thredd

Key Concepts Guide

Version: 1.4
10 July 2025

For the latest technical documentation, see the Documentation Portal.

Copyright

About this Guide

This guide describes the card payments ecosystem and how Thredd 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 Thredd platform, see The Role of Thredd and Thredd Architecture.
- If you are looking to set up a card program and want to understand what this involves, see Setting up a Program with Thredd and Use Case Scenarios.

Related Documents

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 Thredd card project.
Web Services Guide	Describes how to use the Thredd SOAP API to send requests to Thredd and provides specifications on the available web service calls.
Cards API Website	Describes how to use the Thredd REST-based API to send requests to Thredd.
External Host Interface (EHI) Guide	Describes the Thredd External Host Interface (EHI) and provides specifications on how to process and respond to messages received from EHI.
Thredd Portal Guide	Describes how to use the Thredd Portal to manage your cards and transactions.
Transaction XML Reporting Guide	Describes the structure and contents of the Thredd Transaction XML reports.
3D Secure Guide - Apata	Describes the Thredd 3D Secure service (via Apata) and how to implement a 3D Secure project.
3D Secure Guide - Cardinal	Describes the Thredd 3D Secure service (via Cardinal) and how to implement a 3D Secure project.

Tip: For the latest technical documentation, see the Documentation 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.
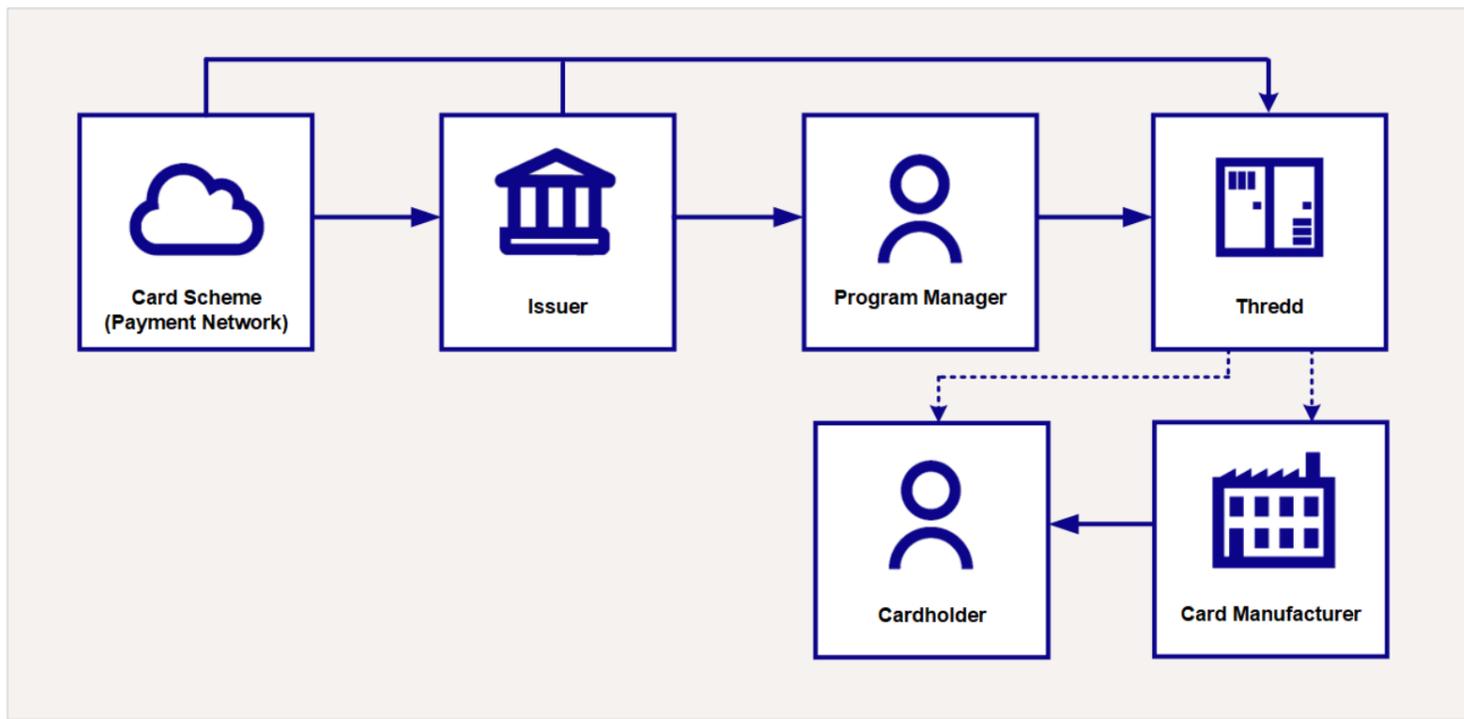
Figure 1: Key Parties in Setting Up a Card Program

Each of these parties is described in further detail below.

1.1.1 Card Scheme (Payment Network)

The Card Scheme (e.g., Visa, Mastercard, Discover) 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, Mastercard, Discover and Diners).

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.

Thredd plugs in directly to the payment network and has partner relationships with Visa, Mastercard, Discover, as well as smaller networks that use the **Mastercard Network Exchange**[1] (MNE), such as STAR and Pulse[1] .Visa, Mastercard and Discover are global networks and allow their branded cards to be used worldwide[2].

The Thredd platform receives transactions from the scheme networks and processes these messages. The platform 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.

---

[1]Enables smaller networks to use Mastercard as a routing platform for payments. Can also be referred to as MNEX or MNGS.

[1]Please contact your account manager for information on Discover network availability and restrictions. Mastercard Network Exchange enables smaller networks to use Mastercard as a routing platform for payments.

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

Key Scheme Responsibilities (Payment Network)

- 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 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

1.1.2 Issuer (BIN Sponsor)

The card issuer is the BIN Sponsor. 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 Thredd.

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.

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

For new Thredd customers starting out on a card program with Thredd, speed to market is quicker and easier when using an existing issuer already set up with Thredd, 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[3].

> **Note:** If your preferred issuer in your region does not currently have a relationship with Thredd, it will require additional Thredd integration support to on-board them. For further details, contact your Thredd 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 (Issuer)

- Ownership and customer (Program Manager) due diligence
- Must comply with Regulator and Card Scheme rules relating to:
  - Anti-money laundering
  - Risk monitoring
  - Fraud monitoring
  - Reporting (such as quarterly member reports and quarterly operating certificate)
  - Auditing
  - Record retention guidelines
  - MIS analysis
- Typically holds funds
- Dispute management and chargebacks: may delegate to the Program Manager
- Maintains a separate cash deposit
- Maintains client money in a separate Trust account
- Responsible for settlement and reconciliation (reconciliation may sometimes be delegated)
- Provides letter of guarantee for Program Manager

---

[3] 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.

- Many need to review and approve aspects of the Program Manager's service, such as the Customer Portal, Customer App and Customer Terms & Conditions.

1.1.3 Program Manager

The Program Manager is a Thredd 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 Thredd 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 Thredd 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.

- You should provide a Customer Portal/ mobile application where customers can sign in and manage their account. You can use the Thredd web services API and real-time data from Thredd 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.

- You should maintain a separate fee arrangement with your customers for usage of the cards and account service charges. Thredd 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), you must be PCI DSS compliant. Thredd provides a means to manage cards without needing to process the PAN, using a Public Token (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 (with EHI Gateway Processing or Cooperative Processing setup options)

1.1.4 Thredd

Thredd has existing partner relationships and connections with schemes, issuers and card manufacturers, and is integrated with service providers such as 3D Secure, Transaction Fraud Monitoring and mobile wallet token providers.

The Thredd Platform is a flexible system 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 Thredd 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.

