



3D Secure Guide (Cardinal)

Version: 2.3

04 June 2026

Publication number: 3DS-2.3-6/4/2026

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

Thredd, 33 Kingsway, London, WC2B 6UF

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

© Thredd 2026





Copyright

© Thredd 2026

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 (Cardinal) authentication service and integrating this service with Thredd.

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

Target Audience

This document is intended for Thredd clients (Program Managers) who are interested in integrating the 3D Secure (Cardinal) service with OTP, Biometric, In-App or KBA authentication into their program. It is aimed at developer users, with an understanding of how to implement the Thredd 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 Biometric/In-app 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 Service Guide (SOAP)	Provides details of the Thredd API and includes a section on 3D Secure web services.
Cards API Website (REST)	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 legacy Thredd Smart Client application to manage your account.
Thredd Portal Guide	Describes how to use the new Thredd Portal, the new online user interface, to manage your account.

Other Guides

Refer to the table below for other relevant documents.

Document	Description
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. This guide contains editable fields and you should work with your Thredd 3DS project manager to review this guide and complete these fields.



Document	Description														
Cardinal Guides	<p>Cardinal provides several guides related to their service. You should refer to these guide when setting up your 3D Secure rules and managing your service on the Cardinal Portal.</p> <table border="1"> <thead> <tr> <th>Guide</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Customer Service Application: Portal User Guide</td> <td>This document provides users step-by-step instructions for using the Customer Service application in the VCAS Portal.</td> </tr> <tr> <td>EMV 3DS Reporting Suite: Portal User Guide</td> <td>This guide outlines how to use the EMV 3DS Reporting Suite application within the VCAS Portal to effectively monitor and control authentication performance.</td> </tr> <tr> <td>EMV 3DS Rules Application : Portal User Guide</td> <td>This document includes information on how to create, edit, test, and publish rules and policies as well as how to generate lists for use in rules.</td> </tr> <tr> <td>User Management Application: Portal User Guide</td> <td>This document provides users step-by-step instructions for using the User Management application in the VCAS Portal.</td> </tr> <tr> <td>VCAS Compliance Manager Portal User Guide</td> <td>This guide provides an overview of how the Compliance Manager application works and outlines how to manage the features of the Compliance Manager application.</td> </tr> <tr> <td>VCAS Test Store Guide</td> <td>This guide provides an overview of how the test store application works and provides instructions on how to run test transactions in the test store application.</td> </tr> </tbody> </table> <p>For the latest versions, please check with your 3DS project manager</p> <p>Note: Thredd also provide training on how to use the Cardinal Portal. For details, please contact your Thredd 3DS project manager.</p>	Guide	Description	Customer Service Application: Portal User Guide	This document provides users step-by-step instructions for using the Customer Service application in the VCAS Portal.	EMV 3DS Reporting Suite: Portal User Guide	This guide outlines how to use the EMV 3DS Reporting Suite application within the VCAS Portal to effectively monitor and control authentication performance.	EMV 3DS Rules Application : Portal User Guide	This document includes information on how to create, edit, test, and publish rules and policies as well as how to generate lists for use in rules.	User Management Application: Portal User Guide	This document provides users step-by-step instructions for using the User Management application in the VCAS Portal.	VCAS Compliance Manager Portal User Guide	This guide provides an overview of how the Compliance Manager application works and outlines how to manage the features of the Compliance Manager application.	VCAS Test Store Guide	This guide provides an overview of how the test store application works and provides instructions on how to run test transactions in the test store application.
Guide	Description														
Customer Service Application: Portal User Guide	This document provides users step-by-step instructions for using the Customer Service application in the VCAS Portal.														
EMV 3DS Reporting Suite: Portal User Guide	This guide outlines how to use the EMV 3DS Reporting Suite application within the VCAS Portal to effectively monitor and control authentication performance.														
EMV 3DS Rules Application : Portal User Guide	This document includes information on how to create, edit, test, and publish rules and policies as well as how to generate lists for use in rules.														
User Management Application: Portal User Guide	This document provides users step-by-step instructions for using the User Management application in the VCAS Portal.														
VCAS Compliance Manager Portal User Guide	This guide provides an overview of how the Compliance Manager application works and outlines how to manage the features of the Compliance Manager application.														
VCAS Test Store Guide	This guide provides an overview of how the test store application works and provides instructions on how to run test transactions in the test store application.														
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).														
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 .														

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



1 Introduction

3D Secure (Three Domain Structure), also known as a payer authentication, is a security protocol that helps to prevent fraud in online credit and debit card transactions. This security feature is supported by Visa, Mastercard and Discover, as well as smaller networks that use the Mastercard Network Exchange (MNE), such as STAR and Pulse. The feature is branded as Visa Secure, Mastercard Identity Check and Discover ProtectBuy respectively.

Thredd use Cardinal Commerce as our 3D Secure service provider. Cardinal provides a real-time 3D Secure enrolment and authentication service called Realtime Data eXchange (RDX). You can implement this service through Thredd to ensure that your cardholders are successfully enrolled and authenticated using 3D Secure.

You can configure the rules which Cardinal use to make a frictionless authentication approval decision, as well as the challenge rules that trigger a request for further authentication.

You can view demos and more information about the authentication process on the Cardinal demo website: [Cardinal Commerce Demo Library](#)

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

1.1 Authentication Types

Thredd supports a number of methods or types of authentication that can be used to further verify the cardholder during an online transaction made from a merchant's website. These authentication types include:

- **Risk based authentication (RBA).** The authentication decision is done based on Cardinal rules, which generate a risk score that determines whether to approve or decline the transaction. This process is managed by Cardinal.
- **OTP SMS authentication.** Cardinal 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 the e-commerce transaction.
- **Biometric authentication.** Cardinal 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 or face recognition, obtained from the cardholder's mobile device. Your customer application manages the Biometric verification and returns a response to Thredd.
- **Out of Band (OOB) authentication.** Cardinal sends an authentication request to Thredd and we forward this to your systems. You need to verify the cardholder using your customer In-App smart phone application, for example by asking them to enter a username and password. Your customer application manages the verification and returns a response to Thredd.
- **Knowledge Based Authentication (KBA).** You enrol the card in KBA using the 3D Secure RDX service and provide the security question ID and answer pair. Thredd provides Cardinal with the security question to use for KBA. During the e-commerce authentication session Cardinal asks the cardholder to answer the security question and then sends a KBA authentication request to Thredd together with the cardholder's answer. Thredd compares the answer returned by Cardinal to the answer stored in the Thredd database and then returns a response to Cardinal. KBA is typically combined with OTP SMS: the cardholder is first asked to authenticate using OTP and then via KBA.

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

Two-factor authentication

Biometric, In-App Out-of-band (OOB) authentication and KBA are types of two-factor authentication that requires a secondary verification method through a separate communication channel¹. If Biometrics is being used for authentication, this secondary verification is obtained via Biometric data². If In-App OOB is being used, the secondary verification is obtained via your customer In-App application. If Knowledge-Based Authentication (KBA) is used, secondary verification is obtained via a security question combined with a One Time Password (OTP) to authenticate the cardholder.

Biometric, In-App OOB authentication and KBA are considered to be a form of Strong Customer Authentication (SCA).

Strong Customer Authentication (SCA)

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

¹ Since Cardinal provide the primary communication channel (3D Secure screens shown to the user), the authentication session must provide a secondary channel for authentication (e.g., via your Smart device application screens).

² Behavioural Biometrics (based on analysis of patterns of user activity such as mouse activity, keystroke movement, touch screen behaviour and device movement) is another form of 2-factor authentication, which is in the Thredd/Cardinal development roadmap.



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 Password).	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 strong customer authentication (SCA) to your cardholders; this is required to comply with the Second Payment Services Directive (PSD2) relating to strong consumer authentication (SCA). These regulations apply to cards issued in the European Economic Area (EEA) and the United Kingdom.

SCA has been in place since **March 2022** for UK issued cards, and across most of the EEA from January **1st, 2021**.



2 Parties Involved in 3D Secure

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

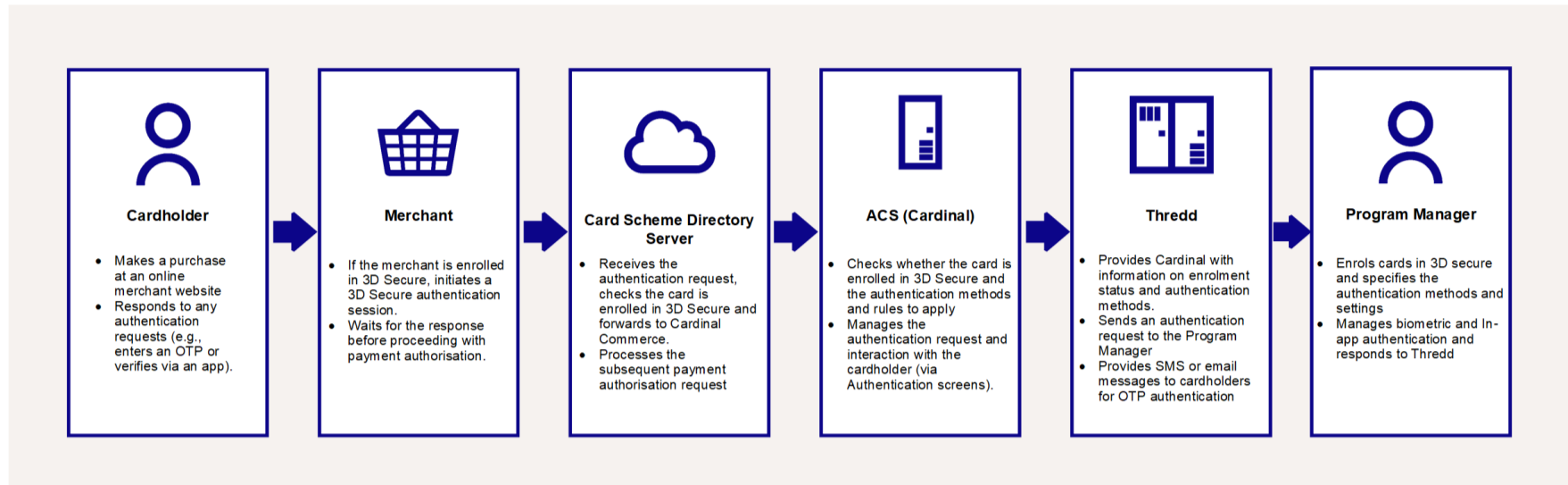


Figure 1: Flowchart of Parties Involved 3D Secure

Cardholder

The cardholder's card must be enrolled in the 3D Secure RDX service and enabled for authentication types such as Biometric authentication and OTP SMS. 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) or via Biometric verification (e.g., fingerprint or face recognition).

