Physical Card Configuration Guide

Version: 1.1

29 April 2024

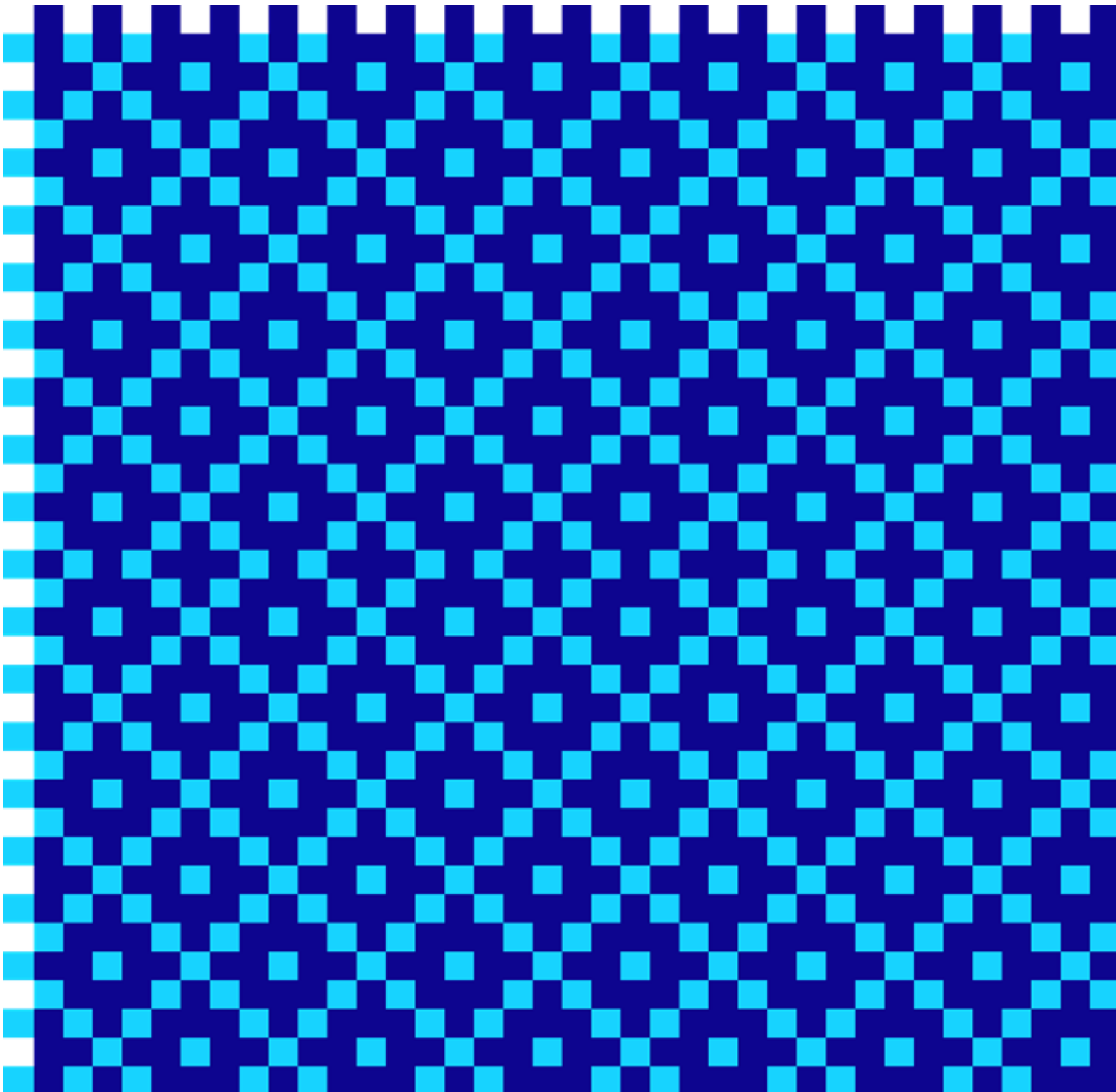
Publication number: PCCG-1.1-4/29/2024

For the latest technical documentation, see the Documentation Portal.

Thredd 6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682



Copyright

1 About this Guide

This guide provides information on how to set up and configure your card programme to support physical (printed) card production.

1.1 Target audience

This guide is aimed at developers who need to understand how to set up their physical card products and use the API to create and update the cards in their programme.

1.2 What's changed?

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

1.3 How to use this Guide

Before you start:

- If you want to understand how card products work on the Thredd system, read the Overview.
- For details of how to go about setting up your card products, see Setting up your Card Products.
- For information on supported card manufacturers and how to work with them, see Working with Card Manufacturers.
- For information on how to use the Thredd web services API or the Cards API to create and manage your cards, see Creating Cards and Managing Cards.

1.4 Related Documents

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

Document	Description
Web Services Guide	Describes how to create and manage the cards in your programme using our Thredd web services API (SOAP).
Cards API Website	Provides details of how to create and manage the cards in your programme using our REST-based Cards API
Thredd Card Generation Interface specification	Provides detailed specifications for card manufacturers on Thredd card creation.
Virtual Cards Guide	Provides details of how to create and manage virtual cards
Tokenisation Guide	Describes how to tokenise your cards
Smart Client Guide	Describes how to use the Thredd Smart Client to view transactions and manage the cards in your programme.
EHI Guide	Provides details of the Thredd External Host Interface (EHI), a system for transaction authorisation and financial messaging.

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

2 Overview

This section provides an overview of how cards are set up on the Thredd system.

2.1 Card Programmes and Card Products

In the Thredd system, each Program Manager (Thredd client) is associated with a card issuer (BIN Sponsor) .

The Program Manager is linked to an internal Institution and internal Thredd Scheme, to reflect the regions, BIN ranges, card type (physical, virtual or a combination) and card manufacturer.

A typical card programme consists of one or more card products. The card product defines aspects of the card, such as the country of issue and base currency.

The Program Manager can define multiple card usage groups that control how and where the card can be used. The card usage group can be automatically associated with a card product and be applied to all newly created cards. Alternatively, an individual card record can be dynamically linked to card usage groups using the Thredd API (either at the time the card record is created, or afterwards).

The figure below provides further details.

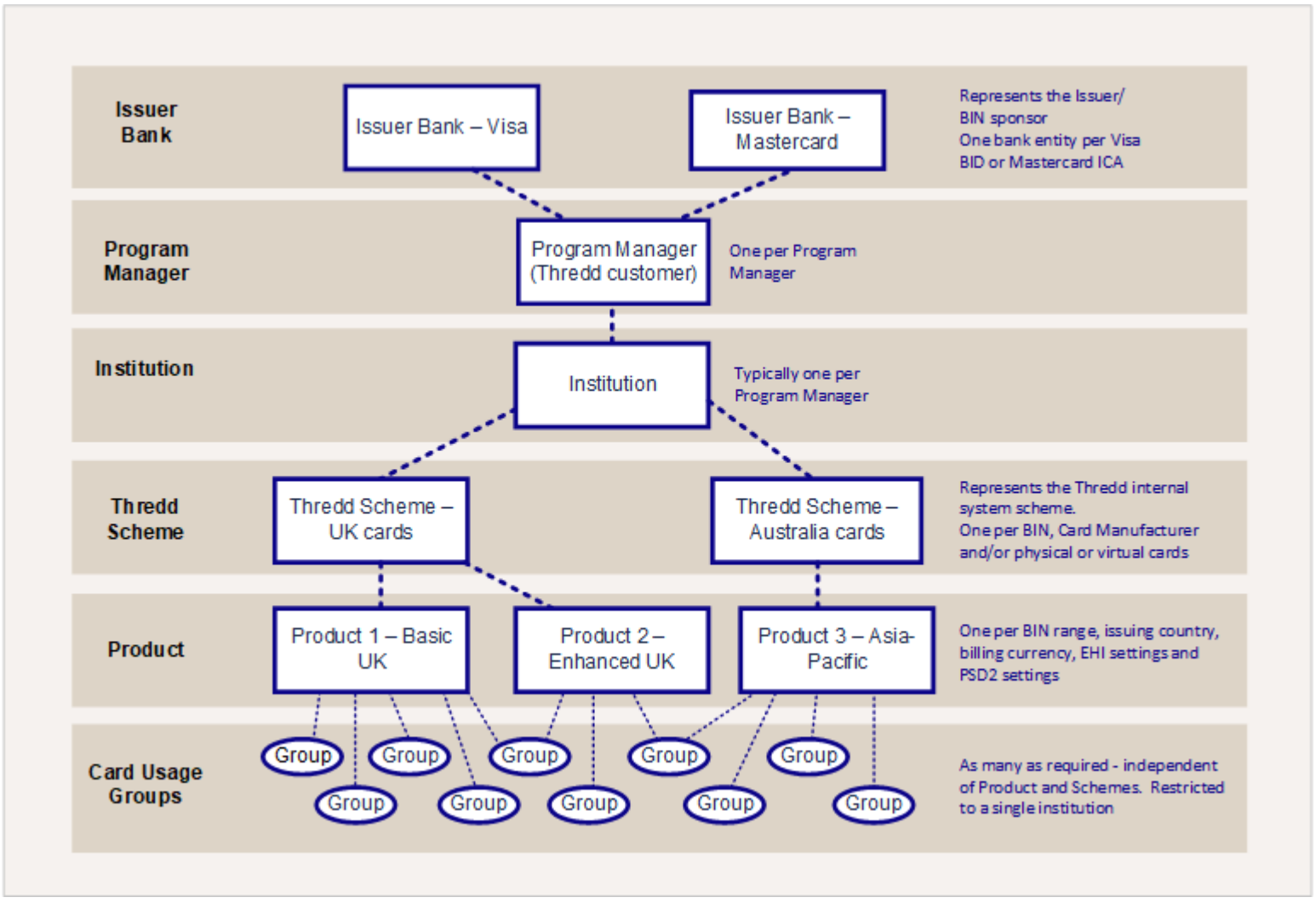


Figure 1: Thredd System Hierarchy

Your Thredd Implementation Manager will work with you to help define the requirements for your card programme and card products. Requirements are specified using a spreadsheet called the Product Setup Form (PSF). Once the requirements in the PSF have been agreed and signed off by the Program Manager and their issuer, the programme and product details are set up in the Thredd system. See Setting up your Card Products.

