Overview

This section provides general information about the solution, terminology description and a high-level description of the business and technical of the Money Transfer Hub.

Abbreviations

Abbreviations used in the document:

Abbreviations	**Description**
ACQ	Acquiring Institution/Acquirer
AP	Admin Panel
ACS	Access Control Server
C2C	Card to card
DC	Data Core API
P2P	Peer to peer API
MDC	Mobile Data Core API
SDK	Software Development Kit
THC	Transaction History Core
OS	Operative System
IBAN	Bank Account Number
MCS20	Mastercard Send 2.0
URI	Uniform Resource Identifier
Mid	Merchant Identifier

Terminology

This section explains a number of key terms and concepts used in this document:

Name	Description
Customer	Institution which is using Verestro products. This institution decides which SDK should be used and how transaction should be processed. Basicly Customer can be called Verestro client.
User	User which is using Money Transfer Hub Application. It is root of entity tree. User is identified in Wallet Server by some unique identifier which is provided after registration. User can have access to his data and operations based on session. User’s session is created after device pairing is performed. When session expires then user authentication have to be performed. Session is valid 10 minutes, however it is configurable parameter.
Card	Card belongs to the user. User can have many cards. Card is identified via internal id given after storing card on Wallet Server. Whole PAN is stored on Wallet Server which has PCI DSS certificate.
Device	Device belongs to user. When user starts using application after installation then device pairing is performed. After pairing device with some unique id, unique device installation id is generated and this installation is assigned to user. It is possible to have one active installation on specific device for specific user.
Session Token	Token which defines User. It is an authorization way of the User. This entity is created after paring device and this is needed to perform any actions in the application. When session is expired then user authentication needs to be performed. Session is valid 10 minute s, however it is configurable parameter.
Sender	Verestro Wallet user which triggers transaction to the Receiver (check User description).

Receiver	Receiver can be identified in Wallet Server (Internal) or may be an entity that does not exist in Wallet Server (External) ◦ Internal – this type of Receiver has his own unique identifier just like sender. It can also act as a Sender in the transaction process, ◦ External – this type of Receiver does not exist in Wallet Server. Transfers that are made to this type of Receiver require the entering of his card data by Sender
Mid	Merchant identifier. This entity is representing Merchant in Acquirer’s system. Customer have to provide the mid information to enable mid configuration in the Verestro system. Required to process 3DS authentication via Verestro System.
Acquirer	External institution responsible for processing transaction and 3ds requests ordered by the Verestro Money Transfer Hub Application. Acquirer connects with banks / card issuers and returns information whether the ordered action on a given card is possible.
PAN	It is 7-15 digits of credit card number. These digits contain the Permanent Account Number (PAN) assigned by the bank to uniquely identify the account holder.
Wallet Server	Provides the backend services to support Mobile Payment Application via Verestro Wallet SDK and is responsible for managing users, devices, cards , device tokens, storing transactions history and communication with Acquirers.
PCI DSS	PCI DSS (Payment Card Industry Data Security Standard) is a security standard used in environments where the data of payment cardholders is processed. The standard covers meticulous data processing control and protection of users against violations.
IBAN	IBAN (International Bank Account Number) is an international standard for bank account numbering that allows you to transfer funds to foreign accounts and to receive transfers from foreign entities to domestic bank accounts. One of the assumptions of the IBAN standard is to simplify the system of cross-border transfers.