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 (payment networks) and the 3D Secure authentication request.

Card Scheme (Network)

The Card Schemes (Networks such as Visa, Mastercard or Discover) receive all payment authorisation requests from merchants. The Schemes maintain Directory Servers, with details of card BIN ranges. They check the BIN range to determine whether the card is enrolled in the 3D Secure service and who the 3D Secure service provider for that card is, and then route the request to the service provider.

Cardinal Commerce

Cardinal is the provider of the Thredd 3D Secure service. They receive 3D Secure authentication requests from the Card Schemes (payment networks) and check their database for the 3D Secure rules you have configured in the Cardinal 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 [Cardinal Configuration of RDX Biometric and Screens](#).

- If OTP SMS is selected, then Cardinal generates the OTP and sends it to Thredd. They provide the cardholder with relevant screens and messages.
- If Biometric In-App or Out of Band In-App is selected, then Cardinal provides the cardholder with relevant screens and messages and sends Thredd a message to initiate an authentication session with the Program Manager.
- If KBA is being used, this typically follows OTP SMS authentication. Cardinal presents a security question to the cardholder and returns the answer to Thredd for verification.

¹ For transactions considered lower risk, such as for smaller amounts, the card payment can be configured to authorise without presenting the cardholder with further authentication screens.

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



Thredd

Thredd manages the communication with Cardinal and the Program Manager. During an authentication session, Thredd sends Cardinal a list of the authentication types for which the card is registered³. Cardinal can use these details to present the available authentication methods to the cardholder.

Depending on the option selected, Thredd support the authentication process as follows:

- For OTP SMS, Thredd receives the OTP from Cardinal and sends the OTP to the cardholder's mobile phone. See [Appendix 2: OTP Message Templates](#).
- For KBA, Cardinal sends the cardholder's security question answer to Thredd. Thredd compares the answer to the details held in the Thredd database and returns a response to Cardinal.
- For Biometric In-App, Thredd notifies your systems of a request to start an authentication session. Your systems manage the cardholder authentication via your smart phone application and return a response to Thredd. Thredd notify Cardinal of the result.

Program Manager

As a Thredd Program Manager, you must sign up for the 3D Secure RDX service with Thredd and set up your 3D Secure rules on the Cardinal Portal. See [Steps in a 3D Secure Biometric/In-app Project](#).

During the implementation phase, you can ask Cardinal to configure the logo and text that appears on the 3D Secure Authentication screens that they display to the cardholder during the authentication process.

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](#).

For KBA authentication, you can use either our Thredd API or our or Cards API to send Thredd details of the question and answer to use during KBA.

For Biometric and In-App authentication, you will need to implement additional API to receive verification requests from Thredd and send verification results to Thredd. See [Using the Thredd OAuth Server](#) and [Using the Biometric/In-App Authentication API](#).

Your customer application must be able to manage the authentication on the cardholder's smart device: when you receive a Biometric/In-App authentication request from Thredd, your systems will need to load your customer application in the user's smart device and authenticate via an appropriate Biometric method (e.g., fingerprint or facial recognition) or In-App method (e.g., username and password or using a Token device). You then need to return a response to Thredd.

³ Based 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 an authentication session.

3.1 Authentication using Non-Delegated OTP

Figure 1 provides an overview of the cardholder authentication process during a transaction, using the Cardinal 3D Secure service with Non-Delegated One Time Password (OTP) authentication.

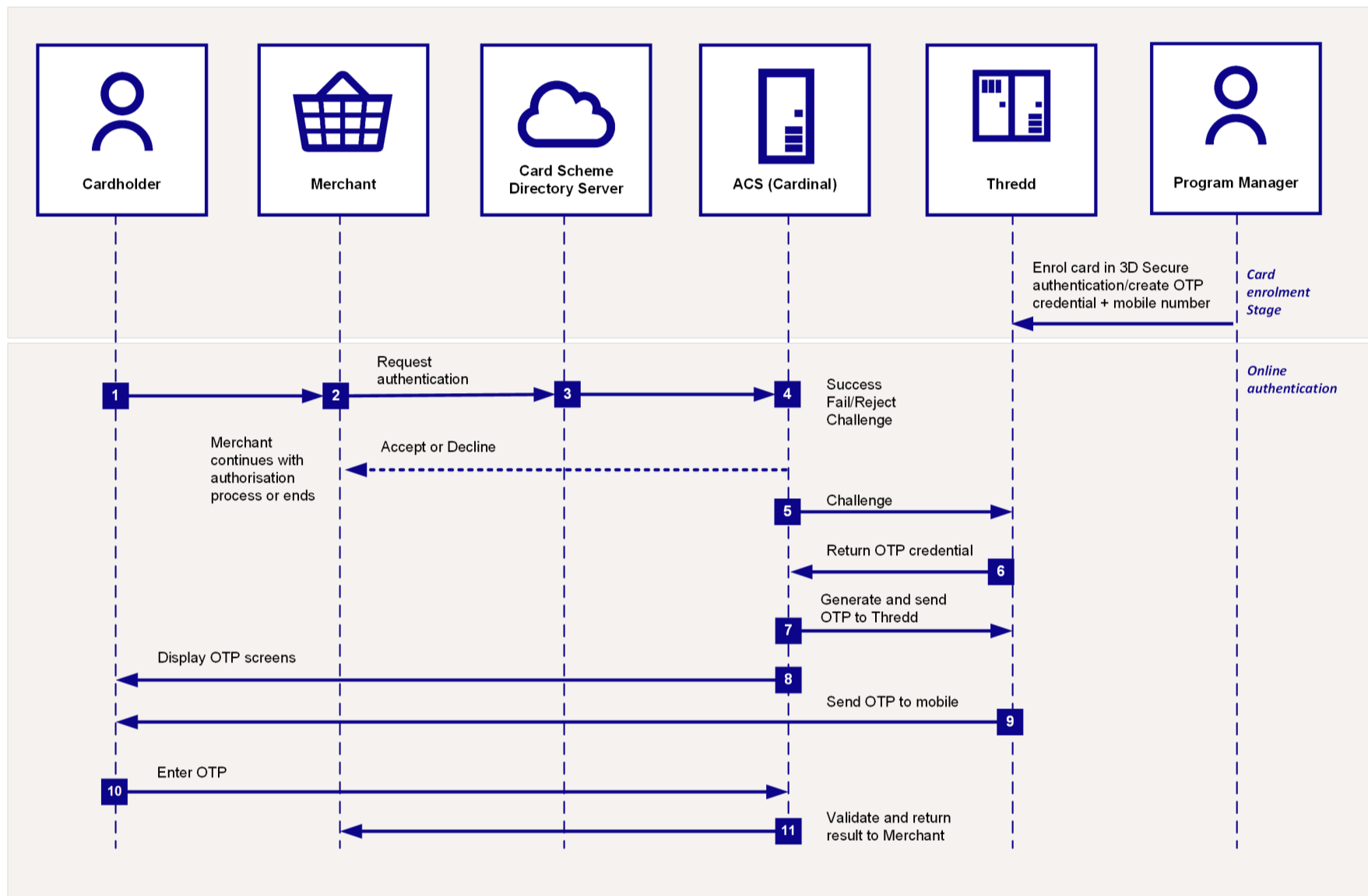


Figure 2: 3D Secure Authentication Process - Using RDX and Non-Delegated OTP

Prior to using OTP, you need to set up the OTP credential on the card. 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/Discover).
3. The Card Scheme looks up the 3D Secure service provider and sends the authentication request to Cardinal.
4. Cardinal checks to confirm the card BIN range is enabled for 3D Secure. Based on the rules you set up in Cardinal for your card program, the outcome is Success, Fail/Reject or Challenge. (See [Appendix 1: Cardinal 3D Secure Rules](#))
 - a. For a Success outcome, an approval response is returned to the merchant. They can continue with the transaction authorisation process.
 - b. For a Fail/Reject outcome, an authentication failure/reject response is returned to the merchant. They can decide whether to continue or ask the cardholder to provide an alternative payment method.
 - c. For a challenge outcome, 3D Secure authentication is required. See the steps below.



Steps for a Challenge outcome

5. Cardinal connects to Thredd in real-time to query the types of authentication the card is registered for (e.g., Biometric, OTP SMS or KBA).
6. Thredd replies to Cardinal with the OTP as the type of authentication registered on the card (based on what you registered the card for using the Thredd API/ Cards API and on the default types set up for your cards)¹.
7. Cardinal generates the OTP and sends it to Thredd in real-time.
8. Cardinal displays the OTP screens to the cardholder.
9. Thredd sends the OTP to the cardholder's mobile number.
10. The cardholder enters the OTP to complete their authentication.
11. Cardinal validates the OTP and sends the result back to the merchant.