2.2 Card Records

A physical card is represented by a unique card record in the Thredd system. You can submit create card requests using the Thredd API. See Creating Cards.

When the Thredd system receives the create card request, it checks that the details submitted are in the correct format and contain all the mandatory fields and then creates the card record. The card record will contain the unique features of the card, together with shared features of the associated card product. See Key Attributes of a Physical Card.

Thredd returns a unique 9-digit Public Token, which can be used for any subsequent API requests against the card record.

2.2.1 Maintaining Card Records

You can use our Thredd Web Services API or the Cards API, together with the Thredd Public Token, to retrieve and update information about a card. For example to: activate the card, load a balance onto the card or adjust the balance, change the PIN, block and unblock the PIN, change the status of the card or update cardholder address and contact details. For details, see Managing Cards.

2.3 Card Manufacturers

The card manufacturer (card Bureau) is set up at a Thredd Scheme level. For more information, see Working with Card Manufacturers.

A card manufacturer is particularly relevant to physical card records, which need to be sent off for production; for virtual cards, Thredd provides an internal Thredd card manufacturer entity.

Note: If you are using multiple card manufacturers for different card products, each will require its own Thredd scheme. If you are offering both physical and virtual cards, each will each will require its own Thredd scheme.

2.4 How to Configure your Cards

Your standard card configuration options are set up at the time when you first implement your card program through Thredd. Options are specified using the Thredd Product Setup Form (PSF). For more information, see Setting up your Card Products.

There are additional customisation options available for designing the appearance and features of your physical cards. See Physical Card Customisation.

If you are also offering virtual cards, details of how to configure your virtual cards are covered in the Virtual Cards Guide.

2.4.1 Card Security Features

Your physical cards can be configured with a range of embedded security features, to help protect your cardholders from the risks of fraud. See Card Security Features.

3 Setting up your Card Products

This section describes the options available for configuration of the cards in your programme. Your Implementation Manager will work with you to discuss your requirements and complete the Product Setup Form (PSF), then send this to you and your Issuer (BIN sponsor) for sign-off.

3.1 Programme Details

Below are examples of settings applied at a Thredd scheme level to the cards in your programme.

Option	Description
Card Validity Period (in months):	Card expiry date period, which will be used to calculate the Expiry Date that is printed on the physical card (e.g., 36 months). For details, see Calculating the Expiry Date. **Note**: The expiry date can be amended during card creation to any date within the validity period; for more information, see Creating Cards.
Card Activation period	Internal expiry date, calculated from the date the card is activated (e.g., 12 months). For details, see Calculating the Expiry Date.
Card Type	Type of physical card product: *Magnetic strip*, *Chip* or both. For details, see Card Security Features.
Card Manufacturer (bureau)	Name of your card manufacturer. For details, see Working with Card Manufacturers.
BIN	The 6-8 digit BIN provided by your issuer. The BIN is used for the first 6-8 digits of the card's Primary Account Number (PAN). For details, see Generating the PAN.
Start Date	Expected period when your BIN will go live (in months).
Card product setup	The type of card products you want: • Physical card only • Virtual card only • Ability to convert virtual card to a physical card • Both physical and virtual cards. For more information, see the Virtual Cards Guide > Virtual Card Setup > Summary of Virtual Card Setup Options.

3.2 Card Product Options

Your programme can consist of one or more card products. Below are examples of options that can be configured at a card product level.

Option	Description
Product ID	Unique identifier of your card product (assigned by Thredd). If your programme supports multiple card products, each card product must have a unique product ID. When creating or updating cards through the Thredd Web Services API or the Cards API, you can use the product ID to link a card to a specific card product.
Product name	Name you assign to your card product.
Currency	Base or default currency of the card product.
Country of issue	Default country of issue.
Card Control Groups	Thredd offer several types of card usage groups, which control where and how the card can be used. For a list of available groups that can be set up and linked to a card product, see Card Control Groups.

Option	Description
Card Acceptor Lists	Acceptor lists are used to control at which Merchant stores the card can be used, based on a list of *permitted* or *blocked* Merchant Category Codes (MCCs). For a list of available card acceptor lists that can be set up and linked to a card product, see Card Acceptor Lists.
Card Design ID	Each card product can have a default card design artwork associated with it. The card design artwork must be provided to your card manufacturer.
Image ID	Each card product can have a customised virtual card image design artwork associated with it, which can be displayed to the customer in your App. This image can be created by Thredd or you can provide your customers with your own customised version. For details, see the Virtual Cards Guide.
Product type	The type of security and card profile features supported on the physical card: This can be one of the following: • 0 – Chip and Magstripe • 1 – Magstripe Only • 2 – Chip and Contactless For details, see Card Security Features.
Card product	The type of card brand. This can be one of the following: • MCRD – Mastercard • MAES – Maestro • VISA – Visa

Note: If your card programme supports multiple currency-country combinations, you will need to set up a separate card product for each combination.

3.3 Card Control Groups

Card Control Groups define where and how the card can be used, and provide other features to ensure card security and reduce the risks of fraud. Below is a list of the available card control groups that can be set up in the system. You can specify your card control requirements on the Thredd Product Setup Form (PSF); your Implementation Manager will set this up for you in the system.

When submitting your create card request via our Web Services or Cards API, the default card groups configured for your card product can be applied. Alternatively, you can specify which card groups to link to the card.

Card Control Group	Description
Usage Group	Enable detaled configuration of how a card can be used. For more information, see Card Usage Options.
Velocity Group	Restricts the frequency and/or amount at which the card can be loaded or unloaded, or used at a POS terminal. For example: £600 daily spending limit
Auth Calendar Group	Controls the dates and times when cards can be used. For example: prevent usage on Sabbath days and religious holidays.
MCC Group	Controls the type of merchants where the card can be used. The Merchant Category Code (MCC) is a four-digit number used by the Card Schemes (payment networks) to define the trading category of the merchant. For example: prevent card usage on gambling sites For a list of MCCs, see EHI Guide > Merchant Category Codes.
FX Group	Controls the rates for FX currency conversions if the purchase currency is different from the card's currency.

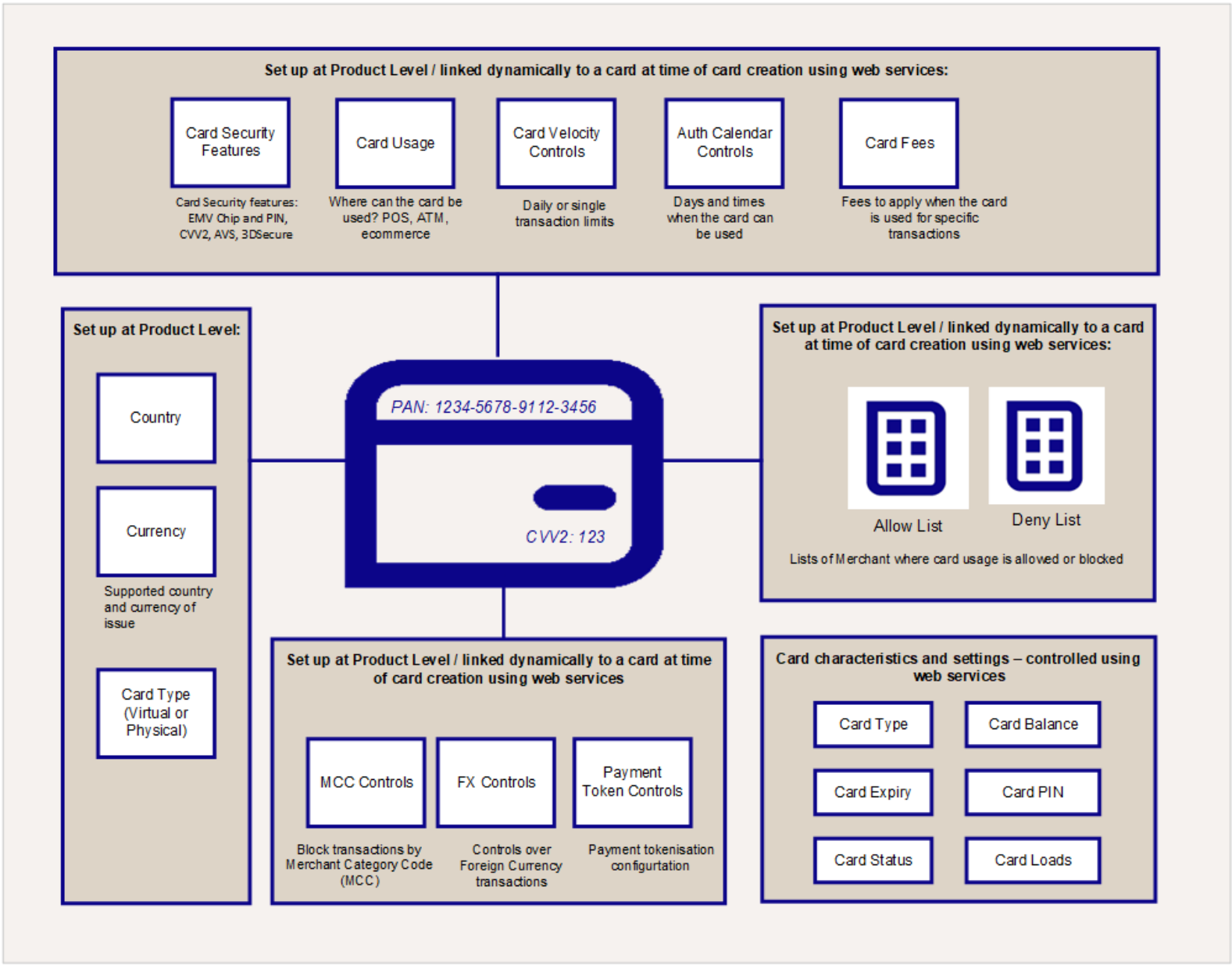
Card Control Group	Description
Payment Token UsageGroup	Defines configuration options specific to the provisioning of a digital payment token. You can specify more than one recipient. **Note**: Only applicable if tokenisation (digital wallets) is enabled for the card product.

