

Tokenisation Service Guide

Version: 1.6
03 August 2022

Global Processing Services
6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Support Email: ops24@globalprocessing.com
Support Phone: +442037409682

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

(c) 2021. Global Processing Services Ltd. 6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Publication number: TSG-1.6-8/3/2022

Copyright

(c)2021-2022. Global Processing Services All Rights Reserved.

The material contained in this guide is copyrighted and owned by Global Processing Services 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 Global Processing Services Ltd., and, then, only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, Global Processing Services 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 Global Processing Services Ltd. assumes no responsibility for any errors.

1 About this Guide

This guide describes the Mastercard and Visa token services and how GPS supports tokenisation. It explains how to set up and process tokens on the GPS 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 GPS customers who wish to add this functionality and enable token-based mobile payments for their cardholders.

Target Audience

This guide is intended for GPS 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.

1.1 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 GPS token service configuration options, see [GPS Configuration Options](#).

1.2 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 GPS Web Services API.
EHI Guide	Provides details of the GPS External Host Interface (EHI).
Smart Client Guide	Describes how to use the GPS Smart Client to manage your account.

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 .
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 [Developer Portal](#).

2 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).

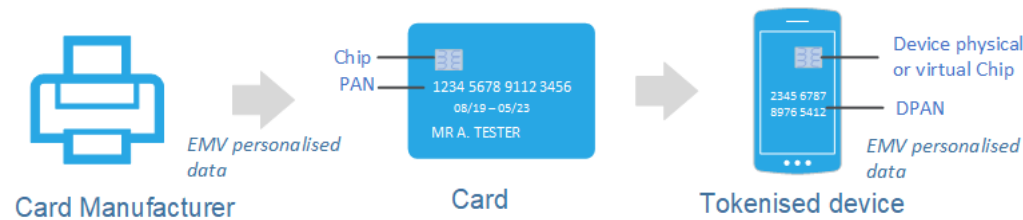


Figure 1: Tokenisation - converting a PAN to a DPAN

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

Note: GPS do not share details of the FPAN or DPAN with Program Managers (GPS clients). When a card is created on the GPS 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 GPS public token is for internal use only between GPS and the Program Manager; it should not be confused with the payment token created during the tokenisation process described in this guide.

3 How Tokenisation Works

3.1 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 GPS, 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 GPS work together to set up and create the token service.

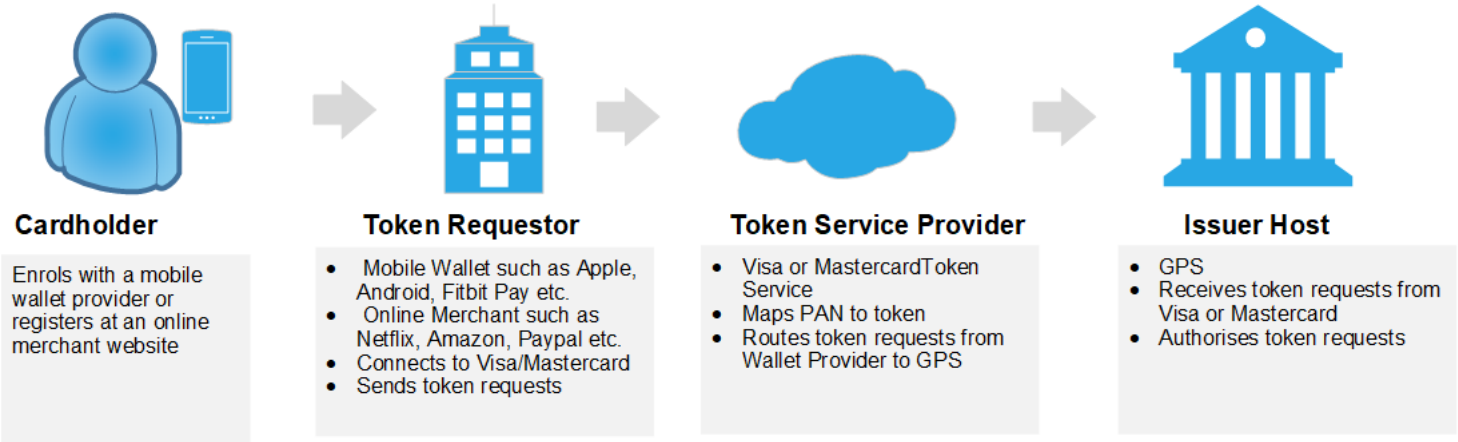


Figure 2: Participants in the Tokenisation Ecosystem

The Token Service Provider (Visa/Mastercard) receives token requests from the Token Requestor and sends them to GPS for authorisation. There is no direct connection between GPS and the Token Requestor during tokenisation and GPS 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 (GPS 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.

3.2 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.

Token Provisioning Steps

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

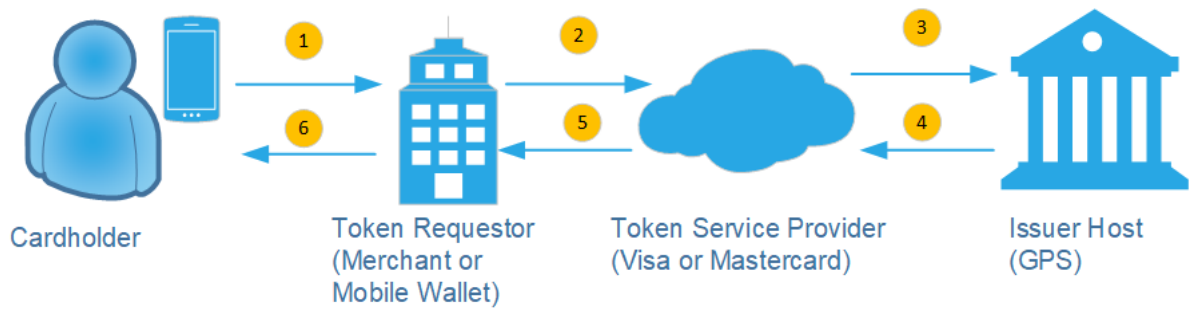


Figure 3: Token Provisioning Flow without Authentication

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 (GPS).
4. GPS decides if token activation can continue, based on the [GPS Configuration Options](#) set up for your programme. (See [Token Authorisation Options](#) below.)
5. With GPS 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.

Token Authorisation Options

When GPS 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 GPS response code in the response triggers three different provisioning flows:

GPS 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.

Approve (Green Flow)

When GPS receives the token activation request (TAR) and we approve, if cardholder authentication is not required, GPS 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](#)

Note: Your GPS Wallet Usage Group configuration is used to determine the appropriate flow to trigger². Most GPS Program Managers implement the approve with authentication flow.

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

²Your 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 [GPS Configuration Options](#).

Approve with Authentication (Yellow Flow)

When GPS receives the token activation request (TAR) and we approve, if cardholder authentication is required, we send an approve with authentication message to the token service provider to create the token with cardholder authentication.

Cardholder authentication is only needed by mobile wallet token requestors (such as Apple and Android), where the cardholder is present at the time the card is being tokenised.

To authenticate a cardholder during token provisioning, the cardholder is provided with a One-Time Password (OTP) generated by the token service provider (Visa/Mastercard). The cardholder enters the OTP value into their mobile app for validation.

The Program Manager decides what delivery options are available to the cardholder for the OTP. These options can include:

- SMS text message to mobile phone
- Push notification/in-app notification
- Email
- Call centre (an operator reads out the passcode to the cardholder to enter; the passcode is available on Smart Client, via GPS Web Services or the GPS [External Host Interface \(EHI\)](#) and will expire after a limited period, such as 2 hours).

Note: GPS currently only sends the OTP via SMS text message directly to the cardholder's mobile phone. For all other OTP methods, you will need to deliver the OTP to the cardholder. The OTP is always sent via EHI, even if GPS also sends an SMS direct to the cardholder. The OTP can be viewed in Smart Client or retrieved via Web services.

Figure 4 below describes the Approve with Authentication (Yellow) flow.

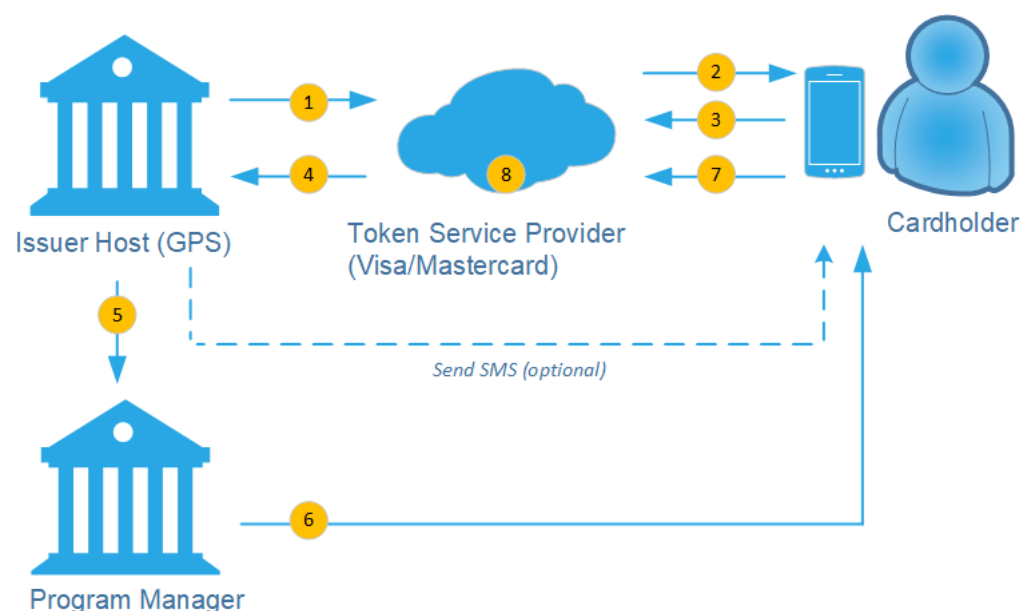


Figure 4: Cardholder Authentication During Token Provisioning

This flow commences after the token has been generated, but further user authentication is required before it can be used:

1. GPS sends an 85 (approve with authentication) response to the token service provider (Visa/Mastercard). The response contains a list of cardholder verification methods (CVMs), based on the configuration of your Wallet Usage Group for your cards.
2. The token service provider sends a list of available cardholder verification methods to the cardholder.
3. The cardholder selects one of the verification methods shown on their mobile phone wallet application.
4. The Token Service Provider receives the method selection and sends the one-time password (OTP) to GPS.
5. GPS always sends the OTP over the External Host Interface (EHI) to the Program Manager.
6. If the cardholder selected the SMS option and you have requested that GPS send the message on your behalf, then GPS 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 systems¹.
7. The cardholder enters the OTP on their mobile device.
8. The token service provider validates the OTP.

¹You must provide GPS with the SMS text message to send to the customer. This message can contain dynamic fields. For details, check with your Implementation Manager. GPS 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).

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

Decline (Red Flow)

When GPS 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.

Push Provisioning

Push provisioning (also referred to as in-app authentication) is a process where the Program Manager (i.e., your systems) pre-authenticates the cardholder before the first token provisioning message is sent to the token service provider (Visa/Mastercard). For information on the requirements for push provisioning cardholder authentication, please discuss with your mobile wallet token requestor.

Push provisioning requires you to share sensitive card data held on your system with the token service provider (without the cardholder needing to manually enter the PAN details into their mobile application). The cardholder must be logged into their account (i.e., logged in to their mobile application) in order to be able to authenticate.

To implement push provisioning, you can either do this directly with the token service provider or via a [GPS Supported Third Party for Push Provisioning](#).

Implementing Push Provisioning Directly

Note: If you are not PCI DSS Level 1 compliant, you will not be able to do push provisioning directly, as this requires obtaining sensitive card data, such as the PAN. In this case, you can use a [GPS Supported Third Party for Push Provisioning](#).

If you are managing the push provisioning process directly, some integration work with the token service provider (Visa/Mastercard) is required during the implementation phase of the project: you must exchange a pre-shared key with the token service provider; see [Exchange of Keys](#). This key is then used to encrypt the sensitive card data which is passed to the token requestor and finally for the token service provider to decrypt.

