Introduction to Card Payments (Abridged version)

Version: 1.3

05 July 2024

Publication number: ICP-1.2-7/5/2024

For the latest technical documentation, see the Documentation Portal.

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

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

© Thredd 2024

Copyright

© Thredd 2024

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

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

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

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

INTRODUCTION

New to card payments and want to understand how they work and how to set up your own card programme?

This guide provides an overview of card payments and highlights information you'll need to know when implementing your own card programme. We'll cover basic concepts about the payments industry, the payment processing life cycle and describe how Thredd can support you.

Thredd has worked closely with many of the world's leading fintechs who have successfully launched their own market leading card services in the UK, Europe, the Middle East and Asia Pacific.

The payments industry is changing rapidly as new technology and new legislation is introduced. This guide describes some of the regulatory changes and new technologies that impact on card programmes.

- Section 1: Overview of Card Payment Networks

  Describes the Thredd model for card payments, the role of Thredd in the payments ecosystem and the regulation of card network participants.

- Section 2: The Technology behind Card Payments

  Describes how card payments have changed over the years and what kind of payment instruments there are.

- Section 3: Introduction to Processing Card Payments

  Describes the way card payments are processed over the card scheme's network.

- Section 4: Implementing a Card Programme

  Describes the considerations to be taken when implementing a card programme and where you can find more information.

- Section 5: Configuring your Card Products

  Describes the available options when setting up a card programme with Thredd.

- Section 6: Managing your Card Programme

  Describes the available options when managing cards and servicing customers.

How Thredd can help you set up your card programme

Thredd provides support through all stages in setting up a card programme. The Thredd Apex payment processing platform is constantly updated to meet the changing needs of our customers.

Tip: Did you know that the Thredd Apex platform has over 40 million active cards and processes nearly 4 million transactions per day? (stats based on data from September 2022)

Section 1: Payment Networks

Overview of Card Payment Networks

- Introduction to the Card Schemes

  What are card schemes and how are they formed? What are the main global card schemes? What do they do, how are they regulated and who has access to them? How do you become a network participant?

- Thredd Model for Card Payments

  What are the roles of the different parties in card payments?

- Issuers and Acquirers

  Who are they and how do they work? What are program managers and Payment Service Providers?

- The role of Thredd in the Payments Ecosystem

  Where does Thredd fit in? Is Thredd a network participant? Does Thredd hold client funds? Is Thredd regulated as a financial services provider? How do we help program managers and issuers? What is our relationship with the card schemes?

- Regulation of Card Network Participants

  What are some of the important rules which card network participants, including issuers and their program managers, need to comply with? Who regulates and monitors activity on the card networks and compliance with the rules? What type of reporting is required from issuers and program managers?

- Scheme Charges and Fees

  What type of fees are charged for operating the card scheme network and processing transactions on the network?

- Holding of Client Funds

  Who holds the cardholder's money and what are the requirements for holding money? How does money get exchanged between cardholders-issuers and acquirers-merchants?

- Using the Services of an Issuer vs. Self-Issuing

  What is the difference between using the services of an issuer and self issuing?

- Banking Networks

  What's the difference between Card Payment Networks and Banking Payment Networks? What are some of the banking network systems and payment methods available?

1.1 Introduction to the Card Schemes

1.1.1 What is a Scheme?

Card schemes are payment networks that enable cards such as prepaid, debit and credit cards issued by the scheme to be used in the regions and countries where the scheme operates. Each card scheme sets its own rules and regulations and promotes its own brand. The schemes are regulated by the financial authorities in the regions in which they operate.

Typically, cards used on the scheme's network will be co-branded with the scheme's logo; the schemes also provide private labelled card products, which do not require scheme branding[1].

Note: Terminology: In this guide we refer to a *Payment Network* as the infrastructure over which payments take place and a *Card Scheme* as the card payment organisation that regulates and controls activity on the payment network and promotes its own brand.

1.1.2 Global and Local Schemes

Over the years there has been a proliferation of both local and global card schemes.

Global card schemes offer their services globally, so that a card issued with their account numbers and branded with their logo can be used in many countries across the globe, not just in the region in which they are issued. The main global card schemes supported by Thredd are listed below.

- Mastercard
- Visa

Other global schemes:

- Union Pay
- Amex (American Express)
- Diners Club
- JCB

Local card schemes issue payment instruments which are local to a country or region and can only be used in that region. Examples include BORICA (in Bulgaria), BOLETO (in Brazil) EFTPOS (in Australia and New Zealand), Network for Electronic Transfers (NETS) in Singapore and Rupay in India.

1.1.3 History of the Major Card Schemes

Let's take a brief look at the history of the two main global card schemes supported by Thredd.

---

[1]Private labelled products such as gift cards have fewer regulatory requirements; they can typically be used at restricted merchant locations and are an easy way to launch a card programme without the usual licensing and approvals required for scheme branded cards.

Mastercard was created in 1959 when several regional US banks formed Interbank, which later became the *Interbank Card Association (ICA)*. In 1968, the ICA and Eurocard formed an alliance that provided access to each other's network. The UK Access card joined the ICA/Eurocard alliance in 1972. In 1979, ICA was rebranded as Mastercard and the Access card became part of Mastercard. In 2002 Mastercard merged with Europay International.

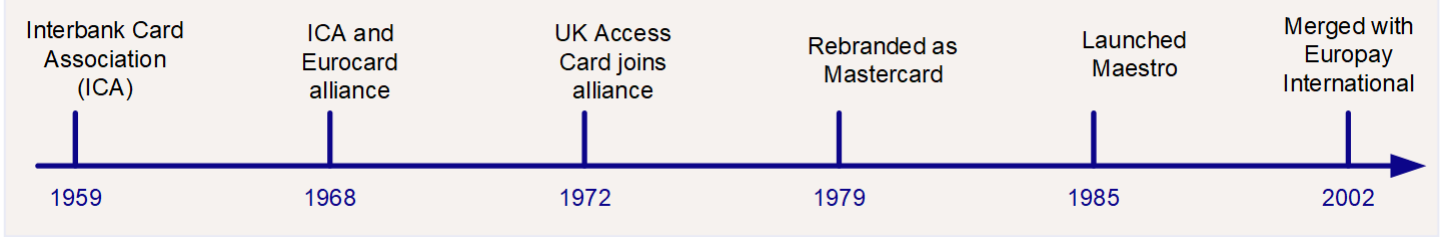

Figure 1: Mastercard Timeline

Visa was launched in September 1958 by Bank of America as the BankAmericard credit card programme.

In 1966 the programme was licenced to other financial organisations, and in 1970 a consortium of issuer banks took over its management. In 1976 the programme was rebranded as Visa. In 2007 Visa formed a global corporation, Visa Inc, while Visa Europe remained member-owned. In 2016 Visa Inc and Visa Europe became one global entity. Visa is currently the world's second largest card scheme (after China UnionPay).

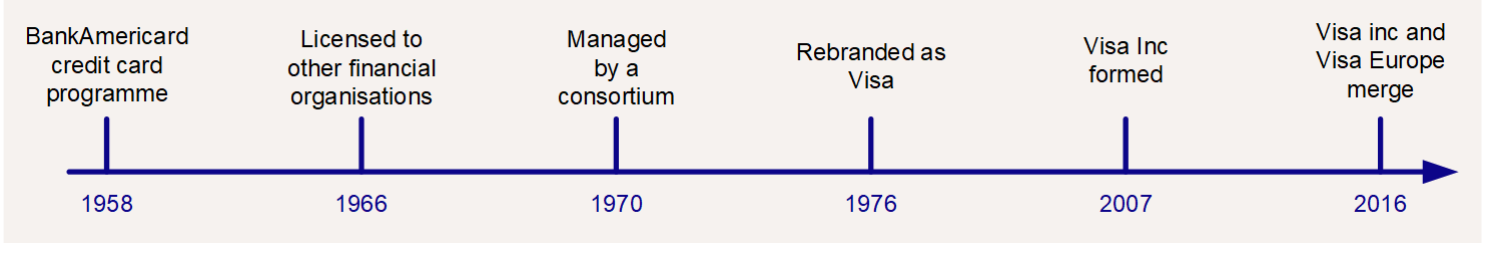

Figure 2: Visa Timeline

Note: The card schemes are constantly evolving, offering new products and services, and expanding their networks through merges and acquisitions. Partnering with a flexible and adaptive issuer-processor like Thredd helps you to keep up to date with the latest card scheme changes and leverage new scheme services.

1.1.4 Becoming a Scheme Member or Participant

To become a scheme member or network participant, you need to sign up to the scheme, be approved by them and contribute to scheme operating costs. There are two types of member licences:

- **Principal licence**: The issuer has a direct relationship with the scheme and full autonomy over their issued cards
- **Affiliate licence**: The issuer is given access to certain features, such as scheme portals, but needs a principal member to sponsor their application

1.1.5 The Role of Thredd within the Scheme

Thredd is certified by Mastercard and Visa and can provide direct connections to their networks as a third-party agent.

Thredd acts as an issuer-processor on behalf of our customers. We receive transactions from Mastercard and Visa and help our customers (card *program managers*) to process and authorise these transactions. We also connect to other linked systems to support additional payment processing needs around security, fraud protection, payment authentication, mobile payments, tokenisation and dispute management.

Thredd is not an issuer or a BIN sponsor, but we have existing relationships to many issuers, who are set up in our systems.

1.2 Thredd Model for Card Payments

The Thredd model of card payments can be used to explain the role of the different parties in card payments. It consists of the following parties:

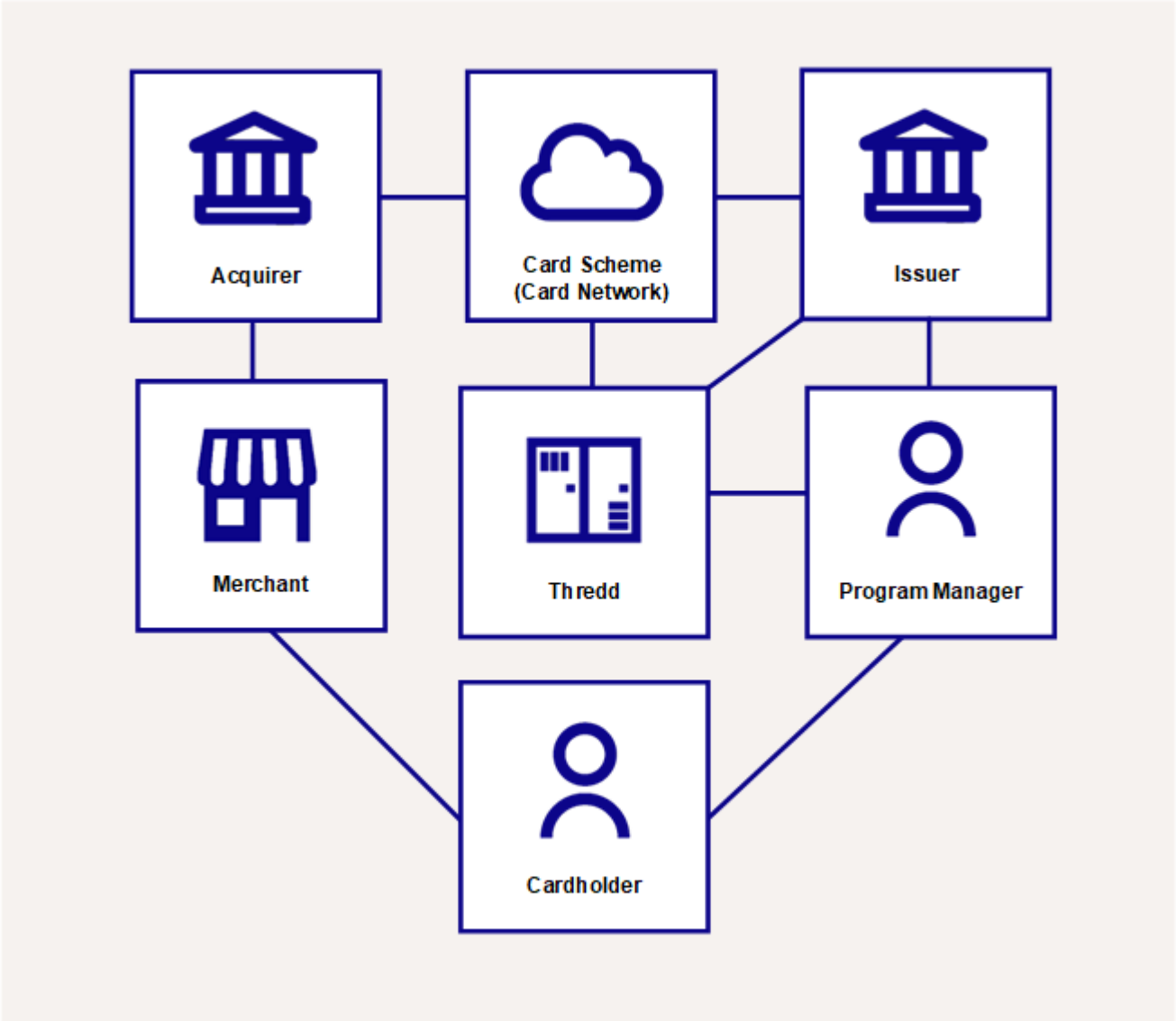

Figure 3: Thredd Model for Card Payments

The blue links in the figure above indicate where there is a connection or relationship between two or more parties. Each of these parties is explained in further detail below.

1.3 Issuers and Acquirers

Issuers and acquirers are two of the key participants in the card payment network. Traditionally, both were large and established financial organisations, such as banks. Issuers are also known as BIN sponsors.

1.3.1 Issuers

Issuers are authorised to issue cards to their customers. The cards are branded with the scheme's logo and can be used across the scheme's network. Traditionally, the card issuer would also provide the customer with the bank account linked to the card, hold the customer's money and update the bank account balance whenever the card was used for a payment transaction. Challenger banks and Fintechs have disrupted the traditional model by offering card issuing services without the need for customers to open a traditional bank account.

1.3.2 Acquirers

Acquirers derive their name from their role in acquiring merchants. Merchants are the business customers of a bank – the shops, stores, retailers and providers of services who want to offer payment facilities to their own customers (i.e., a means to take payments). The Acquirer provides the merchant with a *Merchant Account* for trading using the card payments network. Separate merchant accounts are provided for card present (in store) and e-commerce trading.

1.3.3 Interaction between Issuers and Acquirers

Acquirers enable merchants to take card payments and send payment authorisation requests to the issuer using the card scheme's network. Issuers issue cards with the schemes' logo and authorise (approve or decline) payments made using their issued cards. Every working day, money is exchanged between issuers and acquirers, to reflect transactions that have happened on the network during that day.