3.4 Card Acceptor Lists

Card Acceptor lists control the merchant stores and websites where the card can be used (based on the merchant ID, DE 042) . There are two types of lists:

Card Acceptor List Type	Description
Permission List	Provides a list of merchants where a card can be used.
Deny List	Provides a list of merchants where a card cannot be used.

The figure below provides an overview of how card product controls work.



3.5 Card Production Scheduling

Card production is scheduled on a Program Manager level and applies to all cards in your programme. Below are options available for configuring how the production file is generated:

Option	Options available
Schedule type	Can be sent to the **Card Manufacturer** or to the **Card Manufacturer + Program Manager**.
When scheduled to run	Can be scheduled to run at a specified time on any required days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday.
File format	The file can be produced in one of the following formats: • **Full Format** – sent to the Card Manufacturer only. • **Cut Down Format**– sent to the Program Manager, with sensitive card data removed. • **Cut Down Format with Masked PAN**– sent to Program Managers who are not PCI Compliant).
File production limits	You can specify the following minimum thresholds which trigger the sending of the card production file: • Minimum number of card records – that must be in the file before it is sent to the card manufacturer. • The minimum number of days – between two file creations (regardless of whether the minimum number of requests is met or not).
Email address	The email addresses to notify recipients that the card production file has been produced. The actual file is sent via sFTP.

4 Physical Card Customisation

This section describes some of the options available for configuring the appearance and features of your physical cards:

4.1 Card Appearance

The card appearance includes the card dimensions, weight and the material used in its design. It also includes the baseline artwork, such as the colours and brand logos, and any text to be printed on the card.

- **Card logos**: The Card Schemes (payment networks) have strict rules around the placement and display of their brand logos. The scheme logos typically must be included on the card. The exception to this rule is for certain types of private-labelled cards, such as prepaid gift cards.
- **Your own brand and logos**: This includes any background colours, font types and colours and logo.
- **Text**: If you have any text (such as an email or contact number for card-related queries or to report lost and stolen cards), this is typically included in the card artwork.

These are standard features of the card and are the same for all the cards within your card product. If your programme has multiple card products with different card designs, you can have separate card artwork for each card product. The base artwork features are typically pre-printed in batch as base card plastics to help reduce production and printing costs. (The additional personalised elements, unique to each cardholder are then printed onto the card whenever a new card is ordered.)

Your artwork must typically be signed off by your issuer (BIN sponsor) and potentially by the Card Scheme (payment networks). If you are using standard issuer artwork designs, pre-approved by the card scheme, further approval is not required.

4.2 Card Physical Dimensions and Materials

The example below describes the typical payment card physical dimensions:

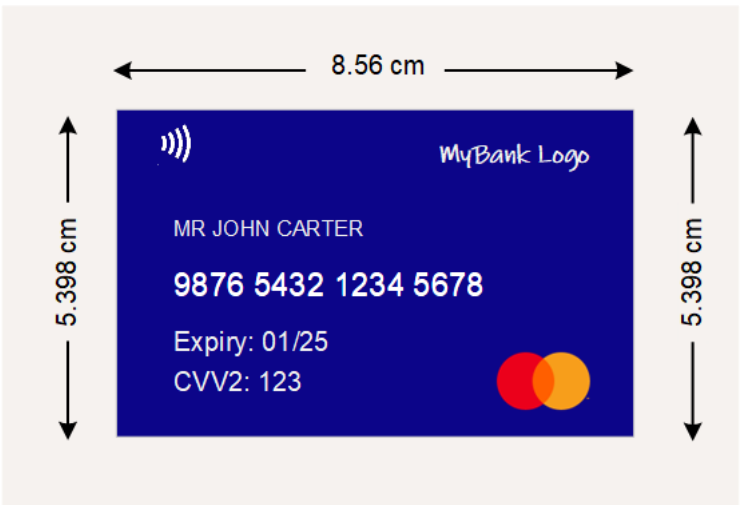


Figure 2: Example of a payment card - showing dimensions

The standard ISO financial payment (Credit/Debit) card size in centimetres is 8.56 cm wide by 5.398 cm high. The standard payment card thickness is 0.76 mm thick. This size standard uses the ISO/IEC 7810 ID-1 format. See Wikipedia: ISO/IEC 7810.

Adopting standard dimensions across card issuers (BIN sponsors) and countries ensures that any payment card will fit into a standard card reader terminal or ATM machine.

The weight and material of the card may differ. The majority of payment cards are made out of plastic (typically PVC) and weigh around 5 grams; some cards may be made out of metal and weigh around 17.5 grams. Please discuss your card requirements with your card manufacturer.

Note: If the card is to be used only as a contactless card or tokenised device (such as a key ring fob), then card dimensions are less important. Please discuss your requirements with your card manufacturer.

4.3 Card Fields and Card Personalisation

A typical card contains dynamic fields which are printed on demand. These fields are personalised to the cardholder or to each card record and are printed or embossed onto the base card plastics (which were previously produced as part of a batch production run). The personalised fields are printed by the card manufacturer based on the card record details supplied by Thredd in the card generation file (see Card Generation File).

The locations of fields, and whether they appear on the front or the back of the card, may vary depending on your card design; please check with your issuer (BIN sponsor) or card manufacturer for any specific requirements and restrictions that may apply. Below is an example.

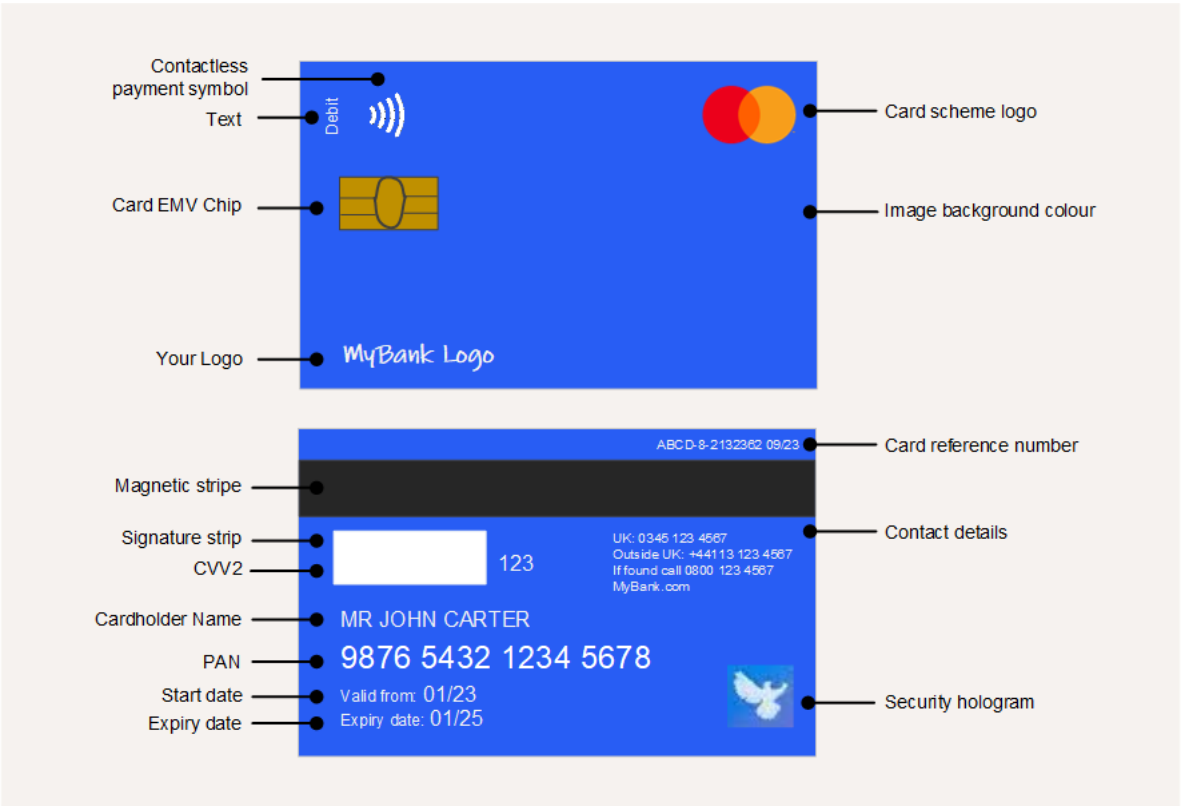


Figure 3: Example of a payment card

Refer to the table below for a description of the fields and other elements on the card:

Field	Description
Personalised elements - customised to the card or cardholder; printed per card record	
PAN	The permanent account number (PAN) is the long number (typically 16-19 digits) that is either printed or embossed on the card. Thredd generates this from the available BIN stock for your programme. This is unique to each card. For details, see Generating the PAN.
Cardholder title	Cardholder title (e.g., Mr, Mrs, Ms) based on the information you supplied in your create card request. This field can be omitted for prepaid gift cards or certain types of corporate cards.
Cardholder first name	Cardholder first name based on the information you supplied in your create card request. This field can be omitted for prepaid gift cards or certain types of corporate cards.
Cardholder last name	Cardholder last name based on the information you supplied in your create card request.
Card start date	Date the card is valid from, based on the card record defined start date. This is an optional field and may not appear on all cards.
Card expiry date	The card's expiry date, as calculated by Thredd according to your card product. This field is mandatory on most open loop cards (which can be used at any merchant site using the card scheme (payment network), but can be omitted on cards with restricted usage, such as prepaid gift cards and certain types of corporate cards. For details, see Calculating the Expiry Date.
CVV2 (Security Code)	The three-digit security code (Card Verification Value). This is a random 3-digit code generated by Thredd.
Card reference	You or the printer can optionally add a text field containing a unique card or account reference.
QR Code	Your card manufacturer may be able to support a QR code that will be printed on the card. You can add separate values to each card using the ThreddWeb Services API. or the Cards API.
Card Security elements - embedded features of the card; printed in batch per card product (EMV Chip and magnetic strip profile are	

