

FAQ

FAQ - General

Verestro is a program manager for our clients. Our platform has a connection to external components, i.e. acquirer, processor, MC / Visa. Thanks to this, our customers connect to a single platform only, choose the modules they want and do not have to talk to different partners.

Our solution resonates with our customers, because we offer one platform with multiple functionalities, simple integration and quick delivery.

Critical values:

- Quicker time to market – launch your fintech in **3-6 months**
- Fully certified by **Mastercard** and **VISA**
- **Effective in maintenance** thanks to SAAS approach

Q&A

Q: For your typical customer, what is the problem Verestro is solving and why is it important to them?

A: The main problem of Verestro's clients is how to implement multiple financial solutions in cooperation with various partners. We solve their problem by providing an all-in-one platform with multiple functionalities.

Q: What are the main points of differentiation: Verestro vs. competitors?

- Product multifunctionality - Verestro is the only company on the market that allows such a fast and comprehensive integration of multiple fintech components. The current state of technology of our competitors allows us to implement single components from our offer. This results in a significant stretch of cooperation over time and higher costs. The breakthrough in the implementation of "fintech as a service" is the integration based on modular, integrated inclusion of all services.
- Simplicity - Verestro connects to services via API and provides SDKs and various integration methods to simplify deployment. On the client side, not many IT resources are needed. We also actively develop white label app platform to have easy entry process for smaller customers.
- Speed – cooperation with Verestro reduces the implementation time of a given service by as much as 75% (comparison, if a fintech had to program a given service itself, from A to Z, e.g. NFC payment is at least 12 months of continuous work, where with Verestro

implementation is possible in 3 months).

- Forward thinking – integration with 1 API is enough to implement more and more services in the future. One integration opens the door wide for more.
- No name – Verestro can bring the same benefits to big brands, banking, generally known, as well as to small fintechs.
- White label – the ability to quickly build a mobile / web application and customize it for a customer from different industries without complex personalization.
- Cost effectiveness - we do care about our cost base which means that we can offer very competitive pricing.

Q: What is Upaid? Why does it appear in some of the URLs or documentations?

A: Upaid is our former name. A couple years ago our company has rebranded to Verestro.

Q: Who are Verestro's clients?

A: Verestro's clients are banks, fintechs, money transfer organizations, micro-lending, insurance and crypto companies, as well as other types of businesses interested in Embedd Finance.

Q: What is the basic business model at Verestro?

A: The basic Verestro's business model is B2B (Business to Business). We sell our products to business clients – usually banks, fintechs, merchants, crypto exchanges, insurances, mobile operators, payment schemes etc. And our main distribution model is SaaS (Software-as-a-Service), a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet. In this model, an independent software vendor (ISV) may contract a third-party cloud provider to host the application. Depending on the product, Verestro charges maintenance and volume fees (e.g., it has different payment caps for the number of cards in the system). The Verestro operating principles are based on the SaaS business model.

We are an integrator and program manager for our clients. Our platform has a connection to external components, i.e. acquirer, processor, Mastercard, Visa. Thanks to this, our customers connect to a single platform only, choose the modules they want and do not have to talk to different partners.

FAQ - Card Issuing

General

Q: I am interested in the card issuing project. On whose side must the customer balances be?

A: They can be both client-side and Verestro. If the client chooses to have them on their side, he will have to expose appropriate methods to Verestro to enable required communication.

Q: How do I access the Antaca API or LC API on the Verestro side?

A: This requires signing a contract with Verestro for access to these services. Verestro will then add to the Whitelist on its side the IPs of the devices from which the API requests will be made, and exchange with customer and sign certificates.

Q: What steps should we conduct in the process?

A: First steps are described here: <https://developer.verestro.com/books/card-management-system/page/quick-start>

Q: Is it possible to use the White Label app for card issuing offline?

A: It depends on the configuration of the application, but overall apps can be configured in a way that end user will be able to move between some of the screens without internet connection.

Q: I tried to register a new user on the white label app, but it displays an error message on the PIN page and I can't register!

A: Please verify the e-mail or phone used on the registration, as this data is probably already registered on our systems.

Certificates & Security

Q: Is the same certificate used for both the lifecycle api and card management api ?

A: Yes, the same certificate will be used for all Verestro APIs. The certificate is the same for both endpoints:

Lifecycle API: <https://lifecycle.upaidtest.pl/>

Antaca API: <https://sandbox-antaca.verestro.dev/>

Q: Where I can find a Verestro Public Key for JWE?