¹ Thredd configure the sub-BIN range to a default main authentication method and a fallback method. See Setup Options in [Client Information](#).



3.2 Authentication using Delegated OTP

Figure 2 provides an overview of the cardholder authentication process during a transaction, using the Cardinal 3D Secure service with Delegated One Time Password (OTP) authentication. For Delegated OTP, you pass the OTP, which Thredd sent to you, directly to the cardholder through SMS. Initially, Thredd would have validated the OTP it received from Cardinal. Thredd sends the OTP to you through the DelegatedOTPNotification endpoint.

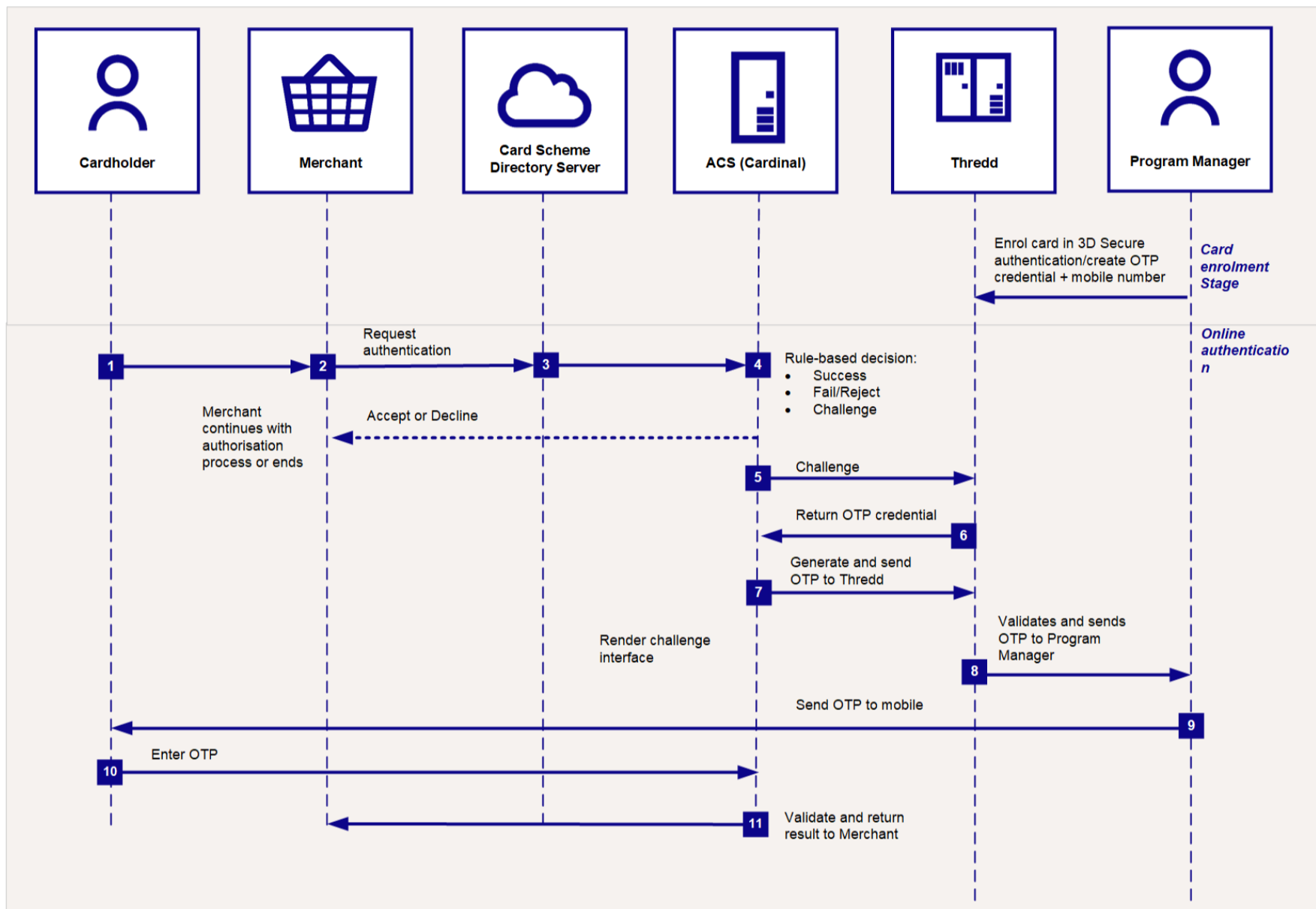


Figure 3: 3D Secure Authentication Process - Using RDX and Delegated OTP

You need to have set up the OTP SMS authentication method on the cardholder's card, and added a valid mobile phone number for completing the authentication.

The steps for client-managed OTP SMS authentication are as follows:

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 (Network).
3. The Card Scheme looks up the 3D Secure service provider for your card programme and sends the authentication request to Cardinal.
4. Cardinal checks to confirm the card BIN range is enabled for 3D Secure. Based on the rules you set up in Cardinal for your card program, 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 Challenge outcome below.



Steps for a Challenge outcome

5. Cardinal connects to Thredd in real-time to check the types of authentication the card is registered for, which include Biometric, OTP SMS or KBA).
6. Thredd replies to Cardinal 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. Cardinal generates the OTP and sends it to Thredd in real-time.
8. Send OTP to Program Manager.
9. You send an acknowledgement back to Thredd.
10. Thredd sends an OK response to Cardinal.
11. You send the OTP that you received from Thredd to the cardholder.
12. Cardinal renders the OTP screen.
13. The cardholder enters the OTP in the 3DS pop up screen on the merchant's website or App to complete their authentication.
14. Cardinal validates the OTP and sends the validation result back to the merchant.



3.3 Authentication using Biometrics or In-App OOB

Figure 3 provides an overview of the cardholder authentication process during a transaction, using the Cardinal 3D Secure service with Biometric authentication.

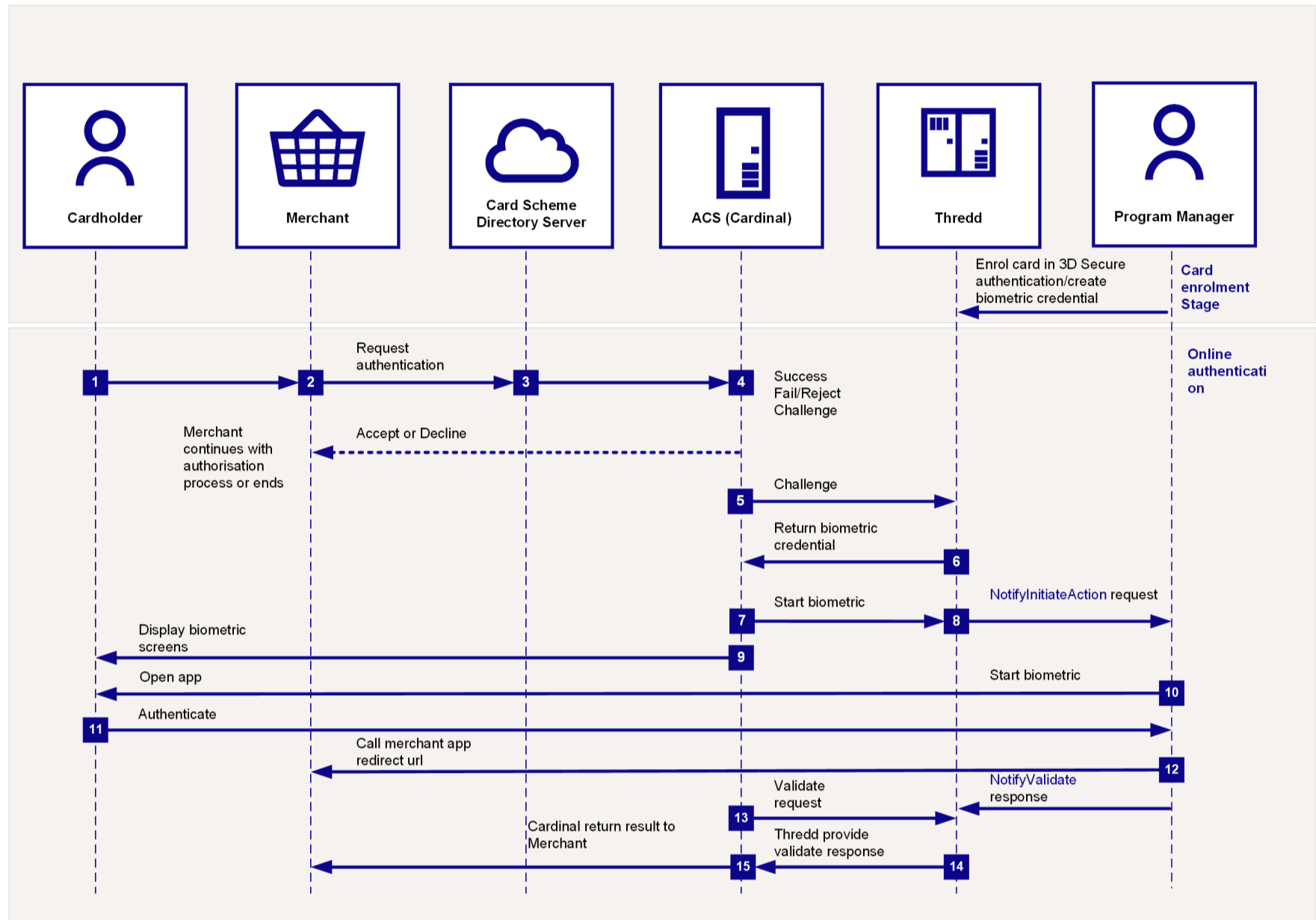


Figure 4: 3D Secure Authentication Process - Using RDX and Biometrics

Authentication via Biometric or In-App OOB

Prior to using KBA, you need to set up the BIOMETRIC credential on the card. See Using the Card Enrolment API.