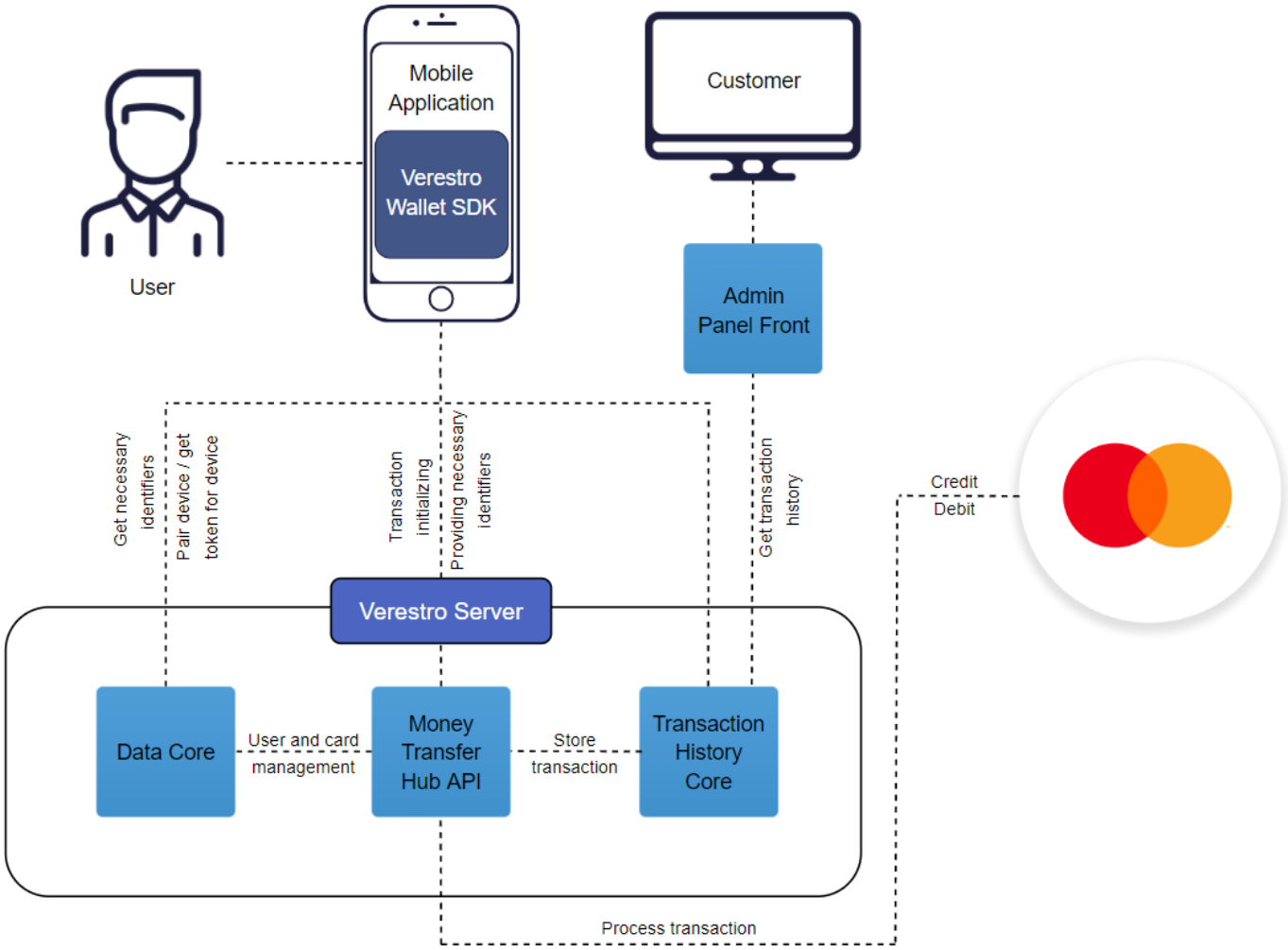
QR	QR code is a type of barcode or scannable pattern that contains various forms of data like website links, account information, phone numbers, or even entire object of the transaction. *Transactions with QR code are detailed in separated documentation: QR Payments*

Mastercard Send 2.0

Mastercard Send 2.0 is a technology which enables peer to peer transfer via mobile device. This functionality allows banks and payment institutions to perform transactions using cards, IBANs, QRs or other URI. Each transaction pushed to Mastercard is settled with the payment institution / bank registered in this program on a settlement basis (collective invoice 1 per day).

MC Send 2.0 Payments high level overview

This diagram shows high level components which are involved in whole solution.



MC Send Payments Key Components

Component	Description
Verestro Wallet Server	Backend services of Money Transfer solution. In the described product, they are responsible for adding / keeping the context of the user and the card in the database, user authentication, calculate commissions, forwarding a transaction requests to Mastercard Send 2.0 or keeping transaction history.
Verestro P2P Wallet SDK	A set of functionalities that allow to handle user requests and provide the required information to backend services which are required in Mastercard Send 2.0. Simply put, this component allows to take advantage of the possibilities offered by Verestro Wallet Server.