Field	Description
data added when the card is printed)	
Signature strip	Blank area on card where the cardholder can add their signature. See Signature Strip.
Magnetic strip	The magnetic strip is the long thin stripe on the back or front of the card, which contains data unique to the card. The card data on the magnetic strip is personalised when the card is printed. See Magnetic Strip.
EMV Chip	Chip embedded on the card, which contains electronic data relating to the card. See Chip Profile.
Card Verification Values	See Card Verification Values.
Security hologram	Visa and Mastercard mandate the use a holographic security logo. The hologram provides a means of protection against card forgery. The hologram is punched onto the pre-printed cards and is designed to reflect light and appear three-dimensional.
Card Design elements - branding elements printed on the card; pre-printed in batch per card product	
Scheme logo	The card scheme logo (Mastercard or Visa) is required for all scheme cards, excluding some private-labelled cards. Your card design should use approved scheme images.
Your brand logo	Your company name or logo can be included in your card design.
Your contact details	Provides your customers with details of how to get in touch, such as an email or contact number for card-related queries or to report lost and stolen cards.

5 Card Security Features

The following are features relating to the use of physical cards in card-present situations, such as at a Point of Sale (POS) terminal or ATM.

5.1 Signature Strip

This legacy feature is still used in some countries (where chip and PIN is not available). When the customer receives their card, they are instructed to immediately sign in the signature strip. The merchant then has the option to do a manual check to verify that the signature provided by the customer at the point of sale matches the one on the back of the card.

5.2 Magnetic Strip

When used in store, the card's magnetic strip can be swiped by a card reader. The card reader is set up with a connection to the Acquirer, and the data can be passed electronically to the scheme for real-time authorisation.

Swipe cards are still in use, but are considered legacy technology which is less secure[1]. Some card Program Managers are no longer including magnetic strips on new cards[2].

Note: You can optionally set the card usage group to disable magstripe, or alternatively use magstripe as a fallback authentication option only, if no other means of card authentication are available.

5.3 Chip Profile

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)

5.3.1 Setting up of Chip profiles

The Issuer (BIN sponsor) chip profiles are set up within the card scheme (payment network). All new chip profiles must go through testing and scheme certification.

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

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

5.3.2 Benefits and Options for Chip and PIN

Chip technology protects against card counterfeit fraud (card cloning). Chip & PIN technology helps to prevent fraudulent use of lost and stolen cards. When used in store, the card can be inserted into a card reader. In the majority of transactions, the cardholder needs to enter their card PIN (typically a secret 4-6 digit number known only to them).

---

1 The magnetic stripe is considered less secure because it is relatively easy to skim read and clone.

2 For example, Program Managers offering European only card solutions, such as VPay cards. Magstripe is mainly used in the US and is being phased out in Europe. Mastercard plan to stop using the magnetic stripe in Europe in 2024 and in the US by 2027.

Options on the chip determine how the card is authorised. For example: the card could approve or deny the transaction offline, or request online authorisation. For an online transaction, the data is passed electronically in real-time to the payment network for authorisation.

The chip is also used to support contactless payments. Contactless payments are a type of EMV transaction that use Near Field Contact (NFC) technology. NFC enables the payment chip to be read by a nearby card reader using a wireless process.

Chip profile data can be updated remotely when the card is used at a POS terminal or ATM.

5.3.3 Card Biometric Authentication

This option enables you to use biometric authentication on the card. During the card present transaction, the cardholder scans their fingerprint (without needing to enter a PIN). The card chip verifies the biometric data and when Thredd receive the transaction authorisation request, we can reset the SCA (Strong Customer Authentication) counters as required by PSD2 (the second Payment Service Directive) rules. For more information on SCA counters, see the SCA and PSD2 Guide. For information on card data input and card authentication methods recorded in the transaction data, see the External Host Interface (EHI) Guide > GPS_POS_Data Field.

Note: For more information on support for Card Biometric Authentication, please speak to your Thredd account manager.

How does Card Biometric authentication work?

Cards with biometric authentication are manufactured with an embedded fingerprint sensor. When the cardholder wants to make a payment, they place their finger on the sensor embedded in the card. The card's processor then compares the live fingerprint scan to the stored template. Biometric matching is done on the card, without transmitting the fingerprint data to any external systems.

Before the card can be used, the cardholder must first enrol their fingerprint by pressing their finger on the card's sensor, usually during an activation process. The biometric card provides a faster, more secure payment experience compared to entering a PIN, as the fingerprint verification is done with a simple touch. It also meets industry standards for on-card biometric comparison. For more information see biometricupdate.com.

5.4 Card Verification Values

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, entered by the customer in an e-commerce transaction.

5.5 Holographic Security Image

This is a security design on the card, which makes it difficult for the card to be counterfeited. The hologram reflects light and is three-dimensional. On Visa cards, when the card is tilted back and forth, a dove appears in the hologram and it seems to 'fly'. Mastercard cards have interlocking globes showing the continents with the word 'MasterCard' in the background.

6 Working with Card Manufacturers

The production of physical (printed) cards requires the services of a card manufacturer (Card bureau). You will need to sign a commercial agreement with one of the card manufacturers which Thredd supports. The card manufacturer is responsible for the printing of cards; they can also handle other aspects of card fulfilment, such as packaging and delivery of cards and PIN letters directly to your customers.

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

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

For further details of working with card manufacturers, please contact your Business Development Manager.

6.1 Card Generation File

Thredd provides an XML file-based interface which allows card manufacturers to accept card generation files from Thredd.

You can use the Thredd Web Services API or the Cards API to submit card creation requests. Card records can be created individually or in batch.

When we receive your create card requests, we create a card record in the database. Multiple card records are then included in the daily XML file that Thredd sends to your card manufacturer; the card records contain the instructions for generating the cards in your program.

Thredd provides two version types of the card manufacturer XML file:

- **Full version** - sent to your card manufacturer, containing sensitive card details, such as PAN, CVV2, PIN and track data
- **Truncated version** - this optional version can be sent to you, for your reference. In this version, fields containing sensitive card details (such as PAN, CVV2 and track data) will be removed

Note: The frequency of sending of the card generation XML files is configurable. Note that some manufacturers charge per file or per record included in the file; check with your card manufacturer for details.

XML files are sent to the manufacturer using Secure File Transfer Protocol (sFTP).

6.2 Where to find out more

- For a list of Thredd-supported card manufacturers, see the Web Services Guide > Card Manufacturers.
- For details of the XML file format which your card manufacturer must be able to receive, see the Thredd Card Generation Interface Specification.
- For examples of card generation XML files, see the Card Generation Interface Specification > Example Files.
- For details of how to use web service or cards API to create card records, see the Web Services Guide or Cards API Website.

7 Card Production and Testing

This section describes the typical steps in producing, testing and releasing into production the card products for your programme.

7.1 Creating White Test Plastics

White test plastics are generic, non-branded cards with test keys on the card and a Chip profile. Your Implementation Manager will work with your card manufacturer to produce test cards. Below are the typical steps in creating your test cards:

1. Create several test cards and provide Thredd with a list of the generated Public Tokens.
2. Thredd produces a card generation file for any test cards that have been created and manually sends the file to the card manufacturer via sFTP.
3. The card manufacturer produces white test plastics in line with the agreed project plan. Test cards are sent to the relevant parties (e.g. the Program Manager and Visa or Mastercard).
4. Testing is undertaken in line with the agreed scope.

7.2 Setting up on Production

When all production readiness activities are complete, Thredd provides you with production credentials and generates a limited number of PAN stock, as approved by your card issuer.

7.2.1 Production testing steps

Additional end-to-end transaction testing is required at this stage. In particular:

1. Create card tokens for automated card production.
    - Thredd will send a card generation file to the card manufacturer via sFTP. The card manufacturer generates live physical cards and despatches to the relevant parties for testing (Thredd, Programme Manager and Card Schemes).
2. Make sure you understand any messages returned from the card schemes (payment networks) and card issuers and know how to handle them.
3. Thredd can provide you with a test script to run tests that cover aspects you should test, such as:
    - Test traffic through the BIN tables (BIN databases held by the card scheme).
    - Test the card chip profile is working in line with how it has been configured (for example, if the card is enabled to draw out money at ATMs and charges a fee for ATM withdrawals, check this works as expected).
    - Test to ensure usage groups and velocity limits set up for your products work as expected and return the expected results.
4. Test the end-to-end customer experience and confirm that the card and account are operating as expected.

8 Creating Cards

8.1 Submitting Card Requests

You can use the Thredd API to create new card records. Thredd offers two types of API: SOAP Web Services or REST-based Cards API. These two options provide slightly different approaches to card creation. They also differ in the field options available with each request.

8.1.1 Using Thredd Web Services API (SOAP)

The Thredd Web Services API uses the SOAP protocol to send and receive messages in XML format. For common use case scenarios on how to use our web services to create and manage the cards in your program, see the Web Services Guide > Use Case Scenarios.

For details of how to use the *Card Create* Web Service to create a physical card record, see the Web Services Guide > Card Create.

