ALFEBA

PROCESSING SOLUTIONS

SEQUOIA MOSAIC 3000:

INTERNET-ACQUIRING PLATFORM

Functional description

User's manual

Version 1.0

This page doesn't contain any information

Content

Chapter 5. Attachments   47

Chapter 1.   About the document

This chapter contains the next sections:

This page doesn't contain any information

1.1. Purpose of the document

This document describes the functionality of the SM 3000 Internet-acquiring platform and it place in the SM3000 processing solutions. This document was prepared for users of the SM 3000 Internet-acquiring platform.

1.2. How to use this manual

The manual is designed to show the main functions of the Platform and to give a short description of the SM3000 IAP for users.

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.

To know how to use the ALFEBA documentation, to find information about the register structure and graphic tags, used in the documentation, see the Manual 200100 «Documents register».

1.3. Classification

This document has been classified as External.

1.4. Document sheet

200101

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	17.07.2020	-	Init. Version	Natalia Bogorodskaya

This page doesn't contain any information

Chapter 2. About SM3000 IAP

This chapter contains the next sections:

This page doesn't contain any information

2.1. General information

In this chapter we provide the principal information about SM3000 IAP of the Sequoia Mosaic 3000 Internet-acquiring platform [SM3000 IAP].

2.2. About SM3000 IAP

Sequoia Mosaic 3000 Internet - Acquiring Platform [SM3000 IAP] is a e-commerce solution that enables you to manage the payment transactions of your business. The platform supports multiple payment methods and integration methods.

SM3000 IAP is a result of traditional third party (switch or inter-banking/ national) processing products evolution into the the e-commerce direction development since 1992.

2.3. E-commerce business direction parts maintenance

SM3000 supports main parts of the modern e-commerce business direction:

- internet-acquiring processing;
- p2p payments processing;
- m-commerce processing;
- bills payments processing;
- crypto-currencies acquiring support.

2.4. Modern e-commerce business requirements cover

The SM3000 IAP is developed to cover the needs of:

A. Third party processors/ Member service providers of Visa, MasterCard and other international and national payment systems;

B. Banks - members of MasterCard, VISA and other international and national payment systems;

C. Payment operators and facilitators;

D. Agents of payment operators and facilitators (independent sales organizations [ISO])

E. Internet merchants and their subsidiaries;

F. Cardholders and bills payers.

2.5. SM3000 IAP structural parts

The SM3000 IAP has three main internal structural parts:

1. Front-end (Payment gateway system) [SM3000 IAP FE], responsible for the on-line transactions processing and it maintenance;

2. Back-office (Administration part) [SM3000 IAP BO], developed to work with settings of the SM3000 IAP FE and reporting;

3. Merchant profile, developed for the transactions management at the level of the Merchant.

2.6. SM3000 IAP integrations

Developed from the national processing center solution SM3000 IAP has traditionally a wide possibilities of the integration both with internal and external applications:

Internal ones:

- SM3000 EPS,
- SM3000 PAYMENTS,
- SM3000 PERSONALIZATION,
- SM3000 CRYPTO,
- SM3000 RISK.

External ones:

- External authorization processing cores (SWITCHs): Way4, SmartVista, Tieto, Compas+, TPII, Base24;
- E-commerce platforms: CyberSpace,   .
- Banking accounting systems: BankXXI Century, TEMENOS;
- Corporate accounting systems: 1C;
- Internet-shops cores: .

2.2.5. APIs

In according with PSDII requirements, authorized by the Central European Bank, we provide opened Application Programming Interfaces for our partners and partners of our customers, depending on the category of the payment system participation level:

- Merchant;
- Payment operator or Facilitator;
- Bank;
- Processing center;
- National switch.

2.7. The place of SM3000 IAP in the SM3000 processing solutions

SM3000 IAP as independent e-commerce solution, which is integrated with SM3000 EPS - Switch and authorization processing core, and can be implemented with external authorization processing platforms and accounting systems.

The place of the SM3000 IAP you can find in the Picture 2.7.0.0.

Picture 2.7.0.0. SM3000 processing solutions structure

.
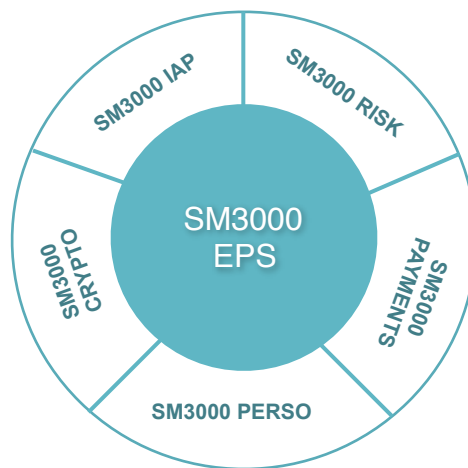
SM3000 EPS   - is a on-line authorization processing core, developed for the Third party processors, national processing centers and banks - members of payment systems MasterCard, VISA and others. The Core processes cards issuing and acquiring banking programs, ATMs and POSs networks, has direct gateways to VISA, MasterCard and other processing systems. The full functional description of the SM3000 EPS see in the Manual SM3000 EPS. Functional description. The Core has integrations with core banking systems, TEMENOS, BANKXXI, DIASOFT and others banking accounting solutions.

SM3000 PERSO   - is a personalization platform for the DataCard and NBS personalization stations. It supports NFC-based, contact chip and magstripe products personalization jobs. The full functional description of the SM3000 PERSO see in the Manual SM3000 EPS. Functional description.

SM3000 RISK   - is a core based fraud prevention platform for the issuing and acquiring cards programs, based both on

- host parameters filters and

- on-line decisions making based on transactions history.

