ALFEBA
PROCESSING SOLUTIONS

SEQUOIA MOSAIC 3000:

INTERNET-ACQUIRING PLATFORM

Description of the application programming interface (API) with external processing systems

Developer's manual

Version 1.0

This page doesn’t contain any information

Content

Chapter 1. About the document 5
1.1. Purpose of the document 7
1.2. How to use this manual 7
1.3. Classification 7
1.4. Document sheet 7
1.5. Document contacts 7
1.6. Document history 7
Chapter 2. General information 9
2.1. About the API 11
2.2. Connections 12
2.3. Requests processing logic 13
2.4. Types of requests and data sets 14
Chapter 3. API internet-acquiring messages formats 15
3.1. About this section 17
3.2. Amount hold request message 18
3.3. Charge request message 21
3.4. Single message 23
3.5. Recurrent payment message 25
3.6. Hold cancelation request message 27
3.7. Reversal request message 29
3.8. Refund request message 31
3.9. Cancellation request message 33
3.10. Operation status check request message 35
Chapter 4. API p2p messages formats 37
4.1. About this section 39
4.2. Card credit possibility check request message 40
4.3. Card debit request message 42
4.4. Card credit request message 44
4.5. Recurrent charge request message 47
Chapter 5. Parameters description 49
5.1. About this section 51
5.2. Register 51
5.3. Notes 51
5.4. Data length 51
5.5. Characters 52
5.6. Main parameters 53
5.7. Additional parameters 55

Chapter 6. Examples 63

6.1. About this section 65

6.2. Example 1 65

6.3. Example 2 65

6.4. Example 3 66

6.5. Example 4 66

6.6. Example 5 66

Chapter 7. Attachments 67

7.1. Terms and abbreviations 69

7.2. External documents references 70

Chapter 1. About the document

This chapter contains the next sections:

Section	Description	Page
1.1.	Purpose of the document	7
1.2.	How to use this manual	7
1.3.	Classification	7
1.4.	Document sheet	7
1.5.	Document contacts	7
1.6.	Document history	7

This page doesn’t contain any information

1.1. Purpose of the document

This document describes the Internet-acquiring platform API with an external processing system for the cards transactions of the MasterCard, Visa and Mir payment systems.

This document was prepared for the specialists in the field of the interfaces programming and architecture and contains the confidential information.

1.2. How to use this manual

The manual is designed to provide a useful reference tool for all information related to the internet-platform of the SM 3000 system to program the application programming interface with a third system.

The terms, abbreviations and useful references to other documents about the SM 3000 system are provided at the final part of the document.

Terms and Abbreviations - A glossary of terms commonly used in the card processing and electronic funds transfer industry.

1.3. Classification

This document has been classified as External.

1.4. Document sheet

200103

1.5. Document contacts

In the case of questions or proposals about information presented in this document, you can contact Alfeba's Documentation Division by email doc@alfeba.com, by phone +598 2 208 31 42 or by mail, using the address: Av. Agraciada 2770, Montevideo, 11823, Uruguay.

1.6. Document history

Version	Date	Modification	Notes	Authors
1.0	16.03.2019	-	Init. Version	Natalia Bogorodskaya
1.1	16.04.2019	Internal information aggregated	Rev.	Natalia Bogorodskaya

This page doesn’t contain any information

Chapter 2. General information

This chapter contains the next sections:

Section	Description	Page
2.1.	About the API	11
2.2.	Connections	12
2.3.	Requests processing logic	13
2.4.	Types of requests and data sets	14

This page doesn’t contain any information

2.1. About the API

The Bank's or the Financial institution's Internet Acquiring Platform (hereinafter, the Platform) is a platform, which is used by aggregators for the Internet-acquiring based payments.

For the internet-acquiring agents (or Platform's customers) of the Bank or of the Financial institution, the platform is performed as a server based application, receiving and processing external authorization requests for the internet-transactions. During their processing, the requests must be redirected for the authorization into the payment system through the Processing Bank or the contracted Processing center, to receive and process the authorization responses.

The application programming interface of the SM3000 internet-acquiring platform with a stand alone cards processing system and the operations data requests logic are described in this document.

2.2. Connections

The requests from the internet-acquiring platform are sent to the specific port of the Cards Processing system server by the HTTP or HTTPS requests with the transfer of requested data by the POST method.

The POST data is transmitted by URL encoding approach, according to the RFC 3986 standard (spaces like %20) in UTF8 encoding.

If the request doesn’t contain the POST data, the Processing system server must return a message with the status 200 and the text "NO PARAM". When the successful response of the request is received, the Processing system server must respond by the message with a status 200, that contains an XML data structure.

In the case of the HTTPS type of request, the data exchange participants are identified by the certificates issued in advance to each participant. Server-side connections are supported by SSL v.3.0, TLS v.1.0, TLS v.1.1 or TLS v.1.2 standards.

Processing system server must maintain the ability of the simultaneous requests parallel processing. Every incoming data request must be processed independently of each other.

Attention!

For the HTTP status 100 (expect / continue mechanism) from the Processing system server side is not necessary to supported even in compatibility mode.

When the request is received, the connection by the Processing system server must be hold until the end of request's processing and the response creation to the Internet-acquiring platform. When the response is sent the connection must be closed. In the case of an unexpected failure of the Processing system server, which may lead to the request processing error without returning of the status to the Internet-acquiring Platform, the Platform sets a timeout to wait for a response from the Processing system server during 45 seconds.

2.3. Requests processing logic

Depending on the status of the internet-acquiring operation, various types of requests are applicable to it. Requests must be used by the Processing system server:

- to create an operation with the Processing system server,
- to process online authorization to Visa / MasterCard payment systems,
- to generate the debit operation, to correct or to cancel the authorization or its debiting, and
- to create recurring payments.

On the internet-acquiring operation request sent to the Payment system through the Processing system server, the Processing system server receives a corresponding response from it and must inform the Internet-acquiring Platform about the result of the actions specified in the request.

When Processing system server receives the request from the Internet-acquiring platform, the field of the Unique Request Number [OrderId] is unique for each request. If the request received with the same OrderId field value that was sent to Processing sometime earlier, this request must be considered a double and must not be processed with a Processing system server. Instead, a response must be sent containing the status of the previously initial request sent with the same OrderId value.

In the case of a timeout or other reason leading to a non-receipt of a response from Processing system server, the Internet-acquiring Platform will send the request again with the same OrderId to avoid re-processing the requested actions and as a result, for example, the occurrence of a duplicate payment.

2.4. Types of requests and data sets

Depending on the status of the operation, various types of requests are applicable to it. Requests must be used by the Processing system server:

- to create an operation with a Processing system server
- to conduct the online authorization,
- to generate debiting for an operation,
- to adjust or cancel the authorization or debiting, and
- to create the recurring payments.

The data of requests and responses to them are contained in a finite set of parameters.

Depending on the type of request, the status of its processing, as well as

- the execution of certain conditions,
- the set of parameters present in the request and
- the response to it

may vary, and the value of the same parameter may have the different semantic meaning (for example, the field RecId).

There is a mandatory fixed set of parameters for any request, as well as the mandatory parameters that must be set with a response.

Chapter 3. API internet-acquiring messages formats

This chapter contains the next sections:

Section	Description	Page
3.1.	About this section	17
3.2.	Amount hold request message	18
3.3.	Charge request message	21
3.4.	Single message	23
3.5.	Recurrent payment message	25
3.6.	Hold cancelation request message	27
3.7.	Reversal request message	29
3.8.	Refund request message	31
3.9.	Cancellation request message	33
3.10.	Operation status check request message	35

This page doesn’t contain any information

3.1. About this section

This section describes the internet-acquiring request messages formats between the SM3000 Internet-acquiring platform and the Processing system server:

- Amount hold request message,
- Charge request message,
- Single message,
- Recurrent payment message,
- Hold cancelation request message,
- Reversal request message,
- Refund request message.
- Request cancellation message,
- Operation status check request message.