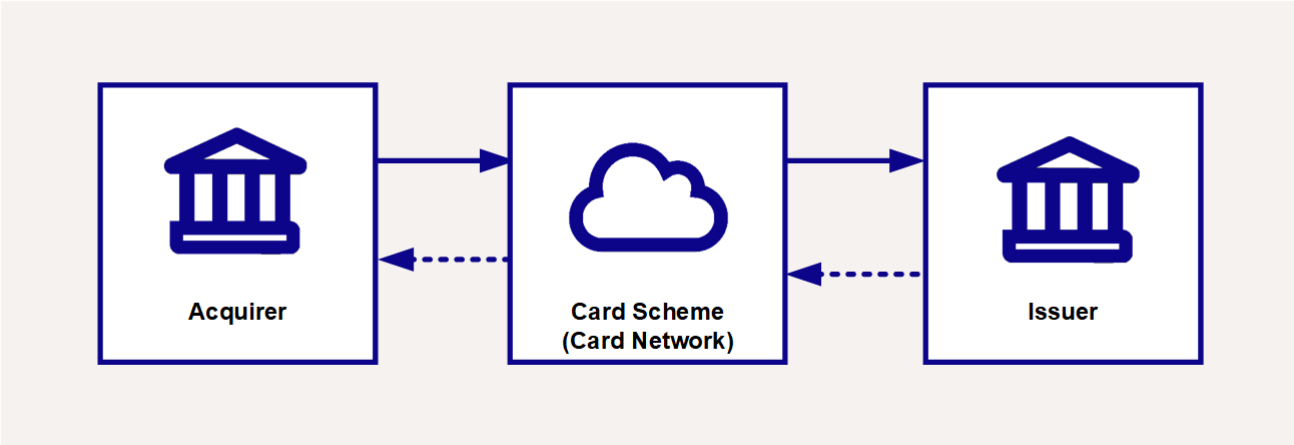

Figure 4: Issuers and Acquirers operating on the scheme's network

1.3.4 Program Managers

What's the difference between an issuer and a program manager?

Thredd refers to a company who implements a card programme as a *program manager*. The majority of Thredd customers are card program managers. Unless they are self-issuers who are licenced by the scheme, program managers must use the services of an existing issuer.

Licencing and Issuing

The issuer operates like a bank and is licenced to issue and maintain card accounts and hold client money.

The issuer has the contractual relationship with the scheme. Upon request, the scheme assigns a number of BINs (bank identification numbers) to the issuer. The issuer can allocate a BIN or sub-BIN range to their program manager customers. Using the assigned BIN or sub-BIN range, the program manager can set up a card programme, create cards, each with a unique Primary Account Number (PAN), and activate the cards for use on the scheme's network. The program manager creates and manages the cards in their programme.

Note: An issuer-processor such as Thredd can be used to create and manage card records and process transactions. Alternatively, the program manager can either build their own infrastructure to do this or use a combination of Thredd and their own systems.

There are two main scenarios for how program managers work with their issuer[1]:

- E-Money licence. (Common)
- The program manager has their own E-Money licence and uses their issuer only for BIN sponsorship. (Common as the program manager grows)

Holding of Cardholder Funds

On a daily basis, the issuer receives and manages any cardholder funds that have transferred to the issuer's bank accounts. Where Thredd performs payment authorisation services on the card, then the Thredd platform will need to be updated with the latest available card balance held by the issuer, and this can be done in one of two ways:

- Some issuers may load the card balance directly onto the Thredd system using the Thredd API (where Thredd is maintaining the card balance for the program manager).
- Alternatively, the program manager will need to load the card balance to Thredd[2].

Issuers receive daily card scheme settlement files containing details of all authorised and cleared card transactions. They will transfer or make funds available to the card scheme to reflect financial transactions on the card; the scheme will then settle directly to the acquirer.

There are additional regulatory requirements in most regions for issuers who hold client money.

Reporting and Billing

Issuers have additional reporting requirements and need to prepare daily, weekly and quarterly reports on active cards and transaction activity, which are sent to the card schemes and regulators to help monitor card usage and reduce incidents of fraud.

Scheme billing is done per identifier (Mastercard or Visa).

The schemes use the issuer's reports on card activity to bill the issuer. If there is a significant discrepancy between the issuer's reporting and the scheme's system of record for that programme, then the scheme will query this discrepancy and can impose penalties.

Since the schemes bill at identifier level and do not bill at BIN level, issuers who have multiple program managers operating under the same identifier will normally divide charges across all program managers using that identifier, rather than at a BIN level. Check with your issuer for details.

Program Manager and Scheme Relationship

The program manager typically has no direct relationship with the scheme[3]. All requests and access to scheme systems must be arranged via their issuer. Some issuers provide their program managers with access to scheme systems, such as those used for payments dispute management (e.g., Visa Resolution Online and Mastercom). Thredd can also provide access to some scheme systems, via integrated API.

Note: The Thredd platform enables program managers to integrate with the card payments network without the need to develop their own systems and infrastructure or arrange separate contractual agreements. Thredd manages the payment transaction messages received from the card schemes.

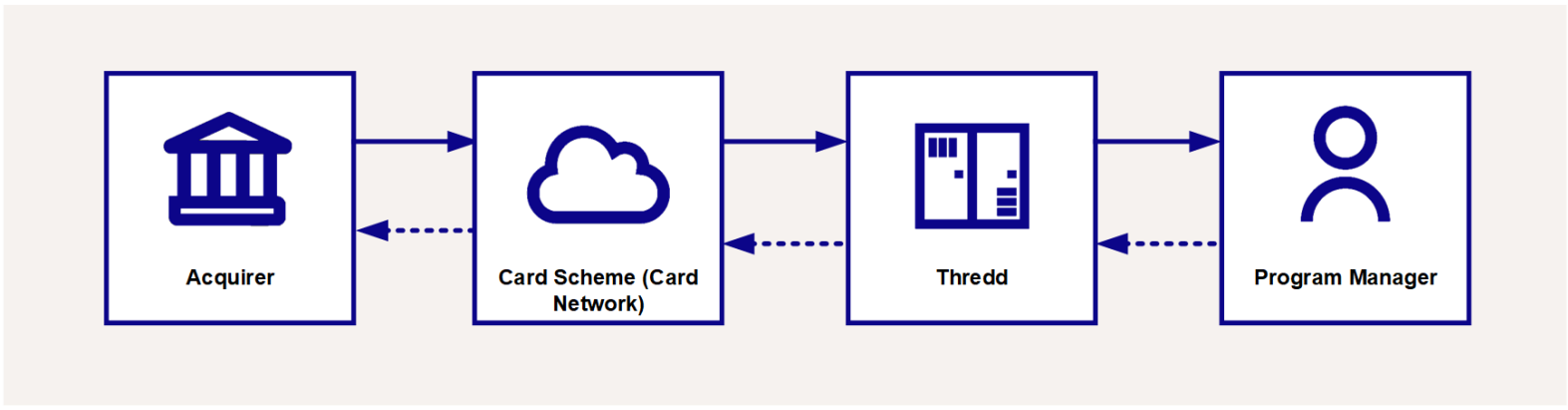

Figure 5: Connecting Program Managers to the Scheme Network

---

[1]There are other ways of working with issuers. Please speak to your Business development manager.

[2]The issuer may ask the program manager to provide prefunding for their cards – normally this covers seven days of transaction volume, but this will differ per issuer.

[3]Some program managers with direct contacts with the scheme may be asked to work under another principal member until they are large enough to become a scheme member.

1.3.5 Payment Services Provider or Payment Gateway

What's a payment services provider (PSP)/ Payment Gateway?

A payment service provider (also known as a Payment Gateway) offers merchants access to payment platforms and other payment processing services, which enables the merchant to take cardholder payments online or via a card reader terminal without needing to build their own payment infrastructure and payment systems. The payment gateway manages the communication of payment transactions between acquirers and merchants.

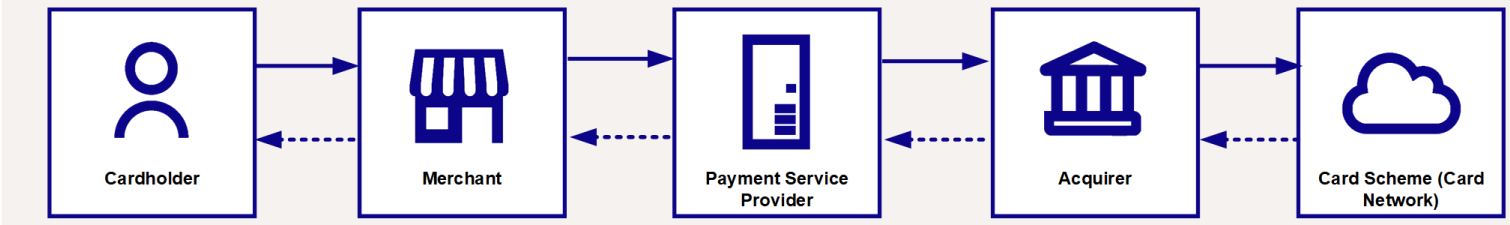

Figure 6: The Role of the PSP (Payment Gateway)

Note: As a Thredd program manager, if you want to offer your customers a means to make card payments into their account, you may need to use a payment service provider/payment gateway.

More Information

Find out more about the schemes and network participants such as issuers and acquirers using the links below.

- Thredd Key Concepts Guide – Understanding Payments

1.4 The role of Thredd in the Payments Ecosystem

Thredd is an issuer-processor, enabling program managers to launch their card programme and connect to scheme network participants using our platform.

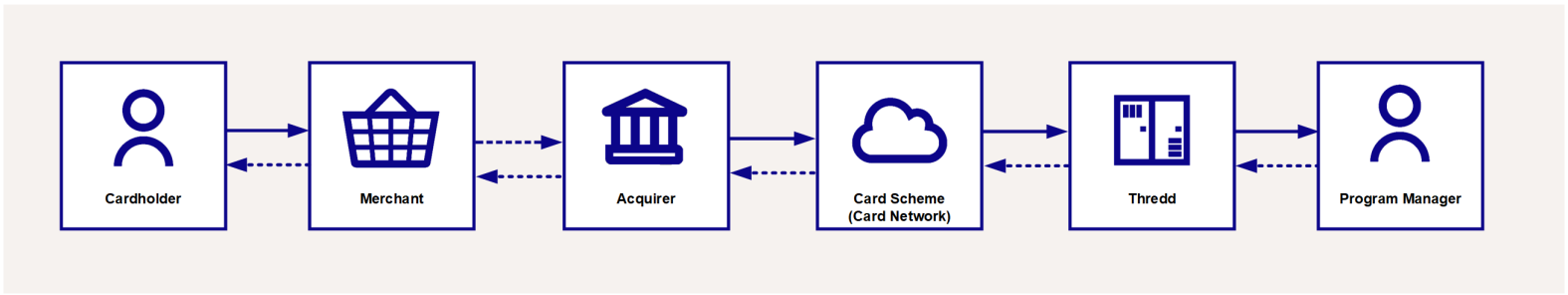

Figure 7: Role of Thredd in the Payments Ecosystem

In addition to theThredd Platform and suite of products and services, we provide detailed consultancy and support to program managers at all stages of their programme, from conception and design, through to live launch.

Thredd does not hold end-customer funds and does not fall under the regulations for financial service providers. Thredd is fully compliant with the Payment Card Industry Data Security Standards (PCI DSS), which enables us to hold and process sensitive cardholder information.

1.4.1 Thredd Platform

The Thredd Platform provides a comprehensive, robust and reliable solution for card payment processing.

The Thredd platform is integrated with worldwide payment networks 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.

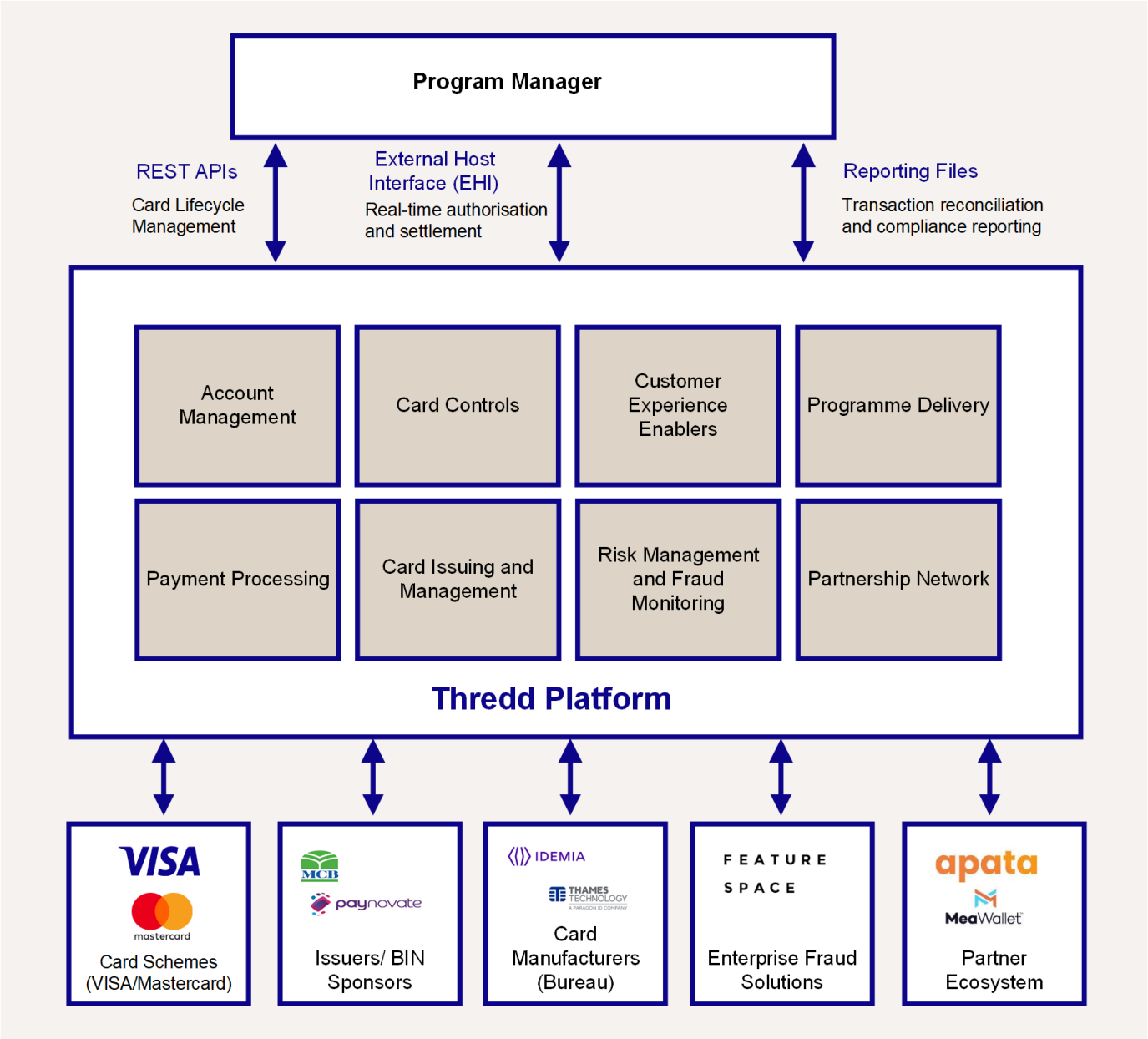

Figure 8: Thredd Platform

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. Thredd currently supports Visa and Mastercard and Discover global payment networks, as well as smaller networks that use the Mastercard Network Exchange (MNE), such as STAR and Pulse[1]. Our cloud-based processing centres ensure resilience, scalability, reliability and fast processing, in whatever region you are processing.

