Virtual Cards Guide

Version: 1.4

12 October 2023

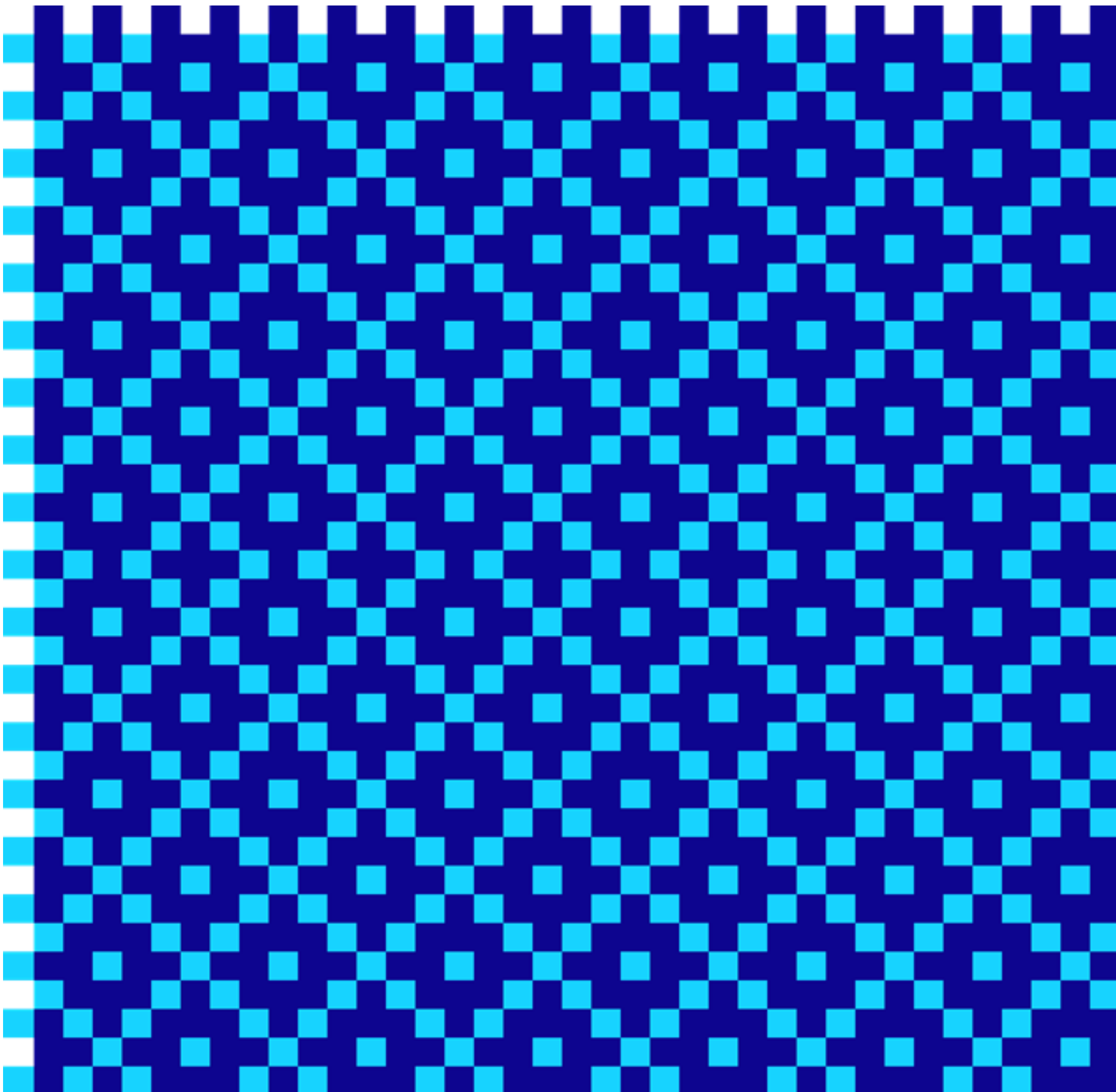
Publication number: VCG-1.4-10/12/2023

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: +442037409682



Copyright

About This Document

This document describes how to set up a virtual card and configure the virtual image which is displayed to your customers on your website or customer app.

Target Audience

This document is intended for Thredd clients (Program Managers) who are interested in implementing Thredd virtual card functionality.

What's Changed?

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

How to use this Guide

If you are new to the Thredd virtual card creation service and want to understand how it works, see the Introduction.

To find out about virtual card configuration options, see Virtual Card Setup. To find out how to configure your virtual image design, see Virtual Card Image Design.

For details of using the Web Services API to create and manage your virtual cards, see Using the Web Services API.

Related Documents

Refer to the table below for other documents which should be used in conjunction with this guide.

Document	Description
Web Services Guide	Provides details of the Thredd Web Services API used for creating and managing both physical and virtual cards.

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

1 Introduction

Thredd supports the creation of two types of cards:

- Physical cards
- Virtual cards

A *Virtual Card* is a card that does not have any physical plastics generated and can only be used to pay for purchases online 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. See Virtual Card Setup.

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 CVV 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[1]. For details, see Virtual Card Image Design.

1.1 Thredd Virtual and Physical Card Options

Thredd provides a number of options for setting up your virtual card program:

- Virtual Cards only
- Both Virtual and Physical Cards – set up as different products with different PANs
- Virtual Cards can be converted to physical – keeping the same PAN

Both virtual and physical cards are created using the Thredd Web services API. At the time of submitting card creation instructions using the API, you can specify whether to create a physical or virtual card and the virtual card image design to use. For details see Virtual Card Image Design.

[1]You must be PCI Compliant in order to process or display card details such as the full PAN on your systems. If you are not PCI Compliant, Thredd can display the masked PAN or the Thredd public token.

2 Virtual Card Setup

Below are details of the steps you need to complete to set up a virtual card product:

- Decide how you want to set up your Virtual Card Product
- Complete Issuer Forms for Virtual Cards
- Confirm whether you are able to display Full Card PAN
- Set up PGP-Encryption for Virtual Card Images
- Complete your Thredd Product Setup Form
- Set up your Virtual Card Usage Groups

Optional setup:

- SMS Message Configuration
- MeaWallet Integration

Each of these steps is described in further detail below.