Each transaction has its own both request and response formats.

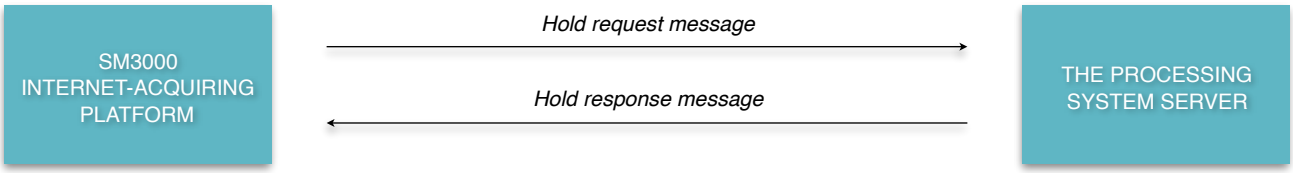
Each section of this chapter presents only one message type.

The P2P messages are presented separately in the Chapter 4 of the Manual.

Parameters of all of the messages are described in the Chapter 5 of the Manual.

3.2. Amount hold request message

This type of request is used as part of a Dual-Message payment to block (hold) funds with a cardholder's card without factual card debit operation.



3.2.1. Hold request format to the Processing system server

The Hold request message consists of the number of fields, described in the Table 3.2.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.2.1.1. The hold request message

Parameter	Mandatory / Optional	Comment
3DSAlg	O	
3DSCavv	O	
3DSEci	O	
3DSId	O	
3DSResult	O	
3DSVer	O	
AcqBin	O	
AcqFee	O	
Amount	M	
CardHolder	O	
CreateRec	O	Flag for creating a recurrent payment initialization
Currency	M	
Description	O	
DirSer_TranId	O	
Dsrp	O	
EMonth	M	
EYear	M	
Hold	M	The value is "1" or "true"
Initiator	O	
OrderId	M	Unique Request Number
Pan	M	

Parameter	Mandatory / Optional	Comment
PaymentSystem	O	
Reqtype	M	The value is "Pay"
SecureCode	O	
ServiceId	M	
StoredCard	O	
TerminalId	M	
TxStatus	O	
TxTime	O	
Version	M	

3.2.2. Hold response message to the Internet-acquiring platform

The Hold response message consists of the number of fields, described in the Table 3.2.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

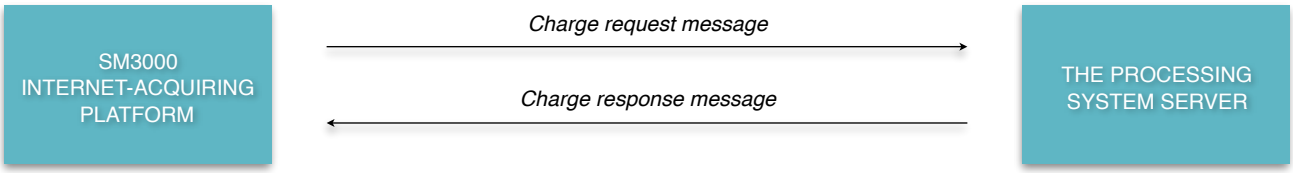
Table 3.2.2.1. The hold response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in GP21 Version	
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
P3DSeci	O	Present if 3DSEci is in the request
P3DSResult	O	Present if result data are available
RecId	O	Present if the Operation “Flag for creating a recurrent payment initialization” was successful
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	

Parameter	Mandatory / Optional	Comment
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.3. Charge request message

This type of request is used as part of a Dual-message payment for debiting a previously made successful authorization without debiting (holding).



3.3.1. Charge request format to the Processing system server

The Charge request message consists of the number of fields, described in the Table 3.3.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.3.1.1. The charge request message

Parameter	Mandatory / Optional	Comment
AcqFee	O	
Amount	O	May contain an Amount less than authorized
Currency	O	Mandatory if “Amount” is present in request
OrderId	M	Unique Request Number
RecId	M	Confirmed hold ID
Reqtype	M	Value "Charge"
ServiceId	M	
TerminalId	M	
Version	M	

3.3.2. Charge response message to the Internet-acquiring platform

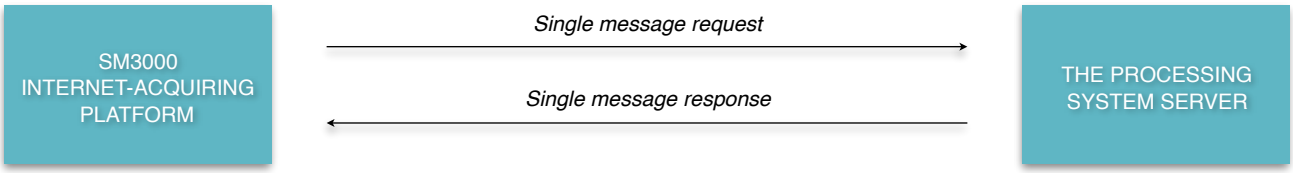
The Charge response message consists of the number of fields, described in the Table 3.3.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.3.2.1. The charge response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
CheckId	M	Confirmed hold ID
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.4. Single message

This type of request is used for authorization with subsequent debiting in case of its successful completion transaction in one request.



3.4.1. Single message request format to the Processing system server

The Single message request consists of the number of fields, described in the Table 3.4.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.4.1.1. The single message request

Parameter	Mandatory / Optional	Comment
3DSAlg	O	
3DSCavv	O	
3DSEci	O	
3DSId	O	
3DSResult	O	
3DSVer	O	
AcqBin	O	
AcqFee	O	
Amount	M	
CardHolder	O	
CreateRec	O	Flag for creation a recurrent payment initialization
Currency	M	
Description	O	
DirSer_TranId	O	
Dsrp	O	
EMonth	M	
EYear	M	
Hold	O	If present, the value is "0" or "false"
Initiator	O	
OrderId	M	Unique Request Number
Pan	M	
PaymentSystem	O	
Reqtype	M	The value is "Pay"

Parameter	Mandatory / Optional	Comment
SecureCode	O	
ServiceId	M	
StoredCard	O	
TerminalId	M	
TxStatus	O	
TxTime	O	
Version	M	

3.4.2. Single message response to the Internet-acquiring platform

The single message response consists of the number of fields, described in the Table 3.4.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.4.2.1. The single message response

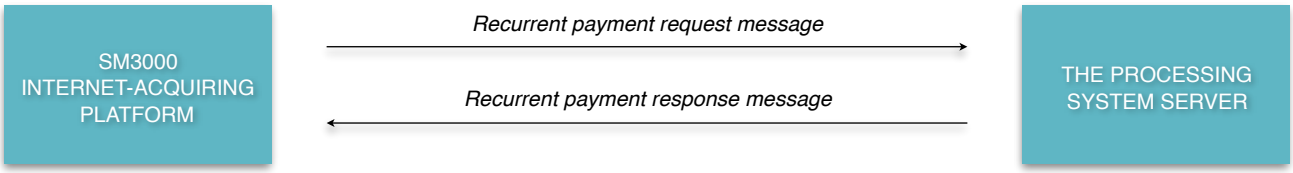
Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
P3DSeci	O	Present if 3DSEci is in the request
P3DSResult	O	Present if result data are available
PayId	M	Pay operation ID The identifier of this operation in Processing, coincides with TrId
RecId	O	Present if the Operation “Flag for creating a recurrent payment initialization” was successful
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.5. Recurrent payment message

This type of request is used to debit an amount, when the previos successful initialization of the recurrent payment was done. This initialization was done

a) as part of the hold creation operation in a Dual-message payment or

b) in a Single-Massage payment by specifying the "CreateRec" parameter in the request.



