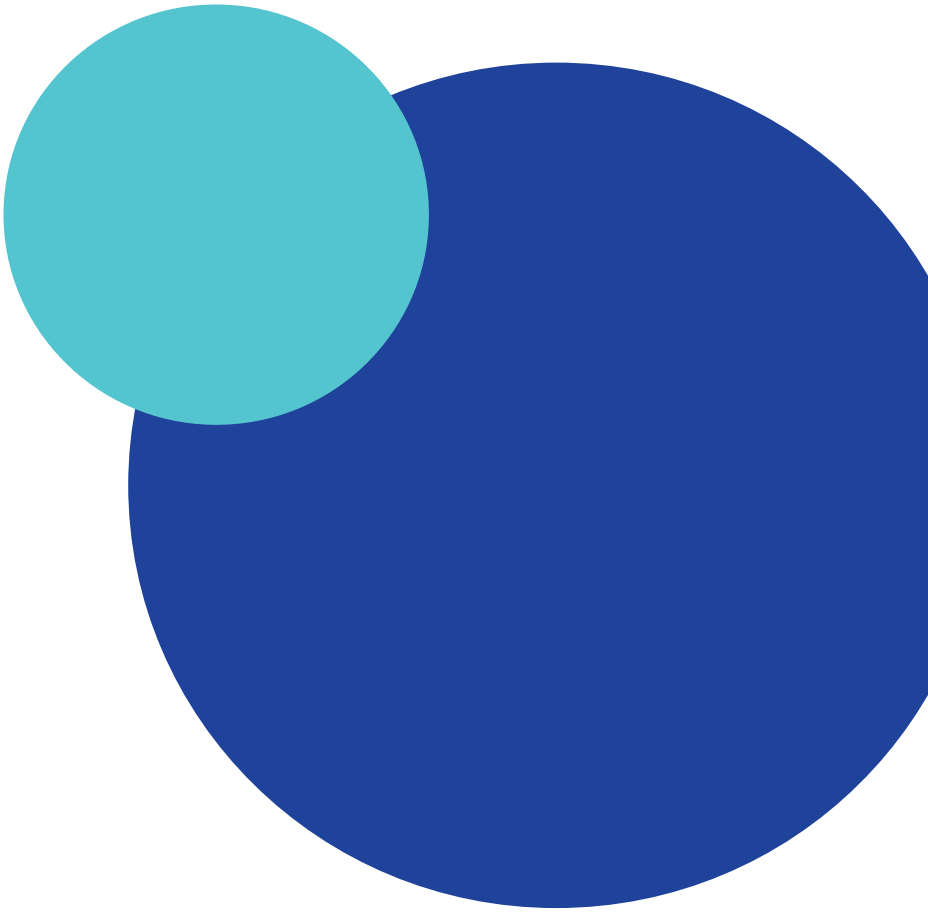
WHITE PAPER

nexi

How tokenization supports digital payment

Contents



Introduction

With the introduction of contactless payments and Host Card Emulation (HCE) technology, mobile proximity payments have begun to emerge in the digital payments landscape. Underpinned by the concept of tokenization, digital giants such as Google and Apple actively engaged with their x-pay wallets, supported by the international schemes providing the core foundation of tokenization. With the rapid increase of contactless acceptance and smartphone market penetration, banks are onboarding their card products to x-pay wallets to provide more seamless and better user experience for their cardholders.

Further acceleration has been observed during the Corona pandemic as contactless payments have been enforced to reduce human interaction to a minimum. As a result, all types of contactless transactions boomed, and x-pay wallet was no exception.

Tokenization

Tokenization enables frictionless, mobile based payments in both contactless and online commerce environments, without exposing cardholders' accounts to fraud.

Tokenization is the process of replacing sensitive data, like PAN, with non-sensitive information by using a surrogate value, referred to as a Token.

