



3D Secure Guide (Apata)

Version: 1.1

22 March 2024

Publication number: 3DS-APATA-1.1-3/22/2024

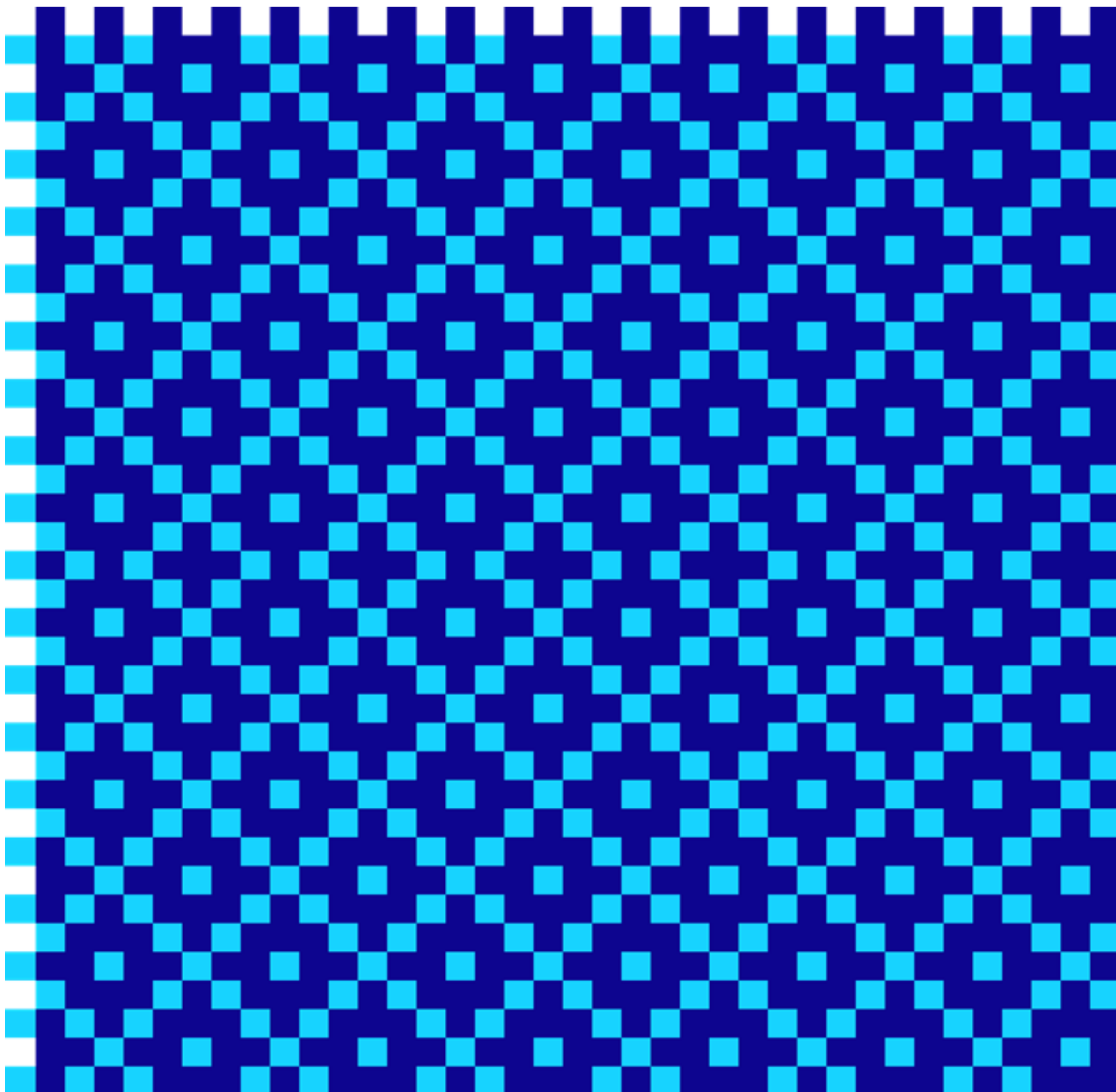
For the latest technical documentation, see the [Documentation Portal](#).

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

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

© Thredd 2024





Copyright

© Thredd 2024

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

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

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

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



About This Document

This document describes the 3D Secure (Apata) service and how to integrate this service with Thredd.

Note: The information provided in this document refers to integrating with Apata as your 3D Secure provider. If you are integrating with Cardinal, refer to the [Cardinal guide](#).

Target Audience

This document is intended for Thredd clients (Program Managers) who are interested in integrating the 3D Secure service into their program. It is aimed at Business Analysts, and Project Leaders and developer users with an understanding of how to implement SOAP web services and REST-based API to connect to Thredd.

What’s Changed?

If you want to find out what's changed since the previous release, see the [Document History](#).

How to use this Guide

If you are new to the 3D Secure service and want to understand how it works, see the [Introduction](#).
To find out about the steps involved in implementing the 3D Secure project, including details of the 3D Secure service configuration options, see [Steps in a 3D Secure Project](#). For information on the 3D Secure API, see [Using the 3D Secure 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 SOAP-based Web Services and includes a section on 3D Secure web services.
Cards API Website	Provides details of the Thredd REST-based Cards API and includes a section on 3D Secure API.
EHI Guide	Provides details of the Thredd External Host Interface (EHI).
Smart Client Guide	Describes how to use the Thredd Smart Client to manage your account.

Other Guides

Refer to the table below for other relevant documents.

Document	Description
EMV® 3-D Secure Protocol and Core Functions Specification	You can download the latest 3D Secure protocol specification from the EMVCo website . This document provides the latest 3D Secure specifications for anyone implementing a 3D Secure project and includes information not covered in the Thredd guides, such as authentication message flows between issuer (BIN sponsor), ACS provider and merchant (PReq, PRes, AReq, ARes), and specific internal message fields that may be passed or validated (e.g., CAVV/ AAV).
Mastercard Identity Check Program Guide	Guide providing details of the Mastercard 3D Secure implementation. Provides details on internal Mastercard message fields (such as acsInfoInd and RequestorAppUrl). Please check on Mastercard Connect for the latest version of this guide, which is available to Issuers (BIN sponsors).



Document	Description
Visa EMV 3D Secure 3DS User Experience Guidelines	Provides information on the Visa 3D Secure service. See https://developer.visa.com/pages/visa-3d-secure .



1 Introduction

3D Secure (Three Domain Structure), also known as a cardholder authentication, is a security protocol that helps to prevent fraud in online (e-commerce) credit and debit card transactions. This security feature is supported by Visa and Mastercard and is branded as Verified by Visa / Visa Secure and Mastercard SecureCode / Mastercard Identity Check respectively.

Thredd's 3D Secure partner is Apata. You can implement this service through Thredd to ensure that your cardholders are successfully enrolled and authenticated using 3D Secure.

1.1 About Apata

Apata is an Access Control Server (ACS) provider.

The ACS is responsible for verifying the identity of the cardholder during a 3D Secure transaction. When a merchant initiates a 3D Secure transaction, the card scheme (Mastercard or Visa) sends the transaction details to the ACS of the card issuer (BIN sponsor). The ACS then interacts with the cardholder, usually through a pop-up window, to request additional authentication information, such as a one-time passcode or biometric authentication. If the authentication is successful, the ACS (Apata) sends a response back to the merchant indicating that the transaction is successfully authenticated and can proceed to authorisation.

You can configure the rules which Apata use to make a frictionless authentication approval decision, as well as the challenge rules that trigger a request for further authentication and rules that result in rejection of a transaction.

Note: The information provided in this document refers to integrating with Apata as your 3D Secure provider. If you are integrating with Cardinal, refer to the [Cardinal guide](#).

1.2 Apata Features

- Authentication flows for One time Passcode (OTP), Knowledge Based Authentication (KBA), Biometric/Out of Band (OOB) authentication, Transaction History and Behavioural biometrics.
- Acquirer transaction risk analysis
- User Portal
- Dynamic linking (matching authentication to authorisation)
- Public token support to identify transaction
- Merchant trust listing – cardholder opt-in to be trusted by this merchant, so not to be challenged by this merchant
- Self-debugging
- Experimentation (A/B testing flows)

1.3 Authentication Methods

Thredd supports a number of authentication methods that can be used to further verify the cardholder during an online (e-commerce) card transaction made from a merchant’s website:

Authentication Method	Description
Risk based authentication (RBA)	Risk profiles define how a transaction is evaluated once it reaches Apata. These are a combination of rules which determine the processing action (challenge, accept or reject) which should be taken based on the individual characteristics of a transaction.
OTP SMS authentication	Apata generates a single-use One-Time Passcode (OTP). Thredd sends the OTP in a SMS text message to the cardholder’s mobile phone number and the cardholder enters the OTP in the 3D Secure screen to authenticate the e-commerce transaction.
OTP Email authentication	Apata generates a single-use One-Time Passcode (OTP). Apata sends the OTP in an email message to the cardholder’s email address and the cardholder enters the OTP in the 3D Secure screen to authenticate the e-commerce transaction.



Authentication Method	Description
Biometric authentication	Apata sends a Biometric authentication request to Thredd and we forward this to your systems. Your cardholders will need to verify themselves with a biometric identifier (e.g., fingerprint, voiceprint, facial scan) within an authenticator app, for example your organisation's mobile banking application. Your application manages the Biometric verification and returns a response to Thredd.
Out of Band (OOB) authentication	Apata sends an authentication request to Thredd and we forward this to your systems. You need to verify the cardholder using your cardholder In-App smart phone application, for example by asking them to enter a username and password. Your cardholder application manages the verification and returns a response to Thredd.
Knowledge Based Authentication (KBA)	You enrol the cardholder in KBA using the 3D Secure service and provide the security question ID(s) and answer pair(s). Thredd provides Apata with the security question and answer to use for KBA. During the e-commerce authentication session, Apata asks the cardholder to answer the security question and validates the answers. KBA is typically combined with OTP to satisfy the two-factor authentication requirement for PSD2 SCA compliance.
Transaction history	Another type of Knowledge based authentication. If the card is configured to use transaction history, the cardholder is asked to identify a recent payment they made with their card. (Transaction history details are taken from previous transactions where 3D Secure authentication was requested.)

You can add multiple authentication types to each card that you enrol in the 3D Secure service.

Note: Strong Customer Authentication (SCA) rules under the Second Payment Services Directive (PSD2) in the EU/EEA and similar regulations may not permit certain authentications on their own (e.g., OTP SMS, OTP Email or KBA). See below.

Strong Customer Authentication (SCA)

Strong Customer Authentication (SCA) requires a combination of two forms of customer identification at checkout. Examples include:

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

If you are supporting 3D Secure on your cards, you must be able to offer SCA to your cardholders; this is required to comply with the Second Payment Services Directive (PSD2) relating to Strong Customer Authentication (SCA). These regulations apply to cards issued in the European Economic Area (EEA) and the United Kingdom.



2 Parties Involved in 3D Secure

During the 3D secure authentication session, several parties are involved in exchanging data. See the example below:

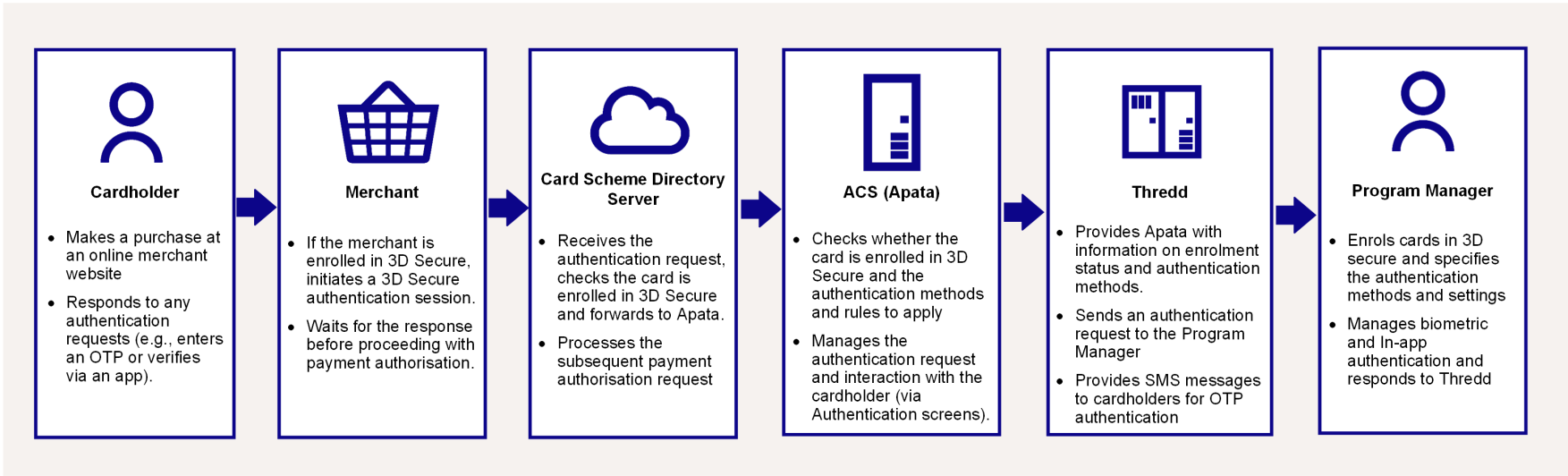


Figure 1: Flowchart of Parties involved 3D Secure

Cardholder

The cardholder's card must be enrolled with the relevant credentials (i.e., mobile phone number, email address, KBA questions and answers) to use the required authentication method. Thredd provides an option to auto-enrol the cards in your program, see [Card Auto Enrolment](#). Alternatively, you can do this using either our SOAP-based Thredd API or our REST-based Cards API. See [Using the Card Enrolment API](#).

During the online checkout process, if the transaction does not meet the rules you have configured for frictionless authentication, the cardholder is presented with 3D Secure authentication screens¹. They authenticate based on one of the selected options set up for their card, for example, by entering a one-time password (OTP).

Merchant

The merchant must support 3D Secure for an authentication session to occur. The cardholder visits the merchant's website, and at the checkout stage, when payment is requested, in the background the merchant's systems initiate a 3D Secure session.

Most merchants use a Payment Gateway, provided by an online payment service provider, to support their payment process. The Payment Gateway handles the connection to the Card Scheme and the 3D Secure authentication request.

Card Scheme

Visa or Mastercard receive all payment authentication requests from merchants. The card schemes maintain Directory Servers, with details of the card BIN ranges and the authentication services they are enrolled to. They check the BIN range to determine whether the card is enrolled in the 3D Secure service and the Access Control Server (ACS) used by the issuer (BIN sponsor). The authentication request is then routed to the ACS to complete the authentication.

Apata

Apata is Thredd's 3D Secure partner. Apata receives 3D Secure authentication requests from the Card Schemes and check their database for the 3D Secure rules you have configured in the Apata Portal for cards in this BIN range².

If 3D Secure authentication is required, they send a request to Thredd for the types of authentication supported by the card. They provide 3D Secure Authentication screens to the cardholder. See [Configuration of 3D Secure Screens](#).

For OTP email, Apata sends the OTP to the cardholder's email address.

¹For transactions considered low risk, such as for smaller amounts, exemption rules can be configured to accept without additional authentication.

²Apata provides an online Admin Portal, where you can set up rules resulting in Accept, Reject or Challenge outcomes, based on parameters such as amount, merchant category, transaction type and country. For details, see [Appendix 1: Apata 3D Secure Rules](#).



Thredd

Thredd manages the communication with Apata and the Program Manager. During an authentication session, Thredd sends Apata a list of the authentication types for which the card is registered³. Apata will use these details to present the available authentication methods to the cardholder in the 3DS pop up screen.

For OTP SMS, Thredd receives the OTP from Apata and sends the OTP to the cardholder's mobile phone. See [Appendix 2: OTP Message Templates](#).

Program Manager

As a Program Manager using Thredd as your Processor, you will need to sign up for the 3D Secure Service with Thredd and set up your 3D Secure rules on the Apata Portal. See [Steps in a 3D Secure Project](#).

During the implementation phase, you can customise the 3D Secure Authentication screens displayed to cardholders during the authentication process (i.e., specify the logo and text to be displayed on these screens).

You can use either the Thredd Thredd API or Cards API to enrol your cards in the 3D Secure service and request to register in Thredd the authentication types supported by the card. See [Using the Card Enrolment API](#). An option is also available for auto-enrolment. See [Card Auto Enrolment](#).

³Based on the authentication types you added to the card or, if none are added, on the default option set up in the system for your card product.



3 Cardholder Authentication Flows

This section provides a description of the message flow between parties in a 3D Secure authentication session.

3.1 Authentication using OTP SMS

Figure 2 provides an overview of the cardholder authentication process during a transaction, using the Apata 3D secure service with One Time Password (OTP) authentication.

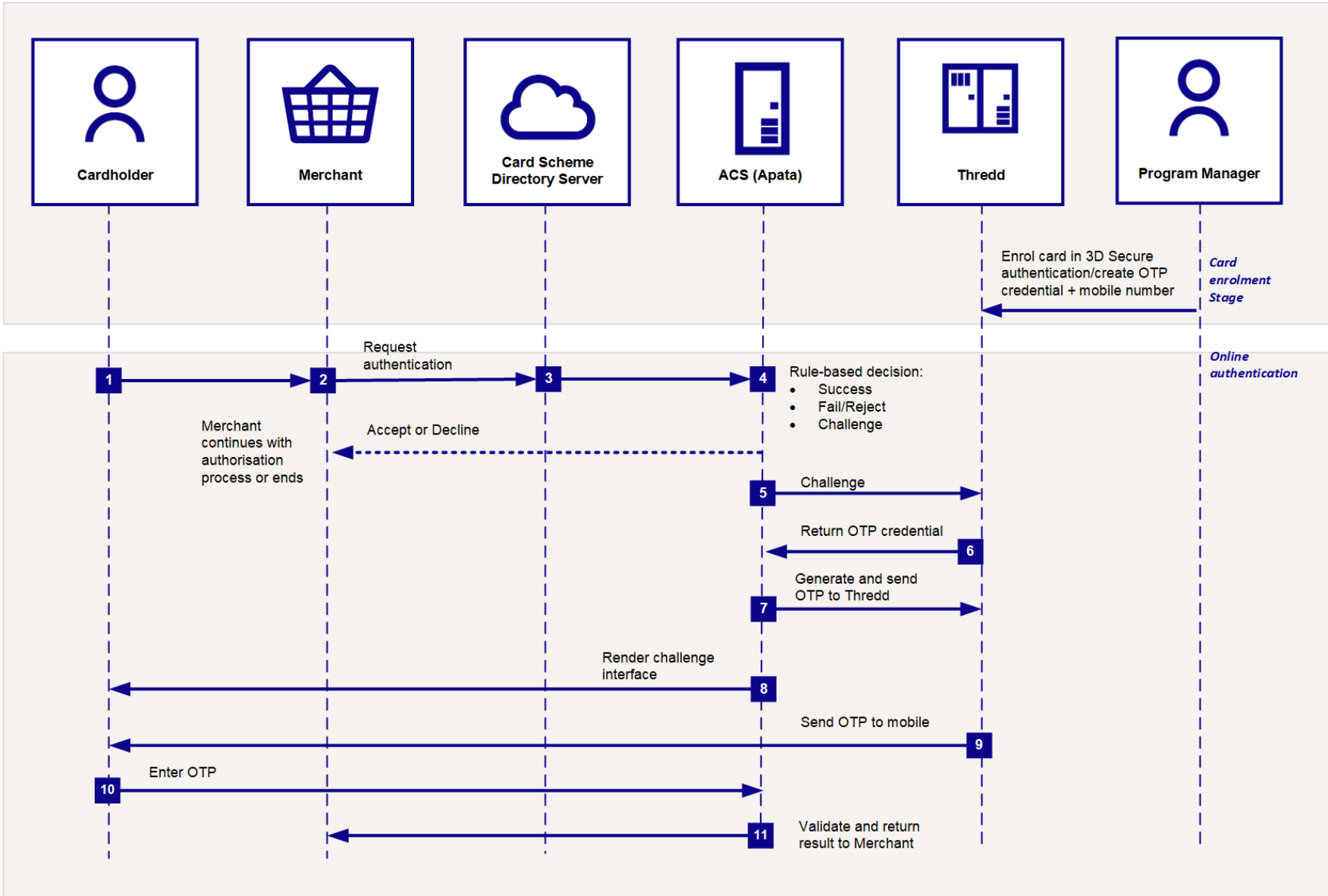


Figure 2: 3D Secure Authentication Process - Using 3D Secure and OTP

Prior to using OTP SMS, you need to set up OTP SMS as an authentication method on the card, and add a valid mobile phone number to use for completing the authentication. See [Using the Card Enrolment API](#).

1. The cardholder uses their card at a merchant website.
2. If the merchant is enrolled in 3D Secure, they send a request for authentication to the Card Scheme (Mastercard/Visa).
3. The Card Scheme looks up the 3D Secure service provider for your card programme and sends the authentication request to Apata.
4. Apata checks to confirm the card BIN range is enabled for 3D Secure. Based on the rules you set up in Apata for your card program (see [Appendix 1: Apata 3D Secure Rules](#)), the outcome is Success, Fail/Reject or Challenge, with the next steps as described in the following table:

Outcome	What happens next?
Success	An approval response is returned to the merchant. The merchant can continue with the authorisation request.
Fail or Reject	An <i>authentication failure</i> or <i>reject</i> response is returned to the merchant. They can decide whether to continue to request transaction authorisation or ask the cardholder to provide an alternative payment method.
Challenge	3D Secure authentication is required, and Challenge screens are shown to the cardholder. See Steps for a



Outcome	What happens next?
	Challenge outcome below.

Steps for a Challenge outcome

- 5. Apata connects to Thredd in real-time to check the types of authentication the card is registered for (e.g., Biometric, OTP SMS or KBA).
- 6. Thredd replies to Apata with OTP SMS as the type of authentication registered on the card (based on what you registered the card for using the Thredd API/ Cards API and your product configuration at Thredd).
- 7. Apata generates the OTP and sends it to Thredd in real-time.
- 8. Apata displays the OTP entry pop-up screens to the cardholder on the merchant website or App.
- 9. Thredd sends the OTP to the mobile number Thredd has on record for the cardholder, via SMS.
- 10. The cardholder enters the OTP in the 3DS pop up screen on the merchant's website or App to complete their authentication.
- 11. Apata validates the OTP and sends the validation result back to the merchant.



3.2 Authentication using Biometrics or In-App OOB (Out of Band)

Figure 3 provides an overview of the cardholder authentication process during an e-commerce transaction, using the 3D Secure service with Biometric or OOB authentication.

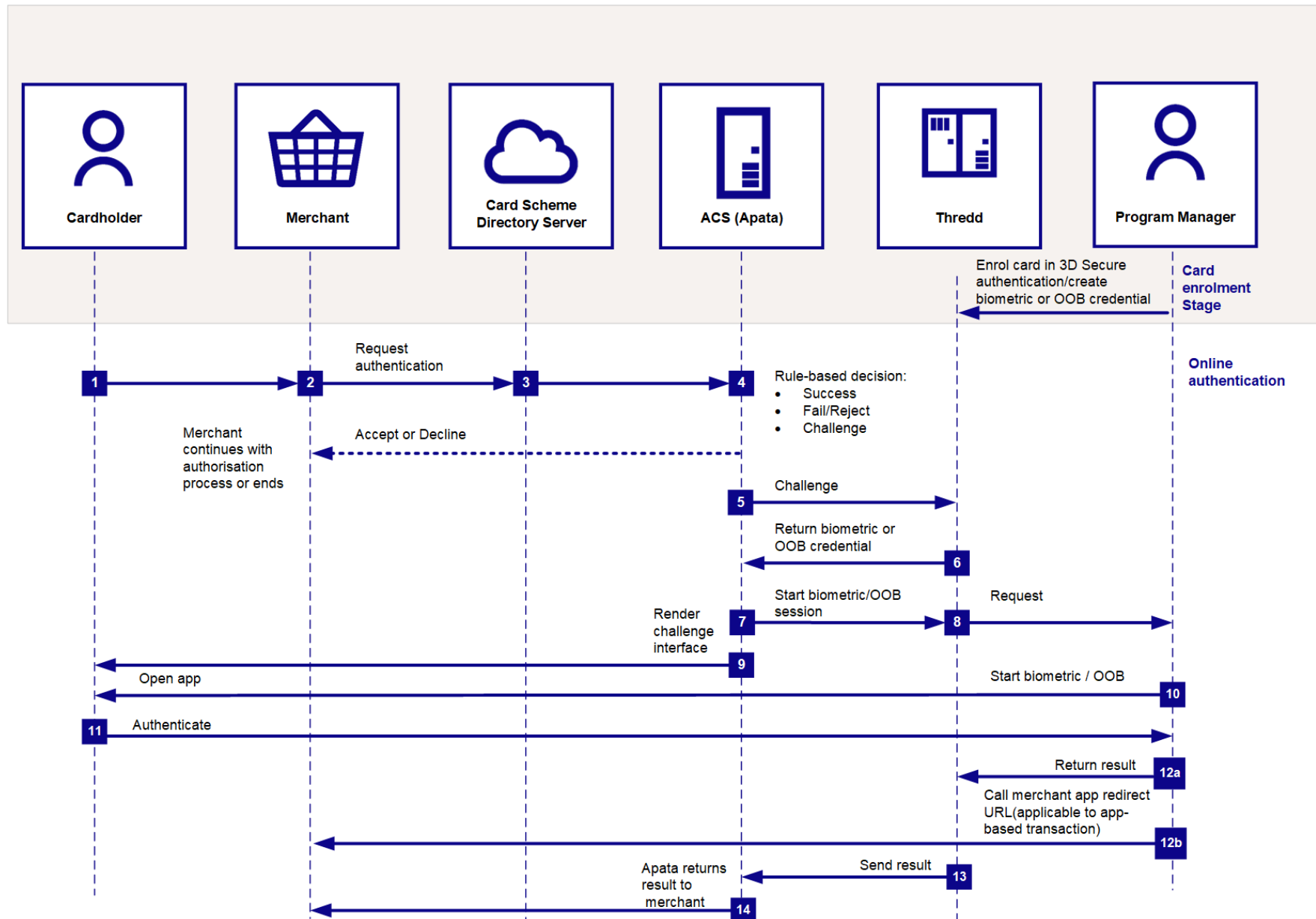


Figure 3: 3D Secure Authentication Process - Using 3D Secure and Biometrics or Out of Band (OOB)

Authentication via Biometric or In-App OOB

Prior to using biometric authentication, you need to set up the BIOMETRIC or OUTOFBANDOTHER credential on the card. See [Using the Card Enrolment API](#).

