Key Concepts Guide

Version: 1.0
01 July 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.

Publication number: KCG-1.0-7/1/2022

Copyright

About this Guide

This guide describes the card payments ecosystem and how GPS supports your card program.

Target Audience

Technical teams responsible for setting up a new card program.

What's Changed?

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

How to use this Guide

- If you are new to card payments and want to understand how card payments work, see Introduction to Card Payments.
- If you want to find out more about the GPS system, see The Role of GPS and GPS Architecture.
- If you are looking to set up a card program and want to understand what this involves, see Setting up a Program with GPS and Use Case Scenarios.

Other Documentation

Refer to the table below for a list of other relevant documents that should be used together with this guide.

Document	Description
Getting Started Guide	Provides information on the stages in a typical GPS card project.
Web Services Guide	Describes how to use the GPS SOAP API to send requests to GPS and provides specifications on the available web service calls.
External Host Interface (EHI) Guide	Describes the GPS External Host Interface (EHI) and provides specifications on how to process and respond to messages received from EHI.
Transaction XML Reporting Guide	Describes the structure and contents of the GPS Transaction XML reports.

Document	Description
3D Secure Guide - RDX with Biometric/In-app authentication	Describes the GPS 3D Secure Realtime Data eXchange (RDX) service and how to implement a 3D Secure project with biometric/In-app authentication.

Tip: For the latest technical documentation, see the Developer Portal.

1 Introduction to Card Payments

This section provides a high-level description of the parties and components involved in setting up a card program and processing transactions on cards.

1.1 Parties Involved in Setting up a Card Program

The figure below provides an overview of the key parties involved in setting up a card program.

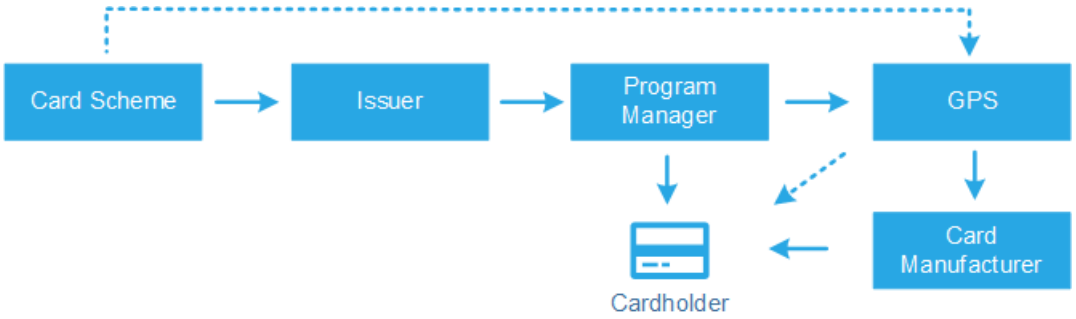

Figure 1-1: Key Parties in Setting Up a Card Program

Each of these parties is described in further detail below.

Card Scheme

The Card Scheme (e.g., Visa or Mastercard) provides the payment network used by all parties during a payment transaction. Cards that use the network are branded with the scheme logo (e.g., Visa or Mastercard).

The scheme provides mandates and rules which card issuers must follow when using their network. The schemes connect acquirers and issuers, provide daily clearing files and support the settlement and dispute management process. Schemes also charge fees to both acquirers and issuers for using their network.

GPS plugs in directly to the payment network and has partner relationships with Visa and Mastercard. Both these schemes are global and allow their branded cards to be used worldwide[1].

[1]GPS is currently developing links to other global and local card schemes. Please contact your GPS Business Development Manager for details.

The GPS system receives transactions from the scheme networks and processes these messages; the system can provide fraud screening, transaction checks and authorisation, before forwarding messages in real-time to your systems via the External Host Interface (EHI). For detail, refer to the External Host Interface (EHI) Guide.

> **Note:** If you are using the services of an Issuer, you do not need a direct relationship with the scheme, as your issuer manages this on your behalf.

Key Scheme Responsibilities

- Provides the payment infrastructure
- Has global relationships with acquirers and issuers
- Sets product rules (e.g., Funds management, Product level capabilities and restrictions)
- Sets interchange and other scheme related fees
- Maintains the full **BIN**[1] table and issues BINs to issuers
- Sets chargeback and dispute rules
- Provides value-added offerings, such as Tokenisation and Chargeback management
- Maintains cardholder usage data

Issuer

The card issuer is the **BIN Sponsor**[2]. The Issuer 'issues' the card BIN ranges that can be used to create new cards (based on their agreement with the card scheme).

Issuers have a direct relationship with the scheme and with GPS.

Issuers hold client money and must have separate, ring-fenced client money accounts. They must hold additional funds in reserve to meet scheme requirements. Issuers are regulated by the Financial Authority in their region (for example, for UK issuers this is the Financial Conduct Authority), so additional regulatory compliance standards apply.

---

[1] The Bank Identification Number (BIN) is the first six numbers on a payment card, which identifies the institution that issues the card. Visa and Mastercard are changing to an eight digit BIN from April 2022.

[2] Issuer, who creates the BIN range used by the Program Manager.

GPS customers (Program Managers) can be self-issuers or use the services of an existing issuer.

For new GPS customers starting out on a card program with GPS, speed to market is quicker and easier when using an existing issuer already set up with GPS, compared to setting yourself up as a new issuer. You can upgrade to self-issuing at a later stage without any impact on your transactions[1].

> **Note:** If your preferred issuer in your region does not currently have a relationship with GPS, it will require additional GPS integration support to onboard them. For further details, contact your GPS Business Development Manager.

If you are using an existing issuer you will not have a direct relationship with the card scheme. Issuers settle transfers of money directly with the schemes and details of issuer are normally printed on the back of their issued cards. Your issuer must provide you with access to relevant scheme resources and administrative portals. They will also need to approve your card program before it can be switched to live.

Key Responsibilities

- Ownership and customer (Program Manager) due diligence
- Must comply with Regulator and Card Scheme rules relating to:
    - Reporting
    - Risk monitoring
    - Fraud monitoring
    - Anti-money laundering
    - Auditing
    - Record retention guidelines
    - MIS analysis Typically holds funds
- Dispute management and chargebacks: may delegate to the Program Manager

[1] Migrating to self-Issuing requires changes to reporting and BIN setup with the card scheme. If you want to find out more about how to become self-issuing, please check with your Business Development Manager.

- Maintains a separate cash deposit
- Maintains client money in a separate Trust account
- Responsible for settlement and reconciliation
- Provides letter of guarantee for Program Manager
- Many need to review and approve aspects of the Program Manager's service, such as the Customer Portal, Customer App and Customer Terms & Conditions.

Program Manager

The Program Manager is a GPS customer who manages a card program.

The Program Manager signs up their customers for an account and can issue cards and other payment products on the GPS platform. They manage the relationship with their customers, and are responsible for customer on-boarding, Know your Customer (KYC)/Know your Business (KYB) and Anti-Money Laundering (AML) checks. The Program Manager is responsible for all customer communications and management of their customers.

Below are examples of what you need to do as a Program Manager:

- Your website/customer mobile application should provide a means for customers to contact you to report issues with cards or transactions on a card. You may need a separate Customer Relationship Management (CRM) system to manage customer queries. Your customer service staff can use the GPS Smart Client application to view transactions on a card, issue refunds and handle chargebacks. See the Smart Client Guide.
- You will need a payment service provider to take customer payments to fund the account. Alternatively, you can use the GPS Agency Banking service, which supports BACS, CHAPS, Faster Payments and SEPA [1].
- You should provide a Customer Portal/ mobile application where customers can sign in and manage their account. You can use the GPS web services API and real-time data from GPS data feeds to enable customers to self-service their account, for example: top up, move money between wallet accounts, link their mobile device to a card (e.g. ApplePay), upgrade their account, report a lost or stolen card, freeze a card and enquire on the balance in their account.

[1] Provided via our Modulr Agency Banking service.

- You should maintain a separate fee arrangement with your customers for usage of the cards and account service charges. GPS offers a Fees module which you can use to manage your card fees. See the Fees Guide.
- If you want to handle or process card details, such as the card's **Primary Account Number (PAN)**[1], you must be PCI DSS compliant. GPS provides a means to manage cards without needing to process the PAN, using a **Public Token**[2] (a unique 9 digit number that represents the card).

Key Responsibilities

- Card product design and development
- Card product management marketing
- Supply chain (ordering card plastics, personalisation and delivery)
- Technology development and testing
- Customer service
- Risk and analytics
- May hold the virtual balance of the card (if using EHI modes 1, 2, 4 or 5)

GPS

GPS has existing partner relationships and connections with schemes, issuers and card manufacturers, and is integrated with service providers such as 3D Secure, Agency banking, Multi-currency Foreign Exchange (FX)[3] and mobile wallet token providers.

GPS provides a flexible system, called GPS Apex, for creating, managing and processing transactions on multi-wallet physical and virtual cards. The system enables Program Managers to set up their card program and configure how their cards will be used. The system can also apply card usage fees on behalf of the Program Manager.

The GPS Apex platform provides integrated support for key add-on services such as 3D secure authentication, Multi-FX, mobile wallet virtual cards/tokenisation, Chargeback management and Fraud mitigation.

---

[1]The card's 16-digit permanent account number (PAN) that is typically embossed on a physical card.
[2]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.
[3]Multi-currency FX is provided via our CurrencyCloud service.

The Agency Banking solution provides a means for Program Managers to fund their customer card/wallet accounts through bank transfers (BACS, CHAPS, Faster Payments and SEPA).

Support is provided through your GPS Business Development Manager and Implementation Manager during the project initiation and integration stages, and from your Account Manager once you are live.

Note: One key aspect of the GPS solution is the dedicated customer support provided at all stages of a project. GPS works closely with you to configure the system to your requirements, and integrate any additional services required.