The **Token** can then be used instead of the original data, thus avoiding exposure of the sensitive data. Using the Token instead of the original data has the following benefits:

- There is no key or algorithm that can be used to derive original data from a Token
- Multiple Tokens can be created for one instance of the original data
- Usage of a Token can be bound to the specific entity requesting the Token, thus preventing unauthorized usage of the Token
- Tokens can be administered independently of the original sensitive data

The token information and its mapping to original card credentials are stored securely in a **Token Vault**.

About payment tokens

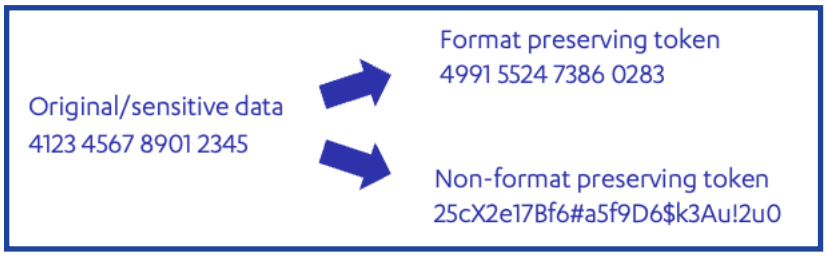
In a payment ecosystem, tokenization is used to replace an original PAN (from the physical card, often referred to as a funding PAN or **FPAN**) with a Token (referred to as device PAN/**DPAN**).

The process of tokenization is applied during the card enrolment process, that is, when a card is added to an x-pay wallet. During this process, the FPAN associated with the card being added is tokenized by a Token Service Provider by creating a token PAN, where the FPAN-DPAN relationship is stored in the Token Vault. The card provisioned to the x-pay wallet is based on the Token (DPAN) created during the enrolment process and will be used when using the x-pay wallet.

There are two types of token formats:

- **Format preserving token** – maintains look and feel of the original payment card data
- **Non-format preserving token** – does not resemble the original data and includes alphanumeric characters

Payment industry uses format preserving tokens with compatibility across existing payment ecosystems, payment network and processes.



Ecosystem participants

Token Requestor is the entity requesting tokenization of the sensitive card data for its services. Token requestors can be either:

- **X-pay wallets,** in case a card is provisioned to e.g. Apple Pay or Google Pay, to enable in-store mobile contactless and mobile-commerce transactions
- **Merchants,** in case cardholder registers their card with a merchant, such as remember-me or recurring payment purposes like Netflix. The merchant can then request a token as an alternative for storing (PAN) on-file

International schemes act as **Token Service Provider** that holds Token Vault and provide tokenization services, thus bridging Token Requestors and issuing banks:

- **VTS** Visa Token Service
- **MDES** Mastercard Digital Enablement Service

To enable tokenization and card enrolment to x-pay wallet for in-store contactless purchases, **Issuer** contracts the service with relevant x-pay wallet providers and registers their card portfolios (or selected card products) with corresponding Token Service Provider(s).

During token transaction processing, no changes are required on the **acquiring** side, whereas technical authorization and detokenization, that is converting a payment transaction based on DPAN to a corresponding transaction based on FPAN, is performed by the Token Service Provider.

Upon detokenization, Card Issuer performs traditional financial authorization based on underlying primary account number.