Steps 1-5 are as described previously (see [Authentication using OTP SMS](#)).

- Thredd replies to Apata with Biometric as the type of authentication (based on what you registered the card for using the API and on the default types set up for your cards).
- Apata calls Thredd to start Biometric or Out of Band authentication.
- Thredd sends a message to your 3D Secure service endpoint, to start authenticating using Biometrics.
- Apata shows the Biometric screens to the cardholder. This informs the cardholder that they will need to authenticate using your smart device app.
- Your organisation sends a push notification to your cardholder and routes them to your bank app.
- The cardholder authenticates from the bank app (e.g., by scanning their fingerprint or face using their smart device).
- You perform the following:
 - When the authentication session is complete, then you must return the result of the Biometric authentication to Thredd, using the [DelegateSCAValidation API](#).
 - If you have received the merchant app redirect URL in the [DelegateSCANotification API](#) from Thredd, you can call this URL. The URL takes the customer from the banking app back to the merchant app.



13. Thredd waits for your validate response ([DelegateSCAValidation API](#)) and sends the results back to Apata.
14. Apata returns the results to the merchant.



3.3 Authentication using KBA

Note: KBA is usually used in conjunction with OTP SMS or OTP Email (as part of two factor authentication requirements under the PSD2 rules of the European Economic Area).

Figure 4 provides an overview of the cardholder authentication process during a transaction, using the 3D Secure service with Knowledge Based Authentication (KBA).

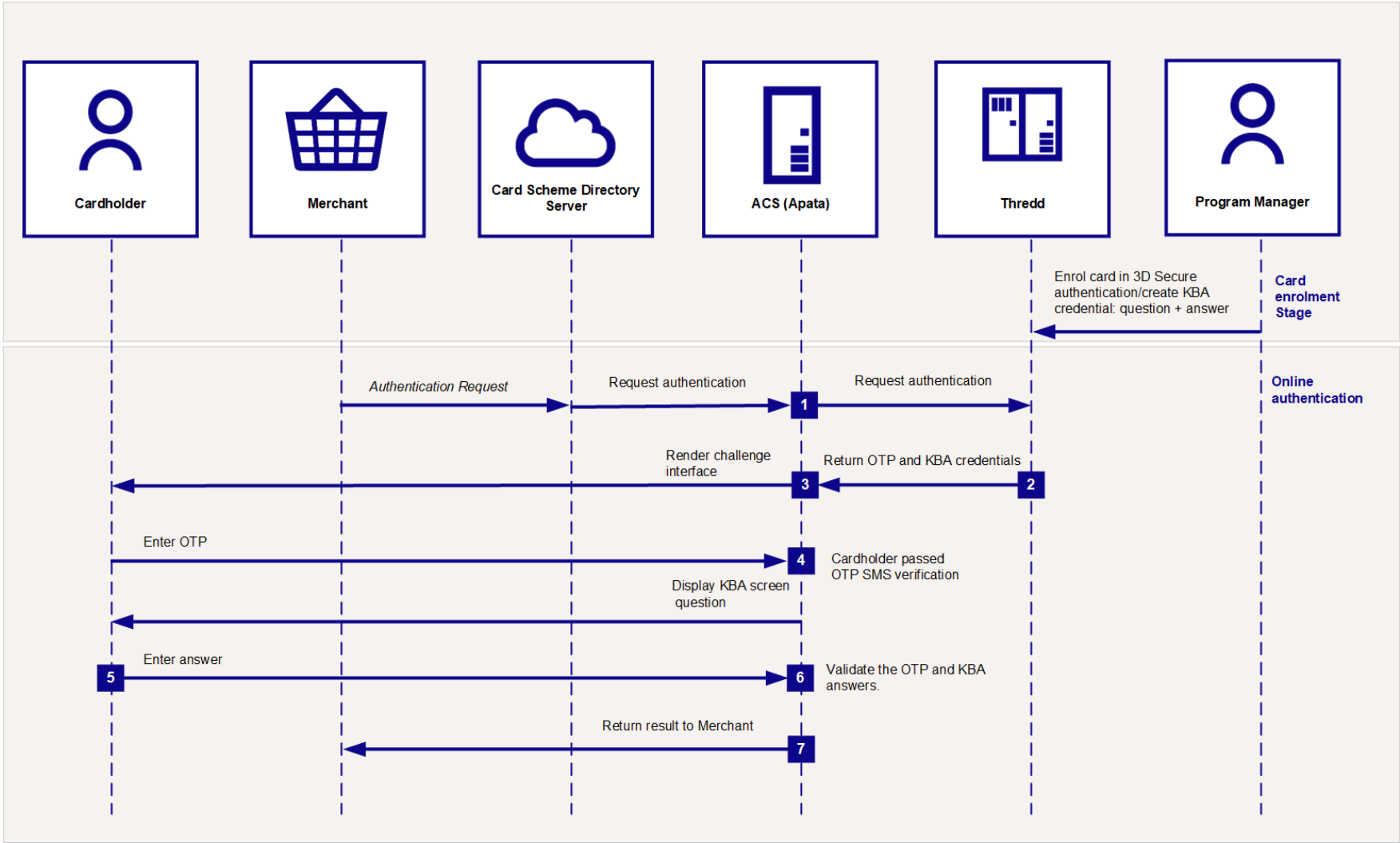


Figure 4: 3D Secure Authentication Process - Using 3D Secure and KBA

Authentication via KBA

Prior to using KBA, you need to set up the KBA credential, including the question and answer pairs to be used for the card during a KBA authentication session. See [Using the Card Enrolment API](#).

If using multiple questions, you must enrol all cards with a sufficient number of KBA questions to challenge the transaction. This should be the sum of the number of correct and incorrect answers permitted.

An online authentication session using KBA is typically combined with OTP SMS. The KBA authentication follows directly after successful OTP SMS authentication. See [Authentication using OTP](#).

1. Apata connects to Thredd in real-time to query the types of authentication the card is registered for (e.g., OTP SMS and KBA).
2. Thredd replies with the OTP and KBA challenge profile configured for your product.
3. Apata follows the process for OTP SMS, presenting the OTP screen to the customer, who enters the OTP which Thredd sends to their mobile phone via SMS.
4. Following OTP authentication, Apata presents an additional screen to the cardholder, asking them to answer the security question(s) set up for their card.
5. The cardholder enters their answer(s).
6. Apata validates the OTP and KBA answers.
7. Apata confirms whether authentication has been successful or not.



3.4 What happens after successful authentication?

Once the cardholder is authenticated, the merchant can proceed with requesting authorisation for the transaction. (The merchant acquirer includes the 3D Secure value they receive from Apata within the transaction: [UCAF](#) field (For Mastercard) and the [CAVV](#) field 126.9 for (Visa).)

If requested, Thredd will validate the Accountholder Authentication Value (AAV) for Mastercard programmes or the Cardholder Authentication Verification Value (CAVV) for Visa programmes. If you need Thredd to validate the CAVV or AAV, then please specify this when **Completing your 3DS Product Setup Form (PSF)** by selecting YES in the [Do you require Thredd to validate the AAV/CAVV?](#) field.

Depending on your External Host Interface (EHI) mode, Thredd approves/declines the transaction or sends details to your EHI endpoint to approve or decline.

You can view details of your 3D Secure transactions in the Apata Portal. See [Searching for Transactions](#).



4 Steps in a 3D Secure Project

This section describes the steps in setting up a 3D Secure service.

4.1 Overview of Steps

A project starts once we have received your requirements. A typical project takes 4-5 weeks, but you should plan for additional time to allow for contingencies.

Figure 5 below provides an overview of the steps in a typical project.

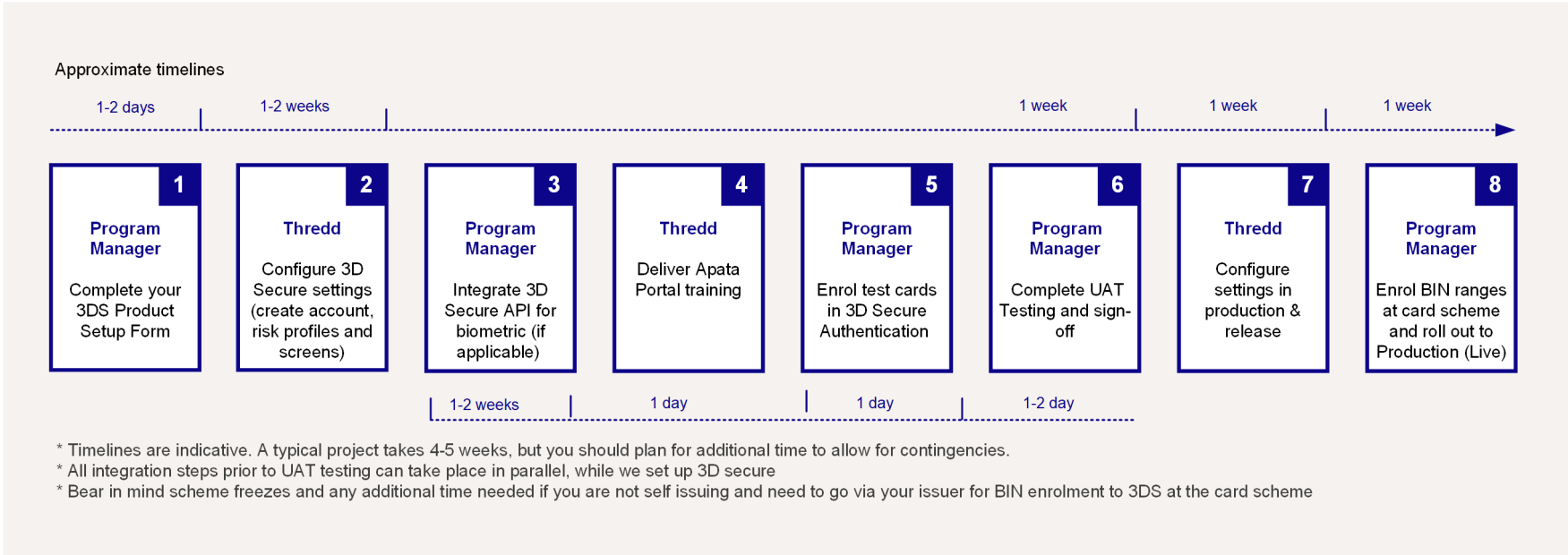


Figure 5: Steps in a 3D Secure Project

Refer to the table below.

#	Step/Action	Approximate time needed
1	Complete your 3DS Product Setup Form (PSF) Your Thredd 3DS project manager can help you complete this form, which provides details of your 3D Secure service configuration at Thredd. To support Biometric or Out of Band, you will need to provide the endpoint for receiving the DelegateSCANotification API call. You will need to supply one endpoint for the UAT environment and another endpoint for the Production/Live environment.	Allow 1-2 days.
2	Thredd configures your 3D Secure account settings Thredd configures your challenge methods, challenge screens, card programs and setup all other requirements in the UAT environment. Sign off by the Program Manager is required after the configuration. Your issuer (BIN sponsor) may also request to review. A configuration review call will be arranged to walk through your Apata 3D Secure configuration for sign off. You will also need to provide your brand logo in svg (scalable vector graphics) image format if required, which will be displayed on the challenge screens.	Allow 1-2 weeks to configure your service.
3	Integrate the 3D Secure API for Biometric/ Out of Band authentication (if applicable) You will need to: - Permit Thredd to access your systems for sending Biometric/OOB calls to your organisation in UAT and Production. For details of the allowed Thredd IP addresses, see Authorising Thredd IP Addresses. - Provide Thredd with your DelegateSCANotification endpoints for UAT and Production, and a list of IP addresses for using the Biometric/OOB services. See more details on Setting up Firewall Permissions. Thredd will set up your oAuth access and provide you with credentials for the Thredd oAuth server. See more details on Using the oAuth Server .	Allow 1-2 weeks. This step can happen in parallel while Thredd set up your account.



#	Step/Action	Approximate time needed
4	Thredd provide training Thredd provide your users with training on the Apata Portal.	Allow 1 day. (Booking at least 2 weeks in advance is suggested.)
5	Enrol your test cards in 3D Secure Thredd activates a single card product in the UAT environment, so you can enrol a few cards for UAT testing. You can enrol your cards and specify the types of authentication: if using Web Services then use the 3D Secure Web service (Ws_AddUpDelCredentials); if using Cards API, then use the Create 3DS Credentials API.	It takes 1-2 hours for Thredd to activate the card product. Allow 1-2 hours to enrol cards in the Thredd UAT environment and run authentication tests. See step 6. Then repeat in Pilot production. See step 7.
6	Complete UAT testing Once 3D secure is configured, Thredd release the project into the UAT environment for you to test and sign off. Note: You are required to provide sign-off by email. A default challenge risk profile will be created for you, with any exemptions specified in the PSF. You will be able to add conditional rules as required. You can then start testing in UAT using the Apata merchant simulator.	It will take you 1-3 hours to set up your rules (e.g., for Success, Fail/Reject or Challenge outcomes) and link your BIN range(s). Allow a week to complete UAT testing and provide sign-off.
7	Complete pilot Production testing Thredd sets up your 3D Secure configuration in the production environment: - Thredd activates a single card product in the Production environment, so you can enrol a few cards for pilot testing. - If you are not self-issuing, your issuer (BIN sponsor) must enrol your pilot cards to be enrolled at the Scheme (by submitting a card range file; Thredd will provide you with the Apata ACS URLs⁴)	The full pilot testing phase takes around 1-2 weeks: - Allow a week for Thredd and Apata to release your configuration to the Production environment for Pilot testing. - Mastercard takes around 3 days to set up pilot cards. - Visa takes 1-2 weeks to set up pilot cards. Note: Providing the pilot cards in advance can speed up the process. - Allow 1-2 days for enrolling the pilot cards (using the web service / cards API) and for pilot card testing.
8	Roll out to Production (Live) Notify Thredd once you have completed your pilot testing. Thredd configures your card products for 3D Secure. You need to enrol all your live cards in 3D Secure and register them for your supported authentication types (e.g., Biometric or OTP SMS). Thredd also offer an auto-enrolment option. See Card Auto Enrolment . Notify Thredd that you have completed enrolment. If you are not self-issuing, your issuer (BIN sponsor) must contact the Card Scheme (payment network) to enrol the rest of your card ranges.	Allow a week to 10 days to complete the roll-out at the Card Scheme (payment network) and to enrol your cards.

Each of these steps is broken down into further detail below.

⁴The URL is unique per Program Manager and is used by the Scheme to direct the transaction to the Apata system.



5 Completing your 3DS Product Setup Form

The Apata 3D Secure service is provided through Thredd, so you do not need to have a direct relationship with Apata. Thredd will complete your 3D Secure setup on Apata. This includes configuring your challenge methods, challenge interface, challenger profiles and users.

Before we can start a project with Apata, you will need to complete the Thredd 3DS Product Setup Form (PSF), which specifies your 3D Secure requirements. This form consists of the following tabs:

- [Cover](#)
- [Client Information](#)
- [BIN ranges by card program](#)
- [Challenge screens](#)
- [Apata Portal access](#)

Each of these tabs is described in further detail in this section.

5.1 Cover tab

This section of the form should be completed and signed by the nominated contact from your organisation. This should be done after all other details on the form have been completed and discussed with your Thredd 3D secure Implementation manager. The information in the form will be used to setup your programme in Thredd's processing system.



5.2 Client Information tab

Complete the following sections on this tab:

5.2.1 Client Information

Field	Description
Client name	Your company’s name. The name provided here will be displayed on the Apata portal as the Financial institution name.
Country of residence	Your company’s country of residence.
Scheme	Card scheme (e.g., Visa or Mastercard).
Issuer name	The name of your issuer (BIN sponsor).
Visa BID	Your issuer’s (BIN sponsor) Visa Business Identifier (BID).
Mastercard Primary ICA Number	Your issuer’s (BIN sponsor) primary ICA, as registered with Mastercard.
Mastercard Company Name (Issuer)	Your issuer’s (BIN sponsor) Company Name, as registered with Mastercard.
Mastercard Company ID (CID)	Your issuer’s (BIN sponsor) Company ID, as registered with Mastercard.
Thredd Program Manager ID	Your Thredd Program ID or code. Assigned by Thredd.
UAT readiness date	Date when you plan to be ready to test 3D Secure in the UAT environment.
Planned Go Live date	Date when you plan to launch 3D Secure for your card programme. Note: Please check with your Implementation Manager to confirm that this date is feasible. For steps and indicative time scales to launch a 3D Secure service, see Steps in a 3D Secure Biometric/In-app Project.
Do you require Thredd to validate the AAV/CAVV?	The AAV/CAVV is a cryptographic value which is included in the authorisation message request from the Merchant⁵. It indicates that the 3D secure authentication session was successful. You can request that either Thredd or the Card Scheme (Mastercard or Visa) validate this value. Card Scheme validation is typically required if you want the card Scheme to provide Stand-In processing. If YES: Thredd will validate the AAV/CAVV. To set this up: • Mastercard – encryption keys must be exchanged between Thredd and Apata; No action is required from the Program Manager. • Visa – encryption keys must be exchanged between Thredd and Apata. Please ensure your Client Information Questionnaire (CIQ) has the correct settings (under the VisaSecure section > ABE1 > K01. Select “I”). If NO: • Mastercard – please ensure the BIN has been enrolled with the required validation set up at Mastercard (i.e. Mastercard On-Behalf of Services (OBS) AAV Verification Service).

⁵The ACS generates the CAVV/AAV for a successful 3D Secure session; if Stand-In processing is enabled at the Card Scheme (for low-risk transactions), then the Scheme can step in when ACS is down and generate this value.



Field	Description
	• Visa – please ensure your Client Information Questionnaire (CIQ) has the correct settings (under the VisaSecure section > ABE1 > K01. Select “F” or “V” as appropriate). Please request for Visa to generate the CAVV key and encrypt with Thredd ZCMK (BIN: 476370, ZCMK KCV: 1CB2C9). Share the CAVV key file securely with your Thredd Implementation Manager.
Type of webservice to be used for 3DS enrolment	API to use for card enrolment. Options include: • SOAP – using our traditional XML-based Thredd API. • REST – using our REST-based Cards API, supporting messages in JSON format. For more information, see Using the Card Enrolment API .
Thredd Environment under which Program Manager is set up	Environment options include: • PRD0 – Not currently in Cloud • PRD1 – Cloud Europe • PRD2 – Cloud Asia Pacific

For more details, refer to the instructions in the 3DS Product Setup Form (PSF).

5.2.2 Required authentication methods

OOB other	The cardholder receives an issuer-generated push notification to authenticate within the authenticator or mobile banking app.
OOB Biometrics	The cardholder receives an issuer-generated push notification to authenticate within the authenticator or mobile banking app using a biometric identifier; for example face ID or fingerprint.
OTP via Email	The cardholder receives a One-Time Passcode (OTP) via email.
OTP via SMS	The cardholder receives a One-Time Passcode (OTP) via SMS (text message).
KBA - Transaction history	Knowledge Based Authentication (KBA). The cardholder is presented with a Challenge screen asking them to identify a recent payment they made on the card.
KBA - custom question	Knowledge Based Authentication (KBA). The cardholder is presented with a Challenge screen asking them to provide the answer to a question they have previously supplied.
OTP via SMS + KBA	The cardholder is first requested to authenticate using OTP via SMS and then by KBA.
OTP via Email + KBA	The cardholder is first requested to authenticate using OTP via email and then by KBA.

5.2.3 Setup options

Field	Description
Default language	Default language to apply to all cardholder Challenge screens, configured at product level.
Other languages	List any additional languages you support. You will also need to specify which language to apply to each card product. Otherwise, the default language will be applied to all products. See Challenge Screens >



Field	Description
	Supported Languages .
Default authentication	Select the default authentication type to support all BINs or sub-BIN ranges. See the drop down on the 3D Secure PSF for all available options. This is used for the following purposes: a) to enable a card to be enrolled in this type; b) to use as the default type of authentication during a real-time authentication session with Apata; c) to support auto-enrolment.
Fallback authentication	Select the fallback authentication type to support all sub-BIN ranges. See the drop down on the 3D Secure PSF for all available options. This is used for two purposes: a) to enable a card to be enrolled in this type; b) to use as the fallback type of authentication during a real-time authentication session with Apata, if the default type cannot be used for any reason.
Enable SMS OTP auto enrolment	Options are: <i>NO</i> – All cards must be enrolled for OTP SMS and the mobile number must be registered using either the Thredd API or the Cards API; see Using the Card Enrolment API. <i>YES - Initial Load</i> – Thredd enrol the existing cards to the OTP SMS credential. Thredd use the phone number linked to the card (i.e., the phone number supplied when the card was created or updated). <i>YES - Continuous</i> – Same as Initial load, however any future cards created will also have their phone numbers automatically registered for 3D Secure in the same way. Note: If using Continuous auto-enrolment, this may restrict your ability to unenroll cards that have been previously enrolled and which currently have a live status. For details, please speak to your 3DS Project Manager.
Enable Biometric auto enrolment	Options are: • NO – All cards must be enrolled using either the Thredd API or the Cards API. • YES – Initial Load only – This will create a biometric credential for all existing card holders which are sent to you for your reference. After initial load, auto-enrolment will be disabled and Program Manager will need to initiate the enrolment in the Thredd API or the Cards API for new card enrolments. • YES – Continuous – Same as Initial load, however auto-enrolment will remain enabled. New cards created will also have biometric credentials created in the same way. Your organisation will not need to send the Thredd API or the Cards API to enrol new cardholders.
Enable Email OTP auto enrolment	Options are: • NO – All email addresses for cards must be enrolled using either the Thredd API or the Cards API. • YES – Initial Load only – This will take email addresses which are added when card is created or card details are updated. After initial load, auto-enrolment will be disabled and Program Manager will need to initiate the Thredd API or the Cards API for new card enrolments. • YES – Continuous – Same as Initial load, however auto-enrolment will remain enabled. New cards created with email addresses will also be enrolled in the same way. Your organisation will not need to send the Thredd API or the Cards API to enrol new cardholders.
Time to complete authentication	Time to complete authentication in seconds. Countdown timer will be displayed in the Challenge screen. This is customisable up to 10 minutes (600 seconds) as per EMVCo requirements. The standard is 300 seconds (5 minutes). Note: If a fallback method is initiated, the timer will be restarted for the new authentication method.
DelegateSCANotification endpoint - UAT	For Out of Band and Biometric authentication, and to access the Thredd oAuth endpoint, in the UAT environment. Your endpoint for receiving the DelegateSCANotification API call to start an Out of Band or Biometric authentication.