At this point the tokenisation flow will begin.

Note: The incoming token activation request (TAR) sent to GPS also confirms whether Push Provisioning has already been completed. In this case, GPS has a configurable option to return an approve or decline decision to Visa/Mastercard without requiring further authentication.

Note: It is important that this override of the authentication response is enabled for your program, otherwise GPS may respond with a request to authenticate a cardholder who has already been authenticated, which will lead to a poor customer experience and may fail Token Requestor live testing.

Using a GPS Supported Third Party for Push Provisioning

If you are not PCI DSS Level 1 compliant, you are not able to retrieve the PAN from the GPS platform to create your own encrypted payload for push provisioning. In this case, GPS provides an integrated solution through one of our supported third-party service providers who can do this on your behalf.

This integration enables your Push Provisioning service provider to retrieve the PAN and other relevant card data directly from the GPS platform. They then encrypt the card data and sends the encrypted payload to your cardholder's mobile phone application to pass to the token requestor and then to the token service provider (Visa/Mastercard).

During the project implementation phase, pre-shared keys are exchanged between your third-party Push Provisioning service provider and the token service provider, allowing them to encrypt and token service provider to decrypt the card data. The Program Manager and token requestor do not have access to the keys.

GPS supported third-party Push Provisioning providers include:

- MeaWallet - provide a software development kit (SDK) to support their MDES/VDEP push-provisioning solution. For details, see the [MeaWallet website](#).
- Digiseq - provide an MDES Push Provisioning service to clients who are not PCI compliant. For more information about Digiseq, see the [Digiseq website](#).

Push Provisioning through a supported Third-Party Provider

Figure 5 below describes the push provisioning process with one of GPS's supported third party service providers.

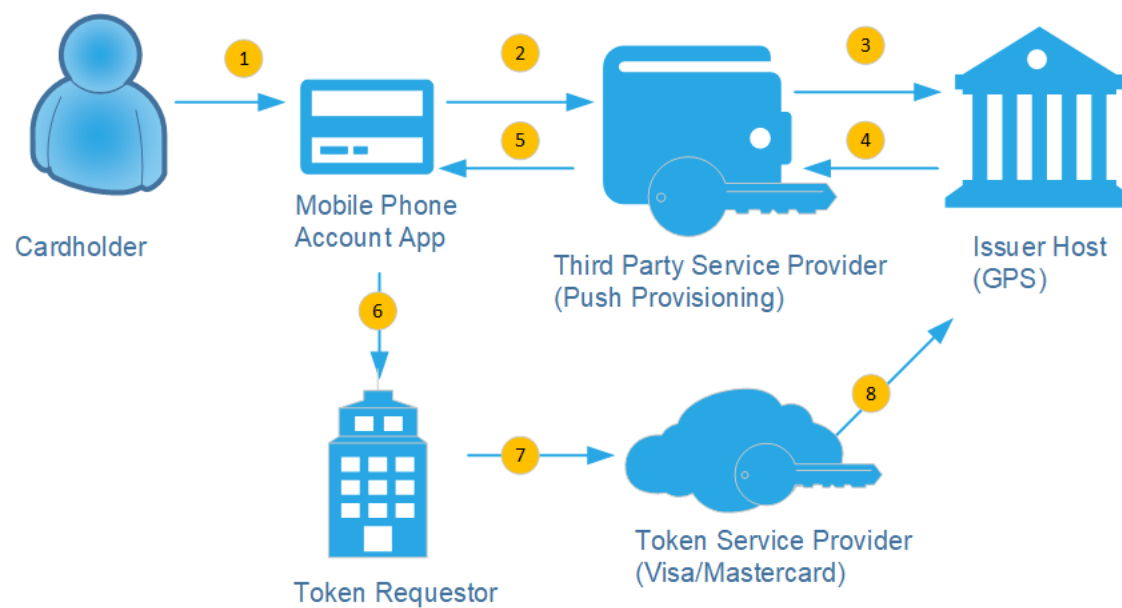


Figure 5: Third Party integration for Push Provisioning

1. The cardholder confirms the card to be added to their mobile phone application for your service.
2. Your mobile phone app requests encrypted card data for push provisioning from your third-party service provider.
3. Your third-party service provider requests the card data (PAN, expiry, CVV2) from GPS.
4. GPS returns the card data to the third-party service provider.
5. The third-party service provider encrypts the data and returns it to the mobile phone app.
6. The encrypted data is passed to the token requestor (e.g., Apple and Android).
7. The token requestor sends the encrypted data to the token service provider.
8. The token service provider decrypts the card data and starts the [token provisioning flow](#).

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 Requestors¹.

As a GPS 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 GPS. This is done to improve card data security.

¹Card on File (COF) is also referred to by Mastercard as MDES for Merchants.

Visa Cloud Token Framework - Online Merchant Device Binding

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

In October 2020, Visa launched the Visa Cloud Token Framework (CTF). This product is a precursor to supporting the EMVCo Secure Remote Commerce (SRC) functionality¹. SRC aims to introduce a common e-checkout experience that cardholders will trust, called Click to Pay.

CTF allows online Merchant Token Requestors to bind their previously created Card On File (COF) tokens with devices which they can authenticate belongs to their customer. The device binding process allows merchants to directly authenticate that the cardholder owns the device they are paying from.

How does it work?

The Online Merchant Token Requestors creates a COF token through the standard [Token Provisioning flow](#) (Green flow, without Authentication).

The token can then be bound to a device. During binding, the Online Merchant Token Requestors 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: Once GPS approves a device binding (Green flow, without Authentication), 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, GPS sends these via SMS on your behalf.

Binding an existing COF Token to a Device

Note that this is relevant to Visa only.

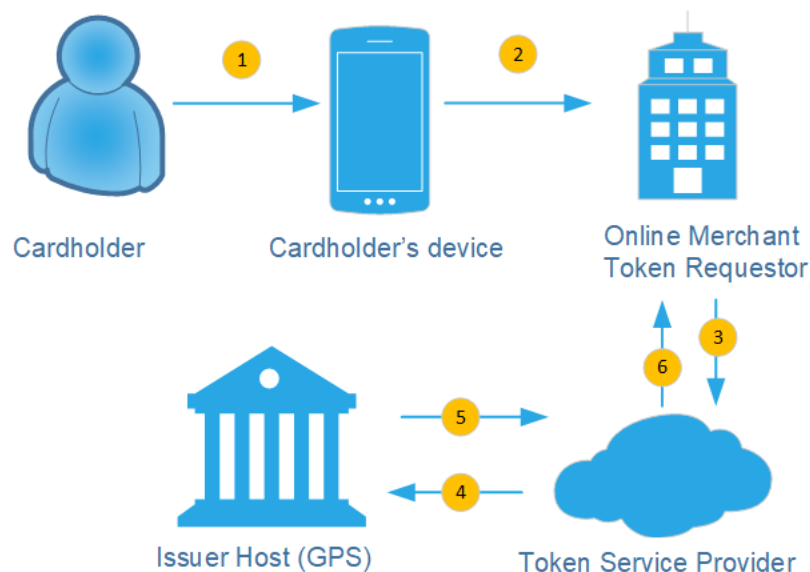


Figure 6: Device Binding Flow

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 GPS.
5. GPS provides a decision on the device binding request: Approve or Decline.
6. With approval, the merchant records the device binding for future purchases.

¹Precursor to Visa Secure EMVCo data.

4 Transactions on a 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. Some of this data needs to be gathered and reported to token requestors such as Apple or Android.

Personalisation on a Device

Tokenisation of devices such as mobile phones and smart watches allows them to be used in the same way as physical cards. During tokenisation the mobile device is personalised. This is the process in which the device is marked with private data specific to that token and device. Personalisation is the same process as used on a physical card when chip data is added to the card prior to issuance.

Personalisation can either be done on the device or SIM card (known as Secure Element tokenisation) or in the cloud using Host Card Emulation (HCE).

- Apple Pay, which has access and control of the device and has pre-installed EMV chips that can be personalised, uses Secure Element (SE)
- Android, which is an operating system installed on various devices owned by other companies, uses HCE¹.

Other Mobile Wallet token requestors vary between SE and HCE and it is their decision which option is implemented. GPS can support both SE and HCE mobile wallet token requestors.

The data from the personalised device is transmitted to the Point of Sale (POS) terminal during an in-store transaction. The POS terminal then formats this into an authorisation request, which does not contain the real PAN, but uses the device token. This authorisation request is sent to Visa/Mastercard who maps the token back to the PAN before sending on to GPS.

Visa/Mastercard Stand-In Processing

When setting up your programme configuration options on Visa or Mastercard, you must specify that they do not authorise Tokenisation Approval Requests (TARs) on behalf of GPS. A TAR must always be generated by the token service provider and approved by GPS². GPS declines transactions on tokens that do not exist on the GPS platform.

Making a Purchase using a Tokenised Device

Figure 7 below shows the flow for a tokenised device:

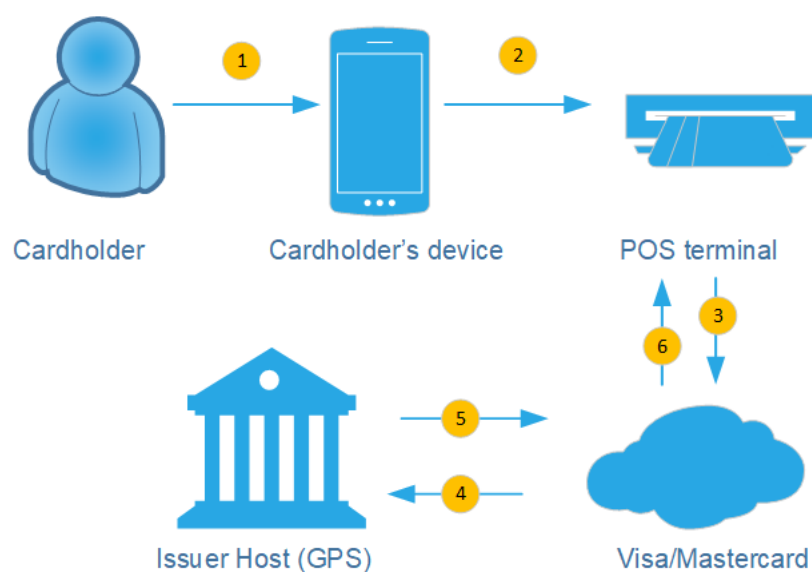


Figure 7: Authorisation Request from Mobile Device

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.

¹An EMV program on the Android device manages transactions and communicates with a secure cloud host card emulator, where the keys for use for a transaction are generated.

²In scenarios where Visa/Mastercard can do Stand-In processing (STIP), they must not have any settings for your programme that pre-approves a tokenisation approval request (TAR); this must always be generated by the Token Requestor. If GPS does not receive the TAR, we will decline transactions on the token.

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)¹.
4. Visa/Mastercard maps the token back to the PAN (FPAN) and sends to GPS for authorisation.
5. GPS 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.

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.

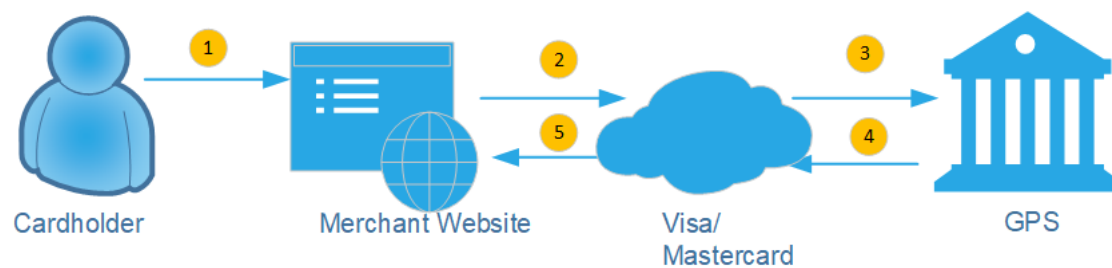


Figure 8: Authorisation Request from an Online website

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 GPS for authorisation.
4. GPS 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.

¹The POS terminal treats the data received from the device in exactly the same way as data transmitted from a normal contactless card.