Processor aggregator role

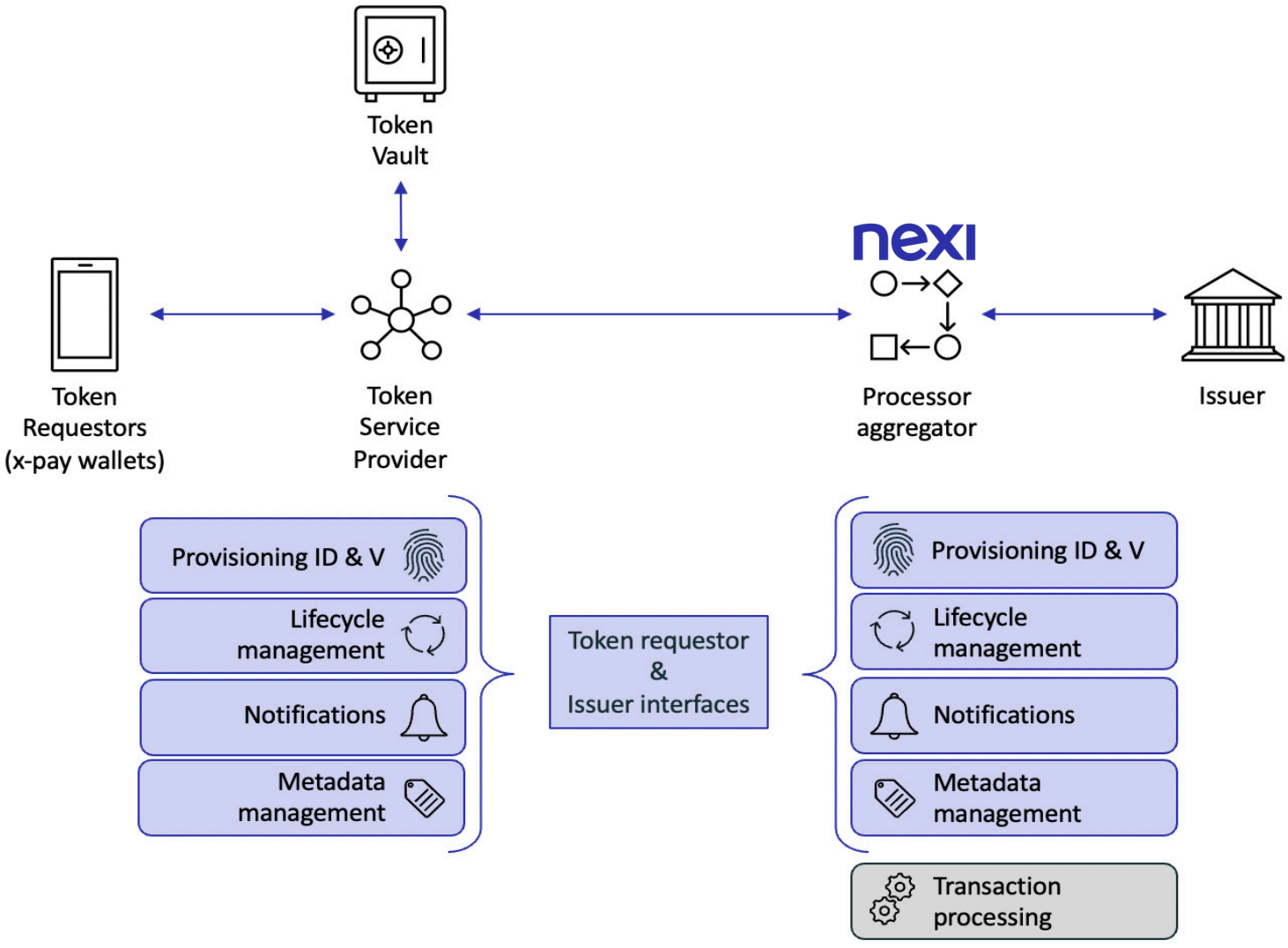
A Processor aggregator can support Card Issuers in the technical integration to Token Service Provider(s) and simplify the technical processes and integration to support Tokenization of the card issuer's card portfolio, on behalf of the issuer. The Processor Aggregator provides (some or all of) the following services to the Issuer:

I. Handles the provisioning (Tokenization) process, including necessary identification and verification process of cardholder

II. Supports necessary Token and PAN Life Cycle Management processes in agreement with the issuer, i.e. token creation, token status updates and enables card issuer to perform necessary token management operations (activate/suspend/resume/delete) as well as necessary token updates initiated in PAN life cycle operations, such as card blocking/unblocking as well as card replacement, renewals and closures

III. Supports necessary issuer and/or consumer notifications, in relation to token and card lifecycle operations. Furthermore, aggregator supports necessary notifications and reporting based on reward and incentive programs, authorized by specific x-pay providers