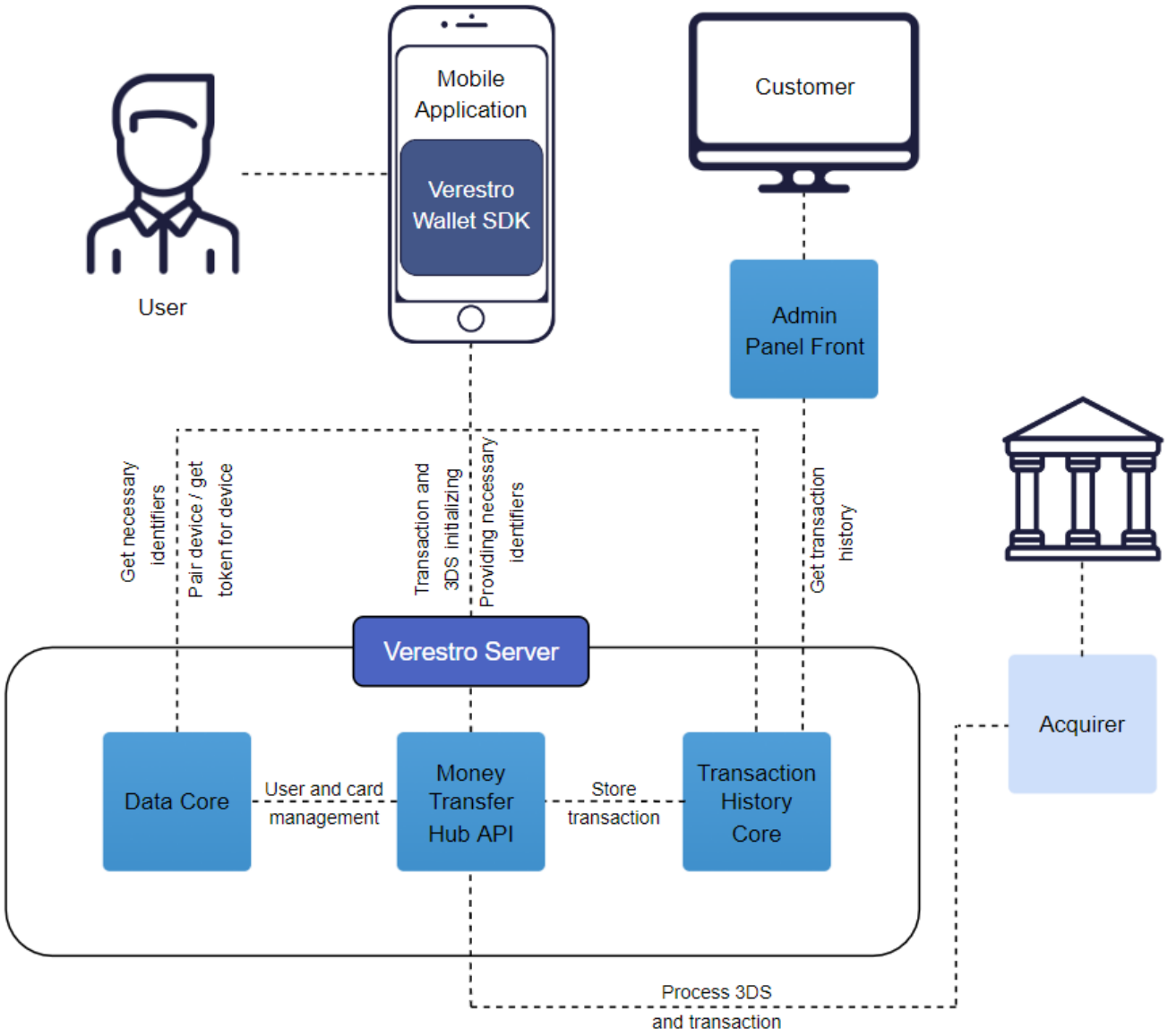
Notification Service	Delivers all necessary information about transaction statuses and other actions offered by Money Transfer which was performed between individual Verestro backend components and/or external.
Admin Panel	Frontend component that allows Customer to check transaction statuses and transaction history of his clients.

Card to card transaction

Card to Card Payments (C2C) is a technology which enables peer to peer transfer via mobile device. This functionality allows banks and payment institutions to perform transactions from Sender card to the Receiver card. In the first setting, the settlement agent performs Funding, in the next, it pushes funds by making Payment. In this type of transaction, Funding is possible only for users strongly verified using the 3DS Authentication method, which is described later in the document and it is an individual requirement depending on the Settlement Agent.

Card to card transaction high level overview

This diagram shows high level components which are involved in whole solution.