Support is provided through your Thredd 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 Thredd solution is the dedicated customer support provided at all stages of a project. Thredd 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[4]

- Maintains the card balance and transaction history if required (EHI Cooperative Processing and Full Service Processing setup or no EHI)

- Connections to card manufacturers

- Reporting

- Product functionality support and velocity controls

- Fee structure

1.1.5 Card Manufacturer

Thredd 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.

Thredd supports full Program Manager branded cards, with dynamic elements and **EMV**[2] 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.

> **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 Thredd 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 Cards API Website (REST API) or Web Services Guide (SOAP API).

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 and expiry date. (This process can take a few days.)

1.1.6 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.

---

[4] 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).

[2] EMV is an acronymn for "Europay, Mastercard, and Visa", the three companies which created the standard. The EMV cards are 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. These cards are smart cards.

1.2 Parties Involved in Transaction Processing

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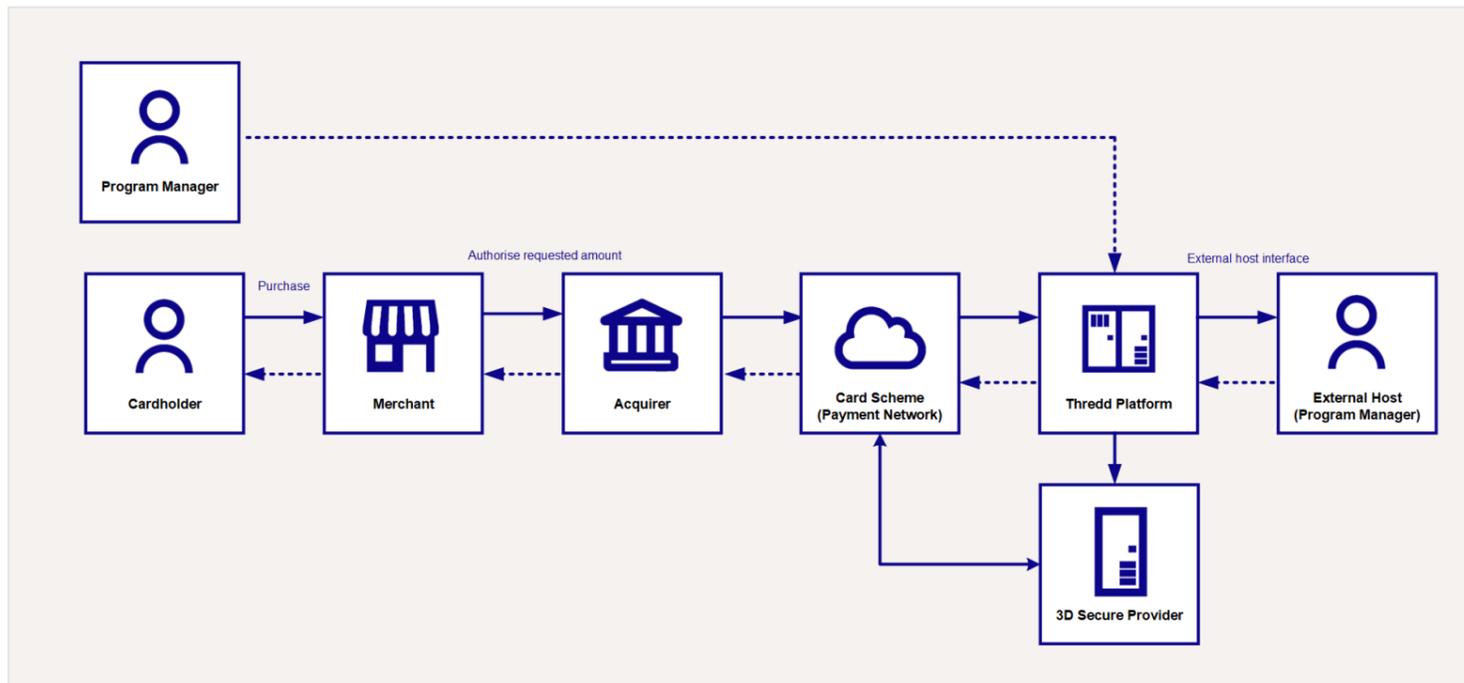

Figure 2: Key Parties in Processing Card Transactions

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

1.2.1 Program Manager (before the card is used)

The Program Manager must activate a card for it to be used. This is done via the Thredd API. See the Cards API Website (REST API) or Web Services Guide (SOAP API).

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 Thredd web services API, you can link it to a Thredd 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.

- Where Thredd holds the card balance on your behalf (such as with Full Service Processing setup), 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 Thredd API to load/unload and perform balance adjustments on a card. These API will update the Thredd cards database, where the transaction and balance ledger on the card is maintained. For details, see the Cards API Website (REST API) or Web Services Guide (SOAP API).

1.2.2 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 reads the **EMV**[1]/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 to verify their identity. For details, see the 3D Secure Guide.

---

[1]EMV is an acronymn for "Europay, Mastercard, and Visa", the three companies which created the standard. The EMV cards are 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. These cards are smart cards.

Thredd is compliant with the **Second Payment Service Directive (PSD2)**[1] regulations relating to how card transactions are handled and authenticated. For details, see the PSD2 and SCA Guide.

1.2.3 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)**[2], 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 or partial authorisation) and may be followed by an **incremental authorisation**[3]. 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.

The Thredd **Smart Client**[4] application enables your customer services staff to view transactions, issue refunds, block cards and raise **Chargebacks**[5] (Mastercard only). For details, see the Smart Client Guide.

1.2.4 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) or Internet Merchant Account (IMA) 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 Thredd receives these messages from the card schemes, the Thredd Platform 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. Thredd reports these charges to the Program Manager.

> **Note:** You will need a payment services provider (PSP) and **Acquirer**[6] if you are taking card payments from your customers to load their accounts. This relationship is between you and the PSP and acquirer. Thredd does not currently provide a direct PSP service.

---

[1]A system used to manage the 3D Secure authentication service for the issuer. During an authentication session, the ACS communicates with the Card Scheme and Thredd systems, and may also interact with the cardholder, by providing Challenge screens.
[2]A unique identifier of the merchant, to identity the type of account provided to them by their acquirer.
[3]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.
[4]Smart Client is Thredd's legacy desktop application for managing your cards and transactions on the Thredd Platform.
[5]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.
[6]Enables smaller networks to use Mastercard as a routing platform for payments. Can also be referred to as MNEX or MNGS.

1.2.5 Card Scheme (Payment Network)

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

Thredd currently supports Visa, Mastercard and Discover schemes. These are global schemes that allow their branded cards to be used worldwide. We also support Mastercard Network Exchange (MNE) for enabling US debit card payments.

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

Where a device PAN (DPAN) 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 Thredd. 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 Visa Resolution Online (VROL)	Payments Dispute Management Guide
3D Secure	Visa Secure and Mastercard Identity Check	3D Secure Guide (Apata) 3D Secure Guide (Cardinal)
Tokenisation	Mastercard Digital Enablement Service (MDES) and Visa Token Service (VTS); Thredd refer to the Visa service as the Visa Digital Enablement Program (VDEP).	Tokenisation Guide

1.2.6 Thredd

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

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

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

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

Thredd 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.

1.2.7 Program Manager (when the card is used)

Thredd can authorise transactions on your behalf where we hold details of the balance on the card (Full Service Processing, Gateway Processing with Stand-in Processing or where EHI is not being used).

Alternatively, you can maintain the card balance on your own systems and manage the authorisation decision (Gateway Processing) or use Thredd as a fallback option for stand-in processing when your systems are not available (Cooperative Processing and Gateway Processing with Stand-In). For details of setup options, see Transaction Processing and EHI.

Where Thredd provides authorisation services and holds the card balance (e.g., Full Service Processing), you will need to update the card balance held by Thredd to reflect card loads/unloads and balance adjustments. This is done using Thredd API. See the Cards API Website (REST API) or Web Services Guide (SOAP API).