3.5.1. Recurrent payment message request format to the Processing system server

The Recurrent payment message request consists of the number of fields, described in the Table 3.5.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.5.1.1. The Recurrent payment message request

Parameter	Mandatory / Optional	Comment
AcqFee	O	
Amount	M	
Currency	M	
Description	O	
Dsrp	O	
Hold	O	If the value is"1" or "true", is present, then hold.
Initiator	O	
OrderId	M	Unique Request Number
RecId	M	Recurrent payment ID
Reqtype	M	The value is "PayRecurrent"
ServiceId	M	
StoredCard	O	
TerminalId	M	
Version	M	

3.5.2. Recurrent payment message response format to the Internet-acquiring platform

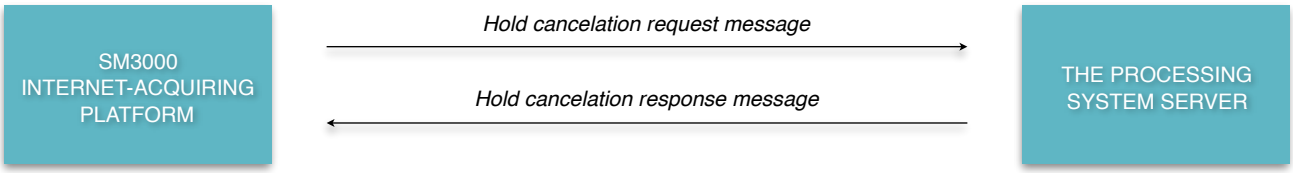
The Recurrent payment message response consists of the number of fields, described in the Table 3.5.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.5.2.1. The Recurrent payment message response

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
PayId	O	Recurrent payment ID. It present in charge operation.
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.6. Hold cancelation request message

By this request, it is possible to cancel the hold operation previously done, or to cancel unconfirmed hold operation after.



3.6.1. Hold cancelation request message format to the Processing system server

The Hold cancelation request consists of the number of fields, described in the Table 3.6.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.6.1.1. The Hold cancelation message request

Parameter	Mandatory / Optional	Comment
OrderId	M	Unique Request Number
RecId	M	Cancel hold ID
Reqtype	M	The value is "Cancel"
ServiceId	M	
TerminalId	M	
Version	M	

3.6.2. Hold cancelation response message format to the Internet-acquiring platform

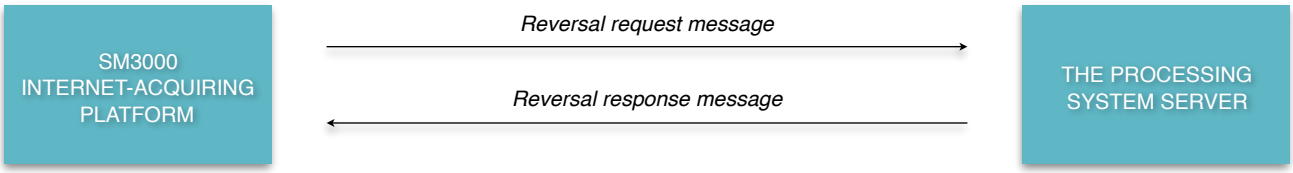
The Hold cancelation response consists of the number of fields, described in the Table 3.6.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.6.2.1. The Hold cancelation message response

Parameter	Mandatory / Optional	Comment
Amount	O	Present if cancel hold was found
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	O	Present if cancel hold was found
CurrencyN	O	Present if cancel hold was found
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.7. Reversal request message

By this request it is possible to cancel or reduce a previously done debit operation. The payment cancelation request, both a full and a partial one, can be sent for each payment one time only.



3.7.1. Reversal request message format to the Processing system server

The Reversal request consists of the number of fields, described in the Table 3.7.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.7.1.1. The Reversal message request

Parameter	Mandatory / Optional	Comment
Amount	O	May contain an Amount less than authorized
Currency	O	Mandatory, if Amount parameter is present in the request
Initiator	O	
OrderId	M	Unique Request Number
RecId	M	Reversal Hold ID or reversal charge ID.
Reqtype	M	The value is "Reverse"
ServiceId	M	
StoredCard	O	
TerminalId	M	
Version	M	

3.7.2. Reversal response message format to the Internet-acquiring platform

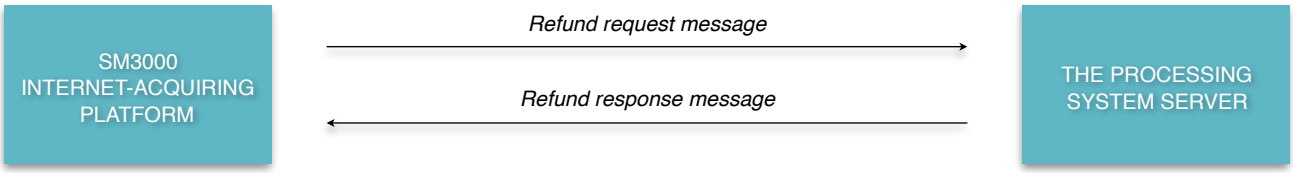
The Reversal response consists of the number of fields, described in the Table 3.7.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.7.2.1. The Reversal message response

Parameter	Mandatory / Optional	Comment
Amount	O	Present if reversal operation was found
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	O	Present if reversal operation was found
CurrencyN	O	Present if reversal operation was found
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.8. Refund request message

This type of request is used to make a refund to the cardholder after the payment operation. The card data for the refund operation is taken from the data of the payment made.



3.8.1. Refund request message format to the Processing system server

The Refund request consists of the number of fields, described in the Table 3.8.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.8.1.1. The Refund request message

Parameter	Mandatory / Optional	Comment
Amount	M	
Currency	M	
Description	O	
Dsrp	O	
Initiator	O	
OrderId	M	Unique Request Number
RecId	M	Hold ID or Charge ID
Reqtype	M	The value is "Refund"
SecureCode	O	
ServiceId	M	
StoredCard	O	
TerminalId	M	
Version	M	

3.8.2. Refund response message format to the Internet-acquiring platform

The Refund response consists of the number of fields, described in the Table 3.8.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

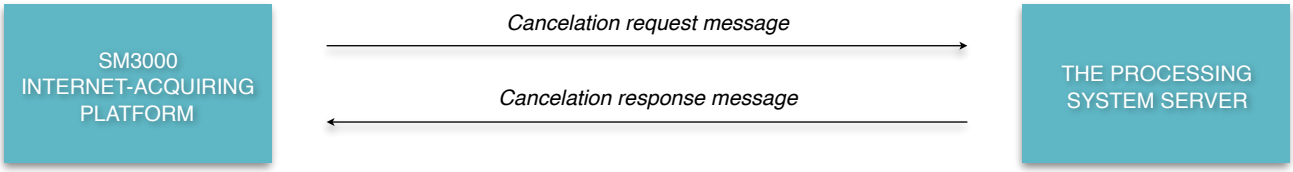
Table 3.8.2.1. The Refund response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
CheckId	O	The parameter “RecId” value from request
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
PayId	O	The parameter “RecId” value from request
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

3.9. Cancellation request message

By this request it is possible to interrupt the execution of a failed request or to cancel it, if it has already completed.

Cancellation is possible for authorizations, payments and refunds operations and can be sent for each request only one time.



3.9.1. Cancellation request message format to the Processing system server

The Cancellation request consists of the number of fields, described in the Table 3.9.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.9.1.1. The Cancelation request message

Parameter	Mandatory / Optional	Comment
OrderId	M	Unique Request Number
OrigOrderId	M	Cancellation request number
Reqtype	M	The value is "Abort"
ServiceId	M	Must be equal to the cancellation request value
TerminalId	M	Must be equal to the cancellation request value
Version	M	

3.9.2. Cancellation response message format to the Internet-acquiring platform

In the case if the cancellation leads to the cancellation of a failed hold or payment, the returned data is equivalent to the corresponding type of cancellation:

- Hold cancellation - Refund,
- Payment cancellation - Reversal.