A: Public key used to generate JWE can be download from method GET /lifecycle/v1/public-key
Please find a link with some details attached below: <https://developer.verestro.com/books/user-lifecycle-card-management-api-sdk/page/overview>.

Q: What is the difference in "CSR" vs "mTLS" auth

A: Actually, it is the same. mTLS is a security protocol that utilizes CSRs to establish a secure connection.

KYC

Q: For KYC on card issuing with Verestro Card Issuing (Quicko as payment organization), what type of documents are allowed to be sent as valid ones?

A: Allowed formats: passport and sometimes other documents valid internationally, we strongly prefer English language in documents (local languages are usually not accepted).

Q: For the KYC API, is it mandatory to send 2 images? (in case of documents that can be opened or have only one side)

A: Yes, but they can be the same file, if only one image has all the customer information needed.

Q: I need to send KYC documents received from my clients to Verestro. How can I do that?

A: Request example here: <https://developer.verestro.com/books/card-management-system/page/quick-start> Step 2. Create user verification form.

Q: Which formats are allowed for "imagefront" field in KYC API?

A: The allowed formats for "imagefront" is: jpeg, jpg, png. Additionally, please remember to include 'Content-Type: multipart/form-data' in the header.

Q: What are the accepted values for "riskLvl" field in KYC API?

A: Accepted values for risk levels are:

- 'LOW',
- 'NORMAL',
- 'HIGH',
- 'NOT_ACCEPTABLE'.

Q: How to deploy documents for small firms in KYC API?

A: Document submission for verification must be done individually, as there is no option to upload documents for multiple users or firms at once.

Q: If user uploads wrong document's photos (e.g. bad quality) what behavior would we expect from the system? Would system block user's cards, balance, etc?

A: In case if KYC will be managed from your side, our system will not recognize that, as we need to have a view for that data only for audit.

Q: Is it possible to increase the file upload limit to 4MB?

A: It is not possible to increase the limit.

IBAN

Q: How do I generate an IBAN? What is the flow?

A: Verestro has internal configuration of supported currencies per client. If customer wants to receive the IBAN then:

1. Customer should create user with LifeCycle API.
2. User has to pass KYC process.
3. Customer should create balance. Currency of the balance can be determined in the body of the request.
4. If in step 2 EUR balance was created, then making a request for GET /IBAN method will result in returning EUR IBAN as a response. If balance was created in PLN, same method will return PLN IBANs.

Q: Can we open an IBAN without a card?

A: IBAN is created as a separate tool for payments, making it unnecessary to have a card there.

Notifications

Q: I would like to receive notifications about new transaction made by user. How should the endpoint look like?

A: Authorization should be done either using mTLS or basic authorization. Endpoint should be ready to handle following parameters from POST request “{ "id": 20, "timestamp": "1665557034" }”.

Balance

Q: What are the differences between a credit balance and a debit balance?

A: A credit balance allows you to make deposits to user balances up to the amount of deposited funds. The deposit balance allows you to exceed this amount when making deposits to user balances, but the amount of card transactions cannot exceed the amount of deposited funds.

As for the transaction of transferring money between accounts using Antaca's "debit" and "credit" methods, they work in such a way that "credit" "gives" money, while "debit" "takes" it, but there is no mention here of where they give and where they take it. If a request is made 2 times to debit user x and to credit user y, then by splicing these 2 requests, it can be said that it is one transaction (taken away from x and given to y).

Q: What's the difference between Master Account and Company Balance?

A: The Master Balance is used to secure funds necessary for on-going user spend, that BIN sponsor uses in the settlement process with Mastercard. More here:

<https://developer.verestro.com/books/card-management-system/page/overview#bkmrk-balances>.

Company balance is a place where FX/Interchange/Fees are settled.

Q: Where can I verify the balance of a company on Budget control system?

A: CardAlias APIs can be used, the same information is also available on the transaction details APIs, under the parameter balanceMinorValueAfterTransaction.

Q: Is there any dashboard provided by Verestro to have an access to customer balances thorough the interface to control Master Balance?

A: Yes, Verestro provides a Wallet Admin Panel, which is a web frontend application dedicated for customers to follow user transactions and manage the Master Balance. Available on the Verestro Developer Zone at: <https://developer.verestro.com/books/money-transfers/page/overview>

Cards

Q: Where the physical cards can be tracked, when this card is issued or what is the current status?

A: We do not provide it via API, but they can do it through an agreement with a courier company that will deliver cards from the personalization company to users.

Q: For the cards issued with Quicko, there is any ATM limitation for withdrawals with the cards, like a specific network cannot be used?

