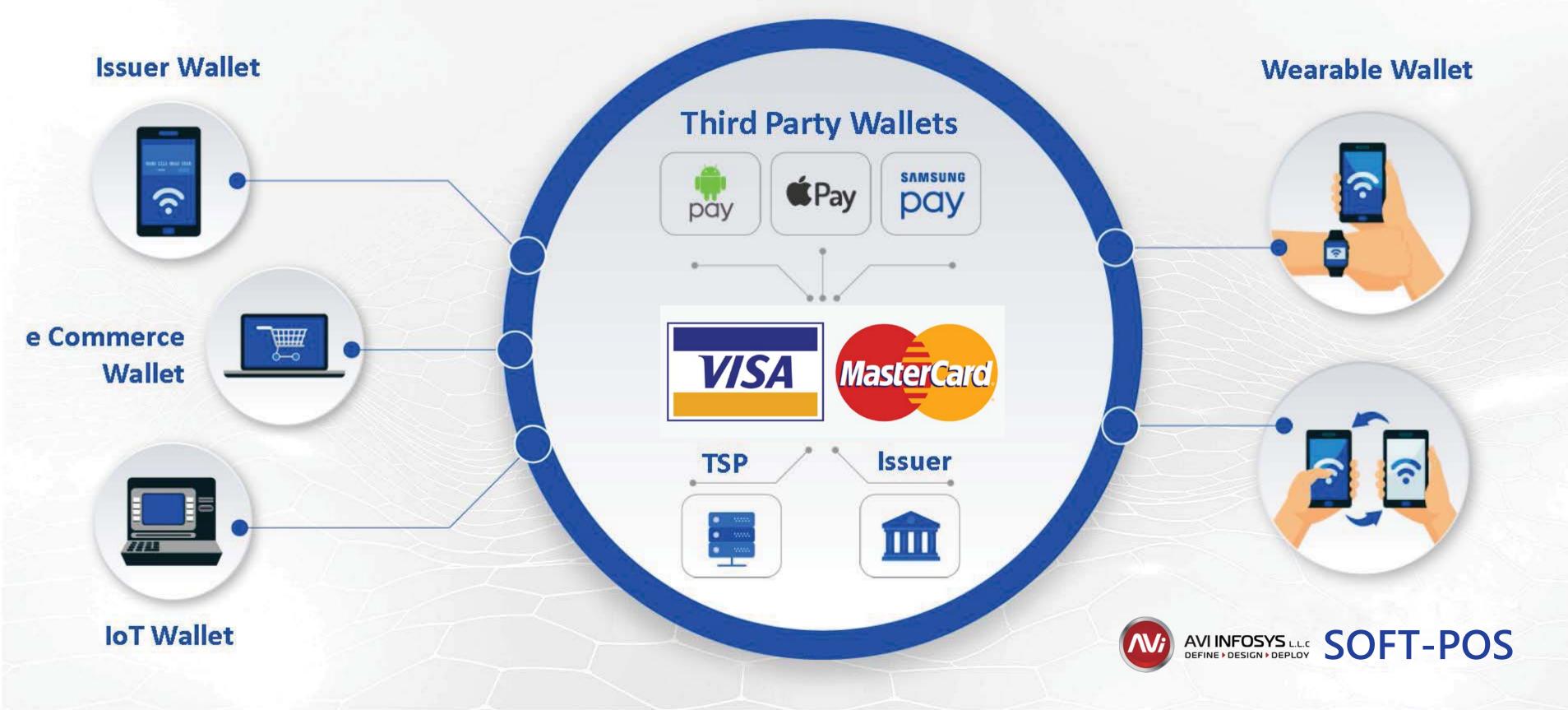


TOKEN ECOSYSTEM IN THE FUTURE



AVI INFOSYS SOFT-POS Solution



Accepting payments using digital wallets and wearables devices

Accepting payments using contactless cards

AVI INFOSYS SOFT-POS SOLUTION OVERVIEW



The merchant' mobile application provides acceptance contactless cards and digital wallets acceptance



Payment processing is performed through the AVI INFOSYS – SOFT-POS TMS (Terminal Management Server)



The merchant's mobile device must be able to exchange data wirelessly through open networks