The success and response code in this case are determined by the result of the cancellation.

In general, if the cancellation request was processing incorrectly, the response will contain the fields, mentioned in the Table 3.9.2.1.

The Cancellation response consists of the number of fields, described in the Table 3.9.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.9.2.1. The Cancelation response message

Parameter	Mandatory / Optional	Comment
AuthTime	M in Version GP21	
Date	M	
Operation	M	
OrderId	M	
ResCode	M	
ServiceId	M	
Success	M	In this contest only false
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

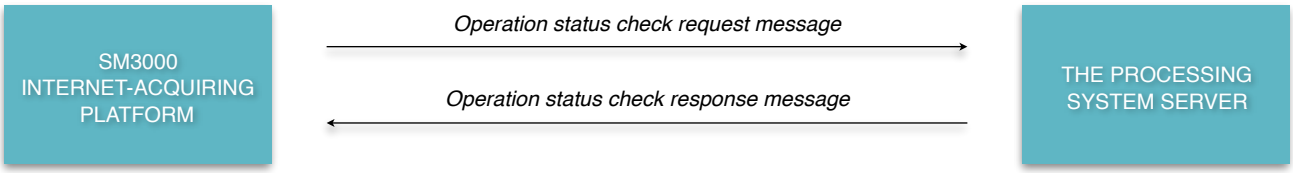
If the ServiceId or TerminalId fields value does not correspond to the canceled request, the response code to the Internet-acquiring Platform must be 842. It must be returned also if OrigOrderId field is not filled or its value matches the OrderId field value.

If the canceled request did not arrive to the Processing system Server, the response code sent by the Processing system Server to the Internet-acquiring platform must be 940, which must be returned in Cancellation response message.

If the wanted request arrives to the Processing system Server after, the status of unsuccessful operation must become assigned to it by the Processing system Server without any attempt to proceed it automatically. The response code must be 921, and TrId field must match the value from the response to the Cancellation request message.

3.10. Operation status check request message

By this request it is possible to check the status of the operation on a previously executed request.



3.10.1. Operation status check request format to the Processing system server

The request must have its own unique OrderId field value, as for any other type of request.

If the new status check request is sent with the OrderId field value of the previous Operation status check request, the new response on the new request will be returned with a new actual data.

The Operation status check request message consists of the number of fields, described in the Table 3.10.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 3.10.1.1. The Operation status check request message

Parameter	Mandatory / Optional	Comment
OrderId	M	Unique Request Number
OrigOrderId	M	Check request number
Reqtype	M	The value is "Status"
ServiceId	M	Must be equal to check request value
TerminalId	M	Must be equal to check request value
Version	M	

3.10.2. Operation status check response to the Processing system server

If the ServiceId or TerminalId value does not match the request being checked, the response code must be 842.

If the OrigOrderId field doesn't exist in the request, the response code 842 must be returned also to the Internet-acquiring Platform.

If the status check request did not arrived to the Processing system Server, the response code, sending by the Processing system Server to the Internet-acquiring Platform must be 940 and and TrId field must be absent. If the TrId field is presented in the response message, it means, that the operation was found, and the response code 940 is a result of its completion already.

The set of response parameters is different, depending on the type of the request must be processed, its status and whether it was found with the Processing system Server or didn't.

This page doesn’t contain any information

Chapter 4. API p2p messages formats

This chapter contains the next sections:

Section	Description	Page
4.1.	About this section	39
4.2.	Card credit possibility check request message	40
4.3.	Card debit request message	42
4.4.	Card credit request message	44
4.5.	Recurrent charge request message	47

This page doesn’t contain any information

4.1. About this section

The requests described in this chapter are used to maintain the processing of the operations of the Card2Card money transfers.

One request is used to charge the money from the sender's card of the transfer. The second request is used to credit the card-recipient of the transfer.

Since the ideology of the money transfer system in all internet payment systems [IPS] assumes the independence of the senders and the recipients and any combination thereof, these operations with the Processing system Server must be carried out independently of each other. The client of the system controls over the consistency of the credit and debit operations.

The main logic of transfers involves, first of all, the preliminary request to verify the possibility of the transfer to the recipient's card. In case of successful verification, the attempt to debit from the sender's card is made. In case of a successful debit operation, the credit operation is initiated on the recipient's side. If the credit operation is unsuccessful, the debit operation must be cancel. In case of the cancellation of the transfer (if there is such a technical feasibility), the credit operation must be canceled firstly and only after it the debit operation must be canceled.

It is also possible to carry out the debit operations only. In this case, within the debiting operation it is possible to create a recurrent payment for subsequent recurrent P2P payments. For the recurring payment, a special type of request is used - P2PRECURRENT.

This section describes the p2p request messages formats between the SM3000 Internet-acquiring platform and the Processing system server:

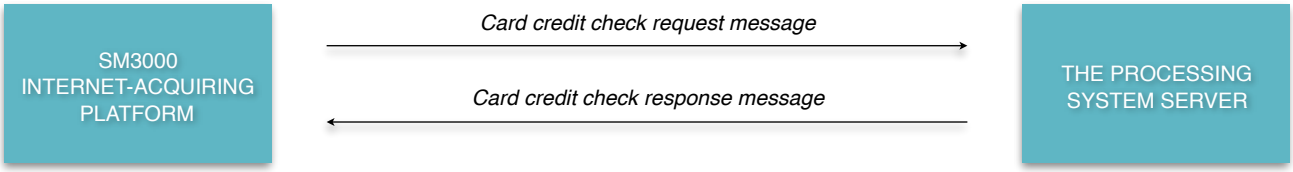
- Card credit possibility check request message,
- Card debit request message,
- Card credit request message,
- Recurrent charge request message.

Each transaction has its own both request and response formats.

Each section of this chapter presents only one message type.

4.2. Card credit possibility check request message

By this request it is possible to check the possibility of the card credit operation. This type of the request is a non-financial.



4.2.1. Card credit possibility check request format to the Processing system server

The Card credit possibility check request message consists of the number of fields, described in the Table 4.2.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.2.1.1. The Card credit possibility check request message

Parameter	Mandatory / Optional	Comment
Amount	M	
Currency	M	
Description	O	
Dsrp	O	
EMonth	O	
EYear	O	
Initiator	O	
OrderId	M	Unique Request Number
Pan	M	
Reqtype	M	The value is "CheckCredit"
ServiceId	M	
StoredCard	O	
TerminalId	M	
Version	M	

4.2.2. Card credit possibility check response format to the Internet-acquiring Platform

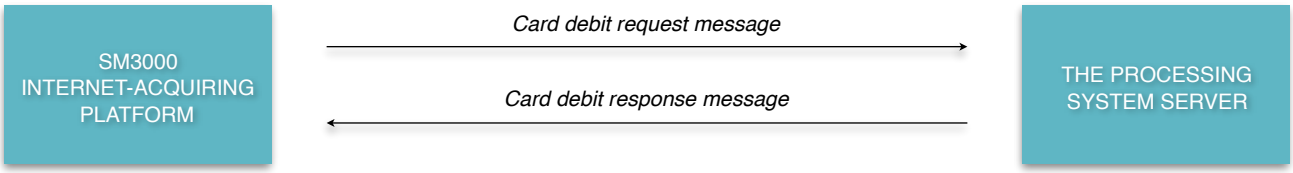
The Card credit possibility check response message consists of the number of fields, described in the Table 4.2.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.2.1.1. The Card credit possibility check response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

4.3. Card debit request message

This request is used to debit a card. The type of the message is a Single message.