Key Responsibilities

- Payments and database infrastructure
- Database management, transaction authorisation, card activation
- Scheme mandate compliance, certification and accreditation[1]
- Maintains the card balance and transaction history if required (EHI modes 2, 3 or no EHI)
- Connections to card manufacturers
- Reporting
- Product functionality support and velocity controls
- Fee structure

Card Manufacturer

GPS has existing partner relationships and plug-ins to over 40 card manufacturers worldwide and can support local card creation programs in regions worldwide. Check with your Business Development Manager or Implementations Manager for details.

[1] We will update our systems to comply with scheme transaction processing mandates; it is the Issuer and Program Manager's responsibility to be aware of and comply with any additional scheme mandates (e.g., around fees, reporting and reconciliation).

GPS supports full Program Manager branded cards, with dynamic elements and EMV[1] configuration options.

You must have a separate commercial agreement with your card manufacturer. Cards are first pre-manufactured as blank cards. These cards contain the chips, antenna and blank magstripe[2].

> **Note:** During the initial pre-manufactured card setup stage, you should allow sufficient time for cards to be manufactured. (This can take a few weeks; please check with your card manufacturer for timelines.)
> Scheme testing may be required for new Chip profile configuration.

Once pre-manufactured cards are set up, you can use the GPS web services API to create physical card instructions, to send to your card manufacturer. These instructions include the personalised details to add to the cards for individual cardholders. See the Web Services Guide.

When the manufacturer receives the card creation instructions, they add the personalised data profile: they update the card's magstripe and Chip data, and print details on the card, such as the cardholder name, PAN, CVV2[3] and expiry date. (This process can take a few days.)*

Cardholder

When the cardholder signs up for your service, you should provide an online website/portal or customer mobile application which customers can use to manage their account, for example: configure their card options, query the balance on their cards, change PINs and load or unload cards.

You should provide your cardholder with a means to contact you with queries or issues related to their account and card service.

---

[1] EMV is a payment standard for smart payment cards, payment terminals and automated teller machines (ATMs). EMV is an acronym for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit Chips, in addition to magnetic stripes for backward compatibility.
[2] The card's magnetic stripe, which stores data on a band of magnetic material on the card. The magnetic stripe is read by swiping a magnetic reading terminal.
[3] The Card Verification Value 2 (CVV2) or Card Validation Code 2 (CVC2) on a credit card or debit card is a 3 digit number on VISA, MasterCard branded credit and debit cards. Cardholders are typically required to enter the CVV2 during any online or cardholder not present transactions.

1.2 Parties Involved in Transaction Processing

The figure below provides an overview of the key parties involved in processing transactions on a card.

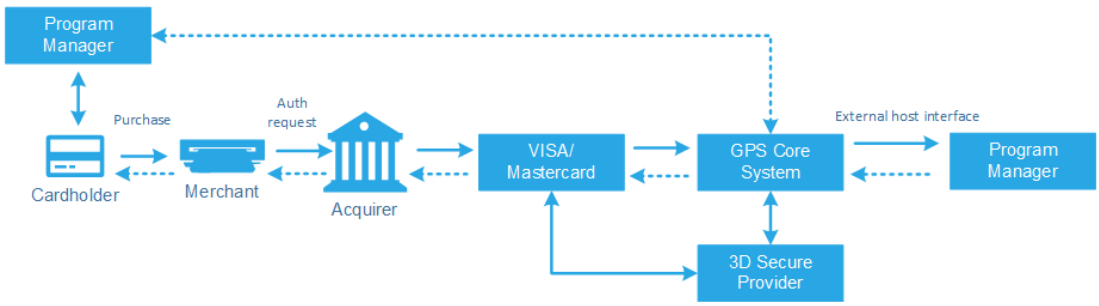

Figure 1-2: Key Parties in Processing Card Transactions

Each of these parties is described in further detail below (in the same order as shown in the figure above).

Program Manager (before the card is used)

The Program Manager must activate a card for it to be used. This is done via the GPS web services API. See the Web Services Guide.

Below are examples of what you need to do as a Program Manager to support card usage:

- Depending on your card offering, you can decide whether or not to activate the card on card creation. For example, for a virtual card, used on a mobile phone, the card can be activated for immediate use on creation. However, for a card that is printed and mailed to a customer, it may be advisable to require the customer to phone in or use your Customer mobile application to activate the card after it has been received.
- When a card is created, using the GPS web services API, you can link it to a GPS card product, which determines the card's usage settings. You can also link the card to card usage groups set up for your program. This determines where and how the card can be used. See Card Usage Groups.
- In EHI modes where GPS holds the card balance on your behalf, you must ensure the balance on the card reflects any customer money paid into or transferred out of their card account, or other balance adjustments made on the card account. You can use the GPS web services API to load/unload and

perform balance adjustments on a card. These web services will update the GPS cards database, where the transaction and balance ledger on the card is maintained. See the Web Services Guide..

Cardholder

The cardholder uses their physical or virtual card online or at a physical merchant shop (also called a Point of Sale (POS) transaction). They may use their card at an ATM (automatic teller machine) to withdraw money, change a PIN or run balance enquiries.

For POS transactions where the card is presented, the **POS terminal**[1] reads the **EMV**[2]/CHIP card configuration data. This data indicates how and where the card can be used.

During a Point of Sale (POS) transaction at a terminal, the cardholder may be asked to authenticate by entering a PIN into the terminal. During an online transaction, they may be asked to enter a One-Time Password (OTP) or use another method such as **Biometric authentication**[3] to verify their identity. For details, see the 3D Secure Guide.

GPS is compliant with the **Second Payment Service Directive (PSD2)**[4] regulations relating to how card transactions are handled and authenticated. Please contact your Business Development Manager for details.

---

[1] 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.
[2] EMV is a payment standard for smart payment cards, payment terminals and automated teller machines (ATMs). EMV is an acronym for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit Chips, in addition to magnetic stripes for backward compatibility.
[3] Biometrics are body measurements and calculations related to human characteristics that are unique to each person (such as face, eyes, voice and fingerprints). Biometrics authentication is used as a form of identification and access control.
[4] PSD2 is an EU Directive which sets requirements for firms that provide payment services. It introduces a number of requirements around how firms treat their customers and handle their complaints, and the data they must report to the FCA.

Merchant

The merchant is the business, shop or online website where the card is used. Each merchant is identified at the acquirer by a Merchant ID (MID) and assigned a **Merchant Category Code (MCC)**[1], which indicates the type of business and business sector they are trading in.

The merchant requests payment authorisation when a card is presented to them via a website, Mail and Telephone Order (MOTO) or at a Point of Sale (POS) terminal.

You can configure your card products to control card usage, for example to allow or deny card usage based on the MCC and limit usage of the card to the domestic country. For example: you can block card usage on gambling and adult sites, based on the MCC. You can also set up permission lists, to allow cards to be restricted for use to a list of specific Merchant IDs (for example, for a corporate card or gift card, which is limited to use at merchant sites linked to a specific shopping mall).

You should be aware that an authorisation request may not be for the full or final amount (e.g., a **preauthorisation**[2] or **partial authorisation**[3]) and may be followed by an **incremental authorisation**[4]. There may also be a delay of several days or more from when the authorisation is made to when the funds are requested by the merchant. (For example, when a card is used at a hotel or a car hire service, an initial amount may be authorised, followed by the final amount several days later).

There is no direct contact between merchants and Program Managers. Your customers should contact the merchant directly in the first instance for any issues or queries relating to an item or service purchased, and only contact your or their card issuer if the problem cannot be resolved.

---

[1] Merchant category codes (MCCs) are four-digit numbers that describe a merchant's primary business activities. MCCs are used by credit card issuers to identify the type of business in which a merchant is engaged.

[2] Transaction where the merchant requests authorisation for an initial or estimated amount. This may be followed by an Authorisation advice to confirm the final amount or authorisation requests for additional amounts.

[3] A transaction where the merchant requests authorisation for an initial or partial amount. This may be followed by authorisation requests for additional amounts.

[4] 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.

The GPS **Smart Client**[1] application enables your customer services staff to view transactions, issue refunds, block cards and raise **Chargebacks**[2] (Mastercard only). For details, see the Smart Client Guide.

Acquirer

An acquirer is typically a large banking organisation authorised to trade in a region, operating within a strongly regulatory framework, and with connections to the card schemes. They provide the banking licenses and accounts that enable merchants to take payments.

The merchant acquirer owns the relationship with the merchant and provides the **Merchant Account (MA)**[3] or **Internet Merchant Account (IMA)**[4] to the merchant. They may also provide the physical terminals that enable merchants to take in-store POS payments.

Acquirers send transaction authorisation and other financial messages to the card schemes. When GPS receives these messages from the card schemes, the GPS Apex system processes each message and then forwards to the Program Manager via EHI data feeds and/or transaction XML reports. See the External Host Interface (EHI) Guide and the Transaction XML Reporting Guide.

Acquirers are responsible for managing the settlement process on behalf of their merchants. They typically hold on to funds received via settlement from the issuers before passing the funds on to the merchant. Any dispute management and chargeback processes are managed between the acquirer and issuer, with the card scheme mediating between them. See the Payments Dispute Management Guide.

Acquirers charge fees for network transactions, which are reported with the transaction messages. GPS reports these charges to the Program Manager.

---

[1] 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.

[2] 0620 Message Transaction Identifier (MTID). This is a Token Event Notification (TEN) which indicates the token has been created. For more information, see the Tokenisation Service Guide.

[3] Merchant account, which an Acquiring bank provides to a merchant to enable them to take card payments.

[4] Online merchant account, which an Acquiring bank provides to a merchant to enable them to take card payments online.

Note: You will need a **payment services provider (PSP)**[1] and **Acquirer**[2] if you are taking card payments from your customers to load their accounts. This relationship is between you and the PSP and acquirer. GPS does not currently provide a direct PSP service.

Card Scheme

The card scheme provides the payment network over which card payments take place, receiving messages from acquirers and forwarding to GPS, and receiving authorisation responses from GPS and returning to the acquirer.

GPS currently supports Visa and Mastercard schemes. Both these schemes are global and allow their branded cards to be used worldwide. GPS is currently developing links to other global and local card schemes. Please contact your Business Development Manager for details.