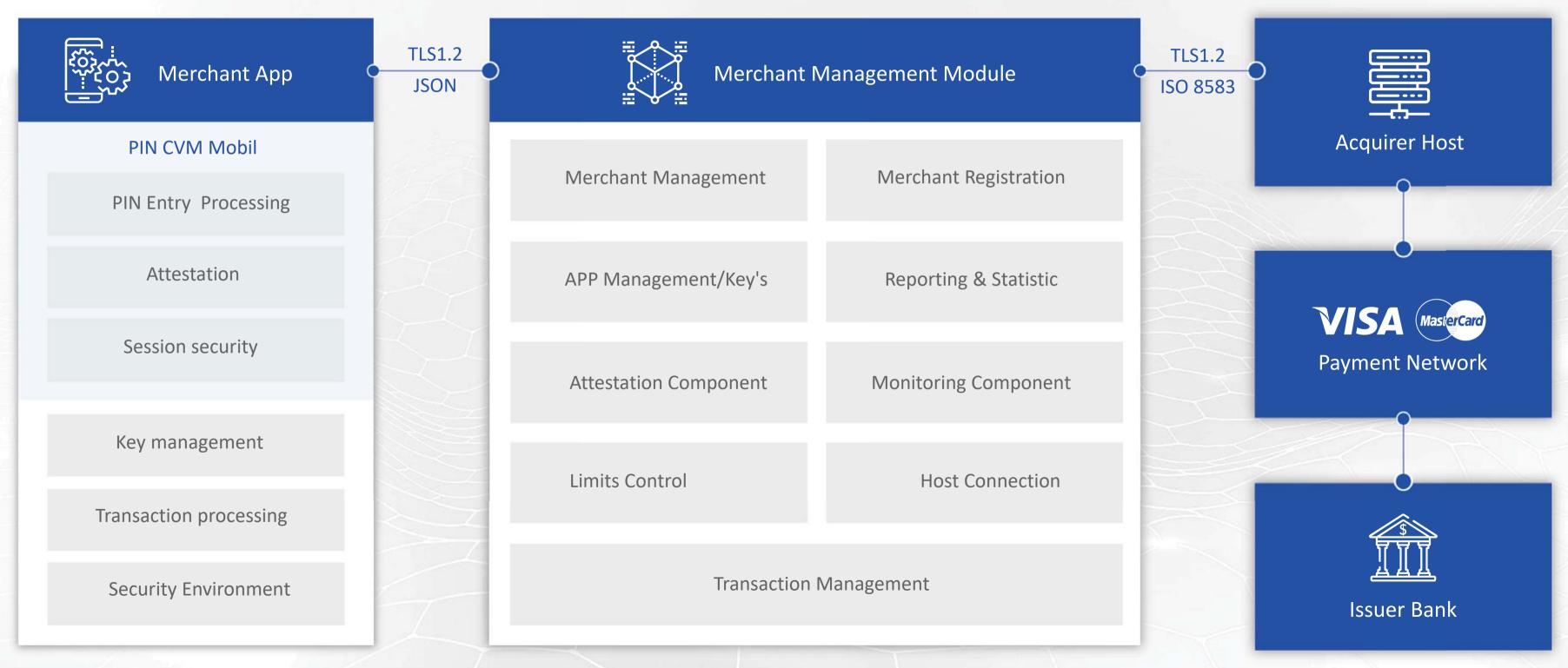


GENERAL ARCHITECTURE

All sensitive data is encrypted, and the solution complies with the requirements set out in the PCI' Software based PIN Entry on COTS document

MERCHANT DEVICE

AVI INFOSYS – SOFT-POS TMS



BASIC FUNCTIONALITY

MOBILE APPLICATION AVI INFOSYS – SOFT-POS App

- Remote merchant registration (activation/deactivation)
- Purchase, Reversal, Refund transactions
- Transaction statistic data collection
- Request transaction history
- Business day transaction receipt
- Configuring Application Settings

AVI INFOSYS – SOFT-POS TMS SERVICES

- Integration with the Bank' merchant registration system and POS acquiring host
- Operational reports
- Secure communications TMS- App
- Protection of the merchant application from threats and modification attempts
- The ability to block single merchant app or group of apps be using specific filters (group, MCC, network) or as a reaction on attestation procedure