4.3.1. Card debit request format to the Processing system server

The Card debit request message consists of the number of fields, described in the Table 4.3.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.3.1.1. The Card debit request message

Parameter	Mandatory / Optional	Comment
3DSAlg	O	
3DSCavv	O	
3DSEci	O	
3DSId	O	
3DSResult	O	
3DSVer	O	
AcqBin	O	
AcqFee	O	
Amount	M	
CardHolder	O	
CreateRec	O	Flag for creating a recurrent payment initialization
Currency	M	
Description	O	
DirSer_TranId	O	
Dsrp	O	
EMonth	M	
EYear	M	
Initiator	O	
OrderId	M	Unique Request Number
Pan	M	
PaymentSystem	O	
RECEIVER_CARD	O	Receiver's card number

Parameter	Mandatory / Optional	Comment
Reqtype	M	The value is "P2PDEBIT"
SecureCode	O	
ServiceId	M	Only for MCC 6538
StoredCard	O	
TerminalId	M	
TxStatus	O	
TxTime	O	
Version	M	

4.3.2. Card debit response format to the Internet-acquiring Platform

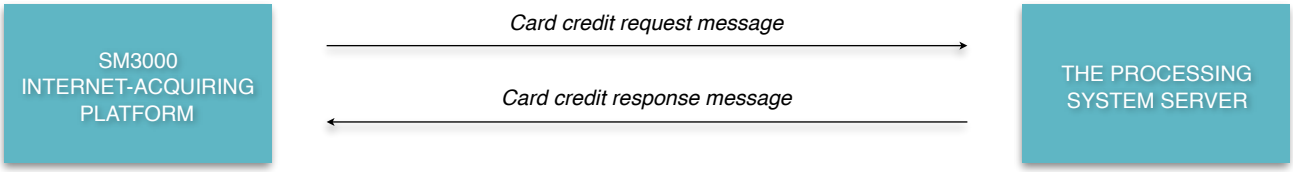
The Card debit response message consists of the number of fields, described in the Table 4.3.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.3.2.1. The Card debit response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
P3DSeci	O	Present if 3DSEci is in the request
P3DSResult	O	Present if result data are available
PayId	M	Pay ID, that is equal TrId
RecId	O	Present if creation a recurrent payment initialization was successful
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

4.4. Card credit request message

This request is used to credit the card.



4.4.1. Card credit request format to the Processing system server

The expiration date of the card is an optional parameter and may be absent.

The fields of the sender's data are mandatory for the request message.

The Card credit request message consists of the number of fields, described in the Table 4.4.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.4.1.1. The Card credit request message

Parameter	Mandatory / Optional	Comment
3DSAlg	O	
3DSCavv	O	
3DSEci	O	
3DSId	O	
3DSResult	O	
3DSVer	O	
AcqBin	O	
Amount	M	
CardHolder	O	
Currency	M	
DirSer_TranId	O	
Dsrp	O	
Description	O	
EMonth	O	
EYear	O	
Initiator	O	
MsgToRecipient	O	
OrderId	M	Unique Request Number
Pan	M	
PaymentSystem	O	
RecId	O	This value is equal the debit transfer operation TrId.

Parameter	Mandatory / Optional	Comment
Reqtype	M	The value is "P2PCREDIT"
SecureCode	O	
SENDER_ADDRESS	M	
SENDER_CITY	M	
SENDER_COUNTRY	M	
SENDER_NAME	M	
SENDER_POSTAL_CODE	M	
ServiceId	M	Only for MCC 6536 or MCC 6537
StoredCard	O	
TerminalId	M	
TxStatus	O	
TxTime	O	
Version	M	

4.4.2. Card credit response format to the Internet-acquiring Platform

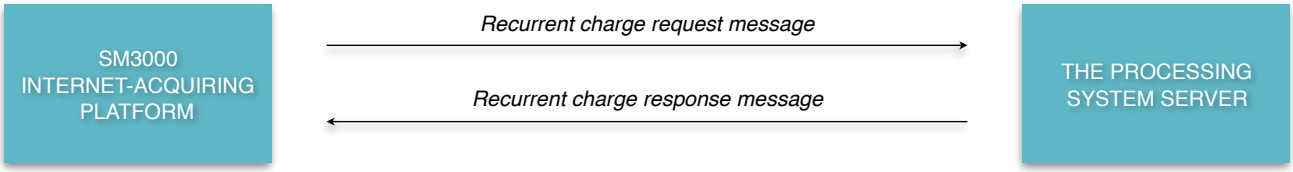
The Card credit response message consists of the number of fields, described in the Table 4.4.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.4.2.1. The Card credit response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
P3DSeci	O	Present if 3DSEci is in the request
P3DSResult	O	Present if result data are available
PayId	M	Present if the request has RecId parameter
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

4.5. Recurrent charge request message

This is a format of a recurrent charge request, which is used for a previously created P2P recurrent payment initialization. This recurrent payment initialization must be done as part of a P2PDEBIT payment by specifying the CreateRec parameter in the request.



4.5.1. Recurrent charge request format to the Processing system server

The Recurrent charge request message consists of the number of fields, described in the Table 4.5.1.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.5.1.1. The Recurrent charge request message-1

Parameter	Mandatory / Optional	Comment
AcqFee	O	
Amount	M	
Currency	M	
Description	O	
Dsrp	O	
Initiator	O	
OrderId	M	Unique Request Number
RecId	M	P2P ID - flag for creation a recurrent payment initialization
Reqtype	M	The value is "P2PRecurrent"
ServiceId	M	
StoredCard	O	
TerminalId	M	
Version	M	

4.5.2. Recurrent charge response format to the Internet-acquiring Platform

The Recurrent charge response message consists of the number of fields, described in the Table 4.5.2.1. below. In this table they use the abbreviation «M» for the mandatory fields and «O» - for the optional fields.

Table 4.5.2.1. The Recurrent charge response message

Parameter	Mandatory / Optional	Comment
Amount	M	
AuthCode	O	Present if successful request
AuthTime	M in Version GP21	
Card	O	Present if available
Currency	M	
CurrencyN	M	
Date	M	
ExpDate	O	Present if available
ExtRC	O	Present if available
Operation	M	
OrderId	M	
PayId	O	P2P ID - flag for creation a recurrent payment initialization
ResCode	M	
RRN	M	
ServiceId	M	
Stan	M	
Success	M	
Terminal	M	
TerminalId	M	
TrId	O	Present if available. Present for successful operations.

Chapter 5. Parameters description

This chapter contains the next sections:

Section	Description	Page
5.1.	About this section	51
5.2.	Register	51
5.3.	Notes	51
5.4.	Data length	51
5.5.	Characters	52
5.6.	Main parameters	53
5.7.	Additional parameters	55

This page doesn’t contain any information

5.1. About this section

This section describes all of the valid parameters, indicates the restrictions on the values they accept, and provides a brief description.

5.2. Register

The parameter register does not matter. For data, in general, the register is important, and this is noted in the description of the data format.

5.3. Notes

The notes are used to describe the data format are described in the Table 5.3.1.0.

Table 5.3.1.0. The parameters notes

Sign	Place	Description
*	Begin of the format	It means that there is additional information about the parameter (see Additional information about the parameters)

5.4. Data length

Data length is defined as described in the Table 5.4.1.0.

Table 5.4.1.0. The parameters data length

Sign	Description
..N	N - number - data of variable length, but not longer than N; N, where N is a number - a fixed data length equal to N
N..	N - number - data of variable length, but not shorter than N
N1..N2	N1, N2 - numbers - data of variable length, but not shorter than N1 and no longer than N2

5.5. Characters

The characters allowed in the data are encoded in the format description as follows in the Table 5.5.1.0.