2.1 Overview of Steps

2.1.1 Decide how you want to set up your Virtual Card Product

Discuss with your Implementation Manager how you want Thredd to set up your virtual card product. Virtual and physical card settings are applied at the internal Thredd scheme level. Options available include:

- **Physical cards only** – all cards are created as physical cards.
- **Virtual cards only** – all cards are created as virtual cards.
- **Conversion of virtual cards to physical cards** – all cards are created initially as virtual cards and need to be converted to physical cards using web services API. See Converting Virtual Cards to Physical Cards.
- **Both physical and virtual cards** – for this option you require separate internal Thredd schemes set up for both physical and virtual cards.

For more information about the Thredd setup and configuration, see Summary of Thredd Virtual Card Setup Options.

2.1.2 Complete Issuer Forms for Virtual Cards

To support virtual cards, your card issuer will need to complete the relevant Mastercard or Visa card setup forms and specify virtual card creation; they will need to assign a sub-BIN range for the use of virtual cards. All card transactions on this sub-BIN range will be restricted to online usage only.

For details of which scheme forms to complete, please check with your Implementation Manager.

2.1.3 Confirm whether you are able to display Full Card PAN

If you want to display the full PAN in the virtual image you must be PCI Compliant.

To remove the need for full PCI compliance, you can use a number of options:

- You can request a virtual card image that replaces the PAN with a *customer account number* that you supply. When you submit a Create Card request using the Web Services API, you can then populate your customer account number using the `<CustAccount>` field. See Create a Card.
- The masked PAN (middle 6 numbers of the PAN) and the CVV could be sent to the cardholder via another means (e.g., SMS). See SMS Message Configuration .
- Thredd can display the Thredd Public Token in place of the PAN.
- The Thredd MeaWallet service provides an alternative option for displaying full PAN and other card details to the cardholder if you are not PCI Compliant. See MeaWallet Integration.

2.1.4 Set up PGP-Encryption for Virtual Card Images

Where Thredd provides the virtual image, we support PGP-encrypted images. Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication and is used for signing, encrypting, and decrypting graphic files to increase the security of email communications.

PGP Keys must be exchanged between the Program Manager and Thredd. Normally, we ask you to generate the PGP key and provide it to us. Separate keys are required for Thredd Test and Production environments.

Thredd use the PGP key to encrypt the virtual card image. The encrypted virtual image of the card (with details such as PAN, CVV and expiry date embossed on it) will be returned in the response to a card create or image regenerate web service request. For details, see Using the Web Services API.

You then use your PGP key to decrypt the image.

2.1.5 Complete your Thredd Product Setup Form

If you are using Thredd to generate the virtual card image, then complete the **Virtual Card Image** tab on the *Thredd Product Setup Form (PSF)*. This form defines the design options for your virtual image. For details see Virtual Card Image Design.

If you are using a customised background image, please provide this to your Implementation Manager in the requested format and specifications, as described in Background Image Specifications.

2.1.6 Set up your Virtual Card Usage Groups

Each of your card products is linked to a default set of card usage groups in the Thredd system. The usage groups enable you to control how your virtual cards can be used.

Examples of card groups include: *Velocity limits* and *Card Usage*.

Velocity Limits Groups

For a virtual card product, cash limits are set zero, so the card cannot be used at a Point of Sale (POS) terminal.

Card Usage Groups

For a virtual card product, card use at Point of Sale (POS) terminal is disabled. The following methods of using the card are typically enabled for a virtual card:

- Card Not Present (Ecommerce)
- Card Not Present (MOTO)
- Manual Key entry transaction - Card Not present

You can decide whether to enable the following transactions:

- Card Not Present (Recurring)
- Allow Manual Key entry transaction - Cardholder Not present

The following transaction types are usually enabled for a virtual card:

- Credits / Refunds transactions
- Purchase of Goods & Services
- Credits Auth

See the example below of setup of card usage groups on the *Product Setup Form*:

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	dits 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 Groups on the Product Setup Form

2.2 Optional Setup

Below are additional options you can set up for your virtual cards.

2.2.1 MeaWallet Integration

This integration enables MeaWallet to retrieve the PAN and other relevant card data directly from the Thredd platform. MeaWallet then encrypts the card data and sends the encrypted payload to your cardholder's mobile phone application.

Note: This is a separate service, provider by MeaWallet. Other service providers are also available, such as Digiseq. You will sign a separate agreement with them.

For more information, please contact your Implementation Manager.

2.2.2 SMS Message Configuration

Thredd provides a default SMS message that can be enabled at the time when you create the virtual card (using the web services API).

If you want to change the wording on the default SMS message, Thredd can optionally configure the dynamic field content included in the SMS message sent to the cardholder when you use the web services API to create a virtual card or renew a card image. This is set at a Program level and applies to all products under a Thredd Scheme.

Example of Default SMS

```
"3 digit Security Code : %CVV% and the middle 6 digits of your Virtual Card is %PAN6%. Thank you"
```

Important code lines:

- `%CVV%` is the card's CVV
- `%PAN6%` is the middle 6 digits of the PAN.

Enabling SMS messages

Once set up, to enable this option in your Create a Card web service request, you must set the <sms_required> field in your request, to 1.

Note: Thredd charge a fee for sending SMS messages. Refer to your Contract for details.

2.3 Converting Virtual Cards to Physical Cards

This section is relevant to Program Managers who are using the Converting a Virtual Card to a Physical Card web service to convert a virtual card to a physical card.

On card convert, the virtual and physical card share the same PAN and Thredd token. Virtual and physical card share the same card record in the Thredd system, so cardholders can track their transactions on the card and view both physical card and historical virtual card transactions[1].

Note: If you want to convert a virtual card to a physical card, you need to use the same card keys (e.g., MDK, CVK, PKI keys) as supplied by the card manufacturer for both the virtual card and physical card.

2.3.1 Printing of Physical Cards

When your card product is set up, it is linked to a card manufacturer (card bureau). You will need to go through the integration and testing process of setting up your physical cards via your chosen card manufacturer: get your card design approved by your card scheme, create test card plastics, test CHIP profiles and create live base cards for use. This needs to be done in advance, so your cards will be ready for personalisation and printing when the virtual card is converted to a physical card.

When you convert a virtual card to a physical card, the card instructions are sent to your card manufacturer, to print and despatch the card to the specified address. The cardholder can continue to use the virtual card until they have received and activated the physical card[2].

2.3.2 Card CVV and Card Expiry

When converting to a physical card, you can optionally keep the same expiry date and CVV2. Note that a new expiry date and CVV2 will be generated if the conversion falls in a different calendar month to the virtual card creation.

The CVV is calculated by encrypting the bank card number and the expiration date with keys, so if the expiry date for the physical and virtual card is different, the CVV will also be different.