When a transaction is received from an acquirer, the scheme checks the card's **Primary Account Number (PAN)**[3] to determine whether it is has an allowed **BIN**[4]. They may perform other fraud management checks. The scheme then forwards the transaction to GPS.

Where a **device PAN (DPAN)**[5] is being used (for example, for a virtual card mobile payment or tokenised service), the scheme converts the DPAN back to the PAN and forwards to GPS. See the Tokenisation Service Guide.

Both Visa and Mastercard provide additional services to cardholders, acquirers and issuers. See the table below.

Service	Scheme Platform	More Information
Chargeback Management	Mastercom Claims Manager	Payments Dis-

[1] An institution which offers payment services to customers, whether they are businesses or retail consumers. Includes banks, building societies, e-money institutions and payment institutions. As defined in the Payment Services Regulations 2017.
[2] 0100 Message Transaction Identifier (MTID). This is a Token Activation Request (TAR) message, requesting authorisation for the token creation. For more information, see the Tokenisation Service Guide.
[3] The card's 16-digit permanent account number (PAN) that is typically embossed on a physical card.
[4] The Bank Identification Number (BIN) is the first six numbers on a payment card, which identifies the institution that issues the card. Visa and Mastercard are changing to an eight digit BIN from April 2022.
[5] 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.

Service	Scheme Platform	More Information
	Visa Resolution Online (VROL)	pute Management Guide
3D Secure	Verified by Visa/Visa Secure and Mastercard Secure Code/ Mastercard Identity Check	3D Secure Guide
Tokenisation	Mastercard Digital Enablement Service (MDES) and Visa Token Service (VTS); GPS refer to the Visa service as the Visa Digital Enablement Program (VDEP).	Tokenisation Guide

GPS

GPS receives transaction authorisation messages and financial messages from the card schemes.

GPS provides initial validation and checking of messages: GPS checks the EMV details, the BIN, the card usage groups and allow/deny lists to confirm whether the transaction is allowed. GPS applies any card transaction fees (where the Program Manager is using the GPS Fees module).

GPS can support transaction authorisation for Program Managers who are using the External Host Interface (EHI); depending on the Program Manager's EHI mode, GPS handles authorisation requests or passes on to the Program Manager's systems for authorisation. EHI modes are flexible, and Program Managers can do a combination, for example where they authorise, but use GPS as a fallback if their systems are not available. For details, see the External Host Interface (EHI) Guide.

GPS reports authorisation decisions to the card scheme in real-time.

GPS provides both daily and real-time transactional data feeds to the Program Manager, which can be used for transaction matching and reconciliation. See the External Host Interface (EHI) Guide and the Transaction XML Reporting Guide.

Program Manager (when the card is used)

GPS can authorise transactions on your behalf where we hold details of the balance on the card (EHI mode 3, and also stand-in processing modes: EHI modes 2, 4, and 5 or where EHI is not being used).

Alternatively, you can maintain the card balance on your own systems and manage the authorisation decision (EHI mode 1) or use GPS as a fallback option for stand-in processing when your systems are not available (EHI modes 2, 4, and 5). For details of EHI modes, see Transaction Processing and EHI Modes.

Where GPS provides authorisation services and holds the card balance (e.g., EHI modes 3), you will need to update the card balance held by GPS to reflect card loads/unloads and balance adjustments. This is done using GPS web services. For details, see the Web Services Guide.

In EHI modes where you manage the authorisation decision, your systems must perform transaction matching and maintain a transaction and card balance database. For details, see the External Host Interface (EHI) Guide.

GPS can provide a Reconciliation service, powered by Kani, to support reconciliation and reporting. For more information, please contact your Account Manager.

3D Secure Provider

3D Secure is a protocol/program supported by the major card schemes, which provides Cardholder authentication during an online transaction.

3D Secure helps to reduce the risk of online fraud by requiring the cardholder to enter or provide some information or something that only they should possess:

Knowledge	Possession	Inherence
Something they know	Something they have	Something they are
Example: password or PIN.	Example: mobile phone, card reader or other device evidenced by a One-Time Password (OTP).	Example: fingerprint, face recognition or voice recognition.

GPS provides full 3D Secure support via Cardinal Commerce. Program Managers are set up with a Cardinal account and access to the Cardinal Portal for configuring their 3D Secure authentication rules and policies.

During an online transaction where 3D secure authentication is required, the card scheme sends the authentication request to Cardinal. Cardinal applies the policy rules, which the Program Manager has pre-configured, to determine whether the transaction can be seamlessly authorised without requiring cardholder input.

If further cardholder authentication is required, Cardinal notifies GPS, and GPS notifies the Program Manager to start the authentication session.

For more information, see the 3D Secure Guide.

2 The Role of GPS

This section provides an introduction to the role of GPS in enabling you to build and deliver a full card and digital payment program.

2.1 GPS as a Super Processor

The GPS Apex platform is an issuer-processor, which provides a comprehensive solution for you to manage your card program.

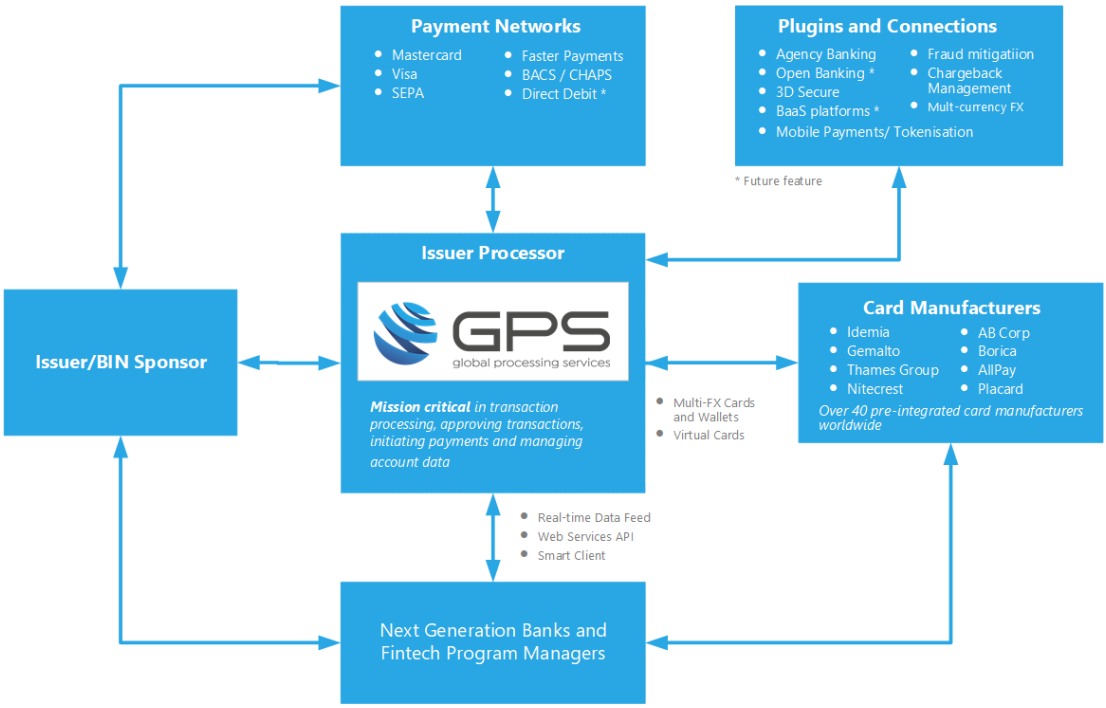

Figure 2-1: GPS as an issuer-processor

The GPS platform is integrated within the global payment network and has existing partner relationships and connections that reduces the time required to launch a card program. You can leverage the GPS payments ecosystem, thus reducing the amount of time-consuming and costly licensing, regulatory compliance, commercial agreements, infrastructure and connections.

GPS plays an essential role in helping our Program Managers understand the regulatory environment. We implement any changes needed to keep the GPS systems up-to-date and compliant with the latest regulatory changes, such as the **Payment Services Directive 2 (PSD2)**[1] and **Payment Card Industry (PCI) Data Security Standard**[2].

If you want to start issuing cards without becoming an **issuer**[3], you can use one of GPS's Issuer/BIN Sponsor partners in your region. For a list of pre-integrated issuers for your region, please contact your Business Development Manager.

GPS offers a global service, across Europe, North America, the Middle East and Asia Pacific regions, enabling you to expand your product offering as you grow. [4]

GPS currently supports Visa and Mastercard global payment networks. BACS, CHAPS, Faster Payments, and SEPA are available via our Agency banking solution.

Our cloud-based processing ensures resilience, scalability, reliability and fast processing, in whatever region you are processing.[5]

---

[1]PSD2 is an EU Directive which sets requirements for firms that provide payment services. It introduces a number of requirements around how firms treat their customers and handle their complaints, and the data they must report to the FCA.

[2]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 merchants who handle customer card data must be compliant with this standard. The PCI Standard is mandated by the Card Schemes, but administered by the Payment Card Industry Security Standards Council.

[3]The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant Card Scheme.

[4]For our current country-specific support and global roll-out roadmap, please contact your GPS Business Development Manager.

[5]We expect our AWS cloud service to be available by end of 2021 for our Asia Pacific customers.

2.2 GPS and the Transaction Processing Lifecycle

This section describes how card transactions are processed using GPS and how transactions on a card are managed during the lifecycle of a transaction.

Transaction Processing and EHI Modes

See the table below for details of how Program Managers can use the External Host Interface (EHI) to support transaction processing.

Mode	Who Authorises?	Who Maintains the Balance?	GPS Stand-In	Details
1	External Host	External Host	No	Your systems maintain the balance and perform authorisation.
2	GPS	GPS / External Host	Yes	GPS maintains the balance and performs authorisation. You can override an approval decision. In Approval with Load your systems maintain the balance and can update the GPS-maintained balance.
3	GPS	GPS	No	GPS maintains the balance and performs authorisation. You receive a read-only response.
4	External Host	External Host	Yes	Your systems maintain the balance and perform authorisation. GPS provides Stand-In authorisation if the external host is unavailable.
5	External Host	External Host	Yes	Your systems maintain the balance and perform authorisation. GPS provides Stand-In authorisation if the external host is unavailable. Clearing transactions, such as presentments, do not update the GPS stand-in balance.