IV. Reporting based on issuers preferences and x-pay requirements



Feature and usage

Token/DPAN features:

- One FPAN can (in theory) have an unlimited number of associated DPANs but is limited to 99 DPANs by the Token Service Providers
- Each DPAN is unique per device/merchant
- Full DPAN is never exposed in clear text to cardholder or merchant
- DPAN may be stored in Secure Element or in the cloud (using Host Card Emulation) depending on device and wallet architecture

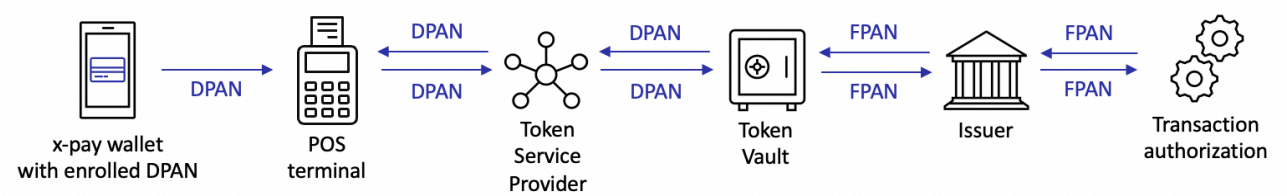
Secure Element is a tamper-proof chip found in handset, designed to prevent unauthorized access, and is used to store sensitive and confidential data like DPAN and associated information to create payment cryptograms.

The Token/DPAN is used and applied during:

- POS purchases and ATM cash withdrawals
- In-app purchases
- Online commerce

Translation of FPAN to DPAN and vice versa is performed by the Token Service Provider during transaction processing, including both authorization and clearing.

Tokenization provides an extra layer of security in digital payment landscape ensuring that sensitive data remains private, thus reducing the risk of fraud.



Enrolment & performance

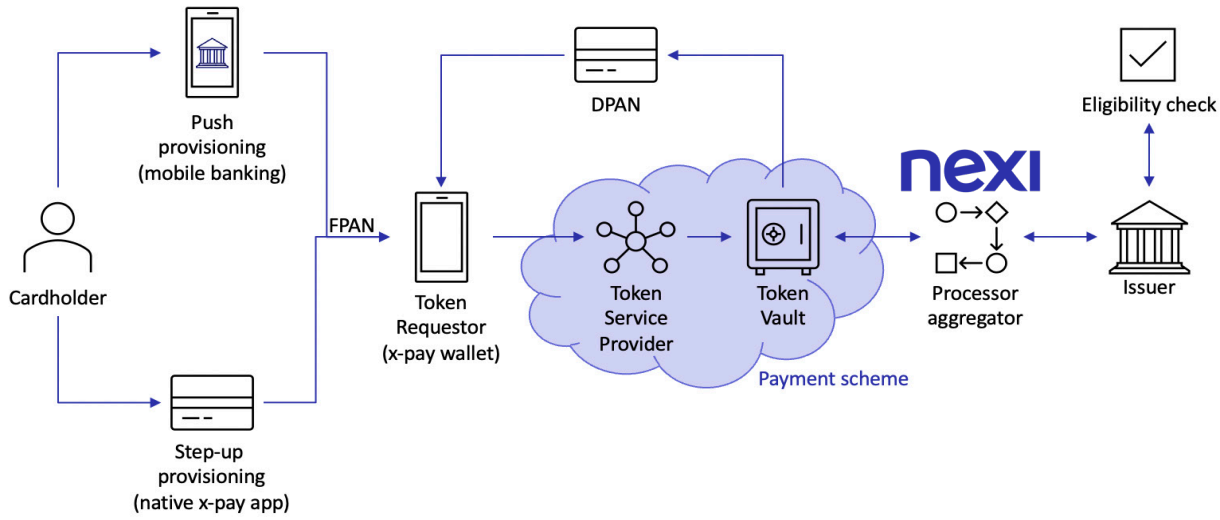
There are two options by which a cardholder can enroll their card to x-pay wallet:

- **Onboarding to native x-pay wallet app** is where the cardholder key-enters (or uses the camera to OCR capture) the card credentials. This process often requires a necessary **Step-up-authentication** of the mobile user, to secure that the user is the genuine cardholder. Step-up-authentication can be performed via OTP challenge, mobile app authentication or by requesting the cardholder to contact issuer's customer call centre for identification and verification. Once the mobile user is securely identified as the genuine cardholder, the Token can be activated to enable payments
- **Push provisioning** is a seamless and more user-friendly way to provision and activate Tokens, as it allows automatic card enrolment directly from the mobile banking app, upon proper authentication of the customer, as this is performed during login to the mobile banking app

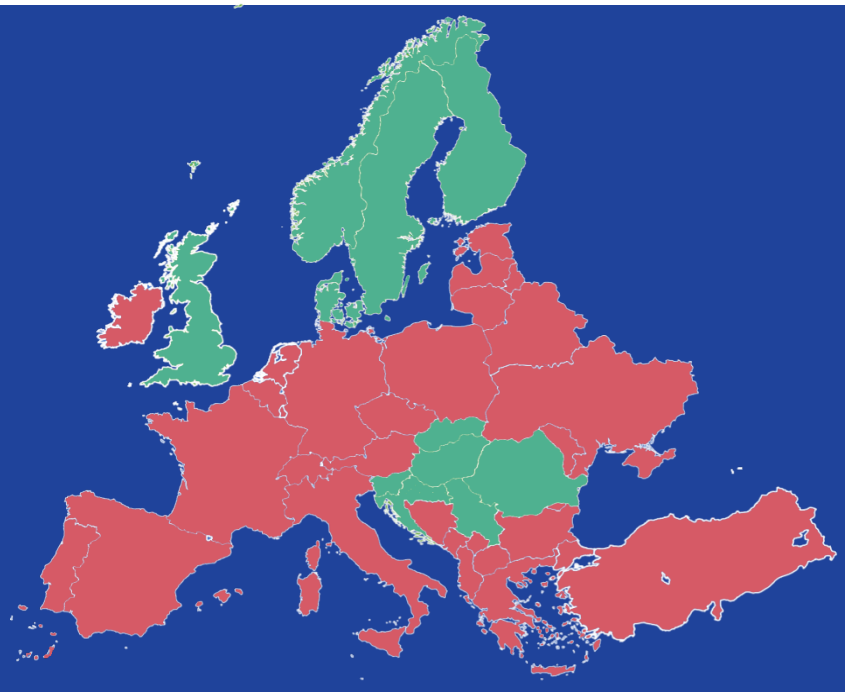
Due to the nature of tokenization, all Token based transactions must be processed via the Token Service Provider as off-us, i.e. there is no support for **on-us (or bilateral) transactions** using cards which have been tokenized.

There are **no changes in authorization and processing flow** for tokenized transactions, however **processing interfaces must be expanded** to include additional fields to accommodate identification of a tokenized transaction and identification of the specific Token instance used to initiate and complete the transaction.

Card enrollment workflow



Nexi Croatia delivers tokenization support to all the green countries



About Nexi Croatia

Nexi Croatia d.o.o. is part of the Nexi Group, a European PayTech operating in high-growth, attractive European markets and technologically advanced countries. We specialize in cutting-edge technological infrastructure and services for financial institutions, central banks, companies, and public bodies in the field of payments, cards, network services, and capital markets.

At Nexi Croatia we are dedicated to developing and managing payment business at the international level. This global mindset is reflected in our customers, staff and locations, while we make every effort to provide our clients with services and solutions that fit their specific needs, local particularities, cultural differences and regional complexities.

Our growing team includes more than 300 professionals, whose combined knowledge, creativity and enthusiasm aid in delivering quality service and value to our clients.

For more information please visit: www.nexi.hr or www.nexigroup.com

Contact us at sales_and_kam.cee@nexigroup.com.