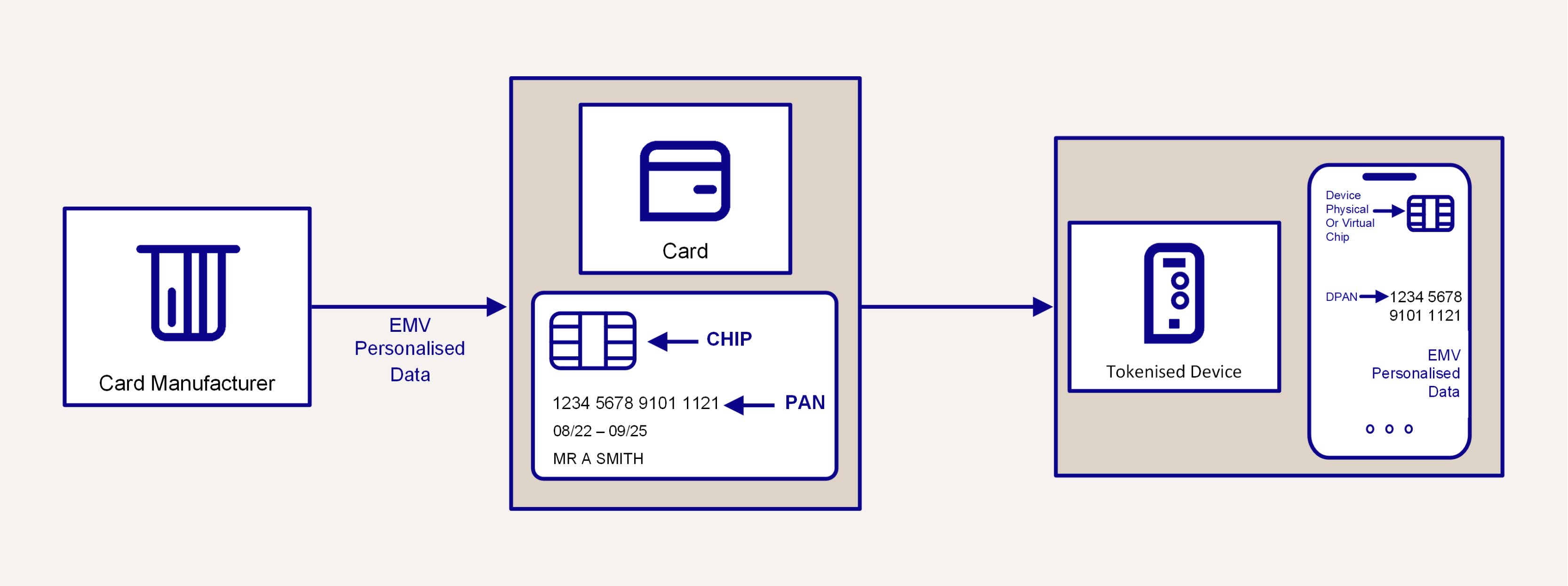
Product Sheet

Tokenisation

Make payments using a Mobile Wallet on a smart device such as a smartphone

Create digital tokens for your cards, which can be used for payments on smartphones and other tokenised devices, and at merchant online stores

Tokenisation is a security technology which replaces the sensitive 16-digit permanent account number (PAN) that is typically embossed on a physical card with a unique payment token (a digital PAN or DPAN). The token can be used in payments and prevents the need to expose or store actual card details. The DPAN is used to make purchases in the same way as a normal Funding PAN (FPAN).



Tokenisation enables cardholders to access mobile wallet functionality – provided by companies such as Apple and Google – which allows payments to be made in store from a smart device such as a smartphone or tokenised device. Tokenisation also helps merchants improve the security of online payment transactions by replacing the sensitive PAN card details with a token and storing this instead. The token can then be used for repeat or recurring payments. Both Mastercard and Visa offer a tokenisation service to card issuers. Mastercard offer the Digital Enablement Service (MDES) and Visa offer the Visa Token Service (VTS), which are both supported by Thredd. Thredd refer to the Visa service as the Visa Digital Enablement Program (VDEP).

Features

Support for Multiple Token Requestors

- Thredd enables you to set up both:
- **Mobile Wallet Token Requestors** – such as Apple and Android, who provide a token service via a smartphone or other mobile device Description.
- **Online Merchant Token Requestors** – who tokenise a payment card so that the token can be used for repeat payments or recurring payments on their website.

Token Provisioning

- During tokenisation Thredd communicates with the Token Service Provider (Visa or Mastercard) in real-time.
- All messages obtained are sent over EHI to the Program Manager.

Push Provisioning

- This option enables you to pre-authenticate the cardholder before the first token provisioning message is sent to the token service provider (Visa/Mastercard).
- Solutions are available for customers who are not PCI DSS Compliant but need to process the PAN.