In transaction processing setups 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.

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

1.2.8 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.

Thredd provides full 3D Secure support via a choice of 3D Secure service providers: Apata or Cardinal Commerce. Program Managers are set up with an account and access to a 3D Secure 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 the 3D Secure service provider's **Access Control Server (ACS)**[1]. The ACS applies the authentication 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, the ACS notifies Thredd, and Thredd notifies the Program Manager to start the authentication session.

For more information, see the 3D Secure Guide.

---

[1]A system used to manage the 3D Secure authentication service for the issuer. During an authentication session, the ACS communicates with the Card Scheme and Thredd systems, and may also interact with the cardholder, by providing Challenge screens.

2 The Role of Thredd

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

2.1 Thredd as an Issuer-Processor

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

> **Tip:** Click the image to expand.
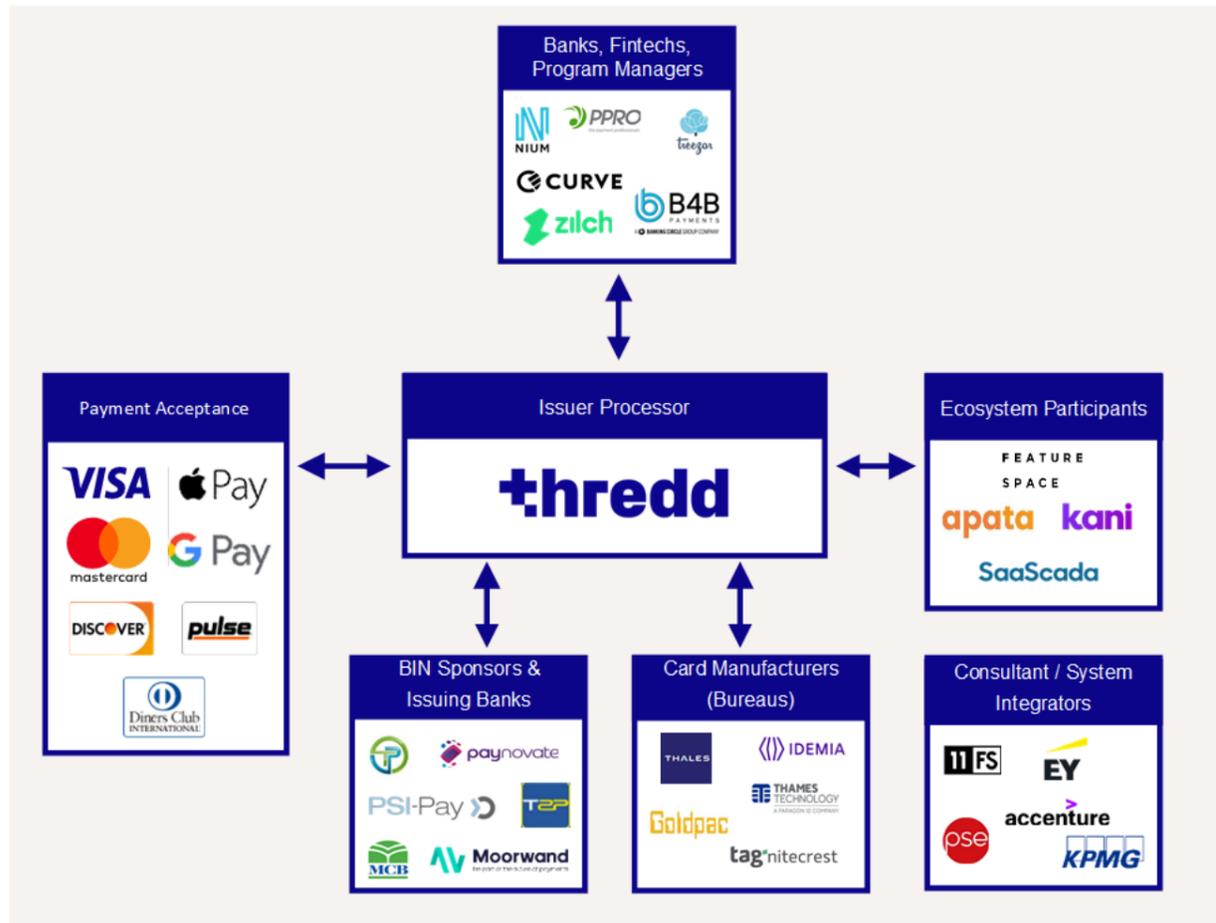
Figure 3: Thredd as an issuer-processor

The Thredd 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 Thredd payments ecosystem, thus reducing the amount of time-consuming and costly licensing, regulatory compliance, commercial agreements, infrastructure and connections.

Thredd plays an essential role in helping our Program Managers understand the regulatory environment. We implement any changes needed to keep the Thredd 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 Thredd's Issuer/BIN Sponsor partners in your region. For a list of pre-integrated issuers for your region, please contact your Business Development Manager.

Thredd 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. [1]

---

[1]A system used to manage the 3D Secure authentication service for the issuer. During an authentication session, the ACS communicates with the Card Scheme and Thredd systems, and may also interact with the cardholder, by providing Challenge screens.
[2]Thredd's Secure Connectivity Framework is the combination of several components which enable secure access to Thredd's resources, using a common identity store.
[3]The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.
[1] For our current country-specific support and global roll-out roadmap, please contact your Thredd Business Development Manager.

Thredd currently supports Visa, Mastercard and Discover networks, as well as smaller networks that use the **Mastercard Network Exchange**[1] (MNE), such as STAR and Pulse[2].

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

---

[1]Enables smaller networks to use Mastercard as a routing platform for payments. Can also be referred to as MNEX or MNGS.

[2] Please contact your account manager for information on Discover network availability and restrictions. Mastercard Network Exchange enables smaller networks to use Mastercard as a routing platform for payments.

2.2 Thredd and the Transaction Processing Lifecycle

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

2.2.1 Transaction Processing and EHI Setup

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

Setup Option	Who Authorises?	Who Maintains the Balance?	Thredd Stand-In	Details
Gateway Processing	External Host	External Host	Yes	Your systems maintain the balance and perform authorisation. Note: If Stand-In is enabled, then your systems maintain the balance and perform authorisation. Thredd provides Stand-In authorisation if the external host is unavailable.
Cooperative Processing	Thredd	Thredd / External Host	Yes	Thredd 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 Thredd-maintained balance.
Full Service Processing	Thredd	Thredd	No	Thredd maintains the balance and performs authorisation. You receive a read-only response.

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

2.2.2 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 an authorisation.

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

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

Program Manager Authorises (Gateway and Cooperative Processing)

With Gateway and Cooperative Processing, the Program Manager is responsible for authorisation.

Pre-requisites to use these EHI setup options:

- You maintain the card ledger balance on your own systems
- You must be able to respond to an authorisation request within the Thredd system time limit[3]

See the example transaction flow below.