Table 5.5.1.0. The parameters characters

Character	Description
b	Case-sensitive data consists of numbers, letters of the Latin alphabet and equal signs, plus and slash (this type is also used to transmit data in base64 format)
f	Boolean type, 1 or 0, case-sensitive data, true or false values (Processing in the responses uses true and false)
h	Data consists of hexadecimal numbers in uppercase without spaces or other characters, only letters "A" - "F" and numbers, data of even length are allowed
m	The sum, without spaces and other separators, the separator of the fractional part is a point
n	Data consists only of digits (from 0 to 9)
N	Data consists of numbers (from 0 to 9) and may contain a minus sign at the beginning to transmit a negative number, a minus sign is taken into account when calculating the length of the data
s	Case-insensitive data, consists of numbers, letters of the Latin alphabet, spaces, punctuation and other readable characters
S	Case-sensitive data consists of numbers, letters of the Latin alphabet, spaces, punctuation and other readable characters
z	Data is strictly lowercase, consists of numbers, letters of the Latin alphabet, spaces, punctuation and other readable characters
Z	Data is strictly in upper case, consists of numbers, letters of the Latin alphabet, spaces, punctuation and other readable characters
c	Case-insensitive data consisting of numbers, letters of the Cyrillic alphabet and the Latin alphabet, spaces, punctuation marks and other readable characters
C	Case-sensitive data consists of numbers, letters of the Cyrillic alphabet and the Latin alphabet, spaces, punctuation marks and other readable characters
a	Data is strictly lowercase, consists of numbers, letters of the Cyrillic alphabet and the Latin alphabet, spaces, punctuation marks and other readable characters
A	Data is strictly in upper case, consists of numbers, letters of the Cyrillic alphabet and the Latin alphabet, spaces, punctuation marks and other readable characters

5.6. Main parameters

This sections contains the main parameters description.

The main parameters are described in the Table 5.6.1.1. The third column of the Table 5.6.1.1. determines the possibility or necessity of the presence of this parameter in the requests sent from the Internet-acquiring Platform to the Processing system Server or the responses of Processing system Server to the Internet-acquiring Platform.

The corresponding abbreviations are defined below in the Table 5.6.1.0.

Table 5.6.1.0. The main parameters. Abbreviations

Character	Description
v	The parameter may be present in the request for the Platform, depending on the type of request
V	The parameter must be present in all requests of the Platform
o	The parameter may be present in the Processing response when certain conditions are met
O	the parameter is always present in the Processing response, but responses to requests with errors in the input data may contain incorrect or empty values for some parameters

The main parameters are described below in the Table 5.6.1.1.

Table 5.6.1.1. The main parameters

Parameter	Data format	Presence	Description
3DSAlg	S..3	v	Algorithm for 3D Secure verification
3DSCavv	b..60	v	3D Secure CAVV / AAV
3DSEci	S..2	v	3D Secure ECI
3DSId	b..255	v	3D Secure XID
3DSResult	*Z1	v	Present if 3D Secured result data are available
3DSVer	*n1	v	3D Secure protocol version
AcqBin	S..20	v	Acquiring BIN in 3D Secure (from VEReq)
AcqFee	m	v	Acquiring fee, in request amount
Amount	m	vO	Amount in the request
AuthCode	Z6	o	IPS authorisation code
AuthTime	S	O in version GP21	Processing Authorisation date in the format YYYY-MM-DDTHH:MM:SS
Card	s	o	Masked card number, it composes from numbers and “*” symbols
CardHolder	S..50	v	Cardholder name
CheckId	n..9	o	Hold ID, wich was confirmed or rejected by this request
CreateRec	f		Flag for creating a recurring payment initialization, if absent - "false"
Currency	n3	vO	Currency code (ISO 4217)
CurrencyN	Z3	O	Symbol currency code or number currency code

Parameter	Data format	Presence	Description
Date	n8	O	Operation date in the format YYYYMMDD
Description	Z..25	v	IPS Merchant name, in case of absent name it used Processing Merchant name
DirSer_TranId	s..36	v	Transaction ID on Directory Server for protocol 3DS 2.0 (EMV 3D Secure)
Dsrp	*n1..4	v	Identifier of the used electronic service or wallet
EMonth	n1..2	v	Expiration month (1 – 12)
ExpDate	n4	o	Expiration date in the format YYMM
ExtRC	s..3	o	IPS response code
EYear	n1..4	v	Expiration year in the format YYYY or YY
Hold	f	o	Hold flag. By default is "false"
Initiator	*n..3	v	Initiator attribute and transaction status
MsgToRecipient	h..400	v	Text message (HEX Unicode, up to 200 symbols)
Operation	s	O	Executing operation. Typically, the value duplicates the Reqtype from the request. Can be the value "Forgot"
OrderId	S..32	VO	Unique Request Number
OrigOrderId	S..32	VO	Request Abort number
P3DSeci	S..2	o	3DSEci value in the request
P3DSResult	Z1	o	Present if available
Pan	n..19	v	PAN
PayId	n..9	o	Payment ID, the data of which this request referred to. For example, recurring payment flag of refund or revarsal
PaymentSystem	S..20	v	Payment system ID in 3D Secure (from VEReq)
RECEIVER_CARD	n..24	v	Receiver’s card number
RecId	n..9	vo	The identifier of a previously completed request or operation on whose data this request is based. The Processing Response is used to pass the identifier of the successfully created recurring payment flag
Reqtype	*s..99	V	Type of request, defines the logic of its processing in the Processing
ResCode	*N..3	O	Internal Processing response code. The value "-1" – successful, others values - error
RRN	n12	O	Unique IPS payment ID
SecureCode	s..4	v	Security code CVV2/CVC2
SENDER_ADDRESS	S..50	v	Sender’s address
SENDER_CITY	S..25	v	Sender’s city
SENDER_COUNTRY	S3	v	Sender’s country code by-099-0 ISO 3166
SENDER_NAME	S..24	v	Sender’s name
SENDER_POSTAL_CODE	S..10	v	Post Index
ServiceId	s..8	VO	Service ID
Stan	n6	o	Operation number in IPS (not unique)
StoredCard	*n..3	o	Flag of transaction using previously saved payment data
Success	f	O	Flag of Request Success termination
Terminal	Z8	O	The identifier of the IPS payment terminal on behalf of which name the operation was processed

Parameter	Data format	Presence	Description
TerminalId	s..8	VO	Platform Merchant ID in Processing
TrId	n..9	VO	Request Current ID
TxStatus	S1	v	Verification status in 3D Secure (from PARes)
TxTime	S..20	v	Date and time in 3D Secure (from PARes)
Version	*s	V	Client Protocol Version

5.7. Additional parameters

This section contains the additional parameters description.

5.7.1. 3DSResult

This parameter carries information about the involvement of the card in the 3D Secure service and about the fact of this verification.

Possible parameter values are described in the Table 5.7.1.1.

Table 5.7.1.1. The parameter 3DSResult

Value	Description
A	3D Secure verification was attempted and failed
N	3D Secure check was not performed, as the client card does not support this service
U	3D Secure check could not be performed for technical reasons on the client or issuer side
Y	3D Secure check was performed

5.7.2. 3DSVer

This parameter carries information about the version of the used protocol of the 3D Secure service.

Possible parameter values are described in the Table 5.7.2.1.

If there is no parameter in the query, the default value is 1.

Table 5.7.2.1. The parameter 3DSVer

Value	Description
1	3D Secure 1.0 (3DS 1.0)
2	EMV 3D Secure (3DS 2.0)

5.7.3. Dsrp

This parameter carries information about the used electronic service or wallet.

Possible parameter values are described in the Table 5.7.3.1.