Steps 1-5 are as described previously.

6. Thredd replies to Cardinal 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)².
7. Cardinal calls Thredd to start the Biometric authentication.
8. Thredd sends a message to your RDX service endpoint, to start authenticating using Biometric. Note that Program Managers must respond to Thredd's `NotifyInitiateAction` API request (200 OK) within 5 seconds as Cardinal is expecting Thredd to respond within 5 seconds. The architecture allows occasional longer running transactions of up to 10 seconds; however, the average response time should be significantly lower. (See [Initiating a Biometric Session](#))
9. Cardinal shows the Biometric screens to the cardholder. This informs the cardholder that they will need to authenticate using your smart device app.
10. You connect to your cardholder via your Biometric or In-App customer smart device application.
11. The cardholder authenticates using your smart phone app (e.g., by scanning their fingerprint or face using their smart device)
12. When the authentication session is complete, then:

²Thredd configure the sub-BIN range to a default main authentication method and a fallback method. See Setup Options in Client Information.



- Your app must return the result of the Biometric authentication to Thredd (validate response using the [NotifyValidate API](#)).
- Your app should call the merchant's app (using the [MerchantAppRedirectURL](#) field value obtained from the Thredd [NotifyInitiateAction API](#) request) to enable the merchant app to redirect the cardholder back to the checkout page.

13. Cardinal sends a validate request to Thredd.

14. Thredd waits for your validate response ([NotifyValidate API](#)) and sends the results back to Cardinal.

15. Cardinal returns the results to the merchant.



3.4 Authentication using KBA

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

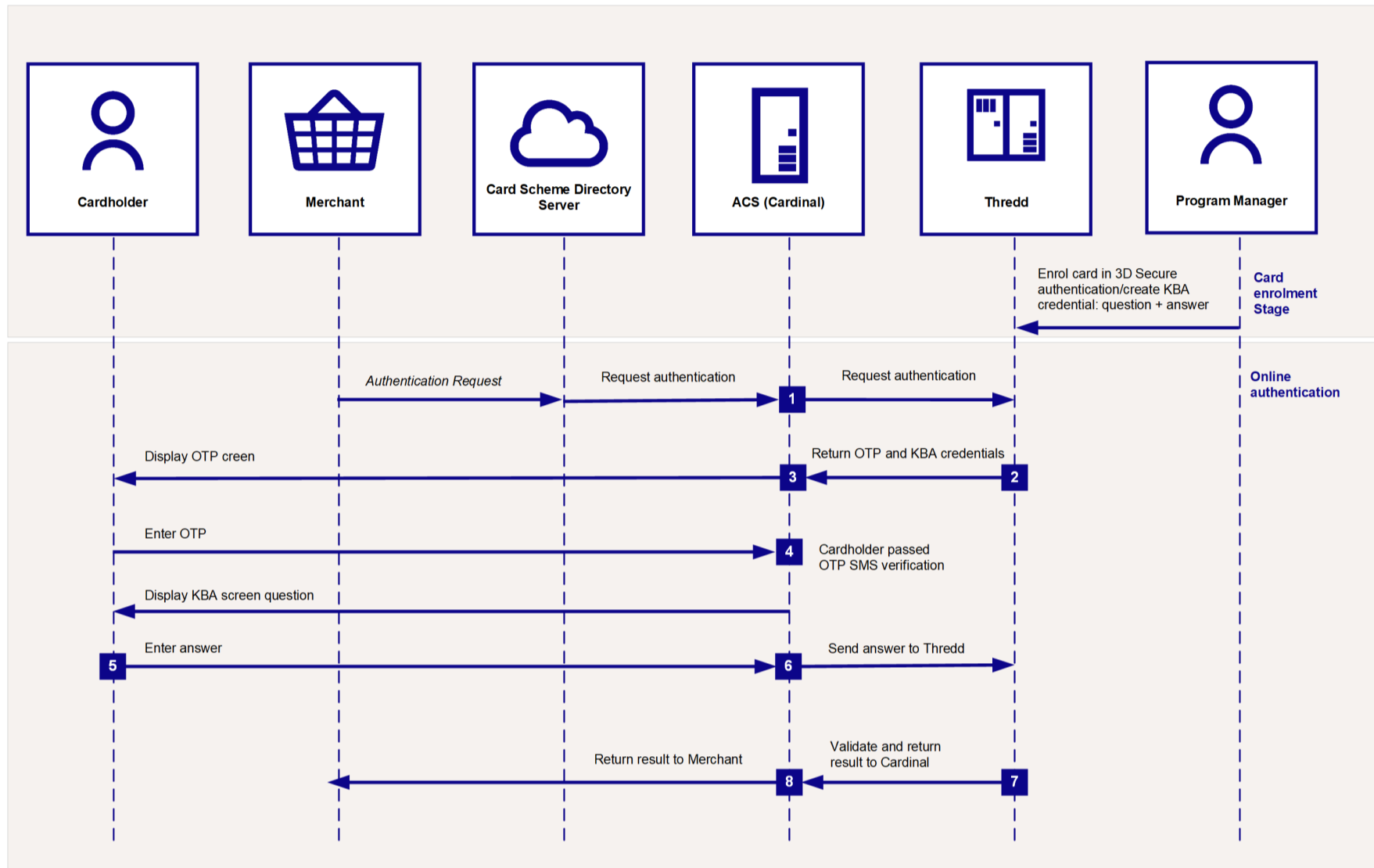


Figure 5: 3D Secure Authentication Process - Using RDX and KBA

Authentication via KBA

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

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

1. Cardinal 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 to Cardinal with the OTP and KBA authentication types. For KBA, Thredd includes the security question to present to the cardholder.
3. Cardinal follows the process for OTP SMS, presenting the OTP screen to the customer, who enters the OTP which Thredd sends to their mobile phone.
4. Following OTP authentication, Cardinal presents an additional screen to the cardholder, asking them to answer the security question set up for their card.
5. The cardholder enters their answer.
6. Cardinal validates the OTP and sends the OTP validation result to Thredd, together with the KBA answer.
7. Thredd compares the answer returned from Cardinal to the answer stored in the Thredd database³. Thredd sends the combined OTP and KBA validation results back to Cardinal.
8. Cardinal returns the results to the merchant.

³ When Thredd receives the answer from Cardinal it is immediately encrypted using a hashing algorithm and compared to the hashed answer value stored in the Thredd database.



3.5 What happens after authentication?

When the cardholder is authenticated, the merchant can proceed with requesting authorisation for the transaction. (The merchant acquirer includes the 3DS secure value they receive from Cardinal within the transaction: [UCAF](#) field (For Mastercard), the [CAVV](#) field 126.9 for (Visa), and Field 122 of the authorisation message for Discover/Diners.)

If requested, then Thredd will validate the AAV (Mastercard) or CAVV (Visa). 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 to your EHI endpoint to approve or decline.

You can view details of your 3D Secure transactions in the Cardinal Portal. See [Configuring Rules in Cardinal Portal Production](#).



4 Steps in a 3D Secure Biometric/In-app Project

This section describes the steps in setting up a 3D Secure RDX service with Biometric or In-App authentication.

4.1 Overview of Steps

The RDX service is required for Biometrics or Out of Band In-App authentication. A project starts once Cardinal Commerce have received your requirements. A typical RDX project takes 7-8 weeks, but you should plan for up to 9-10 weeks to allow for contingencies. (This timeline assumes you have already developed the customer smart device application you will be using to provide Biometric/In-App authentication, and have developed Card Enrolment APIs.)

Figure 1 below provides an overview of the steps in a typical project.

