

MyDebit Tokenisation

Introduction

The PayNet Tokenisation Service (TSP) allows issuers to manage the digital issuance of tokenized MyDebit payment credentials. Through this service, PayNet enables MyDebit payment ecosystem a flexible and scalable way to securely provision and manage payment token credentials. It currently supports issuing of e-Commerce payment tokens and would be expanded to other types of tokens in the future.

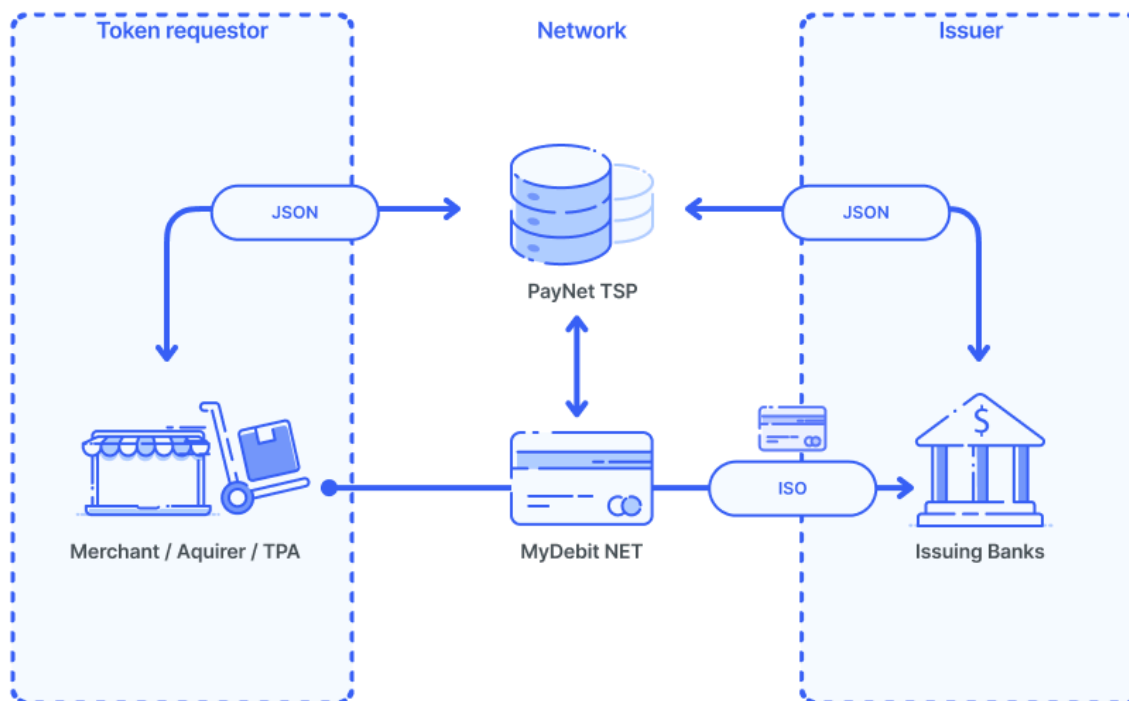
There are two main stakeholders under PayNet TSP Program:

- **Token Requestor (TR):** Participating merchants or Acquirers / Third-party Acquirers (TPA) of MyDebit networks
- **Issuers:** Participating banks that signs-up for PayNet TSP program to allow tokenisation of bank's card BIN ranges by TSP

Both stakeholders can be easily on-boarded by integrating with TSP's Merchant and Issuer API, which support both:

- ISO 8583-based message format (for Issuer only)
- JSON message format (Token Requestor & Issuer)

High Level Diagram



1. PayNet Tokenisation Program Overview

The payments industry is evolving to support payment technologies that provide increased protection from counterfeit, account misuse, and other forms of fraud especially in CNP transaction. While EMV® chip cards can provide substantial protection for CP transactions, a similar need exists to minimize unauthorized use of cardholder account data and to reduce cross-channel fraud in emerging transaction environments that combine mobile devices, e-commerce, and remote payment environments. Tokenisation holds the key to address these issues today