8.1.2 Using the Cards API (REST)

The Cards API use a REST-based method to send and receive messages in JSON format. For common use case scenarios on how to use our Cards API to create and manage the cards in your program, see the Cards API Website > Recipes.

For details of how to use the *Card Create* API to create a physical card record, see the Cards API Website > Creating a Card.

8.1.3 Considerations when creating a card

There are typically three parts to creating a card:

1. Submit the create card request – Thredd returns a 9-digit Public Token, which can be used in all subsequent requests relating to the card record.
2. Activate the card – change the card status to *Active*, so that it can be used. For a physical card, the card should normally be created as inactive and only activated when the customer receives their card (you can provide your customers with an In-app option to request card activation or a phone number service to call to activate the card).
3. Load the card with a balance – update the available balance on the card, to reflect any money the customer has added to their account or loaded onto the card.

Note: Thredd Web Services API and the Cards API provide different ways of implementing the above steps: Web services enable you to combine the above steps in a single API request or as separate requests. The Cards API split this out into three separate API requests.

Note: When creating cards, you can use the default settings defined at a card product level, or for some fields, you can specify unique settings per card. For example, you can: change the default expiry date or change the card usage groups linked to the card.

8.2 Structure of a Card Record

For details of the most important attributes in a typical card record, see Card Attributes.

8.3 Sending Card Records to your Card Manufacturer

When we receive your create card requests, we create a card record in the database. Multiple card records are then included in the daily card generation file that Thredd sends to your card manufacturer; the card records contain the instructions for generating the cards in your program. If required, you can request a copy of the card generation file (with sensitive card information removed for security reasons). For details, see Working with Card Manufacturers.

8.3.1 Cancelling a card order

If you need to cancel a card that has been ordered by mistake or where there is an error in the card record, please use the Thredd API (Cards Status Change web service or Card Update API) to change the card to a status that isn't 00, 02, or G1. This needs to be done before the card generation file is scheduled to be sent. For details, see the Web Services Guide > Card Change Status or the Cards API Website > Update Card Status.

Note: After Thredd has sent the card generation file to the card manufacturer, you will need to contact your manufacturer directly to request removal of the card record. Please check with your card manufacturer for the processes, time-scales and costs around cancelling of orders.

9 Managing Cards

This section provides an overview of some of the Thredd API (SOAP Web Services API or REST-based Cards API) functionality that can be used to manage the cards in your programme. For a details of the full functionality available , see the Web Services Guide (SOAP) or the Cards API Website (REST).

9.1 Initial Actions

9.1.1 Activating the Card

If the card is issued as inactive, it must be activated. This is typical for customers who sign up for a physical card via the Internet or their mobile App and who need to activate the physical card after it is delivered.

- On Web Services (SOAP), use Card Activate.
- On Cards API (REST), use Card Status.

9.1.2 Loading the Card

Where Thredd maintains the card balance on your behalf or has a copy of the balance, you can use the following web services or cards API to update the Thredd-held card balance:

- On Web Services (SOAP), to load a card without activation, use Card Load. To load and activate a card at the same time, use Card Activate and Load.
- On Cards API (REST) use Load or Unload a Card

9.1.3 Applying Fees for Card Services

This service is available to Program Managers using the Thredd fees module (available where Thredd maintains details of the balance on the card). You can apply a fee for specified activities on the card, such as when your customer applies for a new card, or loads the card with money. For more information, see the Fees Guide.

9.2 Updating Cards

9.2.1 Managing the PIN

To set, retrieve, unblock and change the PIN associated with a card:

- On Web Services (SOAP), use Card PIN Control.
- On Cards API (REST), use Set PIN.

9.2.2 Changing Card Status

- On Web Services (SOAP), use Card Change Status.
- On Cards API (REST), use Card Status.

9.2.3 Updating Cardholder Details

To change the cardholder details linked to a card:

- On Web Services (SOAP), use Update Cardholder Details.
- On Cards API (REST), use Update Card.

9.3 Viewing Card Transactions

Thredd provides a number of systems to enable you to generate test card transactions, view transactions on a card, and view both payment authorisation and financial messages relating to the card transactions in your program:

- **Card Transaction System (CTS)** – enables you to test your system's integration before you move into a production environment by running built-in tests to simulate different types of transactions (e.g., Point of Sale terminal, ATM, E-Commerce and refund). For details, see the Card Transaction System Guide.
- **Smart Client** – the user interface for managing your cards and transactions on the Thredd systems. Using Smart Client, you can display details about card activity, transaction type, and customer interaction, and drill down into the details of specific transactions. For details, see the Smart Client Guide.
- **External Host Interface** – a Thredd system which sends real-time payment authorisation requests and other types of financial messages to your systems. For details, see the External Host Interface (EHI) Guide.
- **Transaction Reports** – an XML report containing details of daily transactions. For details, see the Transaction XML Reporting Guide.

10 Key Attributes of a Card

This section provides details of some the key card attributes which are included in the card record and in the Card generation File sent to your card manufacturer.

10.1 Key Attributes of a Physical Card Record

Below are examples of some of the attributes of a card record that are typically associated with a physical card.

Card Attribute	Description	How is this created?
PAN	The permanent account number (PAN) is the long number (typically 16-19 digits) that is either printed or embossed on the card.	Automatically assigned by the Thredd system out of your available PAN stock.
Expiry Date	The card's expiry date. This date determines when you will need to renew or replace the card and is typically printed on a physical card.	Determined by the card record creation date, based on the *Card Validity Period* defined for your card programme. See Calculating the Expiry Date.
Cardholder Name	The cardholder's name, as printed on the card. (May be omitted on certain types of cards, such as Gift cards and corporate cards.)	Based on information supplied in your create card request.
CVC2	The Card Verification Value (CVV) on a credit card or debit card is a 3 digit number on Visa and Mastercard branded credit and debit cards. Cardholders are typically required to enter the CVV during any online or cardholder not present transaction.	Automatically assigned by the Thredd system.
Track data	This is secure data to be included on the card's magnetic strip. This is provided in three track fields. For details, see the Thredd Card Generation Interface Specification.	Generated by the Thredd system.
Chip track data	Chip track data for EMV transactions. This is provided in two Chip track-equivalent fields. For details, see the Thredd Card Generation Interface Specification.	Generated by the Thredd system.
PINBLOCK	Holds the encrypted PIN to be placed on the chip card.	Generated by the Thredd system.
Service code	Three decimal digits as defined in ISO 7813. • First digit: Use and Technology • Second digit: Authorisation requirements • Third digit: Service and PIN requirements For details, see the Thredd Card Generation Interface Specification.	Generated by the Thredd system, based on your card product configuration.
Type	Type of product (e.g., Mastercard, Maestro, Visa card).	Generated by the Thredd system, based on your card product configuration.
Language	Defines the language of the card product, if it is not already defined by the card type elements.	Generated by the Thredd system, based on your card product configuration.

10.2 Other Important Card Record Attributes

Below are examples of some additional attributes that are associated with a card record.

Card Attribute	Description
Public Token	Unique Thredd token that is generated when a card is created and is always linked to the card. You can use the public token to query and update your cards, without needing to store or process the full PAN. (The public token is internal to Thredd only. This is separate from a digital token (DPAN) created using the tokenisation (digital wallets) service, for online merchant or mobile transactions.)
Status	The current status of the card (e.g., active or inactive). A card issued in an *active* status can be immediately used (provided it has an available balance). A card issued in an inactive state must first be activated before it can be used.
Available balance	The available balance on the card. This balance is adjusted after any transaction on the card that affects the available balance, such as a payment authorisation.
Billing and Fulfilment Address	The address that is linked to the card. Note that this address may be used for sending replacement cards, and for payment authorisations that use the Address Verification Service (AVS). You can configure an alternative delivery address for cards such as corporate cards or prepaid cards. **Note**: you can provide separate billing and delivery addresses. Thermal Line 1 and Thermal Line 2 fields can be used to supply additional address details.
Telephone	The telephone number linked to the card. Note that for certain services, such as payment tokenisation, the linked mobile phone number may be used for sending SMS notifications to the cardholder.
Delivery method	For a physical card record, you can specify the delivery method or a delivery code, which your card manufacturer can use for meeting your delivery requirements. (Delivery methods include: Standard mail, Registered mail and Direct delivery (Courier).)
PIN	The PIN associated with the card. The cardholder enters their PIN when using the card at an ATM or Point of Sale (POS) terminal.
PIN Mailer	For printed cards, you can optionally define whether a letter containing the PIN is sent out with the new card, Please discuss your requirements with you card manufacturer.
Order reference	You can optionally define a unique customer order reference number, which can be printed on the card or used to track the card production.

Note: For a list of additional configurable card attributes, please refer to the Web Services Guide or the Cards API Website.

11 Generated Card Elements

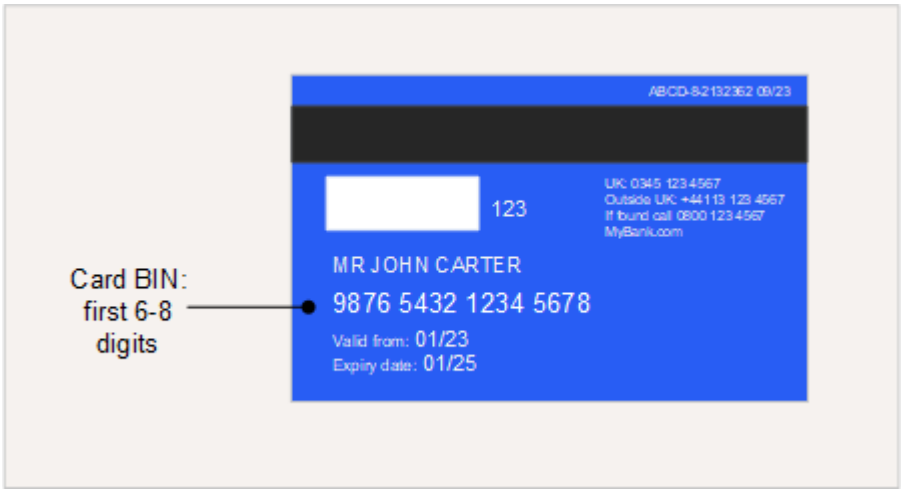
This section provides more information on how some card elements such as the PAN and Expiry Date, are generated.