A: They should. The only dependence could be different surcharge per operator, but some cards may be limited by the network without previous warning.

Q: Can one user as corporation have multiple cards, like 100 000 cards?

A: Yes, there is lack of limitations.

Q: Can a single user have multiple cards and are there any limitations on card total number?

A: One user can have multiple balances and multiple cards under each balance. Each card can have different limits. We do not have card limits per user.

Q: Client is asking about physical cards and where they can track when this card is issued or what is the current status?

A: We do not provide it via API, but they can do it through an agreement with a courier company that will deliver cards from the personalization company to users.

Q: What is the difference between synchronous and asynchronous process of card's creations?

A: In a synchronous process in a response you'll receive a card data, in asynchronous the ID by which you can check if the card has been generated already.

Q: In which case we should use `secure/cards/{cardID}/activation` method?

A: This method should be used for physical cards only.

Q: Is a PIN code required for the virtual card?

A: In context of virtual cards PIN is only required if customer would like to withdraw money from ATM using X-Pay.

Q: How does the customer receive the PIN?

A: You would need to pass it somehow to customer, you can either show it somewhere in the app or send it somehow for example via email.

Q: Is it possible to change the PIN code? If yes, how can this be done?

A: Yes, there is method in Antaca API for that purpose you can use "Change card PIN" method from <https://developer.verestro.com/books/card-management-system/page/technical-documentation-4WI>

Q: Are we correct in understanding that the card details (number, expiration date, CVV) created with the `POST /secure/customers/{customerId}/cards/virtual` method will be identical to the physical card that will be issued later for the specific user? Or will it be a separate card?

A: Those will be different cards, so all the details on physical cards are going to be completely different than on the virtual ones. Having same credentials on both types of cards is only possible once company is "Digital first" enabled on Mastercard side.

3DS

Q: What data should be delivered to Verestro to configure 3DS?

A:

1. Title: **Purchase confirmation**
2. Main text: **Please enter the OTP sent to your mobile number. For help contact us on ### ### ##.**

Error Screen

3. title: **Authentication error**
4. Main text: **There was an error processing your request. Please try again.**
4. Terms and conditions – short text about accepting conditions or URL.

Company logo in PNG format, no larger than 50px by 150px. (Could push to be max 75 pixels by 155 pixels)

Transactions

Q: Can we get transaction info per card?

A: Yes, you can get transactions per card. There is API description under link

<https://developer.verestro.com/books/transaction-history-api/page/technical-documentation-thc-external-api>

Q: Are ATM withdrawals possible with a virtual card?

A: Yes, but only if those virtual cards have configuration for it turned on and only if they have defined PIN (PIN is required when withdrawing money from ATM).

Q: On transaction history API, what kind of values can be received on merchantTransactionID parameter?

A: Any value that is sent to our system from the processor, varying from UUIDs, integers or strings

Q: Is there an endpoint that returns transactions done by card?

A: Yes, you can get it but on dedicated beta environment. It is not present in Sandbox environment.

Q: Why Processor's loadReversal is not being written on THC (Transaction History) as a transaction or update?

A: LoadAuthorization is a QUESTION: "is it possible to DEDUCT/CREDIT a given card?" and it does not cause any movements on the balance/limits/etc, therefore its not reported to THC.

This question is usually followed by loadAdjustment, which already DEDUCTS / CREDITS the balance and this movement is reported to THC. If a loadReversal comes instead of loadAuthorization, its handled as "there was no previous question" and is still not reported to THC.

Q: Why the REVERSED transaction is showing amount:0?

A: The value is updated according with the actual transaction value. For example, a 100.00 EUR authorization will show in THC (Transaction History) 100.00 EUR with status is AUTHORIZED. If 20.00 EUR is reversed on this transaction, the updated amount in THC will be 80.00 EUR and status will still be AUTHORIZED. If instead, it was a 100.00 EUR reversal, the updated amount in THC will be 0.00 EUR and the status would change to REVERSED.

Q: I'm using a simulator to send transactions to the system, why I'm not receiving all the transaction status?

A: The simulator will send exactly what was selected to be sent. If a REVERSAL is sent, only the REVERSAL will reach our systems. Same for all the other status.

Q: In the case when a user is offline on a plane and makes a payment with a card, how is the balance on their card checked?

A: Offline transactions are transactions you cannot reject. From the MC side, we find out that the money has been taken away and they don't ask if this might happen. Offline transaction can occur for example in metro or in airplane. In general, they occur very rarely. In such situations, the only thing you can do is report chargebacks after.

Q: What transaction type should we use instead of withdrawal when a user initiates a crypto purchase?