MERCHANT APPLICATION REGISTRATION

REGISTRATION STEPS

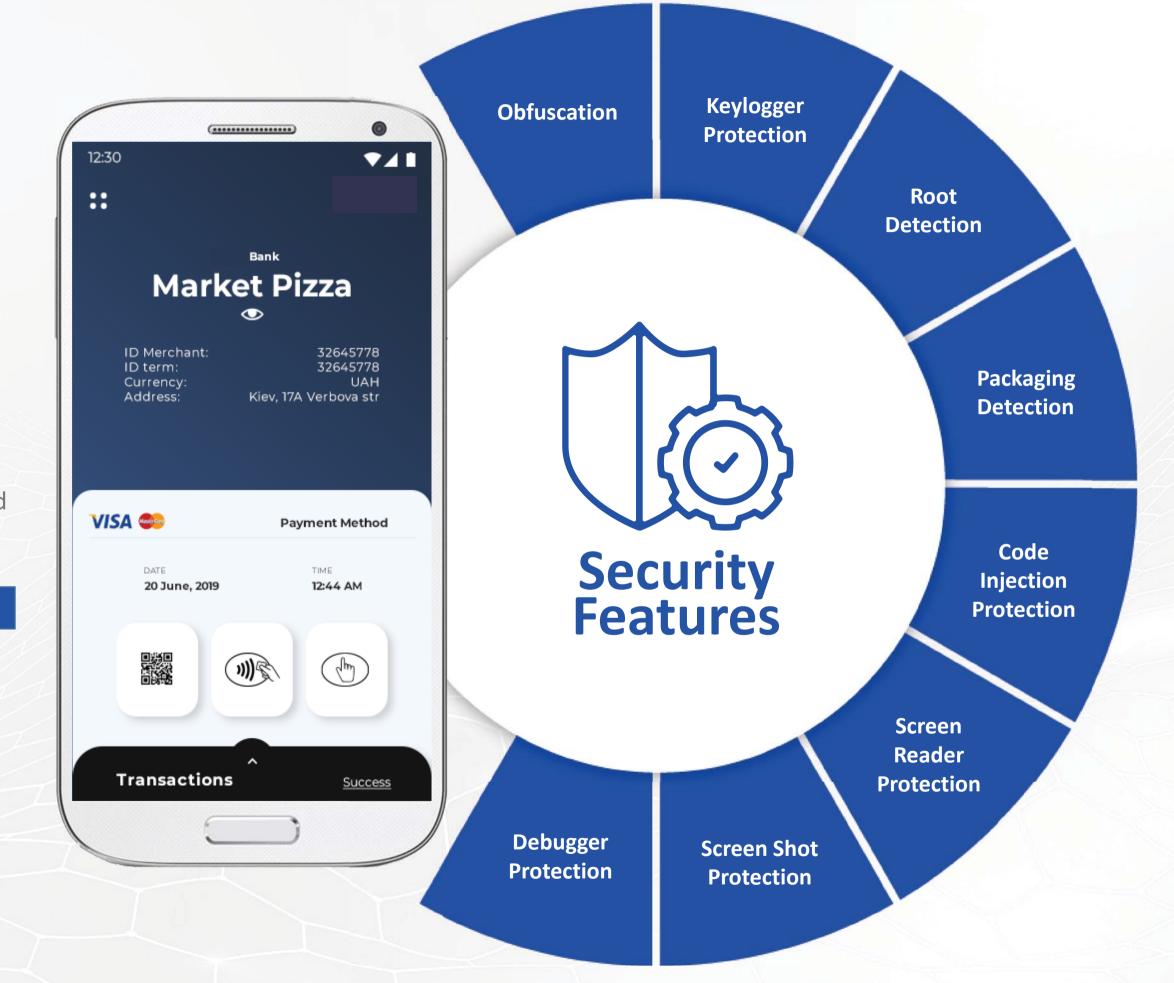
- The merchant has a pre-signed agreement with AVI INFOSYS
- AVI INFOSYS enters (or imports) merchant' data in the TMS system
- AVI INFOSYS tells the merchant the Application Activation Code
- The merchant knows contract details and activation code
- Mechant downloads the AVI INFOSYS SOFT-POS App
- Merchant registers and enters Merchant ID and activation code
- The merchant enters a one-time OTP password
- Terminal data is loaded into the merchant application
 - 1. Merchant ID, Terminal ID, Code Activation (Phone Number)
 - 2. Merchant ID, Activation Code, OTP
 - 3. Merchant Data, Name, MCC, Limits

APPLICATION PROTECTION

Our solution uses technologies that provide a set of protecting mechanisms to satisfy all VISA/Mastercard security requirements.