For more information, see the External Host Interface (EHI) Guide.

Authorisation - When the Card is Used

The purpose of payment authorisation is to confirm that a card is valid for use at the requested merchant and location, and the requested amount is available on the card for spending.

Authorisations require a response in real-time (typically within milliseconds) to a request for authorisation.

Below are details of how an authorisation works, using two common scenarios:

- Where the Program Manager manages the authorisation decision
- Where GPS manages the authorisation decision

Program Manager Authorises (EHI modes 1, 2, 4, 5)

In EHI modes 1, 2 (approve with load), 4 and 5, the Program Manager is responsible for authorisation.

Pre-requisite to use these EHI modes:

- You maintain the card ledger balance on your own systems
- You must be able to respond to an authorisation request within the GPS system time limit[1]

See the example transaction flow below.

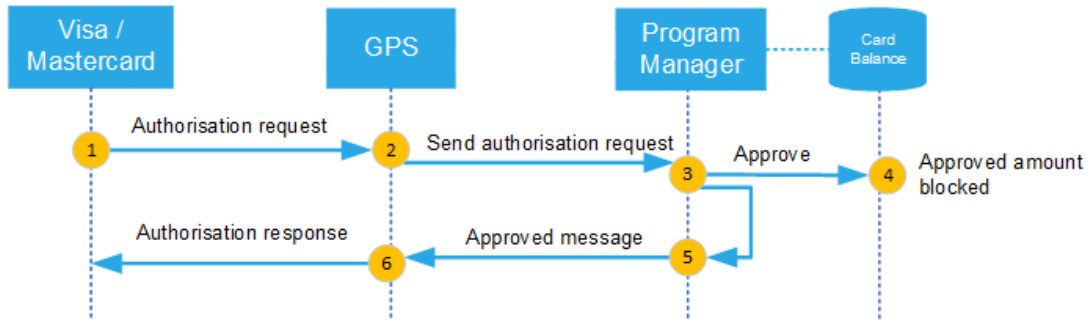

Figure 2-2: Authorisation Flow - Program Manager Approves

1. The scheme sends an authorisation request to GPS.
2. GPS carries out validation checks and sends the request to the external host (Program Manager).
3. The Program Manager approves the request. *

[1]The default system time limit may vary, depending on your region. Please check with your Business Development Manager.

4. The Program Manager blocks the approved amount (including fees) on the card and reduces the available balance.
5. The Program Manager returns an approved response.
6. GPS responds to the scheme with a message indicating approval.

*In the event that the Program Manager's systems are unavailable, GPS can support authorisation through Stand-In Processing (STIP)[1]. STIP options are available for EHI modes 4, and 5.

GPS Authorises (EHI modes 2 and 3)

In EHI mode 3, GPS provides the authorisation decision. EHI mode 2 provides a hybrid, where GPS can support the initial authorisation, but the Program Manager can override the decision.

You should use modes 2 or 3 if:

- You want to get up and running quickly without needing to build a card balance database
- Your systems are unable to respond with an authorisation decision within the time limit.

See the example transaction flow below.

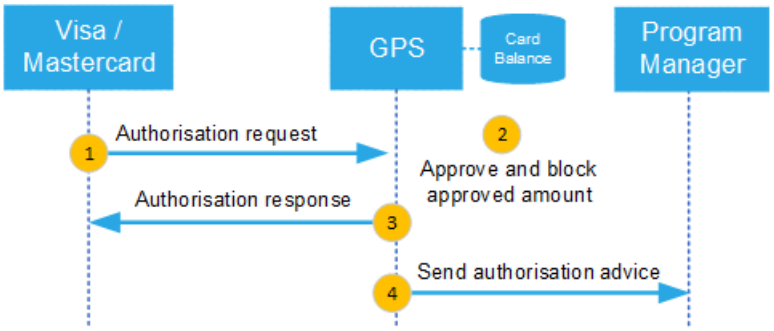

Figure 2-3: Authorisation Flow - where GPS Approves

1. The scheme sends an authorisation request to GPS.
2. GPS carries out validation checks and approves the request. GPS blocks the approved amount (including fees) on the card and reduces the available balance.

[1]The card network (Visa and Mastercard) may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your GPS mode, GPS may also provide STIP on your behalf, where your systems are unavailable. For more information, see the External Host Interface Guide.

3. GPS responds to the scheme with a message indicating approval.
4. GPS sends an authorisation advice to the external host (Program Manager).

2.2.3. Presentments – When Funds are Cleared

A presentment is a financial message provided in the second stage of the life cycle of a transaction.

In the previous stage the funds on the card were blocked by the authorised amount, ring-fencing this amount and reducing the balance on the card available for spending.

In the second stage, the card scheme receives a request from the merchant acquirer to take the authorised funds. This stage is called *clearing* and results in a clearing message or presentment being sent to GPS.

Visa and Mastercard send GPS daily batch clearing files[1]. GPS process the clearing files and send financial advices to the Program Manager. GPS refers to these financial advices as presentments.

When GPS receives the presentment message and sends it to the Program Manager using EHI, the Program Manager's systems should clear the block on the card and deduct the authorised amount. The issuer will then exchange the money with the acquirer, in a process called *settlement*.

> **Note:** Splitting of transactions into separate messages for authorisation and presentment is typical for card scheme networks in Europe, the UK, Middle East and Asia Pacific. In the USA, payment networks support both dual messages and also a single-stage process that combines the authorisation and presentment in a single message.

Below are details of how presentments are processed.

Where the Program Manager Approves (EHI Modes 1,2,4,5)

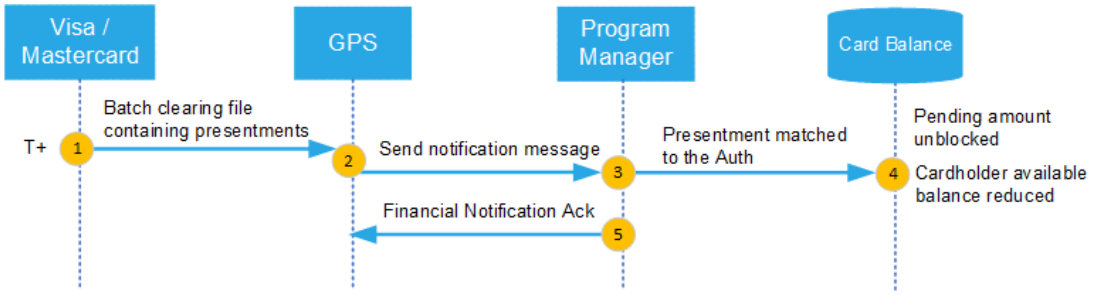

Figure 2-4: Presentment Stage - where Program Manager holds the balance

[1]Clearing messages are received based on the card scheme clearing cycles.

1. The scheme sends a batch clearing file to GPS.
2. GPS processes the file and sends a notification message per presentment, via EHI, to the external host (Program Manager).
3. The Program Manager matches the presentment to the original authorisation.
4. The Program Manager unblocks the pending amount and reduces the cardholder's available balance.
5. The Program Manager acknowledges the message.

Where GPS Approves (EHI mode 2, 3 or no EHI)

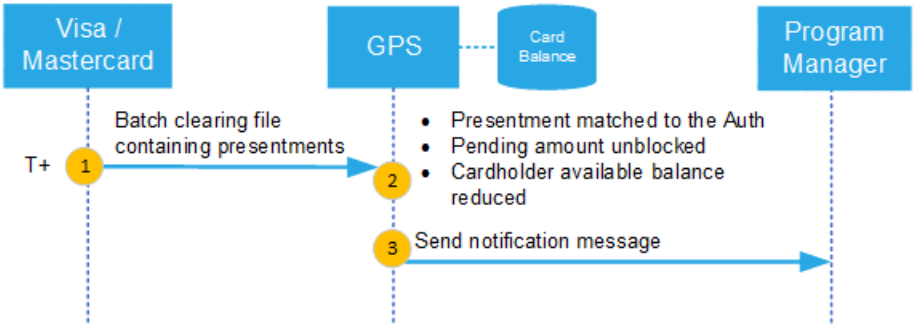

Figure 2-5: Presentment Stage - where GPS holds the balance

1. The scheme sends a batch clearing file to GPS.
2. GPS processes each financial record. GPS matches the presentment to the original authorisation, unblocks the pending amount and reduces the cardholder's available balance.
3. GPS sends a notification message per presentment, via EHI, to the external host (Program Manager).

2.2.4. Other Financial Messages

In addition to presentments, there may be other types of financial transactions that are linked to the original authorisation transaction. For example:

- Authorisation reversals
- Refunds
- Chargebacks

For details, see the External Host Interface (EHI) Guide.

3 GPS Architecture

This section describes the GPS system architecture and key components, as well as interfaces to third party services.

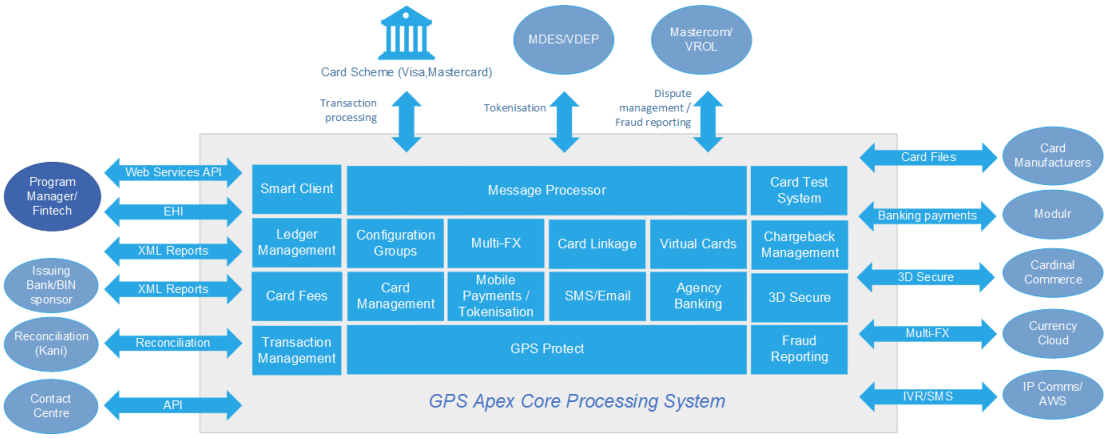

Figure 3-1: GPS System Architecture

The above figure shows the core components of the GPS Apex platform, together with interfaces to third-party service providers and partner systems. Below are details of the GPS platform components and services available to customers.