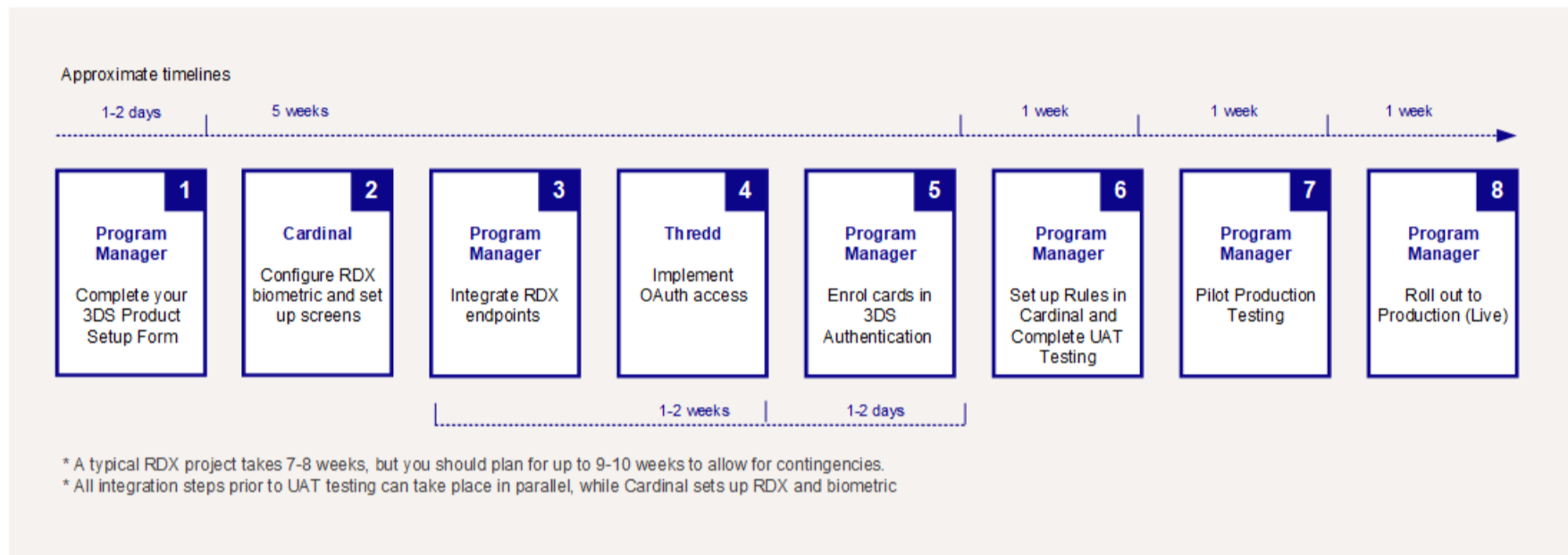


Figure 6: Steps in a 3D Secure RDX Project

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.	Allow 1-2 days. A Statement of Work must be completed between Thredd and Cardinal.
2	Cardinal sets up your 3D Secure account and Screens Specify the Cardinal 3D Secure configuration options. Cardinal will configure your 3D secure settings, provide Cardinal Portal access and customised authentication screens.	Allow around 4 weeks for Cardinal to configure both RDX and biometric.
3	Integrate the 3D Secure RDX endpoints Provide Thredd with your API endpoints and a list of permitted IP addresses for using the services. Develop the functionality to receive and process 3D Secure messages using either our 3D Secure Thredd API or our Cards API.	Allow 1-2 weeks for Thredd to configure the API endpoints and enable access for your IP addresses.
4	Implement OAuth access Thredd sets up your OAuth access and provides you with details to access the Thredd OAuth server. Test that you are able to access the OAuth server in staging and production; see Steps 6 and 7 below.	Included in the 1-2 weeks period for integrating RDX endpoints (step 3 above)
5	Enrol your cards in 3D Secure Thredd activates a single card product in the Staging environment, so you can enrol a few cards for Staging UAT testing.	It takes 1-2 hours for Thredd to activate the card product. Allow 1-2 hours to enrol cards in the Thredd Staging UAT environment and run authentication tests. See step 6. Then



#	Step/Action	Approximate time needed
	You can enrol your cards and specify the types of authentication: if using the Thredd API then use the 3D Secure RDX Thredd API (Ws_AddUpDelCredentials); if using Cards API, then use the Create 3DS Credentials API.	repeat in Pilot production. See step 7.
6	<p>Complete Staging/UAT testing</p> <p>Once RDX and biometric are configured, Thredd and Cardinal release the project into the Staging UAT environment for you to test.</p> <p>You can now create your 3D Secure rules and policies in the Cardinal Staging Portal.</p>	<p>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 to a 3D Secure policy. You can start testing in Staging using the Cardinal UAT simulator in the Cardinal Staging Portal.</p> <p>Allow a week to complete the Staging UAT testing.</p>
7	<p>Complete pilot Production testing</p> <p>Thredd and Cardinal set up your cards in the Production environment:</p> <ul style="list-style-type: none"> • Thredd activates a single card product in the Production environment, so you can enrol a few cards for pilot testing. • 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 Cardinal ACS URLs¹) • Create your 3D Secure rules and policies in the Cardinal Production Portal. 	<p>The full pilot testing phase takes around 1-2 weeks:</p> <ul style="list-style-type: none"> • Allow a week for Thredd and Cardinal to release your cards to the Production environment for Pilot testing. • Mastercard takes around 3 days to set up pilot cards. Visa takes 1-2 weeks. (Providing the pilot cards in advance can speed up the process.) • Allow 1-2 days for enrolling the pilot cards (using the Thredd API/ cards API) and for pilot card testing.
8	<p>Roll out to Production (Live)</p> <p>Notify Thredd once you have completed your pilot testing. Thredd configures your card products for 3D Secure.</p> <p>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.</p> <p>Notify Thredd that you have completed enrolment.</p> <p>Your issuer (BIN sponsor) contacts the Card Scheme to set your card BIN ranges live (For Mastercard). For Visa, Cardinal supplies the card range files for the issuer (BIN sponsor) to load at the Visa Directory Server.</p>	<p>Allow a week to 10 days to complete the roll-out at the Card Scheme and to enrol your cards.</p>

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

¹ The URL is unique per Program Manager and is used by the Scheme to direct the transaction to the Cardinal system.



5 Completing your 3DS Product Setup Form

The Cardinal Commerce RDX service is provided through Thredd, so you do not need to have a direct relationship with Cardinal. Thredd will provide Cardinal with instructions and set up your service.

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

- [Client Information](#)
- [Cardinal Access](#)
- [Supported Languages](#)

Each of these tabs is described in further detail below.

5.1 Client Information

Complete the following details on this tab:

Field	Description
Client Information	
Client name	Your company's name.
Legal Name	Your company's legal name.
Country of residence	Your company's country of residence.
Card Scheme	The payment network for your BIN. Thredd supports cards enabled for use on Visa, Mastercard and Discover payment networks.
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
Default language	The default language for the 3D Secure screens.
Other languages	List any additional languages you support. See Language Support .
SMS Sender ID	The text that appears as the name of the sender of the SMS OTP for validation. This can be up to 11 alphanumeric characters with no spaces.
Are you self-issuing?	Whether your organisation is set up as an issuer (BIN sponsor). Select YES or NO.
Issuer (BIN sponsor) name	The name of your issuer (BIN sponsor).
Is Compliance Manager required?	The Compliance Manager is a Cardinal application which provides tools to identify transactions that require Strong Customer Authentication (SCA), and enables you to configure rules for handling these transactions.



Field	Description
	<p>This option is mainly relevant to Issuers (BIN sponsors) in the European Economic Area (EEA) and in other regions who want to conform to the Second Payment Services Directive (PSD2). See Creating Rules in Compliance Manager.</p> <p>Note: In the Cardinal Access tab of the 3DS PSF, please specify the users who you want to be set up with access to Compliance Manager.</p> <p>Note: For training on how to use Compliance Manager, please contact your 3D Secure project manager.</p>
Customer Support number	The Customer Support phone number, including the country code, for cardholders to contact.
Issuer regulator country	The regulatory country of your Issuer (BIN sponsor).
Are you PCI Compliant?	Select YES or NO. If your organisation is not PCI compliant, this affects the type of card information, such as PAN, which your systems are allowed to process and store.
Do you have an existing ACS Provider?	Whether you currently have a different provider of 3D Secure services/ a different Access Control Server (ACS). Select YES or NO.
Have you been assigned full BIN range? Or sub BIN	If you are using a full BIN Range for your programme, select YES, else select NO.
Planned Go Live date	<p>When do you plan to launch your card programme?</p> <p>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.</p>
Thredd Environment under which Program Manager is built	<p>Indicate your current production environment. For example:</p> <ul style="list-style-type: none"> • PRD1 – European Cloud production environment • PRD2 – Asia-Pacific Cloud production environment
Do you require Thredd to validate the AAV/CAVV?	<p>The AAV/CAVV is a cryptographic value which is included in the authorisation message request from the Merchant¹. It indicates that the 3D secure authentication session was successful. You can request that either Thredd or the Card Scheme (Mastercard, Visa, or Discover) validate this value. Card Scheme validation is typically required if you want the card Scheme to provide Stand-In processing.</p> <p>If YES: Thredd will validate the AAV/CAVV. To set this up:</p> <ul style="list-style-type: none"> • Mastercard – keys must be exchanged between Thredd and Cardinal; No action is required from the Program Manager. • Visa – keys must be exchange between Thredd and Cardinal. Please ensure your Client Information Questionnaire (CIQ) has the correct settings (under the VisaSecure section > ABE1 > K01. Select “I”). • Discover – keys must be exchanged between Thredd and Cardinal. Please ensure you have informed your Discover Implementation Manager that Thredd will validate the CAVV. <p>If NO:</p> <ul style="list-style-type: none"> • Mastercard – please ensure the BIN has been enroled with the required validation set up at Mastercard (i.e. Mastercard On-Behalf of Services (OBS) AAV Verification Service). • 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 Visa to generate

¹The 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
	<p>the CAVV key and encrypt with Cardinal ZCMK (BIN = 763641 and ZCMK KCV = 89CEE0). Share the CAVV key file securely with your Thredd Implementation Manager.</p> <ul style="list-style-type: none"> Discover - Discover will validate the CAVV. Please request for Discover to generate the CAVV key and share it to Cardinal.
Setup Options (provide details for Test and Production separately)	
Default authentication	<p>Select the default authentication type to support all sub-BIN ranges. Options are:</p> <ul style="list-style-type: none"> Biometric SMS OTP KBA OUTOFBAND ALL² <p>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 Cardinal; c) to support auto-enrolment.</p> <p>Note: Please discuss with your Implementation Manager before implementing OOB authentication.</p>
Fallback authentication	<p>Select the fallback authentication type to support all sub-BIN ranges. Options are:</p> <ul style="list-style-type: none"> SMS OTP KBA OUTOFBAND ALL None <p>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 Cardinal, if the default type cannot be used for any reason.</p>
Biometric validation timeout	<p>The period (in seconds) you have to respond to a request for Biometric validation before the system times out³. The maximum is 900 seconds.</p> <p>This is the time from when we notify you to start authentication, up to your validation response.</p>
Out of Band validation timeout	<p>The period (in seconds) you have to respond to a request for Out of Band validation before the system times out. The maximum is 900 seconds.</p> <p>This is the time from when we notify you to start authentication, up to your validation response.</p>
NotifyInitiateAction endpoint	<p>The endpoint Thredd should use to send you the Biometric validation request. (Implemented using the NotifyInitiateAction API. See Initiating a Biometric Session)</p> <p>Note: Your endpoint (in both production and UAT) must resolve to a single or set of static IP addresses.</p>
oAuth and NotifyValidate IP Addresses	<p>Provide details of the IP addresses you want Thredd to allow to use the Thredd oAuth server and NotifyValidate endpoint.</p>
Do you need Introspection credentials? (Optional)	<p>Select Yes or No. If you select Yes, Thredd will generate the credentials that will be used to validate the Token.</p>

² ALL includes Biometric and OTP, but not KBA. If Thredd returns ALL, then during the online transaction the cardholder is shown a screen showing all available options and can select their preferred authentication method.