Field	Description
	Please only supply one endpoint for the UAT environment. Please ensure that the provided endpoint is resolving to one or set of (maximum 5) Static IP addresses.
DelegateSCAValidation IP Address - UAT	For Out of Band and Biometric authentication, and to access the Thredd oAuth endpoint, in the UAT environment. Please provide your endpoint IP addresses for connection to the UAT environment. This should be no more than 5 static IP addresses.
DelegateSCANotification endpoint - Production	For Out of Band and Biometric authentication only in the Production environment. Your endpoint for receiving the DelegateSCANotification API call to start an Out of Band or Biometric authentication. Please only supply one endpoint for the UAT environment, and one endpoint for the Production environment. Please ensure that the provided endpoint is resolving to one or set of (maximum 5) Static IP addresses.
DelegateSCAValidation IP Address - Production	For Out of Band and Biometric authentication only in the Production environment. Please provide your endpoint IP addresses for connection to the Production environment. This should be no more than 5 static IP addresses.
KBA number of questions to answer	Total number of questions which the cardholder is required to answer.
KBA number of correct answers required	Total number of questions which the cardholder is required to answer correctly to successfully authenticate the transaction.
KBA number of incorrect answers permitted	Total number of questions that the cardholder may answer incorrectly before KBA is failed.
Number of retries allowed for OTP (Email/SMS)	The number of times that a cardholder can request for a new OTP to be resent via SMS or Email. The standard retry is 3, however this can be increased up to 5 retries.
Number of attempts allowed for OTP (Email/SMS)	The number of times that a cardholder can input the wrong value and still continue the process. After this the authorisation will decline and would need to be re-attempted.
Number of attempts allowed for KBA authentication	The number of times that a cardholder can enter the incorrect answer for each question. Note: We recommend you keep this at a minimum to prevent brute force attack.
SMS Sender ID	Text that appears as the sender of the SMS OTP (e.g., Program Manager name or Card brand). Can be up to 11 alphanumeric characters with no spaces. This Sender ID will be used for all SMS services. Please make sure to match this with SMS SENDER NAME in the core product Setup Form.
Email OTP sender	The "From" email address for the email OTP (i.e., from your organisation). Apata will complete the registration to send the OTP Email to your cardholders on your organisation's behalf. An authorisation email will be initiated to the email domain administrator. Authorisation will be required via the link in the email to complete the setup.
Dashboard currency	Currency to be applied to the dashboard in Apata. This will apply across your card programme.



5.2.4 OTP SMS Text Support

For OTP SMS messages (sent by Thredd to the cardholder’s phone number), the SMS message is dynamic, and you can specify the text and variables to use. See [Appendix 2: OTP Message Templates](#).

Please contact your Thredd 3DS project manager to ask for these SMS options to be configured.

Language is determined by checking the current value of the card’s [language](#) setting (if using Thredd API, see the [Web Services Guide >Create Card](#); if using our Cards API, see the [Cards API Website > Creating a Card](#)). Below is an example of the OTP SMS message, in French:



Figure 6: OTP SMS Message Example

A single SMS message can contain up to 140 bytes of information. The number of characters which can be included in a single SMS message depends on the type of characters the message contains. Depending on the recipient's mobile carrier and device, multiple messages may be displayed as a single message, or as a sequence of separate messages. If you are looking to avoid OTP message split into multiple parts then our recommendation is to keep it brief.

Thredd uses the default English text below if no customised message is configured (provided that the merchant shares all transactional information).

```
"{{OTP}}" is the One Time Passcode required for completing a purchase of {{CUR}} {{Amount}} at {{MerchantName}} with the last four digits of your card ending in {{CardNumber}}." Please use the One Time Passcode to complete the transaction.
```



5.3 BIN ranges by card program

Please select the required exemptions and risk features required for card program and associated BIN ranges.

Field	Description
BIN Range(s) Low	Include the 16 digit lower range of Bank Identification Numbers (BINs) without spaces (e.g., 4579123400000000).
BIN Range(s) High	Include the 16 digit upper range of Bank Identification Numbers (BINs) without spaces (e.g., 4579123499999999).
Card Program Name	A card program is a grouping of card ranges. Card Programs can be configured with unique Challenge Profiles and Risk Profiles. Provide the name to apply to each card program.
Trust list	Allows exemptions under the card program and associated card ranges if the merchant was previously whitelisted by the cardholder. • Mastercard prerequisites: when enrolling card/BIN ranges in Mastercard ISSM tool, “Whitelisting supported by ACS” under “Additional Service” must be turned on in order to support trust list exemptions via Apata. • Visa prerequisites: Issuers (BIN sponsors) need to be enabled for EMV 3DS 2.2 to use the indicators applicable to trusted beneficiaries. Issuers (BIN sponsors) are required to register their account ranges with Visa’s Directory Server to indicate their support for the trusted beneficiaries’ indicators. Support should be indicated by selecting YES in the Card Range File under field "TRUSTED LISTING SUPPORTED?".
PSD2 Low Value	Applies the low-value payment exemption under PSD2 if the following conditions are met: • Transaction value is less than €30.00 (or equivalent in local currency e.g., SEK, CZK, PLN). • The cumulative spend since the last challenge is less than €100.00. • The number of transactions since the last challenge is less than 5.
Secure Corporate Payment	Permits the secure corporate payment exemption to be used. Payment is made with an eligible commercial card through a dedicated secure corporate process that meets the security protocols set by the National Competent Authority (NCA).
Merchant Initiated Transaction	Identifies the merchant-initiated transactions where previous transaction from same merchant was authenticated with SCA.
Acquirer Exemption	Configure a list of merchants to either allow or disallow the exemption request. If these merchants request an exemption then accept/deny exemption based on presence on this list. If YES is selected, the configuration will accept all acquirer exemptions.
One Leg Transaction	Used for handling transactions where the issuer (BIN sponsor) and acquirer are located in the EEA, then SCA is enforced. If the issuer (BIN sponsor) or acquirer is not within the EEA, SCA is exempted as one leg out.
Recurring Payment	If the payment is recurring, then it does not require SCA and an exemption is applied. First recurring transaction must be SCA.

Note: All the above exemptions are applicable to EEA and UK issuers (BIN sponsors).



5.4 Challenge Screens

This section of the product setup form enables you to specify the text to appear on the Challenge screens, which will be presented to the cardholder during an authentication session. Please provide your brand logo to be displayed on the challenge screen if required. The scheme logo will also be displayed. Your logo must be in SVG (Scalable Vector Graphics) format.

Below is an example of the Challenge screens for OTP SMS. The text in the grey fields is customisable.

OTP SMS challenge screen

SMS OTP Introduction

Verify your payment using the code we sent to your phone number ending with:

Resend code text

Resend code

Transaction details

Your payment of {CUR} {amount} to {merchant name}

SMS OTP incorrect

The code you entered is incorrect. Please try again.

Your Logo

5:00

Verify your payment using the code we sent to your phone number ending with:

Submit code

Resend code

Your payment of £150.99 to Test Merchant

Cancel payment

3D Secure (3DS) helps prevent fraud when using payment cards online.

Figure 7: OTP SMS Challenge Screen Customisation

Note: If you do not wish to customise the text, we will use the default English text for your screens.

Other text

Other Challenge screen text is common to all Challenge screens and appears in the footer or lower part of the screen. See the example below.

Other screen text

Cancel button Label

Cancel Payment

3DS Information label

Learn More About 3DS

3DS Information text

3D Secure (3DS) Helps Prevent Fraud When Using Payment Cards Online.

Fallback SMS text

Receive SMS

Native challenge screen header

Purchase Authentication

Native OTP challenge information label

Enter your code

Figure 8: Other Challenge Screen Text Customisation

Use of variables

You can specify the use of the following variables on the Challenge screens:

Variable	Description
{merchant name}	The merchant name.



Variable	Description
{CUR}	The transaction currency.
{amount}	The transaction amount

The variable values are taken from the information supplied in the authentication request sent from the card scheme to Apata.

5.4.1 Supported Languages

If you support more than one language, make a copy of the Challenge screens tab per language and provide the translated text for each language.

Apata identifies the language in which to display the Authentication screens based on the language settings applied under your products. If you wish to support different languages across your products, please specify which language to use for which product.

The main body of the screen text has a limit of 350 characters. Headers and labels have a limit of 45 characters.



5.5 Apata Portal Access

This section of the form enables you to specify users who can access the Apata portal.

Access to the portal is made secure via 2-factor authentication using an Authenticator Application. See [Using the Apata Portal](#).

Please provide details of the users who need to access the Apata Portal.

Users- Please provide a list of users			
Email (username)	First name	Last name	User role
john.do@bank.com	John	Do	Analyst

Thredd sets up role-based access for your users. See [User Roles](#). All users receive an activation email, to sign in and activate their account.

Note: Any users Thredd set up with Admin level rights will be able to create access for additional users.

5.5.1 User Roles

The Portal provides role-based access to screens and functionality. The table below summarises the functionality and screens available to each user role.

Administrator	Analyst	Customer Service
<i>Suitable for your account administrator, who needs to configure 3D Secure rules and set up users in the system.</i>	<i>Suitable for business analysts who need to create reports and analyse transaction data.</i>	<i>Suitable for call centre staff who need to handle cardholder transaction queries.</i>
• Create users, view and edit existing users. • Create risk profile and rules, view and edit existing risk profiles. • View card programs and card ranges assigned to each card program. • View challenge methods and challenge interfaces (3DS screens). • Can execute test transactions. • View and search transactions for investigation purposes. • Create queries and generate reports, view and edit existing queries. • View audit logs.	• Create risk profile and rules, view and edit existing risk profiles. • View card programs and card ranges assigned to each card program. • View challenge methods and challenge interfaces (3DS screens). • View and search transactions for investigation purposes. • Create queries and generate reports, view and edit existing queries. • Can execute test transactions. • View audit logs.	• View and search transactions for investigation purposes. • View risk profile and rules.

5.5.2 Screen and Functionality Access

Your users are assigned access to the following screens, depending on their user role.

Screen	Description	Who can access?
Authentication > Risk Profiles	Risk profiles define how a transaction is evaluated once it reaches the Apata ACS, for example, whether to accept, reject or challenge a transaction, based on a set of risk rules.	Administrator and Analyst can manage. Customer Service can view.
Authentication > Challenge Methods	Defines the 3D Secure Challenge methods available to your card program.	Administrator and Analyst can view.



Screen	Description	Who can access?
Authentication > Card Programs	Card programs allow you to define card account ranges (BIN ranges) and associate these with the desired Risk Profile, Challenge Methods and Challenge User Interfaces.	Administrator and Analyst can view.
Analytics > Reports	Enables users to run custom reports on transactions.	Administrator and Analyst can manage.
Analytics > Queries	Apata's query builder is available to allow users to configure data queries in a format similar to SQL, in order to configure a data source for reports.. Example: Query for the total number transactions in the last 24 hours.	Administrator and Analyst can manage.
Access Management	View details of users and edit user access.	Administrator can manage.
Merchant simulator	Execute test transactions.	Administrator and Analyst can manage.
Transactions	Search and filter transactions.	All
Audit logs	Documentation of all events completed for a Financial Institution.	Administrator and Analyst can view.



6 Configuration of 3D Secure Screens

It takes 1-2 weeks to configure your 3D Secure requirements, including the Challenge screens.
All integration steps prior to UAT testing can take place in parallel, while Thredd configures your 3D Secure setup.

6.1 Screen Examples

You can customise the logo and text that appears on the 3D Secure Authentication screens during an authentication challenge session. If you support more than one language, you need to provide the text translations for the screens. See the examples below for authentication by One-time Password (OTP).

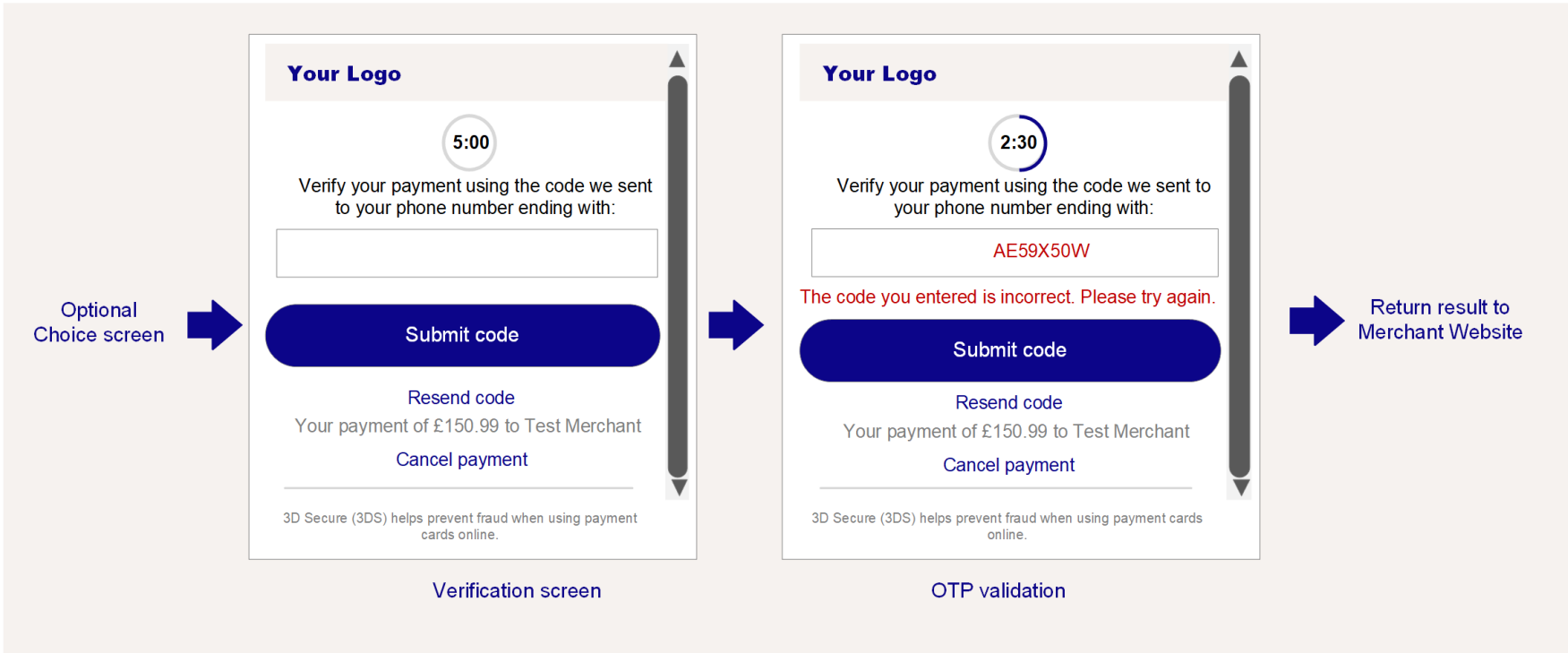


Figure 9: 3D Secure Authentication Screens - for OTP

See the examples below for KBA + OTP authentication.

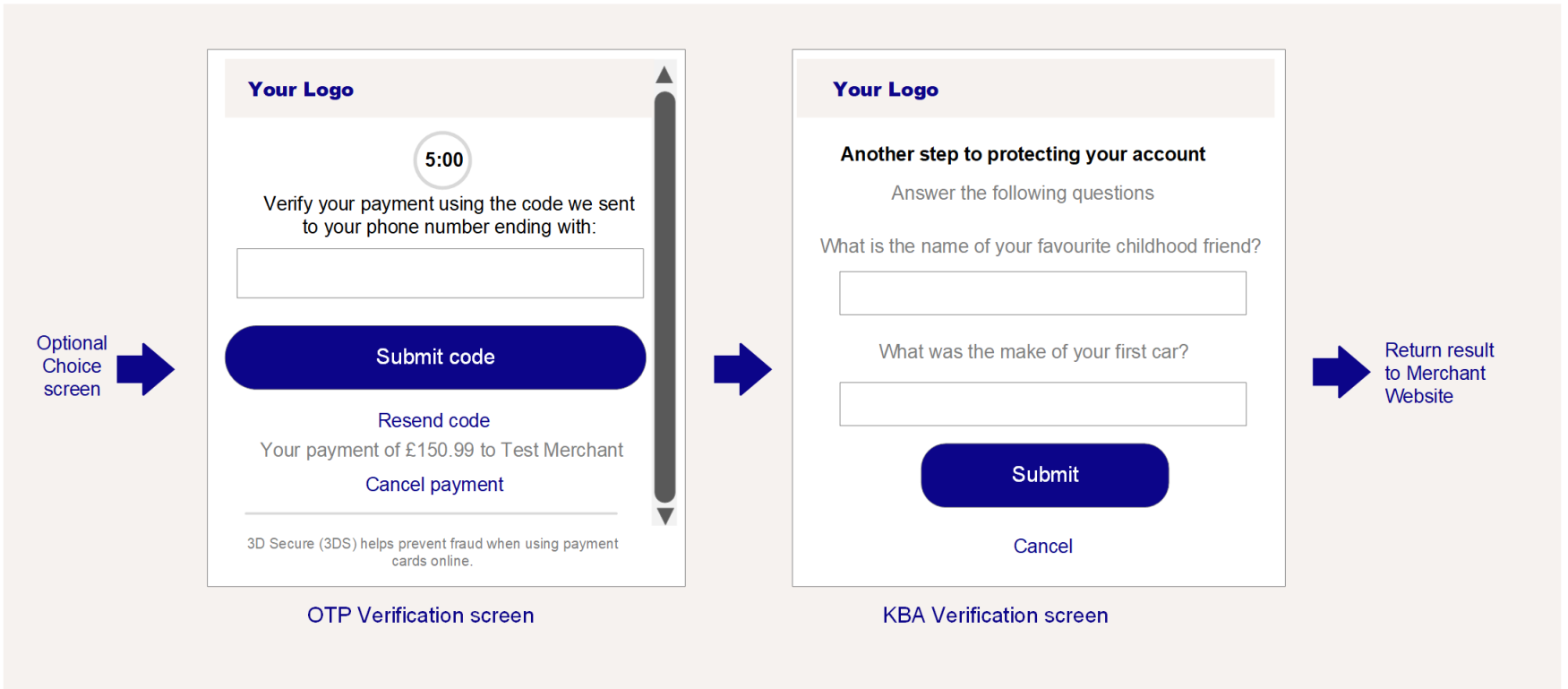


Figure 10: 3D Secure Authentication Screens - for KBA and OTP

See the examples below for Biometric authentication using your customer application.

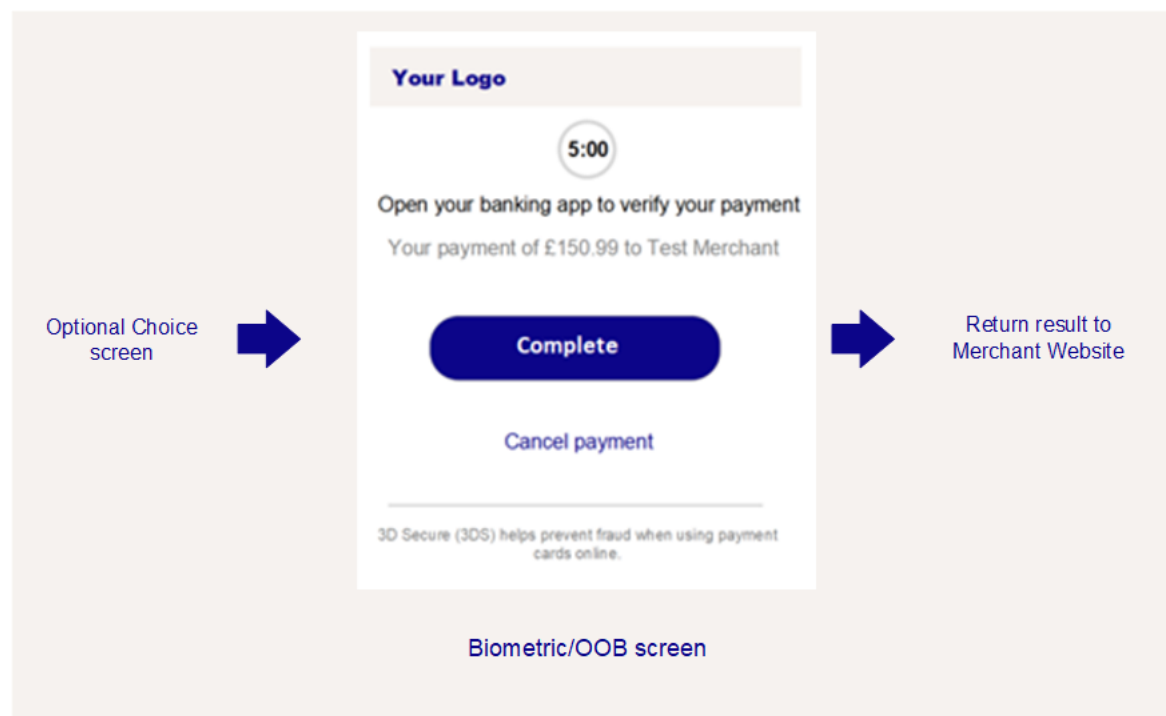


Figure 11: 3D Secure Authentication Screens - for Biometric

For more details on text field customisation, see [Completing your 3DS Product Setup Form > Challenge Screens](#).



7 Integrating 3D Secure Endpoints

This step includes setting up firewall permissions for IP addresses and integrating the Biometrics/OOB API endpoint.

7.1 Setting up Firewall Permissions

Firewall permissions need to be set up in both directions, between Thredd and your systems.

You will need to provide Thredd with a list of IP addresses you will be using, so that we can set up firewall permissions. These include:

- A list of the IP addresses (maximum of 5) you will use to access Thredd systems (in both UAT and Production).
- The IP addresses (maximum of 5) which Thredd will need to contact through the [DelegateSCANotification](#) API call. These are the resolving IP addresses of the [DelegateSCANotification](#) endpoint.
- A list of IP address from which you will be accessing the Thredd oAuth server.

Note: The IP addresses should be public and static. Your organisation must own the IP addresses.

You will need to permit access on your systems to Biometric/Out of Band API calls (in both UAT and Production). For details of allowed Thredd endpoints and IP addresses, see [Authorising Thredd IP Addresses](#).



8 Enrolling your cards in 3D Secure

You can enrol your cards in 3D Secure using either the Thredd 3D Secure Enrolment Thredd API (using SOAP) or the Cards API (using REST). Your request must include the Thredd public token and the authentication type to use during authentication for this card (e.g., BIOMETRIC) and the value. For OTP SMS, you need to provide the mobile number as the value. For the Biometric authentication, the value is for your reference only. See [Using the Card Enrolment API](#).

Note: Thredd also provides an auto-enrolment option, which can be triggered either as a bulk update on all your existing cards not yet enrolled or can be triggered at the time when you create a new card. See [Card Auto Enrolment](#).

Thredd saves the card enrolment record in our database.

8.1 Card Auto Enrolment

If you are upgrading existing cards to 3D Secure, Thredd can automatically enrol all your cards⁶ in the Apata 3D Secure service: you can request auto-enrolment by specifying the authorisation types to auto-enrol on your 3DS Product Setup Form (PSF). See [Completing your 3DS Product Setup Form](#).

Auto-enrol options include:

- *None* – there is no auto-enrolment. You will need to do this using either Thredd API or Cards API; see [Using the Card Enrolment API](#).
- *Initial load* – Thredd creates the authentication type credentials (e.g., OTP SMS or BIOMETRIC) for all existing cards. For OTP SMS, Thredd uses the phone number linked to the card (i.e., the phone number supplied when the card was created or updated). This is done as a single bulk update; adding credentials for any future new cards or applying any changes to credentials for existing cards must be done using either Thredd APIs or Cards API; see [Using the Card Enrolment API](#).
- *Continuous* – same as Initial load, however any future cards created (using the Card Create Thredd API or Card Create Cards API) will also have their credentials automatically registered for 3D Secure in the same way. Applying any changes to credentials for existing cards must be done using either Thredd APIs or Cards API; see [Using the Card Enrolment API](#).

Note: Continuous auto-enrolment is not recommended if you have live or active cards within a Product or BIN range which will need to be unenrolled or do not need 3D Secure.

Thredd auto-enrols the cards in the default main and fallback authentication methods. Auto-enrolment is available for OTP SMS, OTP Email, Out of Band (OOB) and Biometric authentication methods. Where a fallback method is not in use, the cards are enrolled to the default method only. For OTP SMS, Thredd auto-enrols using the mobile number linked to the card as the number for sending the SMS message to the cardholder during an SMS OTP authentication session.

Note: To use this option, you must first have set up the default main and fallback authentication types on your 3DS Product Setup Form. See [Completing your 3DS Product Setup Form](#).

8.2 Card Unenrollment

For cards that have been enrolled manually or auto-enrolled using the Initial Load option, you can un-enroll the card if required by deleting the credentials linked to the card (using Thredd's 3DS Web Services or the Cards API).

⁶auto-enrolment includes cards created (in active, non-active or temporary blocked status), but excluded cards that are expired or permanently blocked.



9 Completing UAT Testing

Once the authentication screens are configured, we will release your project into the Apata UAT environment for you to test.

9.1 Setting up your account in the Apata Portal

Thredd will set up your test account and provide you with your user credentials to access the Apata Portal. We will also set up your default test Risk Profiles.