11.1 Generating the PAN

The Primary Account Number (PAN) is the long number (typically 16-19 digits) printed or embossed on the card. It consists of the following components:

- Banking Identification Number (BIN) - this is the first 6-8 digits of the PAN and is provided by your issuer, for use with cards in your programme. It identifies the card scheme (payment network) and issuer. The same BIN will appear on all cards, unless your programme supports multiple BIN ranges.
- Unique account number - the remaining 8 digits are generated by Thredd when PAN stock generation is requested, and reflect the unique account associated with the card[3]

See the example below.



Thredd creates PAN stock in a batch process. Active products usually have auto-PAN stock generation enabled. PAN stock will be generated when it falls beneath a threshold, which is set at a product level. The PAN stock is linked to a card product in your card programme.

When the card record is created, Thredd assigns a PAN from the stock of available PANs.

11.2 Calculating the Expiry Date

There are two types of expiry dates that can be set up in our system:

- The expiry date to be printed on the card
- An internal system expiry date, which relates to how long the card record remains valid for after it is activated.

Printed Expiry Date

You can define at a Thredd scheme level for your programme the *Card Validity Period*, which is the period over which the card is valid.

Thredd uses the *card validity period* to calculate the card expiry date expiry date that will be printed on your physical cards.

For example:

- Card Validity Period (in months) = 24 months (two years)
- Date of card create request: 25/01/2023
- Expiry date printed on card: 01/2025

If you want to set a specific expiry date to appear on the card which differs from the default expiry date, you can specify this date at the time when submitting your Create Card request. (This date can be up to 8 years in the future, but it cannot exceed the card validity period). See Creating Cards.

Note: Most cards have a default expiry date of 3-5 years, depending on the issuer (BIN sponsor), but this can be set to your required length (e.g., 12 months or 5 years).

---

[3] The last PAN digit is the luhn check digit (used to prevent PAN keying errors at the terminal.) Not all PANs are 16 digits long, so the "unique account number" part might not always be 8 digits.

Note: You can amend the expiry date of the card to any date within the validity period using Thredd Web Services API or the Cards API[4]. For details, see the Web Services Guide > Card Extend Expiry or Cards API Website.

Internal Expiry Date

This date is defined at a Product level and indicates how many days the card is valid for, from card Activation.

If you want to set a specific internal expiry date which differs from the default printed expiry date, you can specify this date when submitting a Card Activate request. See Managing Cards.

Note: This option cannot be used to extend the expiry date past the expiry date printed on the card.

For example:

- Card Validity Period (in months): 24 months (two years)
- Internal Validity (in days): 365 days (1 year) after activation

Examples of usage scenarios for the internal expiry date:

- You offer gift cards - with a maximum card validity period of 3 years (no expiry date is printed on the card). These may sit on a shelf in a store for a while before they are ordered. Once the card is activated, the card is valid for use within a year. If required, after the year, you can use the Extend Expiry Date web service or the Cards API to extend the expiry date for another period.
- You offer customers a virtual card, which can be used until their physical card arrives and is activated. The virtual card is activated for immediate use, and expires after 21 days.

4 Changing the expiry date is mainly used on virtual cards, since changing the printed expiry date requires reissuing the card.

12 Card Usage Options

The options described in this section reflect those available on the **Card Usage** tab in the Product Setup Form. They are defined per card usage group and determine how the card can be used.

CARD USAGE RULES

Card Usage Group Name:		Thredd Code:	

Allow? Y/N	Card Acceptance Method (A)
No	Unknown Acceptance Method
No	Card Not Present (E-commerce)
No	Card Not Present (Phone/Mail/Order)
No	Card Not Present (Recurring)
No	Card Not Present (Manual Key Entry)
No	Mag Stripe transaction at Chip capable Terminal (Technical Fall Back)
No	Mag stripe PAN entry - Common
No	Chip PAN Entry - Offline PIN verification
No	Chip PAN Entry - Online PIN verification
No	Chip PAN Entry - Signature verification
No	Chip PAN Entry - No Verification
No	Cash withdrawal outside country of issue
No	Cash withdrawal in currency other than card billing currency
No	POS usage outside country of issue of a card
No	POS usage in currency other than card billing currency
No	Contactless EMV
No	Manual Keyed Transaction at Chip capable Terminal
No	Cardholder NOT present -Manual Key Entry
No	Contactless MagStripe
No	Card Not Present (Credential on File)
No	Chip PAN Entry - no CVM Required
No	Terminal Indicates Fallback Chip to Mag Stripe

Allow? Y/N	Transaction Type (T)
No	Purchase With Cashback (DE=09)
No	Cash Advance (DE=17)
No	Cash at ATM (DE=01)
No	PIN Change ATM (DE=92 (M), 70(V))
No	Balance Enquiry at ATM (DE=30)
No	PIN Unblock via ATM (DE=91 (M), 72(V))
No	Credits - Refunds (DE=20)
No	Purchase of Goods & Services (DE=00)
No	Visa Quasi- Cash (POS) transactions (DE=11)
No	Credits Auth (DE=28)
No	Original Credits (DE=26)
No	Account Funding transaction (AFT) (DE=10)

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

Allow? Y/N	Verification Checks (V)
No	Bypass Online PIN Check
No	Bypass Expiry Date Check
No	Bypass CVV2/CVC2 Check
No	Blank CVV2 in Card not Present E-commerce
No	Blank CVV2 in Card not Present Phone/Mail Order
No	Blank CVV2 in Card not Present Recurring
No	Blank CVV2 in Card not Present Manual Key Entry
No	Allow Blank DE014
No	Expiry date optional for Recurring Payments
No	Bypass Card Status Check for Refund Authorisations

Allow? Y/N	Misc (M)
No	If declined, force next EMV transaction online
No	If Zero or negative balance, force next EMV transaction online
No	Force next EMV transaction online
No	Reset EMV counters to upper offline limits
No	Transaction Alerts enabled
No	Instant funding
No	Override to allow International e-commerce
No	Override to allow International Credential on File
No	Instant Credit Gambling Payouts
No	Faster Refunds Support

Figure 1: Card Usage tab in the Product Setup Form

Card acceptance methods

The table below describes the methods available to accept card payments. Each option can be set to Allow or Disallow.

Card acceptance method (A)	Description
Unknown acceptance method	Allow card payments when the acceptance method is unknown (i.e., in non-regulated countries where the processing code is not updated). If this option is set to disallow, then card payments with an unknown acceptance method will be declined.
Card not present - E-Commerce	Allow card payments when the card cannot be physically presented to the merchant; in the case of e-commerce or internet-based payment services. If this option is set to disallow, then e-commerce card payments will be declined.
Card not present - Phone/Mail Order	Allow card payments when the card cannot be physically presented to the merchant, in the case of mail order or telephone payments. If this option is set to disallow, then phone or mail order card payments will be declined.
Card not present - Recurring	Allow recurring card payments when the cardholder has set up a regular payment schedule and the card cannot be physically presented to the merchant for each recurring payment, for example, magazine subscriptions. The card is automatically billed on the specified schedule date. If this option is set to disallow, then recurring card payments where

Card acceptance method (A)	Description
	the card is not present will be declined.
Card not present - Manual key entry	Allow card payments when the merchant enters the card details manually and does not use e-commerce, phone or mail order as transaction information. If this option is set to disallow, then card payments where the card is not present and manual key entry is used will be declined.
Mag Stripe transaction at chip capable terminal (technical fallback)	Allow chip card payments when the chip card fails at a terminal that is designed to support chip transactions. In this case, the terminal completes the transaction using the magnetic stripe. This is used as a fallback mechanism. If this option is set to disallow, then magnetic stripe card payments will be declined.
Mag Stripe PAN Entry - Common	Allow PAN entry using magnetic stripe card payments where **DE22 = '02'** are approved providing other validations are successful. This is selected by default. When selecting this option, consider the level of risk in relation to magnetic stripe transactions. If this option is set to disallow, then magnetic stripe card payments using PAN entry will be declined. **DE22 = '02'** denotes one of the following: • Partial magnetic stripe read. • Magnetic stripe read; CVV checking may not be possible. • Exact Track 2 contents read, but transaction is not eligible for CVV checking. **Note:** Do not select if PAN entry using magnetic stripe transactions is not allowed.
Chip PAN entry - Offline PIN verification	Allow offline verification of the PIN entered by the cardholder, for example where the market operates an offline PIN environment (i.e. the UK or Ireland). Cash machines still operate online PIN verification in these markets. If this option is set to disallow, then offline verification of the PIN will not occur and the card payment will be declined.
Chip PAN entry - Online PIN verification	Allow online verification of the PIN entered by the cardholder. Cash machines operate online PIN verification. If this option is set to disallow, then online verification of the PIN will not occur and the card payment will be declined.
Chip PAN entry - Signature verification	Select to request signature verification in the case of chip-capable EMV terminals where the PIN pad is not working or not present. If this option is set to disallow, then signature verification will not be requested and the card payment will be declined. **Note:** The card may be set to signature verification instead of PIN under the Disability Discrimination Act.
Chip PAN entry - No verification	Allow chip card payments where the payment is authorised with no PIN or signature required, for example in unattended car parking payment terminals. If this option is set to disallow, then payment authorisation with no PIN or signature will not occur and the card payment will be declined.
Cash withdrawal outside country of issue	Allow cash withdrawals outside the country of issue. For example, a card issued in the UK can complete cash withdrawals in Spain. If this option is set to disallow, then cash withdrawals outside the country of issue will be declined.
Cash	Allow cash withdrawals in currency other than the billing currency. For example where a card is billed in British Pounds (£) the cardholder can complete cash withdrawals in US Dollars ($). If this option is set to disallow, then cash