³ The request for validation is sent using the NotifyInitiateAction API to the NotifyInitiateAction endpoint you specify for this service. See [Initiating a Biometric Session](#).



Field	Description
Enable SMS OTP auto enrolment	<p>Options are:</p> <p><i>NO</i>– All cards must be enrolled for OTP SMS and the mobile number must be registered using either Web Services or Cards API; see Using the Card Enrolment API.</p> <p><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).</p> <p><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.</p> <p>Note: Auto-enrolment enrolls all live and active cards. It is not recommended if you wish to exclude some cardholders from enrolment. If using Continuous auto-enrolment, this may restrict your ability to unenrol cards which have been previously enrolled and which currently have a live status. See Section 8.2 Card Unenrolment.</p>
Enable Biometric auto enrolment	<p>Options are:</p> <p><i>NO</i>– All cards must be enrolled for Biometric using either Web Services or Cards API; see Using the Card Enrolment API.</p> <p><i>YES - Initial Load</i> – Thredd creates a Biometric credential for all existing cardholders.</p> <p><i>YES - Continuous</i> – Same as Initial load, however any future cards created will also have Biometric credentials created the same way.</p> <p>Note: Auto-enrolment enrolls all live and active cards. It is not recommended if you wish to exclude some cardholders from enrolment. If using Continuous auto-enrolment, this may restrict your ability to unenrol cards which have been previously enrolled and which currently have a live status. See Section 8.2 Card Unenrolment.Enrol_cards_in_3DSecure.htm</p>
KBA Setup Options (provide details for Test and Production separately)	
KBA questions	Enter the KBA questions you want to include. For each KBA question, indicate if required. You can also provide questions in other languages. See KBA Language Support . Thredd will provide you with details of the unique KBA ID linked to each question. You will need to use the relevant KBA ID when enrolling the card for KBA. For more information, see Appendix 4: KBA Questions .
Bin Ranges Low and Bin Ranges High	
Provide the whole range (14, 16, or 19 digit) of the Sub-BIN or BIN. If you do not own the whole BIN, please provide the SUB-BIN range.	
UAT testing cards /UAT product ID	
Provide the staging cards and their product ID you want to use for staging testing.	
Pilot testing cards /Production product ID	
Provide the pilot cards and their product ID you want to use for production testing.	

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

5.2 Cardinal Access

Please provide Thredd with a list of IP addresses you want to allow to access the Cardinal Portal. See [How to Access the Cardinal Portal](#).

For security reasons we can only set up permission lists for client-owned static Office IP addresses; employees working remotely will need to connect securely to their office IP address. Any attempt to access Cardinal from a non-registered IP address will result in the page not being displayed.

Please provide details of the administrator users who need to access the Cardinal Portal. Thredd can set up role-based access for your users to the following Cardinal Portal applications: Customer Service Application, Rules Application, Reporting Application and Admin Application.



Note: Any users Thredd set up with Admin level rights with full access to all Cardinal applications on the Cardinal Portal will be able to create access for additional users.

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



5.3 Supported Languages

Please select the languages you want to support. You must specify a default language. You can specify additional languages and provide the translated text you want to use for each language.

Cardinal identifies the language in which to display the Authentication screens based on the cardholder's web browser language settings (e.g., English, French).

Note: If the cardholder uses a language that has not been configured in Cardinal (i.e., is not provided in the PSF) then Cardinal will show the screens in the default language.

The screen text limit is 350 characters.

5.3.1 KBA Language Support

If you support more than one language, you can provide translations for the Thredd questions in different languages. This is set up per card product. Questions defined in a different language will automatically generate new KBA Question IDs. See [Appendix 4: KBA Questions](#).

Note: Thredd cannot use a different language to what is configured as the language with Cardinal for your BIN/sub-BINs.

5.3.2 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 7: OTP SMS Message Example

The text length limit for the Thredd SMS message is 36 characters. If you pass this limit, the message will be split into two messages.



6 Cardinal Configuration of RDX Biometric and Screens

RDX takes 5-6 weeks to configure at Cardinal. Biometrics is a second phase which takes an additional 4 weeks. All integration steps prior to UAT testing can take place in parallel, while Cardinal sets up RDX and biometric.

6.1 Screens

Note: Screen customisation options are specified using the EMV 3DS Global Consumer Screen Templates Form. For more information, please speak to your Thredd 3DS project manager.

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 translation for the screens. See the examples below for authentication by One-time Password (OTP).

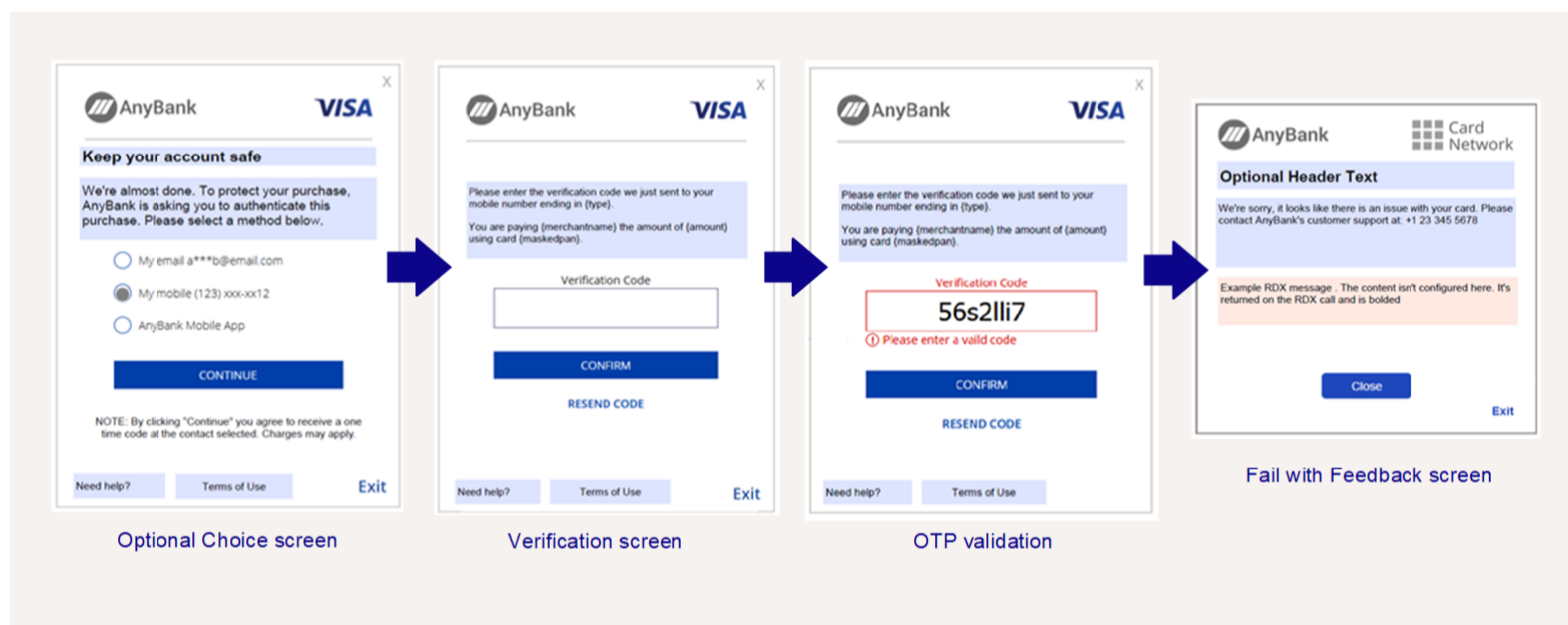


Figure 8: 3D Secure Authentication Screens - for OTP

See the examples below for KBA + OTP authentication.