The full functional description of the SM3000 RISK see in the Manual SM3000 RISK. Functional description.

SM3000 PAYMENTS - is a platform for consumer credits, on-line payments for credit, MO/TO transactions by credit, membership programs, bonus and discounts management for cardholders and merchants. The full functional description of the SM3000 PAYMENTS see in the Manual SM3000 PAYMENTS. Functional description.

SM3000 CRYPTO - is a full platform for the crypto currencies issuing and acquiring, including Merchant profile and mobile applications for users, crypto change offices and crypto stock exchange software, on the government and private level of the implementation. The full functional description of the SM3000 CRYPTO see in the Manual SM3000 CRYPTO. Functional description.

Between the mentioned platforms of the SM3000 processing solutions are local products, like a software for POS terminals (NEW POS and others), self-service terminals etc. Functional description of these products can be provided on demand.

.

Chapter 3. Platform architecture

This chapter contains the next sections:

This page doesn't contain any information

3.1. General information

In this chapter we describe a structure of the Sequoia Mosaic 3000 Internet-acquiring platform [SM3000 IAP].

3.2. The platform architecture

SM3000 IAP architecture uses a service-oriented approach, in which each service is responsible for a certain functionality and interacts with other services (both internal and external) via the API.

The main participants in the interaction with the SM3000 IAP are as follows:

A. Cardholder - a customer who makes a purchase at a Merchant using a debit or credit card.

B. Merchant is an online store that sells goods or provides services on the Internet. Merchant is not required to be PCI DSS compliant because it does not receive, store or process cardholder data.

C. Gateway - a real payment gateway whose operation is described in this document. Compliant with PCI DSS.

D. Acquiring Bank - a credit institution connected directly to Visa and MasterCard. It processes debit or credit card authorization requests.

E. Directory servers - Visa and Mastercard services that provide information about Issue Bank for 3D-Secure.

The general scheme of interaction between the participants is presented in the Picture 3.2.0.0.

Picture 3.2.0.1. SM3000 IAP interaction scheme
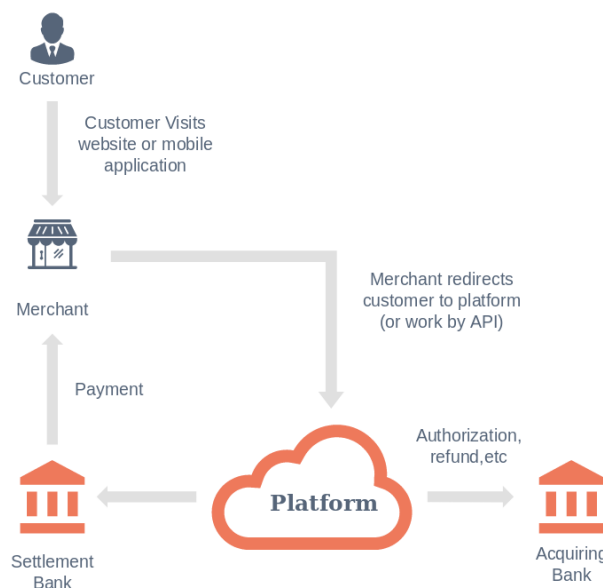
A schematic diagram of services is shown in the Picture 3.2.0.1.

SM3000 IAP includes:

A. SM3000 IAP Back Office are a group of services that are responsible for accounting for Merchant in the system, managing commissions, clearing, creating and submitting reports;
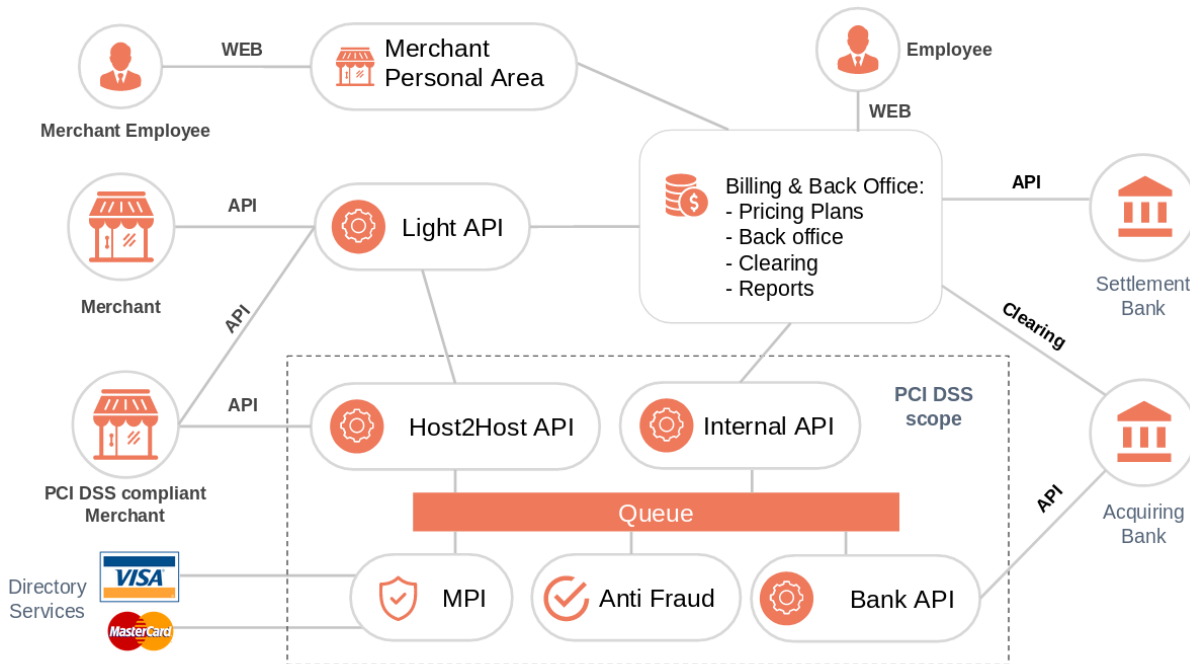
B. Merchant Personal Area (Merchant profile) is a personal office for Merchant, where it can manage its services, unload reports, request technical support, etc.;

