



Tokenisation Service Guide

Version: 2.2

12 June 2025

Publication number: TSG-2.2-6/12/2025

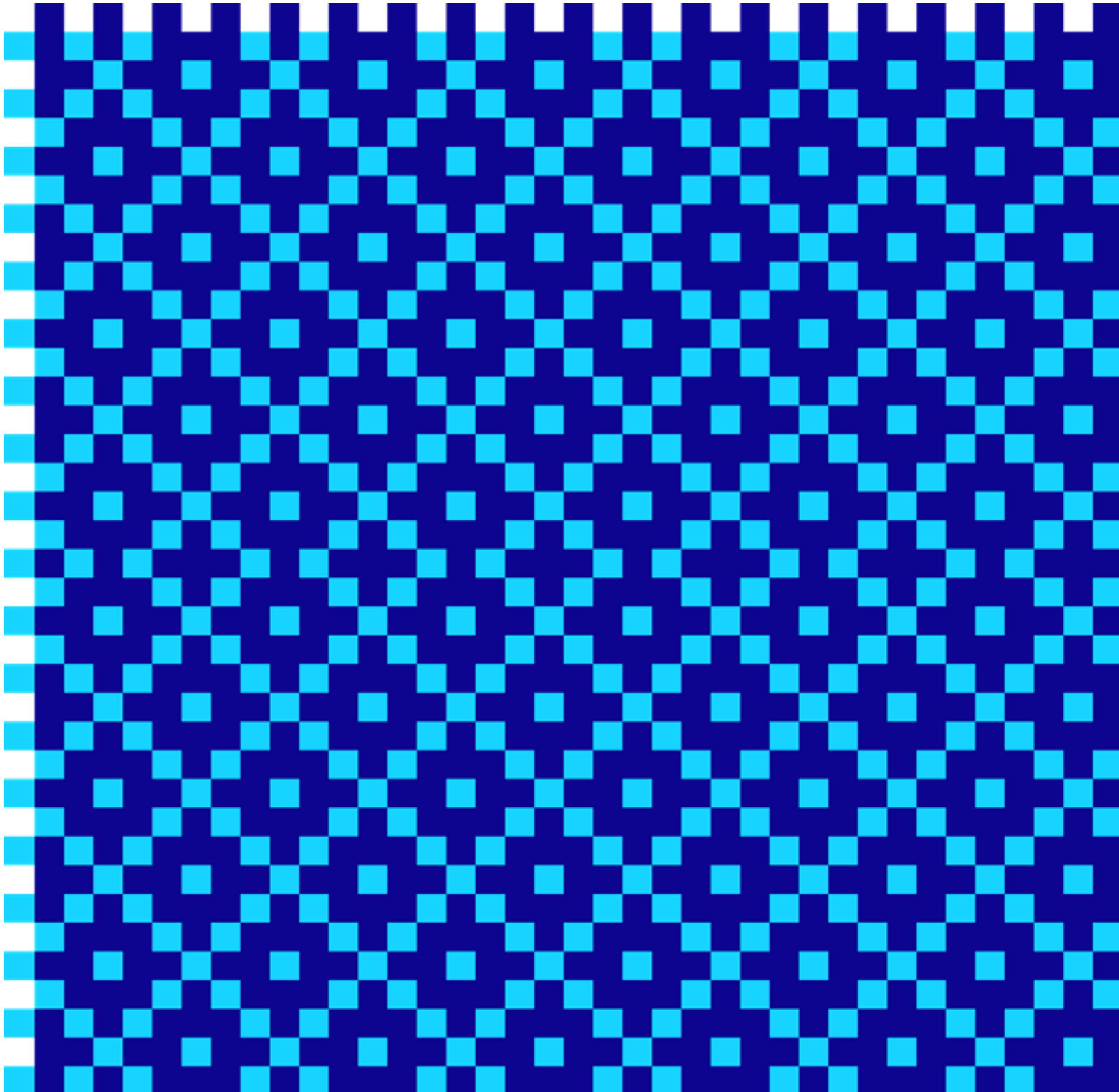
For the latest technical documentation, see the [Documentation Portal](#).

Thredd, Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

© Thredd 2025





Copyright

© Thredd 2025

The material contained in this guide is copyrighted and owned by Thredd Ltd together with any other intellectual property in such material.