Table 5.7.3.1. The parameter Dsrp

Value	Description
0	Not certain, other sources
1	Mastercard Masterpass
2	Google Pay
3	Apple Pay
4	Samsung Pay

5.7.4. Initiator

If there is no parameter in the request, the default value is 1 for operations with the CreateRec attribute set and 0 for all others.

Possible parameter values are described in the Table 5.7.4.1.

Table 5.7.4.1. The parameter Initiator

Value	Description
0	Operation initiated by the card holder
1	The operation was initiated by the cardholder, the client agreed to the Merchant to save the payment details of the card for subsequent operations
2	Pending operation initiated by the cardholder
3	Operation initiated by Merchant
4	Pending operation initiated by Merchant
5	Incremental operation initiated by Merchant
6	Operation initiated by Merchant
7	A penalty operation initiated by Merchant
8	Repeated operation initiated by Merchant
9	A periodically repeated operation initiated by Merchant on a long-term assignment from the cardholder, without a schedule
10	A periodically repeated operation initiated by Merchant on a long-term assignment from the cardholder, according to the schedule

5.7.5. Reqtype

Possible parameter values are described in the Table 5.7.5.1.

Table 5.7.5.1. The parameter Reqtype

Value	Description
Cancel	Cancellation of a previously created current hold
Charge	Write-off (payment) of a previously created existing hold
Pay	Create a hold (authorization without debiting) or a one-step payment depending on the value of the Hold parameter, create a recurrence binding for subsequent recurrent payments, depending on the value of the CreateRec parameter
PayRecurrent	Conducting a recurrent payment based on a previously created recurrinet binding, creating a hold (authorization without debiting) or a one-stage payment, depending on the value of the Hold parameter
Refund	A refund to the client, a credit operation tied to a previously made payment
Reverse	Cancellation, full or partial, of a previous payment

5.7.6. ResCode

Defines the result of an operation in Processing. The value “-1” is the only successful one, all the others mean a denial of the authorization and specify the reason for the denial. In a sense, the exception is the value “940” in the response to cancel the operation, meaning that the original operation to cancel was not found.

Possible parameter values are described in the Table 5.7.6.1.

Table 5.7.6.1. The parameter ResCode

Value	Description
-1	Successful transaction / authorization / request
0	Incomplete operation, during authorization or suspended due to processing failure
800	Completion of the operation is not possible due to hardware limitations (for example, an ATM)
801	A response was not received from the network on time
802	The issuer is unavailable
803	The operation is prohibited until the client contacts his issuerIncremental operation initiated by Merchant
804	Operation not allowed
805	Error (internal processing error)
807	Error
937	Error (internal processing error)
959	Error (internal processing error)
806	The operation is beyond the scope of the law
807	Error
808	Error in issuing funds (usually due to the fault of the ATM)

Value	Description
809	Error in issuing funds (usually due to the fault of the ATM)
810	Response received too late
811	Repeated (duplicated) operation
812	Error in the format of the message or data
813	Error matching request data with the original operation
814	Card limit is exceeded, usually on the number of operations
815	Card limit is exceeded, usually on the number of operations
818	Restrictions on the card / account to the card
819	The card has expired
820	Invalid PIN code value
821	Invalid PIN code value
822	Card with the status of "lost"
823	Card with the status of "stolen"
824	The request currency is unknown to the system
825	Approval of the operation is possible only after the completion of customer identification
826	Refusal without explanation
827	Unknown card bin
828	Incorrect authorization settings for the card
829	Invalid card number (in length)
830	Incorrect card number (characters)
831	The card has not yet expired
833	Data integrity check Error of the of the magnetic stripe
835	A technical error occurred during the verification of the PIN code
836	Data integrity check Error of the of the magnetic stripe
837	Error interpreting the result of the verification of the PIN code
838	The status status of the card is not defined
839	Data integrity check Error of the of the magnetic stripe
840	The specified operation is prohibited
841	The conversion rate from the request currency to the card account currency was not found
842	Improper use of the request or incorrect filling of its parameters
843	Error checking the validity of the card (for the operation of checking the card)
844	No response was received from an external participant
845	preauthorization was canceled
846	on the specified pre-authorization (hold) confirmation (write-off) has already been carried out
847	Withdraw a card (by card status)
849	Error processing the card status at the database level
850	Data on the requested transaction was not found or it is in the wrong status
851	Error occurred while processing activity limits
852	Card limit is exceeded, usually on the number of operations
853	Card limit is exceeded, usually on the number of operations

Value	Description
854	Card limit is exceeded, usually on the number of operations
855	Similar request is already in progress
856	The requested service or service is not available for this card
857	The amount of authorization is beyond the scope established by the issuer / operator
858	Error processing the cryptographic signature
859	Verification of the cryptographic signature failed
860	The limit on the card account has been exceeded
861	The validity period of the card in the system and the request do not match
862	Invalid PIN code value
863	Depository error (cash acceptance module)
864	Depository error (cash acceptance module)
865	Depository error (cash acceptance module)
866	Depository error (cash acceptance module)
867	Invalid CVC2 / CVV2 value in the request
868	Incorrect payment period
869	Refusal due to the established prohibition of authorization of electronic commerce operations
870	The operation is prohibited until the PIN code is changed
871	The amount request exceeds the limit set for this operation
872	The amount of authorization is beyond the scope established by the issuer / operator
873	Invalid BIN map
874	The specified payment type is not available
875	The specified payment type is not available
876	The limit on the card account has been exceeded
877	The amount of authorization is beyond the scope established by the issuer / operator
878	The amount of authorization is beyond the scope established by the issuer / operator
879	There are not enough funds on the card account to complete the operation
881	The total limit for this external participant has been exceeded
890	An error occurred while processing preauthorization and its confirmation
891	The life of the pre-authorization (hold) has expired before the receipt of the request for confirmation (write-off)
892	The amount of confirmation (write-off) exceeds the amount of hold (authorization)
893	Data on the requested transaction was not found or it is in the wrong status
894	Data on the requested transaction was not found or it is in the wrong status
895	Error processing or checking chip cryptography
897	Error checking CVC2
901	Invalid PIN code value
902	Error occurred while authorization
903	Error processing the amount of the request
904	Invalid PIN code value
905	Invalid card (for example, not found in the database)
906	The card has expired

Value	Description
907	The account for the card was not found, or it is incorrect
908	The card has expired
909	Invalid card (for example, not found in the database)
910	Invalid request
911	The limit on the card account has been exceeded
912	The limit on the card account has been exceeded
913	Invalid request
914	The account for the card was not found, or it is incorrect
915	There are not enough funds on the card account to complete the operation
916	Error
917	Card limit exceeded
918	Invalid BIN map
919	The indicated amount cannot be withdrawn by an ATM
920	The indicated amount cannot be withdrawn by an ATM
921	Operation canceled by the customer
922	Communication error with the device (ATM, terminal, etc.)
924	Error in issuing funds (usually due to the fault of the ATM)
925	Error in issuing funds (usually due to the fault of the ATM)
926	Error in issuing funds (usually due to the fault of the ATM)
927	Error in issuing funds (usually due to the fault of the ATM)
928	Denial of authorization due to card account restrictions
929	Error in issuing funds (usually due to the fault of the ATM)
930	Data on the requested transaction was not found or it is in the wrong status
932	The account for the card was not found, or it is incorrect
933	Error
934	Invalid card (for example, not found in the database)
935	Error
936	The card is locked, lock without removal
937	Error (internal processing error)
938	The limit on the card account has been exceeded
939	Unknown failure error (when the error code came from outside)
940	Data on the requested transaction was not found or it is in the wrong status
941	Invalid seller / service provider identifier
942	Invalid store identifier
943	Invalid terminal identifier
944	Communication error with the device (ATM, terminal, etc.)
947	The request amount exceeds the limit set for this operation
950	Response received too late
951	Error
952	Operation recognized as fraud