PROTECTION PROVIDES

- Proactive threat protection
- External attacks detection and blocking
- Integrity checks



OPERATIONAL CONTROL ZONES

AVI INFOSYS – SOFT-POS | Terminal Management

01 Verification

- Credentials verification
- Fingerprint or access code authentication
- Application integrity check
- Device threat detection

02 POS

- Verify TMS connection
- Download session keys
- Block NFC from other apps
- Loading merchant' parameters
- Limits loading
- Operations loading

03 Scan

- Interaction with supported payment instrument
- Threat control
- Card data encryption
- Processing card data in safe environment

04 Pay

- Focus control
- Screen copy prevention
- PIN block encryption
- Attestation parameters sending
- Data deletion

Merchant

Zone 1 – client authentication and mobile application verification. App integrity check. Download operational data.

- Transaction history
- Daily transactions
- Close business day
- Transaction receipt
- Return operation

Zone 2— preparation for payment operation. The server connection is checked, session keys are exchanged, proactive threats are checked.

- Enter transaction amount
- Manual PAN entry (optional)
- Reading a card
- Check limits for merchant

Zone 3 – contactless card data (or token) acquisition by merchant 'app. Blocking possible attacks on the application.

• PIN entry

Zone 4 – transaction data processing zone.
Sending transaction data to TMS.
Waiting for transaction authorization result.

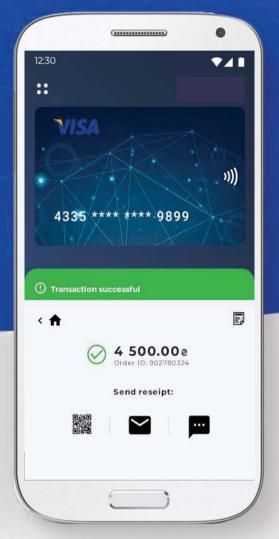
Transaction routingProcess visualizationLast transaction receipt

EXECUTION OF PURCHASE OPERATION











Selecting a card read operation via NFC

Enter the transaction amount and click the Pay button.

Reading a card and sent card data to TMS and to Bank-acquirer

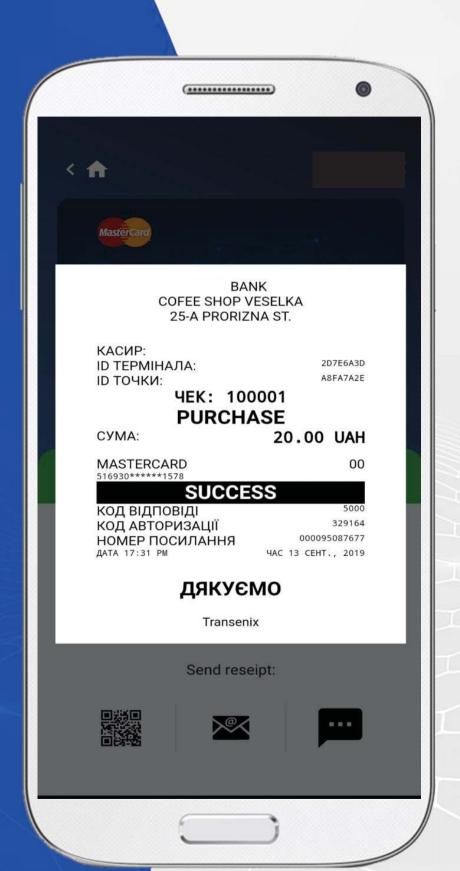
Response received -Successful operation. Request a receipt A customer can receive an
E- receipt by choosing the
option:
Form QR
Get SMS
Get Mail











ELECTRONIC RECEIPT

CUSTOMER CAN GET A RECEIPT BY ONE OF THE METHODS:

QR – receipt data and link to WEB resource SMS – receipt data E-Mail – receipt data

The client, using the transaction reference number, can request a receipt on the TMS WEB resource at any time.

Receipt details:

- Merchant address
- Merchant name
- Terminal ID
- Merchant ID
- Check number
- Transaction type
- Transaction amount
- Masked card number
- Operation result
- Authorization code
- Operation number
- Sequence number of operation
- Date and time