Payment tokens (Token PANs) are surrogate values that replace primary account numbers (PANs) stored electronically throughout the payments ecosystem and can be used to securely conduct payment transactions. In order for payment tokens to provide improved protection against misuse, the token is limited to use in a specific domain, such as a device or channel. These underlying usage controls are a key benefit of payment tokens

2. Benefits

There are benefits for all stakeholders in the payments ecosystem that may help encourage adoption of payment tokens:

Benefits to Consumers/Cardholders:

- Tokenisation is largely unnoticed by the end consumer but it increases the security of online / eCommerce transactions, thus giving consumer a more secure way to pay
- Consumer enjoys seamless payment experience by having their cards tokenized, since they no longer require to enter lengthy card information upon checkout
- In addition, cardholder can now see the exact card art with its details, making it easier for user to identify their favorite card for use.

Benefits to Issuers:

- Card issuers as well benefits from a security perspective, when adopting tokenized payment instead
- In addition, it helps improve transaction approval levels, and reduced risk of subsequent fraud in the event of a data breach in which payment tokens are exposed instead of the underlying PANs.

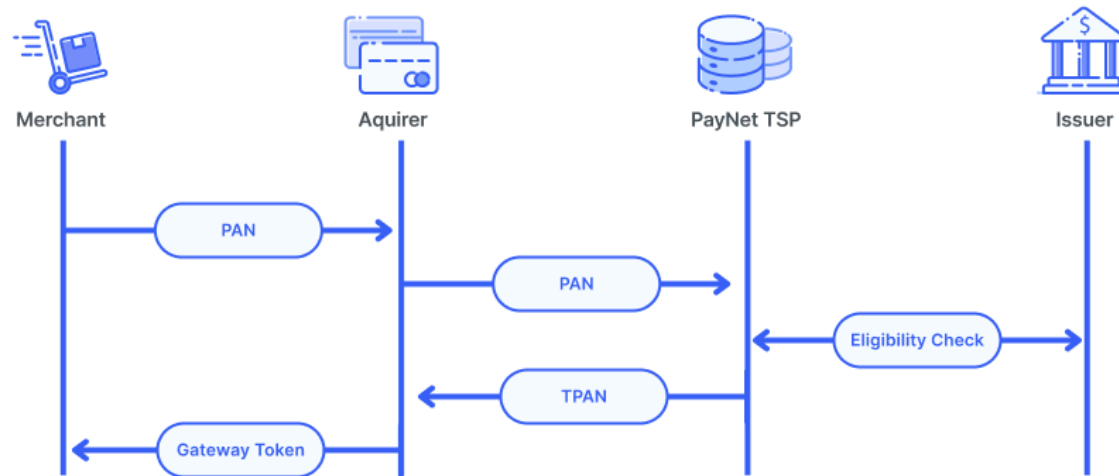
Benefits to Acquirers, Merchants, and Merchant Processors:

- Acquirers and merchants may experience a reduced threat of online attacks and data breaches, as payment token databases may be less appealing targets, given their limitation to a specific domain
- Acquirers and merchants may also benefit from the higher assurance levels that payment tokens offers, with higher approval rate from Issuer since card expiry date stored inside token vault are automatically renewed by Issuer to ensure continuity of the card token

3. Functional Use Case – eCommerce/Online Payment

This chapter describes the functional use case of tokenisation in relation to how a token is initiated, which can then be used for making payments when shopping online

Token Provisioning Diagram



3a. Card Tokenisation Flow

An eCommerce / COF token provisioning is typically an in-purchase or passive user experience, whereby a consumer tokenise their payment card either during or after completing an online purchase

