Elexapay Technical Whitepaper

www.elexapay.com

Version 1.0

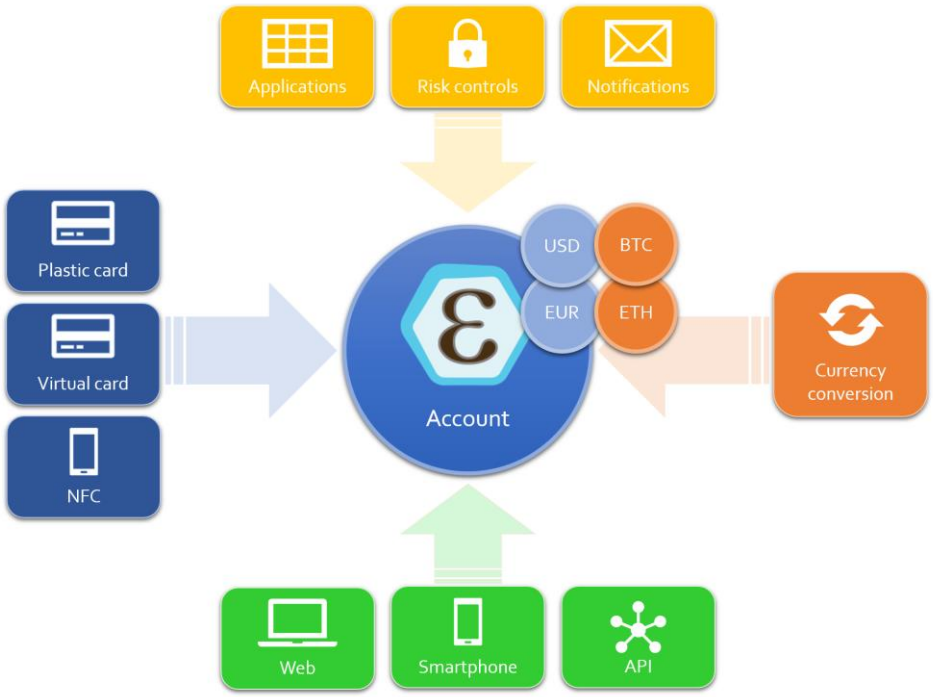
10 Jan 2018

Introduction

The heart of Elexapay is an account with different access methods and functionality built around it. Each account can have unlimited number of components to store different currencies on it. Components can store both regular and cryptocurrencies with instant transfer from one component to another using current market rate. Each account can have unlimited cards attached to it. One card can be attached to one currency component with dynamic currency conversion when required so by incoming transaction.

Besides standard payment card functionality Elexapay offers you advanced account features. Application server allows you to configure different types of automated payments as well as trigger different automatic actions based on different market criteria. Risk management engine protects your funds by analyzing transactions using system and user defined security rules and declining fraudulent attempts.

Elexapay supports different notification features. Notification can be triggered when there is an activity on the account either it is automatic triggered payment or transaction above defined value.



Software Architecture

Elexapay system consists of set of independent service oriented applications. Each application is used for own purpose and exposes its own API. All applications connect to central relational database. Technology stack used is following:

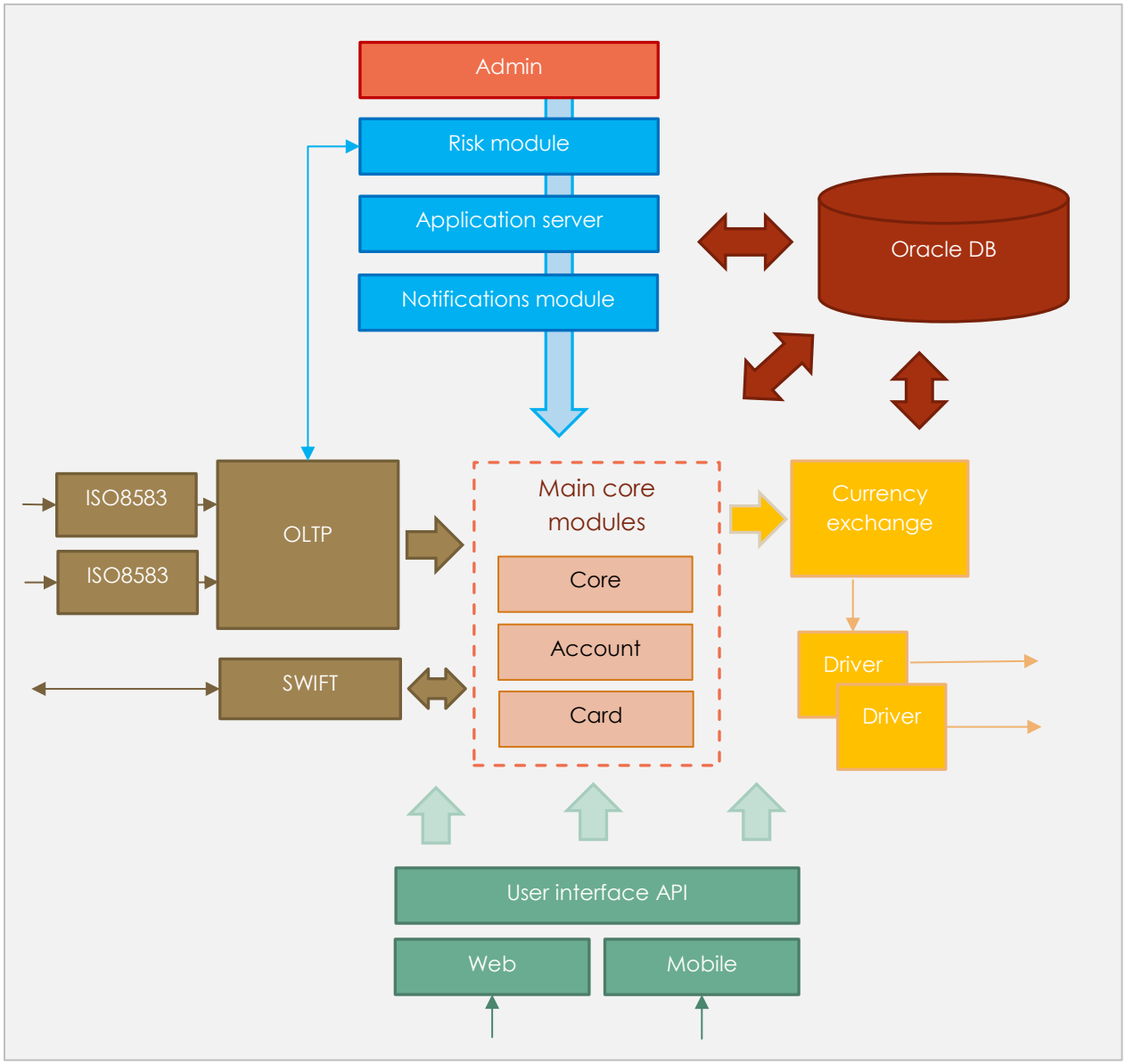
- Node.js JavaScript framework for SOA;
- Debian Linux server;
- Oracle relational database for data storage;
- C++ Linux application for ISO8583 low-level communication;

System itself consists of following modules and software components:

- Core module with API – used for core system activities and API request dispatching;
- Account module with API – responsible for creation and management of account entity and account currency components;
- Card module with API – responsible for issuing and management of plastic, virtual and NFS cards. Performs card related checks and authorization;
- OLTP module – responsible for handling of online transactions received from card networks and devices;
- SWIFT driver – responsible for communication with SWIFT service;
- User interface API – exposes set of actions available from user interfaces;
- Web interface – connects to user interface API and allows user to perform activities using web interface;
- Mobile application - connects to user interface API and allows user to perform activities using mobile device;
- Payment application server with API – standalone module with scheduler, responsible for triggered payments and automated actions;
- Risk module with API – rule based module for transaction security checks;
- Notifications module with API – module responsible for sending account activity notifications to the customer;

- Currency exchange module with API – module responsible for currency exchanges and communication with stock exchange using drivers;
- Stock exchange drivers – drivers, that communicate with cryptocurrency stock exchanges using provided API;
- ISO8583 driver – standalone program used for communication with partner bank via ISO8583 financial protocol;
- Admin module – administration standalone application, used for internal handling of the system;

Diagram below illustrates connections between described software components:



Organizational Structure

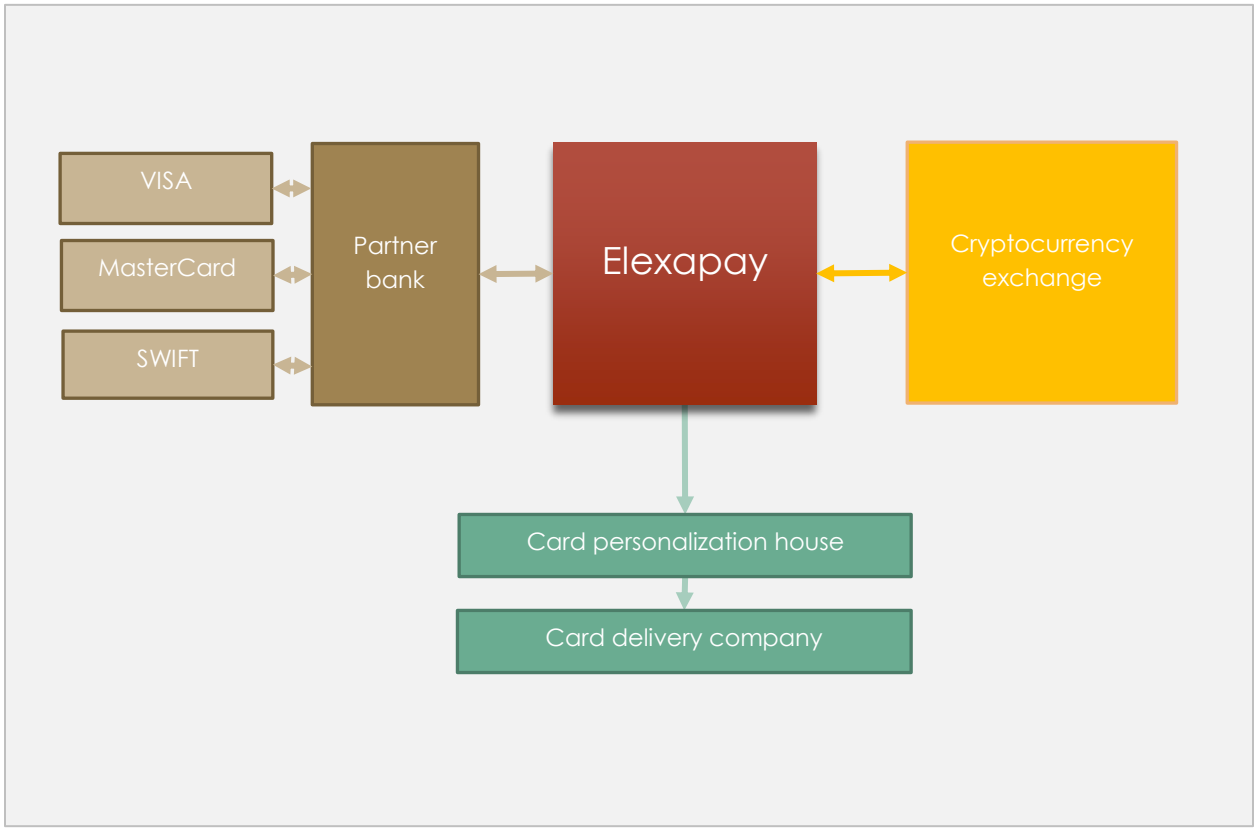
Some payment card related activities require heavy development and significant investments into hardware, so it was decided to outsource these activities to trusted partner organizations with existing infrastructure and certificates within financial institutions. Following tasks will be handled outside of project organization:

- payment card EMV personalization;
- plastic card delivery;
- payment card EMV and PIN authorization;
- MasterCard/VISA interfaces;
- SWIFT interface;

Following tasks will be handled outside of project organization due to risk of financial loses:

- cryptocurrency exchange;

Diagram below illustrates connections between organizations:



Card Types

Elexapay will support following card types:

- Real plastic card – this is regular classic EMV chip card. Card will have contactless interface. Elexapay system will generate all required data and export it to personalization house, where it will be encoded to chip and magnetic stripe.
- Virtual card – Elexapay will generate all required data and make it available instantly. Card is meant for internet purchases and does not require to be encoded into plastic.
- Smartphone application – generated data will be exported to personalization house and sent to customer smartphone with NFC chip.

Transaction Processing

Partner bank organization already has its own interfaces to major payment networks and will ensure full set of supported transaction types to be forwarded to Elexapay. Transaction set includes:

- POS sales;
- POS pre-authorizations;
- ATM cash withdrawal;
- ATM balance enquiry;
- ATM MoneySend transactions;
- Refunds;
- Reversals of all mentioned transaction types;

Disputes will be handled by Elexapay internally. Dispute will be initiated by each customer individually when required using web interface.

Currency Conversion

In order to support currency conversion Elexapay will interface with one or several cryptocurrency stock exchanges. When customer wishes to exchange regular currencies to cryptocurrencies and vice versa, Elexapay will execute market order on selected stock exchange. To avoid sending funds through blockchain every conversion operation Elexapay will have its own pools of cryptocurrencies.

Application Server

One of advanced features that Elexapay will offer is application server. Application server will have its own scheduler and will scan system for events of different types. Customer can set up different actions to be executed at scheduled time or upon particular system event. Scheduled actions can be periodic. Application server can be used as framework and more actions and events can be supported in future. Following actions will be supported at the start of service:

- Funds transfer via SWIFT;
- Mass payouts via SWIFT;
- Funds transfer to another Elexapay account;
- Mass payouts to other Elexapay accounts;
- Conversion between account components;
- Block card;
- Unblock card;
- Change card usage limit;

Actions can be triggered at:

- Particular date and time;
- Upon incoming funds transfer;
- Upon market exchange rate change;

Risk Server

Risk server will check incoming transactions and will try to determine if transaction is fraudulent or not based on defined rules. System will provide set of pre-defined rules which can be switch on or off by each customer. Below are examples of some basic rules:

- More than certain number of unsuccessful attempts to guess the PIN or amount;
- Transactions with physical card made from different countries in short period of time;
- Transactions with physical card made from non-EMV device or with incorrect EMV counters;

Also risk server will allow to configure different card usage limits based on previous usage statistics. Customer will be able to configure:

- Amount and number of transactions allowed within period of time (e.g. day, week, month);
- Decline completely or limit transactions from certain merchants (e.g. casinos, gas stations);
- Decline transactions from particular countries;
- Decline or limit particular operations (e.g. cash withdrawals, transfers);

Notifications

Notifications subsystem will notify customer when there is an activity on the account. Notification can be sent when:

- Account is debited or credited;
- Scheduled action is triggered in Application server;
- Incoming or outgoing funds transfer above defined amount is performed;
- Transaction above defined amount is approved;
- Transaction is declined;
- Risk server rule is triggered;

Notifications can be delivered to customer via:

- Email;
- SMS;
- Mobile application popup;