You can set the expiry date for the virtual card, using the <ExpDate> field in the Create a Card web service. When converting a virtual to physical card, you can use the <ExpDate> field in the Convert Card web service to set the expiry date.

2.3.3 How to use the Card Convert API

For more information, see Converting a Virtual Card to a Physical Card.

Note: Thredd charge a fee for converting virtual cards to physical cards. Refer to your Contract for details.

2.4 Summary of Thredd Virtual Card Setup Options

The table below provides a summary of the configuration options for a virtual card product:

Setup Option	Virtual Only	Virtual converted to Physical	Both Virtual and Physical cards offered
Thredd Scheme setup	1 Thredd Scheme	1 Scheme	2 Thredd schemes required

---

[1] Thredd provide an option to create a separate PAN and Thredd token on card convert. In this case, the system creates two linked card records, and both cards can continue to be used. If you want this option, we recommend you ask your implementation manager to set up separate physical and virtual card products.

[2] For security reasons, we recommend you either set the card to an inactivate status or ensure that the card usage groups linked to the card enforce virtual only usage on the physical card until the cardholder has received and activated the card.

Setup Option	Virtual Only	Virtual converted to Physical	Both Virtual and Physical cards offered
Product setup	1 Thredd Product	1 Thredd Product	2 Thredd products required if Virtual and Physical cards have different sub-BINs. If Virtual and Physical cards share the same PANs, then one product is required per currency and country of issue.
Card Manufacturer	Not required	Required for the physical card	Required for the physical card
Key exchange	Required[3]	Required for the physical card	Required for the physical card
Mastercard/Visa Card validation	Not required	Required for the physical card	Required for the physical card
PAN	Unique per card	Virtual and physical card have the same PAN.	Unique per card
Web Services API	Use Card Create	Use the Create a Card web service to create the virtual card and the Convert Card web service to convert to a physical card[4].	Use Card Create
Card Activation[5]	On card create	Physical card set to inactive and must be activated on delivery. Once activated, the virtual card cannot be used.	Virtual card activated on card create Physical card activated on delivery.

[3]Required where Thredd generates the virtual card image

[4]Cards can be set up to convert with a different PAN if required (not recommended).

[5]Set via Web Services API on card create or card convert.

3 Virtual Card Image Design

This section describes how to configure the design of your virtual card images. Three options are available:

- Thredd generates the virtual card image: Using the Default Thredd Image Design
- Thredd generates the virtual card image: Using a Customised Image Design
- You use the information returned in the response to a card create requestion to Generating your Own Virtual Card Image and display it in your Customer smartphone application or on your Customer Portal.

Each of these steps is described in further detail below.

3.1 Using the Default Thredd Image Design

If you are using the Thredd system to generate a virtual card image and do not specify your own design, the default Thredd background image and dynamic field settings are used, as shown in the figure below:

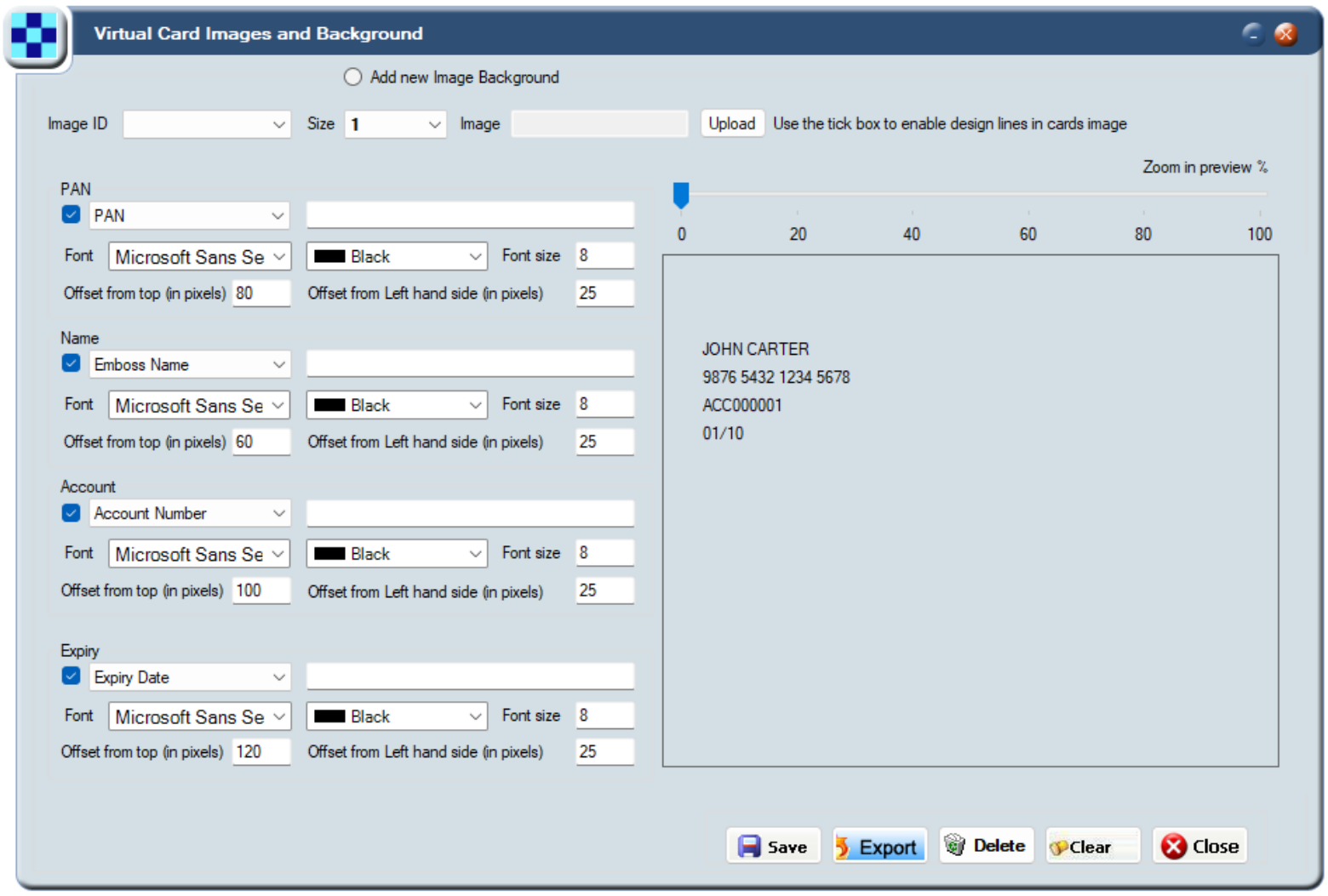
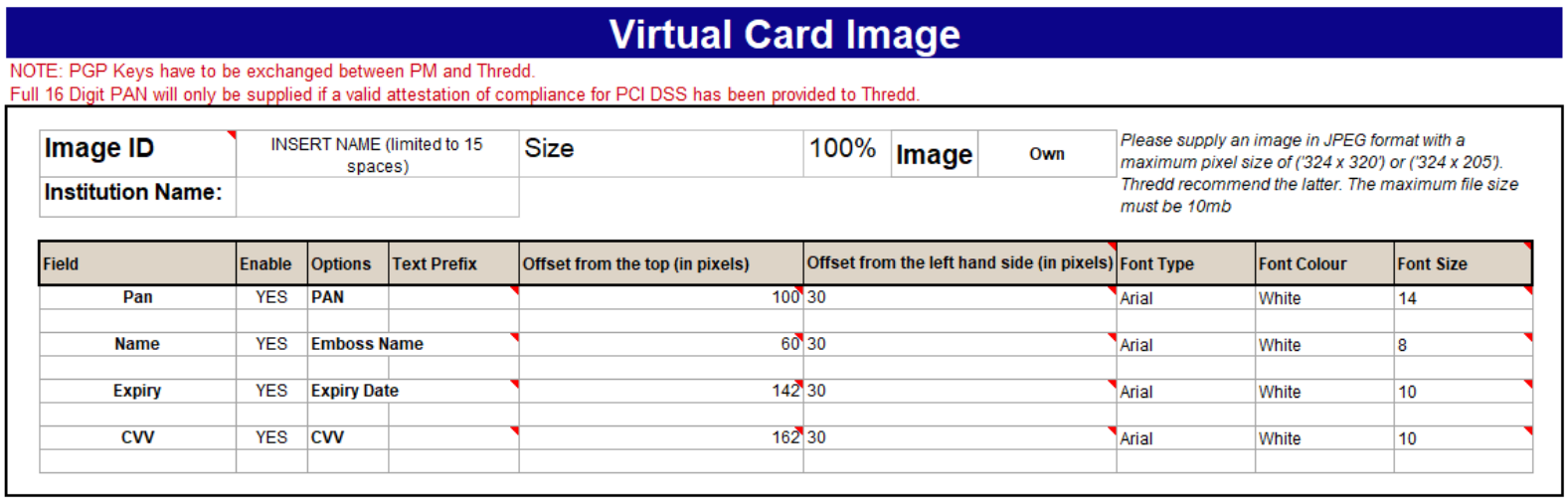


