Overview

This chapter describes the terminology used in the document as well as the components of the Verestro system that are part of the C2C Widget.

Terminology

Name	Description
Client User	A user registered in the client service. Roles in the C2C Widget: • generating and sending links to the C2C Widget to users outside the client application, • is the recipient of a C2C transfer carried out using a widget, • is not a direct user of the widget.
C2C User	A user registered for a service hosted in the C2C Widget. Roles in the C2C Widget: • registration in the C2C Widget, • is the sender of a C2C transfer carried out using a C2C Widget
Client	Verestro partner, enabling its users to receive transfers made by C2C users. The client allows its users to generate a link to the widget to C2C users via its application.
App	A client application in which the client provides services to its users, e.g. a banking application. In the application, the client allows users to generate and send a link to a C2C Widget to a user outside the application.
Acquirer	An external institution that communicates with the card issuer, protects against fraud and taking responsible for executing the transaction and checking the correctness of 3D Secure authentication.
Card	It is a payment instrument issued by the issuer to a given user. Users can send funds using the card.
Issuer	Bank, card issuer. It determines whether a given transaction can be performed and whether 3D Secure authentication is needed.

> Client user ≠ C2C user.
> Application ≠ C2C Widget.

Application components

This chapter is describing all components involved in the processes included in the C2C Widget product. Each of the sections below describes one of the components.
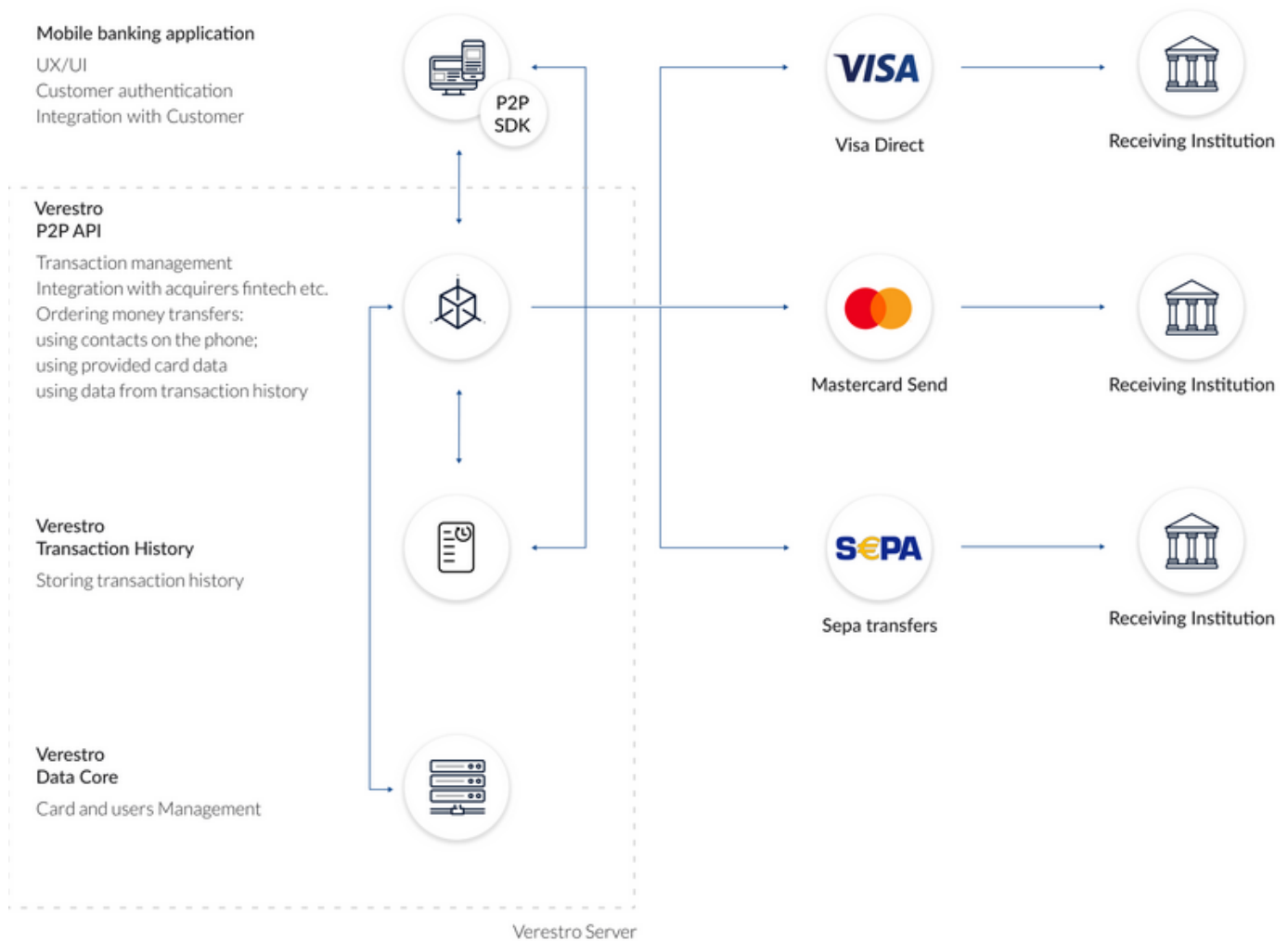
LC API

The main purpose of Verestro Lifecycle API & SDK web service is to add and manage user and payment cards in a safe way. All data are transfered to Verestro Data Core system which is placed in PCI compliant zone and is fully secure.

LIfecycle API is an internal service secured by x509 certificate, which increases the safety of transported data. The API communicates with the data storehouse called DataCore. DataCore is internal service and one of crucial components of Verestro's product line-up. Its main responsibility is to provide secure, PCI-DSS compliant storage for cardholder data. DataCore manages the status of the user and their aggregates. All other product in implementation connect to DataCore which returns information about the user and his aggregates.

P2P Service

Money transfers (P2P Service) enable users to initiate domestic and international transfers. The platform has several available configurations: sending and receiving funds, payments from and to cards, transactions from and to stored value account (SVA), ACH transfers.

Architecture

Mobile banking application
UX/UI
Customer authentication
Integration with Customer

P2P SDK

VISA
Visa Direct

Receiving Institution

Verestro P2P API
Transaction management
Integration with acquirers fintech etc.
Ordering money transfers:
using contacts on the phone;
using provided card data
using data from transaction history

Mastercard Send

Receiving Institution

Verestro Transaction History
Storing transaction history

SEPA
Sepa transfers

Receiving Institution

Verestro Data Core
Card and users Management

Verestro Server

THC (Transaction History Core)

Service is designed to work in cooperation with other services from Verestro product line. This API offers methods that allow managing information about transactions. Transaction History Core allows on checking the history of transactions in the C2C Widget.

KYC (Know Your Customer)

After logging in, the user goes through an intuitive process KYC, which allows for instant identity verification in accordance with the AML (Anti-Money Laundering) regulations. The system automatically analyzes user data, ensuring the highest level of security and protection against financial fraud.

In order to pass KYC, it is necessary to take a photo of an identity document and pass liveness. Liveness is a biometric verification that involves the user recording a short video of themselves showing their face and making gestures as instructed.