A merchant simulator is available in the portal for transaction testing. For more information, see [Using the Merchant Simulator](#).

9.1.1 How to Access the Apata Portal

You can access the Portal at: <https://portal.apata.io/>

For more information on how to use the Apata Portal, see [Using the Apata Portal](#).

Note: To arrange training sessions on the Apata Portal, please contact your 3DS Project Manager.



10 Completing Pilot Production Testing

Thredd set up your cards in the Production environment:

- Thredd activates a *single card product* in the Production environment, so you can manually enrol a few cards for the production pilot testing.
- Thredd releases your 3D Secure configuration in the live environment.
- Your issuer (BIN sponsor) enrolls your pilot cards at the card scheme.

10.1 Viewing Risk Profiles in Apata Portal Production

You can view your rules in the live Apata Portal at:

<https://portal.apata.io/>

You can register the cards for the supported 3D Secure authentication types: if using the Thredd API, then use the 3D Secure Web service ([Ws_AddUpDelCredentials](#)); if using Cards API, then use the [Create 3DS Credentials](#) API.

Once your pilot cards are live with 3DS, the cards are then ready for use on any merchant website that supports 3D Secure. For details of merchants you may want to use for your testing, see [Appendix 4: 3D Secure Test Merchants](#).

You can put through live transactions and test the end-to-end 3D Secure authentication process.

We recommend you test the following:

- Test your main use case scenarios, based on the Risk Profile rules set up in Apata to trigger an *Accept*, *Reject* or *Challenge* outcome. For example, test different amounts, merchant categories, IP addresses, countries and transaction types. For more information, see [Managing Authentication Rules](#).
- Test the authentication process for all the authentication types you support:
 - Are the Authentication screens displayed correctly, with the customised text you provided?
 - If you support multiple languages, is the text displaying correctly on the Authentication screens in each language?
 - For OTP authentication, are the OTP text or OTP email messages displaying the correct details and going to the correct phone numbers?
 - For Biometric/In-App authentication, is your smart device application correctly handling the authentication process and reporting the result to Thredd?
 - For KBA authentication, are the question and answer pairs set up for the card being correctly validated?
- Check that once authentication is complete, the card then follows the normal payment authorisation process:
 - The payment is authorised by Thredd or your systems (depending on your EHI mode) and the balance on the card is adjusted accordingly.
 - You receive EHI authorisation messages and Transaction XML details for the transaction.
 - You can view details of your 3D Secure transactions in the Apata Portal.

Note: Mastercard provides mandatory Test Cases for testing the 3D Secure service in different scenarios, which will need to be completed. For details, speak to your issuer (BIN sponsor) or card scheme.

10.2 Rolling out to Production (Live)

Notify Thredd once you have completed your pilot testing.

If self-issuing, you must enroll your remaining card ranges at the card scheme. If not self-issuing, your Issuer (BIN sponsor) will do this. (This can also be done in one go when enrolling pilot card ranges.)

You must enrol all your live cards in 3D secure and register them for your supported authentication types (e.g., OTP SMS, OTP email, Biometrics or KBA). See [Step 5: Enrol your cards in 3D Secure](#).

If you have specified auto-enrol, Thredd will auto-enrol your cards for you.

Note: Please ensure all cards are enrolled with the relevant credentials for the required authentication methods before the card ranges are live at the card scheme.



11 Authorising Thredd IP Addresses

Thredd IP addresses must be allowed on your firewall to enable Biometric/OOB authentication. There are IP addresses for both UAT and production.

11.1 UAT Environments

These are the IP addresses for the UAT environments.

URL	IP Address	Component	Purpose
<i>https://uat-notifier-sender.thredd.net/api/v1/NotifierSender</i>	3.10.135.193	Thredd.Notifier.Sender	Thredd sends the Delegate SCANotification to the Program Manager from this endpoint.
<i>https://uat-notifier-receiver.thredd.net/api/v1/NotifierReceiver</i>	3.10.135.193	Thredd.Notifier.Receiver	Program Manager sends the Delegate SCAValidation request to this endpoint.
<i>https://uatists.globalprocessing.net</i>	3.11.64.130	GPS.Identity.Api	Program Manager generates and validates the oAuth token.

11.2 Production Environments

These are the IP addresses for the 3 different production cloud environments. PRD1 is for new clients in Europe (EU and the UK) and PRD2 is for new clients in the APAC region. PRDZ is for all existing clients.

11.2.1 PRD1 Environment

URL	IP Address	Component	Purpose
<i>https://p1-notifier-sender.thredd.net/api/v1/NotifierSender</i>	91.194.25.6 91.194.25.7 91.194.25.205 91.194.25.206	Thredd.Notifier.Sender	Thredd sends the Delegate SCANotification to the Program Manager from this endpoint.
<i>https://p1-notifier-receiver.thredd.net/api/v1/NotifierReceiver</i>	91.194.25.6 91.194.25.7 91.194.25.205 91.194.25.206	Thredd.Notifier.Receiver	Program Manager sends the Delegate SCAValidation request to this endpoint.
<i>https://p1ists.globalprocessing.net</i>	35.178.133.151 13.41.153.20	GPS.Identity.Api	Program Manager generates and validates the oAuth token.

11.2.2 PRD2 Environment

URL	IP Address	Component	Purpose
<i>https://p2-notifier-</i>	91.194.104.6	Thredd.Notifier.Sender	Thredd sends the



URL	IP Address	Component	Purpose
<i>sender.thredd.net/api/v1/NotifierSender</i>	91.194.104.7		Delegate SCANotification to the Program Manager from this endpoint.
<i>https://p2-notifier-receiver.thredd.net/api/v1/NotifierReceiver</i>	91.194.104.6 91.194.104.7	Thredd.Notifier.Receiver	Program Manager sends the Delegate SCAValidation request to this endpoint.
<i>https://p1ists.globalprocessing.net</i>	35.178.133.151 13.41.153.20	GPS.Identity.Api	Program Manager generates and validates the oAuth token.

11.2.3 PRDZ Environment

URL	IP Address	Component	Purpose
<i>https://p0-notifier-sender.thredd.net/api/v1/NotifierSender</i>	91.194.25.6 91.194.25.7 91.194.25.205 91.194.25.206	Thredd.Notifier.Sender	Thredd sends the Delegate SCANotification to the Program Manager from this endpoint.
<i>https://p0-notifier-receiver.thredd.net/api/v1/NotifierReceiver</i>	91.194.25.6 91.194.25.7 91.194.25.205 91.194.25.206	Thredd.Notifier.Receiver	Program Manager sends the Delegate SCAValidation request to this endpoint.
<i>https://p1ists.globalprocessing.net</i>	35.178.133.151 13.41.153.20	GPS.Identity.Api	Program Manager generates and validates the oAuth token.



12 Using the 3D Secure API

This section provides details of how to implement the 3D Secure service using the 3D Secure API. It includes the following topics:

- [Using the Card Enrolment API](#)
- [Using the Card Configuration API](#)
- [Using the Biometric/In-App Authentication API](#)



13 Using the Card Enrolment API

You can use either the Thredd Web Services (SOAP) or the Cards API (REST) to enrol your cards in 3D Secure.

13.1 Using Cards API

If you are using our Cards API, you can enrol your cards in 3D Secure and register your cards for different authentication types (e.g., OTP SMS, KBA and Biometric) using the 3D Secure API endpoints. This is a REST-based API, which requires sending your request in JSON format. For more information, see the [Cards API Website > Managing 3D Secure Credentials](#).

13.2 Using Web Services

If you are using our Web Services, you can enrol your cards in 3D Secure and register the card for different authentication types (e.g., OTP SMS, KBA and Biometric), use the 3D Secure ([Ws_AddUpDelCredentials](#)) web service API. This is a SOAP-based web service, which requires sending your request as an XML message. This web service is described in detail in the Thredd [Web Services Guide](#).

See the example below:

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
  <soapenv:Header>
    <hyp:AuthSoapHeader>
      <hyp:strUserName>*****</hyp:strUserName>
      <hyp:strPassword>*****</hyp:strPassword>
    </hyp:AuthSoapHeader>
  </soapenv:Header>
  <soapenv:Body>
    <hyp:Ws_AddUpDelCredentials>
      <hyp:WSID>14012021141223</hyp:WSID>
      <hyp:IssCode>PMT</hyp:IssCode>
      <hyp:PublicKey>123456789</hyp:PublicKey>
      <hyp:Action>Add</hyp:Action>
      <hyp:Credentials>
        <hyp:Credential>
          <hyp:ID>0</hyp:ID>
          <hyp:Type>BIOMETRIC</hyp:Type>
          <hyp:Value> Customer App Biometric </hyp:Value>
        </hyp:Credential>
      </hyp:Credentials>
    </hyp:Ws_AddUpDelCredentials>
  </soapenv:Body></soapenv:Envelope>
```

Notes

Thredd token of the card to enrol in 3D Secure:

```
<hyp:PublicKey>123456789</hyp:PublicKey>
```

To enrol the card and add an authentication type, use the **Add** Action:

```
<hyp:Action>Add</hyp:Action>
```

Specify the credentials to add to the card. In this example BIOMETRIC is specified:

```
<hyp:Credential>
  <hyp:ID>0</hyp:ID>
  <hyp:Type>BIOMETRIC</hyp:Type>
  <hyp:Value> Customer App Biometric </hyp:Value>
</hyp:Credential>
```



Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <Ws_AddUpDelCredentialsResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
      <Ws_AddUpDelCredentialsResult>
        <WSID>14012021141223</WSID>
        <IssCode>PMT</IssCode>
        <ActionCode>000</ActionCode>
        <PublicKey>123456789</PublicKey>
        <Action>Add</Action>
        <Credentials>
          <Credential>
            <ID>123456</ID>
            <Type>BIOMETRIC</Type>
            <Value>Customer App Biometric</Value>
            <KBA_Answer></hyp:KBA_Answer>
            <KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
          </Credential>
        </Credentials>
      </Ws_AddUpDelCredentialsResult>
    </Ws_AddUpDelCredentialsResponse>
  </soap:Body>
</soap:Envelope>
```

pay

Notes

- Your card sub-BIN/BIN range must be set up for 3D Secure at the card scheme (payment network) before you can use this web service.
- If you want to register the card for more than one authentication type in the same request, you can specify an array of credentials; see [Q. How do I add multiple authentication types to a card?](#)
- When registering the *BIOMETRIC* type, the `<Value>` parameter is for your reference only and is not used by Thredd or Apata.
- When registering the *KBA* type, the `<Value>` parameter is the ID of the question to use and `<KBA_Answer>` is the answer for Thredd to store⁷. For more information, see [Appendix 4: KBA Questions](#).
- For details of the types supported, see [Supported Authentication Types](#).
- You can use the same web service to add, update and delete credentials. You can use the [Get](#) function to return a list of credentials linked to a card.

13.3 Card Renewals and Credential Auto-enrolment

When an existing card is about to expire, you can renew the card using either the Card Renew ([Ws_Renew_Card](#)) web service (see the [Web Services Guide > Card Renew](#)), or the [Card Renew](#) Cards API endpoint.

Renewing the card will result in a new card being created, with a new PAN, Expiry Date and CVV. In this case, if old card has already been enrolled with 3D Secure credentials, then the new replacement card is automatically enrolled with the same 3D Secure credentials as the old card.

⁷Answers are stored in hash-encoded format in the Thredd database. Answers are case-sensitive; for example, ‘London’ would be hash-encoded differently from ‘london’ or ‘LONDON’.



14 Using the Card Configuration API

You can use 3D Secure Configuration ([Ws_ApataCardLevelConfigurations](#)), which is a Thredd Web Service using SOAP to add, update or delete card level configurations for Apata. This web service lets you set configurations such as the language used in the Apata Challenge screens and the Challenge Profile. For more details on this web service, refer to the Thredd [Web Services Guide](#).

See the example below:

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
  <soapenv:Header>
    <hyp:AuthSoapHeader>
      <!--Optional:-->
      <hyp:strUserName>*****</hyp:strUserName>
      <!--Optional:-->
      <hyp:strPassword>*****</hyp:strPassword>
    </hyp:AuthSoapHeader>
  </soapenv:Header>
  <soapenv:Body>
    <hyp:Ws_ApataCardLevelConfigurations>
      <hyp:WSID>15012024123478</hyp:WSID>
      <!--Optional:-->
      <hyp:IssCode>PMT</hyp:IssCode>
      <!--Optional:-->
      <hyp:PAN></hyp:PAN>
      <!--Optional:-->
      <hyp:PublicToken>123456754</hyp:PublicToken>
      <!--Optional:-->
      <hyp:Apata3DSLanguage>en-EN</hyp:Apata3DSLanguage>
      <!--Optional:-->
      <hyp:ApataChallengeProfileId>123ab-4fdfd443-43434f352</hyp:ApataChallengeProfileId>
      <!--Optional:-->
      <hyp:ApataCardProgramId>5456</hyp:ApataCardProgramId>
      <!--Optional:-->
      <hyp:ApataKBANumberOfQuestionsToAnswer>10</hyp:ApataKBANumberOfQuestionsToAnswer>
      <!--Optional:-->
      <hyp:ApataKBANumberOfIncorrectPermissible>10</hyp:ApataKBANumberOfIncorrectPermissible>
    </hyp:Ws_ApataCardLevelConfigurations>
  </soapenv:Body>
</soapenv:Envelope>
```

Notes

- **Apata3DSLanguage** – Language to apply to the 3DS challenge screens displayed to the cardholder. [BCP-47](#) is the language format that is used by Apata, for example, en-EN and fr-FR. The language content must first be set up for your card products. Once this is done, your 3DS Implementation Manager will share with you the language codes to use.
- **ApataChallengeProfileId** – Unique ID configured by Apata to represent the challenge profile (default and fallback challenge options).
- **ApataCardProgramId** – Unique ID configured by Apata to represent the specific card program and associated BIN ranges.
- **ApataKBANumberOfQuestionsToAnswer** – Number of KBA questions to answer correctly across all questions presented to the cardholder.
- **ApataKBANumberOfIncorrectPermissible** – Number of incorrect answers permissible for KBA across all questions presented to the cardholder.
- All Apata fields are optional, but at least one field must be populated. Thredd will respond with action code 441 if all five fields are blank.

Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <Ws_ApataCardLevelConfigurationsResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
      <Ws_ApataCardLevelConfigurationsResult>
        <WSID>15012024123478</WSID>
        <IssCode>PMT</IssCode>
      </Ws_ApataCardLevelConfigurationsResult>
    </Ws_ApataCardLevelConfigurationsResponse>
  </soap:Body>
</soap:Envelope>
```



```
<PublicKey>123456754</PublicKey>
<ActionCode>000</ActionCode>
<Apata3DSLanguage>en-EN</Apata3DSLanguage>
<ApataChallengeProfileId>123ab-4fd443-43434f352</ApataChallengeProfileId>
<ApataCardProgramId>5456</ApataCardProgramId>
<ApataKBANumberOfQuestionsToAnswer>10</ApataKBANumberOfQuestionsToAnswer>
<ApataKBANumberOfIncorrectPermissible>10</ApataKBANumberOfIncorrectPermissible>
</Ws_ApataCardLevelConfigurationsResult>
</Ws_ApataCardLevelConfigurationsResponse>
</soap:Body>
</soap:Envelope>
```



15 Using the Biometric/In-App Authentication APIs

REST-based APIs are used to initiate a Biometric or In-App OOB authentication session and to provide the result. The body of a REST-based API message is in JSON format. Three APIs are used to support Biometric/In-App authentication:

- [DelegateSCANotification](#) – sent by Thredd to notify you to set up an authentication session
- [DelegateSCAValidation](#) – as a Program Manager, you use this API to send the authentication result to Thredd.
- [DelegateSCACancelNotification](#) – sent by Thredd to notify you the cardholder cancelled the authentication.

15.1 Initiating a Biometric Session

When Thredd receives a request for Biometric/In-App authentication from Apata, Thredd uses the [DelegateSCANotification](#) API, to send your system a request to initiate a Biometric/In-App session. This request is sent to the [DelegateSCANotification](#) endpoint you specified in the *3DS Product Setup Form* (see [Completing your 3DS Product Setup Form](#)).

See the example below:

Thredd Request

```
{
  "NotificationId" : "f88458df-20ea-49b7-b890-119c2f5e8c6e",
  "PubToken": "123456789",
  "DelegateMethod": "push-confirmation",
  "FinancialInstitutionId": "f88458df-20ea-49b7-b890-119c2f5e8c6e",
  "Language": "en-EN",
  "DelegateScaId": "bcd507g1-7ec8-43b4-8a07-6c5e17078967",
  "CardScheme": "MasterCard",
  "CreatedMode": "GA",

  "Device":{
    "Channel": "BROWSER",
    "Ip": "string",
    "Language": "en-EN"
  }

  "MerchantInfo": {
    "Id": "mer-12345",
    "Name": "Amazon",
    "Country": "840",
    "Url": "https://amazon.com  ",
    "ChallengePreference": "no-preference",
    "RedirectAppUrl": "merchantScheme://appName?transID=b2385523-a66c-4907-ac3c-91848e8c0067"
  },

  "TransactionInfo": {
    "Type": "payment",
    "ProtocolVersion": "1.0.2"
    "Channel": "app",
    "DsTransactionId": "98315a91-e0b6-4fe0-8842-9ed82ea8ef0b",
    "Date": "2023-08-17T10:35:32.061Z",
    "Amount": "12345",
    "Currency": {
      "Code": "978",
      "Exponent": "2"
    }

  }

  "Recur": {
    "Frequency": "30",
    "EndRecur": "20221212"
  },
{
  "Install": "5"
}

  "DelegateStatus": "Active",
```



```
}
```

For more information on the fields in the request, see the [DelegateSCANotification](#) and [DelegateSCACancelNotification](#) message fields.

Your Response

Upon receipt of a request, your systems return a 200-HTTP response code (OK/success).

Note: If Thredd does not receive the 200-HTTP response to the [DelegateSCANotification](#) request, Thredd does not resend the request.

When your systems receive a [DelegateSCANotification](#) request, you can use the Thredd oAuth server to validate the token (as an option.) This prompts the cardholder to open your Smart device customer application and authenticate themselves with the supported Biometric method (e.g., fingerprint or face recognition) or In-App method.

Thredd passes the bearer token in the header of the [DelegateSCANotification](#) request, as shown in the example below.

```
Authorization: Bearer eyJh-  
bGciOiJSUzI1NiIsImt-  
pZCI6IjE5ODI3Q0E4M0NEMkNGNUUzMtAxMUVBQkQ0N0ZDNTg4RkMyRjQ3RTIiLCJ0eXAiOiJh-  
dCtqd3QiLCJ4NXQiOiJHwUo4cUR6U3oxNHhBUjZyMUh-  
fRm-  
lQd3ZSLUki-  
fQ.eyJyYmYiOiJlE2MDc1MzM1Nzk-  
sImV4cCI6MTYwNzU0Nzk3OSwiaXNzI-  
joi-  
aHR0cHM6Ly9vYXV0aHVh-  
dC5n-  
bG9iYWx-  
wcm9jZXNz-  
aW5nLm5ldCI6ImF1ZCI6WyJyZHh-  
hcGkiLCJmaXJi-  
aW9tZXRY-  
aWNh-  
cGkiXSwiY2x-  
pZW50X2lkIjoizmlyYmlyIiwic2NvcGUiOi0siY2xpZW50X2ZhbG1kYXRlIiwiaWZmlyYmlybWV0cm1jYXBpI119.owfqYt7Rf6zHMLY2HT3j0RH7Lti05oWkp-  
bJ41QF1LZyqxaRMZWJAUXuRXJwIWrG2wtC0Q1KFzVPbZhpwKAwJvQTIymJFhryEvRUGTQqM61Nwu_Dnsx8H-Jpi7_0PjQk4MaAhqFv6MEgDMHvxUZ2_Q6vYj_-  
h2rRDunHjBvhvA55-yGLdqxeHRtNvHJQCsaVZHdLBngUpeFpWcvrbhk1SYbNlG1f1YBm5aAX_YDwpWt4p_M6w7TAYJZQvc4Hi_NqAZwUOY7x01-  
hVD69onUmd74k6nt0ncowGgC3naWQieqcVMd3B1kCAnnYZfLlXMhSxeN_XqWtjKTK3wMavYj6vrw
```

As an option, you can also verify the token (check that it is valid and active) using the oAuth introspect API endpoint. For more details, see [Using the oAuth server](#).

15.2 Notifying Thredd of the Result of the Biometric Session

When authentication is complete, you must use the [DelegateSCAValidation](#) REST API to send the authentication outcome to Thredd.

Note: The authentication session times out if Thredd does not receive your [DelegateSCAValidation](#) request before the [challengeExpiry](#) time.

API Endpoints

<https://uat-notifier-receiver.thredd.net:7293/api/v1/NotifierReceiver>

See the example JSON message below:

Your Request

```
{  
  "NotificationId" : "f88458df-20ea-49b7-b890-119c2f5e8c6e",  
  "PubToken": "123456789",  
  "DelegateScaId": "bcd507g1-7ec8-43b4-8a07-6c5e17078967",  
  "PmReferenceId": "refId",  
  "Status": "SUCCESS",  
  "Error": null  
}
```

Notes

Thredd token of the card that was authenticated:



```
"PubToken": "123456789",
```

The message also contains the result of your authentication as: SUCCESS, FAILURE, FAILWITHFEEDBACK or ERROR. For example:

```
"status": SUCCESS
```

Successful Thredd Response

If the request from the client was successful, Thredd provides a response in return.

```
{
  "PubToken": "206187551",
  "DelegateScaId": "ddab0431-a615-42d7-81ab-5a6683bb5c3e",
  "PmReferenceId": "refId",
  "Status": "SUCCESS",
  "Error": {
    "ReferenceNumber": "",
    "Description": "",
    "Message": ""
  }
}
```

When successful, the transaction proceeds to authorisation.

Error Handling

If there was an error in your request, for example, invalid JSON format or incorrect details, Thredd returns details of the error.

For more information on the fields in the response, see [DelegateSCAValidation Message Fields](#).

Example Thredd Response for a Reporting Failure

If Thredd is unable to report the biometric authentication result to Apata, an error message appears similar to this:

```
{
  "Pubtoken": "182293241",
  "DelegateScaId": "82b44d02-71db-4d00-9b3d-9fb7c0aa5eaa",
  "PMReferenceID": "refId",
  "Status": "FAILWITHFEEDBACK",
  "Error": {
    "ReferenceNumber": "504023",
    "Description": "DelegateSca status reporting to 3DSProvider failed",
    "Message": "DelegateSca status reporting to 3DSProvider failed"
  }
}
```

Validation Timeout

When Thredd sends the [DelegateSCANotification](#) message to your system, Thredd expects to receive back a [DelegateSCAValidation](#) response from your system before the challenge expiry time provided in the [DelegateSCANotification](#).

If Thredd does not receive the [DelegateSCAValidation](#) response within this period, the authentication session times out. Apata then returns a Fail result to the merchant.

15.3 Using the Thredd oAuth server

You must authenticate against the Thredd oAuth server before you can use the 3D Secure Biometric API services. The oAuth server provides you with a username (client_ID) and a secret password (Client_secret) that you need to include in your API requests for accessing the Biometric/OOB API services.

You can also use the oAuth server to validate any API requests received from Thredd; Thredd provides you with another username (client_ID) and a secret password (Client_secret) for the token validation.

oAuth is a secure method that replaces TLS and does not require you to set up X509 certificates. There are no additional costs for using the Thredd oAuth server.

The oAuth server complies with the RFC 7662 standard. See: <https://tools.ietf.org/html/rfc7662>

To find out more, see the identity server documentation, available at: <https://identityserver4.readthedocs.io/en/latest/intro/specs.html>

oAuth API Endpoints

Thredd provides the following oAuth API endpoints:



- Token – you can use this to obtain a token. Whenever you use the Biometric/ OOB API, you should include this token in the Authorization header of your HTTP request.
- Introspect – you can use this to validate the token Thredd sends to your [DelegateSCANotification](#) endpoint (to notify you of a request to initiate a Biometric/In-App session)

Thredd oAuth endpoints for Token and Introspect are listed below:

Environment	Endpoint
UAT	https://uatists.globalprocessing.net/connect/token https://uatists.globalprocessing.net/connect/introspect
Live (Production)	https://p1ists.globalprocessing.net/connect/token https://p1ists.globalprocessing.net/connect/introspect

oAuth User Credentials

Check with your Thredd 3DS project manager for your **client_id** and **client_secret** to access the oAuth server.

oAuth Token Expiry

The default lifetime of the token is 4 hours (14400 seconds).

oAuth Token Request Example

You can retrieve an oAuth access token from the Thredd oAuth server using the private credentials (client_id and client_secret) provided to you by Thredd.