5 Implementing a Tokenisation Project

5.1 Steps in Enabling the Tokenisation Service

This section provides an indicative guide to the steps that you need to complete to enable the tokenisation service:

1. Sign up for the service
2. Complete requested forms
3. Configure your GPS settings
4. Complete testing
5. Complete the Wallet Provider certification process

Step 1: Sign up for the Service

To enable the tokenisation service, you need to sign up with each of the following participants in the tokenisation flow:

- The Token Service Provider (Visa or Mastercard); for details, see the links below:
 - Visa Token Service: [Visa.co.uk: Visa Token Service](https://usa.visa.com/merchants/tokenization)
 - Mastercard Digital Enablement Service: [Mastercard.ie: Digital Commerce-solutions](https://www.mastercard.co.uk/digital-commerce)
- The Mobile Wallet Token Requestor(s) of your choice (e.g., Apple, Android, Fitbit, Samsung). for details, see the links below:
 - Apple Pay: developer.apple.com and [Apple Pay implementation](https://developer.apple.com/documentation/apple_pay_on_the_web)
 - Google Pay: pay.google.com
 - Samsung Pay: [samsung.com: Samsung Pay](https://samsung.com)
- The Issuer Host (GPS). Contact your GPS Account Manager

You do not require a project or any pre-existing relationship with any Online Merchant Token Requestor (such as Netflix, PayPal, Amazon). As new Online Merchant Token Requestors are added to Visa/Mastercard, GPS will continue to add these new merchants without further input from you to ensure you remain compliant.

Note: GPS receives around 100-200 new Token Requestor updates a month from Visa. Mastercard add them to their generic MDES for merchant 3-digit token requestor code, so we do not need to update.

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 GPS input as they relate directly to the functionality on the GPS platform. For details, check with your implementation Manager.

Note: Please ensure GPS are involved in helping you complete the documents listed below.

Examples of Visa documents:

- Visa Token Service Program Information Form (PIF)
- Visa Token Service Customer Information Questionnaire (CIQ)

Examples of Mastercard documents:

- MasterCard BPMS guide (Parameter Worksheet)

Wallet provider documents:

- Complete the relevant wallet provider agreements and configuration forms. GPS does not need to be involved in this process.

Step 3: Configure your GPS settings

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

You must complete the GPS Digital Wallet Product Set Up Form (PSF) to confirm your tokenisation service configuration options. For details, see [GPS Configuration Options](#).

If you want to receive tokenisation messages via the GPS 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](#).

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 GPS test environment. You can add your phone to MTF to send test tokenisation messages to GPS. 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 GPS clients prefer to complete tests in the production environment.

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 GPS 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.

5.2 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 GPS.

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

6 Tokenisation Configuration

This section provides details of the GPS configuration options related to the tokenisation service.

6.1 Card Usage Groups

If you are supporting tokenisation on your physical and virtual cards, please ensure that **Card Not Present (Manual Key Entry)** is enabled on your Card Usage Groups to allow your cards to be tokenised. You can specify this on the GPS Product Setup Form (PSF). See the example below.

Card Usage Group Name:		Virtual	GPS Code:		
Allow? Y/N	Card Acceptance Method (A)	Allow? Y/N	Transaction Type (T)	Allow? Y/N	Verification Checks (V)
No	Unknown Acceptance Method	No	Purchase With Cashback (DE=09)		Bypass Online PIN Check
Yes	Card Not Present (E-commerce)	No	Cash Advance (DE=17)		Bypass Expiry Date Check
Yes	Card Not Present (Phone/Mail/Order)	No	Cash at ATM (DE=01)		Bypass CVV2/CVC2 Check
Yes	Card Not Present (Recurring)	No	PIN Change ATM (DE=92 (M), 70(V))		Blank CVV2 in Card not Present E-commerce
Yes	Card Not Present (Manual Key Entry)	No	Balance Enquiry at ATM (DE=30)		Blank CVV2 in Card not Present Phone/Mail Order
No	Mag Stripe transaction at Chip capable Terminal (Technical Fall Back)	No	PIN Unblock via ATM (DE=91 (M), 72(V))		Blank CVV2 in Card not Present Recurring
No	Mag stripe PAN entry - Common	Yes	Credits - Refunds (DE=20)		Blank CVV2 in Card not Present Manual Key Entry
No	Chip PAN Entry - Offline PIN verification	Yes	Purchase of Goods & Services (DE=00)		Allow Blank DE014
No	Chip PAN Entry - Online PIN verification	No	Visa Quasi- Cash (POS) transactions (DE=11)		Expiry date optional for Recurring Payments
No	Chip PAN Entry - Signature verification	Yes	Credits Auth (DE=28)		
No	Chip PAN Entry - No Verification	No	Original Credits (DE=26)		
No	Cash to be withdrawn outside of country of issue	No	Account Funding transaction (AFT) (DE=10)		
No	Cash to be withdrawn in currency other than card billing currency				
No	POS usage outside country of issue of a card				
No	POS usage in currency other than card billing currency				
No	Contactless EMV				
No	Manual Keyed Transaction at Chip capable Terminal				
No	Cardholder NOT present -Manual Key Entry				
No	Contactless MagStripe				
No	Card Not Present (Credential on File)				
No	Chip PAN Entry - no CVM Required				

Please note that all magnetic stripe ATM transactions are blocked by default. If you require this functionality enabled for your product then GPS require explicit issuer sign-off.

Allow? Y/N	Misc (M)
	If declined, force next EMV transaction online
	If Zero or negative balance, force next EMV transaction online
	Force next EMV transaction online
	Reset EMV counters to upper offline limits
	Transaction Alerts enabled
	Instant funding
	Override to allow International e-commerce

Figure 9: Card Usage Groups on the PSF

6.2 Payment Token Usage Groups

To configure your tokenisation usage groups, you need to fill in the Digital Wallet Product Set Up Form (PSF) and return to your Implementation Manager. The key configuration options, specific to the provisioning of a payment token, are found under two groups:

- Payment Token Usage Group: these are your default settings for all Token Requestors
- Payment Token Usage Wallet Groups: these are settings for specific Token Requestors (e.g., for Android and Apple)

To enable the payment token service, you will need at least one payment token usage group, which is set as the default group at a product level. See the example below.

Payment Token Usage					
Token Usage ID		added by GPS		*Please note GPS can only send SMS, all other options are to be managed by the PM.	
Token Usage Name		Select from drop down		Select Y/N	
Institution		Test Financial Services		Activate: Call Centre Tel Number	
Group Usage		Select from drop down		Activate: Mobile App Ref	
CVV2 Missing		Default = A		Activate: Auto Call Centre Tel Num	
AVS Missing		Default = A		Activate: Website URL	
Key:		Wallet Scores :		Activate: Email	
0 = Approve		5= Best		Activate: SMS	
A = Approve-with-Authentication		3 = Neutral		Activate: CallBack	
1 = Decline		1 = Worst		Notify: SMS	
Min. Tokens to Auth (min 1)		2		Notify: Email	
Min. Tokens to Decline (max 10)		10		Notify: POST	
				Override-with-auth to Approve for in-app provisioning	
				Default Wallet Provider Authentication	

Figure 10: Payment Token Usage Group

You then need to set up a payment token usage wallet group for each Token Requestor. See the example in [Figure 11](#) below. Note that all COF Token Requestors are grouped into one payment token usage wallet group for ease of configuration.

Payment Token Usage Wallet

Copy and paste this section for each Wallet Provider (e.g. Apple, Android, Samsung, etc.)

If a field is left blank the setting in Payment Token Usage setting will be used

Select from drop down

Select Y/N

*Please note GPS can only send SMS, all other options are to be managed by the PM.

Payment Token Usage	Test MDES	Wallet Device Score Default	Default = 3	Override Activation and Notification Settings	No
Token Usage Wallet	Apple	Wallet Account Score Default	Default = 3	Complete the below ONLY if YES selected above	
If OWN wallet enter name:		Wallet Decision Auth	Default = A	Activate: Call Centre Tel Number	No
Artwork		Wallet Device Decline	Default = A	Activate: Mobile App Ref	No
Dynamic	No	Select from drop down		Activate: Auto Call Centre Tel Num	No
Default Decision	Default = A	Wallet Device Max Score Auth	Default = 3	Activate: Website URL	No
CVV2 Missing	Default = A	Wallet Device Max Score Decline	Default = 1	Activate: Email	
AVS Missing	Default = A	Wallet Account Max Score Auth	Default = 3	Activate: SMS	Yes
Key:		Wallet Account Max Score Decline	Default = 1	Activate: CallBack	Yes
0 = Approve				Notify: SMS	Yes
A = Approve-with-Authentication				Notify: Email	
1 = Decline				Notify: POST	No
Unset = Do Not Override				Override-with-auth to Approve for in-app provisioning	override enabled
				Default Wallet Provider Authentication	Do not Apply PSD SCA Counters to DPAN

Figure 11: Payment Token Wallet Usage Group

For details of the fields in the Digital Wallet Product Set Up Form, see [GPS Configuration Options](#).

6.3 GPS Configuration Options

The following table describes the available tokenisation service configuration options. Settings in the Payment Token Usage Group apply as a default setting for all Token Requestors. Settings in the Payment Token Wallet Usage Groups apply to individual Token Requestors and override the default settings.

Note: Online Merchant Token Requestors are provided as a single group (called MRCHTOKEN), so you cannot set different token logic for individual online merchant token requestors.¹

Parameter	Function	Suggestions
General Options		
Group Usage	The default usage group that should be assigned to the wallet. (set at Payment Token Usage Group level)	If you want any different functionality for transactions on payment tokens than your existing physical or virtual cards, then specify a different usage group here to be used just for tokens. (For example, to prevent payment tokens to be used for ATMs with NFC enabled, or tokens to be used overseas.)
Artwork	The reference that GPS should return to Visa/Mastercard for T&Cs and card art.	For Static card art: Leave blank (for Visa) or add a Mastercard reference. For Dynamic card art: Leave blank.
Dynamic	Whether the artwork is dynamic For details, see Dynamic vs. Static Card Art	If dynamic, select Yes. When you send GPS a create card request (using the Ws_CreateCard web service) GPS will pass the contents of the ProductRef field to Visa/Mastercard.
Options for responding to a TAR request		
Default Decision	The default response that GPS should provide when a TAR arrives.	Set to approve if you have scenarios where you want to approve a TAR without authentication. ² If you always want to authenticate the cardholder then set to authen-

¹MRCHTOKEN is also referred to as M4M (by Mastercard) and Card on File (by Visa).