Figure 2: Virtual Card Image Setup in Smart Client

Note: The default settings for the Thredd image cannot be changed.

3.2 Using a Customised Image Design

If you are using the Thredd system to generate a virtual card image and you want to customise the appearance of the background image and dynamic text elements, please complete the Virtual Card Image tab on your Thredd *Product Setup Form (PSF)*. See the example below.



Virtual Card Image

NOTE: PGP Keys have to be exchanged between PM and Thredd.
Full 16 Digit PAN will only be supplied if a valid attestation of compliance for PCI DSS has been provided to Thredd.

Image ID	INSERT NAME (limited to 15 spaces)	Size	100%	**Image**	Own
Institution Name:					

Please supply an image in JPEG format with a maximum pixel size of ('324 x 320') or ('324 x 205'). Thredd recommend the latter. The maximum file size must be 10mb

Field	Enable	Options	Text Prefix	Offset from the top (in pixels)	Offset from the left hand side (in pixels)	Font Type	Font Colour	Font Size
Pan	YES	PAN		100	30	Arial	White	14
Name	YES	Emboss Name		60	30	Arial	White	8
Expiry	YES	Expiry Date		142	30	Arial	White	10
CVV	YES	CVV		162	30	Arial	White	10

Figure 3: Product Setup Form - Virtual Card Image tab

3.2.1 Image Options

Refer to the table below for details of image configuration options.

Field	Description	Example
Image ID	If you want to support more than one card image file, then enter a unique image ID, to identity your virtual image. The image ID to use can then be specified when creating the virtual card using the Thredd Web Services API. See Using the Web Services API. Note: To support multiple images, you should create copies of the **Virtual Card Image** form and populate details for each Image you want to display.	ABCD12345
Institution Name	Institution name, as set up in Thredd.	MyBank
Size	Image size to be displayed. The image displayed to the cardholder will be scaled according to this setting. Note: You can only scale up image sizes (e.g., 200%; the maximum size is 500%)	100%
Image	Whether to use the default Thredd image or your own image for the background image. For details of supported image formats and sizes, see Background Image Specifications.	Own
Dynamic Field Display Options:		
Field	There are four default fields: PAN, Name, Account and Expiry. For each field you can configure the type of dynamic content and the text format to be displayed in each field. The dynamic field content is added as a layer on top of the background image supplied. See Background Image Examples	
Enable	Whether to display this field on the virtual image. Options are: YES or NO.	YES
Options	The data value to display, such as *PAN*, *Emboss Name*, *CVV* or *Expiry Date*. You can use this to tweak the field types and the order in which to display them.	PAN
Text Prefix	Whether to include any prefix text on the field, to be shown before the dynamic field value. Example 1: **Name**: *John Smith* (where **name** is the prefix and *John Smith* is the dynamic value) Example 2: **CVV** *123* (where **CVV** is the prefix and *123* is the dynamic value)	Name: CVV:

Field	Description	Example
	See Virtual Card Image Design Examples	
Offset from the top	The offset of this field in pixels, from the top edge of the image. We recommend you use the suggested default offset for each field.	100
Offset from the left-hand side	The offset of this field in pixels, from the left edge of the image. We recommend you use the suggested default offset.	30
Font Type	The font type (e.g., Helvetica, Arial). We have a large number of standard Windows fonts available; please check with your Implementation Manager if you have any non-standard font requirements. We recommend you use a standard font type.	Arial
Font Colour	The colour of the field's font. For a white image background, you should use a dark colour, such as black or grey; for a dark image background, you should use a light font colour, such as white or cream. You must specify the colour name and not an RGB or hex value. A wide range of colours are available. For details, please check with your Implementation Manager.	White
Font Size	Size of the field's font in points. We recommend you use the suggested default field sizes.	10

If you are unsure of how to define any of the above parameters, please provide your Implementation Manager with an example of the card display. Thredd will set the parameters accordingly.

