

# Token Management Platform for Card Issuing

Token Management Platform (TMP) is an application developed by Verestro that enables the implementation of various tokenization solutions. This chapter focuses specifically on card issuing projects and provides information tailored to this type of implementations.

- [Overview](#)
- [User notifications](#)
- [Push provisioning](#)

# Overview

Token Management Platform (TMP) is an application developed by Verestro that enables the implementation of various tokenization solutions. This chapter focuses specifically on card issuing projects and provides information tailored to this type of implementations. Our customers so fintechs, issuers etc. will be referred in this documentation as "issuers".

## Contents

This chapter is divided into 4 pages.

1. **Introduction** - here you will find high level overview of the solution.
2. **User notifications** - page dedicated to different user notifications and possible ways to send them
3. **Push provisioning** - page with all the details necessary to enhance your cardholders experience with push provisioning
4. **InApp authentication** - page dedicated to replace sending SMS OTP codes with InApp authentication

## Overview

Thanks to TMP your cardholders will be able to:

1. Manually add their cards to Apple Pay, Google Pay, Samsung Pay, Garmin Pay and other X-Pays (**manual provisioning**) (*basic feature*)
2. Tokenize the cards in various ecommerce stores with the use of **M4M** (Mastercard for Merchants) service (*basic feature*)
3. Add their cards to Apple Pay, Google Pay, Samsung Pay, Garmin Pay and other X-Pays directly from your mobile application (**push provisioning**) (*additional feature*)
4. Activate pushed token directly from your mobile application, without the need of typing OTP code delivered via SMS (**inapp authentication**) (*additional feature*)

Features and advantages of the solution from Issuer perspective:

1. Admin panel allows your customer service to review the tokenizations and manually activate or deactivate tokens
2. Thanks to integration with Verestro Life Cycle API all token statuses will be updated automatically, according to card statuses
3. Our backend simplifies encryption mechanisms required by X-Pays in Push Provisioning process
4. Apple mandatory requirements are covered.

## Pre-digitization

Pre-digitization is a set of processes that allows to a generation of digital payment tokens to enable simpler and secure digital payment experiences. Simply it turns a payment card into a digital token. In this process, Verestro TMP is taking care of all the requirements from Token Requestors.

Thanks to the use of Verestro Data Core card verification is done internally, between verestro services. No additional development is required from the issuer.

## Tokenization process

1. User enters the card (either manually or pushes from the app) into Apple Pay/Google Pay or another Token Requestor wallet.
2. TMP receives Authorize Service request from Mastercard Digital Enablement System (MDES) on Pre-digitization API with Card Number, CVC, Exp Date, Device Score, and other tokenization data provided by Token Requestor.
3. TMP checks the device score, number of already active tokens for the card, and velocity controls.
4. TMP sends a request to Verestro Data Core with a Card Number and receives the Card Status, Card ID, User Phone Number, CVC validation Result, Product Category.
5. TMP returns the decision to MDES (APPROVED/REQUIRE\_ADDITIONAL\_AUTHENTICATION/DECLINED).

## Token activation

If the decision is APPROVED - token activated instantly after Authorize Service response. Verestro TMP can also notify the issuer if required.

If the decision is REQUIRE\_ADDITIONAL\_AUTHENTICATION - The message will be displayed to the user with activation options (ex. SMS OTP). After the user selects the activation type, TSP will send a DeliverActivationCode to Verestro TMP. Verestro TMP will send the OTP activation code either directly to the user or to issuer's server, depending of the project configuration. After the user enters the OTP, MDES activates the token. The token can also be activated manually via the Administration Panel.

If the decision is DECLINE - a token becomes INACTIVE and cannot be activated again.

When a token is activated, Verestro TMP will receive a notifyServiceActivated call from MDES.