²Not applicable for Push Provisioning. Please see the setting for “Override approve-with-auth to Approve for inapp provisioning” for further information on how to correctly set up push provisioning for Wallet Provider testing

Parameter	Function	Suggestions
		ticate. Set to decline if you are setting up a decline-only group. These groups are used to prevent individual cardholders from using the token service.
CVV2 Missing	The response code that GPS should return if the CVV2 is missing from the TAR.	For Mobile Wallet tokenisation, set to approve or authenticate depending on your risk appetite. For the MRCHTOKEN wallet provider, this should be set to approve. Online merchant token activation requests must not decline for missing CVV2.
AVS Missing	The response code that GPS returns if address data is missing from the TAR.	For Online Merchant tokenisation, this should be set to approve. For Mobile Wallet tokenisation, set to approve or authenticate depending on your risk appetite.
Wallet Decision Auth	The action GPS should take if the incoming TAR from the token requestor recommends authenticate cardholder.	Set to approve or authenticate depending on your risk appetite.
Wallet Decision Decline	The action GPS should take if the incoming TAR from the token requestor recommends decline.	Set to Approve, Authenticate or Decline depending on your risk appetite and the cardholder journey requirements.
Wallet and Device Scoring		
Wallet Device Score Default	The default score that GPS should assign if there is no device score on the incoming TAR.	These scores are often missing (since many Token requestors do not provide a score). The default is 3, but you can set a higher or lower threshold, depending on your risk appetite. See Wallet Device and Account Scoring.
Wallet Account Score Default	The default score that GPS should assign if there is no account score on the incoming TAR.	These scores are often missing if the Token requestor is not Apple. The default is 3, but you can set a higher or lower threshold, depending on your risk appetite.
Wallet Device Score Max Auth	The maximum device score required to trigger the Authenticate flow. Device scores are between 1 and 5.	The default is 3, but you can set a higher or lower threshold, depending on your risk appetite. See Wallet Device and Account Scoring .
Wallet Device Score Max Decline	The maximum device score required to trigger a Decline. Device scores are between 1 and 5.	Default is set to 1. Note that during internal pilots if you are adding and removing cards multiple times from Apple, the score may get low enough to cause declines.
Wallet Account Score Max Auth	The maximum wallet score to trigger the Authenticate flow. Wallet scores are between 1 and 5.	Usually set to 3 but you can set higher or lower threshold depending on your risk appetite.
Wallet account Score Max Decline	The maximum device score to trigger a Decline. Device scores are between 1 and 5.	Usually set to 1. However, during internal pilots if you are adding and removing cards multiple times from Apple the score may get low enough to cause declines.
Token frequency and overrides		
Min. Tokens to Auth	The number of tokens permitted before GPS requests authentication. (set at Payment Token Usage Group level)	The number of existing tokens is specified in the incoming TAR request from the Token Service Provider.
Min. Tokens to Decline	The number of tokens permitted before GPS declines further requests. (set at Payment Token Usage Group level only)	The number of existing tokens is specified in the incoming TAR request from the Token Service Provider.
Override-with-auth to Approve for in-app provisioning	GPS can identify TARs where push provisioning has been used. In these requests the cardholder has already been authenticated so this option allows you to prevent a request for further authentication to be sent.	Always set Override Enabled for a better customer journey. If it is not enabled the cardholders will often need to authenticate twice. The override is required to pass Apple testing.
Default Wallet Provider Authentication	This relates to authentication on the payment token/DPAN. PSD2 requires cardholder authentication when: - The transaction amount is over 50 EUR * - The cumulative non-SCA value exceeds 150 EUR*	Options include: - Authenticated - the payment token/wallet always does implicit cardholder authentication for each transaction performed on it. - Not authenticated - no implicit cardholder authentication happens for transactions. (If PSD2 is enabled, then GPS will track both contactless and e-commerce counters, and will request SCA if

Parameter	Function	Suggestions
	More than five consecutive non-SCA transactions have been processed * The amount/value is configurable per client and currency Note: The Wallet provider should always handle the authentication and update the counters.	these limits are exceeded.) (This option can be set for an online merchant.) Do not apply PSD counters - the payment token/wallet does the PSD2 checking, and GPS should not do any PSD2 checking for transactions. (This option should always be set for Mastercard. It is also recommended for Visa.)¹ Note: PSD2 counters for physical cards is not affected by this setting. SCA counters for physical cards are a separate configuration parameter.
Options for cardholder authentication and token activation		
Override Activation and Notification Settings	Whether to override the Payment Token Usage Group settings	Select Yes if you want different settings specific to your Payment Token Usage Wallet Group. If you select No, then leave the Activate and Notify options blank.
Activate: Call Centre Tel Number	The number to call if you want cardholders to be able to telephone a call centre to activate their payment token.	Leave blank for no call centre, otherwise enter the phone number that GPS should return to the token service provider. If you need different call centre numbers for different groups of cardholders, please set up a Payment Token Usage group for each number. Note: Your call centre staff can view the One-time passcode (OTP) required for activation in Smart Client. The OTP is also available via EHI or web services.
Activate: Mobile App Reference	The reference GPS should send to the cardholder if you want cardholders to be able to activate their payment token in the app.	Leave blank for no mobile app, otherwise enter the reference that GPS should return to the token service provider.
Activate: Website URL	URL cardholders use to retrieve an OTP.	Enter the website URL you want cardholders to go to for their OTP.
Activate Email	Whether to activate email as an OTP delivery option	This option is required if you want email to be returned to the cardholder as an option for authentication; note that GPS will not send the email directly to the cardholder and your systems will need to implement this: you can retrieve the OTP from EHI and handle with your own messaging and branding. If you are interested in GPS sending emails directly, please raise with your Account Manager.
Activate SMS	Whether to activate SMS as an OTP delivery option.	If you want to send your own SMS, then enable this parameter, but do not configure a message.
Activate Call-back	Whether to activate call-back as an OTP delivery option	GPS does not handle call-backs directly with a cardholder. If you want to provide this option, then your systems will need to retrieve the OTP from EHI and call your cardholder directly.
Token complete notification options		
Notify SMS	Whether you want GPS to confirm via SMS to a cardholder that tokenisation is complete	Enable if required.
Notify Email	Reserved for future use	-
Notify Post	Reserved for future use	-

Note: For GPS to return an Approve response code for a TAR (Green flow), all checks based on configuration and card must be approved. If only one check returns an authentication decision, then GPS will request authentication (yellow flow)²; if only one check triggers a decline then GPS will decline (red flow).

¹For Mastercard, GPS do not receive the full authentication data to support this option. We also highly recommend you do not enable for Visa as this may lead to a poor customer journey (where the token is declined and the terminal prompts to insert a card).

²Excludes authentication for push-provisioned token requests, which only allow approve or decline responses.

Visa/Mastercard Rules

Visa/Mastercard have additional requirements when configuring your Online Merchant token activation service. See the table below.

Requirement	What configuration options to select?
Online Merchant token activation requests should not require user authentication.	Set payment token wallet groups to approve for Online Merchant Token Requestors. See GPS Configuration Options .
Do not enable Notifications for Online Merchant token provisioning	Create a separate payment token wallet group for the MRCHTOKEN Wallet provider, then ensure that the Notify SMS, Notify Email and Notify Post fields are disabled. See GPS Configuration Options . Note: You must not send any text messages or any notifications to your cardholders for Online Merchant token provisioning. This should not be visible to the cardholder.
Visa Only	
Online merchant authentication options must not include a reference to a mobile app.	Ensure the field Activate: Mobile App Ref is left blank for the Online Merchant Payment Token Usage Group.
Mastercard Only	
Do not enable Mastercard automatic approval with authentication.	This is a setting for your program on the Mastercard Portal. You should disable the configuration option that enables Mastercard to override a GPS approve response with an approval with authentication.

Enabling Different Configuration Options per Card

GPS provide the option to create multiple [Payment Token Usage Wallet Groups](#) and have different authentication options at a card level for different cards or card products. The GPS Implementation Team set up these usage groups.

Below are some examples of why multiple Payment Token Wallet Usage Groups are used:

- To prevent individual cards from being tokenised, you can set up a “decline only” group (often done for fraud purposes).
- To set up different notification options such as different call centre numbers or to exclude SMS options from some clients.
- To set up different usage roles for tokenised cards, for example exclude MOTO payments or magnetic stripe card payments.
- To have different limits on the numbers of tokens that can be created before authentication and/or decline responses are sent.

How to change a card's usage group

All token service products have a default Payment Token Usage Group. To change a card's usage group using the web services API:

- When creating the card, use the [Ws_CreateCard](#) or when changing a card's usage group at a later time, use the [Ws_Change_Groups](#) web service.
- Enter the unique identifier into the `<PaymentTokenUsageGroup>` field.

For more information, see the Web Services Guide.

It is also possible to change a card's usage group via Smart Client. For more information, see the Smart Client Guide.

Dynamic vs. Static Card Art

There are two options to configure the card art that is displayed to the cardholder at the time of tokenisation:

- Static - the same artwork for the whole account range.
- Dynamic - artwork can vary at card level.

Configuration of artwork differs slightly between Visa and Mastercard.

Visa Configuration

You will need to configure your static card art per account range on the Visa Cardholder Metadata Manager (VCMM) online portal.

- To configure dynamic artwork, you must upload your card art options to VCMM against a **ProfileID**. The **ProfileID** is always 32 characters long.
- When you create a card using the GPS **Ws_CreateCard** web service, you must enter this Profile ID into the **ProductRef** field.

Mastercard Configuration

Upload your artwork to the Mastercard Portal. Use the same product reference for your artwork as is used by your Card Manufacturer.

For static artwork, GPS take the reference from your payment token wallet usage group. For dynamic artwork, GPS take the reference from the **ProductRef** field.

Note: the card art reference (**ProductRef** field) should be the same for both Visa/Mastercard and your Card Manufacturer.

Wallet Device and Account Scores

These scores are returned from Mobile Wallet Token Requestors such as Apple Pay, to reflect how trustworthy they consider the account and device. Scores are between 1-5. The higher the score, the more reliable the account or device is considered to be. 1 = least trusted, and 5 = most trustworthy.

You can use this score to determine how you want GPS to respond to the Token Activation Request (TAR).

Example GPS Settings

What is the maximum number which triggers approve with authentication (yellow flow)?

Wallet Device Score Max Auth = 3

What is the maximum number which triggers a decline (red flow)?

Wallet Device Score Max Decline = 1

If a device score of 4 is received, then GPS approves. If a device score of 3 is received, then GPS approves with authentication. If a device score of 1 is received, then GPS declines.

Default Device and Account Scores

Some wallet providers do not return any device or account scores. In this case, you can configure GPS to assign a default score that can be used in the Token Activation Request to determine how you want GPS to respond to the Token Activation Request.

Device Binding Logic

[Device binding requests](#) use the same authorisation logic as your Online Merchant token requestor. Currently, GPS device binding requests use the same authorisation logic as the Online Merchant token activation requests. If you want different authorisation logic between Online Merchant Token requests and Device Binding Requests, please raise with your Account Manager.

DPAN over FPAN Status

DPAN over FPAN status is an optional setting that specifies how GPS should treat the Digital PAN (DPAN) and Financial PAN (FPAN) statuses during DPAN transactions:

- If DPAN over FPAN status is ENABLED - GPS will check the DPAN status during a token transaction and disregard the underlying FPAN status
- If DPAN over FPAN status is DISABLED - GPS will check BOTH the FPAN and DPAN statuses during token transactions

The default setting is disabled. To enable this setting, please raise a change request or speak to your GPS Implementation Manager.

Note: We recommend that DPAN over FPAN status should not be enabled for Card on File token requestors. This should only be used for device-based tokens through wallet providers such as Apple and Android.

Changing the FPAN and DPAN status

You can use the following web services to change the status of your cards:

- **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](#).

Impact on token transactions

If the DPAN over FPAN setting is enabled, then you must separately set the statuses of both the FPAN and DPAN, using the Ws_StatusChange and [Ws_PaymentToken_StatusChange](#) web services.

If the DPAN over FPAN setting is disabled, then the DPAN status set using the Ws_Payment_Token_StatusChange web service can be overridden in an authorisation by the FPAN status that is set using the Ws_StatusChange web service.

This feature enables you to use a single web service, Ws_StatusChange, to set the statuses of both the FPAN and DPAN.

Note: Do not use status code 41 if temporarily blocking a DPAN, since the Card Schemes treat this as a permanent status. We recommend you use status code G1 instead, as this status is reversible.

6.4 Exchange of Keys

Visa Keys

The following keys are exchanged between Visa and GPS as part of the Visa Token service project. A set of Visa keys are unique per Bank Identification Number (BIN).

- Master Derivation Key (MDK) - used to validate chip cards. This key is per BIN and this process is the same as key exchange for Visa STIP processing. It is optional to share the existing MDK with Visa, as they can create a new one for tokenisation. GPS can support either option.
- Shared Secret (or HMAC key) - this is used by Visa to validate Visa inbound APIs that are sent by GPS. This is shared per issuer via the Visa Developer Portal.
- API Key - this is added to the URL by GPS for Lifecycle Maintenance (outbound) APIs. This is shared per issuer via the Visa Developer Portal
- JWE/JWS certificates - Private/Public key pairs used to sign or encrypt sensitive data within the APIs. The public certificates of these keys will be shared between GPS and Visa during the implementation project.
- Key Identifier (KID) - Visa provides GPS with the Key Identifier (KID) they assign to the GPS JWE for Visa outbound APIs

The following key is exchanged between the party responsible for [Push Provisioning](#) and Visa. GPS has no visibility of this key:

- Pre-shared key for Push Provisioning

Mastercard Keys

- Pre-shared key for Push Provisioning

Note: You do not need to exchange a key with Visa/Mastercard for push provisioning if you are using a [GPS Supported Third Party for Push Provisioning](#).