C. Lite API is a service that provides an external API for Merchant. Cardholder data does not pass through this API;

D. Host2Host API is a service that is responsible for external interactions with Merchants that meet the PCI DSS requirements. This service also provides cardholder with a form for entering card data;

E. Internal API is a service that provides an interface for internal billing requests;

F. Queue is a bus for all services to interact;

G. MPI (Merchant plug-in) is a service for interaction with DS of Visa and MasterCard 3D-Secure. To check 3D Secure;

H. Anti Fraud/ Fraud prevention is a fraud prevention part of the Platform;

I. Bank API is a service that implements protocols for interaction with external systems.

The following external agents interact with Gateway:

A. Merchant Employee who uses a personal account through WEB;

B. Merchant - Merchant services that turn to Gateway to initiate payment, payment status and other activities;

C. PCI DSS Merchant - Merchant services compliant to PCI DSS that turn to Gateway. Merchant data has the right to interact on host2Host API, which allows to accept cardholder data;

D. Employee is a gateway staff Managing Merchants, Reporting, and other needed operations;

E. Settlement Bank - the services of the bank providing settlement;

F. Acquiring Bank - services of the bank providing internet acquiring online (authorization, return, etc.), and clearing.

3.3. Encryption standards

ALFEBA uses the encryption standards for the SM3000 IAP, presented in the Table 3.3.0.0.

Table 3.3.0.0. The SM3000 IAP encryption standards

Purpose	Encryption algorithm
User browser interaction	TLS 1.2 or above
Message signature	HMAC with SHA-256
Database data encryption	AES with 256 bits key size

3.4. On-line transaction flow

The Picture 3.4.0.0. describes the high-level online interaction of the SM3000 IAP with external systems.

Picture 3.4.0.0. SM3000 IAP based on-line transaction flow
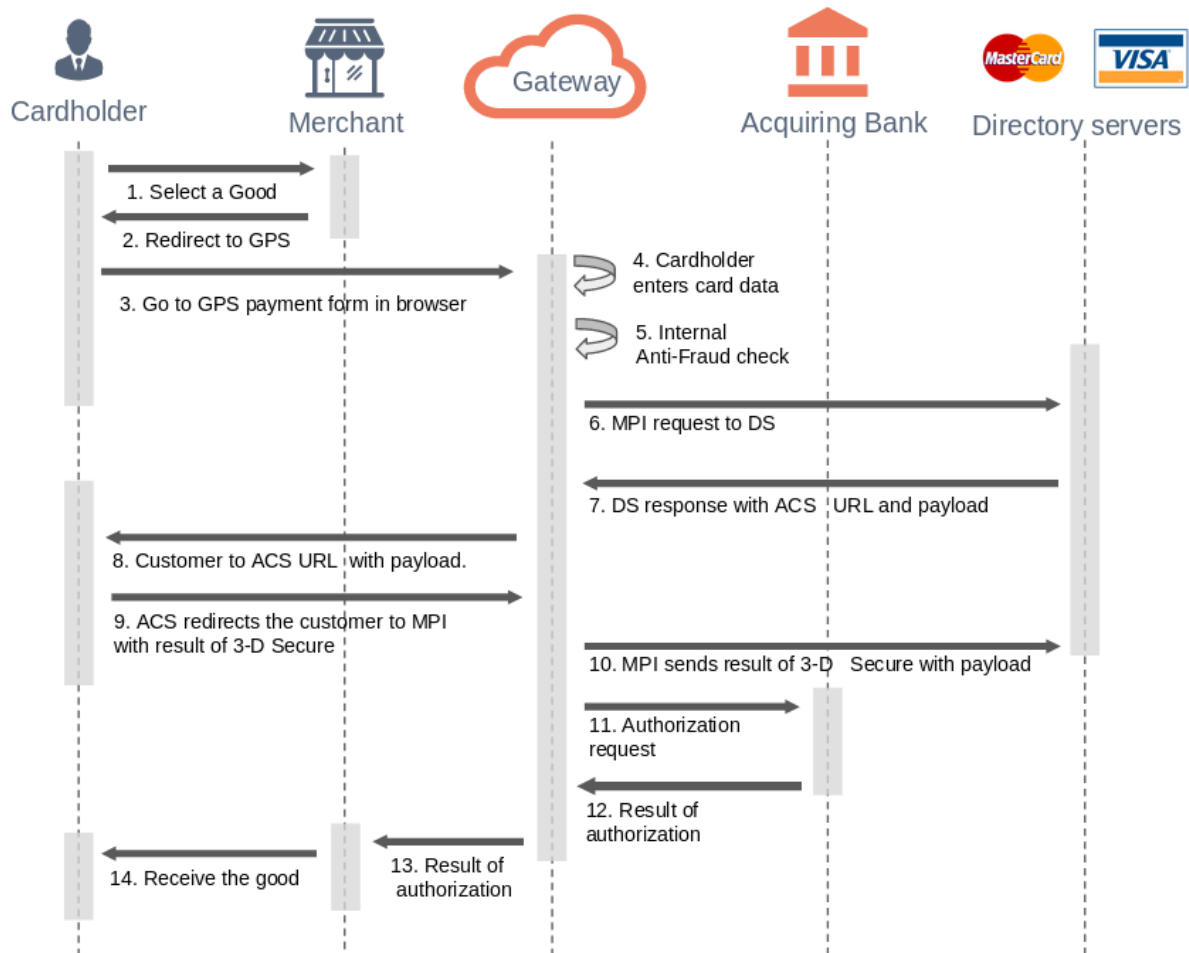
Process description:

1. Cardholder selects a product on the website or in the Merchant mobile application. However, cardholder does not enter cardholder data;

2. Cardholder informs (sends a request to) Merchant about the goods and services that he/she is going to purchase, then Merchant redirects cardholder to the SM3000 IAP card data input page using a redirect in the browser. Cardholder goes to the SM3000 IAP/ Gateway page along with his/her order information, including cost;

3. Each time cardholder goes to the SM3000 IAP page, a secure HTTPS connection is established using TLS 1.2 or higher;

4. Cardholder enters card data including PAN and CVV;

5. SM3000 IAP performs an internal antifraud transaction verification. In case of the fraud suspicion, the transaction is rejected;

6. Depending on the card BIN, SM3000 IAP sends a request to VISA or MasterCard Directory Server (DS);

7. DS provides information on Issuer Bank required for 3D-Secure authorization (if necessary), including a 3D-Secure access code, Access Control Server (ACS) URL;

8. If a 3D-Secure authentication is required, SM3000 IAP sends the Cardholder to the ACS URL and transfers all the necessary data;

9. In case of successful 3D-Secure check, ACS redirects Cardholder back to Gateway;

10. SM3000 IAP validates 3D-Secure results by completing an additional request to DS;

11. SM3000 IAP sends an authorization request to Acquiring Bank, which redirects the authorization request to Visa or MasterCard net;

12. Acquiring Bank returns the authorization response to SM3000 IAP;

13. SM3000 IAP sends a Merchant request with authorization response. Merchant receives all the necessary information about the authorization response, however, the PAN is transmitted in a disguised form (first 6 and last 4 digits);

14. If transaction is authorized Merchant accomplishes the sale.

3.5. Off-line settlement data flow

The off-line settlement data flow describes the offline settlement process on the next business day after the transaction day. Interaction participants:

A. Acquiring Bank - a bank responsible for online authorizations.

B. SM3000 IAP Gateway - a real payment gateway whose operation is described in this document.

C. SM3000 IAP Gateway Settlement Bank - a bank that makes settlements for SM3000 IAP.

D. Merchant's Settlements Bank - the bank (s) in which Merchants' accounts are open. It is possible that all accounts are opened in the SM3000 IAP Settlement Bank.

Off-line settlement data flow is presented in the Picture 3.5.0.0.

Picture 3.5.0.0. Off-line settlement data flow
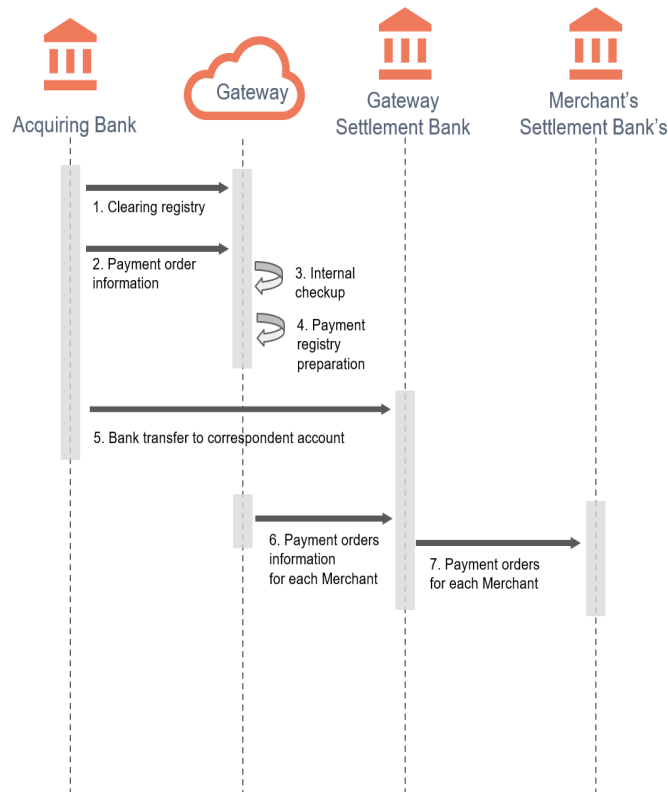
Process description:

1. Acquiring Bank sends the transaction batch to the SM3000 IAP address for reconciliation;

2. Acquiring Bank sends the payment order information to SM3000 IAP for reconciliation;

3. SM3000 IAP reconciles its own billing data, data from the Acquiring Bank transaction batch and information in the payment order.

4. SM3000 IAP calculates the income of each Merchant taking into account all fees and prepares the appropriate batch for Merchant payments.

5. Acquiring Bank makes a payment to the correspondent bank account at the SM3000 IAP Settlement Bank.

6. SM3000 IAP transmits information about payment orders that must be created for each Merchant.

7. SM3000 IAP Settlement Bank creates payment orders for each Merchant.

This page doesn't contain any information

Chapter 4. Functional description

This chapter contains the next sections:

This page doesn't contain any information

4.1. General information

In this chapter we describe the main functions of the Sequoia Mosaic 3000 Internet-acquiring platform [SM3000 IAP] and principal interfaces.