More Information

Find out more about the role of Thredd and what it is like to work with Thredd, using the links below.

- Thredd Key Concepts Guide – Understanding Payments
- Thredd Getting Started Guide
- Thredd Platform

1 Please check with your account manager for availability of Discover and MNE for your programme.

1.5 Regulation of Card Network Participants

1.5.1 Regulation by Region

Region	Description of Regulations
Europe	Regulated by the national regulator. Legislation is created by the European Central Bank (ECB). Note that individual EU member countries have their own regulators which align rules to ECB, but may have additional requirements.
UK	Regulated by the Financial Conduct Authority (FCA).
Singapore	Regulated by the Monetary Authority of Singapore (MAS).
Malaysia	Regulated by Bank Negara Malaysia (BNM)
Australia	Regulated by the Australian Prudential Regulatory Authority (APRA)
New Zealand	Regulated by the Financial Markets Authority (FMA)
Hong Kong	Regulated by the Hong Kong Monetary Authority (HKMA)
Japan	Regulated by the Financial Services Agency of Japan (FSA)
Philippines	Regulated by the Bangko Sentral ng Pilipinas (BSP)
Dubai	Regulated by the DFSA, The Independent Regulator of Financial Services
Egypt	Regulated by the Financial Regulatory Authority (FRA)

1.5.2 Recent Important Areas of Legislation

Below are examples of recent areas of legislation relating to card payments.

Note: Issuers are responsible for meeting card payment regulations. Please contact your issuer for further details.

Open banking and cardholder security

The majority of countries and regions implement open banking legislation to protect customers.

The Second Payment Services Directive (PSD2) is a European Union Directive from the European Central Bank (ECB) which introduced some important new rules related to open banking, to enhance the security of card payments by requiring additional levels of cardholder authentication during a payment transaction. The PSD2 rules have been widely adopted across Europe and the UK. Other regions have implemented similar legislation.

Thredd systems have been enhanced to support open banking rules around card processing. For more information, see the Thredd PSD2 and SCA Guide.

Thredd recommends you consider implementing these rules for the cards in your programme to enhance your cardholder security.

Data Protection

The majority of countries and regions implement data protection legislation covering data privacy and security of user data, designed to ensure that customer data is only collected, stored and processed for legitimate business purposes, with the consent of the customer.

Examples of legislation include the General Data Protection Regulation (GDPR) in Europe, the Personal Data Protection Act (PDPA) in Singapore, the Privacy Act 1988 and Information Privacy Act 2014 in Australia, the Federal Law on the Protection of Personal Data in the United Arab Emirates (UAE) and the Act on the Protection of Personal Information (APPI) in Japan.

Your organisation should be compliant with data protection regulations in your country or region.

Note: Under GDPR rules, Thredd is considered a data processor.

Anti-Money Laundering (AML)

Anti-money laundering (AML) is a set of regulations aimed to monitor and prevent money gained in illegal ways from entering the regulated financial system. Examples of recent regulation include the Anti Money Laundering (AML 5) EU Directive, Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 in the UK and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) in Australia.

Program managers and issuers accepting customer money must be able to verify the identity of the customer and their source of funds. *Know your Customer (KYC)* checks are a set of verification checks to identify and screen customers.

The nature of your card programme and limits associated, along with local regulations, will determine the level of KYC checks you need to do on your customers when signing them up for an account. In some cases, for example on a restricted use gift card, you may just capture information such as cardholder name, date of birth and address. For most programmes you will capture those details and verify them against different sources. For some cardholders or products, you may have to perform enhanced checks such as additional identity verification or confirming the source of their funds.

Cryptocurrency

Issuers and program managers offering cryptocurrency solutions should be aware of the changing local regulations around cryptocurrency usage.

Cryptocurrency regulation differs per country and region. Many countries require licensing and support registration of cryptocurrency exchanges. Some countries do not consider cryptocurrency a form of legal tender[1] so cardholders will not benefit from the same rights and protections as with other forms of legal tender. In Europe and the UK, you must have a licenced local entity to offer cryptocurrency. Earnings on cryptocurrency are subject to Capital Gains Tax (CGT). In some countries, such as China (excluding Hong Kong), cryptocurrency is illegal.

For more information, see https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/.

Note: Visa and Mastercard currently do not allow Cryptocurrency for spend on cards; such programmes may require additional review and programme approvals.

1.5.3 Payment Card Industry (PCI) Compliance

Topics covered: What is it? How do we get it? Who do we speak to?

The Payment Card Industry Data Security Standards Council is a global organisation that provides standards for security policies, technologies and ongoing processes that protect payment systems from breaches and theft of cardholder data. The Council was founded in 2006 by American Express, Discover, JCB International, Mastercard and Visa Inc.

The Council promotes a number of security standards, aimed to protect cardholder sensitive data:

- The **Payment Card Industry Data Security Standard (PCI DSS)** is an information security standard for organisations that handle credit cards from the major card schemes. All program managers who handle customer card data must be compliant with this standard and compliance must be validated annually[2].
- The **Payment Application Data Security Standard (PA-DSS)** is applicable to any payment applications you develop or use which store, process or transmit cardholder data and/or sensitive authentication data as part of authorisation and settlement. You should only use tested and approved applications.

For more information on the standards and requirements around protecting cardholder data, see: https://www.pcisecuritystandards.org/pci_security/

---

[1] Australia and Japan recognise cryptocurrency as legal tender, while other countries such as Singapore consider it a form of goods and service.

[2] PCI DSS validation must be done using a qualified security assessor, approved scanning vendor or, for organisations not required to compliance report, by completing a Self-Assessment Questionnaire.

There are four levels of PCI compliance, which depend on the volume of transactions processed by your organisation. For example: Level One applies to organisations processing over six million transactions a year. Level Four applies to organisations who process less than 20,000 e-commerce transactions or up to one million in-store or telephone transactions annually.

The time and costs of implementing PCI Compliance rules, together with the annual auditing costs, can be a barrier when just starting out a card programme if you do not have the business systems and processes in place to meet PCI DSS standards.

Thredd Solutions for PCI Compliance

Note: Thredd implements strong access control measures on our systems to protect cardholder data. User access to our systems is strictly controlled, using a combination of Virtual Private Networks (VPNs), IP address permissions and two-factor password authentication.

Thredd can manage cardholder data, so that you can implement a card programme without the need for PCI DSS level 1 compliance.

Note that if you are not PCI DSS Level 1 compliant, you are not able to retrieve the full 16-digit PAN from the Thredd platform (this is one of the PCI requirements to protect stored cardholder data). In this case, Thredd provides a number of options to support your requirements.

- Masked PAN: The first 6 and last 4 digits of the 16-digit PAN are displayed, while the middle 6 digits of the PAN are masked on Thredd systems.
- Thredd public token: A unique 9-digit number is used internally within Thredd systems to identify and manage updates to a card record. See Using the Thredd Public Token.
- You can use a Thredd approved third party service provider who is PCI Compliant to securely manage sensitive card data and provide support for MDES/VDEP tokenisation. Tokenisation is also referred to as digital wallets. See: Using a third-party service provider.

1.5.4 Regulatory Reporting

Issuers need to submit regular safeguarding reports (indicating the amount of cardholder money held in safeguarded accounts) and other financial reports to the regulators. For UK and European Union issuers, this format must comply with the European Single Electronic Format (ESEF) regulations.

Note: Please confirm with your issuer or regulator in your region for details.

1.6 Scheme Charges and Fees

Topics covered: What type of fees are charged for operating the card scheme network and processing transactions on the network?

1.6.1 Scheme Fees

Card scheme fees include a combination of fixed fees and variable fees. Fixed fees are based on which card scheme services are used and the volume of transactions processed. Variable fees are typically at a transaction level, based on the card type, payment method and country.

Some issuer fees are based on the quarterly QMR/QOC reports submitted by the issuer for the previous quarter. The scheme reviews the reports and bills the issuer. If there are any discrepancies, the scheme will bill based on details on record and query the discrepancy[1].

Thredd produces most of the data required for the quarterly report. Additional information required typically relates to fraud, chargebacks and losses. (The scheme provides an FX rate to use, which depends on the base currency of the issuer's products with the scheme; the issuer must align all supported billing currencies to provide the details in the equivalent base currency.)

Note: For any queries relating to scheme fees, please check with your issuer. Thredd does not have information about why specific card scheme fees may have been applied to your programme.

1.6.2 Interchange and Processing Fees

An interchange or processing fee is a transaction fee passed between the acquirer (from the merchant's account) and the issuer whenever a customer uses a card to pay for a transaction. The fee includes a handling fee and other charges. Below are examples of interchange and processing fees:

- **POS transactions** – positive interchange fee is paid to the issuer (the merchant pays)
- **ATM transactions** – negative interchange fee is paid to the operator of the ATM
- **ATM card capture** – fee is paid to the operator of the ATM
- **Stolen card fee** – processing fee paid by the issuer to the acquirer of the merchant that held back the stolen card.

Other types of fees include:

- **Foreign Exchange fees** – where the card scheme provides the exchange rate for currency conversion, they will charge a fee for this service
- **Settlement fees** – for clearing and settlement (where money is exchanged between network participants)

Note: Corporate programmes provide a higher level of interchange revenue for the issuer.

1.6.3 Chargeback and Arbitration Fees

Disputed transactions in which a Chargeback is raised may incur additional Chargeback fees, payable to the Card Scheme (Visa/Mastercard) and to the acquirer or issuer.

1.6.4 Penalties

Penalties may be charged for breaches of the scheme's rules, for example, where an issuer fails to authorise a transaction in a timely manner, not processing payments according to the scheme's rules and allowing fraudulent usage of the network.

Note: Issuers and acquirers can pass on some of these costs to their customers (program managers and merchants).

---

[1]Duplicated or missed transactions, or different classification of geographical regions may cause discrepancies. For example, domestic and international transactions should be correctly classified.

1.7 Holding of Client Funds

An issuer needs to be authorised by the banking regulator in their country to hold customer funds; see Regulation of Card Network Participants. Issuers must hold their cardholder's funds within separate, ring-fenced accounts (so that if the issuer's business fails, the cardholder's funds are protected).

The schemes also require that issuers hold a certain amount of funds in a cash reserve fund, to cover any future risks of payment default.

If you are using the services of an issuer/BIN sponsor, your issuer will be responsible for holding client funds on your behalf.

1.7.1 Financial Settlement and Reconciliation

Issuers receive daily settlement files, containing details of all financial transactions (i.e., payment transactions which have cleared and are ready to be paid). The issuer must transfer or make funds available to the card scheme for disbursement to the acquirers (and vice versa if required). This is done on a day-end netting basis, based on the total balance owed for that day.

The issuer must reconcile the cleared amounts for each transaction to the total balance amounts on each card. They also must match balances against card fees, scheme interchange and processing charges.

Note: Thredd does not hold client money. For any queries relating to client money and reconciliation, please speak to your issuer.

1.8 Using the Services of an Issuer vs. Self-Issuing

Different regions have different regulatory requirements for becoming an issuer.

Issuers have a direct relationship with the scheme as a principal scheme member. Becoming an issuer enables your organisation to negotiate better interchange rates and have more control and flexibility over your card programme.

Issuers have stringent regulatory and reporting requirements and must have additional reserve funds for settlement in place to operate as an issuer.

The majority of Thredd program managers start out using the services of an existing issuer. The need for additional finance, plus the operational requirements for regular transaction reconciliation and reporting, are some of the reasons why many program managers decide to launch their card programme using the services of an existing issuer.

The additional costs and time required to set up as an issuer, plus lack of card issuing experience, are also important factors when deciding whether to set up as an issuer or use an existing issuer.

Note: If you are using Thredd as your issuer-processor, it is relatively straightforward to upgrade to self-issuing at a later stage[1].

[1] To upgrade you will need your own dedicated scheme identifiers and the support of your current BIN sponsor

1.9 Banking Networks

In addition to the card payment networks operated by the card schemes, banks offer their customers options for transferring money between banks and into the bank accounts of other customers.

When running a card programme, offering banking services to your customers enables you to reach potentially unbanked customers and provide additional options for making and taking payments using the banking networks. If you do not have a banking licence, your issuer bank may be able to offer this service. Alternatively, an *Agency Banking* service provides an option to accept payments on behalf of your customers.

The main banking networks and systems are described below:

1.9.1 SWIFT

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a member-owned cooperative that provides safe and secure electronic payments for its members (large financial organisations, such as banks). There are over 11,000 global SWIFT member institutions. SWIFT works by assigning each member institution a unique ID code that identifies the bank name, country, city and branch.

1.9.2 BACS

Bacs Payment Schemes Limited (BACS) is an electronic system that is used in the UK to make payments directly from one bank account to another. BACS is mainly used for Direct Debits and direct credits from organisations. Transactions are cleared within 2-3 business days.

1.9.3 Faster Payments

Faster Payments is a UK scheme that enables payments such as one-off payments and standing orders to move quickly and securely between UK bank accounts, often clearing within 1-2 hours.

1.9.4 CHAPS

The Clearing House Automated Payment System is a real-time gross settlement payment system used for sterling transactions in the UK. CHAPS is an interbank money transfer system that runs through the SWIFT network. It's typically reserved for one-off, high-value payments that need to be sent and received on the same day. Transactions are cleared within a few hours.

1.9.5 SEPA payments

The Single Euro Payments Area (SEPA) enables customers to make electronic euro payments via credit transfer and direct debit to anywhere in the European Union, as well as a number of non-EU countries, in a fast, safe and efficient way.

SECTION 2: TECHNOLOGY

The Technology Behind Card Payments

This section provides a brief history of the development of card payments and describes the main types of payment instruments available.

- Card Payment Instruments

  What kind of card payment instruments are there?

3.1 Card Payment Instruments

This section provides a brief overview of the types of card payment instruments.

3.1.1 Prepaid and Debit Cards

Prepaid cards are loaded with a prepaid amount that is available for the cardholder to spend. The card is not allowed to go into negative balance, and you can provide a facility to enable your cardholders to load additional funds to the card if required.

Thredd prepaid cards provide a simple and effective way to rapidly launch a card service.

Debit cards allow the cardholder to make payments up to the available amount in their account. Payments that take the card over the available balance may be declined. The card may have a credit facility or overdraft associated, allowing the cardholder to spend more than they have loaded to the card, which typically results in additional charges[1].

Thredd debit cards provide all the functionality of a typical debit card.

3.1.2 Gift Cards

Gift cards are similar to prepaid cards, as they are loaded with a prepaid amount that is available for the user to spend and the card is not allowed to go into negative balance.

The gift card may be restricted for use to specific locations or merchant stores.

Gift cards can be private labelled and are not tied to usage by a specific cardholder (anyone with the gift card can use it). They typically benefit from reduced regulatory and licensing requirements due to low value load limits and restrictions on the types of spending.

3.1.3 Credit Cards

Credit cards are linked to a credit facility that can be paid back later. The cardholder can make payments up to the available credit limit set for their credit card account. Payments that take the card over the available limit may be declined and/or result in additional card charges. Credit cards are commonly used for certain types of bookings, such as hotel and accommodation, car hire and flight bookings.

