Action Code 080, only in response to Authorisation Request for Payment with Cashback)..

In this case the first 12 digits of BMP 30 of the Authorisation Request Response contain the original transaction amount contained in BMP 4 of the Authorisation Request.

The Authorisation Advice contains BMP 30, if and only if the final amount is less than the previously approved amount. In this case the first 12 digits of BMP 30 of the Authorisation Advice contain the approved transaction amount contained in BMP 4 of the most recent Authorisation Response.

The Reversal Advice contains BMP 30, if and only if it is a partial Reversal. In this case the first 12 digits of BMP 30 of the Reversal Advice contain the approved original transaction amount contained in BMP 4 of the (most recent) Authorisation Request Response.

BMP 32: Acquiring Institution Identification Code

Code identifying the acquiring institution or its agent.

This data element is used to identify a transaction uniquely together with the values of BMP 11 and 12 in the respective Authorisation Request (see section 4.2.1).

For the purposes of this specification the Acquiring Institution Identification Code is a numeric value of variable length structured as follows:

# of Digits	Description
3	Numeric country code according to ISO 3166 identifying the country of the acquirer gateway
2	2-digits number identifying the acquirer gateway, assigned to the acquirer gateway by the community of the gateways in the country identified by digits 1-3
1-6	Number of variable length (1-6 digits) identifying the acquirer, assigned to the acquirer by the acquirer gateway identified by digits 1-5

BMP 35: Track 2 Data

The Track 2 Data are sent as plain text in BMP 35 or in encrypted form in Dataset 3 of BMP 111 (see Table 10).

The Track 2 Data must be present in the Authorisation Request, if the magnetic stripe or the chip of the card was read for the transaction. The Track 2 Data may only be absent from the Authorisation Request for e-Payment and MOTO transactions (identified by the respective value of Position 7 of BMP 22) or from the Update Pre-Authorisation Request if it is a card not present transaction.

For magnetic stripe based transactions:

> The information encoded on track 2 of the magnetic stripe as specified in ISO 7813, excluding beginning and ending sentinels and longitudinal redundancy check characters as defined therein.

For chip based transactions:

> Data element "Track 2 equivalent data" identified by tag '57', excluding pad characters, when present.

BMP 37: Retrieval Reference Number

A reference supplied by the system retaining the original transaction information (usually the card acceptor) and used to assist in locating that information or a copy thereof.

The Retrieval Reference Number must remain unchanged in all messages of Pre-Authorisation Services, Deferred Payments and Recurring Payments.

BMP 38: Approval Code

- Authorisation Request:

  The Approval Code is only present in Update Pre-Authorisation Requests. In this case it contains the Approval Code received in the most recent Authorisation Request Response.

- Authorisation Request Response:

  The Approval Code is only present in the Authorisation Request Response, if approved. In this case the code is assigned by the authorising institution indicating approval.

- Authorisation and Reversal Advice:

  Approval Code received in the respective (most recent) Authorisation Request Response.

  000000, if no or no correct Authorisation Request Response was received.

BMP 39: Action Code

The following Action Codes are used in Authorisation Request Response (1110), Authorisation Advice Response (1130) and/or Reversal Advice Response (1430):

Code	1110	1130	1430	Description
000	x	-	-	Approved
002	x	-	-	Approved for partial amount (only for response to a (Update) Pre-Authorisation Request)
080	x	-	-	Approved for Payment Amount Only, No Cashback Allowed (only for Payment with Cashback)
100	x	-	-	Do not honour
101	x	-	-	Expired card
104	x	-	-	Restricted card

Code	1110	1130	1430	Description
106	x	-	-	Allowable number of PIN tries exceeded
107	x	-	-	Refer to card issuer
109	x	-	-	Invalid merchant
110	x	-	-	Invalid (zero) amount
110	-	-	x	Original amount incorrect
111	x	-	-	Invalid card number (no such number)
115	x	-	-	Requested Function not supported
116	x	-	-	Not sufficient funds
117	x	-	-	Incorrect PIN
118	x	-	-	No card record
119	x	-	-	Transaction not permitted to cardholder
120	x	-	-	Transaction not permitted to terminal
121	x	-	-	Exceeds withdrawal amount limit
123	x	-	-	Exceeds withdrawal frequency limit
125	x	-	-	Card not effective
129	x	-	-	Suspected counterfeit card
180	x	-	-	Issuer does not agree to transaction conditions (only for response to (Update) Pre-Authorisation Request)
181	x	-	-	Validity period expired (only for response to Update Pre-Authorisation Request)
182	x	-	-	Mobile Phone Number unknown for selected Telco
183	x	-	-	Mobile Phone Account cannot be loaded
184	x	-	-	EMV data inconsistent (e.g. DE 55 vs. DE 4, parts of DE 3)
185	x	-	-	Fallback transactions not permitted for this service by issuer
200	x	-	-	Pick up
201	x	-	-	Expired card, Pick up
204	x	-	-	Restricted card, Pick up
206	x	-	-	Allowable PIN tries exceeded, Pick-up
208	x	-	-	Lost card, Pick-up
209	x	-	-	Stolen card, Pick-up
400	-	-	x	Accepted
480	-	-	x	Mobile Phone Top-Up completed successfully, reversal not possible
900	-	x	-	Accepted
902	x	x	x	Invalid transaction (not used for ATM transactions)
904	x	x	x	Format Error
905	x	x	-	Acquirer not supported by switch
907	x	-	-	Issuer or switch is inoperative
908	x	x	x	Transaction destination cannot be found for routing
909	x	x	x	System malfunction
910	x	-	-	Card issuer signed off
911	x	-	-	Time out of issuer response