Except for personal and non-commercial use, no part of this guide may be copied, republished, performed in public, broadcast, uploaded, transmitted, distributed, modified or dealt with in any manner at all, without the prior written permission of Thredd Ltd., and, then, only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in these materials is subject to change without notice and Thredd Ltd. assumes no responsibility for any errors.



About this Guide

This guide describes the Mastercard and Visa token services and how Thredd supports tokenisation. It explains how to set up and process tokens on the Thredd system.

Document Scope

This guide describes the process of implementing and managing the Digital Wallet product on a Visa or Mastercard programme and is aimed at any new or existing Thredd customers who wish to add this functionality and enable token-based mobile payments for their cardholders.

Target Audience

This guide is intended for Thredd clients (Program Managers) who have prior knowledge of the Card Payments industry and are interested in integrating the Mastercard and Visa token services into their programme.

What’s Changed?

If you want to find out what's changed since the previous release, see the [Document History](#) section.

How to use this Guide

If you are new to tokenisation and want to understand how it works, see [How Tokenisation Works](#).
To find out about the steps involved in implementing a tokenisation project, see [Implementing a Tokenisation Project](#).
For Thredd token service configuration options, see [Thredd Configuration Options](#).

Note: In this guide we reference two Thredd API options available for managing your cards and tokens: the Thredd SOAP-based web services (XML format), or the REST-based Cards API (JSON format).

Related Documents

Refer to the table below for other documents which should be used in conjunction with this guide.

Document	Description
Web Services Guide	Provides details of the Thredd SOAP Web Services API.
Cards API Website	Provides details of the Thredd REST-based Cards API.
EHI Guide	Provides details of the Thredd External Host Interface (EHI).
Smart Client Guide	Describes how to use the Thredd Smart Client to manage your account.
Thredd Portal	Describes how to use the Thredd Portal, Thredd's new web application for managing your cards and transactions on the Thredd Platform.

The following documents are available from Visa and Mastercard:

Document	Description
Visa Token Service Guide	Describes the Visa token service. Available online at: Visa Token Service .



Document	Description
Mastercard Digital Enablement Service Guide	Describes the Mastercard token service. Available online at: Mastercard Developers .

Note: You may need to register with an account with Visa and Mastercard to access these sites.

Tip: For the latest technical documentation, see the [Documentation Portal](#).



1 Introduction

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) that 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 Financial PAN (FPAN).

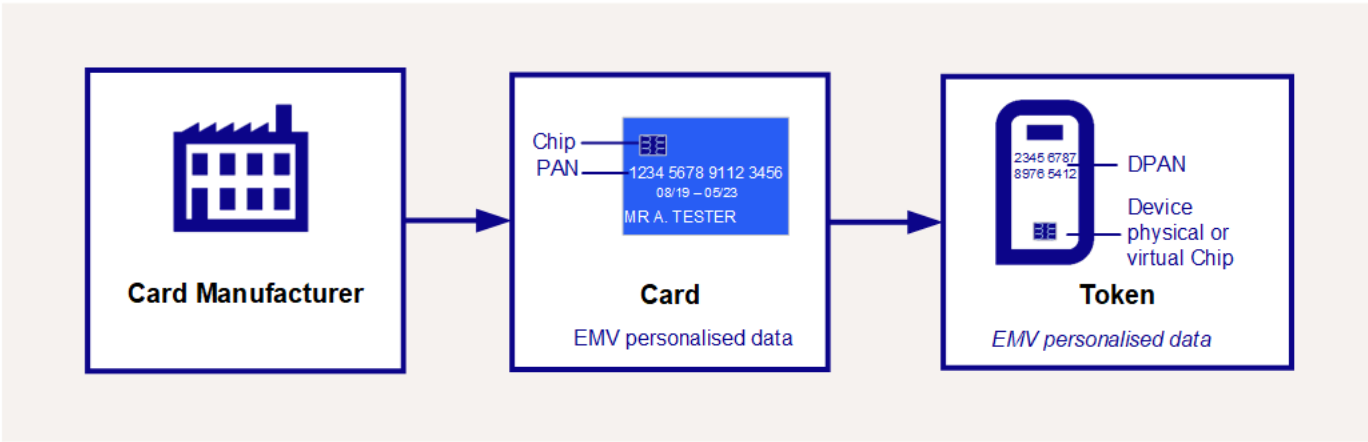


Figure 1: Tokenisation - converting a PAN to a DPAN

Tokenisation enables cardholders to access mobile wallet functionality – provided by companies such as Apple and Android – which allows payments to be made in store from a smart device such as a smartphone or tokenised device. Tokenisation also helps merchants to 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.