The common structure of the SM3000 IAP is presented in the Picture 4.1.0.0.

Picture 2.2.0.0. The SM3000 IAP global structure
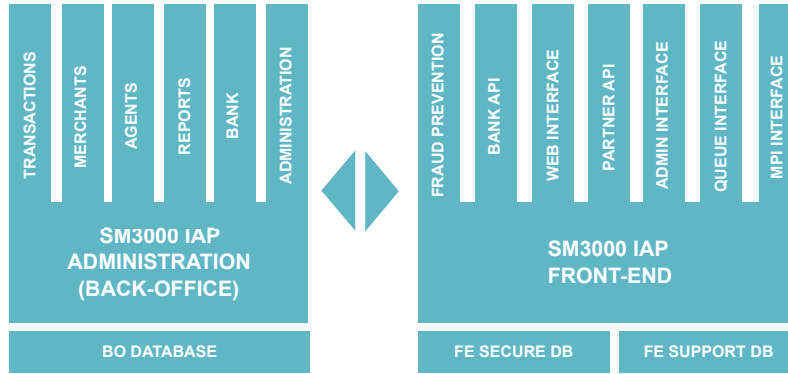
4.2. About Front-End

Front-End of the Platform presents on-line GateWay, that includes a number of internal parts:

- A. Fraud prevention;
- B. Bank API;
- C. Web-interface;
- D. Admin Interface;
- E. Queue Interface and
- F. MPI Interface.

4.3. Fraud prevention

Fraud prevention templates are used to determine how to prevent the fraud with the Platform. The Platform presents predefined templates for the Payment operator/ Facilitator.

Based on slits management, internal algorithms check and black-lists Fraud prevention includes:

- Fraud prevention templates management,
- Fraud prevention parameters management,
- Fraud prevention service parameters management,
- Fraud prevention events management,
- Fraud prevention black-lists management,
- Fraud prevention historical data and reports.

To learn more information about Fraud prevention part of the SM3000 IAP see the Manual 200116 «SM3000: IAP. Front-end interface. Fraud prevention».

4.4. Bank API

Bank API is presented by on-line authorization protocols, used to interact with the external processing systems.

> To learn more about on-line authorization protocol see Manual 200103 «SM3000: IAP. On-line authorization 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.

4.5. WEB-interface

Web-interface

4.6. Partner API

Partner API presents the on-line interface for the interaction with a Merchant's server.

> To learn more about on-line Partner protocol see Manual 200119 «SM3000: IAP. On-line merchant API».

PartnerAPI provides an opportunity to carry out the following operations:

- Hold/ Block - blocking funds on the user's card;

- Charge - completion of payment with debiting funds from the user's card;

- Pay - payment by one team;

- Unblock - change the amount of funds blocked on the user's card;

- Refund - refund (full or partial) to the user's card;

- GetState - clarification of the current state of payment;

- GetStateWait - clarification of the current state of payment.

4.7. Admin interface

Admin interface presents an access through the User's interface to manage the Front-end processes settings. It includes:

- Fraud prevention settings and management;

- Security settings and managements;

- Certificates management;

- Transactions management;

- Gateway and it parameters management;

- Services management;

- Other functions.

4.8. Queue interface

Queue is a bus for all services to interact.

The main on-line operations formats are presented in the Section 4.10. of the Manual.

4.9. MPI Interface

MPI interface is presented to integrate the SM3000 IAP with internal possibility to work with 3dSec.

To learn more bout MPI and certificates see Manual 200115 «SM3000 IAP: MPI certificates generation and implementation process».

4.10. Supported on-line operations formats

4.10.1. 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.
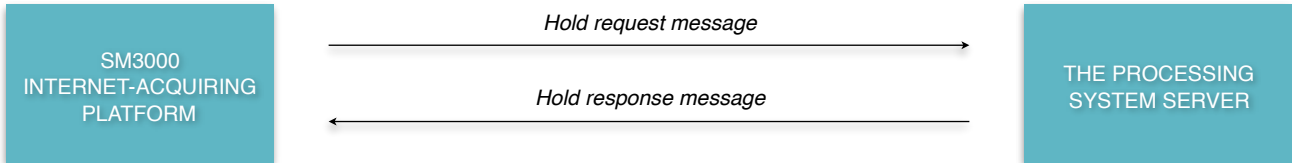
4.10.2. Charge request message

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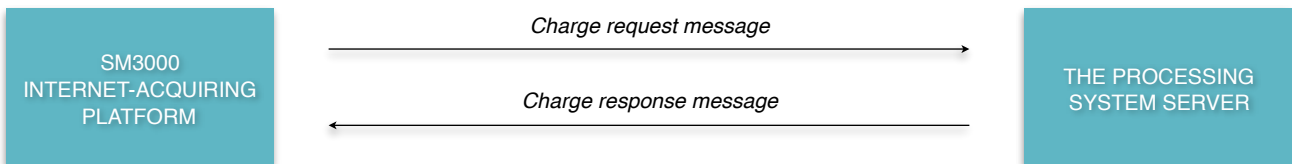
4.10.3. Single message

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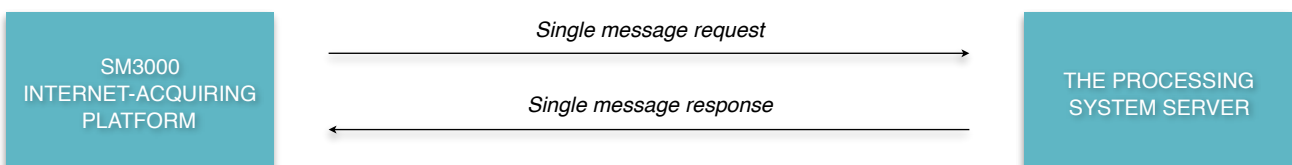
4.10.4. Recurrent payment message

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.