Code	1110	1130	1430	Description
912	x	-	-	Card issuer unavailable
913	x	x	x	Duplicate transmission
914	x	x	x	Not able to trace back to original transaction
940	x	-	-	Mobile Phone Top-Up result unknown
941	x	-	-	Telco not available for Mobile Top-Up

Action Codes requiring pick up shall only be used, if the value of BMP 22 in the respective Authorisation Request shows card capture capability of the terminal.

The Referral Action Code (107) requires completing the transaction with a voice conversation to obtain an approval code. This Function involves neither the card nor the cardholder.

Remark: Note that for a Combined Funds Request/Top-Up Reversal Message, an Action Code "400" does not necessarily imply that the transaction is finally reversed with the mobile operator, due to the store-and-forward principle used for reversals.

BMP 41: Card Acceptor Terminal Identification

Unique code identifying a terminal at the card acceptor's location, assigned by the card acceptor.

BMP 42: Card Acceptor Identification Code

Code identifying the card acceptor, assigned by the acquirer.

BMP 43: Card Acceptor Name/Location

According to this specification the card acceptor name/location field shall be structured according to the definition in section 4.4.1 of ISO 8583:1993 and shall comply with the following additional requirements:

- The data element "Street" shall not be used.
- The length of the concatenation "Card Acceptor Name\\City\" shall not exceed 40 characters.

Thus BMP 43 shall be structured as follows:

Description	**Format**
Card Acceptor Name	ans..40
"\\"	
City	
"\"	
Postal Code	ans 10
Region	ans 3
Alpha Country Code according to ISO 3166	a 3

Note:

- A postal code with less than 10 characters is left adjusted with trailing blanks.
- If no postal code or region is used, the respective data element is filled with blanks.
- If the length of the concatenation of the original card acceptor name and city exceeds 37 characters, the acquirer or acquirer gateway has to truncate the original card acceptor name and/or city in order to meet the requirements for BMP 43 according to this specification. This specification does not define a specific method for truncation.

BMP 48: Additional Data – Private

BMP 48 consists of one or more sub-fields as defined in the following table.

Tag	Attribute	Presence	Description
001	an..8	m	**Accepting Brand**: "EAPS" Euro Alliance of Payment Schemes "VPAY" V PAY "PLUS° Plus "VISA" Visa "MSI" Maestro "MCC" MasterCard "DMC" Debit MasterCard "CIR" Cirrus "JCB" JCB Additional values may be defined as required
002	n..18	c	**Mobile Phone Data:** Domestic mobile number Usage Rule: Mandatory for Mobile Phone Top-Up related messages (Funds Request or Combined Funds Request/Top-up)
003	n5	c	**Mobile Phone Operator ID** Country Code plus 2 digits Operator ID Usage Rule: Mandatory for Mobile Phone Top-Up related messages (Funds Request or Combined Funds Request/Top-up)
004	an..8	o	**Mobile Phone Operator Approval Code** Additional to the Action Code of the Card Issuer in BMP39, the Approval Code of the Mobile Operator might be transported in case of Combined Funds Request/Top-Up Authorisation Response Messages, if available

BMP 49: Currency Code, Transaction

Not present for Inquiries. Otherwise, a code indicating the local currency of the acquirer or the currency used at the source location of the transaction. This currency is used in Amount, Transaction (BMP 4).

BMP 51: Currency Code, Cardholder Billing

BMP 51 is present, if and only if BMP 6 is present, that is, if the transaction currency is different from Euro. In this case BMP 51 must have the value 978 for Euro.

BMP 52: Personal Identification Number (PIN) Data

Used to identify the cardholder at the point of service (in accordance with ISO 9564-1).

BMP 52 must be present in the Authorisation Request for magnetic stripe based transactions if cardholder authentication is not performed via signature and Triple-DES is used as cryptographic algorithm for the encipherment.

BMP 52 must be present in the Authorisation Request for chip based transactions, if the cardholder verification method performed for the transaction is Online PIN and Triple-DES is used as cryptographic algorithm for the encipherment.

BMP 52 is absent from the Authorisation Request in all other cases.

If present, BMP 52 contains the enciphered PIN Block.

PIN Block Format, cryptographic algorithms and related parameters, as well as the cryptographic key that are used for PIN encipherment are indicated by the value of BMP 53.

BMP 53: Security Related Control Information

Identifies security management information used in the current transaction.