6.5 External Host Interface (EHI)

The GPS External Host Interface (EHI) is required if you need to receive messages from GPS relating to the status of tokenisation requests (e.g., TAR, TEN, CAN/TAN and TCN messages) and for Apple Reporting¹.

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

EHI is required when using the tokenisation service if you want to send the One Time Passcode (OTP) message used during the tokenisation process directly to your cardholder ([see the Approve with Authentication](#) flow). Although this can be retrieved via Smart Client or Web services it is harder to automate processes using these services.

The tokenisation flow contains its own 6-digit specific processing codes (ProcCode in EHI), which can be used to identify any EHI messages relating to tokenisation. Refer to the table below.

Processing Code	Message Type	Function
320000	Token Eligibility Request (TER)	Not used by Mastercard. Used for issuers who can't respond to the TAR in time.
330000	Token Activation Request (TAR)	Request for a new token.
340000	Activation Code Notification (ACN)	Contains the OTP delivery message.
350000	Token Complete Notification (TCN)	Token created.
360000	Token Event Notification (TEN)	Token event notification (including activation).
370000	Get verification methods	Visa only message requesting cardholder verification methods for the approve with authorisation flow.
380000	Device Binding DBR	Request to bind an existing token to a device (online merchant token requestors only).

For details of the EHI message fields related to tokenisation and an example of a TAR message, see [EHI Tokenisation Fields](#).

For examples of the different types of tokenisation messages available via EHI, please refer to the EHI Guide.

¹If you do not want to enable EHI, but still want to pursue a tokenisation implementation, please contact your Account Manager to investigate the feasibility of GPS providing data for Apple reporting in another format.

7 Token Provisioning Message Flows

For token provisioning there are several messages that are sent between the Token Service Provider and GPS. These are a mixture of ISO 8583 (for VDEP and MDES) and JSON API (for VDEP only) formats. All ISO 8583 messages and One Time Passwords (OTPs) obtained are sent over EHI to the Program Manager¹.

Note: All EHI messages in the Token Provisioning flow (TAR/TEN/TCN) are advices only. This means that for all EHI modes you are not able to authorise TAR, TEN or TCN advices. You can use these messages to confirm to the cardholder the tokenisation status. They should never be used for payment authorisation approval or decline decisions.

Figures 12-15 below describe the Visa and Mastercard messages that are received for token provisioning requests. Note that since these are asynchronous messages, it is possible they may arrive out of sequence.

Message flow for Mastercard Token Provisioning (Green Flow)

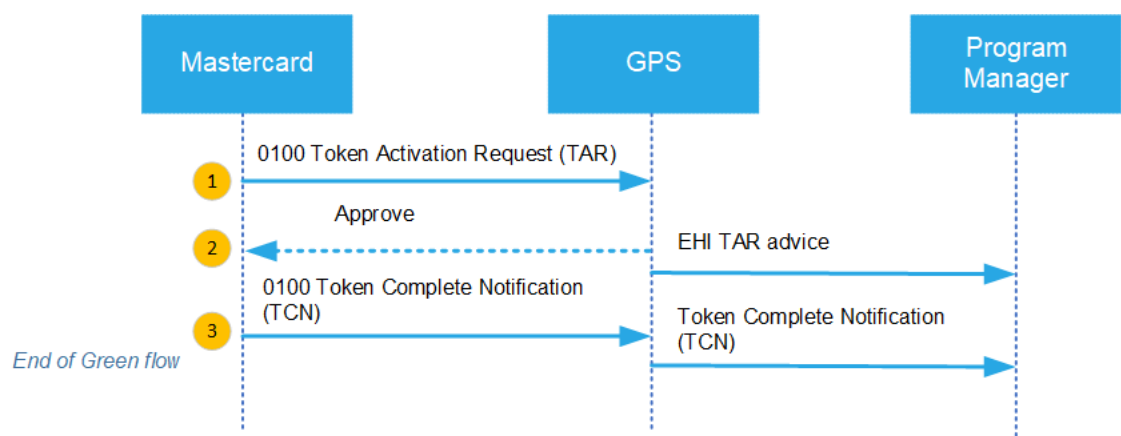


Figure 12: Mastercard Messages (Green Flow)

1. Mastercard sends an 0100 Token Activation Request (TAR).
2. GPS returns an Approve response to Mastercard.
GPS forwards the TAR to the Program Manager, via EHI.
3. Mastercard sends an 0100 Token Complete Notification (TCN).
GPS forward the TCN notification to the Program Manager, via EHI.

Message flow for Mastercard Token Provisioning (Yellow Flow)

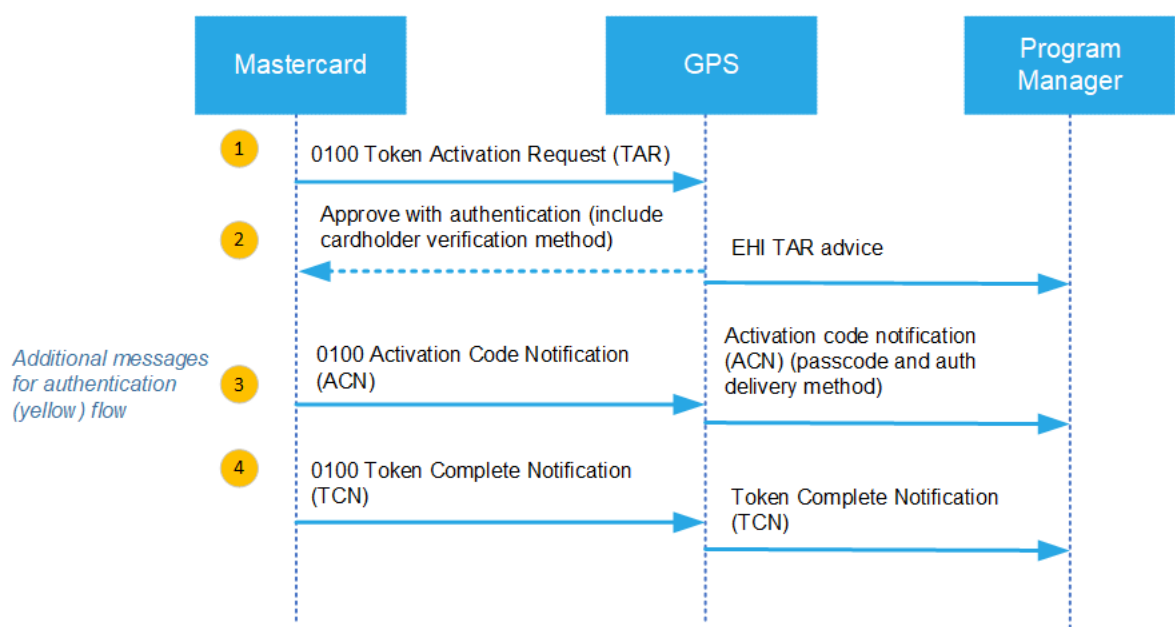


Figure 13: Mastercard Messages (Yellow Flow)

1. Mastercard sends an 0100 Token Activation Request (TAR).
2. GPS returns an Approve with Authentication response to Mastercard. The response includes the available cardholder verification methods (e.g., SMS).
GPS forwards the TAR advice to the Program Manager, via EHI.

¹ISO 8583 is the message format used for authorisation messages passed between Visa/Mastercard and GPS.

- 3. Mastercard sends an 0100 Activation Code Notification (ACN).
GPS forward the ACN notification (plus the passcode and verification method) to the Program Manager, via EHI.
- 4. Mastercard sends an 0100 Token Complete Notification (TCN).
GPS forward the TCN notification to the Program Manager, via EHI.

Message flow for Visa Token Provisioning (Green Flow)

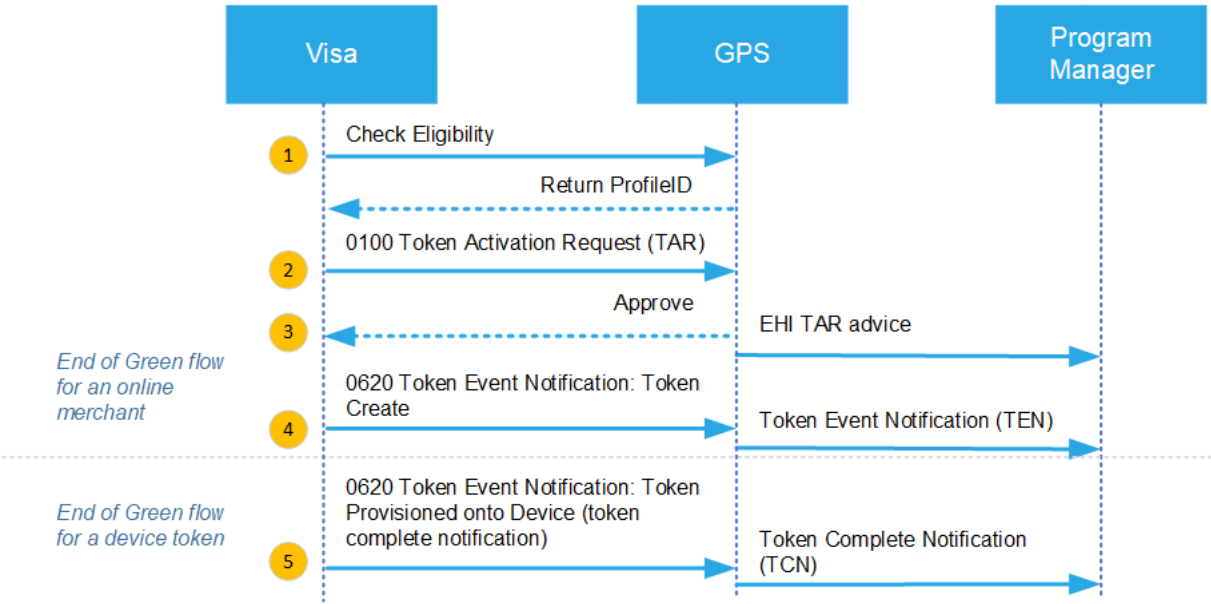


Figure 14: Visa Messages (Green Flow)

- 1. Visa sends a message to GPS to check if the PAN is eligible for tokenisation.
GPS 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 GPS.
- 3. GPS returns an Approve response to Visa.
GPS forwards the TAR to the Program Manager, via EHI.
- 4. Visa sends an 0620 Token Event Notification (TEN) to GPS, to indicate the token has been created.
GPS 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.
GPS forwards the TCN notification to the Program Manager, via EHI.

Message flow for Visa Token Provisioning (Yellow Flow)

Note: This flow is only relevant to tokens that are bound to a mobile phone or other device.