SM3000 INTERNET-ACQUIRING PLATFORM	*Recurrent payment request message* → ← *Recurrent payment response message*	THE PROCESSING SYSTEM SERVER

4.10.5. Hold cancelation request message

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

SM3000 INTERNET-ACQUIRING PLATFORM	*Hold cancelation request message* → ← *Hold cancelation response message*	THE PROCESSING SYSTEM SERVER
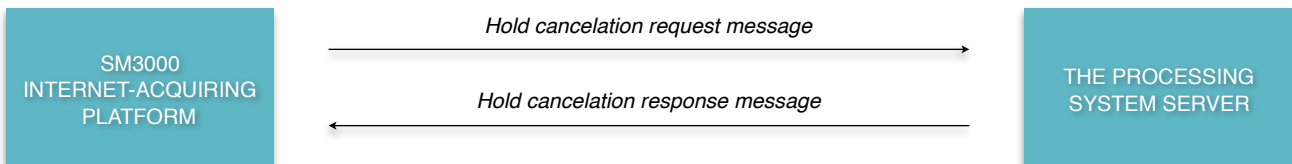
4.10.6. Reversal request message

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.

SM3000 INTERNET-ACQUIRING PLATFORM	*Reversal request message* → ← *Reversal response message*	THE PROCESSING SYSTEM SERVER
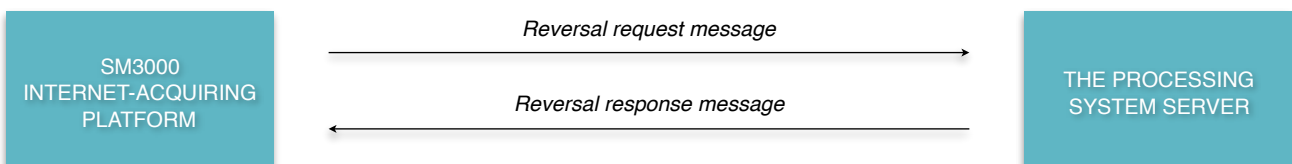
### 4.10.7. Refund request message

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.

| SM3000 INTERNET-ACQUIRING PLATFORM | *Refund request message* → ← *Refund response message* | THE PROCESSING SYSTEM SERVER |
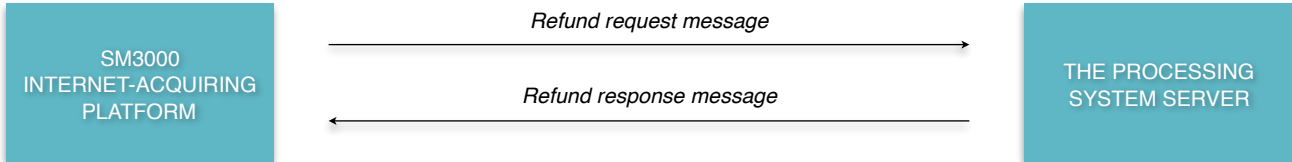
4.10.8. Cancellation request message

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.

| SM3000 INTERNET-ACQUIRING PLATFORM | *Cancelation request message* → ← *Cancelation response message* | THE PROCESSING SYSTEM SERVER |
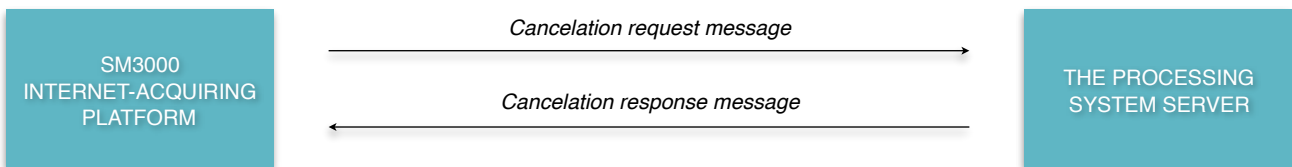
4.10.9. Operation status check request message

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

| SM3000 INTERNET-ACQUIRING PLATFORM | *Operation status check request message* → ← *Operation status check response message* | THE PROCESSING SYSTEM SERVER |
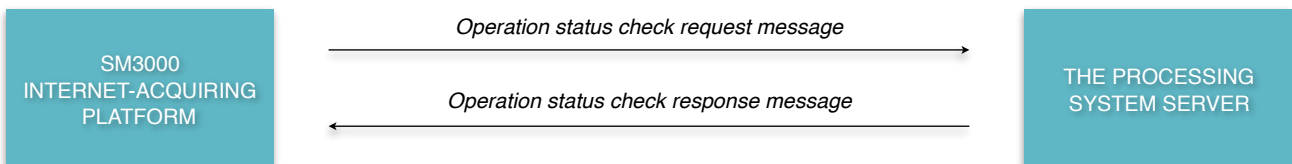
4.10.10. Card credit possibility check request message for p2p

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

| SM3000 INTERNET-ACQUIRING PLATFORM | *Card credit check request message* →

 ← *Card credit check response message* | THE PROCESSING SYSTEM SERVER |
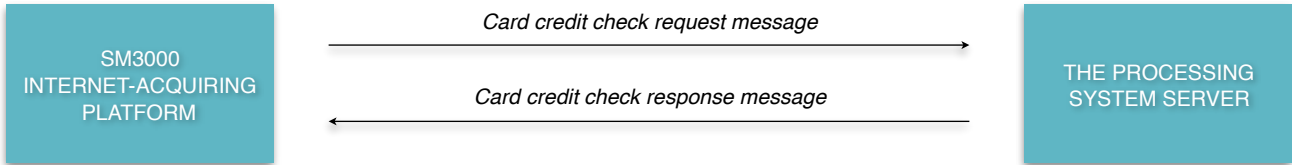
4.10.11. Card debit request message for p2p