BMP 53 must be present in all Interchange Messages for a transaction if and only if Triple-DES is used as cryptographic algorithm for the computation of the PINBLOCK in BMP 52 and/or MAC in BMP 64 or BMP 128.

Structure, contents, and usage of BMP 53 are defined in section 2 of [BG SEC].

BMP 54: Amounts, Additional

BMP 54 shall contain amount information for

- Payments with Cashback (Processing Code 09 00 00, see BMP 3),
- Balance Inquiries (Processing Code 31 00 00, see BMP 3),
- Unsolicited Available Funds - Balance Information in Authorisation Request Responses.

It is recommended that BMP 54 contains the additional amount information for Payments with Increased Amount (i.e. when a gratuity is added before authorisation).

Depending on scheme rules, transactions that are surcharged (i.e. charge to be paid by the cardholder) may have the Surcharge amount specified in BMP 54.

If the transaction is a Payment with Cashback BMP 54 shall be present in the Authorisation Request, Authorisation Request Response and Reversal Advice (Repeat) used to process the Payment with Cashback and contain information on the Cashback amount.

If the transaction is a Payment with Increased Amount BMP 54 may be present in the Authorisation Request. If BMP 54 was present in the Authorisation Request it must be present in the Reversal Advice (Repeat) and contain additional amount information.

If the transaction is surcharged and the Surcharge amount is present in BMP 54 of the Authorisation Request, BMP 54 must be present in all subsequent request/repeat/advice messages used to process the transaction and contain information on the Surcharge amount.

Note:

BMP 54 may contain the details of one or more amounts.

If the transaction is a Balance Inquiry BMP 54 is present in the Authorisation Request Response and contains information on one or more Balance Amount(s).

Optionally Authorisation Request Responses may include BMP 54 to convey one or more Balance Amount(s) to provide Unsolicited Available Funds under the following conditions:

- Insufficient funds (action code 116),
- Transaction would exceed limits (action code 121),
- Balance information on an approved transaction.

Table 5 summarises under which condition BMP 54 is present in a message type that is used to process a transaction.

MTID	Message Type	Presence of BMP 54
1100	Authorisation Request	If Payment with Cashback and/or optionally transaction with Surcharge and/or optionally Payment with Increased Amount
1110	Authorisation Request Response	If Balance Inquiry or return of balance information for Unsolicited Available Funds or Payment with Cashback
1120/ 1121	Authorisation Advice Authorisation Advice Repeat	If transaction with Surcharge and BMP 54 present in the original Authorisation Request
1130	Authorisation Advice Response	Never
1420/ 1421	Reversal Advice Reversal Advice Repeat	If present in (original) Authorisation Request
1430	Reversal Advice Response	Never

Table 5: Conditions for the Presence of BMP 54 by Message Type

Note:

The Debit-/Credit-Indicator sub-element in an amount information is used in the following way:

- Balance amount information: "C" indicates a positive balance and "D" indicates a negative balance.
- Transaction related amount information: "C" indicates a credit to the cardholder account and "D" indicates a debit to the cardholder account.

If present in BMP 54, the Cashback amount and/or the Surcharge amount are included in the transaction amount in BMP 4 and - if the transaction currency is different from Euro - in Amount, Cardholder Billing in BMP 6.

Cashback Amount Information:

For a Payment with Cashback BMP 54 always contains information on the Cashback amount in transaction currency, which is a set of values with a length of 20 characters structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Amount Type "Cash"	40	n 2
Currency Code	Currency code of the transaction currency	as in BMP 49	n 3
Debit-/Credit-Indicator	Debit-Indicator	"D"	a 1
Amount, Cashback	Cashback amount in transaction currency		n 12

If and only if the transaction currency is different from Euro BMP 54 contains in addition information on the Cashback amount in Euro, which is a set of values with a length of 20 characters structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Amount Type "Cash"	40	n 2
Currency Code	Currency code of Euro	as in BMP 51	n 3
Debit-/Credit-Indicator	Debit-Indicator	"D"	a 1
Amount, Cashback	Cashback amount in Euro		n 12

If the transaction currency is different from Euro, the acquirer must convert the Amount, Cashback in transaction currency to Euro.

The conversion rate used to compute Amount, Cashback in Euro from Amount, Cashback in transaction currency is contained in BMP 10.

Note:

Partial Reversals are not allowed for Payment with Cashback.

Additional Amount Information:

For a Payment with Increased Amount (i.e. gratuity) it is recommended that BMP 54 contains information on the additional amount in transaction currency, which is a set of values with a length of 20 characters structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Amount Type "Gratuity"	60	n 2
Currency Code	Currency code of the transaction currency	as in BMP 49	n 3
Debit-/Credit-Indicator	Debit-Indicator	"D"	a 1
Amount, Additional	Additional amount in transaction currency		n 12

If and only if the transaction currency is different from Euro BMP 54 contains in addition information on the additional amount in Euro, which is a set of values with a length of 20 characters structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Amount Type "Gratuity"	60	n 2
Currency Code	Currency code of Euro	as in BMP 51	n 3
Debit-/Credit-Indicator	Debit-Indicator	"D"	a 1
Amount, Additional	Additional amount in Euro		n 12

If the transaction currency is different from Euro, the acquirer must convert the Amount, Additional in transaction currency to Euro.