Card acceptance method (A)	Description
withdrawal in currency other than card billing currency	withdrawals in currency other than the billing currency will be declined.
POS usage outside country of issue of a card	Allow card payments where the cardholder pays for purchased goods or services outside the country of issue. For example, a card issued in the UK can be used at a terminal in Spain. If this option is set to disallow, then card payments where the cardholder pays for purchased goods or services outside the country of issue will be declined.
POS usage in currency other than card billing currency	Allow card payments where the cardholder pays for purchased goods or services in a currency other than the billing currency. For example, a Polish card with a billing currency of Polish Zloty (PLN) can be used for purchases in Singapore Dollars (SGD). If this option is set to disallow, then card payments where the cardholder pays for purchased goods or services in a currency other than the billing currency will be declined.
Contactless EMV	Allow contactless EMV card payments. If this option is set to disallow, then contactless EMV card payments will be declined.
Manual keyed transaction at chip capable terminal	Allow card payments where the merchant manually enters the card details into a chip-capable terminal connected to a computer system. For example, restaurants that use specific computer software for placing orders, taking payments and printing receipts. If this option is set to disallow, then card payments where the merchant manually enters the card details into a chip-capable terminal connected to a computer system will be declined.
Cardholder NOT present - Manual Key Entry	Allow digital wallet card payments, where the physical card is not present. This must be selected for MDES usage groups. For example, mass transit systems, such as TFL in London, MRT in Singapore, NSW Transport in Sydney. If this option is set to disallow, then digital wallet card payments will be declined.
Contactless Mag Stripe	Allow contactless magnetic stripe card payments. This is used where both the card and the terminal do not support contactless EMV but support contactless mag stripe. If this option is set to disallow, then contactless magnetic stripe card payments will be declined.
Card Not Present (Credential on File)	Allow card payments where a cardholder saves their card details with a merchant for future transactions in the case of website or app transactions. If this option is set to disallow, then card payments where the details have been saved with a merchant will be declined. This method uses the following logic: • **Visa**: DE22.1='10' triggers this check • **Banknet (Mastercard)**: DE22.1 in '10','82' triggers this check If this type of transaction is not permitted, but the above logic is true, the transaction is declined with the following note text appended: • **[Card Acceptance Method (A) - Credential-On-File PAN Entry - Failed]**
Chip PAN entry - No CVM required	Allow card payments where the cardholder verification method (CVM) is not required, for example, when the terminal does not request PIN entry from the cardholder. The last 6 digits of CVM results are (DE055.9F34 1st byte is 011111). If this option is set to disallow, then card payments where the cardholder verification method (CVM) is not required will be declined.
Terminal Indicates Fallback Chip to	Allow fallback to magnetic stripe card payments when the chip card fails at the terminal. The terminal detects chip to magnetic stripe fallback has occurred and communicates to Thredd that fallback has explicitly happened. If this option is set to disallow, then fallback to magnetic stripe card payments will be declined when the chip card fails at the

Card acceptance method (A)	Description
Mag Stripe	terminal.

Transaction types

The table below describes the types of card payment available. Each option can be set to **Allow** the transactions or **Decline** when not selected.

Transaction Type (T)	Description
Purchase with Cashback (DE=09)	Allow the cardholder to receive cash as part of a purchase transaction, in addition to purchase of goods or services, If this option is set to disallow, then the cardholder cannot receive cash as part of a purchase transaction.
Cash Advance (DE=17)	Allow the cardholder to withdraw cash over the counter at a bank or other financial agency. The cash advance can only be attempted up to a certain limit, for example, over the counter at a Bureau de Change. If this option is set to disallow, then the cardholder cannot withdraw cash over the counter at a bank or other financial agency
Cash ATM (DE=01)	Allow the cardholder to withdraw cash at a cash machine. If this option is set to disallow, then the cardholder cannot withdraw cash at a cash machine.
PIN Change ATM (DE=92 (M).70 (V))	Allow the cardholder to change their online PIN at a cash machine. If this option is set to disallow, then the cardholder cannot change their online PIN at a cash machine. **Note:** When selecting this option, consider the rules for the prevention of common number patterns, such as 1111 or 1234 or the cardholders date of birth (ddmm or mmyy).
Bal Enquiry ATM (DE=30)	Allow the cardholder to view the available balance at a cash machine. If this option is set to disallow, then the cardholder cannot view the available balance at a cash machine.
PIN Unblock (via ATM) (DE=91 (M).72 (V))	Allow successful processing of PIN based card payments after a PIN has been blocked. Use the Smart Client to reset the online PIN, it cannot be reset at the cash machine. If this option is set to disallow, then PIN based card payments will be declined after a PIN has been blocked.
Credits - Refund (DE=20)	Allow refunds to be applied to a cards in the card usage group. If this option is set to disallow, then refunds cannot be applied to cards in the card usage group.
Purchase Goods & Services (DE=00)	Allow the purchase of physical goods (such as books, pens, shoes) and services provided by other people, for example doctors or barbers. If this option is set to disallow, then the cardholder cannot purchase physical goods.
Visa quasi-cash (POS) transactions (DE=11)	Allow the cardholder to make Quasi Cash card payments. Quasi Cash is the use of a prepaid card to purchase money orders, travellers checks, foreign currency, lottery tickets, casino chips, vouchers which are redeemable for cash, crypto or racetrack wagers. A percentage (%) of the amount of each transaction is applied to the card as a fee. If this option is set to disallow, then the cardholder cannot make Quasi Cash card payments.
Credits Auth (DE=28)	Allow authorisations of credit to be applied to cards in the card usage group. These refer to any money credited to the cardholders account that is not a refund, for example, gambling credits, refund or disbursement of online betting winnings. If this option is set to disallow, then credit authorisations are not permitted. A credit authorisation is a refund or push of credits to the cardholders account, it has a settlement period, during which time the settlement occurs and the funds are made available to the cardholder. Selected by default, as an acquirer may send an authorisation to as if **Credit Auth (DE=28)** is permitted.
Original Credit (DE=26)	For Visa only, allow authorisations of original credit to be applied to cards in the card usage group. Original

Transaction Type (T)	Description
	Credit refers to any money credited to the cardholders account that is not a refund, for example, gambling credits, refund or disbursement of online betting winnings. If this option is set to disallow, then original credit authorisations are not permitted. A credit authorisation is a refund or push of credits to the cardholders account, it has a settlement period, during which time the settlement occurs and the funds are made available to the cardholder. Selected by default, as an acquirer may send an authorisation to as if **Credit Auth (DE=28**) is permitted.
Account Funding transaction (AFT)(DE=10)	Allow account funding transactions. Account funding transactions from Mastercard are based on MCC groups; if you want these to be blocked then you will need an MCC block. Allowed by default by Mastercard. **Note:** Visa has mandated Issuers support this transaction type so must be selected for all Visa programmes. This is not mandatory for Credit.

Verification

The table below describes the verification options available for card payments. Each option can be set to **Allow** the transactions or **Decline** when not selected.

Verification (V)	Description
Bypass Online PIN Check	Allow the card terminal to bypass the Thredd PIN verification and send the transaction (using the EHI) to the Program Manager for PIN verification. If this option is set to disallow, Thredd verifies the PIN. Only available in EHI 1.4 or later (modes 1, 2, 4 or 5)
Bypass Expiry Date Check	Allow the card terminal to bypass the expiry date check. Used when the Program Manager must verify the expiry date instead of Thredd. When selected, the transaction is sent (using the EHI) to the Program Manager for the expiry date verification. If this option is set to disallow, then Thredd verifies the expiry date. Only available in EHI 1.4 or later (modes 1, 2, 4 or 5)
Bypass CVV2/CVC2 Check	Allow the card terminal to bypass the card verification value (CVV2) or the card validation code 2(CVC2) check. Used when the Program Manager must verify the CVV2 instead of Thredd. When selected, the transaction is sent (using the EHI) to the Program Manager for CVV2 verification. If this option is set to disallow, then Thredd verifies the CVV2. Only available in EHI 1.4 or later (modes 1, 2, 4 or 5)
Blank CVV2 in Card not Present E-commerce	Allow the approval of e-commerce transactions where card is not present and the CVV2 is blank. If this option is set to disallow, then these transactions are declined. **Note:** For Visa, the scheme level advanced permission *"Allow if Merchant Provides no CVV2"* must be enabled, or transactions will decline with no CVV2.
Blank CVV2 in Card not Present Phone/Mail Order	Allow the approval of phone / mail order transactions (MOTO) where the card is not present and the CVV2 is blank. If this option is set to disallow, then these transactions are declined. For Visa, the scheme level advanced permission *"Allow if Merchant Provides no CVV2"* must be enabled, or transactions will decline with no CVV2. This only applies to the initial authorisation, which is flagged as recurring. The subsequent recurring payments are flagged as presentments. Subscription services such as Amazon Prime will not have CVV2.
Blank CVV2 in Card not Present Recurring	Allow the approval of recurring transactions where the card is not present and the CVV2 is blank. If this option is set to disallow, then these transactions are declined. For Visa, the scheme level advanced permission *"Allow if Merchant Provides no CVV2"* must be enabled, or transactions will decline with no CVV2. This only applies to the initial authorisation, which is flagged as recurring. The subsequent recurring payments are flagged as presentments. Subscription services such as Amazon Prime will not have CVV2.
Blank CVV2 in Card not Present Manual Key Entry	Allow the approval of card not present - manual key entry transactions where the CVV2 is blank. If this option is set to disallow, then these transactions are declined. For Visa, the scheme level advanced permission *"Allow if Merchant Provides no CVV2"* must be enabled, or transactions will decline with no CVV2.
Allow Blank DE014	Allow to approve transactions without checking the expiry date present in the DE014 field. If this option is set to disallow, then the expiry date present in the DE014 field is checked when approving transactions. **Note:** The default setting for this option is disallowed. Thredd recommends the default setting.
Expiry date optional for	Allow recurring payment transactions where the expiry date is omitted. If this option is set to disallow, then recurring payment transactions where the expiry date is omitted are declined.