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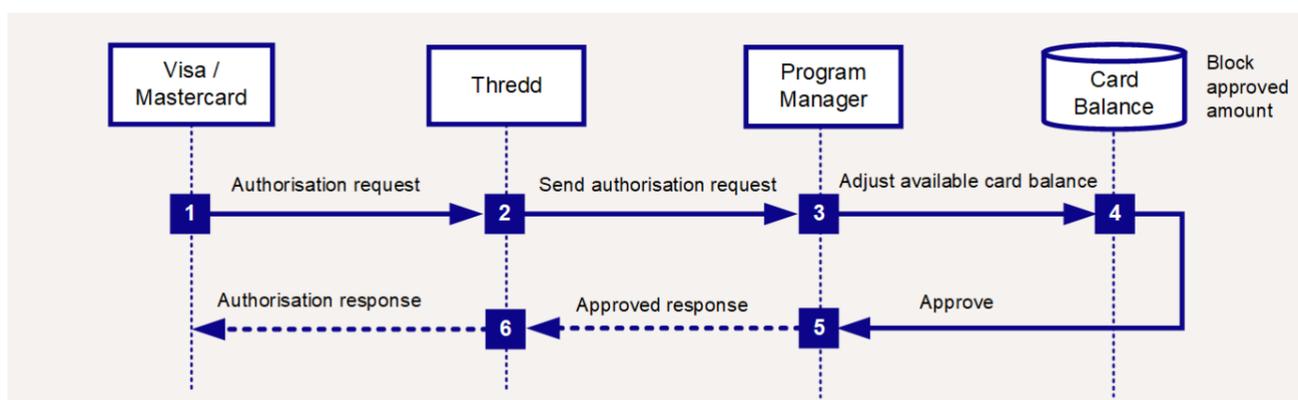
[3] The default system time limit may vary, depending on your region. Please check with your Business Development Manager.

1. The scheme sends an authorisation request to Thredd.

2. Thredd carries out validation checks and sends the request to the external host (Program Manager).

3. The Program Manager approves the request. *

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. Thredd responds to the scheme with a message indicating approval.

*In the event that the Program Manager's systems are unavailable, Thredd can support authorisation through Stand-In Processing (STIP). STIP options are available for Gateway Processing with STIP (mode 4).

Thredd Authorises (Cooperative and Full Service Processing)

In Full Service Processing, Thredd provides the authorisation decision. Cooperative Processing provides a hybrid, where Thredd can support the initial authorisation, but the Program Manager can override the decision.

You should use Cooperative Processing (mode 2) or Full Service Processing (mode 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.
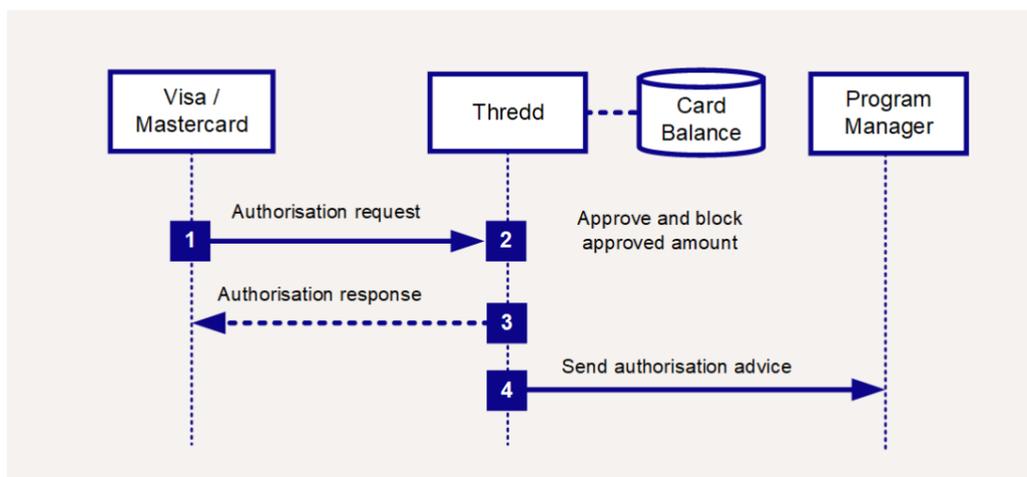
Figure 5: Authorisation Flow - where Thredd Approves

1. The scheme sends an authorisation request to Thredd.

2. Thredd carries out validation checks and approves the request. Thredd blocks the approved amount (including fees) on the card and reduces the available balance.

3. Thredd responds to the scheme with a message indicating approval.

4. Thredd 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 Thredd.

Visa and Mastercard send Thredd daily batch clearing files[4]. Thredd process the clearing files and send financial advices to the Program Manager. Thredd refers to these financial advices as presentments.

When Thredd 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*.

---

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

> **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 (Gateway and Cooperative Processing)
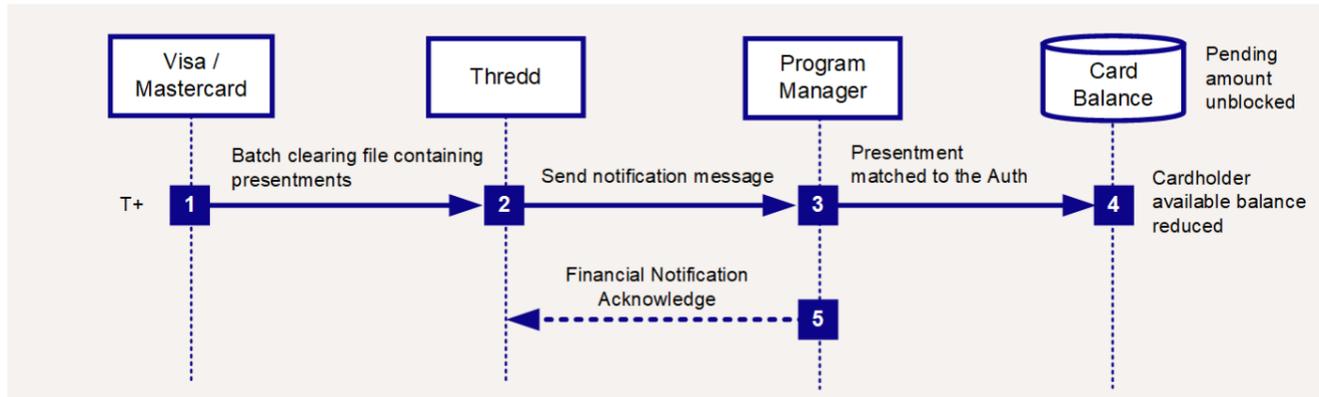

Figure 6: Presentment Stage - where Program Manager holds the balance

1. The scheme sends a batch clearing file to Thredd.

2. Thredd 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 Thredd Approves (Cooperative, Full Service Processing or no EHI)
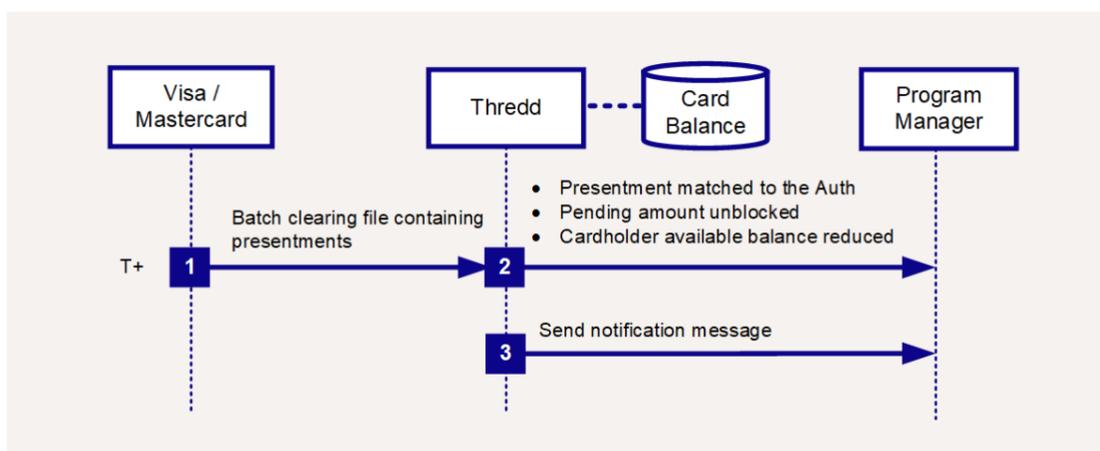
Figure 7: Presentment Stage - where Thredd holds the balance

1. The scheme sends a batch clearing file to Thredd.

2. Thredd processes each financial record. Thredd matches the presentment to the original authorisation, unblocks the pending amount and reduces the cardholder's available balance.