- Consumer agrees to enroll/tokenise their card by entering their PAN, PAN expiry, CVV and other payment account information at online retailer/mobile wallet
- The acquirer/PSP sends token provisioning request to PayNet TSP for card tokenisation to be initiated
- Upon successful eligibility check, i.e. the card BIN range is registered, PayNet TSP will proceed to tokenise the card and respond with TPAN, TPAN Expiry, card art and other token account

information to the acquirer

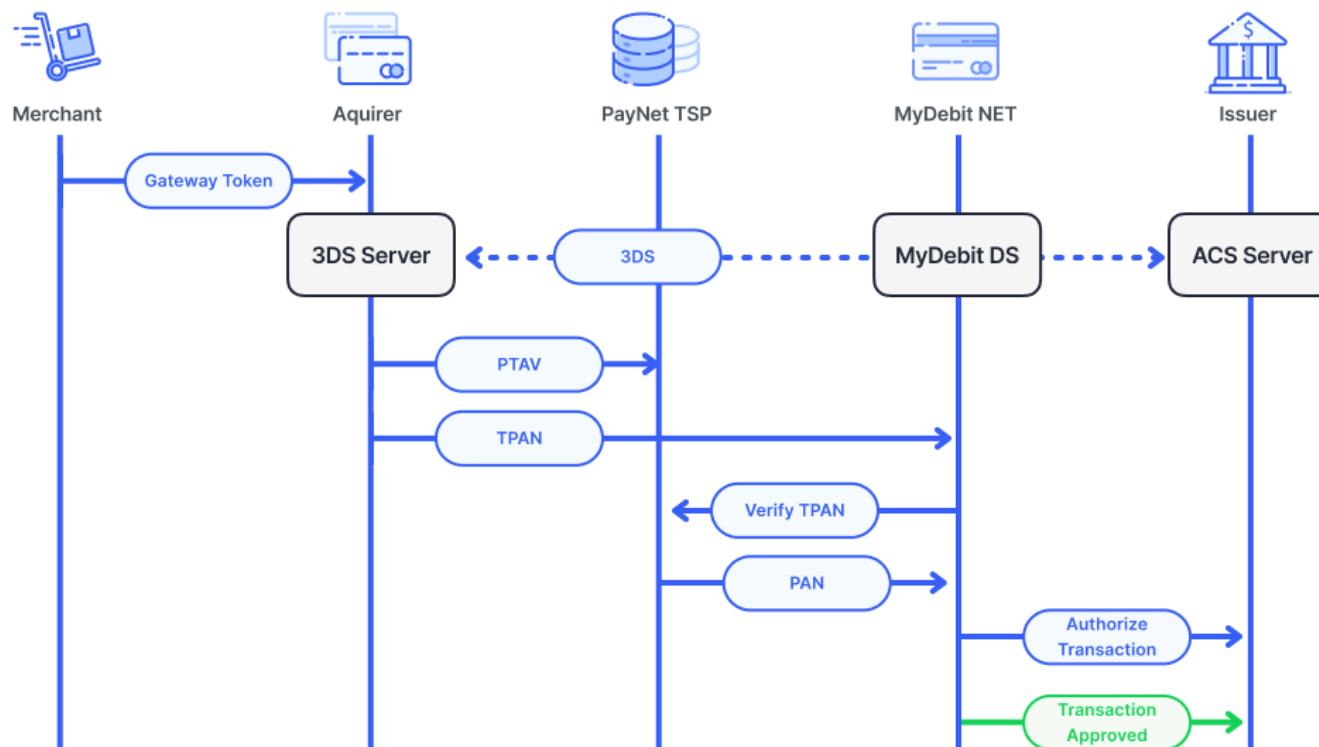
- The acquirer could store that information and returns a gateway token to the merchant instead, or it can also return those TPAN information directly to the merchant

Note:

- It is mandatory for the acquirer / PSP to first perform cardholder verification, by triggering a purchase transaction with 3-D Secure, before tokenizing the card

3b. Token Payment Flow

After token provisioning flow is completed, the tokens are active, and it can be immediately used to make a purchase transaction



Consumer initiates payment using his/her previously tokenized card at merchant checkout. Gateway token and related transaction data are sent to acquirer/PSP for processing

Typically, Acquirer / PSP will perform 3D-Secure by triggering AReq to 3DS server using TPAN instead of PAN. DS will forward to corresponding ACS for authentication. Once consumer are authenticated (if required), ACS will send PIAV and ECI value back to Acquirer