The conversion rate used to compute Amount, Additional in Euro from Amount, Additional in transaction currency is contained in BMP 10.

Note:

Partial Reversals are not allowed for Payment with Increased Amount.

Surcharge Amount Information:

For a transaction with Surcharge BMP 54 may (depending on scheme rules) contain information on the Surcharge amount in transaction currency, which is a set of values with a length of 20 characters structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Amount Type "Surcharge"	42	n 2
Currency Code	Currency code of the transaction currency	as in BMP 49	n 3
Debit-/Credit-Indicator	Debit-Indicator	"D"	a 1
Amount, Surcharge	Surcharge amount in transaction currency		n 12

If and only if the transaction currency is different from Euro BMP 54 also contains additional information on the Surcharge amount in Euro, which is a set of values with a length of 20 characters structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Amount Type "Surcharge"	42	n 2
Currency Code	Currency code of Euro	as in BMP 51	n 3
Debit-/Credit-Indicator	Debit-Indicator	"D"	a 1
Amount, Surcharge	Surcharge amount in Euro		n 12

If the transaction currency is different from Euro, the acquirer must convert the Amount, Surcharge in transaction currency to Euro.

The conversion rate used to compute Amount, Surcharge in Euro from Amount, Surcharge in transaction currency is contained in BMP 10.

Where some/all of a surcharge is to be refunded to a cardholder in the event of a Reversal and the original Surcharge amount was specified in BMP 54 of the Authorisation Request, the amended Surcharge Amount (which could be zero where the Surcharge Amount is to be refunded in full) shall be contained in BMP 54 of a Reversal Advice.

If the transaction currency is different from Euro, the conversion rate used to compute the Euro Surcharge amount in the Reversal Advice must be the same as the conversion rate used to compute the Euro Surcharge amount in the respective Authorisation Request.

Balance Amount Information:

For Balance Inquiry and Unsolicited Available Funds BMP 54 consists of one or more set(s) of values with a length of 20 characters each, structured as follows:

Sub-Element	Description	Value	Attribute
Account Type	As defined in positions 3 and 4 or 5 and 6 of BMP 3	00	n 2
Amount Type	Account Ledger Balance	01	n 2
	Account Available Balance	02	
	Amount Remaining this Cycle	20	
Currency Code	Currency code of the Balance Amount		n 3
Debit-/Credit-Indicator	Credit-Indicator (positive Balance)	"C"	a 1
	Debit-Indicator (negative Balance)	"D"	
Balance Amount			n 12

BMP 55: ICC System Related Data

BMP 55 must be present in the Authorisation Request, if the transaction is a chip based transaction (identified by the respective value of Position 7 of BMP 22) except for Refund, Original Credit or Cancellation transactions.

BMP 55 may be present in the Authorisation Request Response for chip based transactions at the issuer's discretion except for Refund, Original Credit or Cancellation transactions.

For chip based transactions BMP 55 shall be TLV coded, where the data objects listed in Table 6 may or shall be carried in BMP 55:

Data Object	Tag	Length (in Byte)	Format	Presence	
				1100	1110
AIP	'82'	'02'	b 2	m	
DF-Name	'84'	up to '10'	b..16	o	
TVR	'95'	'05'	b 5	m	
Transaction Date	'9A'	'03'	n 6 YYMMDD	m	

Data Object	Tag	Length (in Byte)	Format	Presence	
				1100	1110
Transaction Type	'9C'	'01'	n 2	m	
Transaction Currency Code	'5F2A'	'02'	n 3	m	
Amount, Authorised	'9F02'	'06'	n 12	m	
Amount, Other	'9F03'	'06'	n 12	c[1)]	
Terminal Application Version Number	'9F09'	'02'	b 2	o	
Issuer Application Data	'9F10'	up to '20'	b..32	c[2)]	
Terminal Country Code	'9F1A'	'02'	n 3	m	
IFD Serial Number	'9F1E'	'08'	an 8	o	
Application Cryptogram (AC)	'9F26'	'08'	b 8	m	
Cryptogram Information Data (CID)	'9F27'	'01'	b 1	o	
Terminal Capabilities	'9F33'	'03'	b 3	o	
CVM Results	'9F34'	'03'	b 3	o	
Terminal Type	'9F35'	'01'	n 2	o	
ATC	'9F36'	'02'	b 2	m	
Unpredictable Number	'9F37'	'04'	b 4	m	
Transaction Sequence Counter	'9F41'	'02' - '04'	n..8	o	
Issuer Authentication Data	'91'	'08' -'10'	b..16		o
Issuer Script Template 1	'71'	up to '7E'	b..126		o
Issuer Script Template 2	'72'	up to '7E'	b..126		o

Table 6: Data objects contained in BMP 55

Data objects that are present in BMP 55 but not listed in Table 6 shall not be considered as invalid message syntax or format by the receiver, provided the TLV coding of BMP 55 is correct.

