ALFEBA
PROCESSING SOLUTIONS

SEQUOIA MOSAIC 3000: CRYPTO (CRYPTO EXCHANGE AND WALLETS)

Functional description

User's manual

Version 2.0

This page doesn’t contain any information

Content

This page doesn’t contain any information

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 CRYPTO, SM 3000 crypto platform of the exchange operations maintenance through the Host and e-wallet of the customer, merchant acquiring and its place in the SM3000 processing solutions. This document was prepared for users of the SM 3000 CRYPTO.

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 CRYPTO 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

700001

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	17.07.2000	-	Init. Version	Natalia Bogorodskaya
2.0.	24.09.2020	s/w version released	Version released	Natalia Bogorodskaya

This page doesn’t contain any information

Chapter 2. About SM3000 CRYPTO

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 CRYPTO of the Sequoia Mosaic 3000.

2.2. About SM3000 CRYPTO

SM 3000 CRYPTO is a crypto platform built on a modular principle, which allows you to choose all the necessary functionality and at the same time optimize the cost of its acquisition: for crypto exchanges, merchants to receive payment in crypto currencies and payers, using the e-wallet of the SM3000 CRYPTO.

2.3. Fraud detection and prevention

Advances in crypto technology have opened up new markets and expanded business opportunities. Ease of customer access to products and services has expanded the ability to attract customers in new directions. However, by creating new sources of income, this new environment has opened the door to new risks.

Criminals also took advantage of these opportunities and devised new, more sophisticated ways to commit fraud and money laundering, attacking the most vulnerable areas of information systems used in business. SM3000 CRYPTO has internal features to detect and prevent fraud, check the cryptocurrencies for theft, execute AML procedures and connect to the external KYC databases.

SM3000 CRYPTO can be integrated with a SM3000 RISK to use the instrument of the additional checks, based on cards and cards based payment products.

2.4. Business cover

SM3000 CRYPTO helps financial institutions to maintain exchange operations with currencies, create and store security components, using Host Security Modules Thales or Futurex, that reduces fraud losses, to provide crypto acquiring for merchants, using virtual POS, or POS-terminal, offer e-wallet to customers, providing the possibility of the secure work with both FIAT and crypto-currencies, to enforce new anti-money laundering regulations, increase operational efficiency and reduce customer damage. The tool allows to implement the features that they need most and that provide the most value for the operations they do.

2.5. Rentability of usage

Financial institutions that use SM3000 CRYPTO have seen significant reductions in fraud losses from the stolen crypto currencies and fines for regulatory non-compliance. In many cases, SM3000 CRYPTO users have recouped their software, hardware and additional staff costs in less than a year.

2.6. SM3000 CRYPTO structural parts

The SM3000 CRYPTO has three main internal structural parts:

1. Customer profile
2. Wallet
3. Trading Crypto Pairs (Financial Instruments)
4. Integration with Fiat payment services (via API requests)
5. Matcher
6. Internal accounting (transaction engine)
7. Queue Handler
8. Fees Guide
9. Interaction with trading API sites.

To learn more about parts see sec. 3.2. Applications structure.

2.7. SM3000 CRYPTO integrations

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

Internal ones:

- SM3000 EPS,
- SM3000 IAP,
- SM3000 PAYMENTS,
- SM3000 RISK,
- SM3000 PERSO.

External ones:

- External exchanges and banking cores.

2.8. The place of SM3000 CRYPTO in the SM3000 processing solutions

SM3000 CRYPTO is a crypto platform, which can be implemented with external authorization processing platforms and accounting systems.

The place of the SM3000 CRYPTO 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 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 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 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.

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. SM 3000 CRYPTO overview

This chapter contains the next sections:

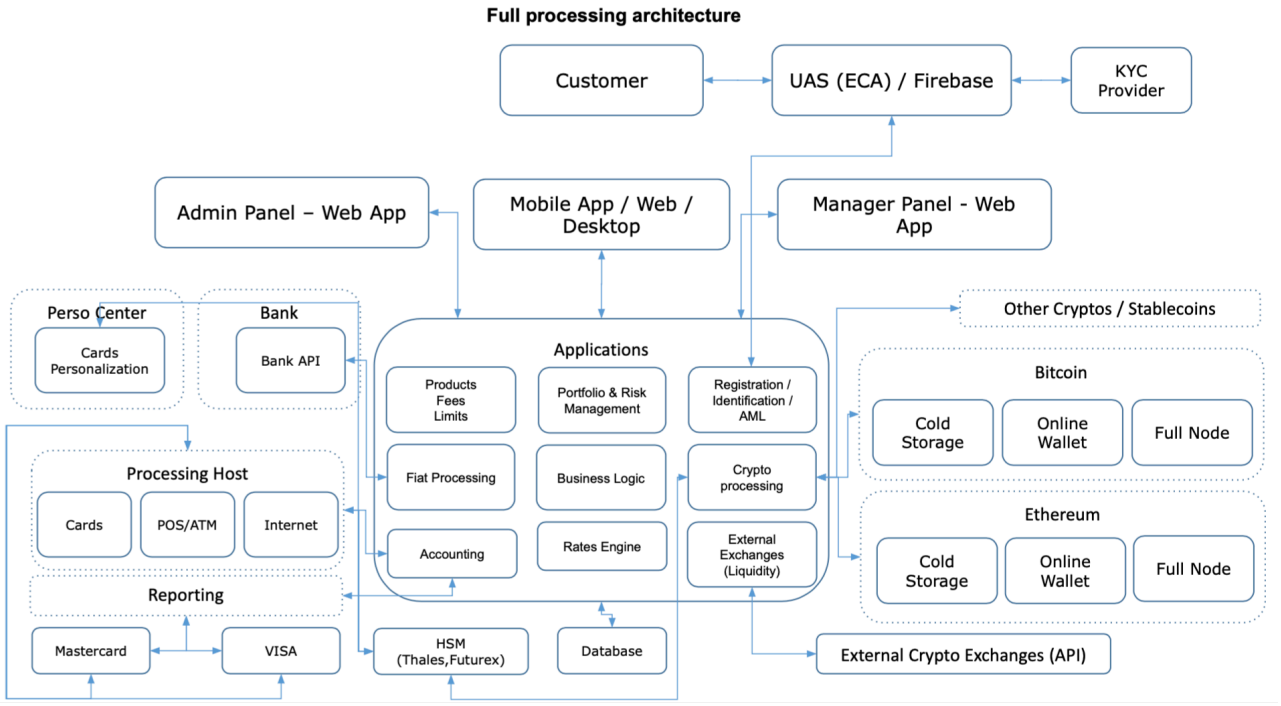
This page doesn’t contain any information

3.1. General information

In the digital economy banks and financial institutions need a new platform, that allows to work with a digital money, or crypto currencies to be competitive on the market. SM3000 CRYPTO offers crypto platform solutions for all participants of the crypto market: issuers, acquires, merchants, exchanges and users.

3.2. Applications structure

The system architecture is presented in the Picture below.



3.3. Components

The SM3000 CRYPTO is an interrelated set of the following components:

- Components that provide support for user accounts (registration, settings, events history, management of the account);
- Components that provide support for cryptographic wallets (cryptocurrency, tokens, cold wallets, monitoring, I / O);
- Components that provide integration with payment services (banks, processing authorization hosts, payment services, monitoring, I / O) and others cryptocurrency exchanges (grabbing quotes, managing your orders, limits, transactions, deposit / withdrawal) applications like mobile apps;
- Components that provide management of balances, orders and user transactions, including the transaction matching mechanism;
- Components that provide internal accounting of all operations, maintaining a queue of payments for each instrument and customer, as well as calculating the required indicators (for example, calculating the effective balance, I / O, writing off fees, calculating the realized financial result and open currency position).
- Components that support the maintenance of the tariff reference book and the implementation of billing (setting tariffs (billing vents)/ commissions (fees), tracking income / expenses, managing the queue for I / O, estimating the deficit / excess liquidity, calculating the most advantageous cross exchange rate).

3.4. User accounts

User account support is provided:

- Each user is represented in the structure of the internal database by a specific set of attributes. The basic set of attributes: email address, login and password, and additional fields are defined additionally and can be expanded, for example, it can be some kind of external system ID with which integration is performed;
- There is a possibility to integrate with two-factor authentication services or a directory system, in this case the user database is the recipient of information from the master system (SM3000 CRYPTO Core);
- If it’ll be necessary, it is possible to customize integration with KYC / AML services and limit the functions of accounts that have not passed KYC / AML, up to blocking the main functions related to trading and depositing / withdrawing funds.