3.1 Core Processing Platform

GPS core processing services are part of the basic service available to GPS customers.

Message Processor

The GPS core Message Processor module performs a number of key roles:

- Receives and processes authorisation and financial messages from the schemes. Authorisation messages are received and processed in real-time.
- Runs internal transaction screening and validation checks on authorisation messages; processes messages according to the unique business logic configured for each GPS card program (e.g., per Issuer, program, product and card usage settings).

- Where GPS holds the card balance and provides the authorisation decision, then the system checks the internal card balance ledger to determine if sufficient funds are available and updates the balance ledger. The system can apply card fees at the same time (if you are using the GPS Fees module).
- Initiates other related services, such as authentication and transaction reporting.

Web Services API

The GPS Web services API is used by Program Managers to create and manage the accounts and cards in their program. Below are examples of functionality that can be managed using the API:

- Creating cards
- Linking cards to usage groups
- Card load and unload
- Card expiry and replacement
- Pin management
- Card activation
- Lost and stolen status
- Balance enquires and balance adjustments
- Card fees
- 3D Secure enrolment

Creating Cards

When you send a request to GPS to create a card, the GPS Apex system allocates an available card **PAN**[1] to the card. It generates a unique internal **Public Token**[2], which is linked to the card. The public token is returned in the GPS response and

[1]The card's 16-digit permanent account number (PAN) that is typically embossed on a physical card.
[2]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.

your systems can use this token for all subsequent queries and card management activities on the GPS system. This enables you to handle card requests without needing to process or store the full PAN (full PAN requires **PCI DSS compliance**[1]).

For more information, see the Web Services Guide.

Managing Cards

You can use the GPS web services to manage your cards. You can integrate the web services into your customer application, to provide your customers with self-service options to manage their account.

This includes services such as card blocking and unblocking, card expiry and upgrades, card replacement, switching from a virtual to a physical card, cards loads and balance transfers, PIN changes and queries.

For more information, see the Web Services Guide.

External Host Interface (EHI)

The External Host Interface (EHI) is a SOAP-based interface[2] which sends XML messages to the endpoint configured by the Program Manager. The Program Manager's systems pick up these messages and can respond and process, based on their EHI mode.

EHI plays an important role in processing real-time authorisation and financial messages. There are five supported EHI modes; see Transaction Processing and EHI Modes. The EHI mode determines who is responsible for payment authorisation and who maintains the card balance ledger.

For more information, see the External Host Interface (EHI) Guide.

XML Reporting

The GPS Apex system provides a number of XML reports to Program Managers and Issuers, which can be used to support transaction matching and reconciliation:

- **Transaction XML Report** – daily report that provides all transaction records processed that day (both authorisation and financial messages). The Program Manager can use this report to check the transactions reported and

[1]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 merchants who handle customer card data must be compliant with this standard. The PCI Standard is mandated by the Card Schemes, but administered by the Payment Card Industry Security Standards Council.
[2]JSON format option is also available.

reconcile against details in their own card database/ received from EHI. See the Transaction XML Reporting Guide.

- **Balance XML Report** – daily report that provides the balance on all cards in the Program Manager's program. The Program Manager can use this report to check the balance and update or reconcile against details in their own card database. See the Balance XML Reporting Guide.

GPS provides additional reports to issuers and self-issuers:

- **Fee Collection Report** – gives a summary of Scheme (VISA/Mastercard) Fees by ICA and currency.
- **Quarterly Management Report (QMR)** – contains information needed to complete your regulatory Quarterly Management Report for Mastercard. The Visa equivalent Quarterly Operating Certificate (QOC) can be provided on request.

Charges for additional reports may apply. Check with your GPS account manager for details.

Smart Client

Smart Client is a software application that can be installed on a personal computer (PC), which provides a front-end administrative tool for viewing and managing transactions on the cards in your program. Users can perform actions such as transaction and card queries, card loads and unloads, balance enquiries and adjustments, and view and manage chargebacks. Chargeback reporting and SAFE reporting[1] is available (Mastercard only).

For more information, see the Smart Client Guide.

Card Transaction System (CTS)

The Card Transaction System (CTS) can be used to put through simulation transactions in the UAT environment. The simulation transactions generate EHI messages and can be used to test your end-to-end EHI integration and message handling.

For more information, see the Card Tranaction System (CTS) Guide.

[1]SAFE (System to Avoid Fraud Effectively) is a Mastercard initiative requiring card issuers to report all cardholder fraud claims. The data sent to Mastercard is used to help identify and track fraudulent activity.

GPS Protect

GPS Protect is a fraud-management service that enables you to set up powerful configuration rules for handling of transactions in almost real-time. GPS protect receives transaction data from the GPS Apex system and makes automated decisions based on the business logic you have configured.

Check with your GPS account manager for details.

GPS Fees

The GPS Fees module is an optional service that enables you to apply fees to the cards in your program. Fees are managed via Fee Groups. Separate fee groups are available for:

- Authorisation fees
- Recurring fees
- Web Service usage fees

You can link a card to a Fee Group and also apply ad-hoc or one-off fees.

For more information, see the Fees Guide.

3.2 Plug-ins and Services

This section describes GPS connections to third party service providers.

Card Manufacturers

GPS has existing partner relationships with over 40 card manufacturers worldwide. We provide a pre-integrated service and interface to these card manufacturers.

The GPS Web services API are used to raise card creation requests. GPS sends card files to the card manufacturer, which contain the instructions for generating the cards in your program.

You will need to sign a separate agreement with your card manufacturer. Please contact your Business Development Manager or Implementation Manager for advice on suitable card manufacturers for your region/service.

For details of using web service to create card instructions, see the Web Services Guide.

3D Secure Cardholder Authentication

3D Secure is a protocol/program supported by the major card schemes, which provides Cardholder **authentication**[1] during an online transaction.

GPS provides full 3D Secure support via Cardinal Commerce. Program Managers are set up with a Cardinal account and access to the Cardinal Portal for configuring their 3D Secure authentication rules and policies.

For more information, see the 3D Secure Guide.

Chargeback Management

Chargebacks are supported via the relevant card scheme (e.g., MasterCard or Visa); both schemes provide online systems where issuers and acquirers can view and respond to chargeback notifications.

Smart Client provides a facility to enable Program Managers to raise and manage chargebacks (Note that this is only available for Mastercard issuers in Europe/UK at present).

For more information, see the Payments Dispute Management Guide.

---

[1] This includes checks to verify the cardholder's identity, such as PIN, CVV2 and CAVV, as well as 3D Secure authentication.

Mobile Payments and Tokenisation

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**[1]) 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)**[2].

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

For more information, see the Tokenisation Service Guide.

Fraud Reporting

The GPS **SAFE Reporting**[3] facility on Smart Client enables Program Managers to report suspected fraudulent transactions to Mastercard.

For more information, see the Fraud Reporting Guide (Mastercard).

Agency Banking

This service is provided via Modulr. It enables support for bank account type features such as BACS, CHAPS, Faster Payments and SEPA. For more information, please contact your Account Manager.

Program Managers can use the web services API to register their customers for agency banking. For more information, see the Web Services Guide.

---

[1]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.
[2]The 16-digit PAN of the card, which Mastercard/Visa converts when authorisations come through to them from Acquirers on the DPAN. For more information, see the Tokenisation Service Guide.
[3]SAFE (System to Avoid Fraud Effectively) is a Mastercard initiative requiring card issuers to report all cardholder fraud claims. The data sent to Mastercard is used to help identify and track fraudulent activity.

Reconciliation

GPS can provide a Reconciliation service, powered by Kani, to support Program Manager reconciliation and reporting. For more information, please contact your Account Manager.

Multi-Currency FX

GPS provides the ability to manage multiple currency balances on a single card. You can configure which currencies are available and the fees associated with transactions, loads and FX. GPS also provides an FX rate API that enable customers to get the current FX rates available.

GPS has partnered with CurrencyCloud to provide a solution that provides competitive real-time rates at point-of-sale as well as weekend FX rates and direct FX currency settlement with the card scheme (Visa only). *

* Service coming soon. Please check with your GPS Business Development Manager for timelines.

4 Setting up a Program with GPS

This section provides an overview of what you need to get started and describes the data model of setting up a program in the GPS system.

Note: For information about the steps in a typical project, see the Getting Started Guide.

4.1 What you need to Get Started

Issuer/BIN-sponsor

The issuer provides GPS with the card BIN ranges (the first 6 or 8 digits of the long card number), which are used to generate the card PANs used in a card program. The issuer has an existing relationship with the card scheme, who authorises them to use cards in this BIN range.

You can use the services of an existing Issuer or become self-issuing.

For advice on which option may be best for your organisation, please contact your Business Development Manager.

Payment Service Provider or Agency Banking Service

If your customers are funding their account via card payments, you will need to use the services of a Payment Service Provider (PSP). Alternatively, the GPS Agency Banking module provides an option to process payments and bank transfer payments via BACS, CHAPS, Faster Payments and SEPA.

Client money linked to your cards must be held in a separate, ring-fenced bank account, which is protected in the event your business fails.

For details, please contact your Business Development Manager.

Card Manufacturer

If you are providing your customers with physical cards, then you will need to sign a commercial agreement with one of the card manufacturers which GPS supports. For details, please contact your Business Development Manager.

Note: To use a card manufacturer not currently integrated to GPS, please discuss with your Business Development Manager or Onboarding Manager.

4.2 GPS Data Model

The figure below provides an example of the typical data hierarchy when setting up a new program on the GPS system.