Data objects that are present in BMP 55 but not listed in Table 6:

- may be processed by the receiver of the message if sender and receiver of the message have bilaterally agreed how to process these data objects,
- or shall be ignored by the receiver of the message.

1) Mandatory for Cashback transactions, when provided by the terminal

2) Mandatory, when provided by the ICC

BMP 56: Original Data Elements

Concatenation of the following four data elements contained in the most recent Authorisation Request:

Description	Source, Value	Format	Attribute
Original MTID	1100		n 4
Original STAN	BMP 11 of the Authorisation Request		n 6
Original Date and Time, Local Transaction	BMP 12 of the Authorisation Request		n 12
Original Acquirer Institution Identification Code	BMP 32 of the Authorisation Request	LLVAR	n..11

BMP 57: Authorisation Life Cycle Code

In Pre-Authorisation Services, BMP 57 shall be present in Pre-Authorisation Requests and Update Pre-Authorisation Requests.

In Deferred Payments, BMP 57 may be present in Pre-Authorisation Requests.

If present, BMP 57 contains a value in calendar days, hours or minutes which defines the time period for which the acquirer is requesting guarantee of funds, i.e. the validity period for a Pre-Authorisation or Update Pre-Authorisation. BMP 57 is structured as follows:

Name	Description	Value	Attribute
Time Code	Calendar Days	1	n 1
	Hours	2	
	Minutes	3	
Time Interval	A numeric value indicating the number of reiterations indicated by the Time Code	01-99	n 2

BMP 58: Authorising Agent Institution Identification Code

BMP 58 may be present in the Authorisation Request Response, if the authorising agent is different from the issuer, identified by the BIN of the PAN. In this case the Authorising Agent Institution Identification Code contained in BMP 58 is a numeric value of variable length structured in analogy to BMP 32:

# of Digits	Description
3	Numeric country code according to ISO 3166 identifying the country of the issuer gateway
2	2-digits number identifying the issuer gateway, assigned to the issuer gateway by the community of the gateways in the country identified by digits 1-3
1-6	Number of variable length (1-6 digits) identifying the authorising agent, assigned to the authorising agent by the issuer gateway identified by digits 1-5

Once received, the Authorising Agent Institution Identification Code must remain unchanged in all subsequent messages of a multi step transaction.

BMP 59: Acquirer Reference Data (Transport Data)

BMP 59 may be present in any request or advice message at the acquirer's discretion. If present it contains data that the acquirer requires to be returned unaltered in the related response message. The contents are not defined by this specification.

For this specification the length of BMP 59 is restricted to a maximum of 100 characters.

BMP 62: e-Payment and MOTO Data

BMP 62 must be present in an Authorisation Request, if and only if the transaction is an e-Payment or MOTO transaction (identified by the respective value of Position 7 of BMP 22).

BMP 62 consists of one or more sub-fields as defined in the following table.

Tag	Attribute	Presence	Description
001	n 3	m	**Security Level** Sequence of two digits indicating the security level of the e-Payment or MOTO transaction: Digit 1: 0 No security protocol 1 Channel encrypted (e.g. SSL) 2-9 RFU Note - This shall be set to 0 for MOTO transactions Digit 2: 0 Cardholder/card authentication not performed though supported by card acceptor 1 Cardholder/card authentication not supported by card acceptor 2 Cardholder/card authentication supported by card acceptor but not supported by card issuer 3 Cardholder/card authentication data present 4-9 RFU Note - This shall be set to 0 for MOTO transactions Digit 3: 0 CVV2/CVC2/4DBC not provided by card acceptor 1 CVV2/CVC2/4DBC present 2 CVV2/CVC2/4DBC is on the card but is illegible 3 Cardholder states that the card has no CVV2/CVC2/4DBC
002	n..4	c	CVV2/CVC2/4DBC value; sent as plain text in this field or in encrypted form in Dataset 3 of BMP 111 (see Table 10).
003	b..40	c	Cardholder/card authentication data, binary format; sent as plain text in this field or in encrypted form in Dataset 3 of BMP 111 (see Table 10).
004	ans..40	c	Cardholder/card authentication data, alphanumeric format

BMP 64: MAC

BMP 64 shall be present in a message if the message does **not** contain any fields from BMP 65 to BMP 127 (inclusive).

Used to validate the source and the contents of the message between the sender and receiver.

Currently 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. It has to be ensured, that the bit indicating the presence of BMP 64 is set in the Primary Bit Map before the calculation of the MAC.

BMP 53 indicates padding mechanism, cryptographic algorithms and related parameters, and key that are used for MAC calculation.

BMP 95: Card Issuer Reference Data

BMP 95 may be present in the Authorisation Request Response at the issuer's discretion. If present it contains data that the issuer requires to be present in the related Clearing Presentment. The contents are not defined by this specification.

If BMP95 is received in the Authorisation Request Response it shall be present in related:

- Update Pre-Authorisation Request, if received in the original Authorisation Request Response for a Pre-Authorisation Request,
- Authorisation Advice (Repeat) and/or
- Reversal Advice (Repeat).