3. Thredd 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 Thredd Platform

This section describes the Thredd Platform key components, as well as interfaces to partner services.

> **Tip:** Click the image to expand.
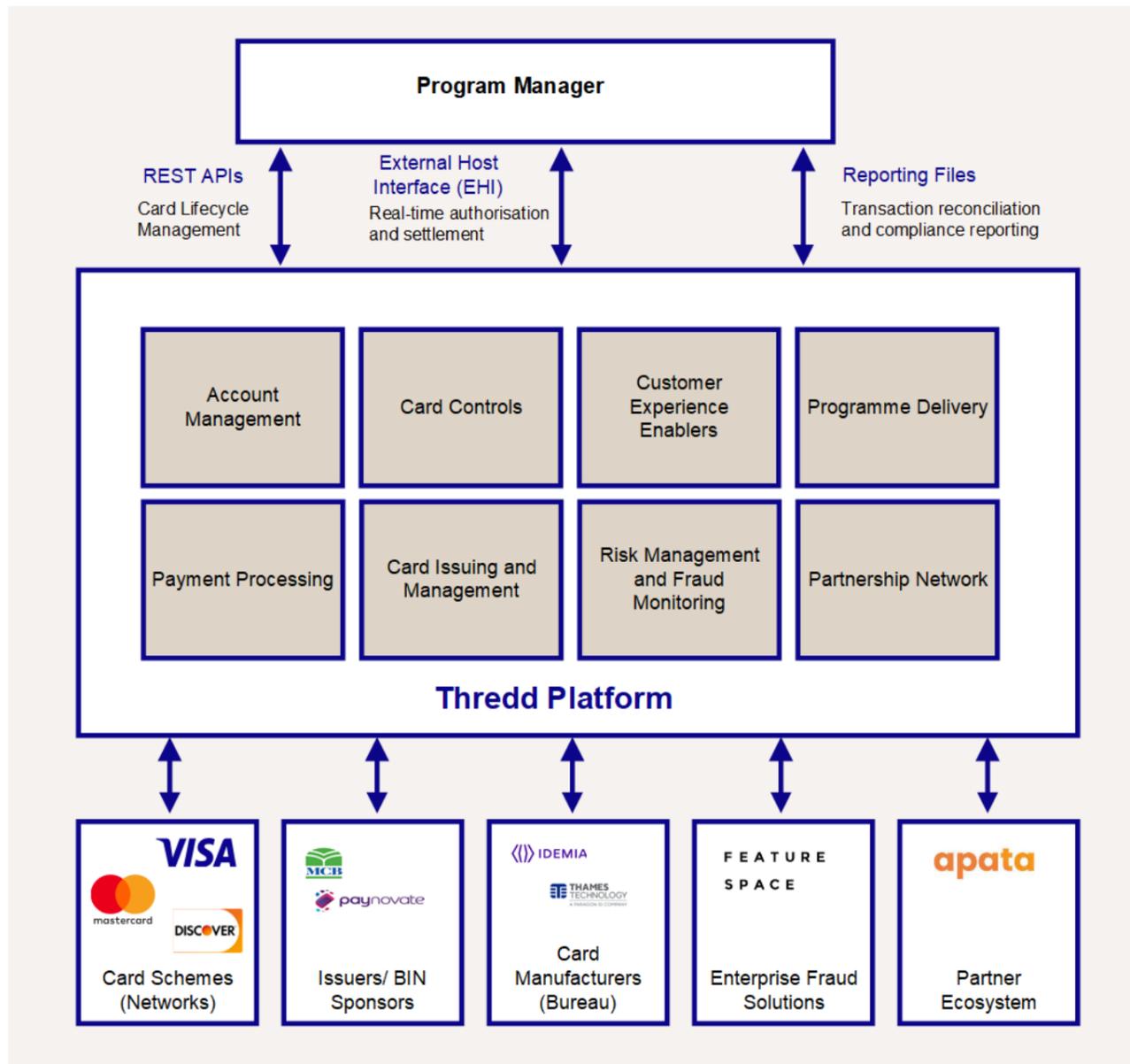
Figure 8: Thredd Platform

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

3.1 Card Issuing and Management

Web Services and Cards API

You can use the Thredd Web services (SOAP) or Cards API (REST) to create and manage the accounts and cards in your 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 Thredd to create a card, the Thredd Platform allocates an available card PAN to the card. It generates a unique internal Public Token, which is linked to the card. The public token is returned in the Thredd response and your systems can use this token for all subsequent queries and card management activities on the Thredd 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 on using SOAP Web Services, see the Web Services Guide. For more information on using REST-based Cards API, see the Cards API Website.

Managing Cards

You can use the Thredd API to manage your cards. You can integrate the API 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 on using SOAP Web Services, see the Web Services Guide. For more information on using REST-based Cards API, see the Cards API Website.

Cardholder Fee Setup and Management

The Thredd 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 Payment Processing

Message Processor

The Thredd 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 Thredd card program (e.g., per Issuer, program, product and card usage settings).
- Where Thredd 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 Thredd Fees module).
- Initiates other related services, such as authentication and transaction reporting.

External Host Interface (EHI)

The External Host Interface (EHI) is an API interface[1] which sends 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 setup.

---

[1]Thredd's Secure Connectivity Framework is the combination of several components which enable secure access to Thredd's resources, using a common identity store.

[1] EHI messages can be provided in either JSON or XML format.

EHI plays an important role in processing real-time authorisation and financial messages. There are flexible transaction processing setup options (see Transaction Processing and EHI Setup). 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.

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.

XML Reporting

The Thredd Platform 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 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.

Thredd 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 Thredd account manager for details.

3.3 Account Management

Thredd Portal

Thredd Portal is our new web application for managing your account on the Thredd platform. Using the Thredd Portal, you can configure and control your payment programmes in real-time. Thredd Portal provides a feature-rich dashboard that allows you to view and manage the full lifecycle of your customers' transactions and card usage.

For more information, see the Thredd Portal Guide.

Smart Client (legacy)

Smart Client is our legacy desktop application that can be installed on a personal computer (PC). It 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 is available (Mastercard only).

For more information, see the Smart Client Guide.

3.3.1 Customer Experience Enablers

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) 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).

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.

Mobile Text Messaging

The Thredd mobile text messaging (SMS) service enables you to communicate better with your customers and enhance the customer experience by enabling you to send messages to customers' SMS-enabled devices. For more information, see the Mobile Text Messaging (SMS) Guide.

Interactive Voice Reponse

The Thredd Interactive Voice Response (IVR) service enables customers to call a phone number to perform various actions for their card.For more information, see the Interactive Voice Response (IVR) Guide.

3.3.2 Risk Management and Fraud

Fraud Transaction Monitoring

Fraud Transaction Monitoring (powered by Featurespace) is a fraud solution that minimises online and offline card risk and offers real-time detection of card fraud.

Fraud Transaction Monitoring adapts to new fraud types and identifies unknown threats by detecting unexpected changes (anomalies) in real-time data.

For more information, see the Fraud Transaction Monitoring Guides.

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.

Thredd provides full 3D Secure support using one of our 3D Secure providers: Apata or Cardinal Commerce. Program Managers are set up with an account and access to a 3D secure Portal for configuring their 3D Secure authentication rules.

For more information, see the 3D Secure Guide (Apata) or 3D Secure Guide (Cardinal).

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 confirm the cardholder identity, such as PIN, CVV2 and CAVV.

Fraud Reporting

The ThreddSAFE Reporting facility on Smart Client enables Program Managers to report suspected fraudulent transactions to Mastercard.