Tokenisation is increasing the adoption of mobile wallet and other new payment technology and improving security across the industry. Its use will continue to grow as more merchants and issuers enable the service.

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); Thredd refer to the Visa service as the Visa Digital Enablement Program (VDEP). Thredd supports both of these tokenisation services.

Note: Thredd do not share details of the FPAN or DPAN with Program Managers (Thredd clients). When a card is created on the Thredd system, we provide a unique public token that is linked to the card, and which can be used for queries and services on that card. The Thredd public token is for internal use only between Thredd and the Program Manager; it should not be confused with the payment token created during the tokenisation process described in this guide.



2 How Tokenisation Works

2.1 Who Participates in Tokenisation?

Tokenisation requires the following participants:

Cardholder

The cardholder enrolls with a mobile wallet provider or registers at an online merchant website.

Token Requestor

The token requestor initiates the request to convert your cardholder’s Permanent Account Number (PAN) into a digital token. Token requestors can be mobile wallets (such as ApplePay) or online merchants (such as Netflix). Mastercard refer to the Token Requestor as the “Wallet Provider”.

Token Service Provider (TSP)

The Token Service Provider is the party that generates the token and securely maps the PAN to a token. This is the Visa (VDEP) or Mastercard (MDES) systems that run the token service.

Issuer Host

The issuer host is Thredd, who receives the tokenisation request from Visa or Mastercard and decides on whether to approve or decline. During the implementation phase of the project, the issuer/Program Manager and Thredd work together to set up and create the token service.

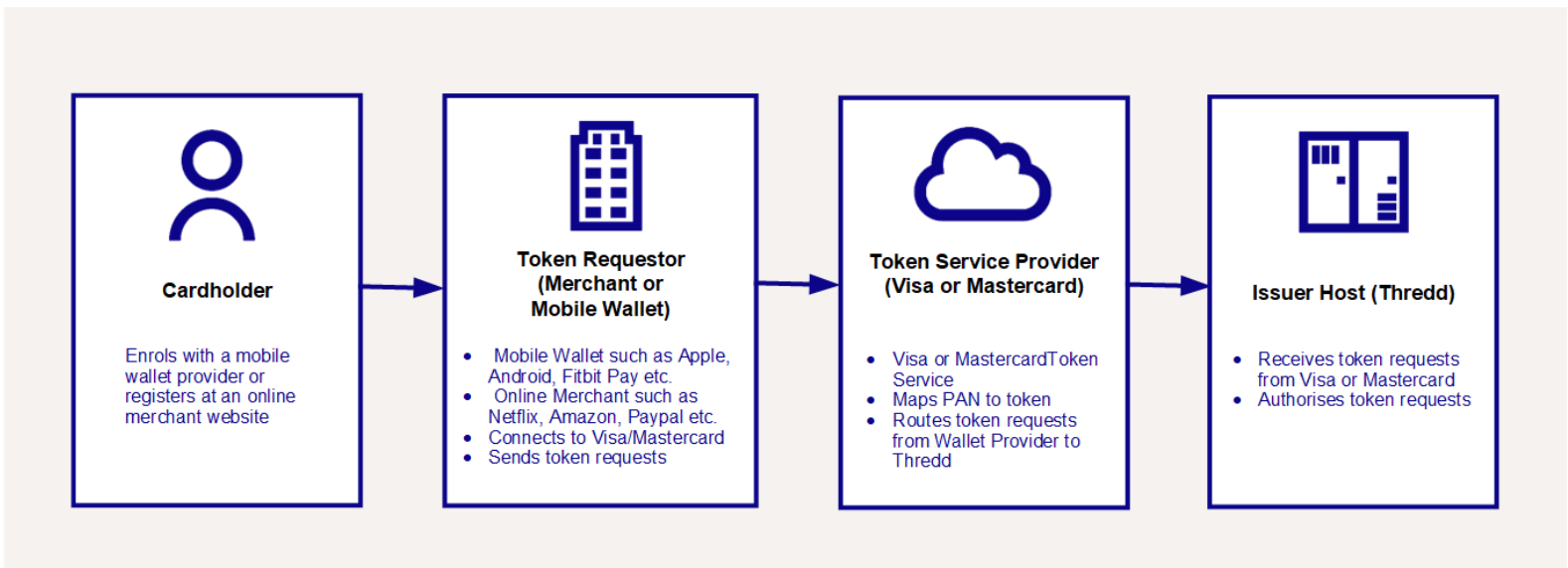


Figure 2: Participants in the Tokenisation Ecosystem

The Token Service Provider (Visa/Mastercard) receives token requests from the Token Requestor and sends them to Thredd for authorisation. There is no direct connection between Thredd and the Token Requestor during tokenisation and Thredd does not have the capability to act as a Token Requestor.