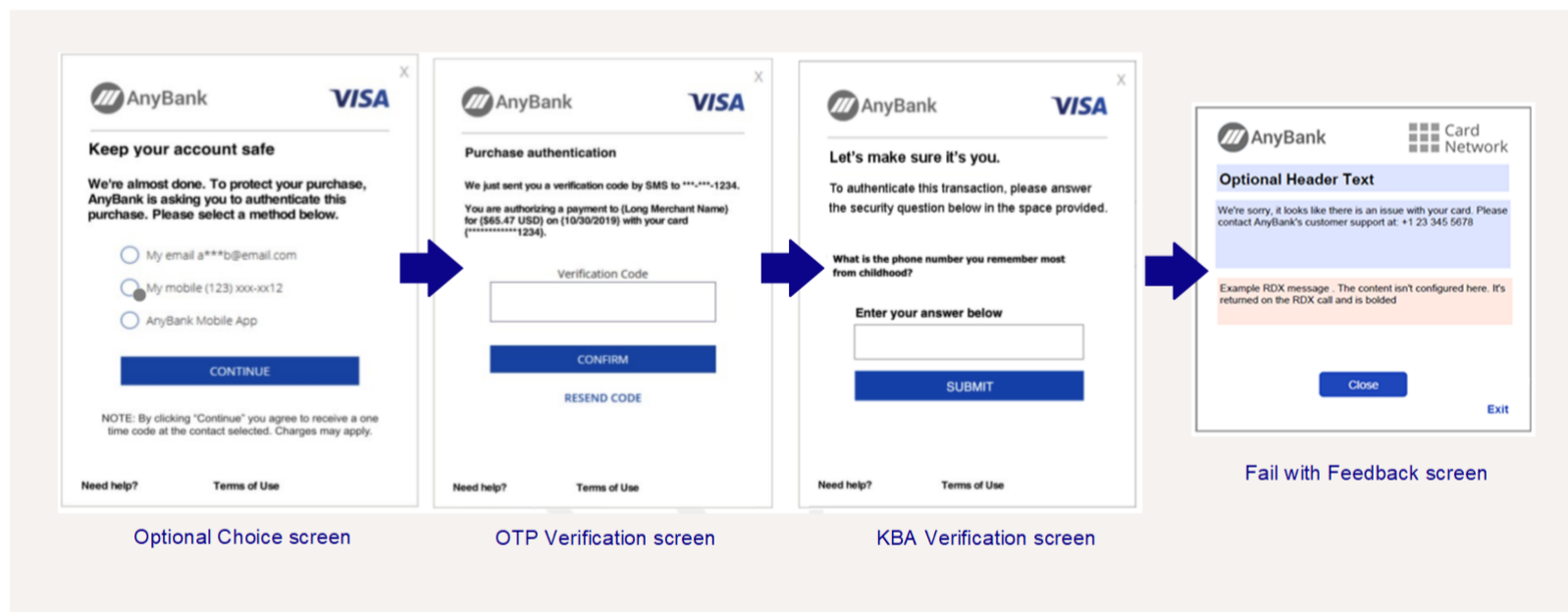


Figure 9: 3D Secure Authentication Screens - for KBA and OTP

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

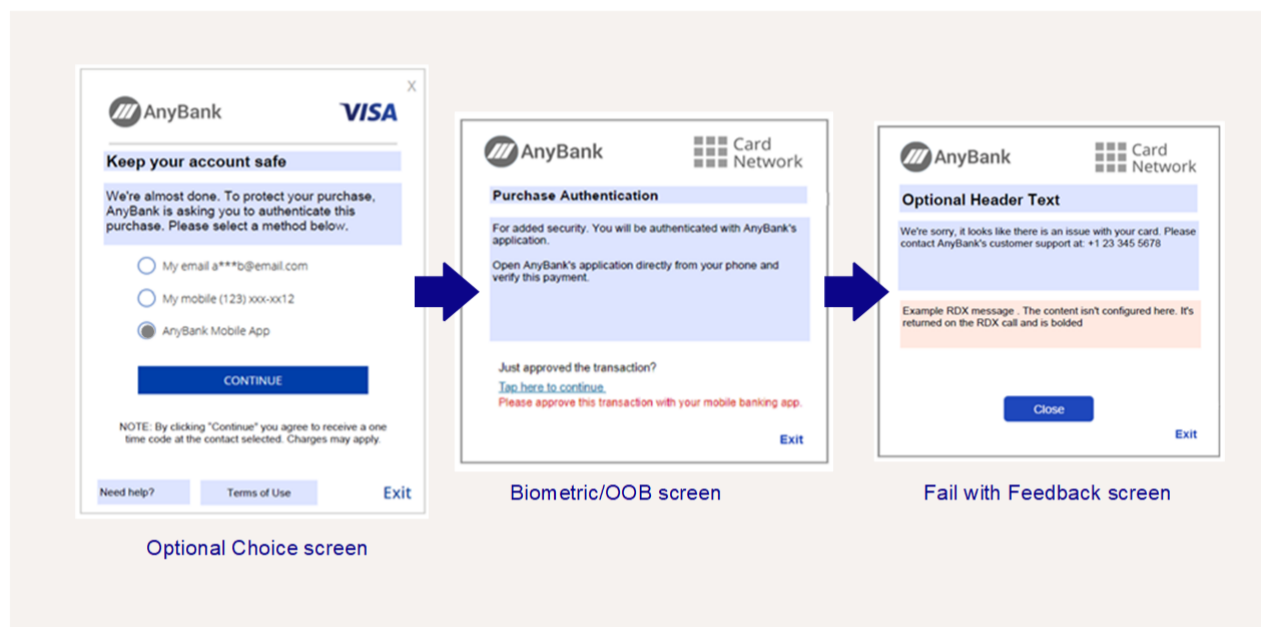


Figure 10: 3D Secure Authentication Screens - for Biometric

For more details on text field customisation, refer to the instructions in the EMV 3DS Global Consumer Screen Templates Form.



7 Integrating RDX Endpoints

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

7.1 Setting up Firewall Permissions

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

You must provide Thredd with a list of IP addresses you will be using, so that we can set up firewall permissions. This includes:

- A list of the IP addresses you will use to access Thredd systems (in both UAT staging and Production).
- The IP addresses you will use for sending API messages to Thredd (in both UAT staging and Production).
- The IP addresses you will use for oAuth (in both UAT staging and Production) to be authorised at Thredd.

You will need to permit access on your systems to [Thredd oAuth](#) and [3D Secure RDX API](#) calls (in both UAT staging and Production). For details of the Thredd IP addresses to allow, see [Authorising IP Addresses](#) (Your Thredd 3DS project manager will provide you with details of any additional Thredd IP addresses that may be needed.)

7.2 Implementing the Biometrics API

Please provide Thredd with the [NotifyInitiateAction](#) API endpoints we should use to send Biometric verification requests to your systems (one for UAT staging and one for Production). You should provide these details on your 3DS Product Setup Form. See the section [Client Information](#).

When your systems receive a request at this endpoint, they should initiate a Biometric or In-App session as described in the section [Using the Biometric/In-App Authentication API](#).

Once completed, your systems should return the result to Thredd, using the [NotifyValidate](#) API. See [Notifying Thredd of the Result of the Biometric Session](#).

7.3 Implementing oAuth Access

You must authenticate against the Thredd oAuth server before you can use the 3D Secure RDX API services. The oAuth server provides you with a token that you must include in your API requests to access the RDX API services. You can also use the oAuth server to validate the Token in the [NotifyInitiateAction](#) API requests received from Thredd.

For details, see [Using the Thredd oAuth Server](#).



8 Enrolling your cards in 3D Secure

You can enrol your cards in 3D Secure using either the Thredd 3D Secure RDX Enrolment Thredd API or the Cards API . 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 migrating existing cards to 3D Secure, Thredd can automatically enrol all your cards in the 3D Secure RDX service: you can request auto-enrolment by specifying the authentication 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 Web Services 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 Web Services 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. When set to continuous, these cards are enrolled again automatically when approaching the expiry date. Applying any changes to credentials for existing cards must be done using either the Thredd API or the Cards API; see [Using the Card Enrolment API](#)

Thredd auto-enrols the card in the default main and fallback authentication types set for your card product. 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](#).

Note: Auto-enrolment enrolls all live and active cards. It is not recommended if you wish to exclude some cardholders from enrolment.

8.2 Card Unenrolment

For cards which have been enrolled manually or auto-enrolled, you can un-enroll the card if required by deleting the credentials linked to the card using Thredd's 3DS Webservice or the Card Enrolment API.. If using continuous autoenrolment, note that cards cannot be un-enrolled if the card status is still live and active. The Program Manager needs to disable Autoenrolment and switch to using the Card Enrolment API before unenrolling cards. To disable Autoenrolment on your products, speak to your Thredd Implementation Manager or Customer Support Specialist.

Note: Thredd does not automatically unenrol cards on behalf of Program Managers. If the status of the card changes to statuses such as Destroyed, Lost, or Stolen, the Program Manager needs to unenrol the respective cards using the 3DS webservice, [Ws_AddUpDelCredentials](#) (SOAP), or the 3DS credentials API (REST).



9 Completing Staging/UAT Testing

Once the authentication screens are configured, Thredd and Cardinal release the project into the Staging environment for you to test.

9.1 Set up Rules in the Cardinal Portal

Thredd will set up your account and provide you with your user credentials to access the Cardinal Portal.

Note: Access is only via permitted IP addresses. Please send Thredd a list of IP addresses you want to add to the authorised access list in Cardinal.