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

3.4 Partnership Networks

Thredd's partners span many parts of the industry:

- Global payment acceptance through Visa, Mastercard and Discover
- 95+ Issuing Banks and BIN Sponsors integrated Certified by Visa and Mastercard to process transactions globally.
- Global and local network of card manufacturers
- Ecosystem partners: Featurespace, Apata, Cardinal, MeaWallet and Kani
- Digital Wallet (Tokenisation) and partners: Mastercard Digital Enablement Service (MDES), Visa Digital Enablement Programme (VDEP)

Card Manufacturers

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

The Thredd API are used to raise card creation requests. Thredd 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 the Thredd API to create card instructions, see the Cards API Website (REST API) or Web Services Guide (SOAP API).

4 Setting up a Program with Thredd

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

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

4.1 What you need to Get Started

4.1.1 Issuer/BIN-sponsor

The issuer provides Thredd 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.

4.1.2 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, you can use an Agency Banking provider 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.

4.1.3 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 Thredd supports. For details, please contact your Business Development Manager.

> **Note:** To use a card manufacturer not currently integrated to Thredd, please discuss with your Business Development Manager or Account Manager.

4.2 Thredd Data Model

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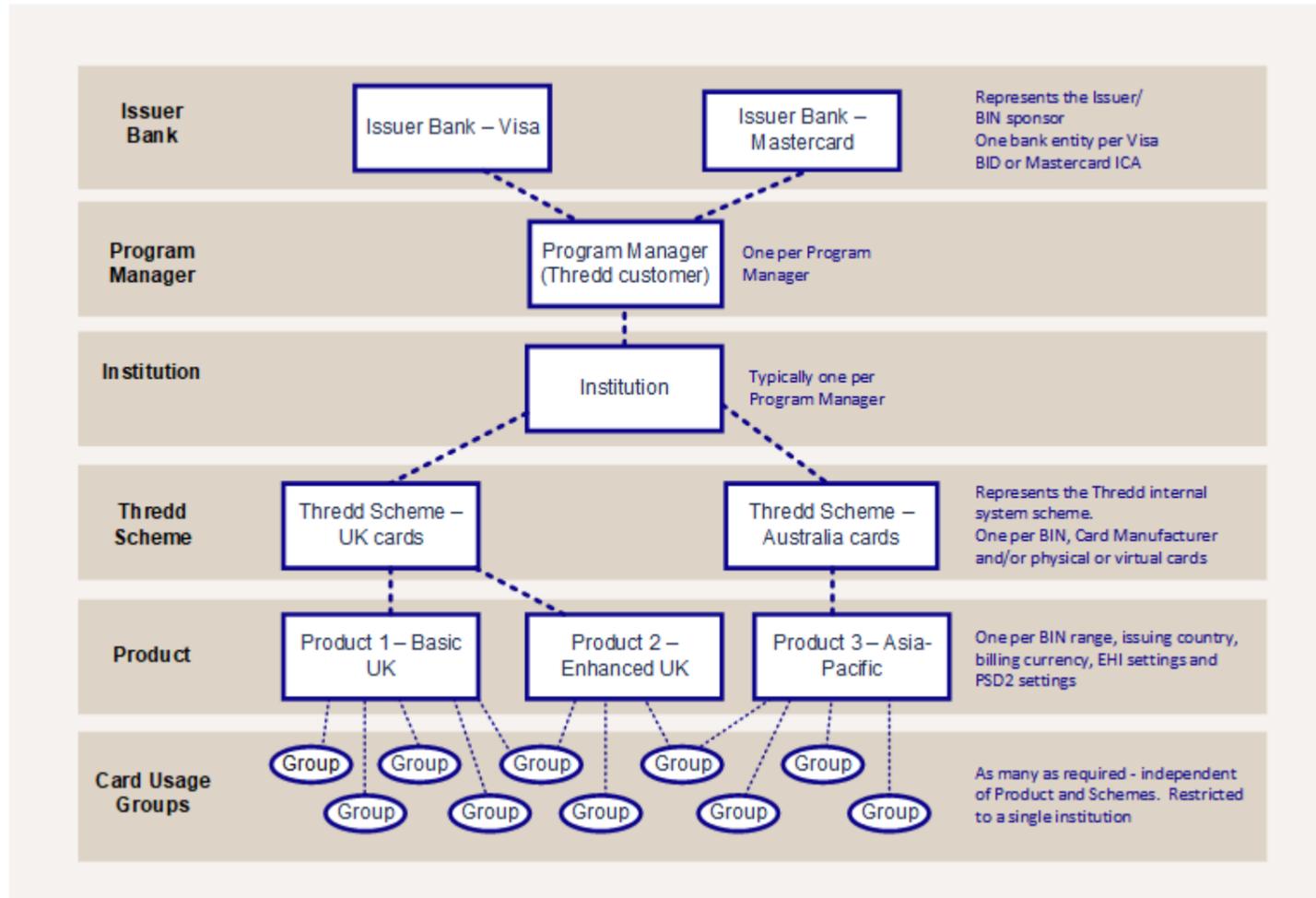

Figure 9: Setting up an Account with Thredd

Each Thredd 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 Thredd Schemes; these are required if supporting multiple BINs or more than one card manufacturer; separate Thredd Schemes may be required if you want to create both physical and virtual cards.

Thredd 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.

4.2.1 Bank

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

---

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

4.2.2 Institution

An institution represents an organisation set up on the Thredd 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)

4.2.3 Program Manager

One Program Manager account is set up per Thredd 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
API credentials (for SOAP web services or REST-based Cards API)
PGP keys for virtual cards

4.2.4 Thredd Scheme

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

One Thredd 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 Thredd Schemes.[2]

You can have multiple Thredd 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

4.2.5 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. A product is linked to an Issuing Bank.

---

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

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

4.2.6 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 Thredd Portal or 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) Group	The MCC is a four-digit number used by the Card Schemes to define the trading category of the merchant.
Usage Groups	Group that controls where a card can be used. For example: POS or ATM.
Linkage Groups	The Linkage Group set up in Thredd Portal or 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.

Group	Description
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 Thredd 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 Thredd 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 Thredd. It covers three common business cases:

- Prepaid Card Service
- Neobank/ Digital Banking
- Travel and Foreign Exchange

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:

Tip: Click the image to expand.
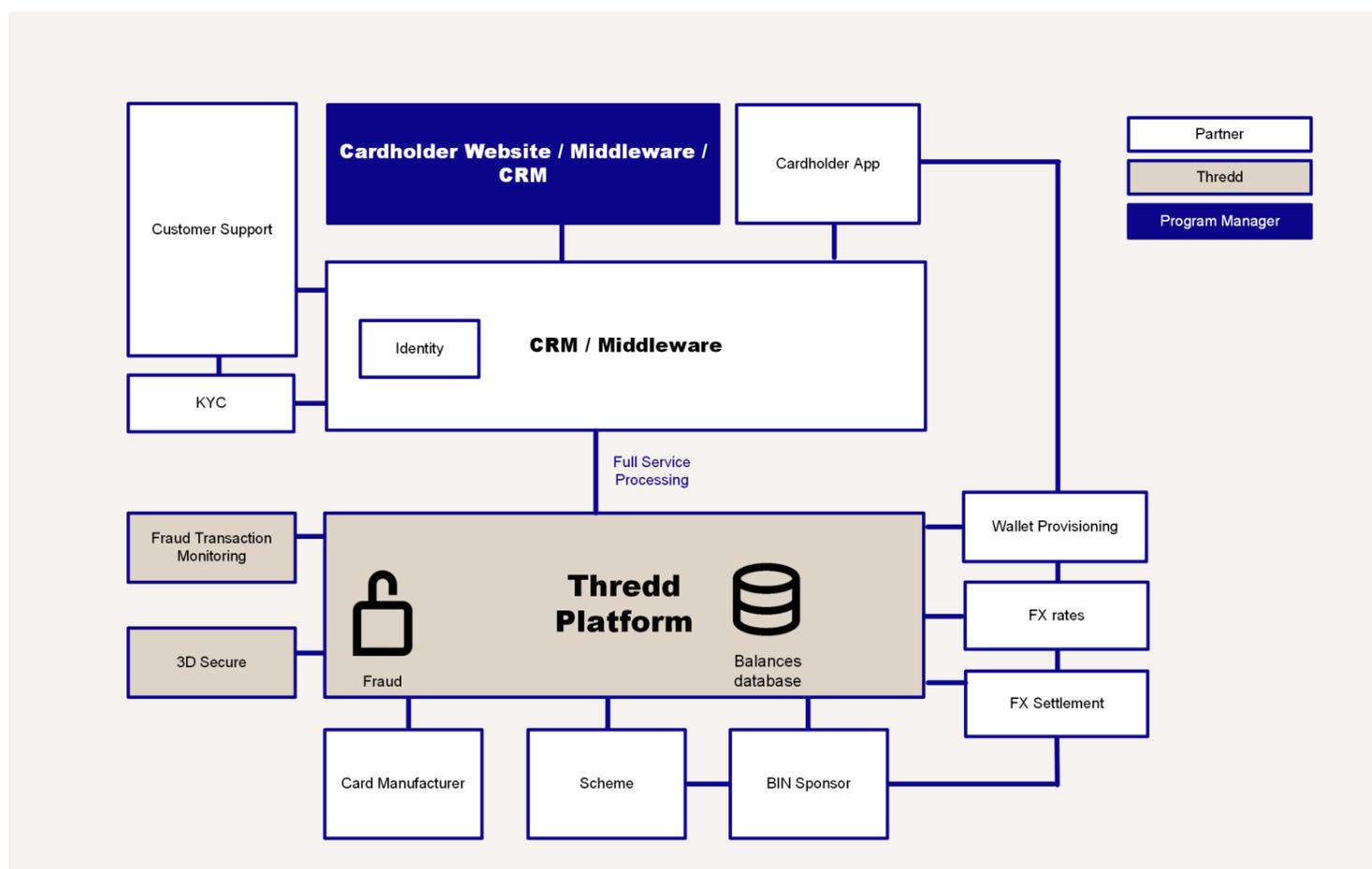
Figure 10: Prepaid Card Service

Service implementation

SchoolCard offers a Customer Portal, where customers can sign up for the card and manage their account (for example, 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 Thredd web services API to connect to Thredd for card services.

All other aspects of the service are provided via Thredd 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 Thredd, 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 Thredd 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 Thredd 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, Thredd provides full card authorisation and management of the card balance (Full Service Processing).

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:

> **Tip:** Click the image to expand.
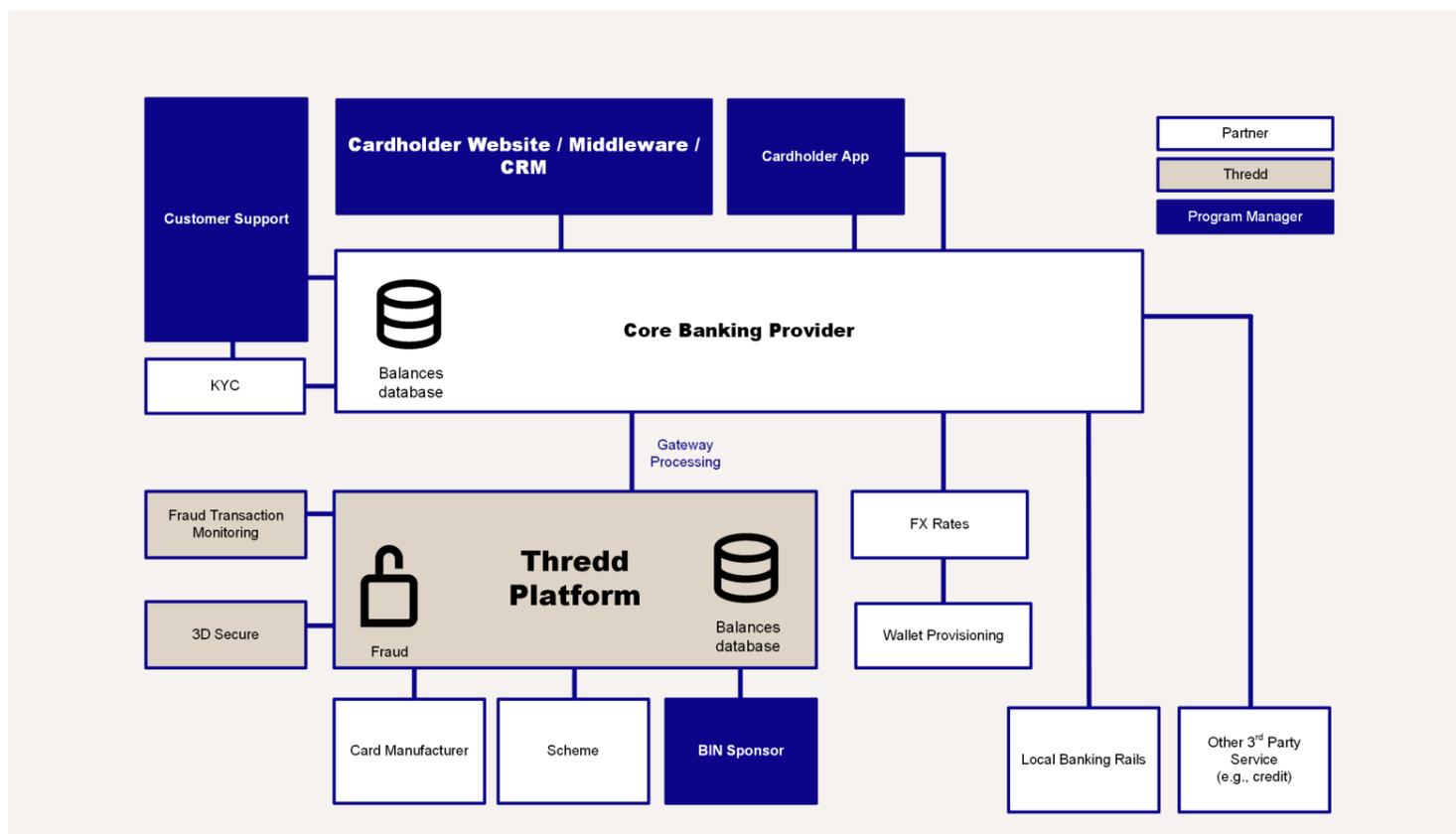
Figure 11: Neobank Digital Banking Service

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 Thredd for each currency and issuing country. For details, see the Thredd Data Model.
- The bank manages card authorisation and updates to the card balance (Gateway Processing).
- The bank manages any fees and charges to customers for using their service.
- Thredd provides fraud management services using Fraud Transaction Monitoring and cardholder 3D Secure authentication.

5.3 Travel and Foreign Exchange

This use case is for a typical travel and foreign exchange service.

Business proposition

SafeHorizons is a new fintech, offering a local debit card for overseas workers. These workers cannot obtain a local bank account and want to have their salaries paid into a local debit card account, in the local currency. They can then use the funds in their country of temporary residence.

Customers can load funds onto their SafeHorizons account or request their employer pay directly into the account. They can use the banking facility provided by SafeHorizons's issuer. Once SafeHorizon has confirmed the funds are in the customer's account, they load the funds onto the customer's local currency card account, using the Thredd API. This ensures that the funds are available for use immediately on the local debit card.

SafeHorizons charge a small load fee to the customer, which is applied each time funds are loaded onto the card, and automatically deducted from the card's balance.