On the Thredd platform there is no distinction between a debit and a credit card. The Thredd card must always hold a sufficient balance to enable a card payment.

Thredd provides the option to support credit payments via our External Host Interface (EHI) product (see External Host Interface). In this use case Thredd does not maintain a record of the card balance and the program manager must provide the payment authorisation decision.

3.1.4 Multi-currency Cards

A multi-currency card is linked to multiple currency wallets and enables the cardholder to pay in any desired currency. The cardholder typically has the ability to load funds into the different wallets. Thredd provides support for multi-currency e-wallets[2].

3.1.5 Virtual Cards

Virtual cards are a popular payment instrument with Thredd program managers. You can offer your customers a virtual card as an easy means to make payments online or in-store using a mobile phone. The virtual card can be activated, loaded with funds and is available for immediate use by the customer (compared to a physical card, which needs to be printed and delivered).

The virtual card image can be customised to your brand and requirements. See the example below.

---

[1] The regulatory permissions of the issuer determine available credit offerings.

[2] Subject to Card Scheme currency availability and restrictions.

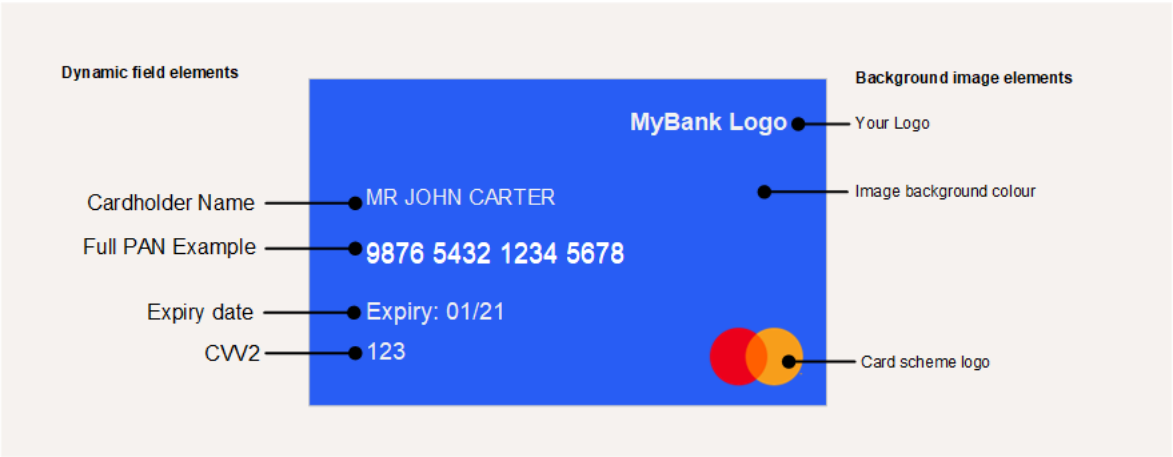

Figure 9: Virtual Card Configuration

Note: For co-branded cards featuring the card scheme's logo, each scheme has specific requirements on how their logo is used[3].

Offering virtual cards enables you to launch your card programme quickly, without the need to go through the costs and time of implementing physical cards through a Card Manufacturer.

Virtual cards can be single use for enhanced security (the card is blocked as soon as the transaction has taken place).

For more information, see Virtual Cards.

[3]For Mastercard branding rules see: https://brand.mastercard.com/brandcenter/branding-requirements/mastercard.html
For Visa branding rules see: https://www.merchantsignage.visa.com/brand_guidelines.

SECTION 3: PROCESSING

Introduction to Processing Card Payments

This section looks at how card payments are processed over the card scheme's network. If you are setting up a card programme for the first time you and your technical implementation team should read this section to understand some of the message standards and process flows relating to processing card payment transactions.

Note: In this guide we concentrate on payments made across European, UK and many Asia Pacific networks using the *Dual Message Standard*. Some regions and acquirers may implement the *Single Message Standard*. Thredd supports both message standards. For more information, see Dual vs. Single Message System.

- Transaction Message Types and More about Message Types

  What are the main transaction message types? Who defines the messaging types that are available and the messaging format used?

- The Payment Lifecycle

  Why do we have a payment life cycle? What is it? Are there regional variations? What's the difference between how Online and Offline messages are processed?

- Processing Transactions with Thredd

  Who decides when to approve or decline a transaction, and how does this process differ depending on the channel in which the payment is made (e-commerce, MOTO, POS)? What happens when a system is unavailable to approve or decline?

3.1 Overview

When a cardholder uses a card at a merchant's website or store, the merchant takes payment (enters the payment amount and cardholder details). The merchant may use the services of a payment service provider (PSP) to process the payment (i.e., provide the physical card reader or online payment gateway). The payment is passed to the acquirer, who then connects to the card scheme. The card scheme then passes the authorisation request to the issuer for approval.

For program managers using Thredd as their issuer-processor, Thredd receives the authorisation request directly from the card scheme and provides an authorisation response (approve or decline). See the figure below.

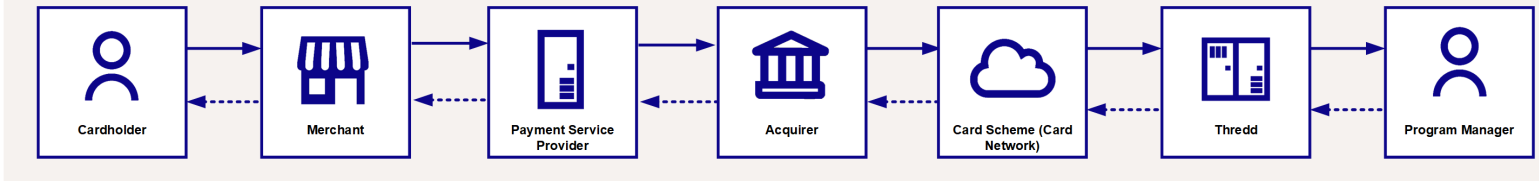

Figure 10: Typical Flow for an Authorisation Request

Note: The Figure above is a simplified view which does not include 3D secure authentication

3.2 Transaction Message Types

The ISO 8583 standard describes the message types to be used for financial transactions. Conformity to an ISO standard helps to ensure a consistent way to present financial transaction messages, which can be adopted across the different schemes. In general, Mastercard, Visa and Discover Card Scheme networks follow the ISO 8583 standard, but with some discrepancies and exceptions.

When acquirers send transactions through the card scheme network, they identify the *message type* they are sending, using a *Message Type Identifier (MTI or MTID)* field. The MTID field contains a four-digit number used for all card-originated transactions, and its format is defined by ISO 8583. It identifies the *version number*, *message class*, *message function* and *transaction originator*. See the figure below.

Version Number	Message Class	Message Function	Transaction Originator
0 — ISO 8583:1987 1 — ISO 8583:1993 2 – 7 — reserved for ISO use 8 — reserved for national use 9 — reserved for private use	0 — reserved for ISO use 1 — authorisation 2 — financial 3 — file action 4 — reversal/chargeback* 5 — reconciliation 6 — administrative 7 — fee collection 8 — network management 9 — reserved for ISO use	0 — request 1 — request response 2 — advice 3 — advice response 4 — notification 5 – 9 — reserved for ISO use	0 — acquirer 1 — acquirer repeat 2 — card issuer 3 — card issuer repeat 4 — other 5 — other repeat 6 – 9 — reserved for ISO use

*Reversal if transaction originator is *acquirer* and Chargeback if transaction originator is *issuer*.

Examples:

0100	ISO 8583:1987	authorisation	request	acquirer
0101	ISO 8583:1987	authorisation	request	acquirer repeat
0220	ISO 8583:1987	financial	advice	acquirer
0402	ISO 8583:1987	chargeback	request	Card issuer

Figure 11: MTID Format

Note: Thredd processes messages received from the Card Scheme networks. We provide our customers with a single and consistent message format which combines fields received from the scheme with additional Thredd enhanced information.

3.2.1 What are the main ISO message types?

The table below summarises the main ISO message types that are sent over card payment networks.

MTID	Message Type	Description
0100	Authorisation Request	Request from the acquirer to authorise a transaction (payment or refund). A response is required to approve or decline the transaction.
0101	Authorisation Repeat (Visa Only)	Request from the acquirer for a repeat authorisation. A response is required to approve or decline the transaction.
0120	Authorisation Advice	Advice from the acquirer to notify of an authorisation. The issuer responds to acknowledge the message.
0400	Authorisation Reversal Request	Request from the acquirer to reverse a previous authorisation. A response is required to approve or decline the transaction.
0420	Authorisation Reversal Advice	Advice from the acquirer to notify of an authorisation reversal. The issuer responds to acknowledge the message.
1240 (Mastercard	Financial Notification	Advice from the acquirer for a financial transaction such as a presentment, financial reversal or chargeback. The notification is received in the scheme's clearing files.

MTID	Message Type	Description
only)		Issuers must use this information to update the card balance details to reflect payments that have been made or any charges on the card. **Note**: Visa clearing messages are not ISO-standard compliant and therefore do not use MTIDs.

* A *Request* is a message type that requires an online authorisation response (approve or decline). An *Advice* is a message type that is sent for information purposes and which does not require an online authorisation response.

3.3 The Payment Lifecycle

3.3.1 Regional Variations

Depending on the region in which your card program operates, the payment transaction message cycle may differ. There are two main types of messaging standards or systems, referred to as *Dual Message System* and *Single Message System*:

- **Dual Message System** – follows a payment messaging standard which provides separate messages for the authorisation and clearing (presentment) stages. It is the prominent method in Europe and also used in other regions.
- **Single Message System** – is a transaction processing message standard which combines authorisation and presentment in a single message. It is more common in regions such as the US and Asia Pacific and within those regions, for certain types of transactions, such as those where payment is captured at the same time as authorisation.

For more information, see Dual vs Single Message Systems.

In this guide, we will be referring to messages processed using the Dual Message System.

3.3.2 Basic Transaction Flow (Dual Message)

A single card payment request may consist of multiple transactions that relate to the same payment request. For example:

	Message Type	From	MTID	Description
1	Authorisation request	Acquirer	0100	A message from the acquirer to approve or decline a payment.
2	Authorisation response	Issuer	0110	A message response from the issuer of *approve* or *decline*.
3	Financial notification (presentment)	Acquirer	1240	A message from the acquirer to indicate that an authorised payment has been taken. This will only be sent if the authorisation response was *approve*.

See the figure below.

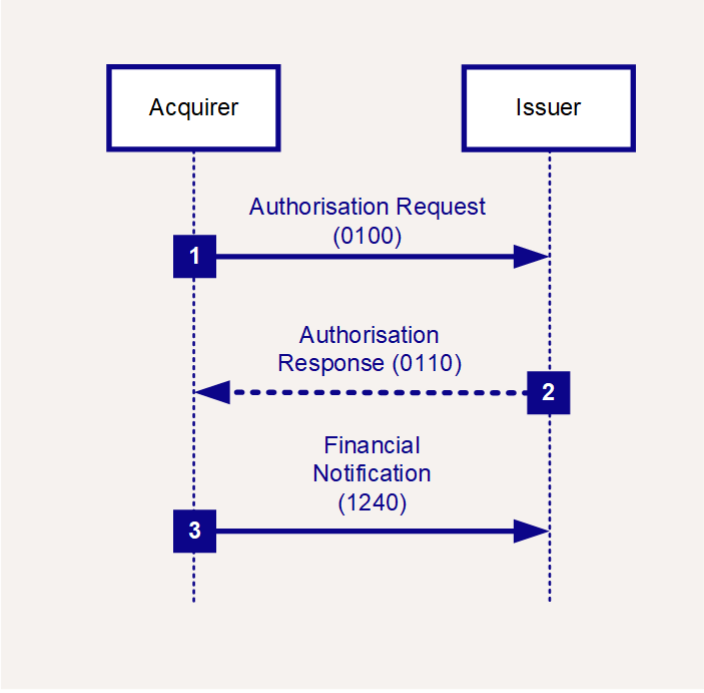

Figure 12: Multiple Transactions in a Cards Payment

The above is a simplified example. During the life cycle of a typical payment there are many other types of transaction messages that may be generated and sent over a card payment network. Let's take a look at some common examples.

Note: In these examples, we have simplified the message flow to show only the interaction between the acquirer and the issuer.

Note: If you are using Thredd, then Thredd acts as the issuer-processor, receiving messages from the card scheme. Thredd provides initial card checks and processing and can either authorise the transaction or forward to the program manager's systems for approval. The program manager can either maintain the card balance or Thredd can maintain this.

Note: In the examples below, where we mention *issuer*, in practise this will be either Thredd or the program manager.

3.3.3 Example 1: Purchasing in store followed by a refund

In this example, a customer purchases an item in store and later on requests a refund.

Message Flow

	Message Type	From	MTID	Proc Code[1]	Description
1	Authorisation request	Acquirer	0100	00	A message from the acquirer to approve or decline a payment.
2	Authorisation response	Issuer	0110	00	A message response from the issuer of *approve* or *decline*.
3	Financial presentment	Acquirer	1240	00	A message from the acquirer to indicate that an authorised payment has been taken.
4	Authorisation request	Acquirer	0100	20	A message from the acquirer to approve or decline a payment refund. This may be for the full amount or a partial amount.
5	Authorisation response	Issuer	0110	20	A message from the issuer of *approve* or *decline*.
6	Financial presentment	Acquirer	1240	20	A message from the acquirer to indicate that the refund has been processed.

Transaction Flow

A cardholder purchases an item in store and the merchant submits a payment authorisation request. The message flow between acquirer and issuer is as follows:

1. The acquirer sends an initial payment authorisation request (0100 authorisation request message) through the card scheme network to the issuer to authorise (*approve* or *decline*) the payment. This authorisation request message is processed in real-time (within milliseconds).
2. The issuer sends a response (0110 message) to the acquirer to approve the transaction (the issuer checks the available balance on the card and can either *approve, decline* or provide a *partial amount approval*; this response must be processed in real-time). The issuer blocks any approved funds on the card, so that the amount cannot be used for other transactions.
3. On the same day, the acquirer sends a financial message (1240 message) to indicate that an authorised payment has been processed.

   The issuer receives this as part of the scheme's daily clearing files. The issuer can now deduct the funds from the card.
4. A few days later, the cardholder returns the purchased item to the merchant's store and requests a refund. The acquirer sends an 0100 authorisation request message for a refund to the issuer.
5. The issuer sends a response (0110 authorisation response message).
6. On the same day the acquirer sends a financial message (1240 message) to indicate that the refund has been processed.

   The issuer adds the refunded amount back on to the card's available balance.

[1] First two digits only of the processing code. 00 = purchase; 20 = refund.

3.3.4 Example 2: Booking hotel accommodation

In this example, a hotel sends an Account Status Inquiry, which has a billing amount of zero, to check the status of the card. This is followed by an authorisation request for the full amount.

Message Flow

	Message Type	From	MTID	Proc Code	Description
1	Account Status Inquiry	Acquirer	0100	00	A message from the acquirer to check the status of the card. (The hotel does not know the final amount at this stage.)
2	Authorisation response	Issuer	0110	00	A message response from the issuer of *approve* or *decline*.
3	Authorisation request	Acquirer	0100	00	An authorisation request from the acquirer to approve or decline the full payment amount.
4	Authorisation response	Issuer	0110	00	A message response from the issuer of *approve* or *decline*.
5	Financial presentment	Acquirer	1240	00	A message from the acquirer to indicate that the full payment has been taken,

Transaction Flow

A cardholder books a hotel on a hotel booking website and the merchant website submits a payment authorisation request to check that the card is valid.