A: for sell/buy with the user when the funds do not leave our "digital system" the best types will be:

- when the user is charged (buys crypto) - transactions/debit with the type funding
- when the user is credited (sells crypto) - transactions/credit with the type payment

Q: What is the difference between FEE & COMMISSION types? Please specify in which cases a transaction with type COMMISSION will be created

A: Commission (if it applies) refers to performing any sort of transactions (for example it can bet set up that for each abroad transaction customer will be charged 0,3EUR or 0,1% value of the transaction). Fees can apply to BIN-Sponsor related fees (if there are any set) like for example charging customer monthly for having active card or balance opened.

Limits

Q: In the documentation for card limits management through the API, we found that there are only three periods: daily, weekly, monthly. What about the limit per transaction? Is it limited to Mastercard limits or is it also set on your side?

A: Yes, it is possible to set limit per transaction. We can indicate limits, such as e-commerce limit, ATM limit, or limit in another currency. Those limits are configured and can be managed by API. More information's about limits and how to set them up can be found in documentation: <https://developer.verestro.com/books/card-management-system/page/technical-documentation-4WI>.

Q: on setting the limits on the cards, like Monthly, weekly, daily. What datetime does it actually start-end?

A: Limits are cleared accordingly:

Daily: every day at 11:59PM

Weekly: 12:00AM on Mondays

Monthly: 12:00AM on the first day of the month

CRON, which clears the limits, runs in UTC time

Finance Admin Panel

Q: Does admin panel is available on sandbox environment?

A: No, it is not available in the Sandbox environment.

Q: Can we create users and validate them in the admin panel?

A: No, it is an administrative tool. You can read about admin panel functions under below link: <https://developer.verestro.com/books/administration-panel/page/finance-administration-panel-overview>

FAQ – Paytool

Q: How to integrate with Verestro Paytool?

A: Customer can implement Paytool solution using Web SDK or integrate directly with the API. In Web SDK integration model Verestro handles transaction and 3D Secure in the Customer's name. In API to API integration model Customer must integrate with every method and handle every response from Paytool API himself. For more details please visit:

<https://developer.verestro.com/books/verestro-paytool/page/how-to-integrate>

Q: What are the supported payment methods?

A: Verestro as a PSP provides several different payment methods. During onboarding the Customer decides what are the one's available to the end users. We support payments using debit/credit card details, Google Pay, Apple Pay, BLIK. Openbanking PIS transactions to follow soon. For more details please visit: <https://developer.verestro.com/books/verestro-paytool/page/use-cases>

Q: Does Verestro offer Openbanking in Paytool?

A: Verestro is implementing open banking (PIS) payments in Paytool payment gateway. Various integrations are used with Fenige and Quicko - payment institutions from Poland. In Dec 2024 we have coverage of the following countries: Poland, Austria, Spain, Netherlands, Germany, Portugal, Italy, Finland, Estonia.

Q: What is the time for automatic refund if the transaction has not been cleared?

A: The funds will be returned to the payer's account in case the transaction is not cleared. The turnaround time = 7 days for VISA cards and 30 days for Mastercard cards.

Q: Is it possible to return only part of the declared amount?

A: In order to return part of the declared amount, a clear/deposit must be made for the amount to which the payer is to be debited. The rest of the amount will be returned to him. For example, a transaction was ordered with no autodeposit/autoclear for 200 EUR. Then a deposit/clear was made for the amount of EUR 150. In this case the payer will be refunded for 50 EUR. In the case of a cleared transaction, only a full refund is possible.

Q: How many terminals can be configured for one merchant account?

A: One merchant can have multiple terminals with one default terminal. The default terminal will be selected that if no specific terminal is specified.

Q: Is it possible to decide which payment methods will be displayed in the Paytool form?

A: Merchant can decide which payment methods are to be active during the execution of each transaction. He can specify all available payment methods at the configuration level and per transaction. For example, the merchant decided that he wanted only GooglePay, BLIK and Card plain payments to be displayed by default for each transaction. In addition, for a selected transaction he can choose which of the above payment methods will not be displayed.

FAQ – Payouts

Q: Does the region-specific availability of Payout apply to the end user or merchant?

A: The availability of the service depends on the merchant's country of registration, the entity must be registered in one of the EEA countries. Its users can be from any country, not covered by sanctions.

Q: Do INTRA or INTER rates apply in the UK?

A: The UK is located outside the EU, so INTRA rates apply.

Q: Are there daily transaction limits for merchants?

A: If the daily turnover is greater than 150K USD/EUR combined on MC and VISA – Acquirer will require SD.