When using mobile wallet token requestors (such as Apple and Android), the Program Manager (Thredd customer) requires a separate commercial agreement with each of the three parties involved in tokenisation.

For online merchant tokenisation (i.e., for online payments), the card issuer does not need to have an existing relationship with the merchant.

2.2 Token Provisioning

Token provisioning is the act of creating and activating a digital token. The digital token is sometimes referred to as the DPAN, and is the same length as a normal 16-digit card financial PAN (FPAN).

This process must be completed first before the token can be used in transactions.

2.2.1 Token Provisioning Steps

Figure 3 provides a high-level overview of the token provisioning flow.

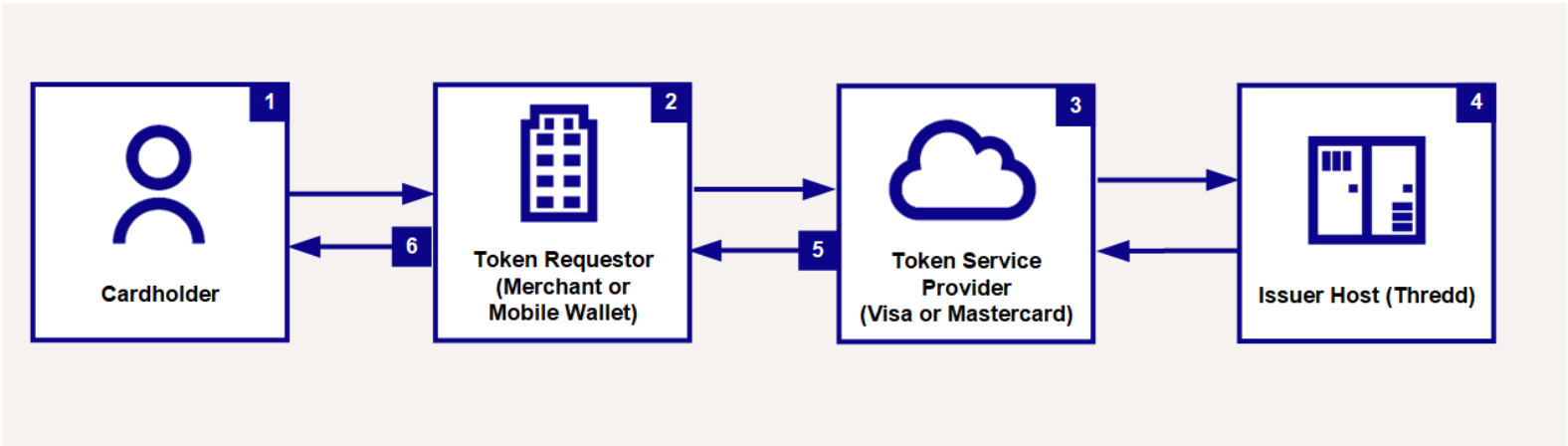


Figure 3: Token Provisioning Flow without Authentication

1. The cardholder enrolls 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.

2.2.2 Token Authorisation Options

When Thredd returns a decision on the token request there are three options:

- Approve - token is active for use
- Approve with Authentication - additional authentication is required before the approved token can be used
- Decline - token is not approved.

The Thredd response code in the response triggers three different provisioning flows:

Thredd Response	Response Code	Provisioning Flow (Token Terminology)
Approve	00	Green Flow
Approve with Authentication	85	Yellow Flow
Decline	05	Red Flow

Each of these provisioning flows is described below.

2.2.3 Approve (Green Flow)

When Thredd receives the token activation request (TAR) and we approve, if cardholder authentication is not required, Thredd sends an approve message to the token service provider to create the token without further authentication¹.

Cardholder authentication is not required in the following circumstances:

- Authentication has already been performed (i.e., token is being push-provisioned; see [Push Provisioning](#))
- For an online merchant
- Based on the configuration for your Wallet Usage Group; see [Payment Token Usage Groups](#)

¹Note that in some circumstances it possible for a Program Manager or issuer to set up rules on Mastercard or Visa to ignore or overrule the Thredd response to a TAR. Please contact the card schemes for details.