Benefits

Business Facing

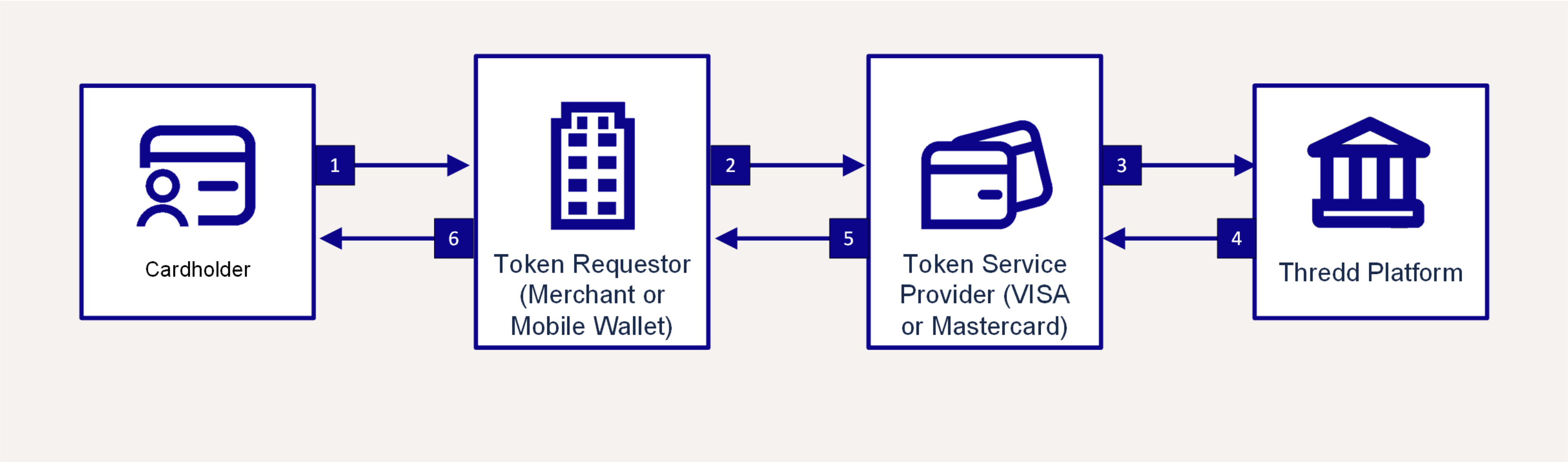
- Increase your service offering
- Increase customer adoption
- Reach more customers by offering exciting and innovative tokenised payment options
- Flexible options for setting up your tokenisation service
- Control where and how the token can be used through card usage and other control groups

Customer Facing

- Access payments on their smartphones or other tokenised devices
- View real-time transaction information

How it works

The figure below provides an overview of how tokenisation works.



Cardholder
1
6
Token Requestor (Merchant or Mobile Wallet)
2
5
Token Service Provider (VISA or Mastercard)
3
4
Thredd Platform

1. The cardholder enrols their card with a token requestor (either an online merchant or a mobile Wallet provider).
2. The token requestor requests a new token from the token service provider (Visa/Mastercard).
3. The token service provider creates the payment token (DPAN), containing EMV and other card data, to replace the cardholder's FPAN. The token service provider sends a Token Activation Request (TAR) to the issuer host (Thredd).
4. Thredd decides if token activation can continue, based on the Thredd Configuration Options set up for your programme. (See Token Authorisation Options below.)
5. With Thredd approval the token service provider (Visa/Mastercard) activates the new payment token and sends the newly created token to the token requestor.
6. For an Online Merchant payment token, the token is stored for use on their website. For a Mobile Wallet payment token, it is installed on the phone for mobile Near Field Communication (NFC) use.

Transactions on the token

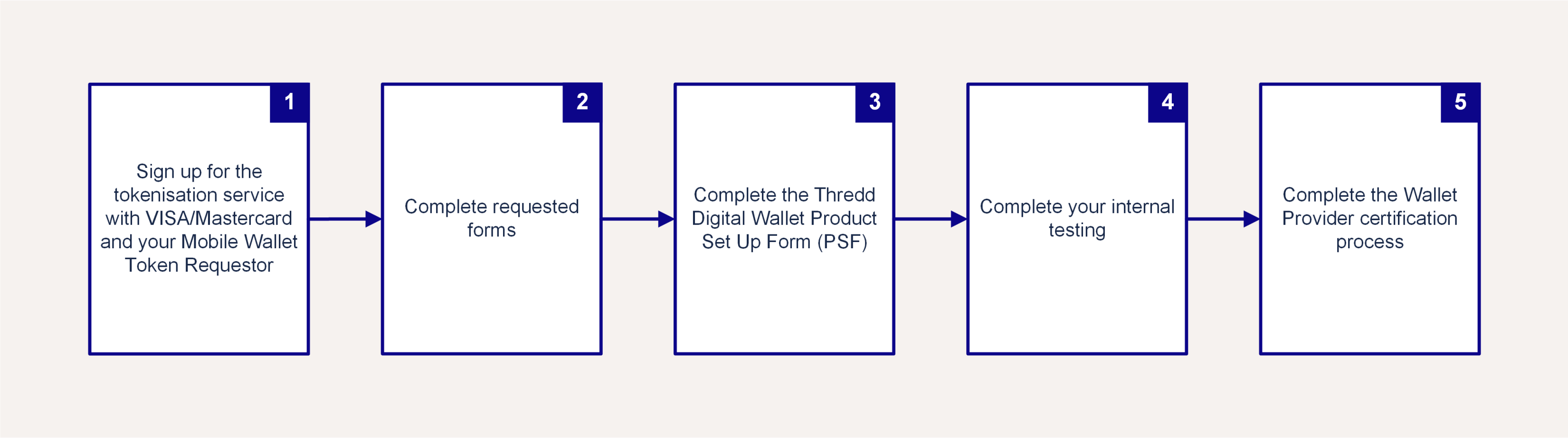
Once the digital token (DPAN) has been created, it can be used in place of the card for payment authorisation transactions. Transactions on a token look like standard transactions on the card, but the payment token has additional data.