Q: What is the maximum time from completing an e-commerce transaction to receiving funds to the Payout account?

A: The time depends on the model/price offer in which the cooperation with Acquirer has been established. We have threshold values, i.e. 4500 PLN, 1000 EUR, 1000 USD. In the fixed fee model, funds from e-commerce are transferred to the merchant's account within 2 business days from the moment the threshold value is reached. In the IC++ model, the threshold values are identical and the time is 5 working days.

Q: Is there a limit to occasional transactions in Payouts?

A: Per month per user it is 1000 EUR.

Q: What is the difference between blended and IC++ rates?

A: Blended are the final rates offered per transaction, so all processing costs are included in one fee known to the merchant. On the other hand, in the IC++ model, we are dealing with a division of the rate into 3 fees, so the cost of the transaction is visible to the merchant at the time of receiving the report. The fees included in the IC++ model include: interchange fee, fee imposed by payment card providers (Mastercard, Visa) and settlement fee.

Q: What do the costs of Payout service with Acquirer depend on?

A: Costs for a P2A service vary depending on: average transaction value, expected monthly turnover, regions, industry (IC), currency

For specific cases, more information may be needed. For example costs for a P2A service vary depending on: country, type e.g. P2P, B2P, etc., channel, e.g. bank deposit, mobile wallet, terminal settlement currency.

Q:

A:

FAQ – IBAN Management Service

Q: Is it possible to test IBAN Management Service?

A: Yes. In order to test the functionalities offered by IBAN Management Service, you need to be onboarded, check [Onboarding chapter](#).

Q: What functionalities can I test?

A: You can call all the methods given in the [Technical documentation](#), using the appropriate URL, but during tests, outgoing and incoming transfers will not be performed. This means that it is possible to call the method, but the funds will not be transferred to the recipient's account.

Q: Which endpoint should be used to generate IBAN?

A: You should use POST /secure/bank-accounts to create IBAN.

Q: What are the possibilities to integrate IBAN Management Service?

A: Verestro provides access to the solution through the server to server communication according with REST protocol.

Q: What does WAITING_FOR_REGISTRATION_IN_BANK status mean?

A: The bank has received an IBAN registration request and is validating on its end. If everything went well, the process should take few seconds.

Q: Which transfer types Verestro supports?

A: We support SEPA transfers for ZEN bank ibans. For PEKAO bank ibans we support ELIXIR, SEPA, SWIFT, SORBNET.

FAQ - User Lifecycle

Q: Which actions Lifecycle API will allow you to manage users and cards?

A: By using Lifecycle API issuer allows to:

- create user objects and objects related to user (address, cards, etc).
- send user objects directly to different products
- edit user objects
- delete user objects
- lock/unlock user objects

Q: Can you explain add user flow in details?

A: In order to add user you should use LC API. You can read more about API uder below link <https://developer.verestro.com/books/user-lifecycle-card-management-api-sdk>

Q: Can the addUserWithCards operation done through sdk method instead of REST API?

A: It is possible to add user and card over SDK, however, pay attention that 3DS should be conducted in each case of adding cards.

Q: Which API should be prepared by the issuer?

A: Within an implementation the next APIs should be prepared by the issuer.

1. Validate CVV
2. Token Update API
3. User Notification Request
4. Get Customer Mobile number
5. Currency rate API (if reports are needed)

An example will be shared within an implementation phase.

Q: What improvements does Admin Panel give for Issuer?

A: Thanks to the Admin Panel Issuer can in easy and quick way ti:

- access tokens and transactions data, manage tokens (statuses),
- manage administrators,
- filter and sort data,
- generate reports, monitor activity.

Q: Which elements does the token list include?

A: Basic list of tokens include:

- VPAN -Issuer card id
- Token - last 4 digits of the token
- Phone number - customer phone number with country prefix
- User name - customer name and last name
- Status - payment token status (check Token statuses)
- Token requestor - name of Token Requestor
- Device - type of device
- Path - authentication paths for the user (check User authentication paths.) Process start - start date of the process
- Actions - actions that can be performed on the token (check Token actions)

Q: Which actions with a token can be done through an admin panel?

A: The actions that can be performed on the token from the token list are as follows:

- Activate token,
- Suspend token,
- Unsuspend token,
- Delete token.

Q: What status can be used for the token?

A: The tokens can have the following statuses:

- Inactive - token has not yet been activated,
- Active - token is active and ready to transact,
- Suspended - token is suspended and unable to transact, Deactivated - token has been permanently deactivated or deleted.

Q: What types of the authentication methods can be used?