6. If the cardholder selected the SMS option and you have requested that Thredd send the message on your behalf, then Thredd sends the OTP to the cardholder via SMS.

For other cardholder verification methods or where you have opted to send the SMS, the cardholder receives the OTP from your systems³.

7. The cardholder enters the OTP on their mobile device.

8. The token service provider validates the OTP.

Figure 4 above has been simplified to show the overall process. Token provisioning with authentication requires several messages between the card schemes (networks) that are a mixture of BASE I (ISO 8583) messages (for Visa and Mastercard) and APIs (for Visa only).

2.2.5 Decline (Red Flow)

When Thredd receives the token activation request (TAR) and we decline, we send a decline message to the Token Service Provider. This ends the token flow. The token requestor must request a new token.

2.2.6 Orange Flow

Orange Flow is for token requests from Apple that indicate if the request is high risk. Apple mandate that these requests must be authenticated using secure authentication methods or be declined. The Secure authentication methods are:

- In-App authentication where the application is tenured
- A call centre where additional fraud analysis is performed

Note: Orange Flow is set up during implementation, where you select the options on the PSF. Contact Implementations to discuss the best option for you.

In the event of a provisioning request being marked as Orange Flow, Thredd will return any of the above authentication methods that you have configured on the Payment Token Usage Wallet.

Note: In-App authentication cannot be returned if the provisioning requests started as In-App push provisioning. This is an Apple rule designed to stop a fraudulent actor with access to your app using it to start the flow and then authenticate themselves through the same channel.

Customers can choose to support secure authentication methods or to decline all requests flagged as Orange Flow. Apple recommend supporting secure authentication methods, however if you are not able to do this we have kept the possibility of declining all requests (In this scenario speak to Apple about getting your use case approved).

³You must provide Thredd with the SMS text message to send to the customer. This message can contain dynamic fields. For details, check with your Implementation Manager. Thredd always sends the SMS to the phone number linked to the card on our systems (note that this may not be the same as the device which is being tokenised).



2.4 Token Requestors

The token requestor initiates the request to convert your cardholder's PAN into a token. There are two types of token requestors:

- Mobile Wallet Token Requestors - such as Apple and Android, who provide a token service via a smartphone or other mobile device that enables the cardholder to use their device for point of sale (POS) transactions
- Online Merchant Token Requestors - who tokenise a payment card for use in repeat or recurring payments on their website (such as Netflix, Domino's and PayPal). These are referred to by Card on File (COF) Token Requestors⁴.

As a Thredd customer, most of your implementation in a tokenisation service project will be focused on the Mobile Wallet Token Requestors, with whom you need to integrate directly.

You will also need to enable online merchant Token Requestors. You do not require a pre-existing relationship with the merchant. Since merchants replace the live PAN with a token, you do not need to store the PAN. The merchant sends only the token to the Token Service Provider who maps it back to the real PAN before sending to Thredd. This is done to improve card data security.

⁴Card on File (COF) is also referred to by Mastercard as MDES for Merchants.



- Authentication has already been performed (i.e., token is being push-provisioned; see [Push Provisioning](#))
- For an online merchant
- Based on the configuration for your Wallet Usage Group; see [Payment Token Usage Groups](#)

Note: Your Thredd Wallet Usage Group configuration is used to determine the appropriate flow to trigger⁶. Most Thredd Program Managers implement the approve with authentication flow.

⁶Your Wallet Usage Group can be viewed in Smart Client. If the token requestor is ApplePay, they populate the request with a score (Wallet device score and Wallet account score), which can be used to determine if further cardholder authentication is required. See [Thredd Configuration Options](#).



2.6 Token Requestors

The token requestor initiates the request to convert your cardholder's PAN into a token. There are two types of token requestors:

- Mobile Wallet Token Requestors - such as Apple and Android, who provide a token service via a smartphone or other mobile device that enables the cardholder to use their device for point of sale (POS) transactions
- 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 (e.g., such as Netflix, Domino's and PayPal). These are referred to by Card on File (COF) Token Requestors⁷.

As a Thredd customer, most of your implementation in a tokenisation service project will be focused on the Mobile Wallet Token Requestors, with whom you need to integrate directly.

You will also need to enable online merchant Token Requestors. You do not require a pre-existing relationship with the merchant. Since merchants replace the live PAN with a token, you do not need to store the PAN. The merchant sends only the token to the Token Service Provider who maps it back to the real PAN before sending to Thredd. This is done to improve card data security.