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

| SM3000 INTERNET-ACQUIRING PLATFORM | *Card debit request message* →

 ← *Card debit response message* | THE PROCESSING SYSTEM SERVER |
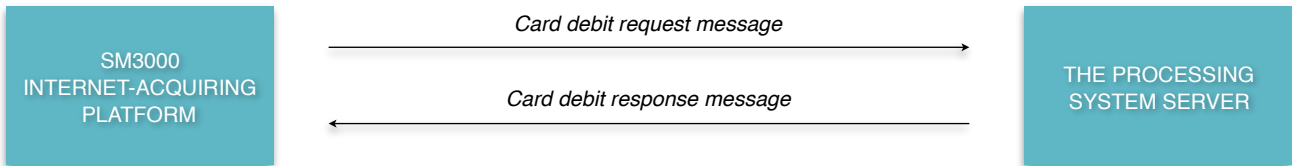
4.10.12. Card credit request message for p2p

This request is used to credit the card.

| SM3000 INTERNET-ACQUIRING PLATFORM | *Card credit request message* →

 ← *Card credit response message* | THE PROCESSING SYSTEM SERVER |
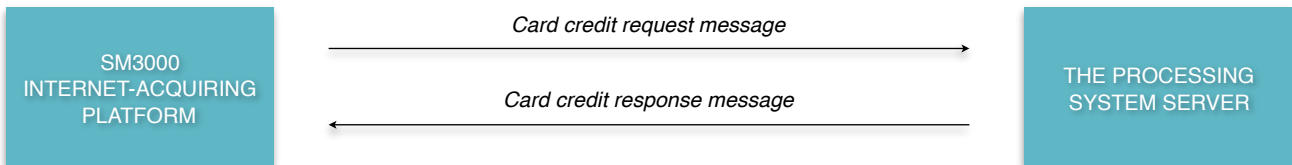
4.10.13. Recurrent charge request message for p2p

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.
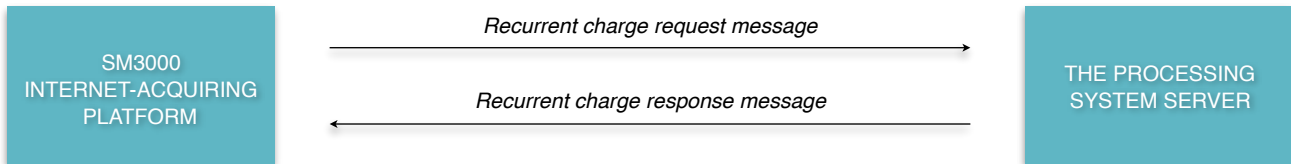
4.11. About Back-office

SM3000 IAP Back-office is developed to cover the main functions of:

- Transactions view and management;

- Merchant and their services management;

- Transactions fees and rates management;

- Payment facilitator/ Operator's Agents management;

- Reports management;

- Customer support management;

- E-mail notification's management;

- Other functions.

4.12. Transactions

Transaction interface covers the functions of:

- transactions search and view;

- corrections management, including chargebacks;

- refunds management;

- notifications management.

To learn more about transactions management see Manual 200105 «SM3000: IAP. Administration interface. Transactions, corrections and refunds».

4.13. Merchants

Merchants part of the SM3000 IAP Back-office covers:

- merchants registration and management functions,
- merchant services registration and management,
- service parameters management.

For further information on the merchants registration and management see the Manual 200106. «SM3000: IAP. Administration interface. Merchants registration and edit»

To learn more about the Merchant's services registration and service parameters management see the Manual 200107 «SM3000: IAP. Administration interface. Merchant services and fees registration and edit».

4.14. Agents

The Platform has the possibility for the Payment operator/ Facilitator to work with their sales agents to contract Merchants for the internet-acquiring services.

The platform covers:

- agents registration and management;

- agent fees management;

- transactions management, made through the Agent.

To know more about the Agents see the Manual 200118 «SM3000: IAP. Administration interface. Agents»

4.15. Reports

The platform has a number of options to work with reports. It has it own internal built-in explorer to create reports using SQL Playground, based on SQL queries and database tables.

In the Platform's documentation we provide some ready-to-go reports, implemented during the Platform installation and setup with a possibility to change them with a new name. To do it we use the built-in SQL explorer.

This part of the Platform covers:

- built-in reports view;

- reports creation, based on SQL;

- graphics and table view of the report's data;

- entire DB view for the SQL creations;

- reports download with the different formats, including MS Excel.

To know more about reports management see the Manual 200109 «SM3000: IAP. Administration interface. Reports»

4.16. Bank

Using this part of the Platform you can manage the data interchange with your Bank-acquirer by the special reports:

- for the clearing and settlement;

- for the merchants and their services creation and changes;

- for the payments to merchants.

> For the further information see the Manuals: 200112 «SM3000: IAP. Administration interface. Merchant registration data export format» and 200113 «SM3000 IAP: Payment register data export format».

4.17. Administration

Administration part of the Back-office covers:

- Logs management;

- Groups and users and their roles managements;

- Customer support management;

- Cardholder notifications management.

To know more about security and logs see the Manual 200110 «SM3000: IAP. Administration interface. Security and logs» and 200104 «SM3000: IAP. Administration interface. Groups and users».