Verification (V)	Description
Recurring Payments	If the expiry date is **present** and **incorrect**, the transaction will be declined.
Bypass Card Status Check for Refund Authorisations	Allow for the card terminal to bypass the card status check for refund authorisations. In this case, a card which is NOT in all good status will accept ONLY Refund Authorisations. If this option is not set to allow, the card terminal will not bypass the card status check for refund authorisations.

Miscellaneous

The table below describes the miscellaneous options available for card payments. Each option can be set to **Allow** the transactions or **Decline** when not selected.

Misc (M)	Description
If declined, force next EMV transaction online	For Mastercard only, allow to force online authorisation of next EMV transaction where the transaction is declined. This occurs if the cardholder has reached the level of offline transactions and then attempts an ATM transaction. Counters are reset and the cardholder can continue to make offline transactions; however, the card has a zero or negative balance. Requires Mastercard M/Chip 4.1 or M/Chip Advance, and only receives this information in EMV contact transaction (not EMV contactless). For Visa, VIS Cryptogram does not support this feature, therefore it is not currently available. When available, use VIS Cryptogram version number 18.
If Zero or negative balance, force next EMV transaction online	For Mastercard only, allow to force online authorisation of next EMV transaction where the balance of the transaction is zero or a negative value. In this case, ensures the next authorisation is NOT approved offline. For Mastercard, this feature requires Mastercard M/Chip 4.1 or M/Chip Advance, and only receives this information in EMV contact transaction (not EMV contactless). For Visa, VIS Cryptogram does not support this feature, therefore it is not currently available. When available, use VIS Cryptogram version number 18.
Force next EMV transaction online	For Mastercard only, allow to force online authorisation of the next EMV transaction. If this flag is selected, it always takes effect, if the current transaction is approved or declined. **Note:** VIS Cryptogram does not support this feature, therefore it is not currently available.
Reset EMV counters to upper offline limits	For Mastercard only, allow to reset the EMV counters to the upper offline limits. In this case, the ARPC response code byte 2 will have lowest 2 bits set to "01" instead of current "10" **Note:** VIS Cryptogram does not support this feature, therefore it is not currently available.
Transaction Alerts enabled	For Mastercard only, allow to enable transaction alerts, the alert mechanism of international e-commerce transactions.
Instant funding	For Mastercard, Visa Fast Funds and MoneySend Instant Funding, allow to enable Instant Funding.
Override to allow International e-commerce	For Mastercard and Visa, allow international e-commerce. If e-commerce is enabled, but international transactions are blocked, this flag will **Override to allow International e-commerce**.
Override to allow International Credential on File	For Mastercard and Visa, allow international credentials on file. This is required for overseas wallet usage by Apple. If Yes, then Credential on File merchant (e.g. Apple & Amazon) can be outside of country of issue. **Note:** This option is only applicable if *"POS usage outside country of Issue of card"* is NOT enabled.
Faster Refunds Support	For Mastercard and Visa, allow for support of Faster Refunds. For a **Fast Refund** inbound authorization request, the cardholder account is credited within a certain time frame. When the Faster Refund criteria is met the cardholder will be updated within 30 minutes of successful authorisation processing. Mastercard have mandated that Instant Credit Gambling Payouts must be credited within a certain time frame from receipt of the authorization.
Instant Credit	For Mastercard, allow instant credit gambling payout. This option only applies to gambling payouts. must be enabled

Misc (M)	Description
Gambling Payouts	for ALL products in the Mastercard Europe Region (mandated by Mastercard); it may be enabled for products outside of this region at the issuers' request. When enabled, cards receiving cash disbursement authorisations matching the appropriate conditions will be credited immediately if approved. For Visa, only applies to Payment Transactions where MCC = 7995 (Gambling Merchants)

General FAQs

This section provides answers to frequently asked questions.

Card Manufacturer

Q. Can you support a new card manufacturer?

If the card manufacturer you want to use is not on the list of card manufacturers supported by Thredd, please contact your Thredd Business Development Manager.

Q. Can I use more than one card manufacturer?

Yes. If your card programme supports special features or issues cards in different regions, you may need more than one card manufacturer, in which case we can this set up in the system. Each card manufacturer will need to be set up under a separate Thredd Scheme.

Q. Can I get a copy of the card generation file sent to the card manufacturer?

Yes. We can send you a copy of the card generation file (note that fields containing sensitive card details, such as Chip and Track data, will be removed).

Supported Card Features

Q. What card features can the card manufacturer provide?

Most card manufacturers should support features such as CVV2, Magstrip, Chip&PIN and contactless payments. They should enable you to supply customised artwork designs for your cards. They should also be able to arrange for packaging and delivery of cards to your customers. Some card manufacturers may support additional value-added features, such as special print formats, support for biometric authentication, or special sizes and materials. Please contact your card manufacturer directly to discuss your requirements.

Q. Can I obtain a list of which text characters my card manufacturer will support?

Yes, you can find a list in the Web Services Guide > String Cleaning and Approved Characters > Card Manufacturer Approved Characters.

PAN Stock

Q. How do I request generation of new PAN stock?

New PAN stock may be required if you run out of existing PANs or your Issuer (BIN sponsor) changes the underlying BIN ranges assigned to you.

Please contact Thredd Customer Services to request additional stock or PAN stock changes.

Note: New card requests can only be fulfilled if there is sufficient PAN stock available for your programme.

Q. Can Thredd delete PAN stock?

Yes, this is required if your underlying BINs change and your card PAN stock needs to be regenerated or if you close your programme with Thredd.

Note: If changing BIN ranges requires generating new PAN stock, your existing PAN stock must first be deleted before the new PAN stock can be used.

Please contact Thredd Customer Services to request deletion of PAN stock.

Card Expiry

Q: How does expiry date work for Gift cards and Flex cards?

The expiry date on the card is mandatory only if it is an open loop card which can be used anywhere the card scheme (payment network) is accepted. It doesn't apply to gift cards or Flex cards that have restricted usage; these types of cards do not need an expiry date displayed on the card.

Q: What are the Scheme rules around displaying the expiry date on the card?

Displaying the *expiry date* is only mandatory for open loop cards.

You can add optional text to clarify when the card expires (e.g., how long it will be valid from issue or activation date).

The *valid from* date is optional.

Q: Is it possible to set an unlimited expiry date?

No. For certain wallet accounts, such as the Master Virtual Cards (MVC), you can set this to the maximum suggested period (8 years).

Q: Why does Smart Client display a different expiry date to the physical card (when converted from a virtual card)?

When converting a virtual card to a physical card, the physical card is printed with the new requested expiry date, but the physical card first needs to be activated; the system will then update the expiry date in Smart Client.

Card Balance

Q. What happens to the Balance and Fees on an expired card?

When a card date passes its configured validity period the card status changes to 54 (*Expired Card*) and the card can no longer be used. Two options are available for handling any remaining balance on the card:

- **Apply breakage fee on expiry is enabled** – the balance on the card is removed from the card automatically and put into an expiry transaction record.
- **Apply breakage fee on expiry is not enabled** – the balance will remain on the card. You can then do a balance adjustment or unload to remove the remaining funds. If a recurring fee has been set up then the system will continue to deduct the fee from the card until there is no balance

Note: Fees are only applicable if you are using the Thredd Fees Module. See the Fees Guide.

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 and is branded as ‘Verified by Visa’ and ‘Master-card SecureCode’ respectively.

A

Acquirer

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

Authentication

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

Authorisation

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

B

BIN

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

C

Card Manufacturer

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

Card Scheme (Network)

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

Chargeback

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

Clearing File/Clearing Transaction

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

E

EMV

A payment card chip standard, to ensure all EMV cards work in all EMV terminals. Derived from the names of the three payment sys-tems that wrote it: Europay, Mastercard and Visa. See www.emvco.com for more information

External Host

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

F

Fee Groups

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

Flex Card

A Flex card works like a prepaid credit or debit card and can have multiple options for use, including online purchases. It can be used to pay for certain types of items, such as healthcare and medicines.

I

Issuer (BIN Sponsor)

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

L

Luhn check digit

The Luhn check is a simple checksum formula used to validate a variety of identification numbers. The check digit is most often the last digit.

M

Merchant

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

Merchant Category Code (MCC)

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

O

Open Loop Card

A card which can be used anywhere the card scheme (payment network) is accepted, without restrictions

P

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 (payment networks). All Program Managers who handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security/

Primary Account Number (PAN)

The PAN is the long number (typically 16-19 digits) that is either printed or embossed on the card.

Private-labelled

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

Product Setup Form (PSF)

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

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.

Public Token

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

S

sFTP

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

Smart Client

Smart Client is Thredd's user interface for managing your account on the Thredd platform. 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.

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 (BIN sponsor). Depending on your Thredd mode, Thredd may also provide STIP on your behalf, where your systems are unavailable.

V

Validation

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

VPay cards

A Single Euro Payments Area (SEPA) debit card for use in Europe, issued by Visa Europe, which uses the EMV chip and PIN system and typically does not include a magnetic stripe

Document History

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

Version	Date	Reason	Who
1.1	22/04/2024	Updates to content to align with taxonomy updates on our Documentation Portal.	WS
	22/04/2024	Added details of use of Card Biometric Authentication as a card security feature. See Card Security Features.	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
1.0	17/04/2023	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

Support Phone: +44 (0) 203 740 9682

Our Head Office

6th Floor,

Victoria House,

Bloomsbury Square,

London,

WC1B 4DA

Telephone: +44 (0)330 088 8761

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.