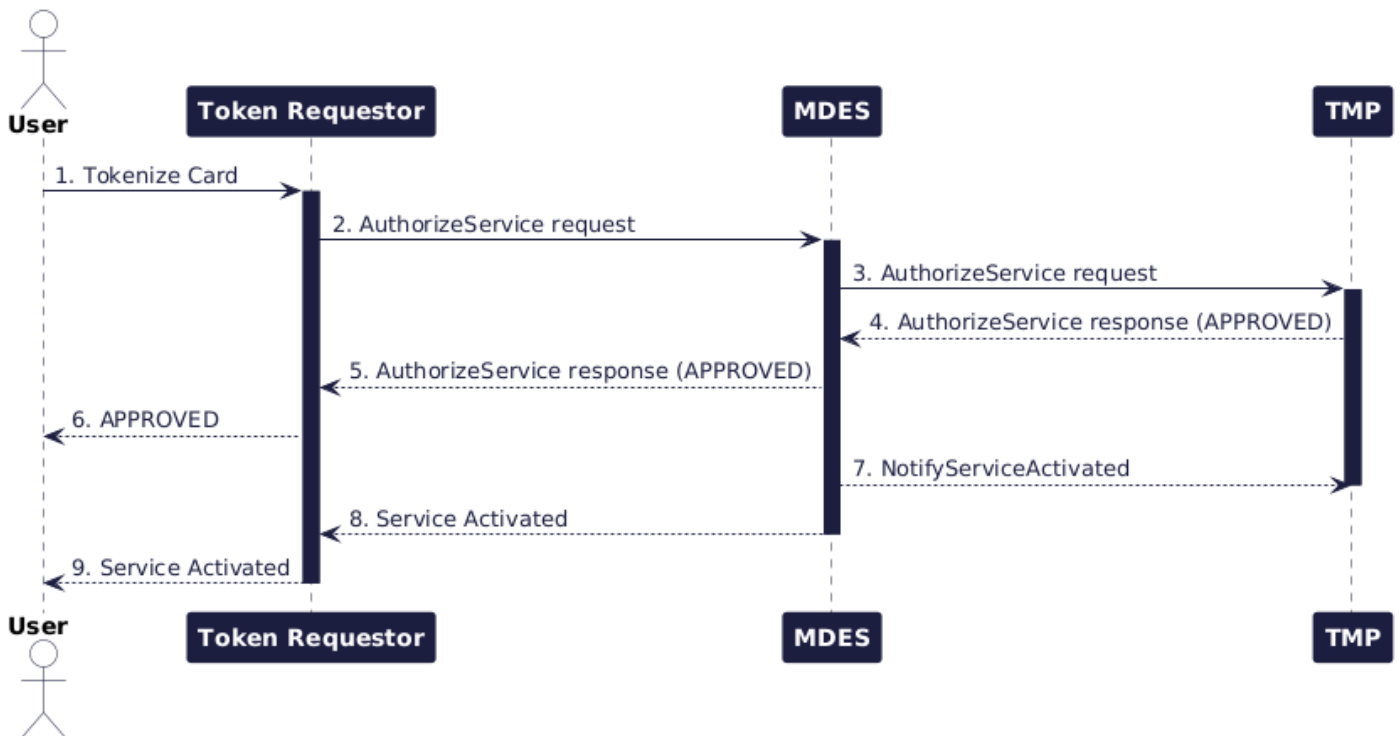
## User authentication

There are 4 authentication paths for the user, TMP chooses one on the basis of different factors and fraud-detection rules which are inline with xPay providers requirements:

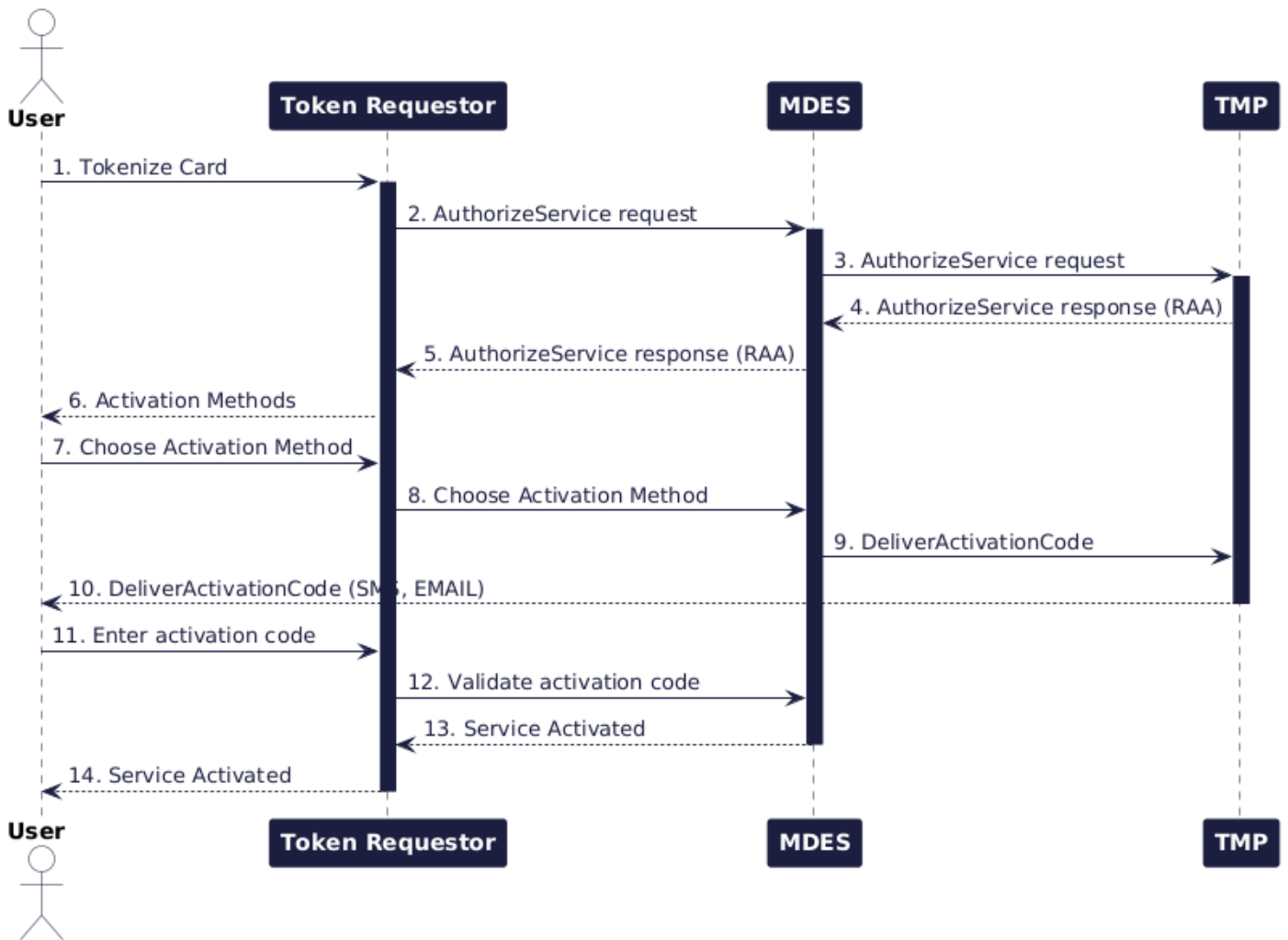
- **Green Path** - Path without user confirmation (authentication) during the token activation process. The payment token is automatically activated.
- **Yellow Path** - Path with user confirmation (authentication) during the token activation process. Payment token is activated after correct OTP is provided.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

More information about rules engine and path decisions can be found [here](#).