BMP 111: Encryption Data

BMP 111 shall be present in a message if and only if AES is used as cryptographic algorithm for the computation of the PINBLOCK in Dataset 01, the MAC in BMP 128 and/or the encrypted transport of other data in Dataset 03.

The PIN-Parameter in Dataset 01 (BMP 111.2) and the MAC-Parameter in Dataset 02 (BMP 111.3) contain security related control information and encryption parameters for AES-based PIN-Encryption and MAC-Calculation, which are present in BMP 53 if Triple-DES is used as cryptographic algorithm.

BMP	Length (in Byte)	For-mat	Field Name	Content
111	(41+/99+)		Encryption Data	Dataset(s) according to [ISO 13492]
111.1	4	NUM	Length field	'F0 F0 F3 F7' or 'F0 F0 F9 F5' or VAR
111.2	58	b	Dataset 01	PIN-Parameter and PAC
111.3	37	b	Dataset 02	MAC-Parameter
111.4	VAR	b	Dataset 03	Data Encryption

The Length field in BMP 111.1 shall contain the length in bytes of the dataset:

- The length field of the datasets contains 95 Byte in Authorisation Requests, if the cardholder verification method performed for the transaction is Online PIN.
- Otherwise the dataset has a length of 37 Byte in all other messages using the cryptographic algorithm AES for MAC computation.

If other encrypted data is present in BMP 111 the length of the Dataset 03 is added.

The composite datasets are constructed as specified in Clause 5.4.4 of [ISO 8583-1:2003]. Each dataset consists of a 1 Byte binary coded dataset identifier, a two Byte long binary coded length component and a list of TLV coded data objects:

Dataset Identifier	**Description**	**Dataset Length** (in Byte)	**TLV-coded Data Objects**
'01'	Dataset 01	'00 37'	see Table 8
'02'	Dataset 02	'00 22'	see Table 9
'03'	Dataset 03	VAR	see Table 10

Table 7: Structure of Dataset 01 und 02

Table 8 contains the data objects, which are present in Dataset 01 for PIN encryption according to [ISO 13492] using the UKPT derivation method:

Tag	**Length** (in Byte)	**Format**	**Field name**	**Content**	**Description**
'80'	'01'	b	Control	'03'	Identifies the key management scheme Unique Key per Transaction (UKPT)
'81'	'04'	BCD	Key Set Identifier	'*id wv* 00 00'	Key ID *id* of the Master Key Key Version *wv* of the Master Key RFU ('00 00')
'82'	'10'	b	Derived Information	'hh..hh'	Random Value RND_{PAC} for PIN Block Encryption session key derivation (binary)
'83'	'01'	BCD	Algorithm	'05'	Value for the algorithm AES
'84'	'02'	BCD	Key Length in Bytes	'00 32'	Length of the PIN Block Encryption session key
'87'	'01'	BCD	PIN Block Format	'04'	ISO-Format 4
'88'	'10'	b	PIN Block	'hh..hh'	ISO-Format 4 PIN-Block (PAC)

Table 8: Data objects in Dataset 01

In Table 9 contains the data objects, which are present in Dataset 02 for MACing according to [ISO 13492] using the UKPT derivation method.

Tag	**Length** (in Byte)	**Format**	**Field name**	**Content**	**Description**
'80'	'01'	b	Control	'03'	Identifies the key management scheme Unique Key per Transaction (UKPT)
'81'	'04'	BCD	Key Set Identifier	'*id wv* 00 00'	Key ID *id* of the Master Key Key Version *wv* of the Master Key RFU ('00 00')
'82'	'10'	b	Derived Information	'hh..hh'	Random Value RND_{MAC} for Message Security session key derivation (binary)
'83'	'01'	BCD	Algorithm	'06'	Value for the algorithm CMAC
'84'	'02'	BCD	Key Length in Bytes	'00 32'	Length of the AES-Sessionkey for MACing

Table 9: Data objects in Dataset 02

Table 10 contains the data objects, which are present in Dataset 03 for Data Encryption according to [ISO 13492] using the UKPT derivation method for host to host communication.

Tag	Length (in Byte)	Format	Field name	Content	Description
'80'	'01'	b	Control	'03'	Identifies the key management scheme Unique Key per Transaction (UKPT)
'81'	'04'	BCD	Key Set Identifier	'*id wv* 00 00'	Key ID *id* of the Master Key Key Version *wv* of the Master Key RFU ('00 00')
'82'	'10'	b	Derived Information	'hh..hh'	Random Value RND_{ENC} for the data encryption session key derivation (binary)
'83'	'01'	BCD	Algorithm	'06'	Value for the algorithm CMAC
'84'	'02'	BCD	Key Length in Bytes	'00 32'	Length of the AES-Sessionkey for data encryption
'87'	'01'	BCD	Padding method	'02'	Padding method used to fill all encrypted data to 16 Byte blocks, Mode 2 of ISO/IEC 9797-1
'8A'	'10'	b	Encrypted PAN	-	AES encryption of the PAN padded to 16 Byte
'8B'	'10'	b	Encrypted Card Sequence Number	-	AES encryption of the Card Sequence Number padded to 16 Byte
'8D'	'20'	b	Encrypted Track 2 Data	-	AES CBC encryption of the Track 2 Data padded to 32 Byte
'8F'	'10'	b	Encrypted Card Verification Data	-	AES encryption of the Card Verification Data (CVV2/CVC2/4DBC) padded to 16 Byte
'90'	'10'	b	Encrypted Expiration Date	-	AES encryption of the Date, Expiration padded to 16 Byte
'F1'	VAR	b	Encrypted Cardholder/card authentication data	-	AES CBC encryption of the Cardholder/card authentication data in binary format