Customers who want to use their new debit card back home, or in another country, are able to create additional currency wallet accounts, linked to their master account. They can transfer funds between their master account and any linked currency accounts. SafeHorizons use an FX services provider to obtain the latest currency rates and charge a small FX transaction fee percentage to the customer.

Service architecture

Below is an example of the setup for a typical travel and foreign exchange service:

> **Tip:** Click the image to expand.
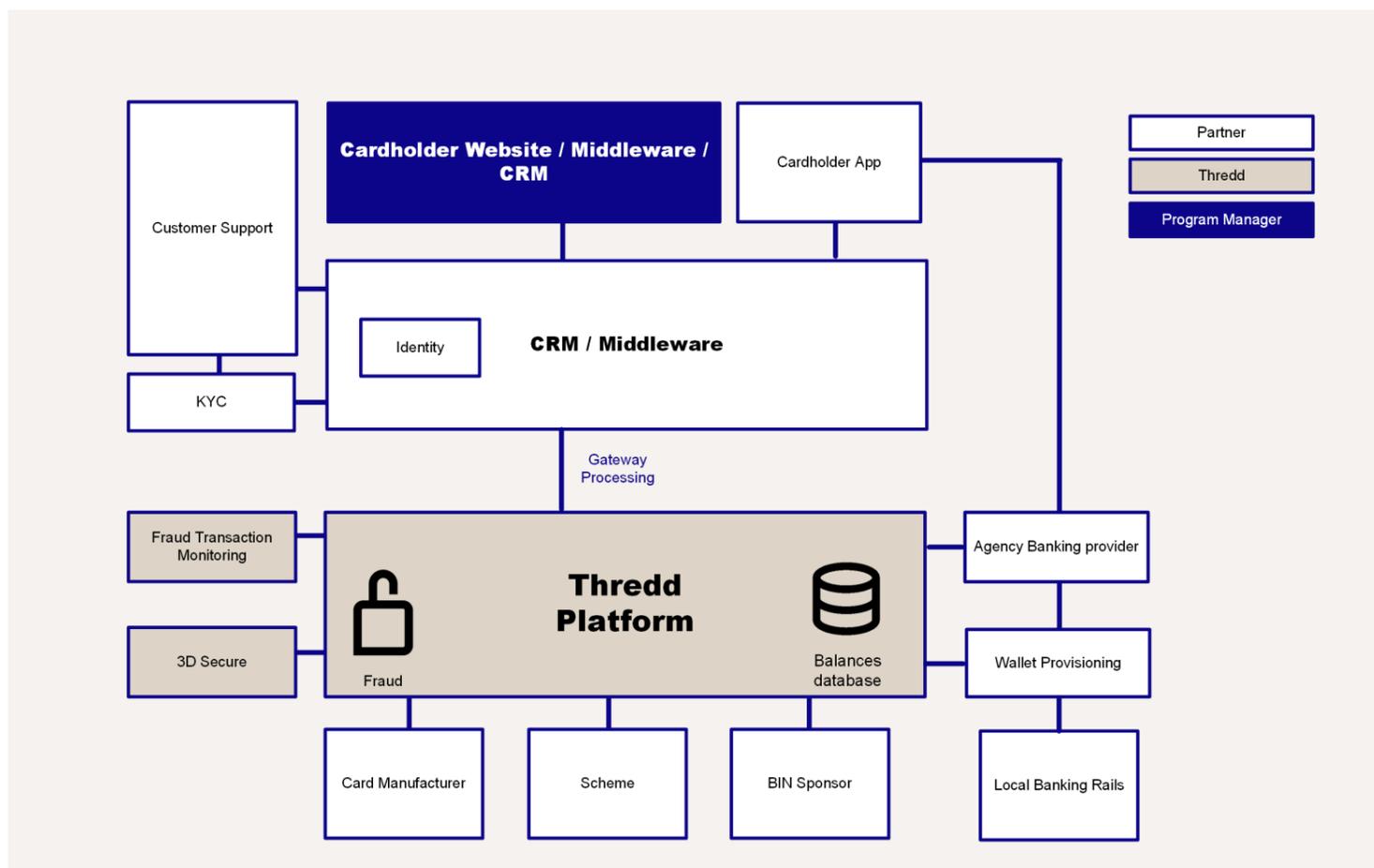
Figure 12: Travel and FX Service

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 card manufacturer, for printing and postage of cards to cardholders.

- SafeHorizons use their Issuer's Banking service to provide their customers with a means to make payments into and out of their card account.
- When the card is used at supporting stores, Thredd processes and sends to the Program Manager for authorisation. SafeHorizons returns the authorisation decision to Thredd (using Gateway Processing).
- SafeHorizons use the Thredd fees module for managing card service and usage charges.
- Thredd provide fraud management services using Fraud Transaction Monitoring and cardholder 3D Secure authentication.

Glossary

#

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 Control Server (ACS)

A system used to manage the 3D Secure authentication service for the issuer. During an authentication session, the ACS communicates with the Card Scheme and Thredd systems, and may also interact with the cardholder, by providing Challenge screens.

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.

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.

C

Card Scheme

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

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.

Clearing File/Clearing Transaction

Thredd 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.

E

EMV

EMV is an acronymn for "Europay, Mastercard, and Visa", the three companies which created the standard. The EMV cards are 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. These cards are smart cards.

External Host

The external system to which Thredd sends real-time transaction-related data. The URL to this system is configured within Thredd 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 Thredd web service API fees.

H

Hanging Filter

The period of time during which Thredd waits for an approved authorisation amount to be settled. This is defined at a Thredd 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.

Issuer

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

M

Mastercard Network Exchange

Enables smaller networks to use Mastercard as a routing platform for payments. Can also be referred to as MNEX or MNGS.

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 identity 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.

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.

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.

Program Manager

A Thredd 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.

S

Secure Connectivity Framework

Thredd's Secure Connectivity Framework is the combination of several components which enable secure access to Thredd's resources, using a common identity store.

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 Thredd's legacy desktop application for managing your cards and transactions on the Thredd Platform.

Stand In Processing (STIP)

The card network (Visa and Mastercard) may approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your Thredd setup/EHI mode Thredd may also provide STIP on your behalf, where your systems are unavailable.

T

Thredd Portal

Thredd Portal is Thredd's new web application for managing your cards and transactions on the Thredd Platform.

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.

V

Validation

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

VROL System

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

Document History

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

Version	Date	Description	Revised by
1.4	27/03/2025	Added glossary item for Secure Connectivity Framework	KD
	11/02/2025	Added references to Thredd Portal, our new web application for managing your cards and transactions.	WS
	12/09/2024	Removed references to VPN.	WS
	27/06/2024	Updated the company address.	PC
1.3	14/06/2024	Updated Thredd_Network.visio and Thredd_Network.png to add Discover, Diners Club, and Pulse.	PC
	14/03/2024	Updates to content and graphics to align with taxonomy updates on our Documentation Portal.	WS
	03/08/2023	Correction to Figure 8, *Thredd Platform* and updates to content in the Thredd Platform section.	WS
	12/06/2023	Corrections to Figures 8, 10, 11 and 12.	WS
	07/06/2023	Updated Operations email address to be occ@thredd.com.	MW
	27/04/2023	Guide rebrand to new company name and brand identity.	WS
1.2	01/12/2022	Updated Copyright Statement.	MW
1.1	17/08/2022	Updates to Figure 4-1: Thredd System Architecture.	WS
	12/08/2022	Removed the Table of Contents from the PDF and updated the page numbering and page layout	MW
	26/07/2022	Updated image captions for online version only. Publication date changed to match online.	MW
	20/07/2022	Updates to the layouts and the PDF Table of Contents	MW
1.0	31/08/2021 09/06/2022	First version Terminology consistency edits	WS

Contact Us

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

Thredd UK Ltd.

Company registration number 09926803

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

Technical Publications

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