The following is an oAuth Token request:

```
POST https://uatists.globalprocessing.net/connect/token
Accept: application/json
Content-Type: application/x-www-form-urlencoded
client_id=9d70c6bbad8ad20262828222fc0f3fdd
&client_secret=a3d5566e8ca0d6da823eb7815c1c2b66
&grant_type=client_credentials
```

The following is an oAuth Token response. The oAuth server returns a token, which you must include in any Biometric/OOB requests.

```
200 OK

{
  "access_token": "eyJh-
bGciOiJSUzI1NiIsImt-
pZCI6IjZhNjd-
m0WEzZTA1OTM0ZWZjOTUzYmY1ZjI1ZjVkdMDMyIi-
widHl-
wIjo1SldUIn0.eyJ1bmYiOiE1ODI1NDExMTYsImV4cCI6MTU4MjU0NDcxNi-
wiaXNzI-
joi-
aHR0cHM6Ly9s-
b2Nh-
bGhvc3Q6NDQzMzYiLCJh-
dwQiOiI0Ii-
aHR0cHM6Ly9s-
b2Nh-
bGhvc3Q6NDQzMzYvcvVzb3VyY2VzIi-
wicmR4YXBpIi-
wicmVsYXl-
hcGkiXSwiY2x-
pZW50X2lkIjo1dmNhcysInNjb3BlIjpbImNsaWVudF92YWxpZGF0ZSI6ImNjkeGFwaSI6ImNjbGF5YXBpI119.Lh5Mp0Qa82QVMzs4y1mzbbB9W9Qk4qiVc0Dewv0q3N1_
JmspkYyYh0i1Vj8KxNxPjiKVYnFA2hDwtlK016l8aL1oEkBky1h4haQuqtPwaUdNirwVDS99R1VqCh3wYmYZmNHNseJvEVIrd__HQ7kTJLG07NkebPc_
QM6rTB2qfYI9nax6JQnMrk72cDzeorwUlxSf2G6p49kpgyhNJoohfptWlRtV6JWUPUVEC7oNEfYnbfjVhSUyF5_11HHi_
2r0zLhFIdPH7fSUXz18000CMqUvSedaAJN6SRIEnTiE5isjIMJG3T4pymqUcc6ujm3upB9UStaBXMe1p7Rom7LVqQ",
  "expires_in": 3600,
  "token_type": "Bearer",
  "scope": "client_validate apataapi"
}
```

The Thredd oAuth server supports basic HTTP status codes. See the table below:



Status	Description
200	The request was successful.
400	The server could not understand the request due to invalid syntax.
401	The client must authenticate itself to get the requested response.
403	The client does not have access rights to the content.
404	The server cannot find the requested resource.
500	The server has encountered a situation it doesn't know how to handle.

When obtained, your Client application must pass the access token on every request made to the Thredd Biometric/OOB service. The access token is included in the standard Authorization header of the HTTP request as shown in the following example:

```
Authorization: Bearer XXXXXX_ACCESS_TOKEN_XXXXX
```

oAuth Introspect Example

Thredd includes a token in the header of the request sent to your [DelegateSCANotification](#) endpoint. As an option, you can use the Introspect endpoint to validate this token where you check that it is active. Below are examples of an oAuth Introspect request and response.

```
POST https://uatists.globalprocessing.net/connect/introspect
Accept: application/json
Content-Type: application/x-www-form-urlencoded
token-
=eyJ-
hbG-
ciOiJSUzI1NiIsImt-
pZCI6IjE5ODI3Q0E4M0NEMkNGNUUzMTAxMUVBQkQ0N0ZDNTg4RkMyRjQ3RTIiLCJ0eXAiOiJh-
dCtqd3QiLCJ4NXQiOiJHWUo4cUR6U3oxNHhBUjZyMUh-
fRm-
lQd3ZSLuki-
fQ.eyJyYmYiOiJlE2MDc1MzM1Nzk-
sImV4cCI6MTYwNzU0Nzk3OSwiaXNzI-
joi-
aHR0cHM6Ly9vYXV0aHVh-
dC5n-
bG9iYWx-
wcm9jZXRz-
aW5nLm5ldCIsImF1ZCI6WyJyZHh-
hcGkiLCJmaXJi-
aw9tZXRY-
aWNh-
cGkiXSwiY2x-
pZW50X2lkIjoizmlyYmlyIiwic2NvcGUiOiIyY2xpZW50X3ZhbGlkYXRlIiwiaWZmlyYmlybWV0cmllYXBpIl19.owfqYt7Rf6zHMLY2HT3j0RH7Lti05owkp-
bJ41QF1ZLyqxaRMZWJAUXuRXJwIWRG2wtC0Q1KFzVPbZhpwKAwJvQTIymJFhryEvRUGTQqM61Nwu_Dnsx8H-Jpi7_0PjQk4MaAhqFv6MEgDMHvxUZ2_Q6vYj_-
h2rRDunHjBvhvA55-yGLdqxeHRTNvHJQCsaVZHDLBngUpeFpWcwrbbhk1SYbNlG1f1YBm5aAX_YDwpwt4p_M6w7TAYJZQvc4Hi_NqAZwU0Y7x0l-
hVD69onUmd74k6nt0ncowGgC3naWQieqcVMd3B1kCAnnYZfLlXMhSxeN_XqWtjKTK3WMavYj6vrw
```

Response (Successful)

```
{
  "nbf":1616170152,
  "exp":1616184602,
  "iss":https://stsdemo.globalprocessing.net,
  "aud":[
    "coreapi",
    "relayapi"
  ],
  "client_id":"coreapidev",
  "active":true,
  "scope":"coreapi"
}
```



Notes

- In the request body, the Content-Type is **application/x-www-form-urlencoded**
- **token** is the bearer token value you received in the header of a [DelegateSCANotification](#) request from Thredd.)
- The authorization header should be in the following format: Basic (hashed value). The hashed value needs to be **resourceid:password** and must be base64 encoded.
- The **scope** field indicates your application permissions. It is sufficient to check that the bearer token is **active**. You can also check the scope.
- If you are using .NET, recommends using the Identity Model middleware software package. For more information, see <https://identitymodel.readthedocs.io/en/latest/>
- The following setting indicates that the bearer token is active.

```
"active":true,
```

Response (Failure)

```
{
  "active":false
}
```

The following setting indicates that the bearer token is **not** active.

15.4 Cancelling an authentication

If a cardholder cancels an authentication, Thredd sends your system a request through the [DelegateSCACancelNotification](#) API.

```
{
  "NotificationId" : "f88458df-20ea-49b7-b890-119c2f5e8c6e",
  "PubToken": "123456789"
  "DelegateMethod": "push-confirmation",
  "FinancialInstitutionId": "f88458df-20ea-49b7-b890-119c2f5e8c6e",
  "Language": "en-EN",
  "DelegateScaId": "bcd507g1-7ec8-43b4-8a07-6c5e17078967",
  "CardScheme": "MasterCard",
  "CreatedMode": "GA",
  "Device":{
    "Channel": "BROWSER",
    "Ip": "string",
    "Language": "en-EN"
  }

  "MerchantInfo": {
    "Id": "mer-12345",
    "Name": "Amazon",
    "Country": "840",
    "Url": "https://amazon.com ",
    "ChallengePreference": "no-preference",
    "RedirectAppUrl": "merchantScheme://appName?transID=b2385523-a66c-4907-ac3c-91848e8c0067"
  },

  "TransactionInfo": {
    "Type": "payment",
    "ProtocolVersion": "1.0.2",
    "Channel": "app",
    "DsTransactionId": "98315a91-e0b6-4fe0-8842-9ed82ea8ef0b",
    "Date": "2023-08-17T10:35:32.061Z",
    "Amount": "12345",
    "Currency": {
      "Code": "978",
      "Exponent": "2"
    }
  }
}
```



```
"Recur": {  
  "Frequency": "30"  
  "EndRecur": "20221212"  
},  
  
  "Install": "5"  
}  
  
"DelegateStatus": "Cancelled",  
  
}
```

Your Response

Upon receipt of a cancellation request, your systems return a 200-HTTP response code (OK/success). If there is an error, your systems return a 400-HTTP response code.



16 Additional 3D Secure Considerations

This section provides information on other aspects of the 3D Secure service.

16.1 Support for 3D Secure Versions

EMV 3D Secure 2.1 and 2.2 are Card Scheme (Visa/MasterCard) versions. Thredd and Apata Commerce support both versions.

Thredd and Apata support Mastercard EMV 3DS 2.1 and 2.2.

Thredd and Apata support Visa EMV 3DS 2.1 & 2.2

Note: Visa and Mastercard discontinued support for 3DS 1.0 in October 2022.

Note: We are awaiting finalised roll-out details of 2.3 from EMVCo. See the [EMVCo website > Enhancing the 3D Secure Specifications](#).

See [Appendix 1: Apata 3D Secure Rules](#).

16.1.1 3D Secure 2.1

EMV 3DS 2.1 provides SCA compliance and merchant fraud liability protection. It provides support for the following features:

- Smart devices and a better customer experience.
- Enables merchants to send additional information to the issuer (BIN sponsor).
- Supports the use of dynamic authentication through Biometrics and In-app authentication methods.
- Supports issuer (BIN sponsor) exemptions through risk-based authentication (e.g. Frictionless Flow).
- Can be used to set up merchant-initiated transactions, such as for recurring payments; the first payment requires SCA while subsequent payments can be set up as merchant-initiated transactions without requiring SCA.

16.1.2 3D Secure 2.2

EMV 3DS 2.2 includes all the features of 2.1, plus:

- Supports SCA exemption flags – to enable more control over SCA decisions and customer experience.
- Offers a new 3RI channel for non-payment authentication.
- Allows merchants to request SCA exemptions through their Acquirer.

For more information on EMV 3DS 2.1 and 2.2, see [EMV® 3-D Secure](#).

16.2 Supported Authentication Types

Refer to the table below for details of the authentication types which Thredd supports. The [<Type>](#) value is the name as used in the 3D Secure web service / Cards API) and as described below:

Type	Description
OTPSMS	OTP SMS authentication. Apata generates a single-use One-Time Password (OTP). Thredd sends the OTP in a SMS text message to the cardholder’s mobile phone number and the cardholder enters the OTP in the 3D Secure screen to authenticate.
OTPEMAIL	OTP email authentication. Apata generates a single-use One-Time Passcode (OTP). Apata sends the OTP in an email message (from the email address specified by your organisation) to the cardholder’s email address and the cardholder enters the OTP in the 3D Secure screen to authenticate.
KBA	The cardholder is asked to verify their identity by providing the answer to a question such as ‘What was the make of your first car?’ or ‘What is the name of your first pet?’ Note: In the EU/EEA, KBA is combined with OTP SMS, to meet the two-factor requirement for Strong Customer



Type	Description
	Authentication (SCA).
BIOMETRIC	Biometric authentication. Apata sends a Biometric authentication request to Thredd and we forward this to your systems. You need to verify the cardholder using your customer smart phone application, via Biometric data, such as a fingerprint scan, obtained from the cardholder’s mobile device. Your customer application manages the Biometric verification and returns a response to Thredd.
OUTOFBAND	In-App authentication. Apata sends the Out Of Band (OOB) authentication request to Thredd and we forward this to your systems. You need to verify the cardholder using your customer smart phone application, for example by asking the user to enter a username and password. Your customer application manages the verification and returns a response to Thredd.

16.2.1 Other Types of authentication

Note: For the services listed below, no card enrolment is required via Thredd web services or Cards API. These services will be available to any card that has been enrolled in 3D secure.

Type	Description
RBA	Risk-Based authentication (done via Apata). Also referred to as TRA (Transaction Risk Analysis). The authentication decision (i.e., accept, reject, or challenge) is determined by the risk rules configured by the issuer (BIN sponsor). In Apata, there are a wide range of data points available to create authentication rules and risk profiles. These define how the transaction is evaluated once it reaches Apata.
Transaction History	During the authentication process, the cardholder is asked to identify a recent payment they made with their card. Transactions history details are taken from previous transactions where 3D Secure authentication was requested. Note: Please specify if you will require this authentication method when completing the 3DS Product Setup Form.



17 Using the Apata Portal

Apata provides an online Portal where users can view and manage their 3D Secure service. Please request access from your Thredd 3D Secure Project Manager or your organisation's Apata Portal administrator.
You can access the Portal at: <https://portal.apata.io/>

17.1 Activating your Account

- 1. You should receive an invitation email from your account administrator, inviting you to activate your account. Click the link in the email or copy and paste it into a browser window.
A screen similar to the following is displayed:

Welcome

You received invitation with following permissions:

Email Address

warren.singer@thredd.com

User Type

FI

Roles

State

ACTIVE

Organisation Id

thredd-sandbox

Expires At

Nov 28, 2023, 2:41:41 PM

FI Permissions

Api Key

- 2. Scroll down to the bottom of this screen and click **Accept Invitation**.
- 3. Enter a username and password, following the on-screen instructions.
- 4. Scan the QR code on your mobile phone using an authenticator app you have installed on your phone to support two-factor authentication.

Note: You can use any authenticator app. Examples include Authy and Google Authentication App.



To be able to use this application it is **mandatory** to set up MFA with some recommended Apps like:

Authy
Google Authentication App
Guardian



HBGCQ3JMMNOVAW2OMRVWSUDXOZIFMPRBKVXXS3DOM
VXHSOLHKFEA

Token

Activate Account

Figure 12: Activating your Apata Account

5. In your mobile phone authenticator app, add an account for Apata. Please follow the instructions of your chosen MFA App.
6. In the **Token** field, enter the token obtained from your authenticator app and click **Activate Account**.

17.2 Signing in to your Account

1. Go to: <https://portal.apata.io/>
2. Enter your username and password and click **Sign in**.

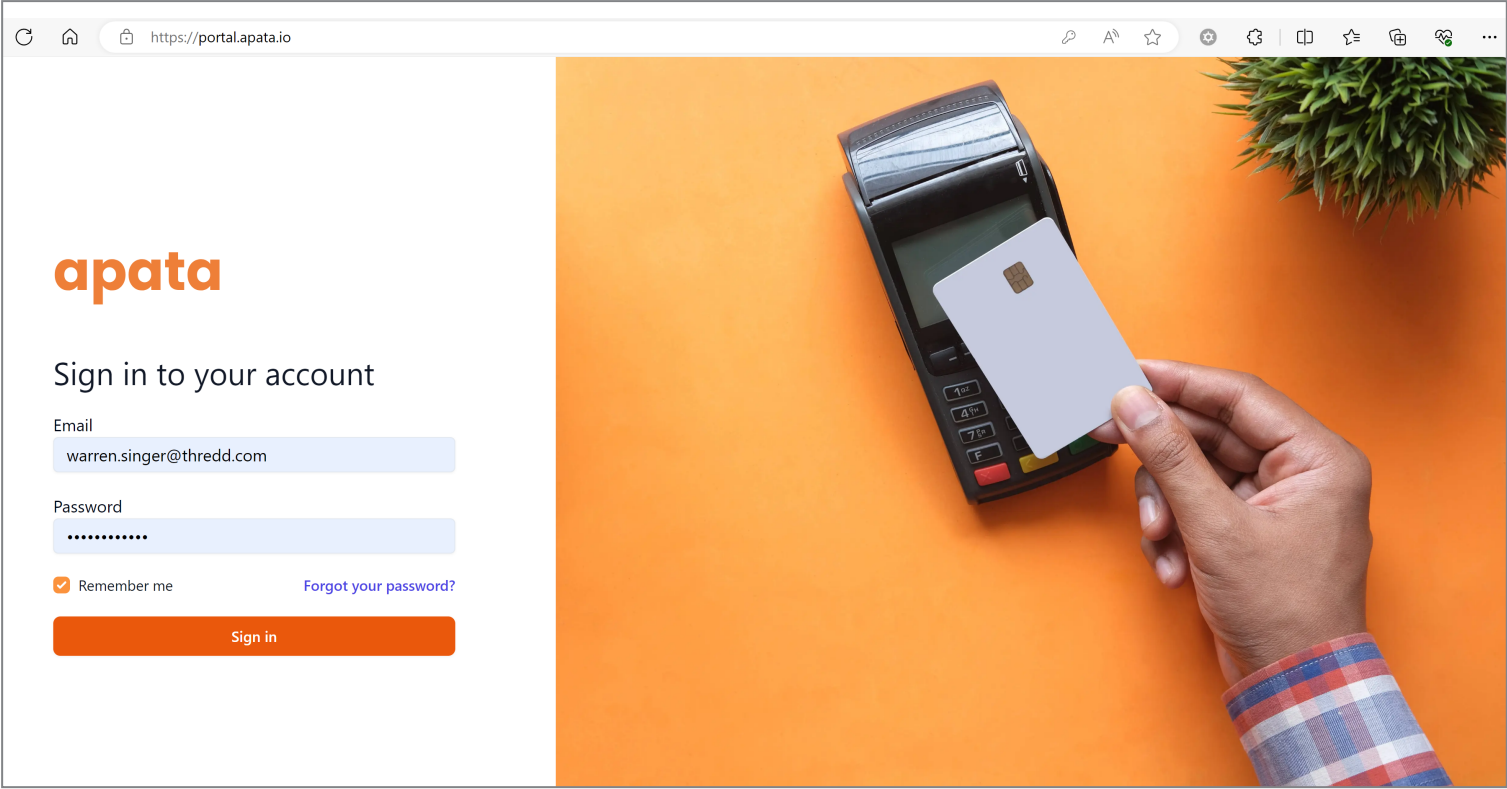


Figure 13: Apata Login screen

3. Enter the token on your mobile phone Authenticator app and click **Log in**.



17.3 Selecting your Financial Institution

- After signing in to your account, select the organisation (Thredd) and financial institution (your organisation's name) and click **Set Workspace**.

The Dashboard for your financial institution is displayed. See [Apata Dashboard](#).



18 Apata Dashboard

The Apata Dashboard provides graphs of 3D Secure transactions for your organisation.
You can filter the graphs to display transactions for: **Last 24 hours**, **Last 7 days**, **Last 30 days**.

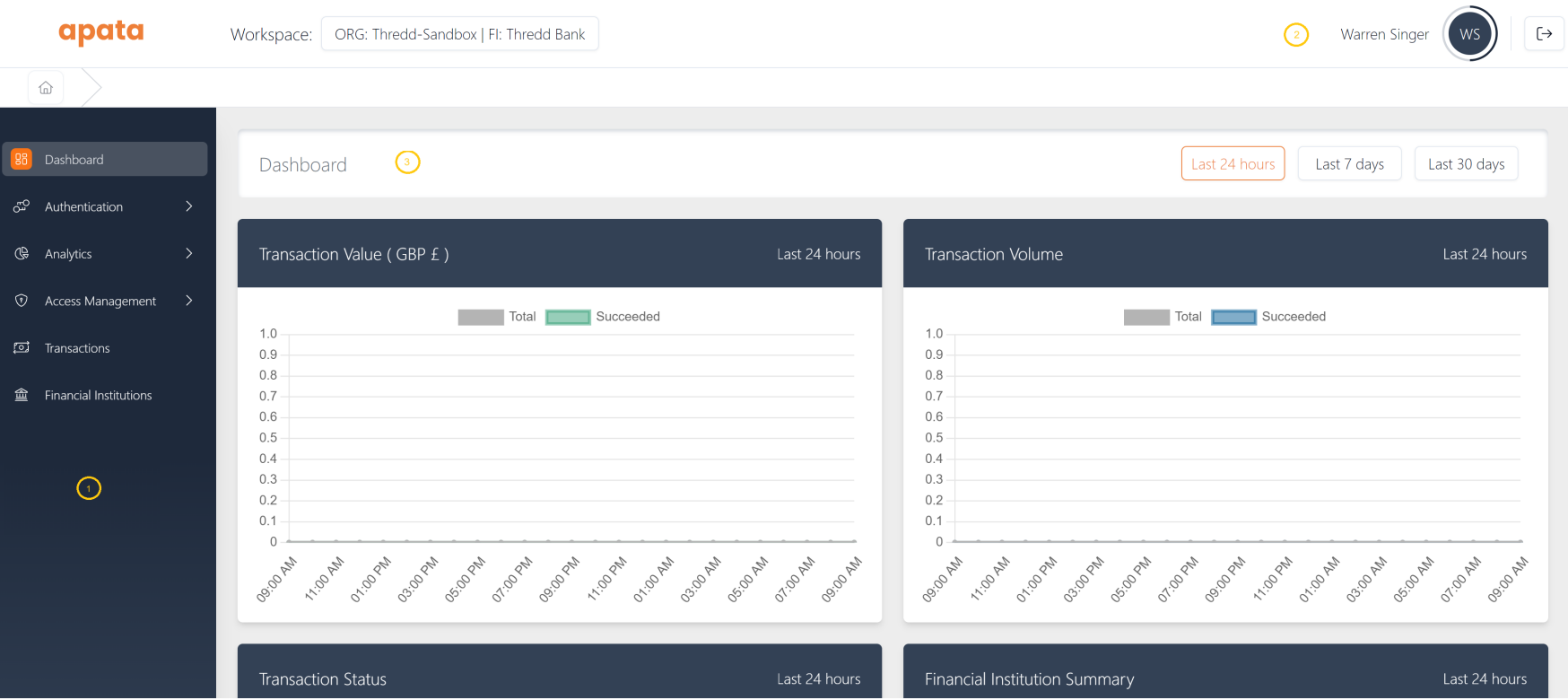


Figure 14: Apata Portal Dashboard

Legend: 1 = Left-hand menu; 2= Account signed into and sign-out icon; 3= Main workspace
Menu options available to you are described below.

Option	Description	User Access Permissions
Authentication	View your challenge methods and card programs. Create and edit your authentication rules	Administrator and Analyst
Analytics	Build reports and run queries.	Administrator and Analyst
Access Management	Set up and manage user accounts.	Administrator
Transactions	View 3D Secure transactions.	All users can view.
Bin & Card Ranges	View details of cards ranges that have been set up in the system.	Administrator
Merchant Simulator	Run transaction simulations to test authentication rules outcomes.	All users, if enabled for your account.

18.1 Signing Out

To sign out of your account, click the  icon at the top right of the Apata Portal.



19 Managing Authentication Rules

The **Authentication** menu on the **Apata Portal Dashboard** enables you to view your challenge methods, card programs and corresponding BIN ranges, and also create and update your authentication rules. Options include:

- Viewing Risk profiles
- Creating and Editing Risk profiles (administrator-level only)
- Viewing Challenge methods
- Viewing Cards Programs

Note: Thredd provides default authentication rules and profiles for your programme; you can edit or add to these rules and profiles to meet your business requirements. (Before making any changes, we recommend you discuss first with your 3D Secure implementation Manager.)

Note: Only Administrator users can edit these options.

19.1 Viewing Risk Profiles

A risk profile defines a set of rules for processing of transaction requests and determining the action the system should take (such as *accept*, *reject* or *challenge*). A Risk profile could be simple, consisting of a single rule, or complex, consisting of multiple rules. You can also define the order in which the rule checks are made.

1. To view a list of risk profiles, select **Authentication > Risk Profiles** from the left-hand menu.

Risk Profiles						+ Create Risk Profile
#	Name	Description	Type	Created	Updated	
1	APAC - prepaid Risk Profile	Set of rules to assess transactions from the c...	V1	Aug 11, 2023, 4:34:41 PM	Sep 21, 2023, 3:23:13 PM	
2	ALLOW ALL		V1	Oct 2, 2023, 12:19:43 PM	Oct 2, 2023, 12:20:23 PM	
3	CHALLENGE ALL		V1	Oct 2, 2023, 12:20:05 PM	Oct 2, 2023, 12:20:05 PM	
4	EU program risk profile	Default Challenge Risk Profile created when ...	V1	Aug 10, 2023, 2:36:01 PM	Sep 21, 2023, 3:24:25 PM	
Items Per Page 100						1

Figure 15: View Risk Profiles

2. To view details of a risk profile, click the button.

Below is an example of a simple risk profile rule, configured to allow all (no challenge screens will appear). This might be suitable for low-value prepaid cards or closed loop card programmes.

ALLOW ALL

111e5220-94f8-48f0-90c0-4e95f23b36b0

Oct 2, 2023, 12:19:43 PM
created at

Oct 2, 2023, 12:20:23 PM
last update

About

1

SIMPLE

9631aa2d-d2bd-4898-9308-e3a5d956bcea

Action: ACCEPT

Figure 16: Risk Profile Rule - Allow All

Below is an example of the opposite risk profile rule, configured to provide challenge screens for all authentication transactions. This might be suitable for cards that are considered very high risk (e.g., issued in higher risk countries).