3.2.2 Background Image Specifications

If you have an approved MasterCard or Visa Card design, we recommend using this as a background image. Any supplied image files must conform to the following requirements:

- The file should be in JPEG/JPG format[1]
- The maximum pixel size is ('324 x 320') or ('324 x 205'). Thredd recommends 324 x 205, which is the same proportions as a standard Mastercard or Visa physical card.
- The maximum file size is 10Mb
- The image resolution should be at 72dpi or at 96dpi

3.2.3 Virtual Card Image Design Examples

Below is an example of a customised image design, as set up on Smart Client.

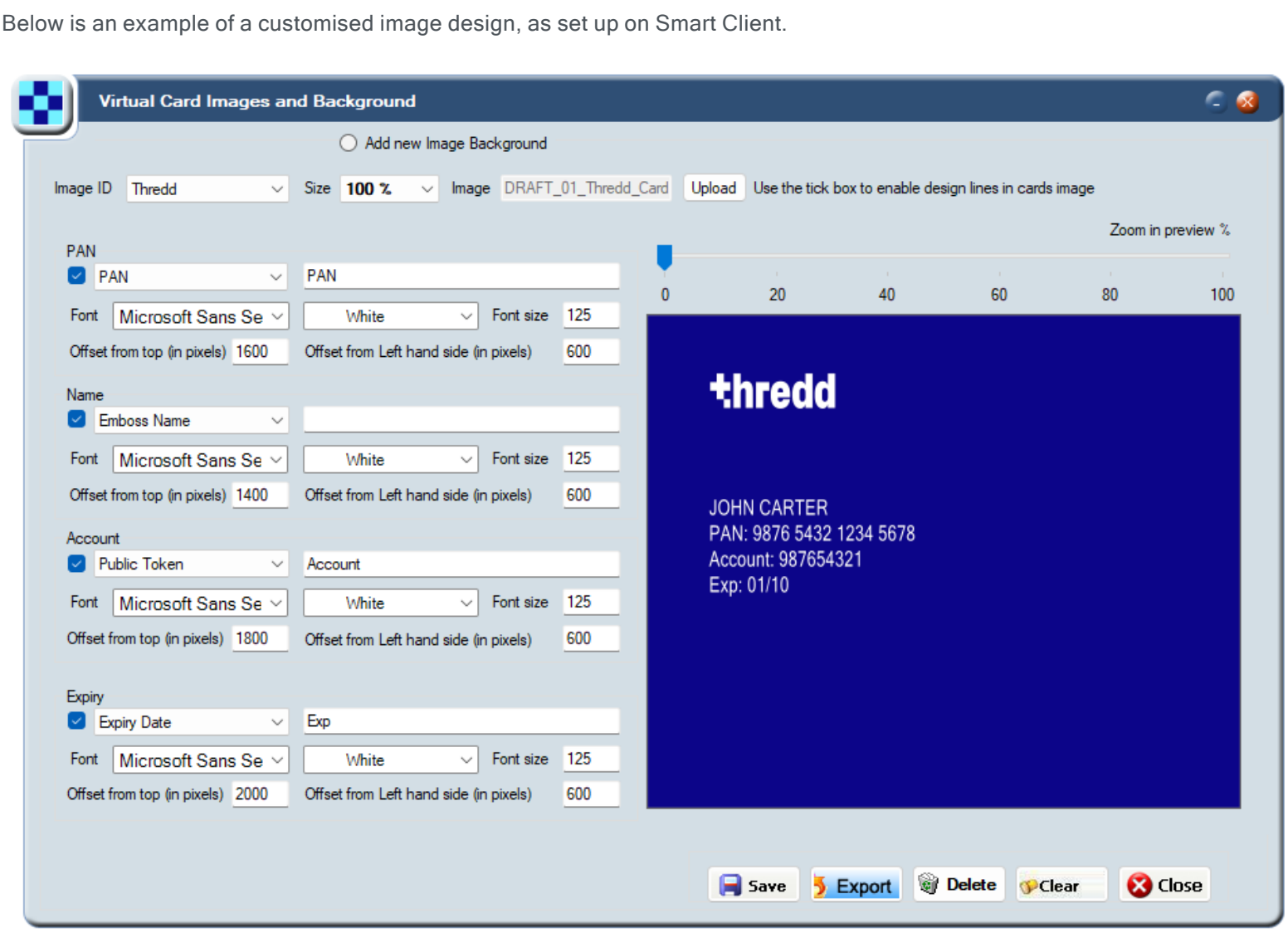


Figure 4: Thredd Virtual Card Image and Background

Background Image Examples

See examples of background images below.

[1]We can accept BMP or PNG file formats and convert to JPEG if required.