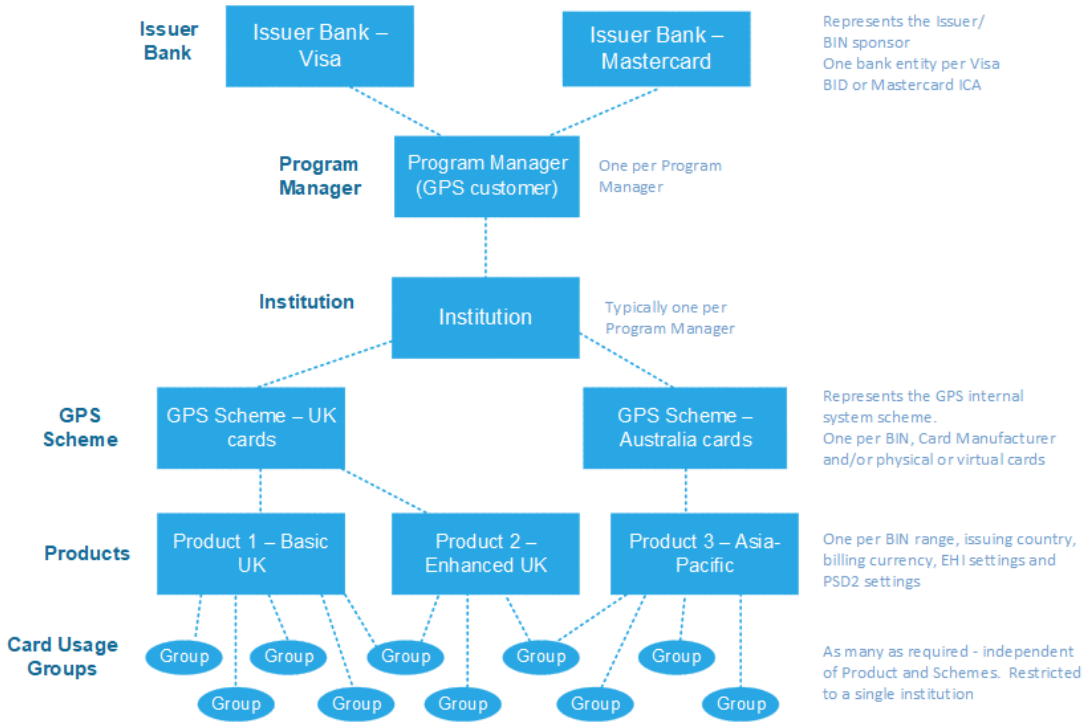

Figure 4-1: Setting up an Account with GPS

Each GPS customer (Program Manager) is set up under an Issuer Bank and Institution. The Institution is linked to a Program Manager.

The Program Manager account may consist of multiple GPS Schemes; these are required if supporting multiple **BINs**[1] or more than one card manufacturer; separate GPS Schemes may be required if you want to create both physical and virtual cards.

GPS Schemes are links to card *Products*. A card product provides most of the configuration options relating to a card. Separate card products are required per issuing country, billing currency and supported EHI mode.

Card *Usage Groups*, which define how the card can be used, are assigned at card level, and can be linked to more than one card product.

Each level of the hierarchy enables different configuration options to be set. See below for details.

[1]The Bank Identification Number (BIN) is the first six numbers on a payment card, which identifies the institution that issues the card. Visa and Mastercard are changing to an eight digit BIN from April 2022.

Bank

The bank represents the issuing bank (**BIN Sponsor**[1] or **IIN**[2] sponsor). A separate bank entity must be set up for each card scheme (i.e., per Visa BID or Mastercard ICA[3]) and region.

A bank can be linked to multiple Institutions, which is managed at card product level.

Configuration options defined at this level
Member ID (5 or 6 digits for Mastercard and 8 digits for Visa).
Chargeback interfaces
Card scheme reporting
Tokenisation keys (VDEP/MDES)

Institution

An institution represents an organisation set up on the GPS system, such as a Program Manager, Bank or Card Manufacturer. Typically, one is set up per Program Manager.

Configuration options defined at this level
Chargeback reporting
Settlement reporting
Issuer Summary report
SAFE reporting (Mastercard only)

[1]Issuer, who creates the BIN range used by the Program Manager.

[2]The Issuer Identifier Number (IIN) Bank is the term used in countries such as Japan for a Bank Identification Number (BIN); this is the first four or six numbers on a payment card, which identifies the institution that issues the card.

[3]An ICA can be unique or shared Visa only allow 1 BID per issuer, per region.

Program Manager

One Program Manager account is set up per GPS customer. Each Program Manager is assigned a unique Program Manager code. This code is included in all web service requests. A Program Manager is linked to an Institution.

Configuration options defined at this level
Web services SOAP credentials
PGP[1] keys for virtual cards

GPS Scheme

This is an internal GPS scheme which defines some features of the card program. It is linked to an Institution.

One GPS scheme is set up per BIN and Card Manufacturer. If you want to support both physical and virtual cards, these must be set up as separate GPS Schemes.[2]

You can have multiple GPS schemes for different setups (e.g., if you use multiple card manufacturers, you will need a different scheme for each manufacturer).

Configuration options defined at this level
Card validity period
Card activation method
BIN (6-8 digit)
Card features (e.g., Magnetic or CHIP)
Card Manufacturer

Products

One product is set up per BIN range, issuing country, billing currency, EHI settings and PSD2. A global program can have hundreds of products.

---

[1] Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

[2] Conversion from Virtual to Physical cards can be supported on the same GPS Scheme.

A product is linked to an Issuing Bank.

Cards are linked to a product, which is defined by a unique Product ID.

Configuration options defined at this level
Product type
Card type
Card details: Embossed name, default usage groups
Card scheme (Visa, Mastercard)
Billing currency
Physical card layout
BIN range
Card acceptor list
PSD2 setup
Risk Management settings

Card Usage Groups

Card usage groups are used to control what the cardholder is able to do with the card, as well as the various card usage fees that are charged to the cardholder. See the table below.

Group	Description
Limit Groups	Velocity limit group which restricts the frequency and/or amount at which the card can be loaded or unloaded. You can view your current Limit Groups in Smart Client.
Authorisation Fee Groups	Group which controls the card transaction authorisation fees.
Recurring/Scheduled Fee Groups	Controls whether a card is charged a recurring fee, such as a monthly platform fee.
Web Service Fee Groups	Controls the fees charges for web service usage. Different web services can have different fees associated with them.
MCC Groups Merchant Category Code (MCC)	The MCC is a four-digit number used by the Card Schemes to define the trading category of the merchant.

Group	Description
Group	
Usage Groups	Group that controls where a card can be used. For example: POS or ATM.
Linkage Groups	The Linkage Group set up in Smart Client controls various parameters related to linked cards; for details, check with your Implementation Manager.
FX Groups	Controls the rates for FX currency conversions if the purchase currency is different from the card's currency.
Auth Calendar Groups	Controls the dates time when authorisations on a card are allowed. You can use this option to control when the card can be used, for example, prevent usage on weekends or out of hours.
Payment Token Usage Groups	Defines configuration options specific to the provisioning of a digital payment token. For details, see the Tokenisation Service Guide.

Notes

- Groups can be shared across multiple Products within an Institution. You can set up as many groups as required.
- You can use the web services API to assign a card to card usage groups at the time of the card creation and also to change the card usage group assigned to the card at a late stage if needed.
- When you create a card on the GPS system, if you do not specify which groups to link to the card, then the groups of the linked card Product are used.

5 Use Case Scenarios

This section provides example use cases illustrating how Program Managers can implement their service through GPS. It covers three common business cases:

- Prepaid Card Service
- Neobank/ Digital Banking
- Agency Banking

Note: Company names and examples provided here are fictional and for illustrative purposes only.

5.1 Prepaid Card Service

This use case is for a typical Fintech offering a prepaid card service.

Business proposition

SchoolCard is a new fintech company offering a simple prepaid card service for use in schools, colleges and universities across the UK. The cards are able to be used in school and campus canteens and to purchase products at participating merchant stores. SchoolCard provides features such as student rewards and loyalty discounts. Users are able to top up funds on the card and the educational faculty are able to use the cards to provide rewards to students.

Service architecture

Below is an example of the setup for the SchoolCard prepaid card service:

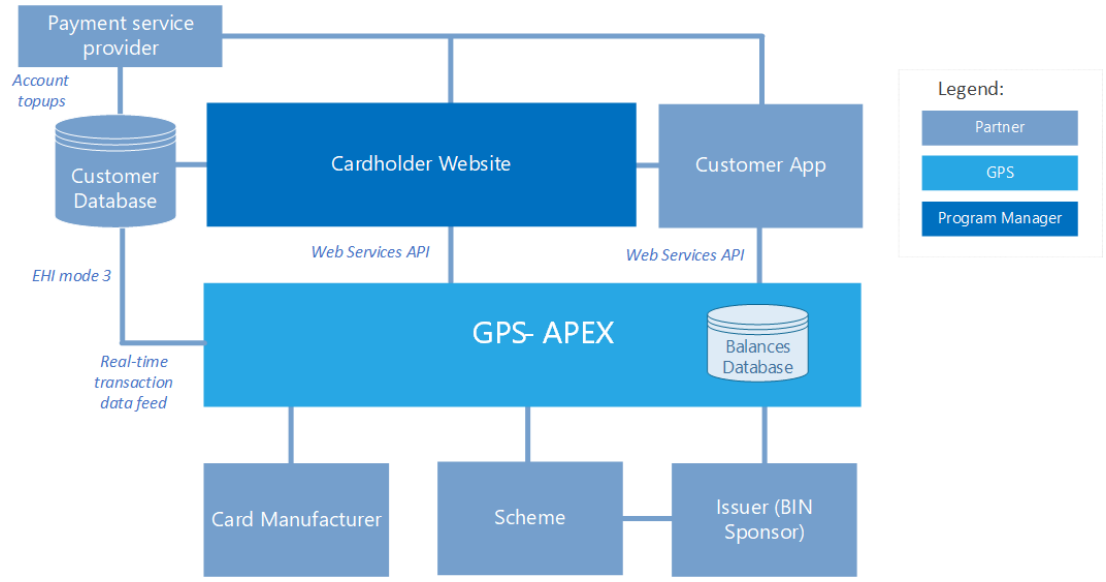

Figure 5-1: Prepaid Card Service

Service implementation

SchoolCard offers a Customer Portal, where customers can sign up for the card and manage their account (e.g., top-up and activate cards). For customers with Smart Phones, SchoolCard has a Customer App that can be downloaded and used to manage the card. The Customer Portal and mobile app use the GPS web services API to connect to GPS for card services.