To know more about the customer support functions see the Manuals 200108 «SM3000: IAP. Administration interface. Customer support» and 200111 «SM3000: IAP. Administration interface. Customer support settings».

Chapter 5.   Attachments

This chapter contains the next sections:

This page doesn't contain any information

5.1. Terms and abbreviations

3

3D-Secure   Is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions.

A

API   Application programming interface

Authorization   Is an approval from a card issuer, usually through a credit card processor, that the customer has sufficient funds to cover the cost of the transaction.

B

BO   Back-office, of the SM3000 IAP, where the Operator's employers work to maintain the Platform jobs, as Merchants, Transactions, Agents, Reports and file exchange with a main Processing system.

C

Cardholder   A person who owns a card, such as a cardholder of a credit card or debit card

ChargeBack   Is a return of money to a payer. Most commonly the payer is a consumer. The chargeback reverses a money transfer from the consumer's credit card. The chargeback is ordered by the bank that issued the consumer's payment card.

F

FE   Front-end, of the SM3000 IAP, where the cards authorizations are processed in on-line mode

I

IAP   Internet acquiring platform. The Platform created as a separate application for the Payment operators and Payment facilitators.

ID   Identification number (f.e. transaction ID or Merchant ID)

Incoming-File   The data file, that Platform receives from the Bank's processor

L

Light API   The interface to connect the Merchant's own platform to the SM3000 IAP

M

MasterCard   MasterCard International payment system

Merchant	A legal entity carrying out trading activities on the Internet using the software provided by the system
MPI	Merchant Plug-in

O

Operator	Payment operator or Payment facilitator, that uses SM3000 IAP
Outgoing-File	The data file, that the Platform sends to the Bank's processor

P

PAN	Primary account number, or simply a card number, is the card identifier found on payment cards, such as credit cards and debit cards, as well as stored-value cards, gift cards and other similar cards.
Payment Gateway	A hardware-software complex developed and supported by a payment system that automates the acceptance of payments on the Internet.
Payment System	Payment system between users, financial organizations and business organizations. Allows you to pay, bills and purchases, transfer money.

R

Refund	A process in which a customer returns a product to the original retailer in exchange for money previously paid
Reversal	The operation of crediting funds to the payer's account as compensation for the cancellation of the provision of the service or the poorly rendered service.

S

Service	Merchant's service entry, registered for each MCC. It has its own parameters, fees etc.
SM3000	Sequoia Mosaic 3000. The processing platform of the cards issuing and acquiring processing, ATMs, POSs, e-commerce and m-commerce processing
System	A payment system that allows you to transfer money, accept payment for goods and services through various payment gateways.

T

Transaction	Within the framework of this service, a completely completed data exchange operation with a payment system, including debiting / crediting funds to an end user account.

V

VISA	VISA International payment system

5.2. External documents references

The manual uses the links to the other documentation of the SM3000 IAP, listed below:

Document code	Document name	Document Purpose	Document category
200100	SM3000: IAP. Documents register	The full list and principles to work with SM3000 documentation	User's manual
200102	SM3000: IAP. Getting started	Contains explications of the first steps to work with the platform	User's manual
200103	SM3000: IAP. On-line authorization API	Describes the API formats for the interaction with external systems	Programmer's manual
200104	SM3000: IAP. Administration interface. Groups and users	Describes the users and their roles processes registration	User's manual
200105	SM3000: IAP. Administration interface. Transactions, corrections and refunds	Describes the work with both own and agent based authorizations' transactions, corrections and refunds	User's manual
200106	SM3000: IAP. Administration interface. Merchants registration and edit	Shows the new merchant registration processs	User's manual
200107	SM3000: IAP. Administration interface. Merchant services and fees registration and edit	Describes the MCC registration for the merchant, subscribed services and contracted fees	User's manual
200108	SM3000: IAP. Administration interface. Customer support	Describes the main functions to work with the merchant tickets	User's manual
200109	SM3000: IAP. Administration interface. Reports	Describes the main reports formats	User's manual
200110	SM3000: IAP. Administration interface. Security and logs	Describes the security processes to work with the system and logs functionality	User's manual
200111	SM3000: IAP. Administration interface. Customer support settings	Describes the tickets management setup	User's manual
200112	SM3000: IAP. Administration interface. Merchant registration data export format	Describes the process and a file formats of the Merchant data export	User's manual
200113	SM3000 IAP: Payment register data export format	Describes the process and a file formats of the Payment register data export	User's manual
200115	SM3000 IAP: MPI certificates generation and implementation process	Describes the process of the MPI digital certificates obtaining and implemnnentation	Administrator's manual
200116	SM3000: IAP. Front-end interface. Fraud prevention	Describes how to work with anti fraud filters and algorithms	User's manual
200118	SM3000 IAP. Workstation requirements by a SAAS mode	Describes the SM3000 IAP workstation requirements, using by SaaS mode	User's manual

5.3. The list of the existent Gateway realizations for SM3000 IAP

Table 5.3.0.0. The Templates details page fields description

Platform name	Bank/ Processing	Realization notes
SM3000 EPS	StreamPay, UY RFI BANK, RU	AlbaProcessing, AlbaProcessing Funding, AlbaProcessing P2P, AlbaProcessing EMoney, AlbaProcessing Foreign
CyberSource	CyberSource, US	
TIETO	PastaBank, UE	Pasta Banka
TSYS	Tinkoff, RU	Tinkoff Bank
Way4	AlfaBank, RU	Emoney Alfabank
SmartVista	CardStandard, RU	CardStandard, CardStandard Funding, CardStandard P2P, CardStandard EMoney, CardStandard MTrans

This page doesn't contain any information