1. The acquirer sends an Account Status Inquiry, which has amount of zero, to check the status of the card.
2. The issuer sends a response (0110 message) to approve the transaction.
3. The hotel requests an authorisation for the full amount, after calculating costs for all hotel services used.
4. The issuer sends a response (0110 message) to approve the transaction.
   The issuer updates the card's available balance.
5. The acquirer sends a message (1240 message) to the issuer to indicate that an authorised payment has been processed. This message is received as part of the daily clearing files.

3.3.5 Example 3: Low value card chip payment in a shop (offline authorisation)

In offline authorisation, the card terminal verifies the card chip and the chip card approves the transaction, with no online authorisation.

Message Flow

	Message Type	From	MTID	Proc Code	Description
1	Financial presentment	Acquirer	1240	00	A message from the acquirer to indicate that an authorised payment has been taken.

Transaction Flow

A cardholder makes a purchase in a shop using their card which authorises the purchase offline. At the end of the day, the acquirer sends a financial notification for the final amount. There will not be a matching authorisation.

The issuer must update the card's available balance.

Note: The program manager can configure their card chips to permit or disallow offline transactions.

3.3.6 Example 4: Purchasing Petrol at an Automated Fuel Dispenser

Generally, Automated Fuel Dispenser (AFD) messages are received with an initial amount. The acquirer then sends a second authorisation advice message as an advice, which contains the exact transaction amount.

Message Flow

	Message Type	From	MTID	Proc Code	Description
1	Authorisation request	Acquirer	0100	00	A message from the acquirer to approve or decline a payment. (The final amount is unknown, so either a nominal one unit of currency or a maximum amount may be specified, depending on the scheme rules for the region.)
2	Authorisation response	Issuer	0110	00	A message from the issuer of *approve* or *decline*.
3	Authorisation advice	Acquirer	0120	00	A message from the acquirer to notify the issuer of the final billing amount.
4	Authorisation response	Issuer	0130	00	A message from the issuer.
5	Financial presentment	Acquirer	1240	00	A message from the acquirer to indicate that an authorised payment has been taken.

Transaction Flow

1. The acquirer sends an initial payment authorisation request (100 message).
2. The issuer responds with *approve* or *decline* (0110 message).
3. The acquirer sends an authorisation advice (0120 message) to notify the issuer of the final billing amount.
4. The issuer responds with an acknowledgement (0130 message).
   The issuer updates the card's available balance.
5. The acquirer sends a financial notification (presentment) for the final amount.

Note: Thredd provides additional authorisation advice messages to program managers:

- If the final amount is more than the initial authorised amount, then Thredd sends an authorisation advice of type J to the program manager.
- If the final amount is less than the initial authorised amount, then Thredd sends an authorisation reversal advice of type D to the program manager.

3.4 Processing Transactions with Thredd

This section describes how Thredd can help you to authorise and process card transactions.

3.4.1 Receiving Transaction Messages

Program managers can use the real-time Thredd External Host Interface (EHI) API to receive card payment transactions from the scheme network.

Depending on your business requirements and resources, you may need to implement your own card balance and authorisation engine to manage transaction messages received from Thredd. Thredd can do these processing steps for you if you do not want to implement a separate authorisation engine.

For more information about the different options for receiving Thredd EHI messages, see EHI Modes.

Note: Details of transactions are also available through Thredd transaction reports and can be viewed on the Thredd Smart Client.

3.4.2 Authorisation Approvals and Declines

When an authorisation request arrives, Thredd runs a number of initial checks:

- Incoming message format and integrity checks.
- Is this a genuine transaction and is the card a valid card?
- Is the cardholder permitted to make this transaction (e.g., the card is not over its configured daily spend amount or single transaction amount)?
- Have any configured risk checks been passed?
- Is there a sufficient *available balance* on the card for the requested authorisation amount?
- Has Strong Customer Authentication (SCA) been performed on the transaction or does the card qualify for any SCA exemptions? (applicable to issuers implementing SCA in relevant regions)

Thredd works in conjunction with the program manager to make all necessary card control, card and transaction validation checks, as well as available balance checks.

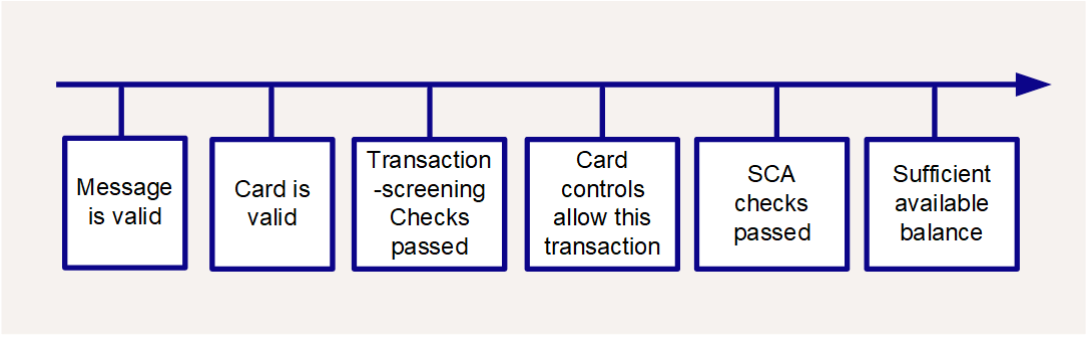

Figure 13: Thredd Card Transaction Checks

If all checks are passed, then the transaction can be *approved*. Otherwise, the transaction is *declined*.

Approving the Transaction

Who approves the transaction depends on a number of factors, including whether it is Thredd or the program manager's systems which hold the latest card balance. See below for details of possible configuration options.

Who authorises?	Who maintains the card Balance?	Description	Recommended EHI Setup Option
Your organisation's	Your organisation's	Your systems maintain the card balance and make the ultimate authorisation decision[1].	Gateway Processing (mode

[1] Thredd may decline the transaction due to reasons such as PIN check failure or chip cryptogram failure.

Who authorises?	Who maintains the card Balance?	Description	Recommended EHI Setup Option
systems	systems	You update the card's balance in your card database to reflect the available balance on the card after this transaction.	1)
Your organisation's systems	Your organisation's systems + Thredd	Both your systems and Thredd manage the card balance, but your systems make the ultimate authorisation decision. You provide Thredd with details of any card loads/unloads and balance adjustments (using the Thredd web services/cards API). *Approve with load* If Thredd declined the transaction due to insufficient balance, you can override the Thredd decline by using *approve with load*. In your authorisation response message you can provide Thredd with details of the latest balance on the card, which will update the Thredd held balance.	Cooperative Processing (mode 2)
Thredd	Thredd	Thredd maintains the card balance and makes the authorisation decision and necessary balance adjustments. You provide Thredd with details of any card loads/unloads and balance adjustments (using the Thredd web services/cards API).	Full Service Processing (mode 3)
Your organisation's systems (Thredd as fallback)	Your organisation's systems + Thredd	In some instances, your systems may be unable to respond to the authorisation request in time (e.g., due to a system failure or processing delay on your end). In this case, Thredd can provide Stand-In Processing (STIP) on your behalf. You provide Thredd with details of any card loads/unloads and balance adjustments. EHI mode 5 is the same as EHI mode 4, except that clearing messages do not update the Thredd held balance.	Gateway Processing with STIP (mode 4) Gateway Processing with STIP (mode 5)
Your Systems (Scheme as fallback)	Your Systems	An alternative option is to enable scheme Stand-In Processing for you when you are unable to respond to an authorisation request in time.	Scheme configuration (not related to EHI)

For more information about the different options for authorisation processing and balance control using the Thredd External Host Interface (EHI), see External Host Interface.

Note: In some cases, a program manager may decide not to use EHI. In this case all authorisation decisions will be made by Thredd. No real-time notifications will be sent to your systems.

3.5 Complying with Payment Services Regulations

Payment processing regulations are defined by the card schemes, together with local and internal regulatory bodies and financial authorities/ombudsmen. See also Regulation of Card Network Participants.

Below is a list of common regulations. Check with your Thredd development manager for additional regulations specific to your region.

Regulation	Description
Payment Card Industry Data Security Standard (PCI DSS)	An information security standard for organisations that handle credit cards from the major card schemes. All program managers who handle customer card data must be compliant with this standard and compliance must be validated annually.
Payment Application Data Security Standard (PA-DSS)	Applicable to any payment applications you develop or use which store, process or transmit cardholder data and/or sensitive authentication data as part of authorisation and settlement.
Second Payment Services Directive (PSD2)	This European Union (EU) Directive from the European Central Bank (ECB) introduced some important new rules relating to open banking to enhance the security of card payments by requiring additional levels of cardholder authentication during a payment transaction (a process called Strong Customer Authentication or SCA). The rules came into force in 2021 and have been widely adopted across Europe and the UK. Other regions are introducing similar legislation to support open banking and reduce card-not-present (CNP) fraud, such as the Consumer Data Right (CDR) in Australia, Open Banking initiatives in Singapore, The Open Banking Framework in Bahrain and the Japanese Banking Act.
General Data Protection Regulation (GDPR)	EU regulation covering data privacy and security of user data, designed to ensure that customer data is only collected, stored and processed for legitimate business purposes, with the consent of the customer. Other regions may also have similar data protection legislation, such as the Personal Data Protection Act (PDPA) in Singapore, the Privacy Act 1988 and Information Privacy Act 2014 in Australia and the Federal Law on the Protection of Personal Data in the United Arab Emirates (UAE) and the Act on the Protection of Personal Information (APPI) in Japan. Your organisation should be compliant with GDPR regulations in your region.
Anti-Money Laundering (AML)	AML requirements vary, depending on the region in which you are located.
Card Scheme Rules	The card schemes issue their own rules and regulations which all network participants must adhere to. It is the responsibility of all issuers and program managers to be aware of these scheme rules.

3.5.1 Where to find out more?

- PCI Compliance: https://www.pcisecuritystandards.org/pci_security/
- PSD2 and SCA: PSD2 and SCA Guide.
- GDPR: https://gdpr.eu/

Section 4: Implementing

Implementing a Card Programme

Assuming you have now decided to implement your programme, what are some of the considerations? Where can you find out more information?

- Determining the Regions in which to Issue Cards

  What considerations must you take when determining the regions in which to issue cards?

- Selecting a Card Scheme

  What card schemes are available? What considerations should you make when choosing a card scheme?

- Selecting an Issuer (BIN Sponsor) or Setting up for Self-issuing and Issuing BIN's

  What considerations must you take when selecting an Issuer (BIN Sponsor) or setting up for Self-Issuing?

- Working with Card Manufacturers

  What do you need to know when working with Card Manufacturers?

- Offering Services to your Customers and Deciding how customers will fund their accounts

  What systems, processes and resources need to be in place to support your customer when you launch your service?

- Integrating the Thredd Service

  What do you need to do to integrate the Thredd Service?

- Stages in Implementing a Card Programme

  What stages are there when implementing a Card Programme?

4.1 Determining the Regions in which to Issue Cards

Has your organisation decided in which regions and countries to launch your service? Below are some considerations:

- Where do you have physical offices or where are your relevant staff members located?
- Do you understand the local cultures and languages of the regions in which you will be operating your service?
- Do you understand the financial and payment regulatory framework of the country in the which you are issuing?
- Do you have a unique proposition or product or service of value to customers in this region?
- What currencies are you going to support?
- What are your current plans for future expansion into other regions?

A local presence may be required to deal with cardholder queries relating to their cards or to specific transactions on their cards. Understanding of the local language, culture and regulatory environment is essential for launching a successful card programme in any region.

Note: Your Thredd business development manager can help you explore some of these considerations. Decisions around the countries and currency combinations in which you are going to issue cards has a material impact on how your card programme is set up within Thredd.

4.2 Selecting a Card Scheme

Thredd currently supports global card issuing through both Mastercard and Visa. Below are some considerations when selecting a scheme:

- If you are self-issuing, you should consider the respective sign-up costs and scheme-specific issuer requirements and systems made available for issuing
- If you are using the services of an existing issuer, they may require you to use a scheme of their choosing or suggest a preferred scheme
- Transaction costs associated with processing messages on the scheme's network may vary, depending on the scheme
- Regions in which the scheme operates

Mastercard and Visa are both global and competitive and offer comparatively similar products and services. You may prefer to select a specific scheme based on the regions in which they operate, any promotional campaign they are currently running or because their service and costs feels a better match for your business requirements. Your Thredd business development manager can help you explore some of these considerations.

4.3 Selecting an Issuer (BIN Sponsor) or Setting up for Self-issuing

An important consideration when launching a card programme for the first time is deciding whether to use the services of an existing card issuer or to start off self-issuing. Below are some important considerations:

- How quickly do you need to launch your card programme?
- Are you compliant with your local or regional financial services regulations around handling of customer money?
- Do you have sufficient reserve capital to set up as an issuer?
- Do you have the necessary financial systems in place to support self-issuing?
- Do you have expertise in the handling of financial messages, clearing, reconciliation and settlement processes associated with being an issuer?
- What are the long-term objectives for your programme? For example, once you are set up as an issuer, do you intend to offer issuing services to other potential program managers?

Setting up as an issuer involves additional regulatory, financial and payment processing requirements and costs.

Using the services of an existing issuer can save considerable time and reduce the financial outlay associated with setting up as an issuer. If speed of launch and initially minimising costs is a concern, then using an existing issuer may be a better option.

Thredd has connections to a wide range of card issuers globally, who are already connected and set up in our systems. If your issuer is not currently set up, we can add them (additional setup costs and time may apply). Your Thredd business development manager can help you explore some of these considerations.

It is relatively straightforward, when using Thredd, to upgrade to self-issuing at a later stage[1].

[1]Subject to additional setup costs and card BIN migration. You will require dedicated scheme identifiers and support from your BIN Sponsor.

4.4 Issuing BINs

The Bank Identification Number (BIN) is the first six or eight numbers on a payment card, which identifies the institution that issues the card. When you select a card issuer, they will provide you with either your own BIN, for use on your card programme, or a range within a shared BIN.