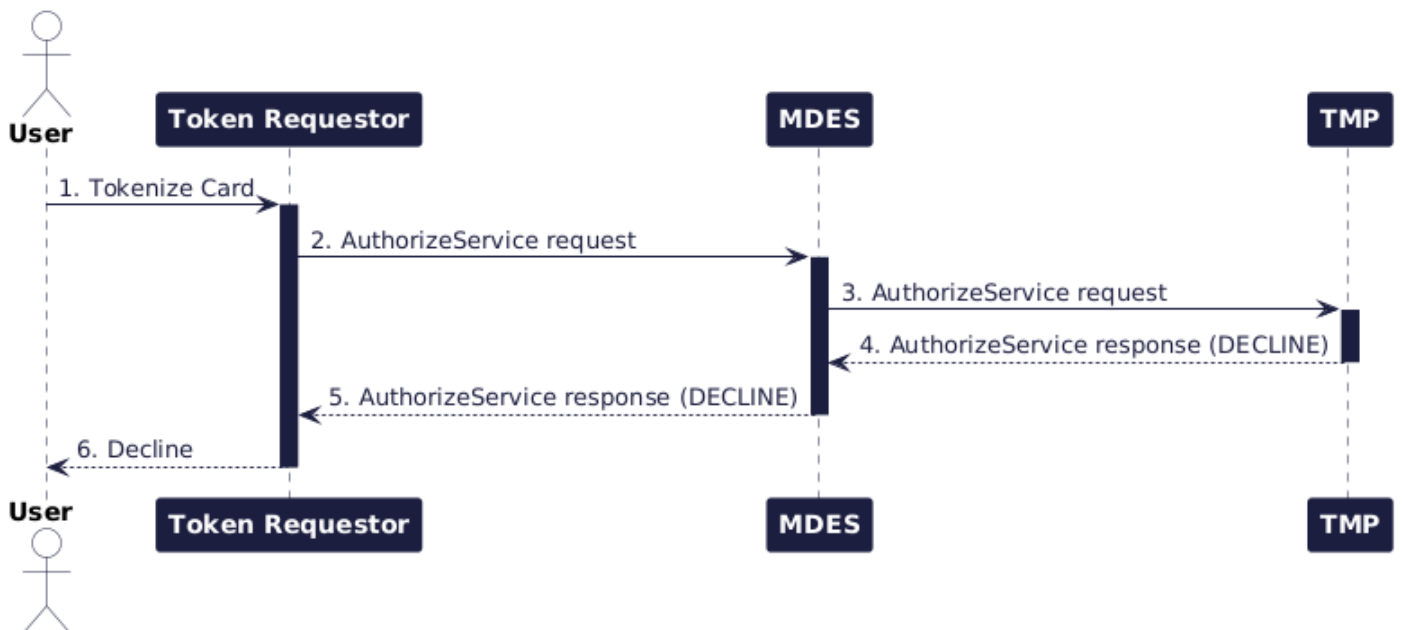
### Green Path



### Yellow Path



### Red Path



Verification steps:

- Verestro TMP sends OTP code via SMS or email (configurable option) to the Account Holder, but there is also possibility to do that by the Issuer, in that case Verestro TMP will notify the Issuer and then Issuer sends it to the Account Holder,
- Account Holder is entering received OTP and Verestro TMP is validating it,
- When OTP code is correct, notifyServiceActivated method is called which means that token is activated and ready to use.

Whole user notification process is described in details [here](#).

## Lifecycle

Token lifecycle support token management which can be use directly by the user or issuer's customer service using Verestro Admin Panel. This feature provides action on token to change token status. Actions what can happen are:

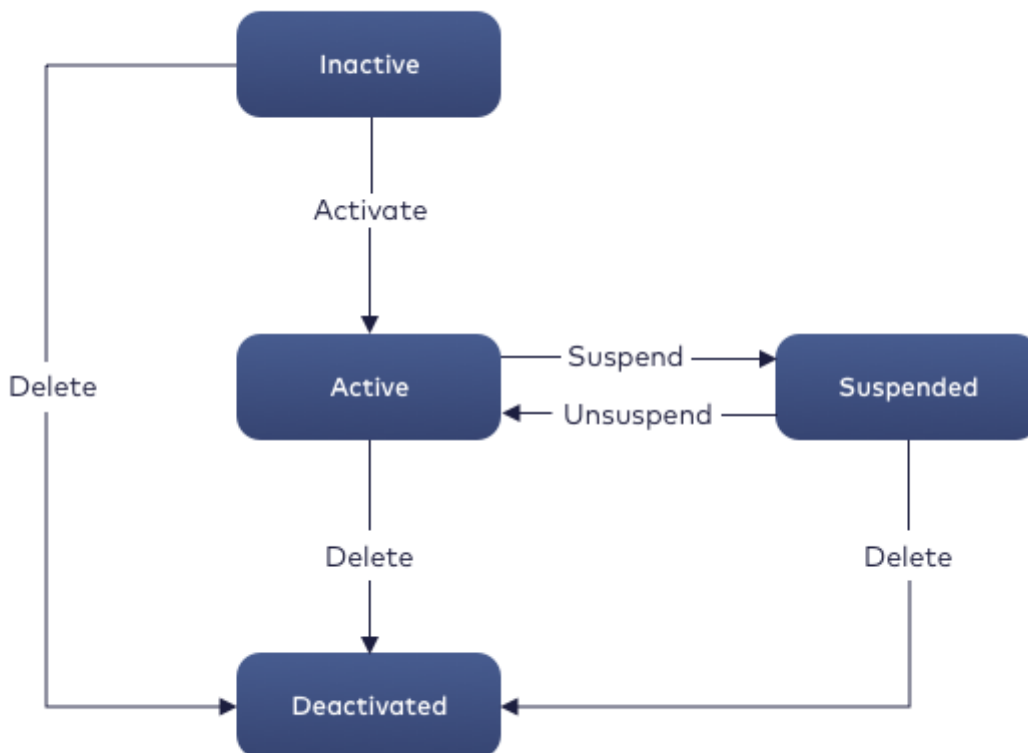
Activate token → change token status to Active,

Suspend token → change token status to Suspended,

Unsuspend token → change token status to Active,

Delete token → change token status to Deactivated,

The diagram below shows the transitions between payment token statuses.



Automatic lifecycle management is supported via Verestro TMP API thanks to integration with Verestron Lifecycle API.

# User notifications

According to xPays requirements, cardholders **must** be informed about the most important events connected with tokenization. Those events are:

- ACTIVATION\_CODE\_DELIVERY - **the most important one.** In most cases additional verification is required to successfully activate the token added to the wallet. To achieve that user needs to enter **6 digits OTP code** which is being sent alongside this event. This additional verification may happen both in Manual and Push provisioning.
- TOKEN\_ACTIVATED - confirmation, that token activation was successful (the card can now be used from the xPay wallet).
- CARD\_REMOVED\_BY\_CUSTOMER - this occurs when the user disconnects the card from the wallet.
- CARD\_REMOVED\_BY\_ISSUER - card removed by the issuer (e.g. when the issuer has cleared the user's balance).