⁷Card on File (COF) is also referred to by Mastercard as MDES for Merchants.



2.7 Visa Cloud Token Framework - Online Merchant Device Binding

Note: Mandatory for Visa only. Not applicable to Mastercard.

The device binding process allows merchants to directly authenticate that the cardholder owns the device they are paying from. The Online Merchant Token Requestor creates a COF token through the standard **Token Provisioning flow**, which can then be bound to a device. During binding, the Online Merchant Token Requestor usually requires cardholder authentication, by sending an OTP to the cardholder. This cannot be done by push notification through an app (this is against the Visa rules and OTP standard). Methods such as SMS are still valid.

Note: When Thredd approves a device binding, the merchant can initiate authentication of the device at any stage. This means you may receive OTP messages (Activation Code Notifications) at any time over EHI and not just immediately following a TAR or Device Binding Request. These OTP messages must be sent to the cardholder. If configured, Thredd sends these via SMS on your behalf.

2.7.1 Binding an existing COF Token to a Device

Note that this is relevant to Visa only.

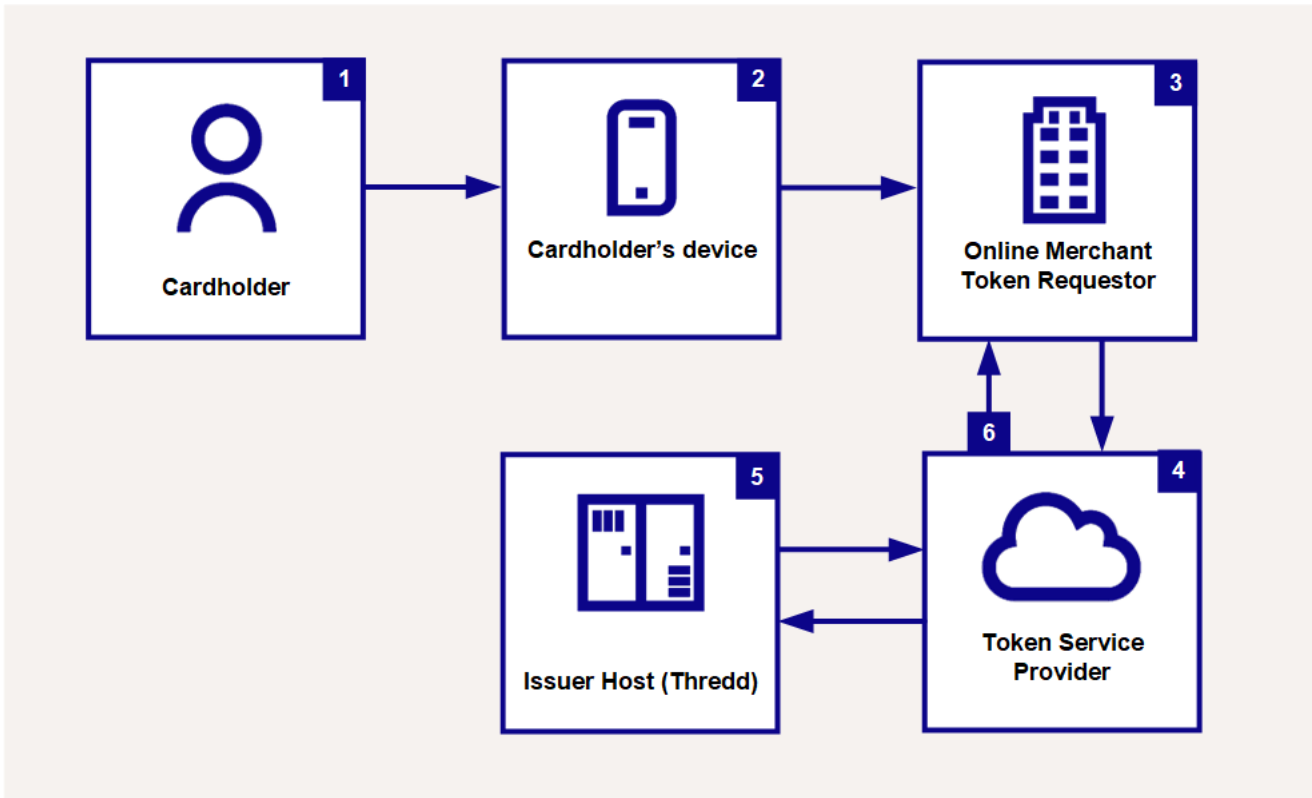


Figure 7: Device Binding Flow

1. The cardholder makes a purchase on their device.
2. The merchant identifies a new device on an existing Card on File (COF) token.
3. The merchant submits a device binding request.
4. The Token Service Provider (Visa/Mastercard) forwards the device binding request to Thredd.
5. Thredd provides a decision on the device binding request: Approve or Decline.
6. With approval, the merchant records the device binding for future purchases.