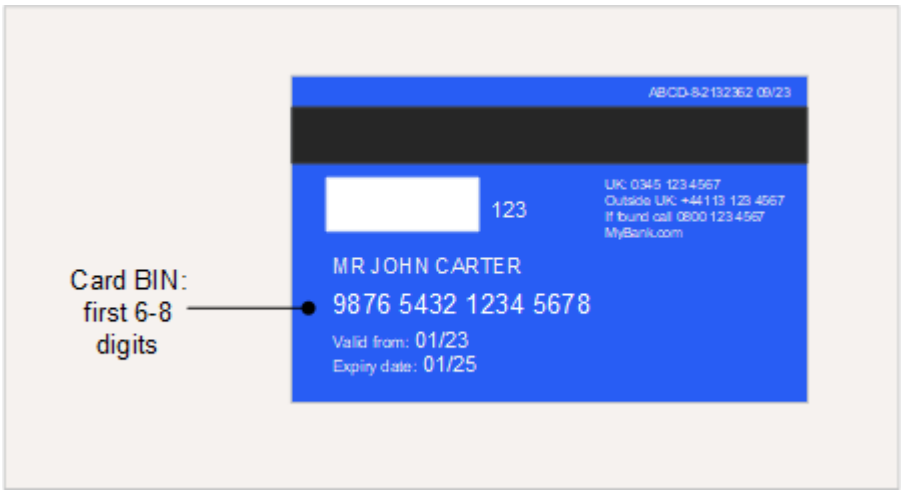

Figure 14: Example of a card BIN

BINs are issued by the relevant Card Scheme (e.g., Visa, Mastercard or Discover). A BIN can only be issued to a licenced BIN sponsor.

The BIN setup and assignment determines the type of card, such as credit, debit or prepaid, and some high-level attributes (such as number of ATM PIN tries allowed).

Scheme reporting can be set up at BIN level or can combine BINs.

You can split your BIN into account ranges (sub-BINs), to support different countries, currencies and products. The account range splits at the Card Scheme must align with the account ranges you have set up at Thredd.

You can use the services of an existing issuer to provide you with BINs or apply for your own BINs directly.

Some issuers provide shared BINs, which are used to issue small programmes and white-labelled solutions, and which offer the benefit of speed to market.

4.5 Working with Card Manufacturers

If your card programme requires printing of physical cards, you can use one of our many pre-integrated card manufacturers in the region where you are issuing cards.

For a list of currently supported card manufacturers, see the Web Services Guide: Card Manufacturers.
If your preferred card manufacturer is not on this list, please contact your Thredd Implementation Manager to discuss.

For details of the steps required in setting up your printed cards with your card manufacturer, see the Getting Started Guide: Stages in a Project.

4.5.1 Instructions for Card Manufacturers

Thredd provides an XML file interface which allows card manufacturers to accept card generation files from Thredd. Card files are sent on a daily basis, or at a frequency that can be customised for your service. The card manufacturer prints the cards and sends these to the cardholder or to the requested delivery address. For details, see the Thredd Card Generation Interface Specification.

4.6 Offering Services to your Customers

Early on during your implementation project you should consider and plan the systems, processes and resources that will need to be in place to support your customers when you launch your service. Below are some important considerations:

- How will customers sign up to your service, activate their cards and load their accounts with funds?
- How will you verify the customer's identity and run basic fraud screening checks to prevent money-laundering and identity theft?
- How will the customer's funds be protected?
- How will customers be able to check their account balance and view details of specific transactions?
- How will customers be able to transfer funds into and out of their account?
- How will customers be able to report lost and stolen cards?
- How will they be able to close their account? What will you do with cardholder data once the account is closed?
- How will customers change their PIN and renew an expiring card?
- What types of fees and services will you be charging your customers? (e.g., for ordering new cards and replacement cards, chargebacks, currency conversion or any overdraft facility being offered)
- What systems, customer service teams and processes will be in place to support customer queries and manage disputes relating to specific card transactions?
- What type of statements will you be providing to your customers?
- What systems and processes will be in place to store customer records and card information and log customer queries?
- Will you provide your customer with a mobile app and web-based customer portal to enable them to self-service? Do you have the capability in-house to build this application layer or will you be outsourcing?
- Before launching your card service, what type of tests will you put in place to ensure that the full end-to-end cardholder journey works?
- How will you record information about the transactions processed on your cards and reconcile card balance and payment information on your systems, with information received from Thredd and your issuer?

Your Thredd business development manager can help you explore some of these considerations.

4.7 Deciding how customers will fund their accounts

Your customers will need a method to transfer funds into their account or take money out of their account. In practice, your website or customer mobile app will need to offer your customer a way to make a payment. This payment could be:

- Using a debit or credit card – you may need to sign up with a Payment Service Provider (PSP) to offer your customers this service.
- Loading funds from their bank account – using the banking network (BACS/CHAPS and faster payments).
- Regular payments from their bank account – using direct debit (UK only).

4.8 Integrating the Thredd Service

Once you have signed up to Thredd and completed your issuer and Thredd product setup forms, you are now ready to start integrating your systems to Thredd. Below is a high-level summary of what your development team will need to do:

√	Explore the Thredd API in our Sandbox environment.
√	Request access to Thredd systems and test account credentials for your dedicated account.
√	Integrate the Thredd API into your front-end apps/back-end systems.
√	Use the Card Transaction System to put through transaction simulations.
√	If using the Thredd External Host Interface (EHI), configure your systems to be able to receive and process EHI messages.
√	If using the Thredd daily XML reports, configure your systems to process these reports.
√	Integrate your back-end authorisation and message processing engine and databases to update card transaction and balance details, based on messages received via EHI and XML reports.
√	Train staff members on the use of Thredd systems and how to support cardholders.
√	Pilot test your initial cards internally before rolling out to your customers.

For more information about the steps in integrating the Thredd service, see the Thredd Getting Started Guide.

4.9 Stages in Implementing a Card Programme

The figure below provides an illustration of the journey in implementing a card programme, with some example timescales. Note that timings will vary, depending on the nature and complexity of your card programme. Your Thredd business development manager can provide you with more information on the steps and timescales relevant to your specific circumstances.

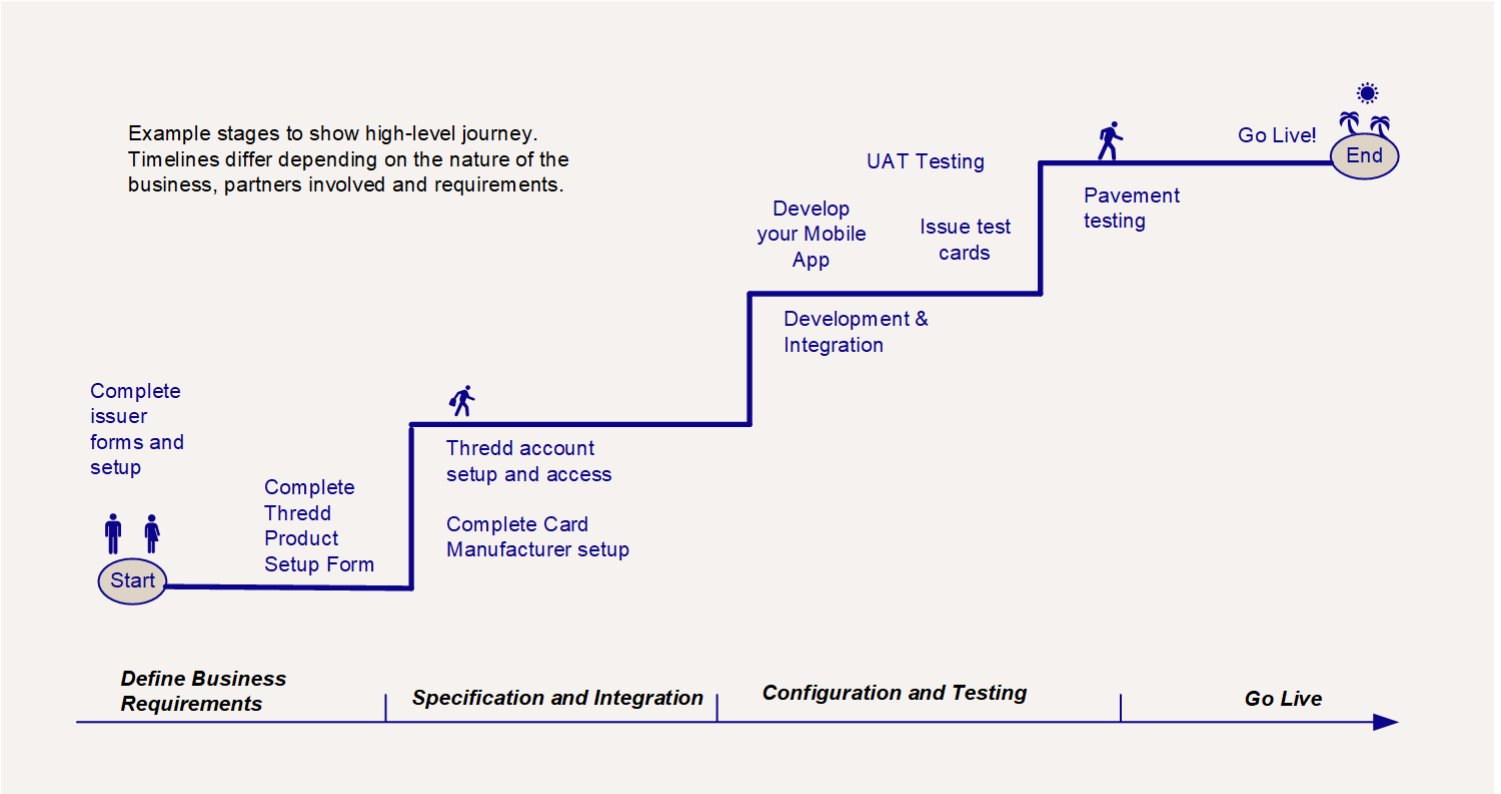

Figure 15: The Card Programme Journey - with typical stages

For more information about each of the steps is implementing your card programme through Thredd, see the Thredd Getting Started Guide.

SECTION 5: CONFIGURING

Configuring your Card Products

In this section we explore some of the options available to you when setting up your card programme through Thredd.

The product options for your card programme are set up during the implementation phase of your project, with the support of your Thredd implementation manager, who will provide recommendations based on your requirements.

- Card Usage and Controls

  What options are available when setting up your card programme through Thredd?

- Virtual Cards

  It is possible to provide virtual cards only, which are available for immediate use, without the need for any physical card? Can you customise the Virtual Card Image?

- Physical Cards

  What options are available when configuring the chip profile? What aspects of the card appearance can be configured? What card personalisation options are available?

- Mobile Wallet Payments and Tokenisation

  What options are available when setting up tokenisation for your mobile wallet ?

- Security and Fraud Management

  What card verification checks can you customise? What card verification and security checks are available? What is Fraud Transaction Monitoring? What card control groups can you customise? What permission lists can you customise? What is 3D Secure?

- Multi-currency FX

  What Foreign Exchange (FX) Services are available?

5.1 Introduction

The product options for your card programme are set up during the implementation phase of your project, with the support of your Thredd implementation manager, who will provide recommendations based on your requirements.

5.2 Card Usage and Controls

Thredd industry-leading card configuration options help to ensure that the characteristics of your cards can be tailored to the needs of your service. Configuration includes features to enhance the security of your cards and reduce the risk of fraud. Configuration can be applied at a product level, across all your card products or to a specific card.

Card configuration and control profiles, known in Thredd as *Card usage groups* are set up during the implementation phase of your project. Thredd provides access to API to enable you to dynamically change the configuration settings of your cards whenever needed. You can maximise customer self-service through the API.

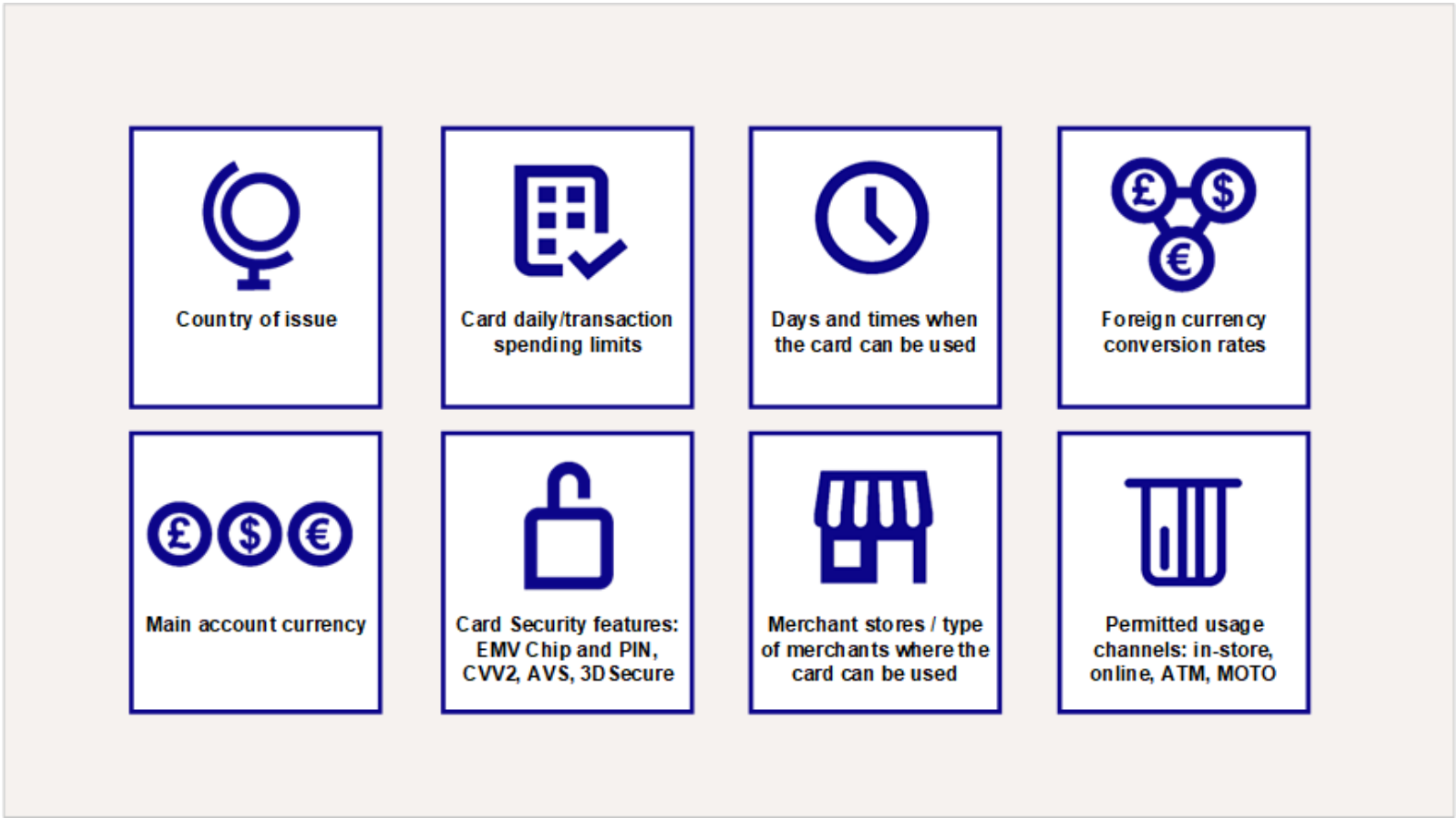

Figure 16: Control how your cards can be used

See below for examples:

- Control the merchant stores and the type of merchants where the card can be used. For example: limit use to a specific shopping mall or set of merchants, or prevent card usage for certain types of merchants (e.g., gambling sites)
- Control the types of transactions enabled on a card. For example: Chip & PIN, Contactless, ATM and e-commerce
- Restrict the frequency and/or amount at which the card can be loaded or unloaded. For example: $12000 load limit
- Restrict the daily spending limit. For example: 600 EUR spending limit
- Control the dates and times when cards can be used. For example: prevent usage on certain days and religious holidays
- Control the rates for Foreign Exchange (FX) currency conversions if the purchase currency is different from the card's currency
- Define configuration options specific to the provisioning of a digital payment token (MDES/VDEP).