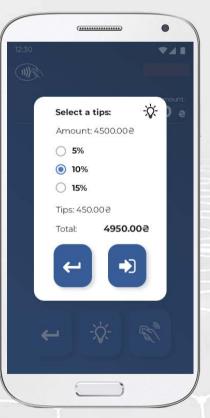
OPERATIONS IN THE APP

ADDITIONAL OPERATIONS AVAILABLE FOR MERCHANT

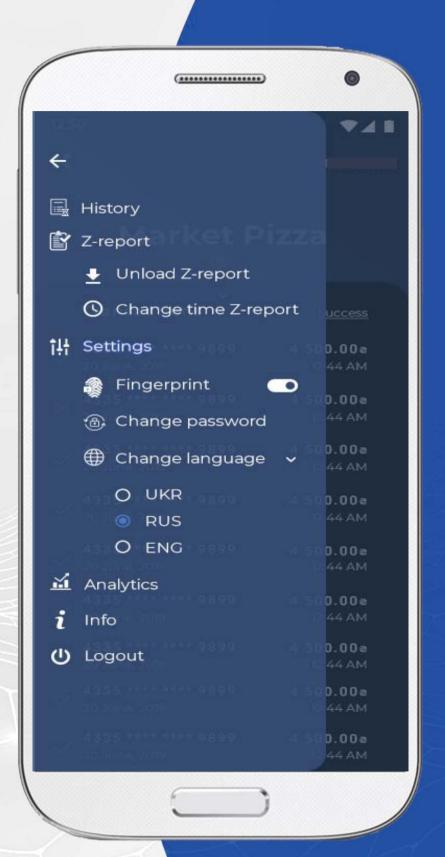
The customer can perform the following operations:

- Transaction history
- Business day (all subsequent operations will relate to the current financial
 - day)
- Reversal
- Refund
- Repeat receipt for current day
- Send message to TMS
- Register additional terminal
- Help
- Configuration
 - language setting
 - tips setting

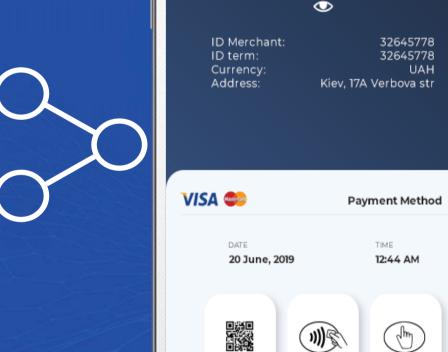




Tips may be added to transaction amount







Transactions

Market Pizza

ADVANTAGES

A MERCHANT CAN SERVE A CUSTOMER AT ANY TIME

Advantages for Merchants

V/1

Success

- The mobile application does not require additional devices to work
- Mobile application is always available (24/7)
- Registration and activation in three clicks (3 screens)
- The merchant can see the total amount of the day directly on the screen
- Merchant can view transaction history

Advantages for Bank

- Simplified merchant service logistics
- No security key management costs
- Improved merchant monitoring mechanisms
- New opportunities to attract merchants from various segments
- Registration automation
- The ability to turn off the merchant app automatically in case of security violation detection
- Application usage history monitoring

PROJECT IMPLEMENTATION

The integration of the AVI INFOSYS – SOFT-POS solution is provided with the support of the project by VISA/Mastercard

HIGH-LEVEL PROJECT REVIEW

Contractual process





Integration process

Creating a communication environment, the test sandbox creating and configuration

API integration with the bank's host system

Opening a project, completing project tasks, describing the architecture, providing connection parameters, generating security keys

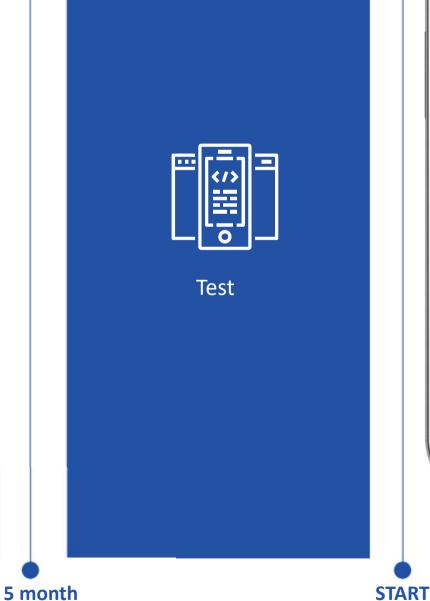
Certification



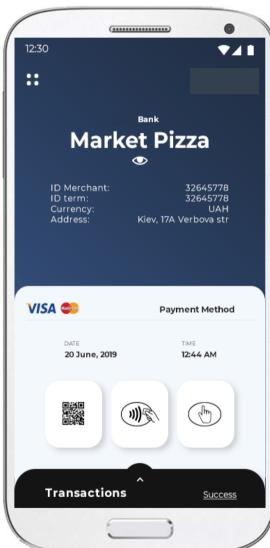
Tests



Solution certification



Ready solution



• The Bank opens a project with VISA together to integrate the solution

START

Solution Integration complete

4 month

Integration with the authorization system

The project goes in operation



Simple and Trusted Payments

Got more questions?

Our team will be happy to assist you at Softpos@avi-infosys.com