Figure 8: Authorisation Request from Mobile Device

1. The cardholder makes an in-store purchase with an NFC-enabled tokenised device.
2. The device transmits personalised data to the POS terminal using the contactless interface.
3. The POS terminal generates the authorises the request, using the stored token (DPAN) and sends, via the merchant Acquirer, to the card scheme (Visa/Mastercard)³.
4. Visa/Mastercard maps the token back to the PAN (FPAN) and sends to Thredd for authorisation.
5. Thredd approves or declines the transaction.
6. Visa/Mastercard returns the authorisation response to the merchant. If approved, the merchant provides the goods to the cardholder.

³The POS terminal treats the data received from the device in exactly the same way as data transmitted from a normal contactless card.



3.4 Making a Purchase using an Online website

For Online Merchant Token Requestors, the merchant uses the token associated with the cardholder to create and send an authorisation request. If it is the first time a card has been used with that merchant, then the tokenisation of the PAN will not have yet taken place; in this case the authorisation uses the real PAN initially and is then tokenised before storage. See *Figure 8* below.

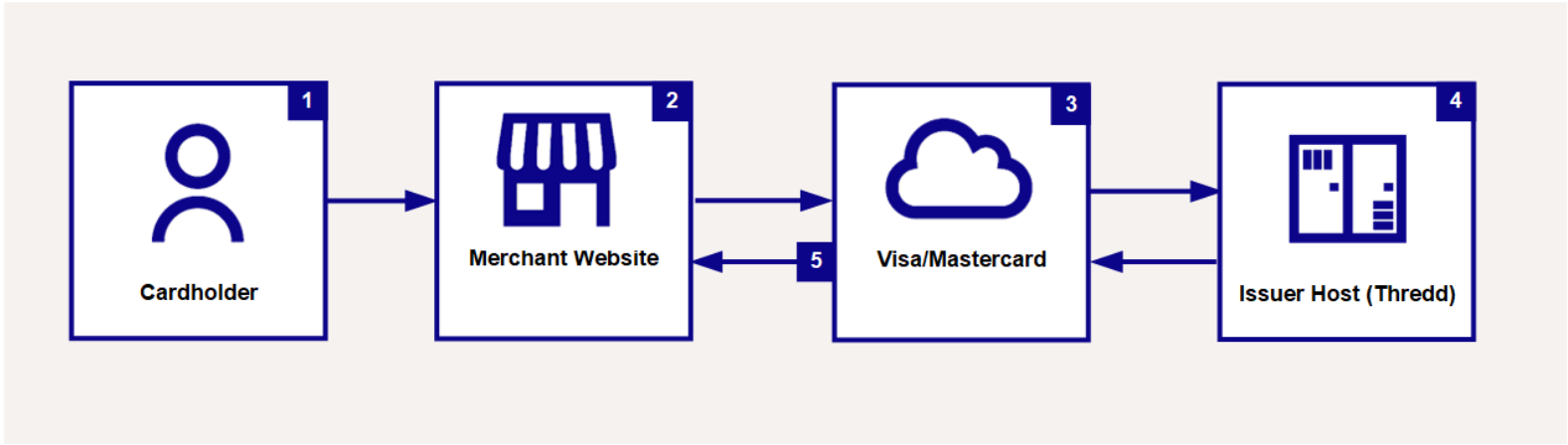


Figure 9: Authorisation Request from an Online website

1. The cardholder makes a payment on a merchant’s website.
2. The merchant’s systems generate the authorisation request using the stored token value and sends the request, via their Acquirer, to the card scheme (Visa/Mastercard).
3. Visa/Mastercard maps the stored token back to the PAN and sends to Thredd for authorisation.
4. Thredd approves or declines the transaction.
5. Visa/Mastercard returns the authorisation response to the merchant. If approved, the merchant provides the goods to the cardholder.



4.1.3 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. For details, see [Thredd Configuration Options](#).