5.3 Virtual Cards

A virtual card is a card that does not have any physical cards generated and can only be used to pay for purchases online (e-commerce) or via Mail and Telephone Order (MOTO). Virtual cards are set up at the Card Scheme (Mastercard or Visa) with restricted usage and cannot be used at a Point of Sale (POS) terminal or for ATM withdrawals. You can define on the Thredd system further restrictions as to how and where the virtual card can be used.

When a virtual card is created, it functions like a normal card record on the Thredd system, however the card record is not sent to print. This means it can be issued instantly to your customers, as there is no need to wait for physical card delivery. All relevant card details, such as the card Primary Account Number (PAN), the Expiry Date and the CVV2 number can be displayed on the virtual card image or delivered by different means, such as: SMS, email, or through your own Customer mobile app or Customer Portal.

5.3.1 Virtual Cards and Tokenisation

It is possible to provide virtual cards only, which are available for immediate use, without the need for any physical card. Virtual cards that have been tokenised via the Mastercard Digital Enablement Service (MDES) or Visa Digital Enablement Platform (VDEP) can also be used at POS and contactless-enabled ATMs. See Tokenisation.

5.3.2 Virtual Card Image Design

If you are using the Thredd system to generate a virtual card image you can customise the appearance of the background image and dynamic text elements. Alternatively, you can generate the virtual card image on your own systems, using the details returned in the Thredd response to a Create Card request. See the example below.

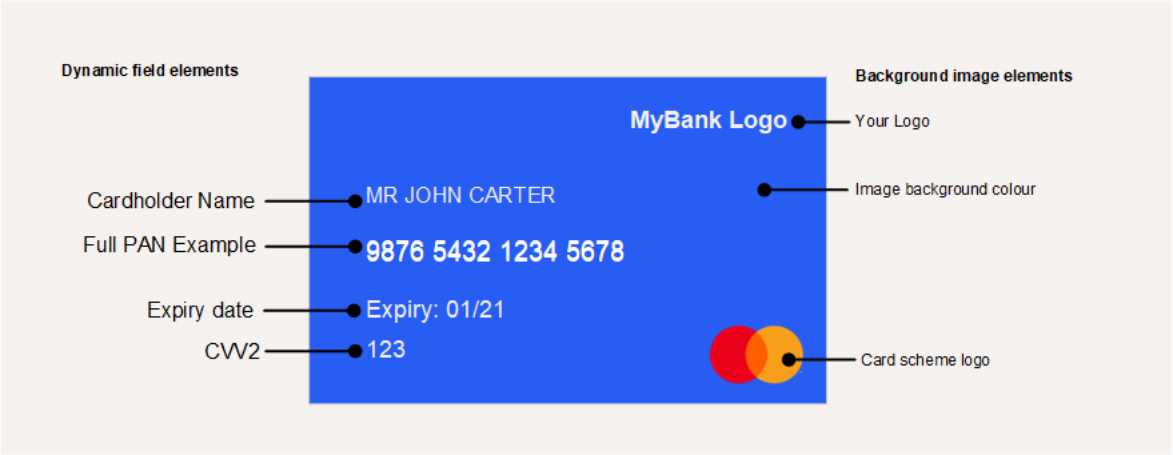

Figure 17: Virtual Card Configuration

Note: We can return full PAN if you are PCI-DSS compliant, else the middle 6 digits of the PAN will be masked.

For more information, see the Virtual Cards Guide.

5.4 Physical Cards

5.4.1 Chip Profiles

The EMV chip is a microchip embedded on the payment card which stores card data. During an EMV terminal transaction, the chip generates a one-time unique code for each transaction.

The chip profile in a card determines where and how the card can be used and how the card will interact with the card reader terminal in-store or at an ATM. Different chip profiles are provided for standard, contactless and dual interface cards.

Below are examples of some of the configuration data set on the chip profile:

- Supported cardholder authentication methods (e.g., support for PIN, signature and none)
- Language, country and currency settings
- Limits and settings to control if transactions can be approved offline
- Transaction types that can be supported (e.g., cash or purchase)
- Channels that will be supported (e.g., POS, ATM)

The issuer chip profiles are set up within the card scheme. All new chip profiles must go through testing and scheme certification.

An issuer can decide to support multiple chip profiles and assign a profile that is best suited for a particular portfolio (BIN). Typically, your issuer will offer a default chip profile for use on your cards. You can submit a change request to change the default chip profile.

Note: In some cases, you may be able to use a previously certified chip, saving time to market. Speak to your card manufacturer about options.

5.4.2 Card Appearance

When issuing printed cards, you can control the branding, layout and appearance of the card.

Cards sizes

The standard credit, debit and prepaid card size is 3.37 inches (85.6mm) length × 2.125 inches (53.98mm) height × 76 mm thick. For more information, see the ISO/IEC 7810:2003 standard (ID-1 category).

Please check with your card manufacturer and issuer for supported print sizes.

Scheme branding vs your own branding

Depending on the type of card being issued, the scheme may stipulate dual branding, or permit you to issue cards with your own brand:

- **Dual branding** – the card features both the scheme logo and the program manager's card brand. Typically required for debit and credit cards.
- **Private labelled cards** – the card features the program manager's card brand only. Used for gift cards and prepaid cards only.

Additional text

The card may feature text such as a contact centre number to call for card queries, or legal information about the legal entity that issued the card.

5.4.3 Card Personalisation

Card personalisation refers to the elements of the card that are customised to each cardholder. The type of dynamic data that is printed onto the base card includes:

- **Cardholder name** – the name printed, indented or embossed on the card, based on details supplied when you submit a create request.
- **PAN** – Thredd generated Primary Account Number (typically 16-digit), based on the available BIN range provided by your issuer. This is unique to each card.
- **Valid from and Expiry date** – Thredd generated date, based on the date of the request. You can optionally specify the card expiry date.
- **CVV2/CVC2** – system generated 3-digit Card Verification Value/Card Verification Code, used in card-not-present transactions to confirm that the cardholder has the card in their possession.

You can customise the order, font size and colour of these fields.

5.5 Mobile Wallet Payments & Tokenisation

Tokenisation is a security technology which replaces the sensitive 16-digit permanent account number (PAN[1]) 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 Funding PAN (FPAN).

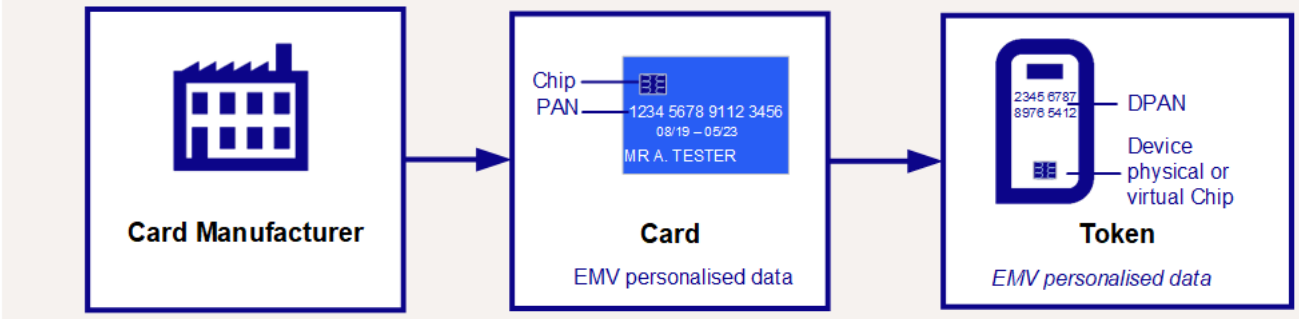

Figure 18: Tokenisation Process

Tokenisation enables cardholders to access mobile wallet functionality – provided by companies such as Apple and Android – which allows payments to be made in store from a smart device such as a smartphone or tokenised device. Tokenisation also helps merchants to improve the security of online payment transactions by replacing the sensitive PAN card details with a token and storing this instead. The token can then be used for repeat or recurring payments.

Both Mastercard and Visa offer a tokenisation service to card issuers. Mastercard offer the Digital Enablement Service (MDES) and Visa offer the Visa Token Service (VTS); Thredd refer to the Visa service as the Visa Digital Enablement Program (VDEP). Thredd supports both of these tokenisation services.

For more information see the Tokenisation Guide.

[1]The PAN is also referred to as a Funding PAN (FPAN).

5.6 Security and Fraud Management

Managing risk is always a trade-off. You can only make your cards 100% secure by not allowing any transactions. The risk of fraud needs to be balanced against the flexibility and ease of use you want to enable for your customers. Thredd offers a number of products and services to help you reduce the incidents of fraud.

5.6.1 Cardholder Verification Checks

These are checks that merchants can use to verify the identity of the cardholder:

- **Signature**: A manual check by the merchant that the signature matches the one on the back of the card.
- **PIN verification**: Typically a 4-6 digit personal identification number (PIN) is entered by the customer at a POS terminal or ATM and verified by Thredd or the chip card. PINs are blocked after three incorrect attempts. You can change card PINs and unblock PINs using the Thredd Web Services.
- **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 to accept an order. AVS is one of the most widely used fraud prevention tools in card-not-present transactions. The usage of AVS varies, depending on the country.
- **3D Secure authentication**: 3D Secure (3-domain structure), also known as *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, Mastercard and Discover. For more information on Thredd support for 3D Secure, see Thredd Docs Portal: Cardholder Authentication (3D Secure).

5.6.2 Card Verification and Security Checks

When the card is used, there are a number of card verification and security checks that can be performed at the point of sale, to validate that the card is a genuine card:

- **Card Verification Value/Code 1 (CVV1 or CVC1)**: A 3-digit number which is located on the card's magnetic stripe tracks 1 and 2. It is used to help prevent fake magnetic stripe transactions, but is vulnerable to copying if someone can see the original magnetic stripe data.
- **Card Verification Value/Code 2 (CVV2 or CVC2)**: A 3-digit number which is located on the card, which is entered by the customer in an e-commerce transaction. It is used to help prevent fraud in card-not-present transactions, since only the cardholder should be able to see this number.

5.6.3 Fraud Transaction Monitoring

Using adaptive behavioural analytics and machine learning, Fraud Transaction Monitoring adapts to new fraud types and identifies unknown threats by detecting unexpected changes (anomalies) in real-time data. This improves transaction monitoring, identifies fraud and reduces the number of occurrences where legitimate transactions are flagged as suspicious, payments are stopped or accounts locked. For more information, see Thredd Docs Portal: Fraud Transaction Monitoring.

5.6.4 Card Control Groups

Thredd provides a number of options to enable you to manage the risks associated with card payments. For example:

- **Limit groups**: Velocity limit group which restricts the frequency and/or amount at which the card can be loaded or unloaded.
- **Usage groups**: Group that controls where a card can be used. For example: Point of Sale (POS) or ATM.

Card control groups are set up at the time when you first implement your card program through Thredd. The control groups linked to a card can be changed dynamically using the Thredd web services or cards API (which you use via your customer app to enable your cardholders to control their card spending limits and card usage).

5.6.5 Permission Lists

You can configure allow and disallow lists which determine where a card can be used, based on the Merchant ID or Merchant Category Code (MCC).

5.6.6 Cardholder Authentication (3D Secure)

Cardholder authentication, also known as Payer Authentication, is a security process that protects both cardholders and merchants by verifying the cardholder's identity during an online transaction. Examples of cardholder authentication programs are Verified by Visa and Mastercard Identity Check, which are both implementations of 3D Secure.

The latest 3D Secure solutions support 2-factor authentication and Strong Customer Authentication (SCA), through means such as biometric identification.

Thredd offers a fully integrated 3D Secure service for both Mastercard and Visa cards. For more information, see Thredd Docs Portal: Cardholder Authentication (3D Secure).

5.7 Multi-currency FX

The Thredd Foreign Exchange (FX) service enables you to deploy seamless currency conversion solutions quickly and easily, avoid complexity, and reduce your operational costs and risks. The solutions support Visa and Mastercard and integrate with leading FX rate providers to provide a shorter time to market, allowing you to focus on delivering the right customer experience and propositions.

SECTION 6: MANAGING

Managing your Card Programme

In this section we explore some of the options available to you for managing your cards and servicing your customers.

Your Thredd implementation manager can help you to set up and maintain card configuration options at a card product and card programme level. In addition to these pre-configured settings, you can dynamically configure many features of a card at the time when the card is created and update some features of the card at any time, using the Thredd API.

- Creating New Cards

  What options are available when creating new cards?

- Card Management

  What Card Management options are available?

- Transaction Management

  What Transaction Management options are available?

- Handling Cardholder Queries

  How do Thredd manage cardholder queries?

- Managing Payment Disputes/ Chargebacks

  How do Thredd manage Payment Disputes/Chargebacks?

- Release Management and Change Control

  How do Thredd handle issues, manage system changes and enhancements, and add new features and services to your card programme?

6.1 Creating New Cards

Creating new card records on the Thredd system is done using either our REST-based cards API or SOAP web services . For more information see:

- REST API: Cards API website > Creating a Card
- SOAP API: Web Services Guide > Card Create

The Thredd API provide flexible options for configuring the appearance and features enabled on the new card. Below are a few examples.

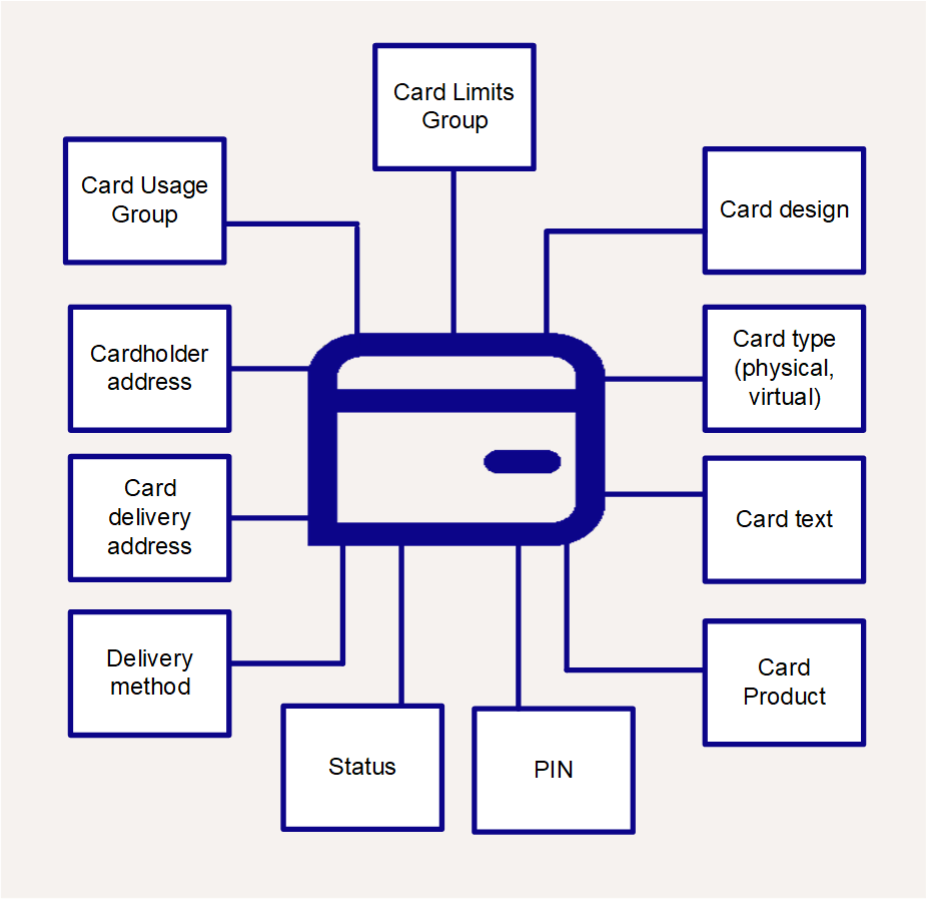

Figure 19: Examples of Configurable Card Features

For details of the card configuration options available when you create a card, see the Cards API website or Web Services Guide.