In Verestro we offer 3 ways of delivering those notifications:

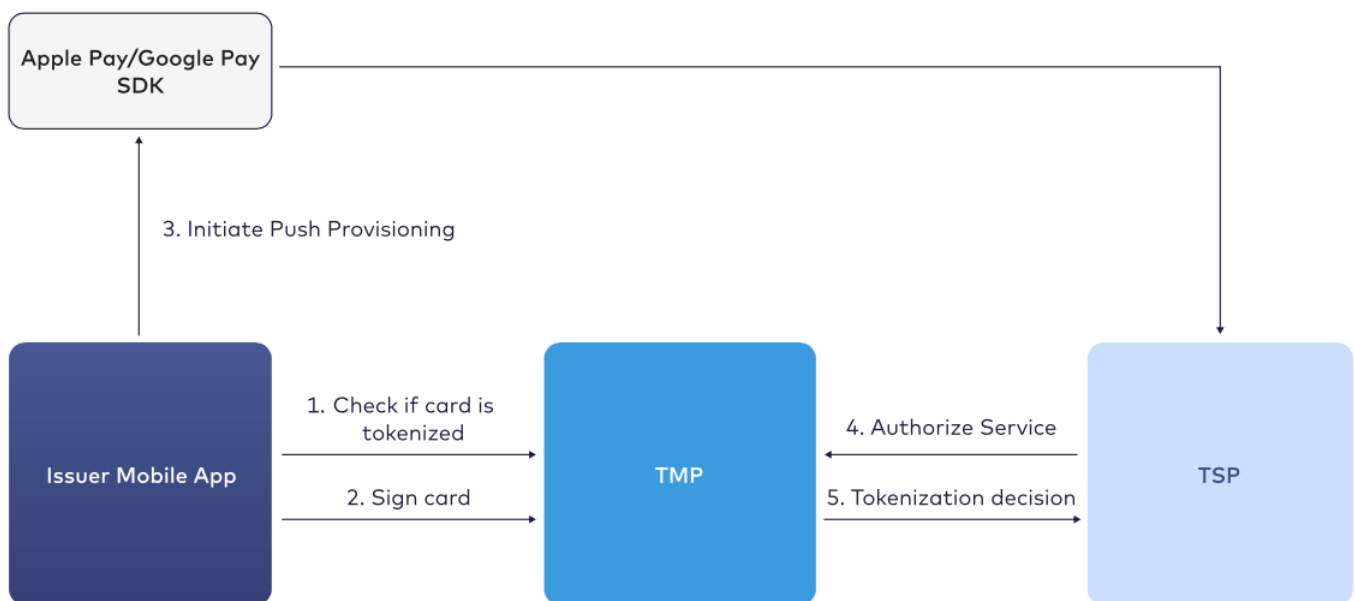
1. Verestro SMS Gateway - no development on the Issuer side needed. We handle all the SMSes sent to the cardholders. Fintech is charged according to agreed SMS pricing.
2. Custom SMS Gateway integration - Verestro backend may integrate with external SMS provider of Issuer choice. Issuer needs an agreement with selected provider and provide documentation necessary for such integration. As this is custom development it's billed and quoted separately.
3. Server-to-server notifications - Verestro backend may send the notifications to issuer's backend. From there it's issuer responsibility to deliver the notifications to the user - for example through different SMS gateway provider or as push notifications. To achieve that, issuer has to expose endpoint to us, according to below swagger documentation:

```
@swagger="https://s3.verestro.dev/valinor-public/user_notifications_issuer_api_1.4.0.yaml"
```

# Push provisioning

Push 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.



Verestro TMP Push Provisioning module API:

1. Check if the card is tokenized.
2. Sign card.

Verestro TMP Push Provisioning module allows the following flow:

1. Check if card is tokenized - Return information if a card is tokenized on the device, so the Issuer's mobile application can show or hide the "Add to Apple/Google Pay" button.
2. Sign card - Prepare an encrypted and signed payload that can be used by the Issuer's mobile application.
3. Initiate Push Provisioning with Apple Pay/Google Pay SDK.
4. Authorize Service to Verestro TMP.
5. Tokenization Decision returned to TSP (APPROVE/DECLINE).

@swagger="https://s3.verestro.dev/valinor-public/push\_provisioning\_tmp\_api\_1.2.1.yaml"