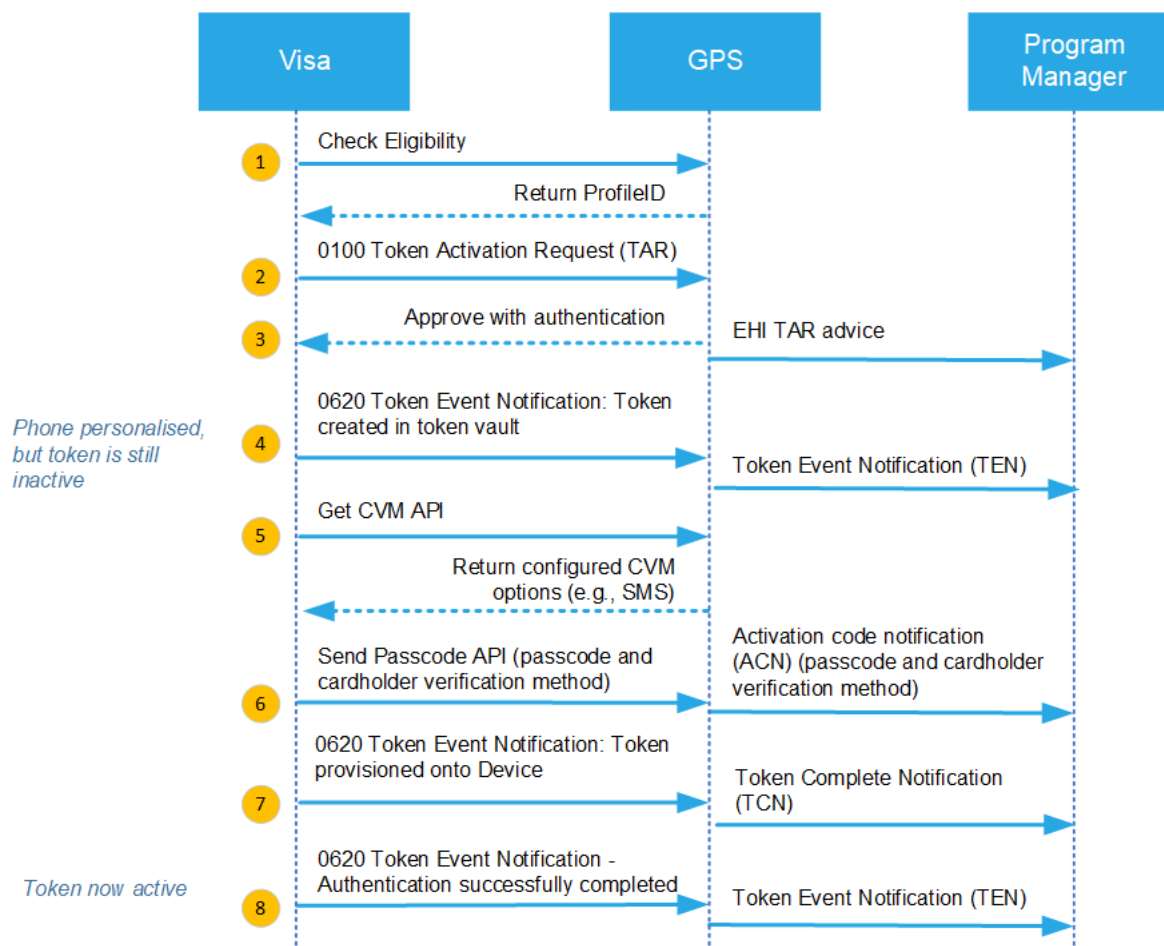


Figure 15: Visa Messages (Yellow Flow)

1. Visa sends a message to GPS to check if the PAN is eligible for tokenisation. GPS 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 GPS.
3. GPS returns an Approve with Authentication response to Visa. GPS forwards the TAR to the Program Manager, via EHI.
4. Visa sends an 0620 Token Event Notification (TEN) to indicate the token has been created (the token is not yet active)
5. Visa uses the Get CVM API to retrieve a list of available cardholder verification methods (CVMs) for this token from GPS (i.e., methods such as SMS).
6. Visa uses their Send Passcode API to send the passcode and the user-selected cardholder verification method to GPS. GPS sends an Activation Code Notification (ACN) to the Program Manager, via EHI. The ACN contains the authentication passcode (One-time password) and user-selected verification method.
7. The OTP is delivered to the cardholder using their chosen verification method. Visa sends an 0620 Token Event: Token Complete Notification (TCN), to indicate the token has been provisioned onto the device. GPS forward the TCN notification to the Program Manager, via EHI.
8. Visa sends an 0620 Token Event Notification (TEN) to GPS, to indicate the token authentication was successful. The token is now active. GPS forwards the TEN notification to the Program Manager, via EHI.

Note: Some Mobile Wallet token requestors require you to confirm to cardholders when the tokenisation process is complete or to follow up with cardholders when tokenisation has not been completed.

Note: The Token Complete Notification (TCN) sent over EHI currently indicates when the device is successfully provisioned. In some cases, later Token Event Notifications (TENs) can arrive once the cardholder is authenticated and Visa has activated the token, which represent the actual end of the token provisioning flow.

The section [When to notify cardholders tokenisation is complete](#) below describes how you can identify the end of the tokenisation flow.

7.1 When to notify your cardholders that Tokenisation is complete

Mastercard sends GPS a Token Completion Notification (TCN) which identifies when the tokenisation process is complete. We send you the Token Completion Notification (**ProcCode** 350000). You must notify your customers within 30 minutes of successful provisioning and activation of the token (an Apple requirement).

For Visa, currently the Token Completion Notification (**ProcCode** 350000) only represents the end of the tokenisation flow for Green Flow Device Tokenisation. Visa send a 620 message to indicate that the token is active. GPS then send a Token Complete Notification (TCN) where the **paymenttoken_creatorStatus** = A (active). For details, see [Visa Tokenisation Messages](#).

7.2 Token Requestor Testing

Some Mobile Wallet Token Requestors require completion of testing before go-live. Please inform your Implementation Manager before this testing has started. GPS do not receive updated test requirements from Mobile Wallet Token Requestors as we do not have a direct relationship with these parties.

Note: If you become aware of a recent change in the Apple or Android requirements, please contact your Account Manager or Implementation Manager before testing begins so GPS can review.

8 Managing your Programme

Managing a tokenisation service programme is handled through both the Visa/Mastercard Online Portals and through GPS web services.

GPS does not have access to the tools available on the Visa and Mastercard online portals.

8.1 Existing Payment Tokens

If you want to know what payment tokens are linked to a GPS public token, you can use the following web services API:

- [Ws_Payment_Token_Get](#) – returns a list of all tokens linked to the specified public token.
- [Ws_Token_Device_Management](#) – returns a list of devices bound to a token.

For more information, refer to the [GPS Web Services Guide](#).

Payment tokens can also be viewed on Smart Client. Refer to the [GPS Smart Client Guide](#).

8.2 Token and PAN Lifecycle Management

Some web service calls to GPS automatically trigger a request to update the digital payment token (DPAN) on the Visa/Mastercard systems¹. The web service response from GPS will indicate the following:

- For Visa DPAN updates, the web service response confirms the update on both the GPS platform and the Visa platform in real-time. The Token Even Notification (TEN) from Visa will be provided over EHI. For details, see the section [Real-time Token Status Change \(Visa\)](#).
- For Mastercard, the web service response confirms the update on the GPS platform only. GPS sends an update file to Mastercard every four hours, at which point Mastercard will update the token. For details, see the section [Token Status Change \(Mastercard\)](#).

Changing the status of a Payment Token

You can use the GPS web service [Ws_Payment_Token_StatusChange](#) to update the status of a payment token on the GPS platform; for details refer to the GPS Web Services Guide. This will trigger a real-time update message to Visa/Mastercard to update the status on their systems and with the Token Requestor.

Real-time Token Status Change (Visa)



Figure 16: Real-time Token Status Change (Visa)

1. The Program Manager uses the GPS web service to change the token status on the GPS platform.
2. GPS sends a request to Visa to update payment token status on their systems.
3. Visa responds with the token status update result.
4. GPS confirms the status update in the web service response and via EHI.
5. Visa sends a Token Event Notification (TEN) with the status change.
6. GPS confirms the status update via EHI.

¹For example, if you replace a card with a token, change the payment token status, regenerate a card image or renew an expired card.

Note: Visa sends a confirmation of token status update via the ISO 8583 message service which GPS forwards to you via EHI. This token status update may be initiated via web services or via the cardholder from their device.

Real-time Token Status Change (Mastercard)

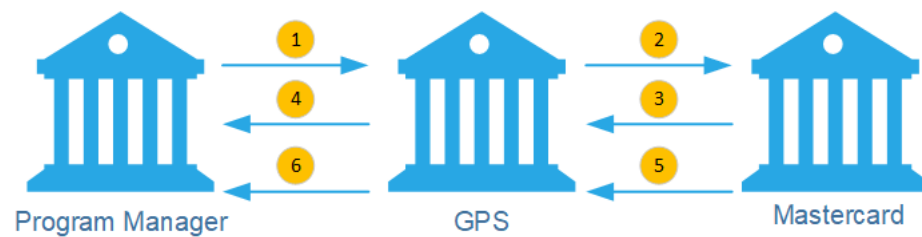


Figure 17: Token Status Change (Mastercard)

1. The Program Manager uses the GPS web service to change the token status on the GPS platform.
2. GPS sends a request to Mastercard to update payment token status on their systems.
3. Mastercard responds with the token status update result.
4. GPS confirms the status update in the web service response and via EHI.
5. Mastercard sends a Token Event Notification (TEN) with the status change.
6. GPS confirms the status update via EHI.

An approval web service response code (000) means the status change has been successful on both GPS and Token Service Provider platforms. If Mastercard receive a status change requesting a block on a card already blocked, an approval response code (000) will be received.

A failed web service response code (951) means that the status change was not successful and neither platform has been updated. If the first attempt at a status change is unsuccessful, GPS recommend re-attempting the status change. If subsequent attempts at a status change continue to be unsuccessful, contact GPS for support.

Status Codes to use for Card Blocks

You should use the following GPS status codes for temporary and permanent blocks:

- Temporary Block: "57 - Transaction not permitted to cardholder" or "62 - Restricted Card"
- Permanent Block: "41 - Lost" or "46 - Account Closed" or "83 - Card Destroyed"

Replacing a Card

If you are replacing a card, then there is a requirement from some Token Requestors that the payment token is automatically switched over to the new card.

If a card is expiring, you can request a replacement card using the Card Renew web service ([Ws_Renew](#)). Once the replacement card is ready it can be activated using the web service [Ws_Activate](#).

- For Visa, GPS send an API to the Token Service Provider in real-time informing them of the new PAN, CVV2 and Expiry which will then be passed to the Token Requestor.
- For Mastercard, GPS queue and send a batch update file, every four hours.

Unbinding a Device from a Card on File Token

Note: Visa only

If you want to remove a device binding from a Card on File token (for example if your cardholder has reported their device as stolen) then you can use [Ws_Token_Device_Management](#). This triggers a real-time API call to the Token Service Provider. An approval action code (000) means the request has been successful on both GPS and Token Service Provider platforms. A failed response means that neither platform has been updated.

Appendix A: Device Scoring

Example of score configurations: 1-5, with 1 = least trusted, and 5 = most trustworthy.

Maximum Scores

Maximum scores which prompt whether we authenticate or decline.

Wallet Device Max Score Auth	3
Wallet Device Max Score Decline	1
Wallet Account Max Score Auth	3
Wallet Account Max Score Decline	1

If set to 0 = never authenticate or decline (use this if you do not want GPS to use any of this logic).

Default Score

These options indicate what default score should be provided if no score is received from the Wallet Provider in the incoming TAR message. (Currently only Apple provide a device score)

Wallet Device Score Default	3
Wallet Account Score Default	3

In the above example, a value of 3 would result in authentication.

Appendix B: View the OTP on Smart Client

If a cardholder calls your call centre to retrieve the One Time Password, these are the steps your call centre staff need to follow.

1. Open the Smart Client Portal.
2. Select **View Transactions**.
3. Enter the cardholder's GPS Token and search for the authorisation records.
4. Right-click the transaction and select **More Details > View Transaction Details**.
The Transaction Details screen is shown.
5. Click the arrow to the right of the **Device** field.
The Payment Token screen is displayed.

LINKED CARD	
Property	Value
Creator's token ref	FAPLMC00002297903a59821b27414e199...
Linked Token	

PERSONALISATION/DIGITISATION	
Property	Value
Creator digi. ref	D0000086709377
Wallet Account Score	3
Wallet Device Score	3
Wallet risk table	000000000001000000000100
GPS decision	Approve with Authentication
GPS decision at	2017-08-13 23:46:28.130
Final decision	Approve with Authentication
Final decision by	Mastercard tokenisation system (MDES)
Terms & Conditions	3914433d6310469aaa3e666953cca8ad on 2017-...

PAYMENT TOKEN	
Property	Value
Creator	Mastercard tokenisation system (MDES)
Creator token ref	
GPS token ref	
Token Expiry	2020-09-01
Token PAN	****1878
Token Type	Secure Element PAN
Wallet Provider	Apple Pay Wallet

TOKEN STATUS	
Property	Value
Tokenised	☒
Tokenisation Date	2017-08-13 23:46:46.667
Status(in GPS)	00 - All Good
External Status	Active
Ext. Status set by	
Ext. status changed	

ACTIVATION INFO	
Property	Value
Activation Code	113814
Activation Expires	2017-08-13 23:16:00.000 GMT/UTC
Activation Method	SMS to mobile

Figure 18: FPayment Token screen on Smart Client

6. The screen shows the payment token details supplied by MDES/VDEP, along with the decision process information. The One Time Password value is shown in the **Activation Code** field.
7. Once provided to the cardholder, they should be able to enter this into their Wallet app to authenticate.