Card to card transaction key components

Component	Description
Verestro Wallet Server	Backend services of Money Transfer solution. In the described product, they are responsible for adding / keeping the context of the user and the card in the database, user authentication, calculate commissions, forwarding a transaction and 3ds authentication requests to various Acquirers or keeping transaction history.
Verestro P2P Wallet SDK	A set of functionalities that allow to handle user requests and provide the required information to backend services which are required by Acquirers in C2C transfers. Simply put, this component allows to take advantage of the possibilities offered by Verestro Wallet Server.
Notification Service	Delivers all necessary information about transaction statuses and other actions which was performed between individual Verestro backend components and/or external.

Admin Panel	Frontend component that allows Customer to check transaction statuses and transaction history of his clients.

> Verestro Money Transfer Hub also supports transfers using a QR code. Transfers using the QR code are described in a separate document here

Verestro Money Transfer Hub

Verestro Money Transfer Hub is a solution that was created to make it easier for customers to make quick transfers between two entities - Sender and Receiver. Money Transfer Hub provides functionalities for the management, identification and verification of Users and the possibility of making transfers based on specific methods of data transfer, such as internal user identifiers, data entered basicly "from the finger", QRs etc.

Solution consists of:

- Server components:
  - Wallet Server – backend component,
  - Wallet Admin Panel – frontend component,
- Mobile components:
  - Wallet SDK – Android / iOS libs.

Wallet Types

Money Transfer Hub Solution supports one type of wallet which can be used in the implementation:

- OPEN - user registers itself in the application and provides data like PAN etc.

Note that the Receiver is not required to be a client of the application. The Sender can perform transactions to external Receivers this way as well.

Implementation models

Verestro provides three different implementation models for products: REST API, integrated and standalone version.

REST API

In this model Verestro provides Money Transfer Hub API methods. Customer is responsible for integrate with provided API methods with his own application and manage User authentication (based on MDC SDK).

Integrated

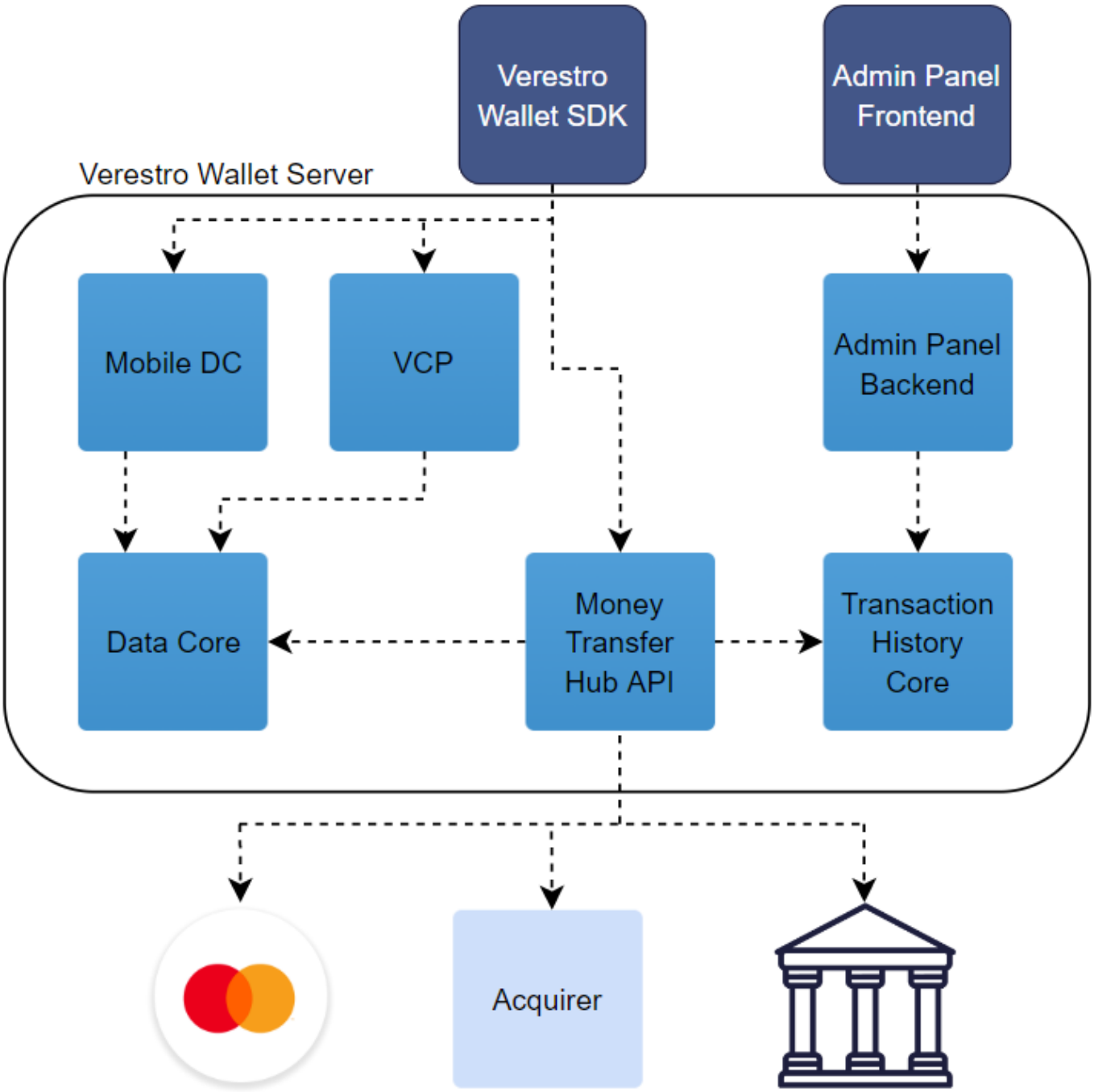
In this model Customer is owner of Money Transfer Hub Solution. Verestro provides Wallet SDK and Wallet Server. Customer is responsible for integrate provided SDK with his own application and manage User authentication (based on MDC SDK).