CHALLENGE ALL
791a739a-c725-4a5b-86da-be9f54346399
Oct 2, 2023, 12:20:05 PM created at | Oct 2, 2023, 12:20:05 PM last update

1

SIMPLE
7724a338-1880-40ba-824f-b741ecc6778e

^

Action: CHALLENGE

Figure 17: Risk Rule - Challenge All

Below is an example of a complex risk profile, consisting of multiple rules, created for a card program in the EU. The risk profile consists of rules to allow frictionless authentication in the following circumstances:

- the merchant is on a trust list
- the transaction is within the PSD2 rules for low-value transaction
- the transaction is a secure corporate payment
- the transaction is merchant-initiated
- the merchant acquirer has requested an exemption from authentication
- the transaction is not a payment transaction (e.g., account funding)
- the transaction is within the cumulative number for frictionless authentication
- the transaction is within the maximum cumulative spend (e.g., €100 or £100)

EU program risk profile
9f6ffbf8-aa6d-4ac0-814e-9c9e4219aa05
Aug 10, 2023, 2:36:01 PM created at | Sep 21, 2023, 3:24:25 PM last update

About
Default Challenge Risk Profile created when a Financial Institution is onboarded

1

WHITELIST
226522cd-3c15-4ccc-aa36-339fafe42461

^

2

PSD2_LOW_VALUE
67a34301-9db8-486c-b3e1-6ac21152cc8d

^

3

SECURE_CORPORATE_PAYMENT
ab918081-fe7b-4aff-81e1-88fb2c410d82

^

4

MERCHANT_INITIATED
4b009d66-a3ce-41a6-a317-a03495b4fd06

^

5

ACQUIRER_EXEMPTION
fff55ab5-82a2-4dfb-9fc2-3d2ba9b34706

▼

6

NON_PAYMENT
51c47438-d88c-4468-b464-2cff8d415394

▼

7

MAX_FRICTIONLESS_TRANSACTIONS
a21181f5-d09e-4267-be62-0dc11a7b264e

▼

8

MAX_CUMULATIVE_FRICTIONLESS_SPEND

▼

Figure 18: Example of Risk Profile Details

IMPORTANT: Each Risk Profile and its associated rules is assigned a unique system ID, which is then assigned to a card program (i.e, grouping of cards of BIN ranges).

- To view further details of the rule, click the ▼ button next to the rule.
The example below shows the configuration for rule 6. In this example, you can select the type of transactions (identified by codes: 04, 05, 06, 07, 08, 09 and 10) that are treated as non-payment transactions and which will be allowed without any Challenge screens.



=

2

i

NON_PAYMENT

78999eea-8515-4365-890e-16f6477163b9

^

🗑️

Types

☐ 04 - Add card

☐ 05 - Maintain card

☐ 06 - Cardholder verification as part of EMV token ID&V

☐ 07 - Billing Agreement

☐ 08 - Split shipment

☐ 09 - Delayed shipment

☐ 10 - Split payment

Action

ALLOW

▼

Figure 19: Example of a rule configuration

19.2 Creating and Editing Risk Profiles

To create a new risk profile, in the Risk Profiles screen, click the **Create Risk Profile** button.

Note: Only administrator users can access this functionality.

To edit an existing risk profile, click the  button.

19.2.1 Adding a new rule

- To add a new rule, scroll down to the bottom of the screen and click the  button.
- Select the rule you want to add. For a list of available rules, see [Appendix 1: Apata 3D Secure Rules](#).

19.2.2 Adding a Conditional Rule

- To add a new rule, scroll down to the bottom of the screen and click the  button.
- Select the **Conditional** rule.
- Select an action for your rule. Options include:

Rule	Description
Accept	If rule condition is met, allow frictionless authentication.
Reject	If rule condition is met, reject the authentication.
Challenge	If rule condition is met, show Challenge screens.
Next	If none of the previous rule conditions are met, move on to the next rule.

- Configure the conditions which trigger the rule:
 - Click the **Add Rule** button.
 - Use the operator selector (e.g., AND, OR) to add multiple conditions.
 - Select a **Field Name**, **Operation** and **Value** for the condition. The value that can be selected or entered depends on the field name selected.
See the examples below:



Field Name	Operation	Value	Action Configured
Risk Score	Is	Low	Accept
MCC	Is	7995	Reject
Amount	Is greater than	200	Challenge

5. If you have multiple rules, you should order your rules in the order in which you want them to be checked. The system will move on to the next rule in the list, provided that the **Next** rule action has been specified. (If no Next rule action is specified, the final decision is returned (accept, reject or challenge).

Note: If the transaction does not meet the criteria of any rules in the risk profile created, the transaction will be challenged as a default behaviour. You can also set a SIMPLE rule as the last rule in the risk profile and set desired “Action” (example: Accept or Reject).

6. To delete a condition, click the  button.
7. To save your changes, click the  Update button.

Below is an example of a conditional rule. In this rule the Challenge action is triggered when the following conditions are met: *Amount if greater than 100 and risk score is HIGH.*

Match Action

CHALLENGE

No Match Action

NEXT

Conditions

AND

+ Add Rule

+ Add Group

Field Name

Amount

Operation

is greater than

Value

100

Field Name

Risk score

Operation

is

Value

HIGH

Figure 20: Example of a Challenge rule configuration

19.3 Viewing Challenge Methods

The Challenge method defines the type of Challenge options used to authenticate a cardholder during an online 3D Secure session. Examples include OTP SMS, OTP email and biometric. The Apata system provides a number of default Challenge options that can be selected as default for your programme. Please check with your Thredd 3D Secure Implementation Manager to determine which methods can be used with Thredd.

Note: If you require any changes to your configuration including adding new challenge methods, please speak to your Thredd 3D Secure Implementation Manager.



1. To view a list of challenge methods, select **Authentication > Challenge Methods** from the left-hand menu.

Challenge Methods

Create Challenge Method

#	Name	Type	Alias	Description	FinancialInstitutionName	Created	Updated	
1	Transaction History challeng...	TRANSACTION_HISTORY	transaction-history	Transaction History challeng...		Aug 16, 2023, 4:23:22 PM	Aug 16, 2023, 4:23:22 PM	
2	Email OTP Method	EMAIL_OTP	email-otp	Email OTP Method		Aug 16, 2023, 3:26:55 PM	Aug 16, 2023, 3:26:55 PM	
3	SMS OTP v2	SMS_OTP	smsotp			Sep 29, 2023, 3:42:17 PM	Sep 29, 2023, 3:42:17 PM	
4	OOB Method	DELEGATE_SCA_V1	oob			Aug 16, 2023, 4:31:14 PM	Aug 16, 2023, 4:31:14 PM	
5	My Challenge Method	SMS_OTP	sms	string		Aug 16, 2023, 4:21:55 PM	Oct 3, 2023, 12:10:40 PM	

Items Per Page 100

< 1 >

Jump to: 1

Figure 21: View Challenge Methods

2. To view details of a challenge method, click the  button.

Below is an example of a challenge method, using SMS OTP.

SMS OTP v2

Challenge Method details and application.

Created at: Sep 29, 2023, 3:42:17 PM
Updated at: Sep 29, 2023, 3:42:17 PM

Edit Challenge Method

FinancialInstitutionId423b566d-c9d0-4602-90d9-dea5206c3ab1

Id8bf1a6a1-b3fc-495c-a255-beef32e5008f

Aliassmsotp

NamesMS OTP v2

TypesMS_OTP

ChallengeInterfaceId8db8871a-ff37-4c46-80cf-aea15f8d9276

Retries1

Attempts1

Properties

Open Challenge Interface Locales

Locales

DEFAULT

Primary Challenge Interface

App HTML

Browser

Your Logo

4:29

Verify your payment using the code we sent to your phone number ending with:

Submit code

Resend code

Your payment of €1,000.00 to Test Merchant

Cancel payment

3D Secure (3DS) helps prevent fraud when using payment cards online

Figure 22: OTP SMS Challenge Method Example

A mock-up view of the Primary challenge screen is displayed in the right-hand pane. For details of how to specify text and logo changes, see [Configuration of 3D Secure Screens](#).

IMPORTANT: Each challenge method is assigned a unique system ID.

19.4 Viewing Card Programs

Apata's options for authentication at card program level enable you to set up different risk profiles, depending on the card BIN range. This is a useful option to enable you to assign different risk profiles to different types of cards, based on BIN range. For example, your issuer (BIN sponsor) may have assigned you with different BINs for Corporate cards versus Consumer cards, or separate BINs (BIN ranges in the EEA) for each of the countries in which you intend to issue cards.



1. To view a list of card programs, select **Authentication > Card Programs** from the left-hand menu.

Card Programs

Name, Description, Created, Updated, ...

Create Card Program

#	Name ↓↑	Description ↓↑	Choice Challenge Interface Id ↓↑	Created ↓↑	Updated ↓↑		
1	APAC programme - prepaid			Aug 11, 2023, 4:18:27 PM	Oct 2, 2023, 5:50:07 PM	Make Default	
2	UK programme - physical	Default Enabled Card Program create...		Aug 10, 2023, 2:36:01 PM	Oct 2, 2023, 5:49:55 PM	Default	
3	EU programme - virtual	EU programme - virtual		Sep 21, 2023, 3:20:23 PM	Sep 21, 2023, 3:20:23 PM	Make Default	
4	EU programme - physical			Aug 11, 2023, 4:17:41 PM	Oct 2, 2023, 5:49:20 PM	Make Default	
5	Pilot card programme			Oct 2, 2023, 12:20:52 PM	Oct 2, 2023, 5:49:40 PM	Make Default	
6	IntegraionTest1	4f8b7489-b9cd-4f48-a3b1-4e... string		Oct 4, 2023, 9:08:19 AM	Oct 4, 2023, 9:08:19 AM	Make Default	
7	US card programme	US card program		Oct 2, 2023, 5:57:20 PM	Oct 2, 2023, 5:57:20 PM	Make Default	

Figure 23: View Card Programs

If the Card Program is set to **Default**, it will automatically include all card ranges that are not already associated with another Card Program.

Note: To apply any changes to your card program setup, please raise a change request with your Thredd 3D Secure Implementation Manager.

2. To view details of a card program, click the button. Below is an example of a card program.

UK programme - physical (Default)
26c516e2-e675-41e2-83e7-5fb2aeba427c

Edit

Description: Default Enabled Card Program created when a Financial Institution is onboarded

Risk Profile: 9f6ffb78-aa6d-4ac0-814e-9c9e4219aa05

Card Ranges

Challenge Interfaces

Type ↓↑	Start ↓↑	End ↓↑	State ↓↑	PaymentAlgorithm ↓↑	NonPaymentAlgorithm ↓↑	Created ↓↑	Updated ↓↑	
RANGE	4123456720000000	4123456720000099	ENABLED	DS_ID_PAN	DS_ID_PAN	Aug 24, 2023, 9:41:15 AM	Sep 1, 2023, 6:36:00 PM	

Items Per Page 100

<

1

>

Figure 24: Card Program Example - UK Physical Cards

3. To view the Risk profile associated with the card program, click the button.
4. To view the card BIN ranges, status and other details associated with the card program, click the button.



20 Managing User Access

The **Access Management** menu on the **Apata Portal Dashboard** enables you to set up and manage user accounts. Options include:

- Viewing Users
- Viewing User Roles
- Viewing and Creating User Invitations

20.1 Viewing Users

1. To view a list of users, select **Access Management > Users** from the left-hand menu.

Users						
#	Email	FirstName	LastName	State	Created	Updated
1	avinash.m@thredd.com	Avinash	Parameswaran	ENABLED	Oct 3, 2023, 12:01:11 PM	Oct 3, 2023, 12:01:52 PM
2	jithin.kp@thredd.com	Jithin	KP	ENABLED	Sep 20, 2023, 12:28:09 PM	Oct 3, 2023, 12:20:00 PM
3	warren.singer@thredd.com	Warren	Singer	ENABLED	Oct 3, 2023, 9:00:02 AM	Oct 3, 2023, 2:13:48 PM
4	ramya.raj@thredd.com	Ramya	Rajan	ENABLED	Oct 3, 2023, 12:16:56 PM	Oct 3, 2023, 12:17:51 PM
5	arathy.pc@thredd.com	arathy	dev	ENABLED	Oct 3, 2023, 12:19:16 PM	Oct 3, 2023, 12:20:12 PM

Figure 25: View Users

2. To view details of a user, click the  icon.

20.2 Viewing User Roles

1. To view a list of available user roles, select **Access Management > User Roles** from the left-hand menu.

Roles						
#	Type	Name	FinancialInstitutionId	Description	Created	Updated
1	FI	Manager3	423b566d-c9d0-4602-90...		Sep 29, 2023, 5:19:44 PM	Sep 29, 2023, 5:19:44 PM
2	FI	View only	423b566d-c9d0-4602-90...		Oct 2, 2023, 12:58:09 PM	Oct 2, 2023, 4:45:50 PM
3	FI	Manager2	423b566d-c9d0-4602-90...		Sep 29, 2023, 5:18:11 PM	Sep 29, 2023, 5:18:11 PM
4	FI	Manager1	423b566d-c9d0-4602-90...		Sep 29, 2023, 5:17:36 PM	Sep 29, 2023, 5:17:36 PM

Figure 26: View User Roles

2. To view details of a user role, click the  icon.

Note: Your organisation will be provided with a preconfigured list of standard roles (Administrator, Analyst and Customer Service). You will be able to assign these roles to your users.

Note: If you require customised roles, please contact your Thredd 3D Secure Project Manager to discuss. This changes will be chargeable.



20.3 Viewing and Creating User Invitations

- 1. To view a list of users who have been invited to the Apata Portal, select **Access Management > Invitations** from the left-hand menu.

Invitations

Create User Invitation

AllActiveExpiredRevokedAccepted

Email Address	User Type	State	Created	Expires At	
aju.vijay@thredd.com	FI	ACTIVE	Sep 29, 2023, 7:37:46 AM	Oct 6, 2023, 7:37:46 AM	RevokeView
avinash.m@thredd.com	FI	ACCEPTED	Oct 3, 2023, 11:57:14 AM	Oct 10, 2023, 11:57:14 AM	View
ramya.rajan@thredd.com	FI	ACCEPTED	Oct 3, 2023, 12:08:12 PM	Oct 10, 2023, 12:08:12 PM	View
arathy.pc@thredd.com	FI	ACCEPTED	Oct 3, 2023, 12:07:09 PM	Oct 10, 2023, 12:07:09 PM	View
warren.singer@thredd.com	FI	ACCEPTED	Oct 2, 2023, 4:25:32 PM	Oct 9, 2023, 4:25:32 PM	View
jithin.kp@thredd.com	FI	ACCEPTED	Sep 29, 2023, 7:34:41 AM	Oct 6, 2023, 7:34:41 AM	View

Figure 27: View User Invitations

- 2. To filter the list of user invitations, select a status button: **All**, **Active**, **Expired**, **Revoked** and **Accepted**.
- 3. To view details of a user invitation, click the **View** button.
- 4. To revoke an invitation, click the **Revoke** button.
- 5. To create a new user invitation, click the **Create User Invitation** button.



21 Searching for Transactions

The Transactions menu on the [Apata Portal Dashboard](#) enables you to search for transactions.

- 1. To search for a transaction, select **Transactions** from the left-hand menu.

Transaction ID

DS Transaction ID

BIN

Card Search

Include Deleted Cards

Was Challenged

Was Frictionless

Merchant

Card ID

CardId

Equal

Search Merchant

Date

State

Reason

Error Code

Exemption

Protocol Version

Device Channel

From

X

All

All

All

All

All

All

to

X

search

Clear All

Figure 28: Search for Transactions

- 2. Enter the details you'd like to search on and click **Search**.

Refer to the table below for further details of search options.

Option	Description
Transaction ID	Search by Apata's ACS unique ID for the transaction.
DS Transaction ID	Unique transaction ID as provided by the directory server of the card scheme (payment network).
BIN	The Bank Identification Number (BIN) of the card (first 8 digits).
Card ID	Apata configured ID for the card that performed the transaction.
Include Deleted Cards	Note: Not applicable to Thredd clients.
Was Challenged	Check this option to include transactions where the cardholder was challenged.
Was Frictionless	Check this option to include transactions where the cardholder was not challenged (frictionless authentication).
Merchant	You can specify the name of the merchant to search for transactions linked to a specific merchant.
Date	Specify the start and end date range to search for transactions within a specific period.
State	Search by transaction status. Options include: Succeeded, Aborted, Failed, Error, Rejected, Timeout and Cancelled. For details see Appendix 6: Transaction Status .
Reason	Search by decline reason. For details see Appendix 6: Transaction Status > Decline Reasons .
Error Code	Search by transaction error code. For details see Appendix 6: Transaction Status > Error Codes .
Exemptions	Search by permitted acquirer exemptions. For details see Appendix 6: Transaction Status > Exemptions .
Protocol Version	Search by 3D Secure protocol version. Options include: <i>1.0.2</i> , <i>2.1.0</i> and <i>2.2.0</i> . Note: version 1.0.2 was discontinued in Oct 2022.
Device Channel	Search by the channel used during the authentication session. Options include: <i>App</i> , <i>Browser</i> and <i>Requestor Initiated</i> .



21.1 Viewing Transactions

The **Transactions** screen lists all transactions that match your search criteria. See the example below.

#	Id	CardId	MerchantName	External Id	State	Amount	Date	Reason	Error Code
1	7965...	8875f...	Amaz...		Succeeded	€1,234.23	Nov 20, 2023, 9:10:49 AM		
2	3b43c...	8875f...	Amaz...		Cancelled	€1,234.23	Nov 20, 2023, 9:10:06 AM	CANCELLED_VIA_CHALLENGE_PAGE	
3	f7ea3...	8875f...	Amaz...		Error	€1,234.23	Nov 20, 2023, 8:38:41 AM		webhook_call_failed
4	72723...	8875f...	Amaz...		Error	€1,234.23	Nov 20, 2023, 7:56:59 AM		webhook_call_failed
5	4e6af...	8875f...	Amaz...		Error	€1,234.23	Nov 20, 2023, 7:53:27 AM		webhook_call_failed
6	b828f...	8875f...	Amaz...		Error	€1,234.23	Nov 20, 2023, 7:50:47 AM		webhook_call_failed
7	600ef...	8875f...	Amaz...		Error	€1,234.23	Nov 20, 2023, 7:48:44 AM		webhook_call_failed

Figure 29: Viewing Transactions

Note: If the Merchant Simulator option has been enabled for your organisation, you can use the **Transaction Simulation** toggle button (which will appear at the top-right of the **Transactions** page) to view simulated transactions. See [Viewing Simulated Transactions](#).

- To view details of a specific transaction, click the  button. See the example below.

Transaction 7965bf31-cfe7-4363-abe5-9f60b2a39d81

Amazon

created on: Nov 20, 2023, 9:10:49 AM

update on: Nov 20, 2023, 9:11:21 AM

Protocol v2.1.0 Lang: EN-E

Was Challenged

Was Frictionless

Was Presented Choice

Did Make Choice

Did Whitelist

financialInstitutionId4462b1f4-7462-43fb-adfd-dea478666b8e

cardId8875fc70-c25e-4caf-b27c-d8f693c99242

cardExternalId108980508

dsTransactionId254a5d3a-e251-4fc0-915a-51c01d3420a7

deviceChannelBROWSER

stateSUCCEEDED

categoryPAYMENT

transactionTypePAYMENT

purchaseCurrencyEUR

purchaseAmount123423

Card Link Event9:10:48 am

Areq9:10:49 am

Eval Log9:10:49 am

Ares9:10:49 am

Creq9:10:49 am

Challenge Html9:10:49 am

Browser Action9:11:21 am

Rreq9:11:21 am

Figure 30: Viewing a Transaction's Details

Viewing Cardholder Interaction Status

- To view details of the system interaction with the cardholder during the 3D Secure session, mouse-hover over the relevant icons: **Was Challenged**, **Was Frictionless**, **Was Presented Choice**, **Did Make Choice** and **Did Whitelist**. If any of these conditions occurred, the status is indicates as *true*.

Viewing Details of Message Types

- To view details of the message types that have been sent during the 3D Secure session between the Card Scheme (payment network), the ACS (Apata) and the cardholder's browser, in the right-hand pane of the screen, click the expand button next to the relevant message type.



For example, to view the Challenge HTML message sent to the cardholder, click the  icon in the **Challenge Html** row. This displays a copy of the Challenge screen that was shown to the cardholder:

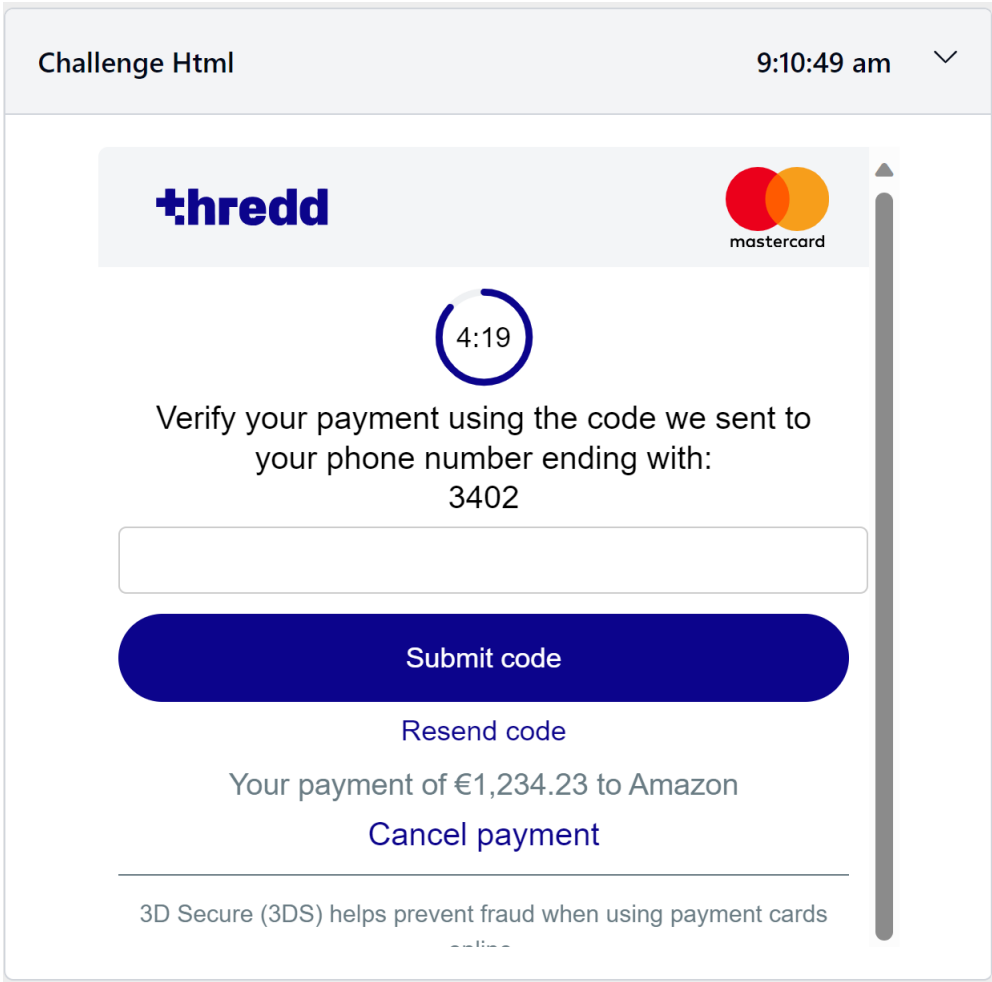


Figure 31: Example of the Challenge HTML Screen



22 Creating Reports and Queries

The **Analytics** menu on the **Apata Portal Dashboard** enables you to create custom reports and build queries on you 3D Secure transactions. Reports can be sent to a list of email addresses or uploaded to an SFTP Server.

22.1 Viewing and Generating Reports

- 1. To view a list of available reports, select **Analytics > Reports** from the left-hand menu.

Reports

Report Builder

#	Name	Type	QueryId	Description	Created	Updated	Last Executed	
1	Daily Status Report	CUSTOM_V1	9f6eacdc-c3df-4a66-8acf-4d...	List of daily transaction statu...	Oct 4, 2023, 9:08:35 AM	Oct 4, 2023, 9:08:35 AM		
2	Transaction status report	CUSTOM_V1	9f6eacdc-c3df-4a66-8acf-4d...	Report showing all EMV 3D...	Aug 14, 2023, 2:35:11 PM	Sep 14, 2023, 11:53:28 AM	Oct 4, 2023, 1:01:00 AM	

Items Per Page 100

< 1 >

Jump to: 1

Figure 32: Viewing Reports

- 2. To view information about the report, click the icon.
- 3. To change details in the report, click the **Edit** button. After you have made your changes, click **Update Report**.
- 4. To generate a new report, click the **Report Builder** button.
- 5. Add a **Name** and **Description** to your report, select the type of **Query** and report **Schedule** (Daily, Weekly, Monthly).
- 6. If you want to deliver reports to an email address:
 - a. Select the **Enable automatic report delivery** option and enter the user's email address.
 - b. To add additional email addresses, click the **+ Email** button.