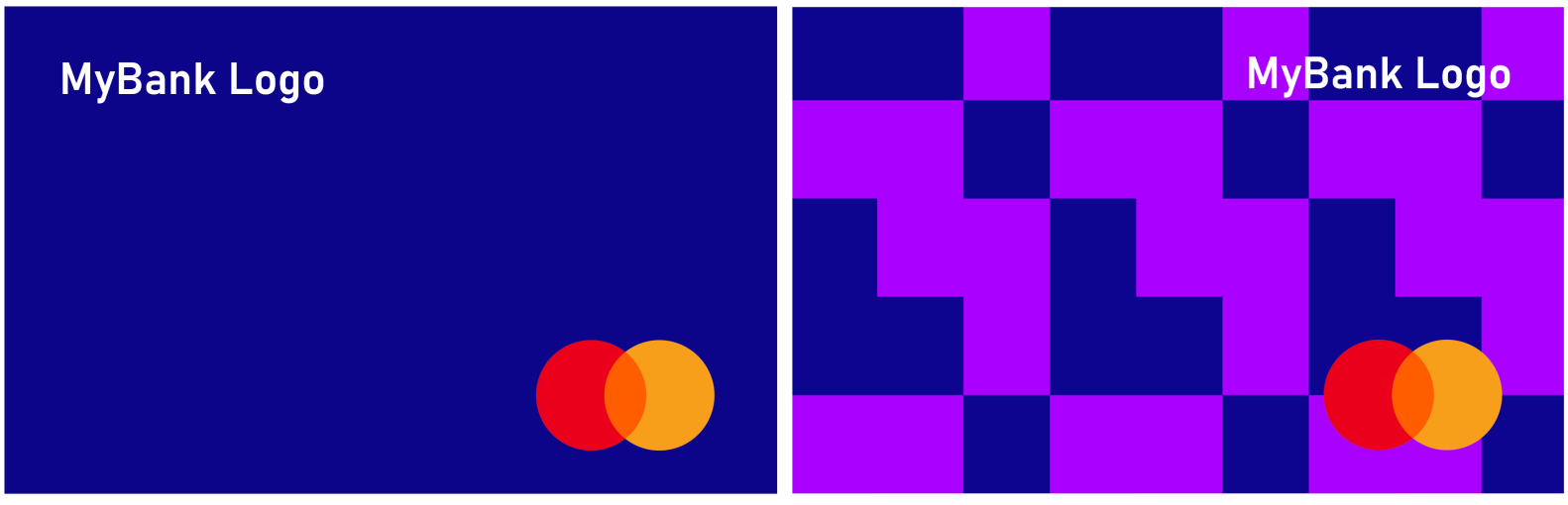


Figure 5: Example Background Images

Full Card Image Displayed to the Cardholder

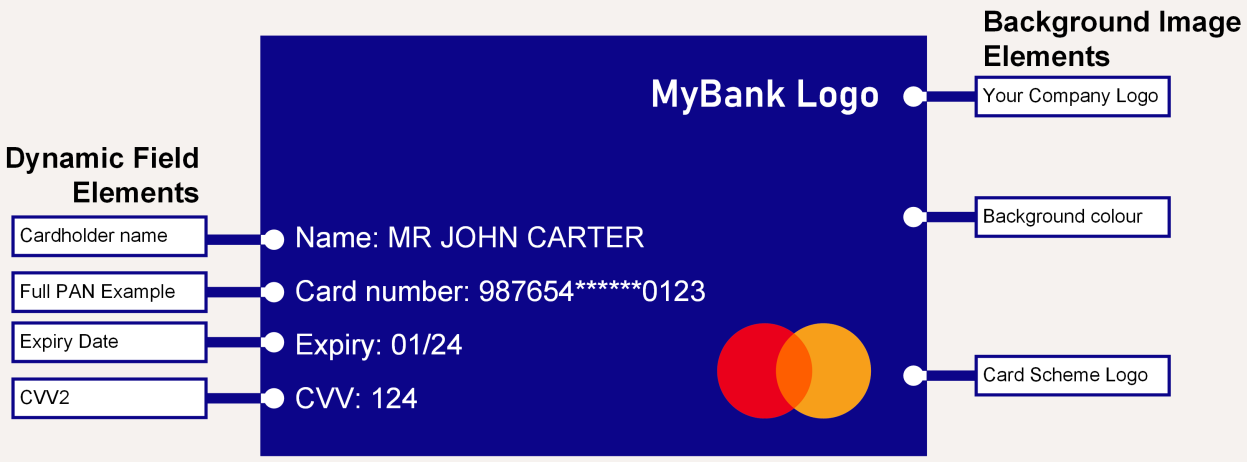
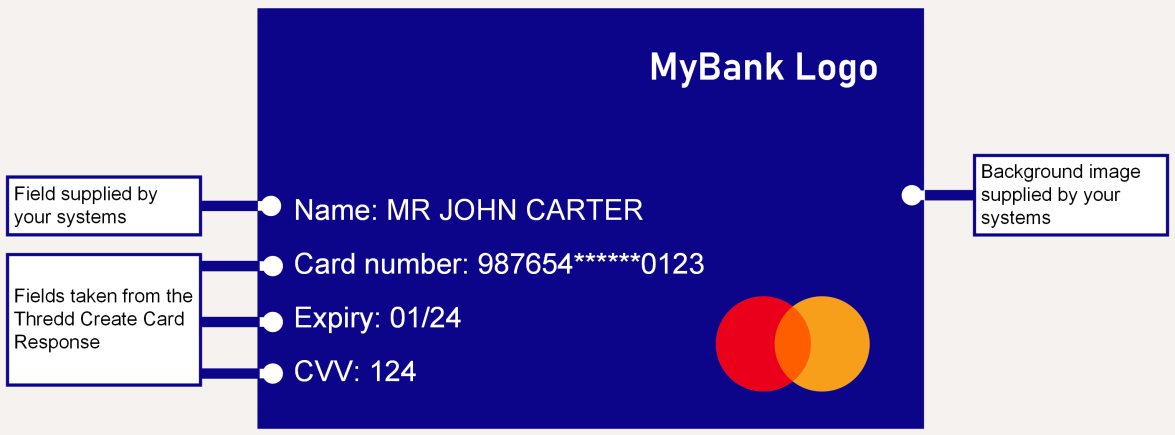


Figure 6: Example of a Virtual Card Image

If you are not PCI compliant, the image can display your customer account number or the Thredd token.

3.2.4 Generating your Own Virtual Card Image

You can generate the virtual card image on your own systems, using the details returned in the Thredd response to a Create a Card request. See the example below:



4 Using the Web Services API

The Thredd Web Services API can be used to create physical or virtual cards, regenerate virtual card images and retrieve virtual card details. For a full description, see the Web Services Guide. Below is a summary.

4.1 Create a Card

API: Ws_CreateCard

This web service is used to create both virtual cards and physical cards.

If the newly created card is virtual, and PGP keys have been exchanged, then it will create a JPEG image for the newly created card with the PAN, Public Token and Expiry Date embossed on it.

This image will be returned in the response and will be encrypted via a pre-shared PGP key. If SMS is enabled, then an SMS is sent to the cardholder's mobile number with the CVV of the card.

If you are PCI compliant, Thredd can return the full PAN in the web service response[1].

See the example code snippet below: (only key fields are shown)

```
    <hyp:Ws_CreateCard>
      <hyp:WSID>1234</hyp:WSID>
      <hyp:IssCode>ABCD</hyp:IssCode>
      <hyp:TxnCode>10</hyp:TxnCode>
    ---------
      <hyp:CreateType>1</hyp:CreateType>
      <hyp:ActivateNow>1</hyp:ActivateNow>
      <hyp:CardName>Virtual Card</hyp:CardName>

       <hyp:Sms_Required>1</hyp:Sms_Required>

     <hyp:VirtualCardImage>ABCD12345</hyp:VirtualCardImage>
    ------------
    </hyp:Ws_CreateCard>
```

Notes

- <CreateType>1 = virtual card; 3 = Create a virtual card with intention to convert it into a physical card later.
- <Sms_Required> indicates whether an SMS is sent to the cardholder with the card's CVV. 1 = yes; 0 =No. The default is '0'. The SMS is configurable.
- <VirtualCardImage> is the Image ID for the virtual image for the new card. Image IDs are set up in Smart Client. If you do not provide an image ID, the default virtual card image for the product is used.