Standalone

In this model Verestro provides whole Money Transfer Hub Solution: “Ready to use” application with implemented SDK. Furthermore, Verestro manages direct User authentication.

Architecture

This diagram shows big picture of Verestro Money Transfer Hub architecture.



Server Components

Server components are backend services which are designed to process requests from the mobile part, provide the necessary information such as user ID and communicate with Acquirers.

Deployment Models

In Money Transfer Hub Solution Server components are deployed and configured on Verestro side. Verestro is responsible for maintaining infrastructure, deploying applications and monitoring.

Wallet Server

Wallet Server is the backend component which consists of few internal services which are responsible for managing users, cards, IBANs, security tokens, transactions and transactions history. This component is also responsible for connection with Acquirers. Services included in the Wallet Server component can be divided into two groups:

- Services that are part of the Money Transfer Solution.
- Services supporting the functionalities offered by Money Transfer Solution.

List of services which are the part of the Money Transfer Solution:

- Mobile API - available via Wallet SDK to performs operations directly from mobile device, performs client app authentication.
- Wallet Mobile SDK - The mobile part of the Money Transfer solution. Responsible for forwarding customer requests to the appropriate Verestro backend components. All key processes such as logging in, authentication or transaction take place through this component.
- Money Transfer API – One of the Verestro backend services. This service handles requests from Verestro Wallet SDK and communicates with other Verestro internal services which are supporting the Money Transfer solution. Money Transfer Hub API is also responsible for communication with the Acquirer.

List of services which are supporting the functionalities offered by Money Transfer Solution (each of the services listed below has dedicated documentation):

- LC API - server API dedicated for Issuer to manage users and cards data on Wallet Server. Connection is secured using VPN,
- MDC API - server API which is responsible for providing access token to Mobile API. It is also an intermediary between the mobile SDK and Data Core,
- DC API - server API which stores card and user data,
- Admin Panel – frontend application which allows Customer to check transaction status and/or history,
- Midas API - server API integrating Acquirers and their individual 3ds authentication strategies. Additionally Midas API stores mid configuration,
- THC API - server API responsible for keeping transaction history. The data stored in the THC API is used by the Admin Panel.

Wallet Server operates with domain objects like:

- User (Sender) - User which is using Money Transfer Hub Application,
- Session Token – Token which defines User. It is an authorization way of the User,
- Device – This entity is created after user registration and is required to login the User,
- Card - User Card which can be charged or recharged,
- Receiver - Verestro Wallet user or external entity which receives funds from the Sender,
- IBAN - belongs to user. User can have many IBANs. IBAN is identified via id which is sha256Hex value of IBAN. One IBAN can be assigned to multiple users.

More detailed information about objects above are described in Terminology chapter.