Note: SFTP configuration is currently not available

Report Builder

Save Report

Name

Daily Status Report

Description

List of daily transaction status's

Query

EMV 3DS Transaction Status query

Schedule

Daily

Enable automatic report delivery

☒

Email Delivery

SFTP Config

+ Email

warren.singer@thredd.com

Figure 33: Report Builder

The report is added to the list of available reports. (If you cannot see it in the list, refresh the page.)



22.2 Viewing and Building Queries

1. To view a list of available transaction queries, select **Analytics > Queries** from the left-hand menu.

Queries

Query Builder

#	Name	Description	Schedule	DeliveryDetails	Tags	Created	Updated	
1	EMV 3DS Transaction Status ...	Query for generating transac...				Aug 14, 2023, 2:21:15 PM	Aug 14, 2023, 5:09:48 PM	
2	Custom query	Custom query				Oct 4, 2023, 11:21:28 AM	Oct 4, 2023, 11:21:28 AM	

Items Per Page: 100

<

1

>

Jump to: 1

Figure 34: Viewing Queries

2. To view details of a query, click the icon.
3. To build a new query, click the **Query Builder** button.



23 Viewing BIN and Card Ranges

The **BIN & Card Ranges** menu on the **Apata Portal Dashboard** enables you to view details of BIN and cards ranges that have been set up in the system.

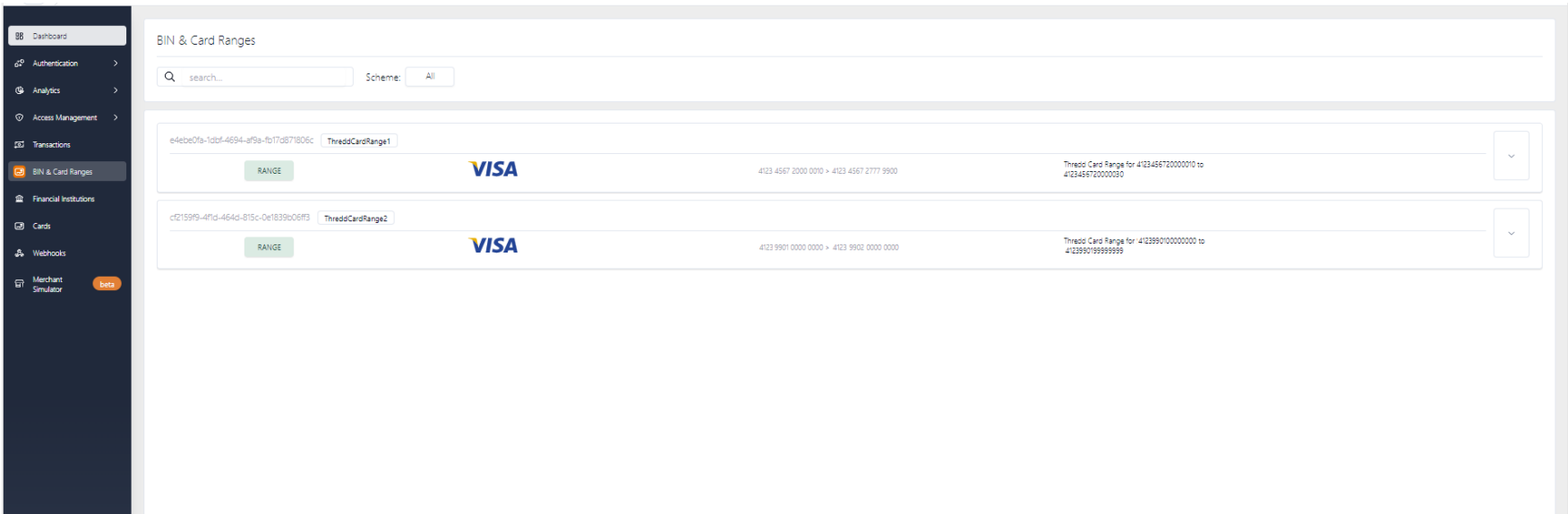


Figure 35: View BIN & Card Ranges

To view details of a card range, click the  icon. See the example below.

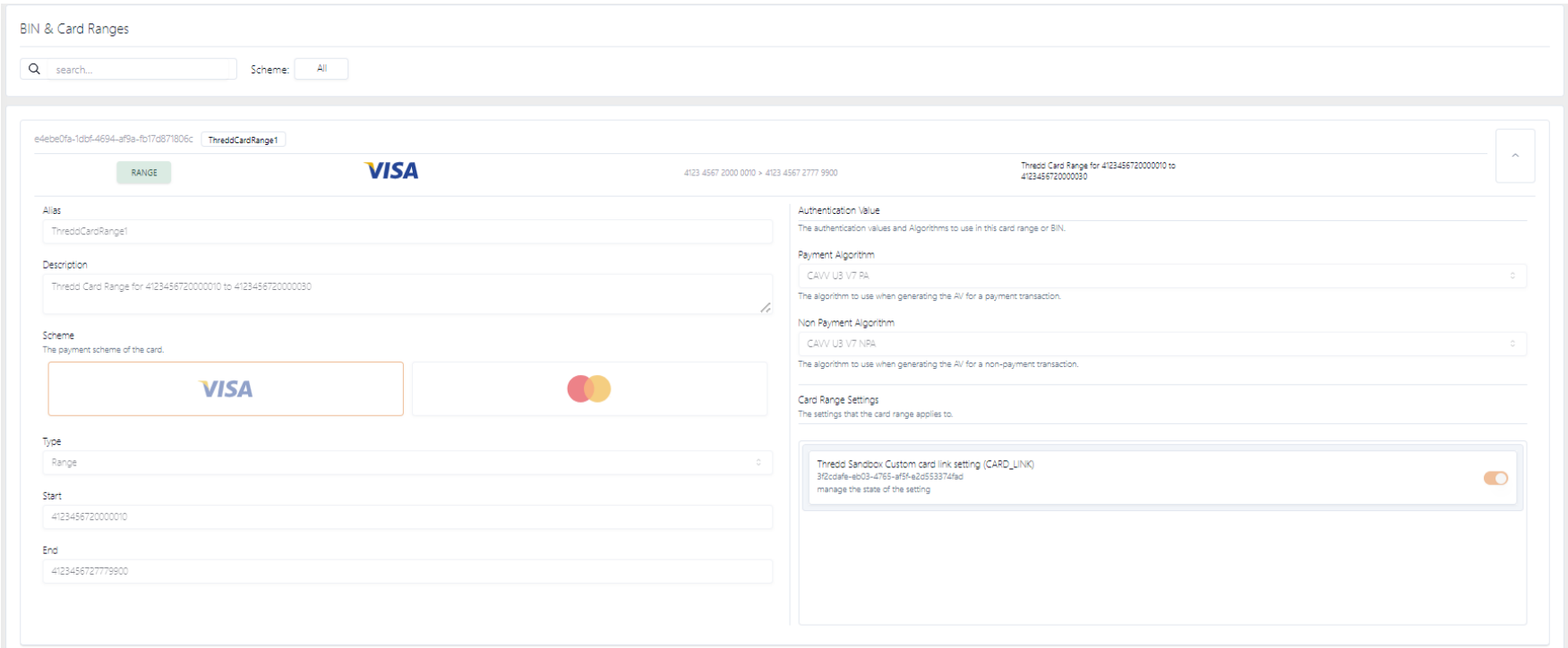


Figure 36: View Details of a BIN & Card Range

Note: Card range details shown in this section are dummy examples.



24 Using the Merchant Simulator

The Merchant Simulator menu on the [Apata Portal Dashboard](#) enables you to run simulated 3D Secure transactions. You can use simulated transactions to test the outcome of your cardholder authentication rules when applied to different types of card usage scenarios.

Note: This option will only be visible if enabled for your organisation. For details, please check with your 3D Secure project manager.

24.1 Running a Simulated Transaction

- 1. To run a simulated transaction, select **Merchant Simulator** from the left-hand menu.

Merchant Simulator

BasicAdvanced

Test Cards

Add Test Card

PAN

Use the PAN field when a card link setting is configured and card details need to be fetched from the external system.

Merchant

Merchant NameMerchant IDMerchant Country

Choose country

Amount

AmountCurrency

Euro (EUR - €)

Figure 37: Merchant Simulator screen

- 2. Enter the details of the 3D Secure transaction you want to simulate. See [Transaction Simulation Fields](#).
- 3. Scroll down to the bottom of the page and click **Submit Test Transaction**.

24.1.1 Transaction Simulation Fields

Refer to the table below for details of transaction simulation fields.

Field	Description
Test Cards	Ignore this field. it is not relevant to Thredd programmes.
PAN	Enter the full Primary Account Number (PAN) of the card you want to test.
Merchant	Enter details of the merchant requesting cardholder authentication: Merchant name , Merchant ID and Merchant Country .
Amount	Enter the Amount and Currency of the transaction.
Protocol Version	Select the 3D Secure protocol version (e.g., 2.1.0 or 2.2.0). For more information, see Support for 3D Secure Versions .
Challenge Preference	Select the required challenge method from the drop-down:



Field	Description
	No preference - 01 No challenge requested - 02 Challenge requested (3DS Requestor preference) - 03 Challenge requested (Mandate) - 04 No challenge requested (transactional risk analysis is already performed) - 05 No challenge requested (Data share only) - 06 No challenge requested (strong consumer authentication is already performed) - 07 No challenge requested (utilise whitelist exemption if no challenge required) - 08 Challenge requested (whitelist prompt requested if challenge required) - 09
Device	Select the device type used for the 3D secure session. Options are: <i>Browser</i> or <i>App</i> .
Alias	Provide a name for your test transaction.

24.1.2 Viewing Simulated Transactions

You can use the **Transactions** menu to search for your simulated transactions.

Note: This option will only be visible if enabled for your organisation. For details, please check with your 3D Secure project manager.

- To view simulated transactions, click the **Transaction Simulation** toggle button (at the top-right of the **Transactions** page).

Transaction Simulation

When enable, You can search for simulated transactions by using the filters below.



Appendix 1: Apata 3D Secure Rules

You can use the Apata Portal to create risk profiles to trigger an Accept, Reject or Challenge outcome on the Apata system (see [Managing Authentication Rules](#)).

See below for a list of available rules that can be included in a risk profile.

Rule	Description
Acquirer Exemption	Permits exemptions requested by the merchant acquirer.
Max Frictionless Transactions	The maximum number of transactions with frictionless authentication (no challenge) allowed before Challenge screens are shown to the cardholder when attempting an ecommerce transaction.
Conditional	Applies the configured action if the configured conditions are met. See Adding a Condition Rule .
Secure Corporate Payment	Permits the Secure Corporate Payment Exemption to be used.
Merchant Initiated	Exemption applied to a repeat transaction (i.e., repeat payment for fixed or variable amount, and fixed and variable interval, to the same payee, governed by an agreement to these payments). The Merchant must flag the transaction as merchant initiated. The first transaction, to set up the transaction, must be authenticated. An example of this type of transaction is a Card on File (CoF) transaction, at a store such as Amazon.
Whitelist	Exempts the transaction if the cardholder has added the merchant to the Trust List of allowed merchants.
Non Payment	Permits exemption from 3D Secure for a transaction type classed as a non-payment transaction (e.g. adding card to a digital wallet, adding a card on file).
Max Cumulative Frictionless Spend	The maximum cumulative total (in default rule currency) up to which a frictionless authentication is allowed (the cardholder will not be presented with any challenge screens).
PSD2 Low Value	Applies the low value exemption under the PSD2 rules, if the following conditions are met: • Transaction value is less than 30.00 EUR • Cumulative spend since last challenge is less than 100 EUR • Number of transactions since last challenge is less than 5
One Leg Transaction	Used for handling transactions where the issuer (BIN sponsor) or acquirer is not within EEA; in this case Strong Customer Authentication (SCA) is exempted as one leg out.
Recurring Payment	Exemption applied to a recurring transaction (i.e., repeat payment for fixed amount, such as a subscription, to the same payee). The Merchant must flag the transaction as recurring. The first transaction, to set up the recurring payment, must be authenticated.



Appendix 2: OTP Message Templates

This section provides examples of the message templates for OTP SMS.

OTP SMS

Note: If using bespoke text, we commend you keep your message brief. Otherwise it will be split into multiple parts, which are sent separately.

Default Template (Full)

The template can contain OTP, Card Number (last 4 digits), Currency, Amount and Merchant Name:

English:{{OTP}} is the One Time Passcode required for completing a purchase of {{CUR}} {{Amount}} at {{MerchantName}} with the last four digits of your card ending in {{CardNumber}}.
Please use the One Time Passcode to complete the transaction.

Note: The {{CardNumber}} is the last 4 digits of the card number.

Shortened Template

The template can only contain the OTP and card number:

{{OTP}} is the 3DS OTP from card ending by {{CardNumber}}.
Please use the OTP to complete the transaction.



Appendix 3: KBA Questions

If you are using *Knowledge Based Authentication* (KBA), when you set up the KBA credential for a card, you can link to one of the following default security questions, set up in the Thredd database.

KBA ID	KBA Question
1	What was your first pet's name?
2	What is your maternal grandmother's maiden name?
3	What is the name of your favourite childhood friend?
4	What was the make of your first car?
5	In what city or town did your mother and father meet?

Language Support for KBA Questions

If you offer your card products in languages other than English, you can provide Thredd with your translated KBA questions. Any additional languages for your card products must also be configured for the relevant BIN/sub-BINs at Apata. Thredd will create a separate KBA ID for your non-English questions. For example:

KBA ID	KBA Question	Language
1	What was your first pet's name?	English
6	Quel était le nom de votre premier animal?	French
7	Wat was de naam van je eerste huisdier?	Dutch
8	Wie hieß Ihr erstes Haustier?	German
9	你的第一个宠物叫什么名字?	Chinese (Simplified)

For an example, see [Translated KBA Question Example](#).

KBA Question Examples

Below is a code snippet example, showing the use of the KBA credential in the 3D secure Card enrolment Thredd API or Cards API. For details, see [Using the Card Enrolment API](#).

```
<hyp:Credentials>
  <hyp:Credential>
    <hyp:ID>0</hyp:ID>
    <hyp:Type>KBA</hyp:Type>
    <hyp:Value>4</hyp:Value>
    <hyp:KBA_Answer>Skoda</hyp:KBA_Answer>
    <hyp:KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
  </hyp:Credential>
```

Notes

Example shows KBA ID with a [Value](#) of 4. The answer stored in the Thredd database will be Skoda:

```
<hyp:Type>KBA</hyp:Type>
<hyp:Value>4</hyp:Value>
<hyp:KBA_Answer>Skoda</hyp:KBA_Answer>
<hyp:KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
```



Adding Multiple KBA Questions

If you enrol a card with multiple question and answer pairs, then during the online authentication session Thredd will randomly select questions and pass these questions to Apata in real-time for displaying to the cardholder. The number of questions selected will depend on what has been configured in the **KBA number of questions to answer** field in the PSF (see [Completing your 3DS Product Setup Form > Client Information tab](#)). Below is an example of a credential array, where the card is enrolled with two KBA questions:

```
<hyp:Credentials>
  <hyp:Credential>
    <hyp:ID>0</hyp:ID>
    <hyp:Type>KBA</hyp:Type>
    <hyp:Value>4</hyp:Value>
    <hyp:KBA_Answer>Skoda</hyp:KBA_Answer>
    <hyp:KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
  </hyp:Credential>
  <hyp:ID>0</hyp:ID>
  <hyp:Type>KBA</hyp:Type>
  <hyp:Value>5</hyp:Value>
  <hyp:KBA_Answer>London</hyp:KBA_Answer>
  <hyp:KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
</hyp:Credential>
```

Translated KBA Question Example

Below is an example of a KBA credential for a card where the default language of the card product is French:

```
<hyp:Credentials>
  <hyp:Credential>
    <hyp:ID>0</hyp:ID>
    <hyp:Type>KBA</hyp:Type>
    <hyp:Value>6</hyp:Value>
    <hyp:KBA_Answer>Amélie</hyp:KBA_Answer>
    <hyp:KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
  </hyp:Credential>
```



Appendix 4: 3D Secure Test Merchants

Below is a list of online merchants who are enrolled in the 3D Secure service, who you can use for your 3D Secure pilot testing.

Note: This list is provided for reference only and is subject to change. For more information, please contact your 3D Secure Implementation Manager.

Location	Merchants	Additional Merchants
Australia	www.amazon.com.au	
Belgium	http://www.sncb.be https://www.nike.com/be	https://www.tuifly.be/ https://delijn.be
France	https://www.leboncoin.fr/ https://www.disneylandparis.com/ http://www.laposte.fr http://www.ticketmaster.fr	https://www.cofidis.fr https://boutique.canalplus.com/ https://www.vertbaudet.fr/
Germany	https://www.amazon.de https://www.zalando.de	https://www.nintendo.de/ http://www.shop.deutschepost.de
Italy	http://www.trenitalia.com https://www.amazon.it	http://www.sisal.it https://www.windtre.it/
Malaysia	shopee.com	
Netherlands	https://www.youuniqueproducts.com/ http://iherb.com https://www.ns.nl	https://www.amazon.nl http://www.thuisbezorgd.nl/
New Zealand	www.thewarehouse.co.nz	
Spain	https://www.crtm.es http://www.edreamsodigeo.com/	http://www.packlink.es https://www.loteriasyapuestas.es
Singapore	www.lazada.sg	
UK	Just Eat.Co.UK Ltd Screwfix Holland And Barrett H&M Wirex Ltd	ASDA Groceries John Lewis Lolita Bakery Toolstation Ltd Friday Ad Ltd



Appendix 5: Transaction Status

A transaction in Apata will conclude with one of the following states:

State	Description
Succeeded	The transaction was approved by the ACS and the result was returned to the directory server (payment scheme) successfully. A transaction in the SUCCEEDED state may have been approved frictionlessly or the cardholder completed SCA successfully. In the event that the challenge was approved frictionlessly, the exemption field will be set. See Exemption Values .
Failed	The cardholder failed to complete the challenge for SCA. If the state is FAILED then the reason field will be populated by one of the following: - CHALLENGE_ATTEMPTS_EXCEEDED – The number of attempts that a cardholder may perform has been exceeded. For example, the cardholder entered the OTP received over SMS incorrectly 3 times (Program Manager can set the challenge attempts to a maximum of 9 times) - CHALLENGE_RETRIES_EXCEEDED – The number of times that a challenge can be retried has been exceeded for the cardholder. For example, the cardholder requested that the SMS be resent too many times.
Error	An error occurred during the processing of the transaction. If the state is ERROR then the errorCode field will be set. The errorMessage field may also be set to provide more information on the cause of the error. See Error Codes .
Timeout	The cardholder failed to complete the challenge within the allotted period of time configured (as specified in the Time to complete authentication field; see Completing your 3DS Product Setup Form).
Aborted	The 3DS requestor (usually a merchant) sent an authentication request (AReq), but never followed up with a challenge request (CReq) when Apata determined that a challenge was required.
Cancelled	The transaction was cancelled either by the cardholder or by the 3DS requestor (usually a merchant). If the state is CANCELLED then the reason field will be set: - CANCELLED_VIA_CHALLENGE_PAGE – the cardholder selected the cancel option on the challenge page displayed in their browser or app. - CANCELLED_OUT_OF_BAND – the cardholder could not complete the Biometric or Out of Band authentication. - CANCELLED_BY_REQUESTOR – the transaction was cancelled by the 3DS requestor (typically a merchant). This can occur when an error occurs on the merchant side for example.
Rejected	The ACS determined that the transaction could not proceed. This may be due to the card being blocked or TRA (Transaction Risk Analysis) determining that the transaction is too risky. Possible reason values are: - CARD_DISABLED – The card has been blocked in the Apata system. - LOW_CONFIDENCE – The risk engine determined that the transaction was too risky to continue.

Exemption Codes

Value	Description
LOW_VALUE_PAYMENT	For cards issued where PSD2 applies (EEA/UK) the low value payment exemption described under PSD2 was applied. This exemption can be applied if the following conditions are met: - The value of the payment is less than €50. If the transaction amount is not denoted in Euro, it will be converted to Euro using live exchange rates. - The cumulative spend of all transactions for the card since the last application of SCA cannot exceed €100.



Value	Description
	The number of transactions since the last application of SCA cannot exceed 5.
LOW_RISK	The transaction has been determined to be low risk using transaction risk analysis (TRA) performed by either Apata's risk engine or a customer specified risk engine. The maximum value that may be exempted using TRA is determined by the institution's fraud levels.
WHITELISTED	The cardholder previously opted to add the merchant to their Trust List of allowed merchants. This exempts future transactions for that merchant from challenges. Note: SCA must be performed in order to add a merchant to the Trust List.
RECURRING	The transaction is a fixed, recurring payment for a particular merchant and the first payment of the recurring transaction was challenged. This allows subsequent payments for the same amount and the same merchant to be exempted from SCA.
ACQUIRER_EXEMPTION	The merchant has requested an exemption from SCA as they have already applied either transaction risk analysis (TRA) or performed SCA.
SECURE_CORPORATE_PAYMENT	The transaction falls under the secure corporate payment exemption as outlined by PSD2.
ONE_LEG_TRANSACTION	The transaction has been exempted under PSD2's one-leg transaction exemption. This exemption may be used when the acquirer is outside of the EEA.
MERCHANT_INITIATED	The transaction was exempted as the request was initiated by the merchant. In this case the cardholder is not present and as a result cannot perform a challenge.

Decline Reasons

Reason	Description
Card disabled	The card has been disabled. Note: Not applicable to Thredd clients.
Card expired	The card has expired. Note: Not applicable to Thredd clients.
Card not Enrolled	The card is not enrolled in 3D Secure authentication.
Challenge Attempts Exceeded	The number of Challenge attempts configured for this Challenge Method has been exceeded (e.g., entering an incorrect OTP or KBA answer too many times).
Challenge Retries Exceeded	The number of Challenge retries configured for this Challenge Method has been exceeded (e.g., asking for the OTP to be resent too many times).
Low Confidence	The risk engine determined that the transaction was too risky to continue.
Required Details Missing	The transaction was missing mandatory details required for authentication.
Risk Engine Error	There was an error on the Apata risk engine.



Error Codes

Refer to the table below for a list of error codes.

State	Description
ds_error	The directory server (card scheme) returned an error when the Apata Access Control Server (ACS) attempted to report the success of the transaction.
client_error	The 3DS requestor (typically a merchant) experienced an error on their side and they reported the error to the ACS.
validation_error	One of the 3DS messages received by the ACS was invalid according to the 3DS protocol.
decoupled_not_supported	A decoupled transaction (valid only under 3DS 2.2+) was required, but the challenge method selected for the card does not support decoupled challenges.
non_payment_not_supported	The ACS has been configured not to support non-payment transactions, but a non-payment transaction was received.
card_not_enrolled	The card does not exist in the Apata ACS.
webhook_call_failed	The webhook call from the Apata ACS to Thredd failed.
sms_send_failed	The sending of the SMS to the cardholder failed.
invalid_config	The transaction cannot be completed due to invalid or incomplete configuration of the solution.
internal_server_error	Any error not classified above.



Appendix 6: Biometric/OOB Fields

This section provides details of the fields used in Biometric/OOB message requests and responses.

DelegateSCANotification and DelegateSCACancelNotification Message Fields

Below are details of the fields in the [DelegateSCANotification](#) and [DelegateSCACancelNotification](#) requests which Thredd sends to your systems. For more information, see [Initiating a Biometric Session](#).