6.1.1 Activating your cards

Thredd supports multiple card activation scenarios for the cards in your programme:

- If you are creating a virtual card, the card can be created in a status of *active*, so that it can be used immediately.
- If you are creating a physical card, then the card can be created in an initial status of *inactive*, and when the customer receives their card, they can activate it using an App or online (with Thredd web services/cards API), through the Thredd IVR (interactive Voice Response) system or contacting your call centre.

6.1.2 Printing of cards

For a physical card, instructions are sent (on a daily basis or at a customised frequency) to your card manufacturer, for printing and dispatch (either directly to the cardholder or to the designated delivery address).

Virtual cards are created with a virtual image, which you can display to your customers on your customer portal/mobile app or send to them via email.

6.1.3 Loading cards

You can load a balance onto the card at the time when the card is created or at any time, using the Load/Unload Cards API (REST) or Card Load web service (SOAP) .

6.2 Card Management

Thredd provides you with a wide range of Thredd API for on-demand configuration and updates to your cards. See below for examples.

PIN Change	Status Change	Balance Adjustment	Card Renew
Change the card PIN	Change the status of the card (example, active, lost, stolen, destroyed)	Load, unload and adjust the balance on the card	Renew an expiring card

Control Group	3D Secure	Balance Enquiry	Convert Card
Change the usage and control groups linked to the card	Enrol a card in 3D Secure and add 3DS credentials	Find out the balance on the card	Convert a virtual card to a physical card

For more information, see the Cards API website (REST) or Web Services Guide (SOAP)..

6.3 Transaction Management

To help you view, or approve and manage real-time and financial transactions processed across the scheme networks, Thredd provides an API interface, which we call the *External Host Interface (EHI)*.

EHI is a Thredd system which sends real-time payment authorisation requests and other types of financial messages to your systems.

Your systems must be able to receive and process messages sent from EHI to your external host endpoint.

6.3.1 EHI Modes

Depending on your EHI mode, you may need to authorise (approve or decline) payment requests on a card and adjust the card balance held in your systems to reflect any authorisation or financial messages received. Detailed information on how to do this is provided in the External Host Interface (EHI) Guide.

EHI supports the following modes:

Setup Option	Mode	Description
Gateway Processing	1	Your systems maintain the balance and perform authorisation.
Cooperative Processing	2	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	3	Thredd maintains the balance and performs authorisation. You receive a read-only response.
Gateway Processing with STIP	4	Your systems maintain the balance and perform authorisation. Thredd provides Stand-In authorisation if the external host is unavailable.
Gateway Processing with STIP	5	Your systems maintain the balance and perform authorisation. Thredd provides Stand-In authorisation if the external host is unavailable. Clearing transactions closed, such as presentments, do not update the Thredd stand-in balance.

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

6.4 Handling Cardholder Queries

Your cardholders should have a means to contact you directly to raise queries about a transaction on their account. This is typically via a call centre number printed on their card[1] or advertised on your website. Alternatively, your customer mobile app or portal may provide a form to enable customers to raise a support ticket, which is handled via your customer app or a dedicated system.

When a cardholder queries a transaction, you can use the Thredd Smart Client application to view details of the transaction. For more information, see the Smart Client Guide.

[1] You can configure the contact number printed or displayed on your card products.

6.5 Managing Payment Disputes/ Chargebacks

A chargeback is a type of transaction where a cardholder contacts their card issuer to dispute a payment and request their money back for an item or service purchased using their card. The cardholder can only dispute a charge on their account and request a chargeback where they have a valid reason (for example, where payment has been taken fraudulently or goods were not received). Funds can only be recovered in line with card scheme rules.

The card schemes provide rules and processes, as well as systems to handle chargebacks.

You can also view and manage your chargebacks via Smart Client.

Thredd provides a chargeback service that enables you to raise chargebacks directly with Mastercard[1].

For more information, see the Payments Dispute Management Guide.

[1]Not available in all regions. Currently restricted to Mastercard cards only.

6.6 Release Management and Change Control

After you go live, your organisation will need to provide resources to handle issues, manage system changes and enhancements, and add new features and services to your card programme.

6.6.1 System Changes

Thredd provides Pre-Release Notifications (PRNs) to inform you of any system changes that may affect your service. Notifications are sent to affected customers 4 weeks in advance.

Depending on the type of change, we may not notify you via the PRN process (e.g., where you do not need to change your systems).

6.6.2 Regulatory and Scheme Changes

Thredd will implement mandatory financial services regulations and card scheme mandates.

Regulatory changes affecting financial services and payments are region and country specific. For example, the European Union issues directives which all financial firms operating in the European Union must follow, such as the Second Payment Services Directive (PSD2). Countries may enact specific local regulations relating to payment processing. Thredd will endeavour to update our systems where required to comply with these regulations and provide you with advance warning.

Note: If you know of any upcoming local regulation in your region that may require a change to card transaction processing for your programme, then you should contact Thredd as soon as possible to discuss your requirements.

Visa and Mastercard operate a 6-month Business Enhancement Release process (with major releases in April and October[1]). Changes are communicated to Thredd and issuers via Visa *Articles* and Mastercard *Announcement Notifications (ANs)* –also called Mastercard Bulletins and Release Announcements.

We will notify you of these changes, where they affect our systems, via our PRN process. Some changes require that you also update your systems and processes.

6.6.3 Adding New Features

Thredd adopts an agile development process, with four builds and one planned release per month. These changes include regular patches, fixes and enhancements to our systems, software and infrastructure.

Where a change impacts on your service or requires you to update your systems, we will notify you of these changes via our PRN process.

[1] There are four releases in total annually: two major plus two additional minor releases.

6.7 What to Look Out for

6.7.1 Checklist

The checklist below provides a summary of key factors to consider in implementing an manging your card programme through Thredd.

Area	Description
Business Case	Do you have a well thought out business case that considers anticipated costs and future user needs?
Programme Setup	Has your programme been set up in a way that considers future needs, such as supported countries and currencies?
Card Configuration	Have your card products been set up and configured to match your business requirements?
Card Controls	Do you have appropriate card usage controls in place to ensure cards can only be used at the locations you permit and for permitted amounts, to reduce the risks of fraud?
Development and testing	Have you fully designed, developed and tested all systems and applications providing the service, and checked that everything works from an end-to-end perspective?
Cardholder Interaction	How are you going to interact with your customers? What staff and systems will be in place to answer queries about problems with the card, change of address, issues with specific transactions or to report fraudulent transaction?
Customer self-service	How will you provide options for customers to self-service their account? Will customers be able to change their PIN, change their contact details, view the account balance, view recent transactions, view account statements or request a new card?
Transaction Handling	Do you have the systems in place to manage the authorisation and card balance update process?
Reporting and Reconciliation	Do you have the systems in place to manage transaction reporting and reconciliation?
System Maintenance	Do you have development resource in place to support updates to your card programme systems and routine maintenance tasks?

6.7.2 Common Challenges and Thredd Recommendations

- It takes longer than you think.
- Many third parties are involved in setting up a card programme – such as schemes, issuers, tokenisation service providers and 3D secure providers. Time to market will vary depending on the complexity of your programme.
- For new cards, we recommend you always run an internal staff pilot before rolling out your service to external customers.
- Plan for change. Your card programme doesn’t stop when you go live – system changes and maintenance will require ongoing resources and investment.

6.8 How Thredd can Support You

Thredd provides customers with support through all stages of implementing a card programme:

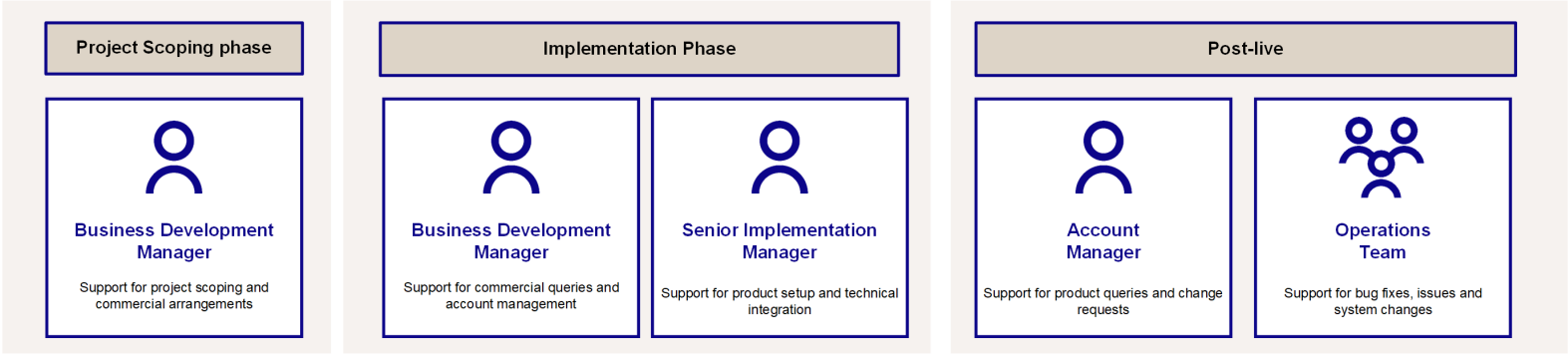

Figure 20: Thredd Support Roles

After you go live, Thredd provides 24*7 customer support through our globally distributed Thredd Customer Care team. The Thredd Command centre and Monitoring teams are available 24*7 to monitor network activity and respond to any issues identified.

Glossary

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

A

Acquirer

Banking organisation and licensed scheme member that enables merchants to take card payments and send payment authorisation requests to the issuer using the card scheme's network.

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.

B

BID

The Business Identification Number (BID) is an ID number assigned by Visa that identifies an issuing bank. A BID can have multiple BINs associated with it.

BIN

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

BIN Sponsor

An issuer that allocates a BIN or a BIN range to their program manager customer, to enable the program manager to launch a card programme.

Buy Now, Pay Later (BNPL)

Buy now, pay later (BNPL) is a financing option that allows customers to purchase goods or services and pay for them in installments over a period of time, typically a few weeks or months, instead of paying the full amount upfront.

C

Card Manufacturer

Company that prints newly issued physical cards and sends to cardholders.

Card Scheme (Network)

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

Chargeback

A chargeback is a type of transaction reversal initiated by the Issuer or Programme Manager in order to recover funds from the acquirer of the transaction, in a case of a cardholder dispute; or merchant error resulting in a financial loss to the issuer. The reversal is typically passed on to the merchant by their acquirer.

Clearing

The process of exchanging financial transaction details between an acquirer and an issuer to facilitate posting of a cardholder's account and reconciliation of a customer's settlement position.

Cryptocurrency

A digital currency in which transactions are verified and records maintained by a decentralised system using cryptography, rather than by a centralised authority.

E

E-Money licence

License provided by the scheme or issuer which enables a program manager to offer card services and other financial products to their customers, without the need for a full banking licence.

EHI

The External Host Interface (EHI) is a Thredd system that enables Thredd customers to receive and respond to real-time transaction data as well as financial messages.

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.

F

Fintechs

Innovative Financial Technology Companies.

I

ICA

The Interbank Card Association (ICA) number is a four-digit number assigned by MasterCard that identifies an issuing bank. An ICA can have multiple BINs associated with it.

Issuer-processor

Third party agent certified by the card scheme to accept and process card network transactions on behalf of the issuer.

Issuer (BIN Sponsor)

Financial organisation and scheme member, licensed by the scheme to issue cards and process transactions using the scheme's network.

L

Legal tender

Coins or banknotes that must be accepted if offered in payment of a debt.

M

Mastercom

System from Mastercard for raising disputes and sharing messages during the dispute management process.

MDES

The MasterCard Digital Enablement Service (MDES) is a platform for generating and managing digital payment tokens.

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.

N

Near Field Contact (NFC)

A short-range wireless connection that uses magnetic field induction to enable communication between devices within a few centimetres of each other.

O

Offline authorisation

An authorisation transaction which relies on the card reader terminal scanning the card chip and authorising, without going through the online card payment network to request authorisation from the issuer.

Online authorisation

An authorisation message that requires real-time and immediate processing via the card payment network and an immediate response from the issuer.

Original Credits Transactions (OCT)

Original credits are fund transfer transactions from one entity to another and are not linked to a previous transaction. Visa Fast Funds/OCT and Mastercard Money Send are examples. Unlike refunds, most of the Fund Transfer transactions should be funded to the target card within 30 minutes of authorisation.

P

Payment service provider (PSP)

Enables merchants to take cardholder payments online or via a card reader terminal without needing to build their own payment infrastructure and payment systems.

PCI Compliance

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 customers who handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security

Primary Account Number (PAN)

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

Private Labelled Card

A card which features the program manager's card brand only (without the Visa or Mastercard logo).

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

Settlement

Process where the issuer provides funds to the scheme (Mastercard or Visa) equivalent to the sum of all transactions. It is the physical movement of funds between issuer and acquirer.

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

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 Thredd mode, Thredd may also provide STIP on your behalf, where your systems are unavailable.

Strong Customer Authentication (SCA)

Authentication which is a combination of two factors of identification at checkout. Examples include something they know (such as a password or PIN), something they get (such as an OTP in a mobile phone or other device) or something they are (such as their fingerprint).

T

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.

Two-factor authentication

Cardholder authentication which combines two separate authentication channels during the authentication process (e.g., PIN entry + One-Time Password sent to a mobile phone).

V

VDEP/VTS

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

Visa Resolution Online

System from Visa for raising disputes and sharing messages during the dispute management process.

W

White Labelled Card

Card solution where you provide the physical or virtual card, but enable other companies to offer a card with their brand image included.

Document History

Version	Date	Description	Revised by
1.3	04/07/2024	Updated the company address.	PC
1.2	09/04/2024	Updates to content and graphics to align with taxonomy updates on our Documentation Portal.	WS
	10/08/2023	Update to Figure 3. Payments Model. Update to Figure 8, Thredd Platform.	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
1.1	01/12/2022	Updated Copyright Statement.	MW
1.0	10/11/2022	First version	WS

Contact Us

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

Thredd Ltd.

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

Technical Publications

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