Acquirer / PSP then triggered “Get Token Data” API to PayNet TSP in order to obtain PTAV, which is a unique payment token cryptogram for each transaction

Acquirer constructs “Payment / Purchase Request” message with all the information obtained from 3DS and TSP and send it to MyDebit NET

MyDebit NET will then forward the token payment transaction with its related data, e.g. TPAN, PTAV, TRID and others, to be verified by TSP

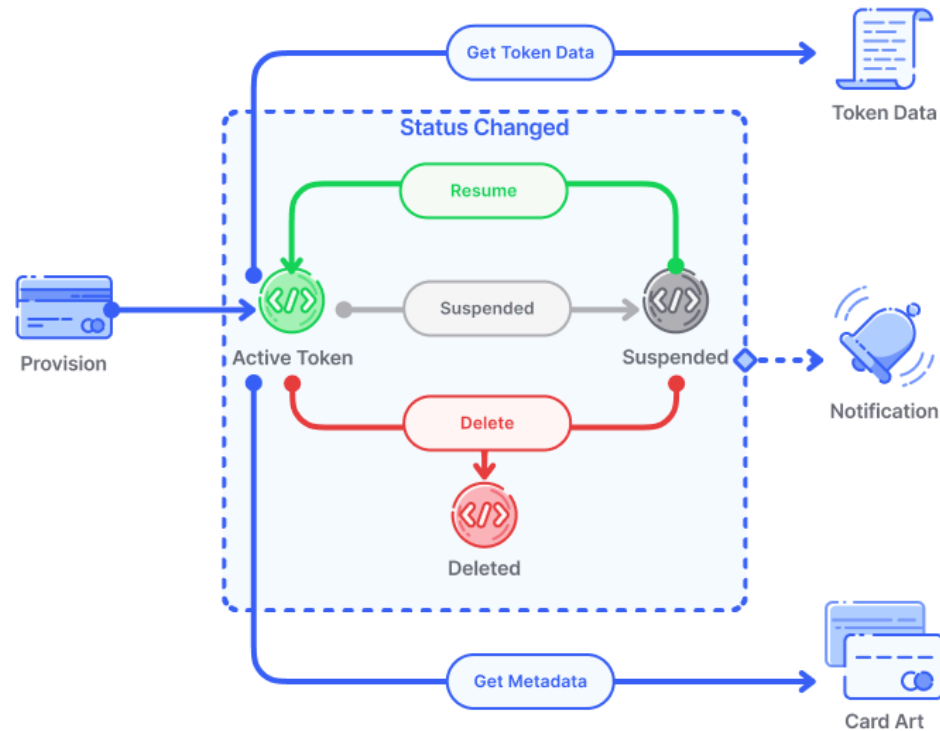
Once the token transaction is verified, TSP will perform de-tokenisation and returns PAN information to MyDebit NET

MyDebit NET then forwards the transaction to be authorized by corresponding Issuer

If authorization is successful, an approval will be generated and return to Acquirer / PSP via MyDebit NET as usual. It does not pass through via TSP in the return flow