All other aspects of the service are provided via GPS and third-party partners:

- SchoolCard use the service of an existing issuer (BIN Sponsor).
- They hire a software firm to develop a customer mobile app, to enable the service to be managed from a mobile phone.
- They sign an agreement with a local card manufacturer who is pre-integrated to GPS, for printing and postage of branded cards to educational institutions. The cards can then be distributed to students. Student users must use their app or Customer Portal to activate the card and load with funds.
- SchoolCard is set up in the GPS system with a simple, single card product configuration, supporting a single currency (GBP). Card usage groups are used to control the features of the card, such as where and how it can be used; usage groups are assigned dynamically at card creation. SchoolCard use the GPS fees module to charge a small one-off setup fee and an annual card usage fee.
- Users can top up their account using the SchoolCard payment service, supported via a third-party payment service provider.
- When the card is used at supporting stores, GPS provides full card authorisation and management of the card balance (EHI mode 3).

5.2 Neobank/ Digital Banking

Below is an example of the setup for a typical Neobank offering a digital banking service.

Business proposition

Sunrise Bank is a new bank, being launched in the Middle East. The service offers a digital account and multi-currency wallet functionality, enabling cards to be used in countries across the Middle East.

Service architecture

Below is an example of the setup for the Sunrise Bank digital banking service:

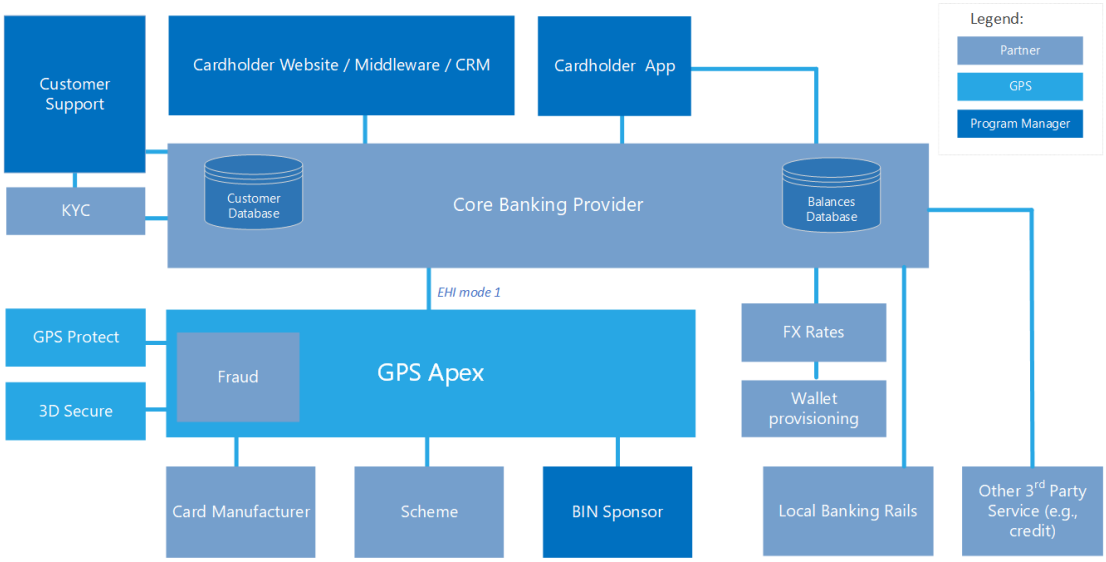

Figure 5-2: Neobank Digital Banking Service

Service implementation

- Sunrise Bank is self-issuing. They have an agreement with their card scheme to issue BIN ranges.
- The bank provides its own in-house CRM, Customer Support and Cardholder mobile App.
- Customer identity, address verification and PEPs checks are carried out by a third-party service provider.
- They sign an agreement with a local card manufacturer for printing and postage of cards to cardholders.

- Since they are supporting multiple countries and currencies, they will need a separate card product set up in GPS for each currency and issuing country. For details, see the GPS Data Model.
- The bank manages card authorisation and updates to the card balance (EHI mode 1).
- The bank manages any fees and charges to customers for using their service.
- GPS provide fraud management services using GPS protect and cardholder 3D Secure authentication.

5.3 Agency Banking

This use case is for a typical Agency Banking service.

Business proposition

SafeHorizons is a new fintech, offering an Agency Banking solution and debit card for overseas students and workers who cannot obtain a UK bank account and want to have their salaries paid into a local debit card account, for use in the UK.

Customers can load funds onto their SafeHorizons account using Faster Payments (one-off, flexible payments) or via direct debit (regular, fixed amount payments). Once in their account, the funds are available for use on the UK debit card.

Service architecture

Below is an example of the setup for a typical Agency service:

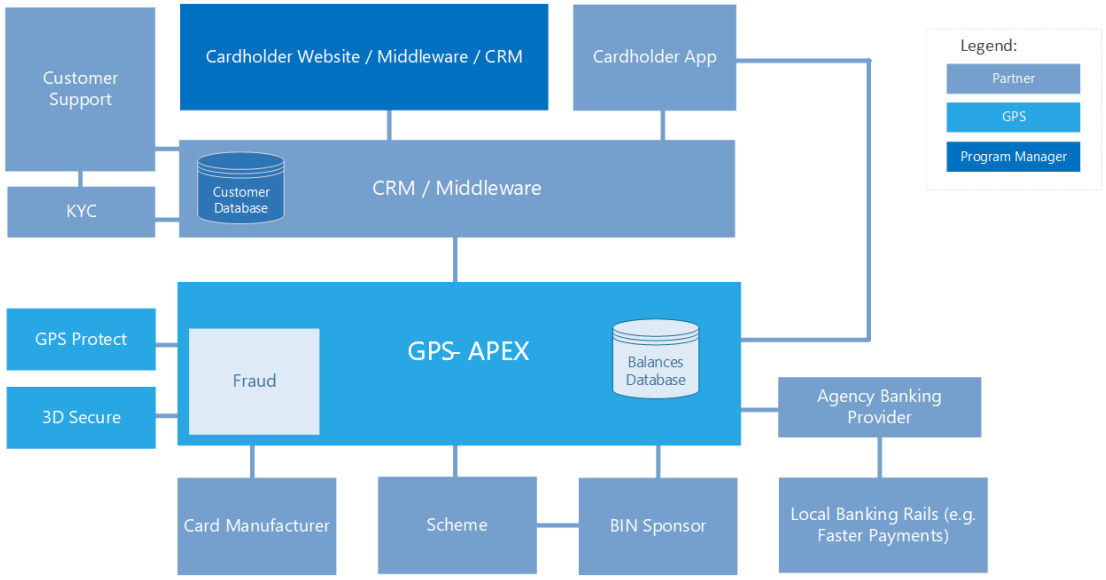

Figure 5-3: Agency Banking Service

Service implementation

- SafeHorizons use the services of an existing issuer that has agreement with the card scheme to issue BIN ranges in a number of countries.
- SafeHorizons use a third-party service for Customer Relationship Management (CRM) and Customer Support. Their cardholder mobile App is also developed by a third-party provider of app services.
- Customer identity, address verification and PEPs checks are carried out by a third-party service provider.

- SafeHorizons sign agreements with a local UK card manufacturer, for printing and postage of cards to cardholders.
- SafeHorizons use the GPS Agency Banking service via Modulr to provide their customers with a means to top up their debit card account via Faster Payments, and transfer money out of their wallet using Faster Payments.
- When the card is used at supporting stores, GPS provides full card authorisation and management of the card balance (EHI mode 3). GPS also provides advices on banking payments made via the Agency Banking service.
- They use the GPS fees module for managing card service and usage charges.
- GPS provide fraud management services using GPS protect and cardholder 3D Secure authentication.

Glossary

0

0100 Message

0100 Message Transaction Identifier (MTID). This is a Token Activation Request (TAR) message, requesting authorisation for the token creation. For more information, see the Tokenisation Service Guide.

0620 Message

0620 Message Transaction Identifier (MTID). This is a Token Event Notification (TEN) which indicates the token has been created. For more information, see the Tokenisation Service Guide.

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

Access Code

Passcode or activation code which you supply to GPS. You can use the access code to authenticate user access to card services or to request a user to activate the card by entering their access code.

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 (CAN)

Activation Code Network Message. The message sent to GPS and also the Programme manager via EHI which contains the One Time Password (OTP) to verify the cardholder. For more information, see the Tokenisation Service Guide.

Address Verification Service (AVS)

An AVS check compares the billing address used in the transaction with the issuing bank's address information on file for that cardholder. Depending on whether they match fully, partially, or not at all, the merchant can use that information in their decision on whether or not to accept or cancel the order. AVS is one of the most widely used fraud prevention tools in card-not-present transactions.

Anonymous Transactions

Transactions such as for prepaid gift cards where the cardholder's identify is not known

Arbitration

Process of managing disputes raised between merchants and cardholders, where the dispute cannot be resolved. The arbitration process is managed by the card scheme, who will make the final decision. For more information, see the Payments Dispute Management Guide.

Auth Calendar Group

Controls the dates and times when authorisations on a card are allowed. You can use this option to control when the card can be used, for example, prevent usage on week-ends or out of hours. For more information, see the Web Services Guide.

Authentication

This includes checks to verify the cardholder's identity, such as PIN, CVV2 and CAVV, as well as 3D Secure authentication.

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

Bank Identification Number (BIN)

The Bank Identification Number (BIN) is the first six numbers on a payment card, which identifies the institution that issues the card. Visa and Mastercard are changing to an eight digit BIN from April 2022.