In the base case, the user's personal account is implemented, in which the user have access to the main information on his account:

- Profile Settings;
- User Balances;
- User Transactions;
- Cryptocurrency entry applications (history and status);
- Cryptocurrency withdrawal requests (history and status);

- Orders (requests) of the user (history and status).

Additionally, you can configure any other information relevant to the user:

- Verification process (KYC / AML procedure);
- View and edit profile;
- View user logs in the SM3000 CRYPTO.

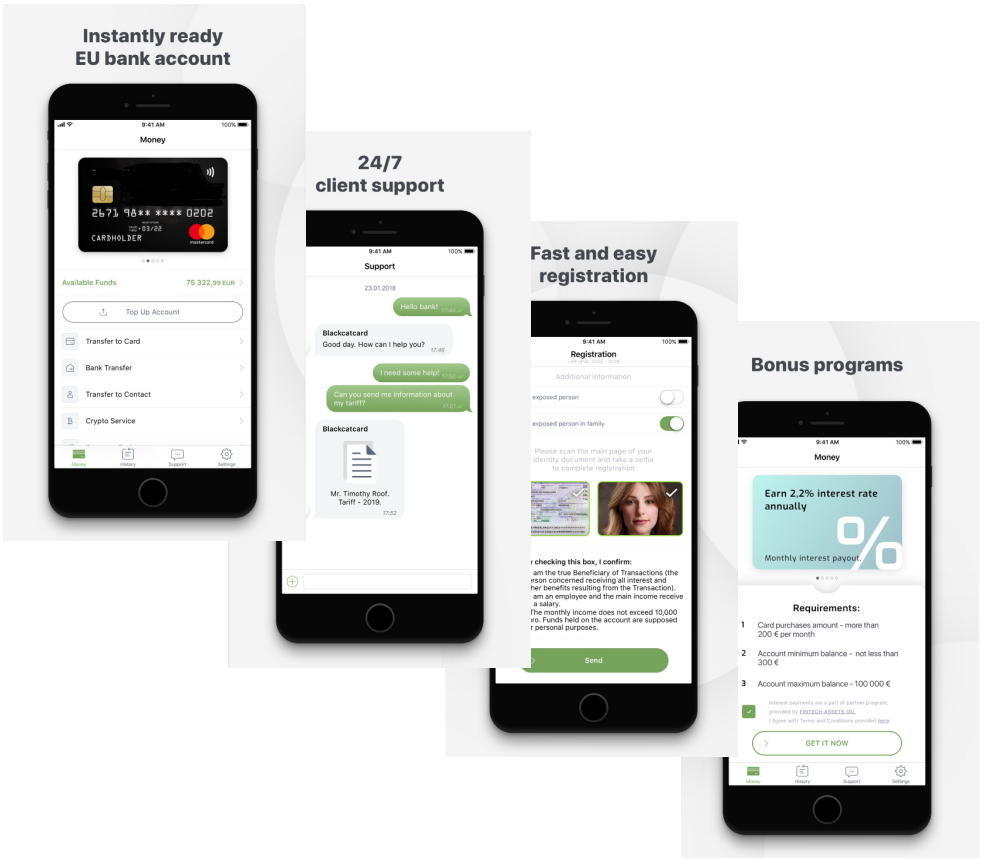
3.5. Crypto wallets

As part of the SM3000 CRYPTO, a cryptocurrency support subsystem (a specific set) is deployed to perform the functions of monitoring cryptocurrency networks, generating addresses / accounts, sending transactions and receiving information about incoming transactions:

- Every cryptocurrency wallet is a raised server with a running domain, a configured config, a downloaded chain (for the needs of parsing transactions and accounts);
- Every cryptocurrency wallet is a customized strapping for generating and storing keys to the cryptocurrency addresses in a safe place;
- Every cryptocurrency wallet has an additional bundle to work with cold wallets (a pre-generated set of private keys that are stored on a separate server without constant online access of internal services;
- Each cryptocurrency wallet has a ready-made set of methods for monitoring the network, receiving information about incoming transactions, generating a new address and sending a transaction. In addition, in some wallets there are additional methods such as address validation, which are also used by SM3000 CRYPTO to increase the security of outgoing transactions;
- A single integration layer has been developed for working with cryptographs using their methods. This single integration layer is used by the main logic of the SM3000 CRYPTO back-office;
- Not only the assets of the SM3000 CRYPTO, but also client cryptoactive assets can be stored in crypto wallets;
- As part of the SM3000 CRYPTO, there is an internal accounting subsystem that allows to keep parallel records of assets without their physical movement in the blockchain;
- Crypto wallets also interact with the queue system, providing input / output of cryptoactive assets.