Acquirer / PSP then informs Merchant application of payment success

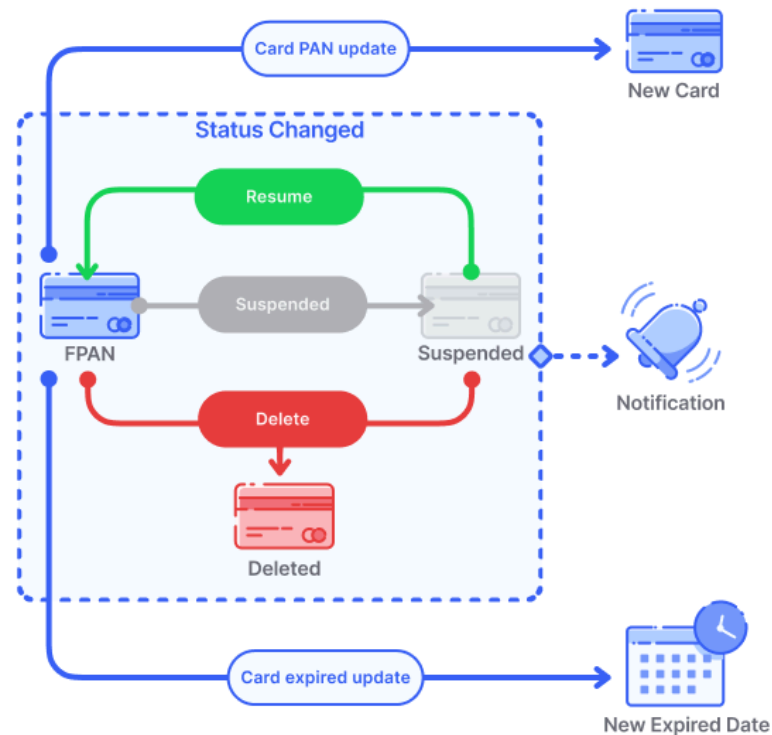
3c. Token Lifecycle Management – For Acquirer / Merchant



PayNet TSP exposes an easy-to-use API interface for Merchant/ Acquirer/PSP to interact with payment tokens under its care. Notification API is a very important API features of TSP, because it informs the Merchant/Acquirer/PSP in real-time if there are any changes to the status of the tokens

Example: If a cardholder reports lost/stolen card, issuing bank can immediately trigger an API to “Suspend Card”, and therefore all corresponding tokens bound to the card is immediately suspended and notification is sent to all merchant/acquirer that has that corresponding token in their vault Since Issuing bank holds cardholder liability, any changes in card lifecycle events triggered by Issuing bank will override/supersede existing payment token status and will be notified accordingly to the acquirer/merchant

3d. Card Lifecycle Management – For Issuer



PayNet TSP also exposes a number of API for Issuer to perform card lifecycle management, which is crucial to ensure validity of the card in association to the tokens

- Card DELETE/SUSPEND/RESUME API
- Card EXPIRY DATE UPATE API
- Card PAN UPDATE API

Example: If a cardholder recently renews or replaces his/her debit card, upon fingerprint verification at branch, issuing bank can trigger an API to “Update Card PAN”, so that all corresponding tokens bind to the card is now updated with the new card information. This prevents transaction decline due to change in card PAN or expiry information, which is very common for eCommerce card-on-file transaction

4. Token Transaction Authentication and Authorization Principle

Irrespective of the business processes that a merchant uses for eCommerce transactions, there are some fundamental principles, which PayNet have defined, that shapes the approach when it comes to token transaction. These principles are summarized below and are the basis for the approach in handling for each scenario

Principle	Rationale
1. PIAV proves authentication has taken place and carries liability shift protection, while PTAV does not	PTAV acts as an added security in place to ensure originating online transactions is received “as-is” from Acquirer to PayNet TSP. Liability shift protection still falls back to existing EMV 3DS scope and framework
2. If PayNet TAV verification failed or if token is invalid, MyDebit NET should reject the transaction	Failed PTAV verification are indications that originating transactions are highly suspicious, possibly an MITM attacks or Acquirer/PSP was partially compromised. Transactions will be rejected to prevent possible fraud in the network
3. Token Transactions require a PTAV unless they are being submitted as MITs	PTAV is to be present in all Token transactions unless the transaction is identified as a Merchant Initiated Transaction (MIT). Typically, MIT can only occur after an initial Cardholder Initiated Transactions (CIT) has been performed to establish a customer agreement Examples of MIT: Installment payment, recurring and unscheduled COF

5. Merchant and Acquirer Participation

</> See also API reference for Tokenisation Services for Acquirer/Merchant [Check API](#) >