Wallet Admin Panel

Wallet Admin Panel - web frontend application which is dedicated for Customer to follow user's transactions. Using the admin panel, the customer can also add his users to the Verestro Wallet database.
This component is not a part of the Money Transfer Solution but it is supporting some features. For more information about Wallet Admin Panel see "Verestro Wallet Admin Panel Documentation".

Mobile Components

Mobile components are dedicated for using on Android and iOS mobile devices.

Wallet SDK

Verestro provides Software Development Kit (SDK) called Wallet SDK which can be used for mobile money transfer. As a company Verestro provides many products which can be used in single application. For that reason Wallet SDK is divided into separated modules which covers different functionalities. There are two main modules dedicated for Verestro Money Transfer Hub Solution: P2P SDK and QR SDK. P2P SDK provides user data management such as authentication and payment cards management. It is also responsible for initiating peer to peer transactions and for adding individual recipients to "favorites".

QR SDK is responsible for creating the appropriate QR code, parse it and for transferring the data contained in this code. Based on such data, a transaction will be initiated.
Note that both SDKs are separated. This means that the for example P2P SDK will not have components that have a QR SDK.

Below is a detailed list of SDKs included in Mobile Components:

- P2P Transfers SDK - supports the process of generating and reporting transactions. The share of this module in the application takes its payment functions to a higher level, enabling the initiation of transfers to a card, telephone number or QR code *(for more technical information please check "P2P Transfer SDK documentation")*.
- P2P Receivers SDK - supporting module that improves the service of senders. The function allows you to store a list of recipients for a given user and to obtain data for transaction initiation to a telephone number *(for more technical information please check "P2P Receivers SDK documentation")*.
- QR SDK - The QR module was designed to work with the applicable MPQR (Merchant Presented QR) standard developed by EMV. Thanks to the integration of this module with P2P and meeting the requirements of Mastercard, the user will be able to pay with sellers using QR codes. An additional functionality is that the user can use the code generated for his card and thus receive funds from other people within one implementation *(for more technical information please check "QR SDK documentation")*.

Access

The account at Verestro Artifactory is required to get access to Verestro repository.

Versioning

SDK version contains three numbers. For example: 1.0.0.:
(For more information check what is “Semantic Versioning” standrand)

- First version digit tracks compatibility-breaking changes in SDK public APIs. It is mandatory to update application code, to use SDK, when this is incremented.
- Second version digit tracks new, not compatibility-breaking changes in public API of SDK. It is optional to update application code, when this digit is incremented.
- Third version digit tracks internal changes in SDK. No updates in application code are necessary to update to version, which has this number incremented.

Changes not breaking compatibility:

- Adding new optional interface to SDK setup,
- Adding new method to any domain,
- Adding new enum value to input or output,
- Adding new field in input or output model.

Communication with Wallet Server

Wallet SDK at the very beginning performs authentication of application and device to Wallet Server.

Security

MDC SDK is responsible for most of the security issues. However, in the Money Transfer Hub solution, sensitive data such as PAN or CVC are processed. They are taken as an array of characters. This data is not held, but immediately wiped from RAM.

Security Checks and Data Clearing

There are performed security checks on Wallet SDK side. Security checks consists of:

- root access detection,
- hooking protection,
- debugging protection,
- custom ROM protection,
- data tampering protection.

Requirements

Wallet SDK has some mandatory requirements to make it work:

- device cannot be rooted,
- Android OS should be in version 6.0 or above,
- iOS OS should be in version 13.0 or above,
- devices cannot have enabled debugging,
- MDC SDK integration.

Configuration

The entire solution requires configuration data necessary for the product to operate in line with the Customer's expectations. The most important information is:

- Product’s name – this name will be representing a given Issuer in Verestro system,
- How transactions are reported to THC – this point tells about what type of transactions and transactions with what status will be reported to the transaction history database. For example:
  - whether the transaction should be stored in THC while at the funding stage or only when the recipient's account top-up has been performed,
  - whether transactions with FAILED status should be reported or only successful transactions,
- To which ACQ we should send the transaction request,
- Whether the product is supposed to support 3DS or not,
  - If the Product supports 3DS, Verestro have to integrate into this process with a given ACQ (unless it has already been done),
  - If the Product supports 3DS, the Customer have to provide the data of his account created in the ACQ’s system such as login, password, merchant Id (mid) and terminal Id if exists (unless the whole mid configuration already has been done in Verestro system).

Revision #37
Created 18 March 2022 13:29:20 by Wojciech Nowakowski
Updated 27 July 2022 06:00:48 by Jakub Kotyński