Switching of one or another cryptocurrency to the support mode is supported (in case of updating the node).

In the basic version, the SM3000 CRYPTO has a standard set of support for popular cryptocurrencies - BTC, ETH, XRP, DASH, LTC, EOS. To add additional cryptocurrencies, you need to connect additional nodes, configure them and expand the integration layer of the SM3000 CRYPTO with methods to work with these cryptocurrencies.



3.6. Financial instruments

Within the framework of the SM3000 CRYPTO, there is a possibility to set up financial instruments - the objects within which the circulation of cryptocurrency assets takes place. This includes both the configuration of the cryptocurrency used and tokens produced on some protocols, and fiat currencies when they are integrated.

In addition to setting financial instruments, can be also configured the relationship of one financial instrument to another - the so-called currency pairs.

3.7. Matcher

The central node of the SM3000 CRYPTO is the match engine, which provides the possibility of placing orders of users, their comparison and conclusion of transactions.

Matcher supports the work of several types of orders (limit, market, trailing). It is possible to develop a list of supported order types.

The result of the matcher is stored in the internal database.

It is possible to enable the mode of mass sale at fixed prices, that is, the sale of tokens to a large number of users.

In addition to the match, the central component is the internal accounting system (transaction engine) that performs the accounting and accounting function. It is within this framework that all financial events within the SM3000 CRYPTO are taken into account, as well as the calculation of the effective balance and the current position for each pair. In addition, internal accounting provides to debit commissions, as well as accounting for external commissions and exchange differences.

For operational and flexible management of income / expenses within the SM3000 CRYPTO, the billing events manual (tariff reference book) is supported, allowing to set up a percentage or fixed rate for each operation, currency pair, financial instrument and customer segment. In addition, the required minimum spread to the quotes of external sites, as well as parameters for determining the minimum allowable cross-currency path, are also indicated here.

To ensure the correct and orderly input / output of users' assets, as well as the assets of the SM3000 CRYPTO itself, there is a system for processing and managing the queue of payments. The queue parameters are configured directly in the internal database, but it is possible to pull them into the personal account of the manager / administrator of the SM3000 CRYPTO. If necessary, the processing and queue management system can also be used to work with applications for input / output of fiat assets.

3.8. Integrations

The SM3000 CRYPTO can be integrated with various Fiat payment services and banks. It is implemented a full set of functions for I / O and lock assets, as well as obtaining information about the client and his accounts. To connect a payment service, it is necessary to conduct a mapping between internal methods of the SM3000 CRYPTO and external methods of a connected payment service.

Within the user's personal account there is a section that displays information about the user's assets with the necessary buttons for input / output assets.

The SM3000 CRYPTO for reinforcement with liquidity or for selling excess liquidity must have customized integration gates on other exchanges and exchange offices. For this, mapping and tuning methods between the platform and the SM3000 CRYPTO are also performed.

Within the personal account of the manager of the SM3000 CRYPTO, there is a section within which information about current positions on all partner sites is displayed, as well as buttons for managing orders, making deals and entering / withdrawing assets.

3.9. Encryption standards

ALFEBA uses the encryption standards for the SM3000 CRYPTO, presented in the Table 3.9.0.0.

Table 3.9.0.0. The SM3000 CRYPTO 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, 3DES, RSA

Chapter 4. Attachments

This chapter contains the next sections:

This page doesn’t contain any information

4.1. 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

4.2. External documents references

The manual doesn’t use any link to the other documentation of the SM3000 IAP.

ALFEBA

Agraciada 2770 Montevideo 11823 Uruguay

Phone: + 598 2 2083142

E-mail: docs@alfeba.com

www.alfeba.com