Response Code Snippet Example

Below is an example of the response to the create card request.

```
<Ws_CreateCardResult>
            <WSID>1234</WSID>
            <IssCode>ABCD</IssCode>
            <TxnCode>10</TxnCode>
            <PublicToken>123456789</PublicToken>
            <ExternalRef/>
            <LocDate>2013-01-01</LocDate>
            <LocTime>120000</LocTime>
            <ItemID>1234</ItemID>
            <ClientCode>0</ClientCode>
            <SysDate>2013-01-01</SysDate>
            <ActionCode>000</ActionCode>
            <LoadValue>10</LoadValue>
            <IsLive>true</IsLive>
            <ExpDate>03/14</ExpDate>
            <CVV>123</CVV>
            <MaskedPAN>987654******0123</MaskedPAN>
```

[1] Full PAN must be enabled on request. Proof of PCI Compliance is required.

```
            <Image> hQEMA3Rjt-
snLP518AQgAjZ9wE8WmVGgjm7Ewi6WO0O/9rKa4W5bz/+oOVe+hWV2Ufp13GMJoao-
g4dtKbxGsYCr8mgJqtKxrd-
hD46JeUkZqbKv8hQdWn4Gj0iGuqlYIt+bBE+KwY3bIu-
muFhehB6x64R3gLLWYb+tttjhxFNt-
gp1t+I1uZX6+ey-
fUg-
dsJdl0B1fm-
c0n-
bBC47LoAQAqe-
add6K/Iot6ffCZt-
grhOwdP1FcmZCr6SatZBoRYNc/Mn6Cy-
iXcwp-
gSvAGCzvLIRCGcMtJoM7JsXDHDTFp+6iWaEq7+MQ3vi-
bILT24byn6M1oA/Ka7GAb2sSwTOKNhyxwKWsgBDg0IgeAsogNc+BCoW5vMnt/+9eioHbigaAlwOa5Hwpthcq033MS</Image>
         </Ws_CreateCardResult>
```

Notes

- <PublicToken> is the unique 9-digit internal Thredd token that can be used for all web services queries on the card.
- <MaskedPAN> is returned if you are not PCI Compliant. You can use the SMS service to provide your cardholder with the masked digits of the card. See SMS Message Configuration .
- If you are you are generating your own card image to display to your cardholder on your Customer Portal or Customer app, you can use the returned new card details to build your image. See Generating your Own Virtual Card Image.
- <Image> if you are using Thredd to generate your image, then this field contains the PGP-Encrypted image, which you will need to decrypt using your Thredd key. See Set up PGP-Encryption for Virtual Card Images.

4.2 Regenerate the Card Image

API: Ws_Regenerate

This web service can be used to recreate a virtual card image if needed for any reason.

An SMS is sent to the cardholder's mobile number with the CVV of the card if the <Sms_Required> field is set to 1.

See the example code snippet below: (only key fields are shown)

```
<hyp:Ws_Regenerate>
         <hyp:PublicToken>123456789</hyp:PublicToken>
         <hyp:RegenType>1</hyp:RegenType>
         <hyp:Sms_Required>0</hyp:Sms_Required>
          -----------
         <hyp:WSID>12345678</hyp:WSID>
         <hyp:IssCode>CLIENT</hyp:IssCode>
 </hyp:Ws_Regenerate>
```

Notes

- <RegenType> indicates whether to regenerate the card. 0 = only return the CVV and do not regenerate; 2 = Only create the card image, do not regenerate card.
- If a PGP key has been shared and configured, then a PGP-encrypted image of the card is returned in the <Image> field of the response.

Response Code Snippet Example

Below is an example of the response to the regenerate card request.

```
Ws_RegenerateResult>
            <PublicToken>123456789</PublicToken>
            <ActionCode>000</ActionCode>
            <CVV>123</CVV>
            <PAN>123456******4321</PAN>
</Ws_RegenerateResult>
```

4.3 Converting a Virtual Card to a Physical Card

When you convert a virtual card to a physical card it will adopt the same settings as the virtual card. The card is created with the same PAN[2]. A new expiry date and CVV2 are generated if the conversion falls in a different calendar month to the virtual card creation. The card instructions are sent to your card manufacturer for printing and despatch to the cardholder.

Following successful conversion, any replacement or renewal cards are generated as physical cards. The cardholder can still continue to use their virtual card until the physical card is activated, after which the virtual card will stop working.

How to convert a card

- Prior to converting the card, you should update any cardholder details, using the Update Cardholder Details web service API (Ws_Update_Cardholder_Details or Ws_Update_Cardholder_Details_V2). For details, see the Web Service Guide.
- To convert the card, you can use the Convert Card web service (Ws_Convert_Card).

See the example code snippet below: (only key fields are shown)

```
<hyp:Ws_Convert_Card>
         <hyp:PublicToken>123456789</hyp:PublicToken>
         <hyp:ConvertDate>2013-01-01</hyp:ConvertDate>
         <hyp:Apply_Fee>0</hyp:Apply_Fee>
         <hyp:ExpDate>2015-03-31</hyp:ExpDate>
         <hyp:ImageId></hyp:ImageId>
</hyp:Ws_Convert_Card>
```

Notes

- <ConvertDate> can be used to specify the date on which to convert the card
- <ExpDate> can be used to specify the expiry date of the new physical card
- <ImageId> identifies the card manufacturer's image file that will be printed on the face of the card. If not supplied, then the ImageId supplied with Ws_CreateCard will be used if available.

Response Code Snippet Example

Below is an example of the response to the convert card request.

```
<Ws_Convert_CardResult>
            <ActionCode>000</ActionCode>
            <PublicToken>123456789</PublicToken>
            <ConvertDate>2013-01-01</ConvertDate>
</Ws_Convert_CardResult>
```

4.3.1 Activating the Physical Card

Where a virtual card has been activated, the physical card will also be active in transit. We therefore recommend you set the status of the physical card to inactive and enforce virtual only usage until the cardholder has received their card and activated it.

You should use the Card Activate web service (Ws_Activate) to activate the physical card.

---

2 Thredd has an option to generate a different PAN on card convert; we recommend that if you require different PANs, you ask your implementation manager to set this up as separate card products. See Virtual Card Setup.