Managing tokens

Managing a tokenisation service program is handled through both the Visa/Mastercard Online Portals and through Thredd API.

Setup At-a-Glance

Below is a high-level view of the setup steps.


1
Sign up for the tokenisation service with VISA/Mastercard and your Mobile Wallet Token Requestor
2
Complete requested forms
3
Complete the Thredd Digital Wallet Product Set Up Form (PSF)
4
Complete your internal testing
5
Complete the Wallet Provider certification process

Step 1. Sign up for tokenisation

Sign up with each of the following participants in the tokenisation process:

- The **Token Service Provider** (Visa or Mastercard)
- The **Mobile Wallet Token Requestor(s)** of your choice (e.g., Apple, Android, Fitbit, Samsung).
- The **Issuer Host** (Thredd). Contact your Thredd Account Manager

Note: If you are using a BIN Sponsor, you will need to go contact them to discuss your tokenisation project.

Step 2. Complete Requested Forms

Once you have signed up with Visa/Mastercard, your assigned Visa/Mastercard project manager or contact will send you a number of documents for completion. The Visa and Mastercard documents require Thredd input as they relate directly to the functionality on the Thredd platform.

Step 3. Configure your Thredd settings

Once a project is open with Thredd, your Implementation Manager will work with you to understand how you want your token service programme to work.

You must complete the Thredd Digital Wallet Product Set Up Form (PSF) to confirm your tokenisation service configuration options.

Step 4: Complete your internal testing

Complete internal pilot and pavement testing in the production environment. Get to know how your tokenisation app works and test against the wallet provider test scenarios.

Step 5: Complete the Wallet Provider certification process

Some Wallet providers, such as Apple Pay, have a formal certification process. Thredd recommends speaking to Apple Pay or your issuer in the first instance.

Google Pay does not have a formal certification process. Instead Google will send test scripts to you or your Issuer.

FAQs

Q. What is the role of Thredd in the tokenisation process?

Thredd are the issuing host and can approve or decline the tokenisation requests. Thredd plays an important role in connecting your program to the Token Service Providers (Mastercard/Visa), configuring the service and providing your systems with messages to support the tokenisation service.

Q. How do we start a project?

You need to open a project with the Token Service Providers (Visa/Mastercard) and with Thredd. Please discuss with your Account Manager.

Q. What do we need to do as a Program Manager?

Essentially, you are the owner of the project and need to manage all parties involved in the setup of the service (mobile wallet token requestors, token service providers and Thredd).

Q. How long does a project take?

Adding tokenisation to an existing product takes approximately 3 months. This depends on many external factors and delays may occur in the live testing with Token Requestors.

Q. Why do we need EHI?

EHI is used to retrieve the One Time Passcode (OTP) used in authentication. You need to send the OTP to the cardholder quickly and so cannot be sent via any reports. If you choose not to use EHI, you will only be able to use the Thredd SMS option to send the OTP to the cardholder.

Q. Do we need to develop an app?

If you wish to support Mobile Wallet Token requestors, then an app is required. Please discuss with your chosen Token Requestor. You do not need an app for Online Merchant Token Requestors.

Q. What is in-app provisioning and do we need to be PCI compliant?

In-app or push provisioning is done within your own app. This means that you have pre-authenticated the cardholder (check with Apple for a suitable authentication option) and want the token request to be approved. During push provisioning the cardholder will not enter their PAN and instead an encrypted blob must be sent to Apple to confirm the card details. Since a PAN is needed, you must be PCI compliant to complete this yourselves. Alternatively, you can use the MeaWallet service to do this on your behalf, and you will be able to extract PAN data directly from Thredd to complete this.

Q. Where can I find out more?

For more information, refer to the Tokenisation Service Guide or contact your Account Manager.

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd Ltd.

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House
229-231 High Holborn
London
WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.