A: There are 4 authentication paths for the user:

- Green Path - Path without user confirmation (authentication) during the token activation process. The payment token is automatically activated.
- Yellow Path - Path with user confirmation (authentication) during the token activation process. Payment token is activated after correct OTP is provided.
- Orange Path - Path with user confirmation (authentication) during the token activation process. Payment token is activated by the Bank after the user's request via call.
- Red Path - Path when the Issuer rejected activation payment token during the token activation process.

Q: How the authentication step in device pairing is completed at our end? How do we create the trustedIdentity (JSON web token) ?

A: There is an example of generation of trustedIdentity in the documentation

<https://developer.verestro.com/books/user-lifecycle-card-management-api-sdk/page/technical-documentation-mdc-sdk#bkmrk-loginbytrustedidenti>. Generating of CA and required for trusted identity is described in the documentation under section "Data signing and encryption"

Q: Which user roles will be supported in an admin panel?

A: Admin panel roles and elements that can be managed:

- admin - can create/edit/delete any administrators in any role
- manager - can create/edit/delete only administrators with role employee employee -can create/edit/delete only administrators with role employee

Q: How do we plug/provide our own userId and cardId as externalUserId and externalCardId?

A: Yes, you can use your own (external) cardID and UserID. According to team the majority of methods allow for that option.

Q: When does new added user (through LC API) will synch to app? How does SDK know which user info to pulled from wallet server is there any initial id we need to pass during SDK initialization?

A: SDK doesn't know about that, application must call the process where device is paired with user:
use case:

<https://developer.verestro.com/books/token-requestor/page/use-cases#bkmrk-pair-device-on-walle>

Android and backend implementation:

<https://developer.verestro.com/books/user-lifecycle-card-management-api-sdk/page/technical-documentation-mdc-sdk#bkmrk-pairbytrustedidentit-0>

like on first screen of sample app, where application must provide trusted identity.

FAQ - Tokenization

Q: What is the difference between Pre-Digitization and Push-Provisioning?

A: Pre-digitization and push provisioning are two different processes in the tokenization workflow.

Pre-digitization refers to a set of processes that enable the generation of digital payment tokens. It involves turning a payment card into a digital token to facilitate secure and simplified digital payment experiences. During pre-digitization, the Verestro Token Management Platform (TMP) takes care of all the requirements from Token Requestors.

The pre-digitization process involves the following steps:

1. User enters the card details into a Token Requestor wallet (e.g., Apple Pay, Google Pay).
2. The TMP receives an Authorize Service request from the Token Service Provider (TSP) with the card details and other tokenization data provided by the Token Requestor.
3. The TMP checks device score, existing active tokens, and velocity controls.
4. The TMP sends a request to the Issuer's Card Verification API to validate the card details and receives the Card Status, Card ID, User Phone Number, CVC validation Result, and Product Category.

5. Based on the verification result, the TMP returns a decision to the TSP (APPROVED/REQUIRE_ADDITIONAL_AUTHENTICATION/DECLINED).

Push provisioning refers to the process of delivering the digitized card profile to the user's device after a successful pre-digitization. It is a crucial step in tokenization where the payment token is provisioned on the user's device, enabling secure transactions.

During push provisioning, the following steps occur:

1. After successful pre-digitization, the digitized card profile is delivered to the user's device.
2. If the pre-digitization decision is APPROVED, the token is activated instantly, and the Verestro TMP may notify the issuer if required.
3. If the pre-digitization decision is REQUIRE_ADDITIONAL_AUTHENTICATION, the user is prompted with activation options (e.g., SMS OTP), and the token is activated after successful user authentication.
4. If the pre-digitization decision is DECLINED, the token remains inactive and cannot be activated.

In summary, pre-digitization focuses on the initial token generation process, while push provisioning involves delivering and activating the digitized card profile on the user's device. Both processes are essential for enabling secure and convenient digital payments.

Q: What are the steps for having Push Provisioning in application? I already have manual provisioning.

A: Android - Push Provisioning to Google Pay

1. In order to start the Push Provisioning requesting process company responsible for deployment of the application (Verestro or customer) should visit following website: <https://developers.google.com/pay/issuers/apis/push-provisioning/android/launch-process> and select "Request access". Company should enter all necessary details in the form that should pop-up.
2. Once the access from step 1 will be granted company has to fill in next form and pass to Google:
 - screenshots from application - especially those that shows how "Google Pay" button was placed in the application.
 - screen recording showing user flow for adding card to Google Pay
3. Passing additional, paid certification is not needed in case of Google Pay.