Appendix C: EHI Tokenisation Fields

The table below lists the EHI message fields relevant to the tokenisation service.

Field	Description
PaymentToken_id	Unique GPS token reference.
PaymentToken_creator	The token service provider (Mastercard or Visa).
PaymentToken_exp-date	The expiry date of the token.
PaymentToken_type	The payment token type. Defines the technology the token is being held on.
PaymentToken_status	Indicates the status of the token. Please note, this can differ from the status of the PAN.
PaymentToken_creatorStatus	Indicates the status as set by the token service provider (Mastercard/Visa) and also on the device itself. This adds information around the progress of token setup along with whether a post-setup token is active or not.
PaymentToken_wallet	The wallet provider (e.g., Apple Pay, Google Pay) the token is linked to.
PaymentToken_deviceType	The type of device the token is linked to (e.g., Mobile Phone, watch, tablet).
PaymentToken_lang	The language configured on the device linked to the token (if available).
PaymentToken_deviceTelNum	The telephone number of the device linked to the token.
PaymentToken_deviceIp	The IP address of the device linked to the token.
PaymentToken_deviceId	The device ID of the device linked to the token. (Also called the DE124 Payment Application Instance Id at Mastercard and SEIDs (Secure element ID) at Apple.)
PaymentToken_deviceName	The name of the device linked to the token.
PaymentToken_activationCode	The token activation code.
PaymentToken_activationExpiry	The token activation expiry date.
PaymentToken_activationMethod	The token activation method (e.g., 0=none; 1 = SMS)
PaymentToken_activationMethodData	The token activation method details (e.g., if the activation method is 1 for SMS, then provides the mobile phone number to send the SMS).

For more information, refer to the [EHI Guide](#).

11.1 Example EHI TAR Message

The example below shows a typical EHI 0100 authorisation message for a Token Authorisation Request (TAR). Your systems need to respond to tokenisation messages with an acknowledgement. For more information, refer to the [EHI Guide](#).

Note: Empty fields have been removed from this example.

[illegible]

Appendix D: Visa Tokenisation Messages

The scenarios below describe how you can determine the end of the tokenisation flow on Visa.

Tip: When you get a message with payment token status of A, this means the token is active and ready to do transactions and should be the last message in the flow.

Scenario 1: Online Merchant Token Request - Green flow

Look for this information in the following EHI fields to identify the message flow and when you need to send a notification to your cardholder of successful provisioning.

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	BW or CF	330000 (TAR)	00	(omitted)	71	Approve
2	BW or CF	360000 (TEN)	00	A	71	Indicates end of Green flow. Do not notify cardholder ¹ .

Scenario 2: Mobile Wallet Token Requests with Green flow

For a mobile wallet: Look for this information in the following EHI fields to identify the message flow and what you need to do.

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	SE or CL	330000 (TAR)	00	(omitted)	71	Approve
2	SE or CL	360000 (TEN)	00	A	71	
3	SE or CL	350000 (TCN)	00	A	72	Last message in flow. Cardholder notification of successful provisioning can be sent here.

¹These are used by e-commerce merchants who tokenise PANs for storage (e.g. Netflix) and the cardholder is not necessarily present so would be confused by a message confirming tokenisation and likely to consider it fraudulent.

Scenario 3: Mobile Wallet Token Requests Yellow flow with successful authentication

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	SE or CL	330000 (TAR)	85	(omitted)	71	Approve with authentication
2	SE or CL	360000 (TEN)	00	I	71	Token Event Notification
3	SE or CL	340000 (ACN)	00	I	0	Activation Code Network Message. Contains the OTP to verify the cardholder.
4	SE or CL	350000 (TCN)	00	I	72	In yellow flow - do not send messages using the TCN.
5	SE or CL	360000 (TEN)	00	A	73/74/75	Last message in flow. Cardholder notification of successful provisioning can be sent here.

Scenario 4: Mobile Wallet Token Requests with Yellow flow with unsuccessful authentication

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	SE or CL	330000 (TAR)	85	(omitted)	71	Approve with authentication
2	SE or CL	360000 (TEN)	00	I	71	Token Event Notification
3	SE or CL	340000 (ACN)	00	I	0	Activation Code Network Message. Contains the OTP to verify the cardholder.
4	SE or CL	350000 (TCN)	00	I	72	In yellow flow - do not send messages using the TCN.
5	SE or CL	360000 (TEN)	00 or 06	A	53/54/55	Last message in flow. No notification of tokenisation completion as authentication was unsuccessful.

Appendix E: Mastercard Tokenisation Messages

The scenarios below describe how you can determine the end of the tokenisation flow on Mastercard.

Tip: When you get a message with payment token status of A, this means the token is active and ready to do transactions and should be the last message in the flow.

Scenario 1: Online Merchant Token Request - Green flow

Look for this information in the following EHI fields to identify the message flow and when you need to send a notification to your cardholder of successful provisioning.

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	BW or CF	350000 (TEN)	00	A	72	Indicates end of Green flow. Do not notify cardholder ¹ .

Scenario 2: Mobile Wallet Token Requests with Green flow

For a mobile wallet: Look for this information in the following EHI fields to identify the message flow and what you need to do.

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	SE or CL	330000 (TAR)	00	(omitted)	71	Approve
2	SE or CL	350000 (TCN)	00	A	72	Last message in flow. Cardholder notification of successful provisioning can be sent here.

Scenario 3: Mobile Wallet Token Requests Yellow flow with successful authentication

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	SE or CL	330000 (TAR)	85	(omitted)	71	Approve with authentication
2	SE or CL	340000 (ACN)	00	I	0	Activation Code Network Message. Contains the OTP to verify the cardholder.
3	SE or CL	350000 (TCN)	00	A	72	Last message in flow. Cardholder notification of successful provisioning can be sent here.

Scenario 4: Mobile Wallet Token Requests with Yellow flow with unsuccessful authentication

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
1	SE or CL	330000 (TAR)	85	(omitted)	71	Approve with authentication
2	SE or CL	340000 (ACN)	00	I	0	Activation Code Network Message. Contains the OTP to verify the cardholder.
3	SE or CL	350000 (TCN)	00	A	72	Last message in flow. No notification of tokenisation completion as authen-

¹These are used by e-commerce merchants who tokenise PANs for storage (e.g. Netflix) and the cardholder is not necessarily present so would be confused by a message confirming tokenisation and likely to consider it fraudulent.

Message Order	PaymentToken_Type	ProcCode	Resp_Code_DE39	PaymentToken_creatorStatus	Message_Why	Comments
						tokenisation was unsuccessful.

Appendix F: Apple Pay Tokens

Apple technology enables you to offer your customers an option to use their Apple devices to make contactless and secure e-commerce payments.

Your Mobile App can use an iOS API to view cards you've issued that have been provisioned onto the Apple device. You can use the Apple API to present your customer with their chosen card for payment. The cardholder can then provide consent for the transaction using Touch ID / Face ID or a passcode to make a payment. Upon completion of the payment, the cardholder is automatically returned back to your Mobile App.

Note: Apple require certification to use their service, which must be done directly with them. For further information, please refer to the Apple document: [Functional Requirements Direct NFC Access and Apple Pay](#).

For more information on Apple Pay services for developers, see the [Apple Pay Developer Website](#).

Apple Pay Token Provisioning

For details of token provisioning flows supported by GPS, see [Token Provisioning Message Flows](#).

Token provisioning requests that are flagged as Apple Orange Flow and/or a Device Score = 1 indicate that more rigorous authentication of the cardholder is required. See [Apple Pay Orange Flow](#) below.

Apple Pay Orange Flow

Note: GPS currently does not support Apple Pay orange flow additional authentication checks. For options and workarounds, please discuss with your GPS Account Manager.

Orange is represented by the Apple reason code "0G" and is triggered when Apple's account or device history infers an elevated statistical probability of fraud. From a GPS perspective, the transaction is identified by device score = 1 (i.e., highest risk). Any provisioning request with device score = 1 is treated according to the GPS [Red Flow](#) and is declined.¹

FPAN Reissue and Replacement

Apple Pay require that when the FPAN is reissued (due to expiration or lost/fraud replacement), the DPAN should continue to work without the need to re-provision the new physical card. The card in the Wallet displays the new FPAN number, if it has changed.

Note: By default, the FPAN and DPAN are connected, so if the FPAN is lost and the card status is changed this will also change the status of the DPAN. If you need the DPAN to continue to work while the FPAN is replaced you must split them, by enabling the DPAN_over_FPAN option. For details, see [DPAN over FPAN Status](#).

When replacing a card, you should always use the Card Renew ([Ws_Renew](#)) web service. For details, see the [Web Services Guide](#).

Once the new card is activated, the update to the FPAN/DPAN details will be immediate for a Visa token and will be added to the next batch file cycle for a Mastercard token. Alternatively, if you are using Mastercard, you can log on to Mastercard's MC Connect > MDES Portal and make the changes directly once the card is renewed.

¹If you do not want GPS to use the device score, you can set the value to 0 (never authenticate or decline).

Frequently Asked Questions

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

GPS are the issuing host and so approve or decline the tokenisation requests. GPS 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. See [Who Participates in Tokenisation?](#)

Q. How do we start a project?

A project needs to be opened with the Token Service Providers (Visa/Mastercard) and with GPS. Please discuss with your Account Manager.

Q. At what point does GPS get involved?

GPS needs to be involved when the Visa/Mastercard project is started, as we need to provide details in the documentation about the GPS setup. See [Implementing a Tokenisation Project](#).

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 GPS). See [Implementing a Tokenisation Project](#).

Q. How long does a project take?

To add tokenisation to an existing product typically 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. This needs to be sent 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 GPS SMS option to send the OTP to the cardholder. See [External Host Interface \(EHI\)](#).

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 one of the supported GPS third party push provisioning providers to extract the PAN data directly from GPS to complete this. See [Using a GPS Supported Third Party for Push Provisioning](#).

Q. Are there any web service calls we need to make?

Yes. See below:

- [Ws_CreateCard](#) – create card
- [Ws_Activate](#) – activate card
- [Ws_Payment_Token_Get](#) – get the payment token
- [Ws_Token_Device_Management](#) – manage the token device
- [Ws_Payment_Token_StatusChange](#) – change the status of the payment token

For details, see the GPS Web Service Guide.

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 Requestors. You do not need an app for Online Merchant Token Requestors.

Q. On the PSF what does “override enabled/disabled” mean, what does it do?

This option on the Payment Setup Form (PSF) means that GPS will override any logic that would send an authentication request to the cardholder when we detect that push provisioning has been carried out. Since the cardholder has already been authenticated during push provisioning, GPS does not need to request further authentication.

This must be enabled to pass Apple testing and is a good cardholder journey for other token requestors. See [GPS Configuration Options](#).

Q. What is the difference between VTS and VDEP?

They both refer to the same service. VTS is the Visa Token Service and VDEP is the Visa Digital Enablement Programme. You are required to sign a VDEP agreement with Visa when starting a new Visa Token Service integration.

Since VTS is also an abbreviation for the Visa Test Simulator (VTS), we use the term VDEP to avoid confusion.

Q. What's the difference between a Token and a Payment Token?

GPS refer to the 9-digit public token for use on GPS systems as the Token or Public Token and the digitised tokens from the schemes is called a Payment Token.

Q. What's the difference between a Token Requestor and a Wallet Provider?

These are used interchangeably between the schemes however Visa will more often use Token Requestor and Mastercard use Token requestor. Because the Mastercard Digital Enablement Service (MDES) was integrated first at GPS you will often see references to token requestor.

Q. What is the difference between an FPAN and a DPAN?

These are Apple terms to specify which PAN is being discussed as following tokenisation there are two PANs for one card. The FPAN is the Funding PAN and refers to the original PAN on the card and the DPAN is the Device PAN and refers to the PAN personalised onto the device.

Q. Does GPS know the DPAN?

Yes. GPS receives and stores the DPAN during the provisioning process and validates it during subsequent transactions on that DPAN. IF GPS does not receive the DPAN then it will decline transactions.

Glossary

This page provides a list of glossary terms used in this guide.