Field	Description	Data type	Length	Status
NotificationId	Unique key of the message notification.	String	256 characters	Required
PubToken	Thredd 9-digit public token linked to the card.	BigInt	Up to 9 characters	Required
DelegateMethod	This is the method in which the program manager needs to contact the cardholder for approving or declining an authorisation. In this case, it is a push notification.	String	20 characters	Required
FinancialInstitutionId	Unique identifier defined for the Program Manager in Apata.	String	36 characters	Required
Language	Language setting of the device performing the transaction in BCP 47 format. For example: en-EN (English).	String	Up to 5 characters	Optional
DelegateScald	Unique alpha-numeric identifier for tracking the delegated authentication session.	String	36 characters	Required
CardScheme	The card scheme (payment network) being used: <i>MasterCard</i> or <i>Visa</i> .	String	Up to 20 characters	Optional
CreatedMode	This field indicates how the token was enrolled into 3D-Secure. This is indicated through one of the following codes: – GA Thredd auto-enrolment process. – PM -The Program Manager calling the Thredd Hyperion API Credential Call.	String	2 characters	Optional
Device	Details of the device of the cardholder when the transaction is initiated.	Object		Required
Channel	Device channel in which the transaction is initiated (App or Browser).	String	Up to 20 characters	Optional
Ip	IP address of the device used to initiate the transaction.	String	Up to 20 characters	Optional
Language	Language setting of the device performing the transaction in BCP 47 format. For example: en-EN (English).	String	Up to 5 characters	Optional
MerchantInfo	Provides details of the merchant requesting the authentication	Object		Optional



Field	Description	Data type	Length	Status
Id	Unique identifier of the merchant initiating the authentication request. This is assigned by the acquirer.	String	64 characters	Required
Name	Merchant name.	String	Up to 64 characters	Required
Country	Country code of the merchant. This value is the 3-digit number format (e.g., 840).	String	Up to 3 characters	Optional
Url	URL or name of the merchant's website or app.	String	Up to 2048 characters	Required
ChallengePreference	Challenge preference indicated by the merchant in the Authentication Request (AReq).	String		Optional
RedirectAppUrl	For app-based transactions only. This is the callback URL for the merchant's app. Your authentication app should use this to redirect the cardholder back to the checkout page on the merchant app once they have authenticated. ⁸ Note: If this field is empty, your app does not need to initiate a callback to the merchant's app.	String	Up to 256 characters	Optional
TransactionInfo	Provides details of the transaction for which the authentication is being requested.	Object		Optional
Type	Type of transaction. For example: <i>payment</i> or <i>non-payment</i> .	String	Up to 20 characters	Required
ProtocolVersion	3D Secure protocol version being used, for example, 2.2.0. For details of supported versions, see Support for 3D Secure Versions .	String	Up to 5 characters	Required
Channel	The channel in which the transaction is initiated (App or Browser).	String	Up to 20 characters	Required
DsTransactionId	Unique alpha-numeric transaction identifier provided by the Card Scheme's directory server. This helps to identify a transaction.	String	36 characters	Optional
Date	Unix Epoch timestamp in seconds.	Int	10 characters	Required
ChallengeAt	Unix Epoch timestamp in seconds of when challenge occurred.	Int	10 characters	Required
ChallengeExpiresAfter	The TTL(Time-To-Live) for the challenge.	Int	3 characters	Required
ChallengeExpiry	Unix Epoch timestamp in seconds for when challenge expires.	Int	10 characters	Required
ChallengeMethod	The Challenge method for authentication.	String	20 characters	Required

⁸In the challenge flow, the merchant app, through the 3DS software development kit (SDK), interacts with the Access Control Server (ACS) and declares its URL, thus enabling the authentication app to call the merchant app after the OOB authentication has occurred.



Field	Description	Data type	Length	Status
	For a Biometric or Out of Band session, this is a push-confirmation.			
Amount	Transaction amount in minor currency units (for example, 1000 for \$10.00).	String (Numeric)	64 characters	Required
Currency	Provides details of the currency.	Object		Required
Code	3-digit numeric ISO 4217 currency code (e.g., EUR, USD, JPY).	String	3 characters	Required
Exponent	Exponent for formatting the given ISO 4217 currency code. For example: 2. (Most currencies have an exponent of 2, which gives two digits after the decimal point, for example: 199.99.)	String (Integer)	1 character	Required
Recur	Provides details of a recurring payment that is set up.	Object		Optional
Frequency	The frequency with which the payment is repeated (in days). For example: 30 (repeats every 30 days).	String	8 characters	Optional
EndRecur	The date at which the recurring payment expires, in YYYY-MM-DD format. For example: 20241230 (30 December 2024).	String	8 characters	Optional
Install	The number of instalments. For example, 5 indicates that 5 additional payments after the first payment.	String	Up to 8 characters	Optional
DelegateStatus	Status of the DelegateSCANotification request. This is set to either Active or Cancelled.	String	10 characters	Required

DelegateSCAValidation Message Fields

Below are details of the fields in the [DelegateSCAValidation](#) message which you should use to notify Thredd of the result of the Biometric/OOB session. For more information, see [Notifying Thredd of the Result of the Biometric Session](#).

Field	Description	Data type	Length	Status
NotificationId	Unique key of the message notification.	String	256 characters	Required
PubToken	The 9-digit Thredd public token linked to the card (must be copied from the DelegateSCANotification request).	BigInt	9 digits	Required
DelegateScald	The unique alpha-numeric identifier of the notification request (must be copied from the DelegateSCANotification request).	String	36 characters	Required
PmReferenceId	Program Manager Reference ID for the Biometric/Out of Band transaction. This is defined by the Program Manager.	String	Up to 36 characters	Optional



Field	Description	Data type	Length	Status
Status	One of the following status values must be returned: - SUCCESS - the cardholder was successfully authenticated. - FAILURE - the cardholder could not be successfully authenticated.	String	Up to 20 Characters	Required

Thredd Response

Below are details of the Thredd response to your [DelegateSCAValidation](#) message:

Field	Description	Data type	Length	Mandatory / Optional
PubToken	Thredd 9-digit Thredd public token linked to the card.	Bigint	9 characters	Required
DelegateScald	A unique identifier for each DelegateSCANotification request.	String	36 characters	Required
PmReferenceld	Program Manager Reference ID for the Biometric/Out of Band transaction. This is defined by the Program Manager.	String	Up to 36 characters	Required
Status	The authentication status: - SUCCESS - the 3DS result was received before the timeout period - TIMEOUT - the 3DS result was received after the timeout period. - ERROR - In case of any internal technical failures. - FAILURE - In case of any validation failures.	String	Up to 20 characters	Optional
Error		Object		
ReferenceNumber	Thredd reference number for the error. Used by Thredd for referencing purposes. Used for ERROR status only.	String	Up to 15 characters	Optional
Description	Short description of the error. Used by Thredd for referencing purposes. Used for ERROR status only.	String	Up to 50 characters	Optional



General FAQs

This section provides answers to frequently asked questions.

The 3D Secure Service

Q. How does the 3DS authentication affect authorisation?

3DS authentication happens before payment authorisation. If the cardholder passes authentication, the transaction is sent to Thredd for authorisation: either Thredd or your systems authorise, depending on whether the card balance is maintained by Thredd or on your systems. (This is the following EHI modes: Gateway Processing (mode 1), Cooperative Processing (mode 2), Gateway Processing with STIP (mode 4) and Gateway Processing with STIP (mode 5).

If the cardholder does not pass 3DS authentication, the transaction will not reach Thredd for authorisation. The transaction will not be visible in Smart Client.

Q. What versions of 3D Secure are available and will Apata work with all of them?

There are two current versions of 3D Secure: EMV 3DS 2.1 and 2.2.

We are awaiting finalised roll-out details of 2.3 from EMVCo. See the [EMVCo website > Enhancing the 3D Secure Specifications](#).

The rules you set up on the Apata Portal apply to both EMV 3DS 2.1 and 2.2. Both versions work with all the authentication types available within 3D Secure (OTP SMS or Biometric/In App).

For more information, see [Support for 3D Secure Versions](#).

Q. Where can I find out more background information about 3D Secure?

The [EMVCo website](#) provides detailed specifications for anyone implementing a 3D Secure project. This includes information not covered in the Thredd guides, such as authentication message flows between Issuer (BIN sponsor), ACS provider and merchant (PReq, PRes, AReq, ARes), and specific internal message fields that may be passed or validated (e.g., CAVV/ AAV).

Starting a 3D SecureProject

Q. What are the steps in an 3D Secure project?

For details, see [Steps in a 3D Secure Project](#).

Q. Can we use a dynamic IP address cloud environment for REST-based API calls?

No, Thredd are unable to handle dynamic IP addresses behind the fixed DNS name.

Testing

Q. How do we test 3D Secure authentication?

Testing can start once your requirements are built and released to the UAT environment, and you have successfully set up your network connection and enrolled test cards.

Thredd provides a UAT environment, where you can use the Apata Merchant Simulator to test transactions. See [Completing UAT Testing](#).

Q. How do we test 3D Secure in Production?

When you have completed testing in the UAT environment, Thredd will set up your products in the production environment and you can start pilot testing. This works as follows:

- You can use the Card Create web service ([Ws_CreateCard](#)) to create pilot cards in the production environment. For details, refer to the Thredd Web Services Guide.
If you are using Thredd's Cards API, for similar create card functionality, see the [Cards API Website](#).
- Your issuer (BIN sponsor) must enrol your pilot card ranges at the card scheme (payment network).
- Thredd activate your products for 3D Secure , and you enrol your cards in 3D Secure by calling the 3D Secureweb service ([Ws_AddUpDelCredentials](#)) or the [Create 3DS Credentials](#) Cards API. See [Using the Card Enrolment API](#).



- You need to set rules in the Apata Portal to challenge transactions, so transactions are authenticated.
- Once the Scheme confirms that the pilot cards are live, you can start using your pilot cards: online transactions with 3DS merchants will route through Apata.

Q. Can we use the Thredd Card Transaction System (CTS) to test a 3D Secure transaction?

No, the Thredd CTS system does not currently have a connect to Apata and cannot be used for this purpose. Note that the e-commerce transaction option on the Thredd CTS system does not include any 3D Secure authentication elements.

If you want to test your 3D Secure transactions, you can use the Merchant Simulator in the Apata Portal. See [Completing UAT Testing](#).

3D Secure Card Enrolment

Using Cards API

Q. How can I enrol cards in 3D Secure and manage them using Cards API?

For details, see the [Cards API Website](#).

Using Web Services

Q. Which web services do I use to enrol cards in 3D Secure?

When using the Apata 3D Secure service, you only need to use a single a web service ([Ws_AddUpDelCredentials](#)) for enrolling cards and for editing and deleting 3D Securerecords. See [Using the Card Enrolment API](#).

Q. What is the Web Service WSDL file format and content?

The SOAP web services WSDL is available here:

<https://ws-uat.globalprocessing.net:13682/service.asmx?WSDL>

Q. Can I auto-enrol all cards in 3D Secure 3D Secure?

Yes, Thredd can auto-enrol your cards.

Note: Auto-enrolment may not be available for all BINs and card products.

There are two options for auto-enrolment, set up per credential type: *Initial Load* and *Continuous*. For details, see [Completing your 3DS Product Setup Form](#).

Note: You must ensure that both existing and new cards have the information required for 3D Secure in Smart Client, such as a valid mobile phone number to use for OTP authentication.

Note: You still need to use the 3D Secure Thredd API or Cards API to manage your cardholder records (e.g., to update the linked cardholder mobile phone number or delete a card from 3D Secure authentication).

Q. How can I check if a card is enrolled in 3D Secure?

You can use the 3D Secure Thredd API ([Ws_AddUpDelCredentials](#)) with the [Get](#) option provided in the [<Action>](#) field to return details of the card's Credential IDs. See [Using the Card Enrolment API](#).

If the card is not enrolled in 3D Secure (no credentials are found), then the Thredd API returns an action code of 437. (See the [Web Services Guide \(SOAP\) > Action Codes](#).)

If you are using our Cards API, then you can use the [List 3DS Credentials](#) API endpoint. If the card is not enrolled in 3D Secure, then the API returns a blank 200 code response.

Q. How can I unenroll a card from 3D Secure?

You can remove any credentials linked to a card using Thredd API or the Cards API with the [Delete](#) option specified in the [<Action>](#) field. See [Using the Card Enrolment API](#).

Note: Please check with your 3DS Project Manager for unenrollment restrictions if you have *continuous auto-enrollment* enabled for your cards.



Q. How do I add multiple authentication types to a card?

In your 3D Secure enrolment request (using [Ws_AddUpDelCredentials](#)) you can specify the [Add](#) action and include an array of `<credentials>` to enrol a card in multiple types of authentication. See the example code snippet below:

```
<hyp:Action>Add</hyp:Action>
<hyp:Credentials>
  <hyp:Credential>
    <hyp:ID>0</hyp:ID>
    <hyp:Type>OTPEMAIL</hyp:Type>
    <hyp:Value>john.carter@test.com</hyp:Value>
  </hyp:Credential>
  <hyp:Credential>
    <hyp:ID>0</hyp:ID>
    <hyp:Type>OTPSMS</hyp:Type>
    <hyp:Value>+58585858588</hyp:Value>
  </hyp:Credential>
</hyp:Credentials>
```

Q. How can I list what type of authentication methods are configured for a card?

You can use the 3D Secure Thredd API ([Ws_AddUpDelCredentials](#)) and specify the [Get](#) Action to request the authentication methods for any enrolled card.

If you are using our Cards API, then you can use the [List 3DS Credentials](#) API endpoint.

This returns a list of all the type of authentication the card is enrolled in. This is displayed in the [Credentials](#) fields: [ID](#) lists the unique ID of the authentication method and [Type](#) list the type of authentication. [Value](#) lists the mobile phone number linked to the card.

You can use the [ID](#), [Type](#) and [Value](#) fields in a request to update the authentication type and mobile number.

Q. What is the Credential ID?

The Credential ID is a unique identifier of the type of authentication. If the same card is enrolled for two different types of authentication, then each enrolment will have a unique Credential ID.

In the [Ws_AddUpDelCredentials](#) web service and Cards API [3ds-credentials](#) endpoint, this is up to 8 characters. For example: **669**

Default and Fallback Authentication Types

Q. How do I choose the default and the fallback authentication types?

When you complete your 3D Secure Product Setup Form, you can specify the default and fallback authentication methods for your card product (e.g., Biometric as default with fall back as OTP SMS). See [Completing your 3DS Product Setup Form](#).

The supported authentication types must then be added to the card using either the Thredd API or the Cards API; see [Using the Card Enrolment API](#). Alternatively, if enabled for your account, through auto-enrolment.

Q. When is fallback authentication used and how is it triggered?

If a cardholder cannot authenticate using your default method (e.g. their phone or device doesn't support biometric or they do not have their phone to hand so cannot receive SMS) and you have a fallback authentication option configured, the cardholder can select an alternative option on the challenge screen. Please note this applies to browser-initiated transactions only.

Q. Can cardholders be given the choice of the authentication method?

Yes, you can allow cardholders to select the type of authentication.

During the project implementation stage, you can customise the text that appears on the Apata Choice screen shown to cardholders: you specify this on the 3DS Product Setup Form; see [Challenge Screens](#).

To populate the options that appear on this screen, you need to register your cards for the required authentication types using either the Thredd API or the Cards API; see [Using the Card Enrolment API](#). Alternatively request auto-enrolment from your 3DS Project Manager.



Knowledge-Based Authentication (KBA)

Q. What happens if the card is not enrolled with a sufficient number of KBA questions?

If your organisation is configured to use multiple questions, you should enrol cards with the correct number of questions. Otherwise, Thredd selects one question at random to complete the KBA authentication.

Language Support

Q. Can the OTP messages be displayed in different languages?

Yes, the dynamic OTP SMS message can be configured in a language other than English if you request this; you can only have one SMS language per card product. Please provide the translation for the OTP message. The list of supported languages is regularly updated.

See [Appendix 2: OTP Message Templates](#).

Apata Portal

Q. How can I access the Apata Portal?

For more information on how to access the Apata Portal, see [Using the Apata Portal](#).

Q. How do I define and set up Risk Profiles ?

You can set up your risk profiles in the Apata Portal. See [Managing Authentication Rules](#).

Q. How do I set up rules to pass Mastercard PSD2 Test Cases?

Mastercard provides test cases for Program Managers to verify the 3D secure authentication process under the PSD2 rules. If you have been contacted by your issuer (BIN sponsor) to complete Mastercard PSD2 test cases, please contact your 3DS Project Manager.

Q. How can I manage my PSD2 and SCA requirements and exemptions?

The Authentication section on the Apata Portal allows you to manage any PSD2 and Strong Customer Authentication (SCA) requirements and exemptions relating to cardholder authentication; see [Managing Authentication Rules](#). Please check with your issuer (BIN sponsor) for any Scheme-mandated requirements relating to PSD2 and Strong Customer Authentication (SCA).

There are also a number of SCA settings you can configure with Thredd. For information on the PSD2 and SCA checks run by Thredd, see the [PSD2 and SCA Guide](#).

3D Secure Fields

Q. Does Thredd provide data linked to the merchant's Requestor App URL?

Yes, during an app-based transaction with authentication, if provided by the merchant, then Thredd receives data from Apata in an optional [redirectAppUrl](#) field which indicates the merchant's app URL. For more information, see [Initiating a Biometric Session](#).

Q. Who validates the CAVV or AAV, and how are these details used?

The Accountholder Authentication Value (AAV) for Mastercard programmes or Cardholder Authentication Verification Value (CAVV) for Visa programmes is a cryptographic value which is included in the authorisation message request from the Merchant⁹. It indicates that the 3D secure authentication session was successful or attempted. Merchants include this value in the authorisation request which follows after a 3D authentication session. The value is encrypted to ensure that merchant's cannot tamper with the authentication result. You can request that either Thredd or the Card Scheme (Mastercard or Visa) validate this value. Card Scheme 'on behalf' validation is typically required if you want the card Scheme to provide Stand-In processing. For more information, see [Completing your 3DS Product Setup Form](#).

⁹The ACS generates the CAVV/AAV for a successful 3D secure session; if Stand-In processing is enabled at the Card Scheme (for low-risk transactions), then the Scheme can step in when ACS is down and generate this value.



If Thredd was selected to validate and the CAVV/AAV is not valid (or 3D secure failed or was not performed), then Thredd will decline the authorisation request with CAVV error. Thredd provides relevant details relating to 3D secure (e.g., method of authentication used and result) in the [GPS_POS_Data](#) field. For more information, see the [External Host Interface \(EHI\) Guide > GPS_POS_Data Field](#).

Q. Do you provide details of the *acsInfoInd* Field?

No, this is a Scheme-generated optional field in the message between the ACS and the merchant server; you will not need this information. The [acsinfoInd](#) is the ACS information indicator which indicates all of the authentication services (e.g., Device Binding, Transaction Risk Analysis, Authentication, Attempts, Trust Listing, Secure Corporate Payments Exemption and so on) supported by the ACS for the issuer's (BIN sponsor) card ranges. Refer to the [EMVCo guides](#) for details.



Troubleshooting

Q. Why are some cardholders not receiving the OTP?

Below are possible reasons why cardholders may not receive the OTP:

- SMS is successfully delivered to the mobile phone carrier, but has not been received: possible issue with the carrier passing it to the cardholder; this could be due to spam filtering , blocking overseas SMS messages or mobile network reception issues
- SMS provider (Thredd uses AWS SNS) does not send SMS to sanctioned countries
- Network issue affecting the message transmission on the Thredd side



Glossary

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

A

- AAV/CAVV**
- Accountholder Authentication Value (AAV) and Cardholder Authentication Verification Value (CAVV) are cryptographic values returned by the Access Control Server (ACS) or Card Scheme to the Merchant after a successful cardholder authentication. The merchant includes this value in the authorisation message sent to the issuer.
- Access Control Server (ACS)**
- A system used to manage the 3D Secure authentication service for the issuer (BIN sponsor). During an authentication session, the ACS communicates with the Card Scheme and Thredd systems, and may also interact with the cardholder, by providing Challenge screens.
- Accountholder Authentication Value (AAV)**
- Unique 32-character transaction token for a Mastercard 3D Secure transaction. For Mastercard Identity Check, the AAV is named the UCAF.
- 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**
- Process to verify the identity of a cardholder.
- Authorisation**
- Process that seeks approval for a payment transaction. The process starts when a merchant requests approval for a card payment by sending a request to the card issuer (BIN sponsor) to check that the card is valid, and that the requested authorisation amount is available on the card.
- Authorisation Request Message (AReq)**
- The initial message in the 3-D Secure authentication flow. The 3DS Server forms the AReq message when requesting authentication of the Cardholder. It can contain Cardholder, payment, and Device information for the transaction. There is only one AReq message per authentication.
- Authorisation Response Message (ARes)**
- The Issuer's ACS response to the AReq message. It can indicate that the Cardholder has been authenticated, or that further Cardholder interaction is required to complete the authentication. There is only one ARes message per transaction.

B

- Biometrics**
- Biometrics are body measurements and calculations related to human characteristics that are unique to each person (such as face, eyes, voice and fingerprints). Biometrics authentication is used as a form of identification and access control.
- Business identifier (BID)**
- A business ID, which is unique to each Visa business customer.

C

- Card Scheme (payment network)**
- Card scheme or payment network, such as Mastercard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.
- Cardholder**
- Consumer, employee cardholder or account holder who is provided with a card to enable them to make purchases.
- Cardholder Authentication Verification Value (CAVV)**
- For Visa Secure transactions, a CAVV is generated by the issuer's (BIN sponsor) Access Control Server (ACS). The CAVV provides evidence that cardholder authentication occurred or that the merchant attempted authentication. A CAVV is unique for each



authentication transaction.

Cards API

The Thredd Cards API are REST-based API that enable you to create and manage the cards in your card programme using JSON messages.

E

EHI

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

EMV 3DS Global Consumer Screen Template Guide

A PDF guide for configuration of the 3D Secure Authentication Service screens shown to cardholders during a 3D Secure session.

EMVCo

EMVCo is a technical body which manages and evolves EMV Specifications and supporting programmes that enable card-based payment products to work together seamlessly and securely worldwide.

F

Fraud Liability Protection

3D Secure transactions provide the online merchant with fraud liability protection.

Frictionless Authentication

When a transaction is approved without requiring any manual input from the cardholder.

I

ICA

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

In-App

Purchase or activity made or available from within a particular app on a mobile device, without the need to visit a separate online site.

Issuer (BIN sponsor)

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

K

Knowledge Based Authentication (KBA)

Authentication method used in e-commerce transactions where the cardholder is asked to verify their identity by providing the answer to a question such as 'What is your mother's maiden name?' or 'What is the name of your favourite pet? KBA may be combined with OTP SMS.

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.

O

One Time Password (OTP)

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



Out-Of-Band (OOB) Authentication

A type of two-factor authentication that requires a secondary verification method through a separate communication channel. Both Biometric and In-App authentication methods are out of band.

P

PAN

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

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

Preparation Request Message (PReq)

Message sent from the 3DS Server to the Directory Server (DS) to request information about the Protocol Version Number(s) supported by available ACSs and the DS and if one exists, any corresponding 3DS Method URL. This message is not part of the 3-D Secure authentication message flow.

Preparation Response Message (PRes)

The Directory Server (DS) response to the PReq message. The 3DS Server can use the PRes message to cache information about the Protocol Version(s) supported by available ACSs and the DS, and if one exists, about the corresponding 3DS Method URL. This message is not part of the 3-D Secure authentication message flow.

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

R

Risk-Based Authentication (RBA) /Transaction Risk Analysis (TRA)

The authentication decision is based on the risk rules configured for the service (i.e., rules you have configured in the Apata Portal).

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 provides a means of transferring files to a secure server.

Smart Client

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

Soft Decline

An issuer (BIN sponsor) can use a soft decline if they receive a request from a merchant to authorise a payment, but they want to use authentication first. The cardholder will be prompted to retry the transaction with authentication. The transaction could still decline on the second attempt for other reasons (e.g., perceived fraud risk, insufficient funds).

Strong Customer Authentication (SCA)

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



T

Thredd API

The Thredd API consists of web services that use SOAP and the Cards API based on REST.



Document History

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

Version	Date	Description	Revised by
1.1	21/03/2024	Updates to content and graphics to align with taxonomy updates on our Documentation Portal.	KD
	13/03/2024	Updates to endpoint URLs and examples in Using the Biometric/In-App Authentication APIs . Updates to a field name in the Delegate SCAValidation Message Fields .	KD
	22/02/2024	Corrections to diagrams. These include: • Figure 3: 3D Secure Authentication Process - Using 3D Secure and Biometrics or Out of Band (OOB). • Figure 7: OTP SMS Challenge Screen Customisation • Figure 11: 3D Secure Authentication Screens - for Biometric	KD
	21/02/2023	Added details of how to add, update or delete card level configurations for Apata, such as the language of the Apata Challenge screens and the Challenge Profile to use. See Using the Card Configuration API .	WS
	16/02/2024	Removed information on report settings. Updated description on adding reports to email in Analytics .	KD
	08/02/2024	Included updated descriptions on Knowledge Based Authentication in Cardholder Authentication Flows , added the Production API endpoints to Authorising Thredd IP Addresses , updated reference details in Appendix 6: Biometric OOB Fields .	KD
	08/01/2024	Correction to Figure 1: Flowchart of Parties involved 3D Secure .	KD
	05/01/2024	Added Biometric endpoint content on Apata. This includes updates in the following areas: • Summary of steps for Biometric and OOB in Completing Your 3DS Product Setup Form. • Step-by-step instructions on using the APIs in Using the Biometric/In-App Authentication APIs. • Reference information in Appendix 6: Biometric OOB Fields. • IP address information in Authorising Thredd IP Addresses.	KD
1.0	23/11/2023	Updates to the description of the fields in the Product Setup Form (PSF), added sections describing new features on the Apata Portal, plus other corrections.	WS
	01/11/2023	First version of 3D Secure Guide for Apata.	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.