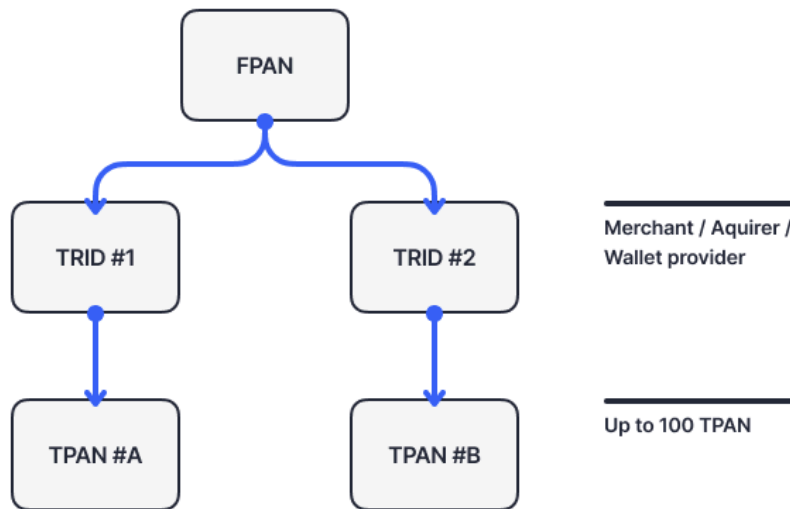
This section gives an overview from the perspective of merchant/acquirer system including some participation requirement when merchant/acquirer participates the PayNet TSP program

5.1 Correlations between TRID and TPAN

Upon successful on-boarding of merchant / acquirer into PayNet TSP program, the system will assign a unique identity to the token requestor. This identity is an 11-digit numeric called the Token Requestor ID (TRID)

TRID = [TSP Code (3-digit)][Assigned by TSP, (8-digit)]

TRID is used by TSP to diversify the TPAN assigned to the token requestor. For the same FPAN, a different TPAN is generated for a different TRID. TRID is only assigned to Token Requestor which stores their own token



Example:

If Merchant #A stores its tokens with the payment gateway / acquirer vault, then TPANs are generated based upon the TRID of the payment gateway / acquirer

However, if the Merchant #A manages its own token vault, but just uses the payment gateway for authorization service, then a separate TRID should be used. In this case, Merchant #A will connect directly to PayNet TSP for token provisioning. It is also responsible to obtain PTAV prior to any payment transaction triggered to the payment gateway

TRID also used by TSP as a security measure within the tokenisation ecosystem

- Token Domain Control
 - Since TRID is only restricted to a particular merchant, it limits the exposure of the system
- Cross-domain/channel Fraud
 - During token transaction verification, TSP will examine if the corresponding TPAN belongs to the appropriate TRID, to detect any abnormal transaction behaviors

5.2 Authorization Routing

Participating acquirer/PSP will receive a separate token BIN range from PayNet, so it could detect that these transactions are token transactions. Acquirer could then make the right routing decision when forwarding to scheme network for authorization

Merchant Opt-In

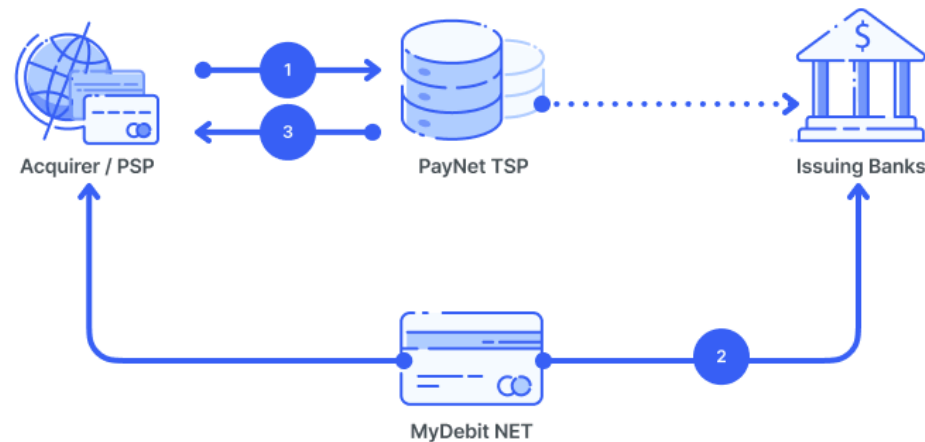
Emulating the same behavior in CP environment today, if an online/eCommerce merchant opted-in with MyDebit for CNP transactions, the acquirer / PSP must be able to route those transaction to MyDebit NET, based upon the token BIN range that is provided by PayNet