0

0100 Message

0100 Message Transaction Identifier (MTID). This is a Token Activation Request (TAR) message, requesting authorisation for the token creation.

0620 Message

0620 Message Transaction Identifier (MTID). This is a Token Event Notification (TEN) which indicates the token has been created.

3

3D Secure

3D Secure (3-domain structure), also known as a payer authentication, is a security protocol that helps to prevent fraud in online credit and debit card transactions. This security feature is supported by Visa and Mastercard and is branded as 'Verified by Visa' and 'Mastercard SecureCode' respectively.

A

ACN

Activation Code Network Message. The message sent to GPS and also the Programme manager via EHI which contains the OTP to verify the cardholder.

Acquirer

The merchant acquirer or bank that offers the merchant a trading account, to enable the merchant to take payments in store or online from cardholders.

Activation Code Notification

A message over EHI containing the OTP.

Authentication

This includes checks to confirm the cardholder identity, such as PIN, CVV2 and CAVV.

Authorisation

Stage where a merchant requests approval for a card payment by sending a request to the card issuer to check that the card is valid, and that the requested authorisation amount is available on the card. At this stage the funds are not deducted from the card.

Automated Fuel Dispenser (AFD)

Automatic fuel dispensers (AFDs) are used at petrol or gas stations for customer self-service fuel payments. Typically the customer inserts their card and enters a PIN number and the AFD authorises a fixed amount (e.g. £99). Once the final payment amount is known, the AFD may reverse the authorisation and/or request a second authorisation.

B

BIN

The Bank Identification Number (BIN) is the first four or six numbers on a payment card, which identifies the institution that issues the card.

BLOB

Binary Large Object file. A blob is a data type that can store binary data. It can be used to store images or other multimedia files.

C

Card Scheme

Card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.

Clearing File/Clearing Transaction

GPS receive batch clearing files from the card networks, containing clearing transactions, such as presentments and network fees. The card issuer transfers the requested settlement amount to the acquirer and 'clears' the amount on the card, reducing the available card balance accordingly.

COF Token

Card on File token request created by an online merchant.

COF Token Requestors

Online merchant Token Requestors are referred to as Card on File (COF) Token Requestors. These are merchants who tokenise a payment card so that the token can be used for repeat payments or recurring payments on their website.

Counter

A counter under the PSD2 rules is used to track the number of transactions and cumulative amount before the cardholder is requested to authenticate using Strong Customer Authentication (SCA): for example, via PIN for a card or via 3D Secure authentication for an online transaction.

CVV2

The Card Verification Value (CVV) on a credit card or debit card is a 3-digit number on Visa, MasterCard and Discover branded credit and debit cards. Cardholders are typically required to enter the CVV during any online or cardholder not present.

D

Device Score

The score applied by the wallet provider defining the level of satisfaction the wallet provider has in the request being a genuine cardholder attempt, based on the wallet providers internal fraud parameters.

DPAN

Device PAN. The PAN value set up on the cardholder's device. This is not visible to the cardholder, but is the PAN used for the transactions as far as the merchant is concerned.

E

EH

External Host Interface. This is a GPS product providing clients either a real time feed or the ability to be involved in authorisations.

EMV

EMV is a payment standard for smart payment cards, payment terminals and automated teller machines (ATMs). EMV is an acronym for "Euro-pay, Mastercard, and Visa", the three companies which created the standard.

EMVCO

Organisation that facilitates worldwide interoperability and acceptance of secure payment transactions. Created by EuroPay, Mastercard and Visa.

External Host

The external system to which GPS sends real-time transaction-related data. The URL to this system is configured within GPS per programme or product. The Program Manager uses their external host system to hold details of the balance on the cards in their programme and perform transaction-related services, such as payment authorisation, transaction matching and reconciliation.

F

Fee Groups

Groups which control the card transaction authorisation fees, and other fees, such as recurring fees and GPS web service API fees.

FPAN

Funding PAN. The true 16-digit PAN of the card, which Mastercard/Visa converts when authorisations come through to them from Acquirers on the DPAN.

G

Green Flow

This is an Apple term for a Token Provisioning request that is approved.

H

Hanging Filter

The period of time during which GPS waits for an approved authorisation amount to be settled. This is defined at a GPS product level. A typical default is 7 days for an auth and 10 days for a pre-auth.

I

Incremental Authorisation

A request for an additional amount on a prior authorisation. An incremental authorisation is used when the final amount for a transaction is greater than the amount of the original authorisation. For example, a hotel guest might register for one night, but then decide to extend the reservation for additional night. In that case, an incremental authorisation might be performed in order to get approval for additional charges pertaining to the second night.

ISO 8583

The message format for BASE I/Authorisation messages between GPS and the token service provider (Visa/Mastercard). This is the industry standard for authorisations.

Issuer

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.

Issuer Host

This is the host connected directly to Visa/Mastercard for authorisation messages (i.e., GPS).

M

MDES

The MasterCard Digital Enablement Service (MDES) is a data interchange platform for generating and managing secure digital payment tokens. It enables devices such as smartphones, smart watches, as well as merchants, to create a tokenised version of a Mastercard, which is specific to that device or merchant. Then the device/merchant can use the tokenised version of the card to perform transactions. The tokenised version of the card appears as just a normal Mastercard card number to the merchant and acquirer, and Mastercard will map the transactions onto the original cardholder Mastercard.

Merchant

The shop or store providing a product or service that the cardholder is purchasing. A merchant must have a merchant account, provided by their acquirer, in order to trade. Physical stores use a terminal or card reader to request authorisation for transactions. Online sites provide an online shopping basket and use a payment service provider to process their payments.

Merchant Category Code (MCC)

A unique identifier of the merchant, to identify the type of account provided to them by their acquirer.

MIP

Mastercard Interface Processor (MIP) The processing hardware and software system that interfaces with Mastercard's Global Payment System communications network.

Mobile Wallet Token Requestor

A token requestor connected to a mobile device.

MRCHTOKEN

GPS name for the Wallet Provider group, representing Online Merchant Token Requestors. Also referred to as M4M (by Mastercard) and Card on File (by Visa).

N

NFC

Near Field Communication (NFC) is a technology that enables a device, such as a mobile phone or payment ring, to transmit data to a Point of Sale (POS) terminal, enabling contactless payments.

O

Offline Transaction

This is often used in scenarios where the merchant terminal is not required to request authorisation from the card issuer (for example for certain low risk, small value transactions used by airlines and transport networks). The card CHIP EMV determines if the offline transaction is permitted; if not supported, the terminal declines the transaction. Note: Since the balance on the card balance is not authorised in real-time, there is a risk that the card may not have the amount required to cover the transaction.

Online Merchant Token Requestor

A token requestor that is an e-commerce merchant.

OTP

One Time passcode/ Activation code which is sent to the cardholder for use in authenticating during token provisioning, during the setup of Google Pay, Apple Pay or other wallet on their device.

P

PAN

The Primary Account Number (PAN) is the card identifier found on payment cards, such as credit cards and debit cards, as well as stored-value cards, gift cards and other similar cards. The card's 16-digit PAN is typically embossed on a physical card.

Partial Amount Approval

Some acquirers support a partial amount approval for Debit or Prepaid payment authorisation requests. The issuer can respond with an approval amount less than the requested amount. The cardholder then needs to pay the remainder using another form of tender.

Payment Token

GPS term for a MDES/VDEP token. This is used to differentiate between a GPS public token and a MDES/VDEP token. GPS use this in EHI and web service calls to identify a particular DPAN

Payment Token Usage Wallet

The default set of parameters GPS will use to authorise a TAR.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle credit cards from the major card schemes. All Program Managers who handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security/

Personalisation

The technical process of marking private data specific to a given card or device. The same terminology is used when putting private data on a chip card or a smart device.

Point of Sale (POS) Terminal

A hardware device for processing card payments at retail stores. The device has embedded software that is used to read the card's magnetic strip data.

Program Manager

A GPS customer who manages a card program. The program manager can create branded cards, load funds and provide other card or banking services to their end customers.

PSD2

Payment Service Directive 2. PSD2 is an EU Directive which sets requirements for firms that provide payment services. It aims to improve consumer protection, make payments safer and more secure, and drive down the costs of payment services.

Public Token

The GPS 9-digit token is a unique reference for the PAN. This is used between GPS and clients to remove the need for GPS clients to hold actual PANs.

Push Provisioning

The process of pre-authenticating the cardholder prior to a token request being sent to Visa.

R

Red Flow

This is an Apple term for a Token Provisioning request that is declined.

S

sFTP

Secure File Transfer Protocol. File Transfer Protocol (FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Smart Client

Smart Client is GPS's user interface for managing your account on the GPS Apex system. It is also called Smart Processor GPS. Smart Client is installed as a desktop application and requires a VPN connection to GPS systems in order to be able to access your account.

Strong Customer Authentication (SCA)

Strong Customer Authentication (SCA) requires a combination of two forms of identification at checkout during an online transaction.

Examples include: something they know (such as a password or PIN), something they have (such as a mobile phone or other device) or something they are (such as their fingerprint).

T

TAV

Tokenisation Authentication Value. Used as part of In-app provisioning process and is the encrypted message that contains the PAN details for Mastercard from the Programme Manager.

TLS

Transport Layer Security (TLS) is a security protocol that provides privacy and data integrity for Internet communications. Implementing TLS is a standard practice for building secure web apps.

Token Activation Request (TAR)

Tokenisation Authorisation Request messages enable the issuer to provide a real-time decision as to whether the token service provider (MDES/VDEP) can digitise a card and designate a token on their behalf.

Token Complete Notification (TCN)

Tokenisation Complete Notification. Sent from Mastercard/Visa to GPS and made available via EHI to the Programme Manager to confirm the setup of the token was successful (note: there may be further messages for activation).

Token Event Notification (TEN)

Tokenisation Event Notification. Informs the issuer of unsuccessful Activation Code entry attempts and subsequent invalidation of an Activation Code or when a token is suspended, resumed or de-activated.

Token Service Provider (TSP)

The entity who stores the mapping between the PAN and the token. With the existing GPS integration this would be Visa or Mastercard.

Triple DES

Triple DES (3DES or TDES), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block to produce a more secure encryption.



Validation

Checks to confirm the card is valid, such as CHIP cryptograms, mag-stripe data (if available) and expiry date

VDEP

Visa Digital Enablement Programme. Also called the Visa Tokenisation Service (VTS).

VTS

Visa Tokenisation Service - is the Visa product name for tokenisation and equivalent of Mastercard's MDES (see MDES). GPS refer to this service as the Visa Digital Enablement Program (VDEP).

Document History

Version	Date	Description	Revised by
1.6	03/08/2022	Updated the PDF page layout	MW
	21/07/2022	New online version of the Tokenisation Service Guide is now available.	PC
	28/4/2022	Added details of Mastercard Real-Time Token to Token and PAN Lifecycle Management. See Real-time Token Status Change (Mastercard) .	MW
1.5	14/04/2022 28/04/2022	Addition of Digiseq as a third-party push provisioning service provider . Correction: If the DPAN over FPAN setting is enabled , then you must separately set the statuses of both the FPAN and DPAN. See DPAN over FPAN Status .	WS
1.4	08/02/2022 02/02/2022 01/04/2022	Added information on the DPAN over FPAN Status option. Added note to clarify usage of cards status codes for temporary blocks. See Status Codes to use for Card Blocks . Added details of MRCHTOKEN and Apple Pay Orange flow. Added new Appendix on ApplePay Tokens . Added details of enabling Manual Key Entry in the Card Usage Groups used by tokenised cards.	WS
1.3	9/08/2021 25/08/2021 03/09/2021	New advice on Status Codes to use for Card Blocks . Updates to diagram and description in Section Message flow for Visa Token Provisioning (Yellow Flow) . Note added to section Token Provisioning Message Flows to highlight that tokenisation messages receive via EHI are advices only and should never be used for payment authorisation approval or decline decisions.	WS
1.2	28/06/2021	New Mastercard Tokenisation Messages .	WS
1.1	14/05/2021	Changes to section GPS Configuration Options , and updates to Figures 9 and 10.	WS
1.0	29/03/2021	First version	WS
0.1	4/11/2020	Initial draft	SB