BIN Sponsor

Issuer, who creates the BIN range used by the Program Manager.

Biometric Authentication

Biometrics are body measurements and calculations related to human characteristics that are unique to each person (such as face, eyes, voice and fingerprints). Biometrics authentication is used as a form of identification and access control.

C

Card Linkage Group

The Linkage Group set up in Smart Client controls various parameters related to linked cards; for details, check with your Implementation Manager.

Card Manufacturer

GPS has relationships with existing card manufacturers, who we can instruct to print your cards. We use Secure FTP (sFTP) to send the card manufacturer a generated bulk XML file containing card details. This is sent on a daily basis, or at a frequency that can be customised for your service. The card manufacturer prints the cards and sends to the cardholder. Any white label test cards are typically sent to GPS, the Program Manager and the Card Schemes.

Card Scheme

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

Cardholder

Consumer or account holder who is provided with a card to enable them to make purchases.

Cardinal Commerce

Cardinal Commerce provide an Access Control Server (ACS) that enables support for the 3D Secure cardholder authentication scheme. See: https://www.-cardinalcommerce.com

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction.

Chip and PIN

Chip and PIN is a verification method used by payment cards which comply with the EMV standard. The cardholder enters a personal identification number (PIN), typically of 4 to 6 digits in length. This number must correspond to the information stored on the chip. This improves the security of the card, since only the cardholder should know the PIN.

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.

CVV2/CVC2

The Card Verification Value 2 (CVV2) or Card Validation Code 2 (CVC2) on a credit card or debit card is a 3 digit number on VISA, MasterCard branded credit and debit cards. Cardholders are typically required to enter the CVV2 during any online or cardholder not present transactions.

D

Device PAN (DPAN)

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

EMV

EMV is a payment standard for smart payment cards, payment terminals and automated teller machines (ATMs). EMV is an acronym for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit Chips, in addition to magnetic stripes for backward compatibility.

European Banking Authority (EBA)

The EBA is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.

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.

External Host Interface (EHI)

The External Host Interface provides a facility to enable exchange of data between GPS and external systems via our web services. All transaction data processed by GPS is transferred to the External Host side via EHI in real time. For certain types of transactions, such as Authorisations, the External Host can participate in payment transaction authorisation.

External Host Interface (EHI) mode

For authorisation type of transactions, the External Host Interface (EHI) can operate in one of five modes: Mode 1 the External Host maintains card balances and participates in transaction authorisation by approving or declining the transaction. Mode 2 - GPS maintains balances and performs all types of the authorization, but the External Host can overrule in some circumstances. Mode 3 - read-only data feed from the GPS system to the Client's system. Mode 4 - External Host maintains Balance (with GPS stand-in). Mode 5 – Same as EHI Mode 4, but clearing transactions do not update the GPS stand-in balance. For more information, see the External Host Interface Guide.

F

Fee Groups

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

Fee Types

A card usage fee type that defines the fees that are applied to a specific type of transaction, such as a debit card payment or an ATM withdrawal. A Fee Group will consist of one or more fee types. For more information, see the Fees Guide.

Financial PAN (FPAN)

The 16-digit PAN of the card, which Mastercard/Visa converts when authorisations come through to them from Acquirers on the DPAN. For more information, see the Tokenisation Service Guide.

Fraud Rate

The fraud rate is the percentages of transactions received by the acquirer which are identified as fraudulent. For example, if 10,000 transactions per day are received, and 10 of these are identified as fraudulent, the fraud rate would be 0.01.

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.

Hard Decline

A transaction decline which indicates that the card was declined by the issuing bank or card processor due to the card not being valid (e.g., lost, stolen or expired). It indicates to the merchant that they should not retry the transaction on the card.

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.

Internet Merchant Account (IMA)

Online merchant account, which an Acquiring bank provides to a merchant to enable them to take card payments online.

Issuer

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

Issuer Identifier Number (IIN)

The Issuer Identifier Number (IIN) Bank is the term used in countries such as Japan for a Bank Identification Number (BIN); this is the first four or six numbers on a payment card, which identifies the institution that issues the card.

M

Magstripe

The card's magnetic stripe, which stores data on a band of magnetic material on the card. The magnetic stripe is read by swiping a magnetic reading terminal.

Mail and Telephone Order (MOTO)

Transaction where payment instruction is taken over the telephone or via a mail order. Since the cardholder is not present, these are classed as "Cardholder Not Present" transactions.

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 Account (MA)

Merchant account, which an Acquiring bank provides to a merchant to enable them to take card payments.

Merchant Category Code (MCC)

Merchant category codes (MCCs) are four-digit numbers that describe a merchant's primary business activities. MCCs are used by credit card issuers to identify the type of business in which a merchant is engaged.

MIP

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

MTID

The Message Type Identifier (MTI) is a four digit number used for card originated financial transactions. For each message, it identifies: version number, message class, message function and transaction originator. The MTI standard is defined by ISO 8583.

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.

One-Leg-Out transactions

Occurs when one of the payment service providers (either the payer or payee) is outside the European Union (EU). If the Acquirer is from outside the EU and the payer is from the EU, the Acquirer does not need to comply with PSD2 regulations

Online PIN

With online PIN, the PIN is encrypted and verified online by the card issuer. This is in contrast to offline PIN, where the PIN is verified offline by the EMV chip card.

Original Credit Transactions (OCT)

Transaction that can be used to send funds to a card-based account, resulting in a credit of funds to the cardholder's account.

P

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.

Partial Authorisation

A transaction where the merchant requests authorisation for an initial or partial amount. This may be followed by authorisation requests for additional amounts.

Payment Card Industry (PCI) Data Security Standard

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 merchants who handle customer card data must be compliant with this standard. The PCI Standard is mandated by the Card Schemes, but administered by the Payment Card Industry Security Standards Council.

Payment Services Directive 2 (PSD2)

PSD2 is an EU Directive which sets requirements for firms that provide payment services. It introduces a number of requirements around how firms treat their customers and handle their complaints, and the data they must report to the FCA.

Payment Services Provider (PSP)

An institution which offers payment services to customers, whether they are businesses or retail consumers. Includes banks, building societies, e-money institutions and payment institutions. As defined in the Payment Services Regulations 2017.

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.

Preauthorisation

Transaction where the merchant requests authorisation for an initial or estimated amount. This may be followed by an Authorisation advice to confirm the final amount or authorisation requests for additional amounts.

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Primary Account Number (PAN)

The card's 16-digit permanent account number (PAN) that is typically embossed on a physical card.

Product Setup Form (PSF)

The Product Setup Form is a spreadsheet that provides details of your GPS account setup. The details are used to configure your GPS account.

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.

Project Initiation Document (PID)

The Project Initiation Document (PID) is put together at a start of a project. This document outlines the initial project requirements and parties involved.

Project Requirements Document (PRD)

The Project Requirements Document (PRD) provides full details of the requirements of your project. Project schedules and implementation are based on the details provided in this document.

Project Scoping Document (PSD)

The Project Scoping Document (PSD) defines the scope of the project and is typically produced before the start of the project.

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.

R

Recurring Transaction

Recurring transactions are multiple transactions processed at predetermined intervals, representing an agreement between a customer and a merchant to take payments over a period of time. Typically, SCA is performed on the first transaction, while subsquent transactions are treated as cardholder not present and not subject to SCA.

S

SAFE Reporting

SAFE (System to Avoid Fraud Effectively) is a Mastercard initiative requiring card issuers to report all cardholder fraud claims. The data sent to Mastercard is used to help identify and track fraudulent activity.

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.

SOAP

SOAP (Simple Object Access Protocol) is a messaging protocol for exchanging structured information in the implementation of web services. It uses Extensible Markup Language (XML) for its message format and relies on application layer protocols such as HTTP for message negotiation and transmission. SOAP allows developers to invoke processes running on disparate operating systems (such as Windows, macOS, and Linux) to authenticate, authorise, and communicate using XML. For more information, see the Web Services Guide.

Soft Decline

A Soft Decline is a decline response to the terminal or online merchant, indicating that the transaction failed due to being non-SCA. The transaction should be re-attempted with SCA. This may include (for card present transactions) requesting that the terminal authenticates the cardholder using PIN.

SSL Certification

An SSL certificate displays important information for verifying the owner of a website and encrypting web traffic with SSL/TLS, including the public key, the issuer of the certificate, and the associated subdomains.

Stand-In Processing (STIP)

The card network (Visa and Mastercard) may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your GPS mode, GPS may also provide STIP on your behalf, where your systems are unavailable. For more information, see the External Host Interface Guide.

Strong Customer Authentication (SCA)

Type of cardholder authentication process where the cardholder is authenticated using a combination of at least two of the following tests: Possession (something the cardholder has), Knowledge (something the cardholder knows) and something they are (such as a fingerprint, face recognition or voice recognition).

T

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 Service Provider

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.

U

Usage Group

Group that controls where a card can be used. For example: POS or ATM. For more information, see the Web Services Guide.

V

Validation

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

VPN

Virtual Private Network. A secure, encrypted remote connection over the public internet to the private GPS network, designed to safeguard the security and integrity of the network. Users are set up to access defined GPS services via their VPN connection.

VROL System

Visa Dispute Resolution Online system, provided by Visa for managing transaction disputes.

W

Wallet Provider

These are providers such as Apple, Android (Google), Samsung etc. who supply the payment apps (also known as Mobile Wallet token requestors).

Contact Us

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

Global Processing Services Ltd.

Support Email: ops24@globalprocessing.com

Support Phone: +442037409682

GPS Offices

UK Central Office	Singapore	Australia	Dubai, UAE
6th Floor, Victoria House Bloomsbury Square London WC1B 4DA	Republic Plaza 9 Raffles Place Singapore 048619	Stone & Chalk Level 4, 11 York Street Wynyard Green Sydney, NSW, 2000	EO 10, Ground Floor, Building 1 Dubai Internet City Dubai, United Arab Emirates

Technical Publications

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

Document History

This section provides details of what has changed since the previous document release.

Version	Date	Reason	Who
1.0	31/08/2021 09/06/2022	First version Terminology consistency edits	WS