If you want to receive tokenisation messages via the Thredd External Host Interface (EHI), in your Product Setup Form (PSF), ensure you tick the option to enable TAR transaction types. For details, see the [External Host Interface \(EHI\) Guide](#).

4.1.4 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.

Mastercard provide a Mastercard Test Facility (MTF), which can be used to test your MDES integration. MTF connects to the Thredd test environment. You can add your phone to MTF to send test tokenisation messages to Thredd. Please contact Mastercard to enable this service.

Visa provide a test service sandbox, which can be used to test outbound calls. For details, please contact Visa.

Note: Some integration work may be required on your end to integrate to the Mastercard or Visa test services. Many Thredd clients prefer to complete tests in the production environment.

4.1.5 Step 5: Complete the Wallet Provider certification process

Some Wallet providers, such as Apple Pay, have a formal certification process. Documentation for this is not available publicly, so 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.

4.2 Implementing a Customised Token Service

Testing with Visa and Mastercard is not required if you are using the out of the box tokenisation service provided by Thredd.

Note: If you require non-standard functionality, you will need to raise a separate Thredd project (development work is required). Check with your account manager for details.



Using Web Services (SOAP)	Using Cards API (REST)
• Ws_StatusChange - changes the status of a card (the FPAN status) • Ws_PaymentToken_StatusChange - changes the status of a digital payment token (the DPAN status) Note that the card status is changed in both web services using the <NewStatCode> field. For more information, see the Web Services Guide.	• Update Card Status - changes the status of a card (the FPAN status) • Update Payment Token Status - changes the status of a digital payment token (the DPAN status) For more information, see the Cards API Website.



6 Implementing In App Provisioning

The following section details how to implement our in-app provisioning. There are four different types of in-app provisioning available:

- Apple Mastercard
- Apple Visa
- Google Mastercard
- Google Visa



1. Visa sends a message to Thredd to check if the PAN is eligible for tokenisation.
Thredd returns the Profile ID (if applicable) so that the token response displays the correct card art and T&Cs on the cardholder's mobile device screen.
2. Visa sends an 0100 Token Activation Request (TAR) to Thredd.
3. Thredd returns an Approve response to Visa.
Thredd forwards the TAR to the Program Manager, via EHI.
4. Visa sends an 0620 Token Event Notification (TEN) to Thredd, to indicate the token has been created.
Thredd forwards the TEN notification to the Program Manager, via EHI.
5. For a token that is bound to a device, Visa sends an 0620 Token Event: Token Complete Notification (TCN), to indicate the token has been provisioned onto the device.
Thredd forwards the TCN notification to the Program Manager, via EHI.



```
<PaymentToken_deviceIp>192.0.0.8</PaymentToken_deviceIp>
<PaymentToken_deviceId>01234B234C1230011230054848300695D86E17C703548A4A</PaymentToken_deviceId>
<PaymentToken_deviceName>Test Apple Wa</PaymentToken_deviceName>
<PaymentToken_activationCode />
<PaymentToken_activationExpiry />
<PaymentToken_activationMethodData />
<PaymentToken_activationMethod>0</PaymentToken_activationMethod>
.....
</GetTransaction>
</s:Body>
</s:Envelope>
```




```
"TXN_Time_DE07": "0605010001",
"Txn_Type": "A",
"Additional_Data_DE48": "063T260332733260101H06115019291999808020375130103001020291710418C ",
"Authorised_by_GPS": "Y",
"CU_Group": "PMT-CU-002",
"InstCode": "PMT",
"MTID": "0100",
"ProductID": 3004,
"SubBIN": 53759000,
"TLogIDOrg": 0,
"VL_Group": "PMT-VL-020",
"Dom_Fee_Fixed": 0.0000,
"Non_Dom_Fee_Fixed": 0.0000,
"Fx_Fee_Fixed": 0.0000,
"Other_Fee_Amt": 0.0000,
"Fx_Fee_Rate": 0.0000,
"Dom_Fee_Rate": 0.0000,
"Non_Dom_Fee_Rate": 0.0000,
"Additional_Data_DE124":
"195TAD00162036556451
1
C",
"SendingAttemptCount": 0
}
```

Response

Example response from the external host system:

```
{"Acknowledgement": "1"}
```




Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
						the TCN.
5	SE or CL	360000 (TEN)	00 or 06	I	53/54/55	Last message in flow. No notification of tokenisation completion as authentication was unsuccessful.