Verestro activities:

- in case when Verestro is owner of the application: configure SDK responsible for Push Provisioning internally
- in case customer is owner of the application: provide customer with SDK and ask them to configure it

iOS - Push Provisioning to Apple Pay

In order to start the Push Provisioning requesting process company responsible for deployment of the application (Verestro or customer) should write directly to Apple using Apple Pay

provisioning@apple.com and applepayentitlements@apple.com.

Email example:

"Hi,

I would like to start the in-app push provisioning process with FIME certification. Can you enable the in-app push provisioning on appstoreconnect for testing purposes for XYZ application
<https://apps.apple.com/pl/app/XYZ>

Regards,

XYZ"

We provide the data of the application that is on the App Store, and we perform tests on TestFlight using the same application (the same ADAM ID)

Then company should contact with FIME to pass required certification and follow their instructions. Last time we checked with Fime cost was 3125 euro.

Verestro should:

- in case when Verestro is owner of the application: configure SDK responsible for Push Provisioning internally
- in case customer is owner of the application: provide customer with SDK and ask them to configure it

Q: Can you provide exact sequence of steps for whole tokenisation process?

A: The sequence in the documentation presents the flow which you should follow.
<https://developer.verestro.com/books/token-requestor/page/use-cases> In each diagram Issuer = PhonePe in your case

Q: What is the difference between push provisioning and in-app provisioning?

A: There is no difference between push and in-app provisioning.

Push Provisioning (or in-app provisioning) provides the ability to initiate the card provisioning process for Apple/Google Wallet directly from the issuer's app.

Users will find the Push Provisioning feature an extremely convenient method to provision their cards or passes into their devices by avoiding the need to input those details manually.

Q: How we will use Verestro TMP for M4M tokenization's, do we need to configure something on MDES/Verestro side or else?

A: From Verestro side - we are ready to accept M4M tokenizations. You will have to ask MC for MDES side of configuration.

Q: Where can we find Verestro TMP public key used for encryption? Can you send us an example of encryption as we cannot find it in documentation?

A: The JWE certificate will be different for beta and production environment. We will be sending CV requests from the domain <https://bifrost.upaid.pl>

You can get this public key from the API:

```
curl --location 'https://bifrost.upaidtest.pl/issuer/public-keys' \
```

```
--header 'Authorization: Basic ***\
```

Q: Can you please send, if you have, the example of code written in .Net which is an alternative to this one written in Java, as we cannot use much from this one (we use .Net)?

A: We don't have any example code written in .Net, only in Java. You can find some examples on the internet – JWE is a common standard and there should be some library for .Net that supports it. But please make sure that you are providing the necessary headers in JWE (ex. iat and kid).

Q: Can we have native NFC payments (issuer wallet) on Apple devices?

A: No, Apple doesn't allow such solution. It is possible to pay with NFC on iOS only by using ApplePay. NFC payments (issuer wallet) is only available on Android devices.

Q: What is manual provisioning and push provisioning to XPays (Apple Pay, Google Pay)?

A: If you apply for manual provisioning it means that your users will be able to add card and later use it for NFC Payments to XPays by filling in card data manually in XPay application. If you apply for push provisioning it means that your users will be to add card directly from your application by pressing developed button "Add card to <name of the XPay>".

Q: In what step we get the paymentTokenId?

A: The paymentTokenId you can get after digitization.

Q: Is there a callback which inform about SDK initialisation completion?

A: There is lack of callback related to "SDK initialisation completion" , it is synchronic function, once it is finished it means it was conducted.

Q: Once we add the card and complete the whole tokenization process , does the pan no (actual card number) gets deleted?

A: Yes, we do not store PAN after tokenization.

Q: When user came again to do tokenisation again for same card how can I map this with instrumentId?

A: When you try to add same PAN again LC API should return error CARD_ALREADY_EXISTS Passed card is in the system. Cards number for issuer is unique. You can check detail under below link: <https://developer.verestro.com/books/user-lifecycle-card-management-api-sdk/page/technical-documentation> Method Add Card

Q: Can delete card only once token is successfully created on app and backend is notified about it? What will be the tokenization flow?

1. The main flow for tokenization is add card digitize card.
2. When card is added you can get it by MobileDC:CardsService:getAll().
3. Card deletion is possible by MobileDC:CardsService:deletecard(id) or LC API : Delete Card. If removed card was tokenized it automatically removes token on backend side.

Q: What's difference between below methods?