Value	Description
953	Restrictions on the card / account to the card
954	Card in the STOP list
955	Invalid transaction date
956	The requested service or service is not available for this card
957	The specified payment type is not available
959	Error (internal processing error)
960	Payment recipient is incorrectly selected
964	Verification of the cryptographic signature failed
966	Error processing the cryptographic signature
967	Error
968	Incorrect transaction amount
969	Verification of the cryptographic signature failed
971	Restrictions on the card / account to the card
972	Restrictions on the card / account to the card
973	Restrictions on the card / account to the card
977	Refusal with notification of cancellation of the recurrent binding
979	Denial of authorization due to card account restrictions
980	The new PIN block is incorrect (in the change request, the PIN code
981	The account for the card was not found, or it is incorrect
982	The account for the card was not found, or it is incorrect
983	The account for the card was not found, or it is incorrect
984	The account for the card was not found, or it is incorrect
985	The account for the card was not found, or it is incorrect
993	Payment recipient is incorrectly selected

5.7.7. Storedcard

Possible parameter values are described in the Table 5.7.7.1. If there is no parameter in the request, the default value is 0 for the operation "Pay" and 1 for all others.

Table 5.7.7.1. The parameter Scorecard

Value	Description
0	Payment data entered by the cardholder
1	Previously saved payment data is used

5.7.7. Version

The protocol version may in certain cases redefine the logic of processing the request data, and also indicates to the Processing Party which response format can be successfully processed by the Platform.

This is a required parameter that must be present in every request.

The current version of the protocol supports the values "GP20" and "GP21". The latter is distinguished by the presence of a standard XML header and the presence of additional fields in the response.

Chapter 6. Examples

This chapter contains the next sections:

Sección	Descripción	Página
6.1.	About this section	65
6.2.	Example 1	65
6.3.	Example 2	65
6.4.	Example 3	66
6.5.	Example 4	66
6.6.	Example 5	66

This page doesn’t contain any information

6.1. About this section

This section contains 5 examples of the API.

6.2. Example 1

Request data:

OrderId=1586939963532015&3DSAlg=3&3DSEci=02&Description=Tex%20Pay%2001&3DSCavv=jKFlAIE1shR5CREFKbrACHcAAAA%3D&SecureCode=XXX&EYear=23&TerminalId=83868&3DSResult=Y&EMonth=03&Currency=643&Amount=2154.00&Version=GP20&3DSId=ICAgICAk%2Ff0B%2Ff1K%2Ff1y%2Ff3sJ1M%3D&CardHolder=Yunus%20Simsek&Reqtype=Pay&ServiceId=83868&Pan=516840XXXXXX5697

Response data:

<response><Success>false</Success><OrderId>1586939963532015</OrderId><Operation>PAY</Operation><PayId>69779021</PayId><TrId>69779021</TrId><Amount>2154.00</Amount><Currency>643</Currency><CurrencyN>RUR</CurrencyN><ServiceId>83868</ServiceId><TerminalId>83868</TerminalId><ResCode>827</ResCode><ExtRC>05</ExtRC><Terminal>ACQ04427</Terminal><RRN>041569779021</RRN><Date>20200415</Date><Card>516840******5697</Card><ExpDate>2303</ExpDate><STAN>779021</STAN><P3DSeci>212</P3DSeci></response>

6.3. Example 2

Request data:

OrderId=1586947071225985&Description=RCIWLPay&Reqtype=PayRecurrent&TerminalId=83378&Currency=643&Amount=1000.00&Version=GP20&RecId=69638131&ServiceId=83378

Response data:

<response><Success>true</Success><OrderId>1586947071225985</OrderId><RecId>69638131</RecId><Operation>PAYRECURRENT</Operation><PayId>69638131</PayId><TrId>69794079</TrId><Amount>1000.00</Amount><Currency>643</Currency><CurrencyN>RUR</CurrencyN><ServiceId>83378</ServiceId><TerminalId>83378</TerminalId><ResCode>-1</ResCode><ExtRC>00</ExtRC><Terminal>ACQ04190</Terminal><RRN>010669794079</RRN><AuthCode>260580</AuthCode><Date>20200415</Date><Card>220220******0000</Card><ExpDate>2412</ExpDate><STAN>794079</STAN></response>

6.4. Example 3

Request data:

OrderId=1586947276031435&3DSAlg=3&3DSEci=02&Description=WalletPay-recurrent&3DSCavv=jGn5XnJpA4vWCBECqg0zBSAAAAA%3D&SecureCode=XXX&EYear=22&TerminalId=83686&3DSResult=Y&EMonth=04&Currency=643&Amount=499.00&Version=GP20&3DSId=ICAgICD9%2Ff1%2FD0b9%2FTsO%2FXX9TWM%3D&CardHolder=NEMATJ%20NEMATJ&Reqtype=Pay&Hold=1&ServiceId=83686&Pan=532315XXXXXX2754

Response data:

<response><Success>true</Success><OrderId>1586947276031435</OrderId><Operation>PAY</Operation><TrId>69794537</TrId><Amount>499.00</Amount><Currency>643</Currency><CurrencyN>RUR</CurrencyN><ServiceId>83686</ServiceId><TerminalId>83686</TerminalId><ResCode>-1</ResCode><ExtRC>00</ExtRC><Terminal>ACQ04345</Terminal><RRN>041569794537</RRN><AuthCode>559659</AuthCode><Date>20200415</Date><Card>532315******2754</Card><ExpDate>2204</ExpDate><STAN>794537</STAN><P3DSeci>212</P3DSeci></response>

6.5. Example 4

Request data:

OrderId=1586947279982941&Reqtype=Charge&TerminalId=83686&Currency=643&Amount=499.00&Version=GP20&RecId=69794537&ServiceId=83686

Response data:

<response><Success>true</Success><OrderId>1586947279982941</OrderId><Operation>CHARGE</Operation><CheckId>69794537</CheckId><TrId>69794544</TrId><Amount>499.00</Amount><Currency>643</Currency><CurrencyN>RUR</CurrencyN><ServiceId>83686</ServiceId><TerminalId>83686</TerminalId><ResCode>-1</ResCode><ExtRC>00</ExtRC><Terminal>ACQ04345</Terminal><RRN>041569794537</RRN><AuthCode>559659</AuthCode><Date>20200415</Date><Card>532315******2754</Card><ExpDate>2204</ExpDate><STAN>794544</STAN></response>

6.6. Example 5

Request data:

OrderId=1586946744024975&Reqtype=Refund&TerminalId=83719&Currency=643&Amount=741.71&Version=GP20&RecId=69316178&ServiceId=83719

Response data:

<response><Success>true</Success><OrderId>1586946744024975</OrderId><Operation>REFUND</Operation><PayId>69316178</PayId><TrId>69793289</TrId><Amount>741.71</Amount><Currency>643</Currency><CurrencyN>RUR</CurrencyN><ServiceId>83719</ServiceId><TerminalId>83719</TerminalId><ResCode>-1</ResCode><Terminal>ACQ04359</Terminal><RRN>041569793289</RRN><Date>20200415</Date><Card>519896******5633</Card><ExpDate>2204</ExpDate><STAN>793289</STAN></response>

Chapter 7. Attachments

This chapter contains the next sections:

Section	Description	Page
7.1.	Terms and abbreviations	69
7.2.	External documents references	70

This page doesn’t contain any information

7.1. Terms and abbreviations

To be inclosed

7.2. External documents references

In this document they use references to the following documents:

Number	Description	Category
100100	SM 3000 Functional description	External

This page doesn’t contain any information

ALFEBA

Agraciada 2770 Montevideo 11823 Uruguay

Phone: + 598 2 2083142

E-mail: docs@alfeba.com

www.alfeba.com