Frequently Asked Questions

Virtual Card Usage

Q. Can a Virtual Card PAN be used for POS transactions?

No, you cannot use a virtual card at a Point of Sale (POS) terminal. Virtual card usage is restricted at the card scheme level to online (ecommerce) or Mail and Telephone Order (MOTO) transactions.

The card scheme sets the BIN range for virtual cards issued by your Issuer. Further usage restrictions are applied when setting up card Usage Groups for your cards in the Thredd system.

Q. When I convert a virtual card to a physical card, can the virtual card still be used?

The cardholder can continue to use the virtual card until the physical card has been activated. Once the physical card is activated, the virtual card cannot be used.

Q. Can the cardholder view the transaction history on the virtual card after it has been converted to a physical card?

Yes, both physical and virtual cards share the same card record, so card and transaction enquiries will return transaction details.

Virtual Card Setup

Q. Can I add restrictions to how the Virtual Card can be used?

Yes, you can set up card Usage Groups, which define how and where the virtual card can be used. Card usage groups are linked to a card product or can be linked to a card using the Thredd Web Services API. See Set up your Virtual Card Usage Groups

Virtual Card Image Display

The FAQs below are relevant where Thredds generating the virtual card image.

Q. Why is the image text not displaying correctly?

The layout of the dynamic text elements that are overlayed on top of your background image is controlled by the settings you defined for each field: offset from top, offset from left, font size, font type, font colour, and field prefix text to display. See Using a Customised Image Design.

Consider adjusting the following:

- If the field text is too big and therefore running into the edge of the image or clashing with other fields, then adjust the font size.
- If fields are running into each other or clashing with background images, then adjust the field top and left offset settings. We recommend you use the default Thredd offsets.
- If field text is difficult to read, consider changing the font type and font colour.

Q. The text displays fine, but why is the background image blurred?

Please ensure the background image you supply meets the minimum Thredd requirements. See Background Image Specifications. Suggestions for improving the image quality:

- Provide a background image with a higher resolution (e.g., 96dpi).
- Use the recommended Thredd image size: 324 pixels width x 205 pixels height
- Provide your image in JPEG format. While Thredd can convert from other formats such as BMP, this conversion can result in loss of image resolution

Q. For a masked PAN, which digits of the PAN are masked?

If you are not PCI compliant, then Thredd returns the masked PAN in the response to a create card request. A full PAN consists of 16 digits. Thredd displays the first 6 digits and the last 4 digits. The middle 6 digits are masked. See the example below:

```
123456******7891
```

Where: ****** is the masked 6 digits.

Virtual Cards and Other Thredd Digital Products

The FAQs below provide details of other Thredd products, which shouldn't be confused with virtual cards.

Q. What is a Master Virtual Card (MVC)? Is it a type of Virtual Card?

No, the Master Virtual Card (MVC) is not a virtual card that is provided to a cardholder. The MVC is a card record that is restricted to loading or unloading and to card-to-card transfer. Physical card production, e-commerce transactions and ATM use are not permitted.

Q. What's the difference between a Virtual Card and a Mobile wallet device PAN?

A Thredd virtual card and a mobile wallet device PAN (DPAN) both provide a method of digital payment. The Thredd virtual card is a card in its own right, while the DPAN is a payment token, generated by the card scheme, that is linked to a card and is bound to a device for use on that device.

The Thredd virtual card is restricted to online/MOTO usage, while a DPAN/token can be used anywhere. For more information, see the Tokenisation Service Guide.

Q. Is it possible to set up Tokenisation on a Virtual Card?

Yes, provided that you have set up your card BIN range at Scheme level to support dual usage and set up your card product to create virtual cards with the intention to convert them to physical cards.

The virtual card can be tokenised and bound to a mobile device or other token device in the same way as with a normal physical card. Once the token is activated, make sure your card velocity and usage groups are updated to enable usage at the locations and merchants your require.

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.

Automated Fuel Dispenser (AFD)

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

B

BIN

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

C

Card Scheme

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

Cardholder

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

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.

CVV

The Card Verification Value (CVV) on a credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. Cardholder's are typically required to enter the CVV during any online or cardholder not present transactions. CVV numbers are also known as CSC numbers (Card Security Code), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to guess.

CVV2

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

numbers are also known as CSC numbers (Card Security Code), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to guess.

E

EMV

EMV originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit chips, in addition to magnetic stripes for backward compatibility.

External Host

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

F

Fee Groups

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

H

Hanging Filter

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

I

Incremental Authorisation

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

Issuer

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

M

MeaWallet service

Service provider integrated with Thredd who provides push provisioning and cardholder services where sensitive card details such as PAN need to be stored and processed. This service is suitable for Thredd customers who are not PCI compliant and want a means to process details such as PAN on behalf of their cardholders.

Merchant

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

Merchant Category Code (MCC)

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

MIP

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

O

Offline Transaction

This is often used in scenarios where the merchant terminal is not required to request authorisation from the card issuer (for example for certain low risk, small value transactions used by airlines and transport networks). The card CHIP EMV determines if the offline

transaction is permitted; if not supported, the terminal declines the transaction. Note: Since the balance on the card balance is not authorised in real-time, there is a risk that the card may not have the amount required to cover the transaction.

One Time Password (OTP)

A password that is valid for a single use only. During an authentication session (where the authentication type is with OTP SMS or OTP Email), the cardholder must enter this OTP to authenticate.

P

PAN

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

Partial Amount Approval

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

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

Product Setup Form (PSF)

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.

S

Second Payment Services Directive (PSD2)

PSD2 is a European regulation for electronic payment services. It seeks to make payments more secure, boost innovation and help banking services adapt to new technologies. The regulations are available here: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

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 Apex system. 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.

T

Thredd Public Token

A unique 9-digit number assigned by Thredd, to represent the linked card. The public token can be used instead of the PAN for all web services API requests.

TLS

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

Triple DES

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

V

Validation

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

VROL System

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

Document History

Version	Date	Description	Revised by
1.4	12/10/2023	Updated Smart Client images and Card Example images in Virtual Card Image Design	MW
	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
1.3	01/12/2022	Updated the Copyright Statement	MW
1.2	12/08/2022	New guide layout and HTML version now available	PC
1.1	28/09/2021	Thredd Office address updates. Revised instructions for virtual to physical conversations. New FAQ on support for tokenisation	WS
1.0	12/08/2021	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: +442037409682

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.