Table 10: Data objects in Dataset 03

More details for BMP 111 are defined in section 3 of [BG SEC].

BMP 128: MAC

BMP 128 shall be present in a message if the message contains any fields from BMP 65 to BMP 127 (inclusive).

Used to validate the source and the contents of the message between the sender and receiver.

Currently 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. It has to be ensured, that the bit indicating the presence of BMP 128 is set in the Secondary Bit Map before the calculation of the MAC.

BMP 53 indicates padding mechanism, cryptographic algorithms and related parameters, and key that are used for MAC computation if and only if Triple-DES is used as cryptographic algorithm.

BMP 111 indicates padding mechanism, cryptographic algorithms and related parameters, and key that are used for MAC computation if and only if AES is used as cryptographic algorithm.

4.3 Network Management Messages

4.3.1 Overview

The following table gives an overview of the message structure of network management messages exchanged between acquirer gateway and issuer gateway.

BMP	1804	1814	Name	Format	Attribute
	m	m	Message Type Identifier		n 4
	m	m	Primary Bit Map		b 8
1	m	m	Secondary Bit Map		b 8
11	m	=	System Trace Audit Number (STAN)		n 6
12	m	=	Date and Time, Local Transaction	YYMMDDhhmmss	n 12
24	m	-	Function Code		n 3
25	m	-	Message Reason Code		n 4
39	-	m	Action Code		n 3
53	c	c	Security Related Control Information	LLVAR	b..48
93	m	=	Transaction Destination Institution Identification Code	LLVAR	n 5
94	m	=	Transaction Originator Identification Code	LLVAR	n 5
111	c	c	Encryption Data	LLLLVAR	b..9999
128	m	m	Message Authentication Code (MAC) Field		b 8

4.3.2 Data Element Description

In this section the data elements contained in network management messages are described in more detail where necessary.

Primary Bit Map

The Primary Bit Map is a series of 64 bits (8 bytes) used to identify the presence (denoted by 1) or the absence (denoted by 0) of the first 64 data elements, defined for a message in ISO 8583.

BMP 1: Secondary Bit Map

The Secondary Bit Map is a series of 64 bits (8 bytes) used to identify the presence (denoted by 1) or the absence (denoted by 0) of the data elements 65 through 128, defined for a message in ISO 8583.

BMP 11: System Trace Audit Number (STAN)

The STAN is a number assigned by the sender of a Network Management Request (identified by the value of BMP 94) in a way that a network management dialogue is identified uniquely together with the values of BMP 12 and 94 in the respective Network Management Request.

The STAN shall never have the value 0.

The STAN contained in a Network Management Request is mirrored in the respective Network Management Request Response.

BMP 12: Date and Time, Local Transaction

The local date and time at which the network management dialogue is initiated at the acquirer gateway or issuer gateway.

This data element is used to identify a network management dialogue uniquely together with the values of BMP 11 and 94 in the respective Network Management Request.

BMP 24: Function Code

Code indicating the specific purpose of the message within its message class. The following Function Codes are used for the purposes of this specification in Network Management Requests:

801: Sign-on

802: Sign-off

831: Echo-Test

BMP 25: Message Reason Code

The following Message Reason Codes are used in Network Management Requests (1804):

8600: Request sent by acquirer gateway

8601: Request sent by issuer gateway

BMP 39: Action Code

The following Action Codes are used in Network Management Request Responses (1814):

Code	Description
800	Accepted
904	Format Error
909	System malfunction
913	Duplicate transmission

BMP 53: Security Related Control Information

Identifies security management information used in the current network management dialogue.

BMP 53 must be present in all network management messages if and only if Triple-DES is used as cryptographic algorithm for the computation of the MAC in BMP 128.

Structure, contents, and usage of BMP 53 are defined in [BG SEC].