PayNet Token BIN range: 608727 [000-999] *Token BIN range will be updated from time-to-time by PayNet*

5.3 Migration for Existing Acquirer Tokens

There are two options which are available for merchant/acquirer who already have tokens already stored in the vault but would like to tokenise those with PayNet

Option A: File-based via SFTP



This method mainly caters for merchant / acquirer which has large pool of existing tokens:

PayNet will provide a secure SFTP endpoint for acquirer / merchant to upload a CSV file containing necessary card that can be used for token provisioning

Using batch process, card verification is performed, by sending a CNP Pre-Auth transaction to Issuer (zero value and immediately reversed), to ensure that the card is still active

Tokenisation is then done, and the process repeats itself for the entire information in the file.

PayNet will place the output file back to the SFTP service, to be pick up by merchant at their convenience

Migration procedures to be discussed in more detail with merchant/acquirer during implementation

** Option B: Trigger through UAT API

This method is mainly suitable for merchant / acquirer who did not have a large number of existing tokens yet. In this case, it might be easier to trigger via API

The flow would be the same with SFTP, except that Step 1 triggering is from backend using UAT API (which uses different API keys and endpoint from the production environment). Merchant / Acquirer will receive real-time response to all request, and once

6. Issuer Participation

</> See also API reference for Tokenisation Services for Issuer

[Check API](#) >

Overview of the participation requirement of Issuers and how they could interact with PayNet TSP system

6.1 BIN Range Configuration

Participating issuers in the PayNet TSP program will enroll their corresponding debit BIN range to be eligible for tokenisation. Card information like card metadata, and card art can be uploaded into the system

If no card art is provided during configuration and initial setup, TSP system will automatically assign a generic card, which is tailored to the corporate color of the issuing bank respectively. For a start, BIN range configuration process will be managed by PayNet administrator. However, Issuer can manage non-essential data themselves by logging into TSP Issuer portal provided by PayNet

Admin Console

Home / Issuers / Add New BIN Range

Issuer

ISS000000001 Big Bank

PAN BIN

456710

PAN Range

Token BIN

780010


Token Range

Description

Platinum Card

Card Metadata

Card Art



Card Art

Click card art image to upload a new image and replace the current image.

Foreground Color

#F3FFB8

6.2 Authorization for Token Transaction

In order to process token transactions for authorization, issuing bank need to upgrade their Host system backend. Token transaction carries additional data in Field 120 of ISO-8583

Please refer to “PayNet MyDebit ISO8583 Interface Specification VX.X” for more information

6.3 Issuer Portal Access

Participating issuer will be provided access into PayNet TSP Issuer portal for the following:

- To view / edit non-sensitive Issuer profile like Card metadata or upload Card Art
- To query token events history given a particular FPAN

These functions are provided to assist issuer in their own transaction-related investigation or accessed by customer support department for cross checking.

These accounts will be created by PayNet administration, to be send to Issuer upon successful on-boarding and integration into the system

Issuer Portal

Hi, Mac Michael

Home / Tokens / Token Events

All Token Events

Export to Excel

Items per page: 10

PAN	Token PAN	Event	Requestor	Request ID	Response ID	Date	
5312341111060414							
5312 34** **** 0414	5412 34** **** **5 019	TOKEN_DATA	MER00000001	REQ0001591254168076	TSP1FZEIOWWCcoQkQTlp	2020-06-04 15:02:46	Show
5312 34** **** 0414	5412 34** **** **5 019	PROVISION	MER00000001	REQ0001591254106174	TSP1FZEIQ00CcCVhaYGB	2020-06-04 15:01:45	Show

Total number of records: 2

Given FPAN

List of Tokens

List of Token Events