1. restart()
2. userService.logout()
3. userService.deleteUser()
4. deviceService.unPairDevice()

Answers:

1. Clear only UCP context like payment tokens, user, cards and session for Mobile DC remains on device
2. Just clears user session token - next actions requires login
3. delete user, tokens, cards and clears SDK data as there is no user
4. Remove binding between user and device and clear SDK data. Requires pairDevice to use SDK

Q: Is there any method to release SDK (MDC,UCP) resource(like SSE etc) for better resource utilisation ?

A: SDK doesn't provide such methods. It should be out of the box in JVM. The objects are not cleared, but objects do not keep any data during lifecycle. The data is cleared by GC in context of method usage. Only HCE related methods keeps data context until contactless payment is finished.

FAQ - Admin Panel and Reports

Q: What are the roles in the Administration Panel?

A: Customer, Manager, Admin. However, on production environment for customers only Customer and Manager role is available.

Q: My invitation to Admin Panel (CMS) has expired - what should I do to create an account?

A: You should enter the Admin Panel and use option "Reset password". Then enter your email to which the invitation was sent and complete the password reset flow. After that, you should be able to login.

Q: Are there any reports or API from which I can retrieve all my clients' transactions?

A: In the Administration Panel there is a tab "Payment History" after clicking which all transactions within the instance will be displayed. Being in it, you can define appropriate filters (e.g. date range of executed transactions) and then by clicking the button in the upper right corner "Generate transactions report" you can generate a report. The created report will appear in the "Reports" tab - from there it is possible to download it locally and perform further analysis.

Q: I would like to receive notifications about new transaction made by user. How should the endpoint look like?

A: Authorization should be done either using mTLS or basic authorization. Endpoint should be ready to handle following parameters from POST request "{ "id": 20, "timestamp": "1665557034" }".

Q: How do I receive credentials to Admin Panel?

A: Access to Admin Panel should be provided by Verestro. Please ask about it your account manager on Verestro side.

Given path must direct to the image of required documents.

Q: What is the SLA form should be used for Token Management Platform?

A: Required data to solve the issue:

- Brief description of the error (user story)
- Date and time
- Type of environment (default: production. Cases from the test environment will be considered individually.)
- Card details: last 4 digits, card ID, BIN (if applicable) or Token identifier
- Text (or screenshot) of the error message (if applicable)

FAQ - Transaction History and Notifications

Q: How do I get notified when there is a new transaction made by a customer?

A: For this purpose, the POST /transaction-event method in the THC API was created. It requires the creation of a corresponding endpoint on the client side. Then, when Verestro receives any transaction sends an event to the created endpoint with the timestamp and id of the transaction, which can be used later to retrieve transaction details using another method in the THC API.

Q: Is it possible to define the content of the SMS sent when the corresponding actions are performed (card added to XPay, registration OTP etc.)?

A: Yes, Verestro can change texts in the SMSes as per customer's demand.

Q: I would like to have access to THC (Transaction History) API External. How do I authorize to this API?

A: To access THC API, you need to provide Verestro with CN from the certificate that you have generated for LifeCycle/Antaca APIs. Then, Verestro will need to configure it internally and each of the requests should be done using this given certificate.

Q: Can we download transactions through THC (Transaction History)?

A: You can use THC API to download all transactions (i.e. the first Inbound endpoint from here <https://developer.verestro.com/books/transaction-history-api/page/technical-documentation-thc-external-api>). You can also be notified about the creation or update of a transaction. In that case you must create an endpoint as in the "Outbound" section in the link and then you will be able to download the transaction individually, i.e. through the second endpoint with "Inbound"

FAQ - Security

Q: What is the process of signing an authorization certificate?

A: Verestro sends instructions to the customer. Based on it, the client generates a certificate and sends it to the CSO on Verestro's side using a PGP key. The CSO signs it, passes it internally at Verestro for configuration and sends the signed one back to the client. The signed certificate should then be used in the execution of each request.

Q: Is the mobile PIN stored in Verestro in accordance with Mastercard PIN Security Standards?

A: Yes, Verestro stores it according to Mastercard PIN Security Standards.

FAQ - Fee collection

Q: Should we charge the end user's balances or cards?

A: We can do both: card and balance

Q: Can we charge fees instantly (right after a transaction occurs) or once a month?

A: We can do both, depending on the type of the fee.

Q: What kind of fees can we configure and can be charged from user's balance?

A: We are able to define fees per card's, balance ID, currency conversion, per period of time, per user. For more details check here <https://developer.verestro.com/books/fee-management-system>

Revision #30

Created 23 February 2024 10:20:30 by Krzysztof Drzyzga

Updated 19 March 2025 15:21:38 by Barbara Tudruj