BMP 93: Transaction Destination Institution Identification Code

The Transaction Destination Institution Identification Code contained in BMP 93 must identify the issuer gateway or the acquirer gateway, which is the destination of the Network Management Request uniquely. It is a numeric value consisting of 5 digits structured as follows:

# of Digits	Description
3	Numeric country code according to ISO 3166 identifying the country of the gateway
2	2-digits number identifying the gateway, assigned to the gateway by the community of the gateways in the country identified by digits 1-3

BMP 94: Transaction Originator Institution Identification Code

The Transaction Originator Institution Identification Code contained in BMP 94 must identify the acquirer gateway or the issuer gateway, which is the originator of the Network Management Request uniquely. It is a numeric value consisting of 5 digits structured as follows:

# of Digits	Description
3	Numeric country code according to ISO 3166 identifying the country of the gateway
2	2-digits number identifying the gateway, assigned to the gateway by the community of the gateways in the country identified by digits 1-3

This data element is used to identify a network management dialogue uniquely together with the values of BMP 11 and 12 in the respective Network Management Request.

BMP 111: Encryption Data

BMP 111 shall be present in all network management messages if and only if AES is used as cryptographic algorithm for the computation of the MAC in BMP 128. The content is specified in section 4.2.2.

BMP 128: MAC

Used to test the presence and correct usage of cryptographic keys.

Currently 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. It has to be ensured, that the bit indicating the presence of BMP 128 is set in the Secondary Bit Map before the calculation of the MAC.

BMP 53 indicates padding mechanism, cryptographic algorithms and related parameters, and key that are used for MAC computation if and only if Triple-DES is used as cryptographic algorithm.

BMP 111 indicates padding mechanism, cryptographic algorithms and related parameters, and key that are used for MAC computation if and only if AES is used as cryptographic algorithm.

5 References

[BG SEC] Bilateral and Multilateral Processing of Card Transactions in Europe, Security Features, Version 3.0 AES, 20/09/2018

[ECSG] SEPA Cards Standardisation (SCS) "VOLUME", Version 8.0, 01/03/2017

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

[ISO 8583-1:2003] ISO 8583-1, Financial transaction card originated messages - Interchange message specifications - Part 1: Messages, data elements and code values. 2003

[ISO 13492] ISO 13492, Financial services - Key management related data element - Application and usage of ISO 8583 data elements for encryption

Annex 1 BIN File

A BIN file contains the following records in the given sequence:

1. one header record
2. one or more data records
3. one trailer record

The BIN file is coded in ASCII. Records are separated by the Line Feed character '0A'.

The following abbreviations are used to specify the format:

n = Numeric
an = Alphanumeric
ans= Alphanumeric and Special

Annex 1.1 Header record format

A header record in a BIN file is structured as follows:

No.	Name	Format	Description
1	FILE TYPE	an 10	Constant value "BG-BINFILE" for a BIN file using the format described in this document. REQUIRED
2	FILE TYPE VERSION	n 2	The current version of the BIN file type is "01". Other values are reserved for future use. REQUIRED
3	CREATED BY	n 11	The ID of the creator of the BIN file. REQUIRED
4	ACTIVATION DATE	n 8	The BIN file shall be used for routing from this activation date on. The activation date has the format YYYYMMDD. YYYY: year MM: month DD: day REQUIRED
5	Filler	an 20	Blanks; RFU. REQUIRED

Annex 1.2 Trailer record format

A trailer record in a BIN file is structured as follows:

No.	Name	Format	Description
1	RECORD TYPE	an 10	Constant value "BINTRAILER" for the trailer record of the bin file. REQUIRED
2	NUMBER OF DATA RECORDS	n 8	The number of data records (i.e. without trailer and header record) contained in this BIN file. REQUIRED
3	Filler	an 20	Blanks, RFU. REQUIRED

Annex 1.3 Data record format

A record in a BIN File for the definition of cards participating in bilateral or multilateral processing of transactions in Europe shall be structured as follows:

Name	Format	Description
ISSUER BIN LENGTH	n 2	Number of digits of the Issuer BIN REQUIRED
ISSUER BIN	n 19	Issuer BIN If the issuer BIN is shorter than 19 digits, it is padded with trailing spaces (character '20'). REQUIRED
TERMINAL CATEGORY	n 5	Terminal Category Position 1: 0=No ATM, 1=Yes ATM Position 2: 0=No POS, 1=Yes POS Position 3: 0=No E-Com, 1=Yes E-Com Position 4, 5: 0 (RFU) REQUIRED for Information Acquirers might not be able to oblige in all cases
CARD TYPE	an 1	D - Debit Other RFU REQUIRED
CARD CURRENCY	n 3	Numeric ISO Currency Code of the card's currency REQUIRED
PAN LENGTH	n 2	Account number length. Values from 13 thru 19. REQUIRED
ISSUER COUNTRY	n3	Numeric ISO standard country codes. REQUIRED

Name	Format	Description
ISSUER PROCESSOR	ans 11	ID of the issuer processor (as defined by the entity producing the BIN table) REQUIRED
PRIMARY URL	an 124	URL for cardholder authentication in e-Payment. Value: https://.. OPTIONAL
BACK-UP URL	an 124	URL for cardholder authentication in e-Payment. Value https://.. OPTIONAL

Longer BINs take precedence over shorter BINs.

Duplication of BINs is allowed as long as they do apply to different Terminal Categories as indicated by the field "TERMINAL CATEGORY".

The e-Payment URLs are only meaningful if position 3 of the terminal category is equal to 1.