9.1.1 How to Access the Cardinal Portal

You can log in at:

<https://identiportalstaging.cardinalcommerce.com/home/dashboard>

See the example below:

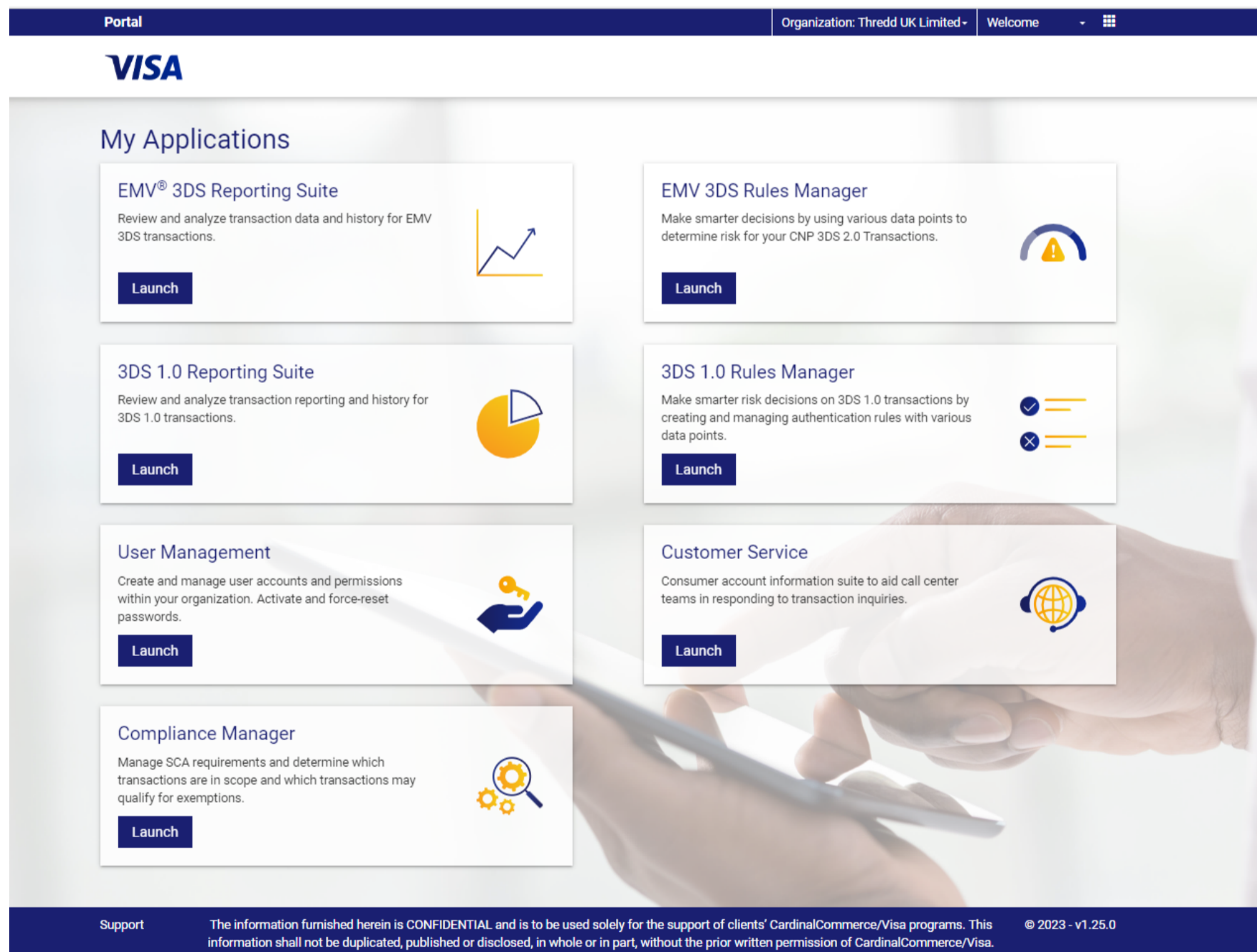


Figure 11: Cardinal Portal

In the Cardinal Portal, create your 3D Secure policy and set up the rules required to trigger Success, Fail/Reject or Challenge outcomes. You should complete rules for both 3DS 1.0 and 3DS 2.0. For details, see Appendix 1: Cardinal 3D Secure Rules.

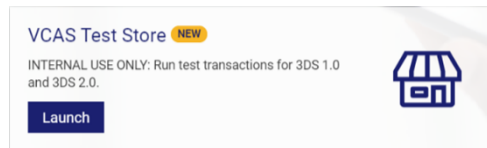
For more information on how to use the Cardinal Portal, including arranging training sessions, please contact your 3DS project manager.



9.1.2 Using the Cardinal Test Simulator

You can start testing in Staging using the Cardinal Test Simulator:

1. Log in to the Cardinal Portal and in the **VCAS Test Store** box, click **Launch**.



2. This opens the VCAS Test Store web form, where you can submit test transactions. See the example below:

Figure 12: VCAS Test Store

You can use the **Test Setup** and **Additional Fields** sections to configure the test details (such as IP address, merchant country and merchant category code).

We recommend you test different use case scenarios, based on the Policy rules you have set up in Cardinal, to trigger *Success*, *Reject/Fail/Fail with feedback* or *Challenge* outcomes. For example, test different amounts, merchant categories, IP addresses, countries and account types.

Note: When testing using the simulator, the authentication screens for OTP and Biometric are displayed and you will be able to complete the simulation of the OTP and Biometric authentication.

9.1.3 Viewing 3D Secure Transactions and Unblocking Cards

The Cardinal Portal enables you to view 3D Secure transactions processed on the system and unblock any blocked cards (e.g., cards blocked due to too many failed 3D Secure attempts).

Note: You must be PCI Compliant in order to view the full card PAN,



10 Completing Pilot Production Testing

Thredd and Cardinal set up your cards in the Production environment:

- Thredd activates a *single card product* in the Production environment, so you can enrol a few cards for the production pilot testing.
- You provide Cardinal with your pilot cards to be enrolled at the Scheme.
- Cardinal contacts the Scheme to set your pilot cards live with 3DS Cardinal.

10.1 Configuring Rules in Cardinal Portal Production

You can configure your rules in the live Cardinal Portal at:

<https://identiportal.cardinalcommerce.com/home/dashboard>

Note: You must access this link from a trust-listed IP address (as you provided on the 3D Secure PSF).

You can register the cards for the supported 3D Secure authentication types: if using the Thredd API, then use the 3D Secure RDX 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 5: 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 Policy rules you have set up in Cardinal, to trigger a *Success, Fail, Reject* or *Challenge* outcome. For example, test different amounts, merchant categories, IP addresses, countries and account types.
- 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 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 pair 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 Cardinal Portal.

Note: Mastercard provides Test Cases for testing the 3D Secure service in different scenarios. For details, speak to your 3DS project manager. You will be notified by your issuer (BIN sponsor) if it is required for your program.

10.2 Rolling out to Production (Live)

Notify Thredd once you have completed your pilot testing.

Cardinal contacts the Card Scheme to set all your Sub BIN/BIN ranges live. You can confirm the full production 3DS roll out with the Scheme.

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

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

Note: Once your sub-BIN/BIN ranges are live with the Scheme, the card must be enrolled for 3D Secure, otherwise any transactions on the card where authentication is required will fail.



11 Authorising Thredd IP Addresses

The following URLs must be allowed on your firewall to enable OAuth and RDX API communication to support Biometric/In-App authentication:

UAT Environment (RDX.API)

Endpoint	Server name	Inbound IP	Outbound IP	Components
https://vcasuat.globalprocessing.net	GPS-UAT-RDX-01	3.10.135.193	3.10.135.193 3.9.27.216	GPS.VCAS.RDX.API
https://oauthuat.globalprocessing.net	GPS-UAT-RDX-01	3.10.135.193	3.10.135.193 3.9.27.216	GPS.Identity.Api

PRDZ Cloud Production Environment

Endpoint	Inbound IP	Outbound IP	Components
https://p0ivcas.globalprocessing.net	3.10.200.197 3.10.133.128	3.10.200.197 3.10.133.128	GPS.VCAS.RDX.API
https://p1ists.globalprocessing.net	3.10.200.197 3.10.133.128	3.10.200.197 3.10.133.128	GPS.Identity.Api

PRD1 Cloud Production Environment

For secure RDX API communication between Thredd and your systems when using one of our cloud-based production environments, please allow the following public IP address on your firewall: 91.194.25.213 and 91.194.25.212.

Note: PRD1 is for Thredd clients using the Cloud Europe Instance of Thredd platform.

Your firewall also allows the following additional IP addresses:

Endpoint	Environment	Server name	IP	Components
p1ivcas.globalprocessing.net	PRD1	P1B-I2-RDX01 P1A-I2-RDX01	18.156.16.255	GPS.VCAS.RDX.API
p1ists.globalprocessing.net	PRD1	P1B-I2-RDX01 P1A-I2-RDX01	3.123.216.247	GPS.Identity.Api

PRD2 - Cloud Production Environment

For secure RDX API communication between Thredd and your systems when using one of our cloud-based production environments, please allow the following public IP address on your firewall: 91.194.104.212 and 91.194.104.213.

Note: PRD2 is for Thredd clients using the Cloud Asia Pacific Instance of Thredd platform.

Your firewall also allows the following additional IP addresses:

Endpoint	Environment	Server name	IP	Components
p2ivcas.globalprocessing.net	PRD2	P2B-I2-RDX01 P2A-I2-RDX01	3.1.92.70	GPS.VCAS.RDX.API
p1ists.globalprocessing.net	PRD2	P2B-I2-RDX01 P2A-I2-RDX01	3.1.92.70	GPS.Identity.Api





12 Using the 3D Secure API

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

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



13 Using the Card Enrolment API

You can use either the Thredd API or the Cards API 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 the Thredd API

If you are using our Thredd API, 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](#)) Thredd 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 [Web Services Guide \(SOAP\)](#).

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. This will be used together with the phone number set up for the card, for 3D secure SMS OTP messages:

```
<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>
```

Notes

- Your card sub-BIN/BIN range must be set up for 3D Secure 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 Cardinal.
- 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 store¹. 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](#)) Thredd API (see the [Web Services Guide \(SOAP\) > Card Renew](#)), or the [Card Renew Cards](#) API endpoint.

Renewing the card may 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.

¹ Answers 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 Biometric/In-App Authentication API

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

- [NotifyInitiateAction](#) - sent by Thredd to notify you to set up an authentication session
- [NotifyValidate](#) - you use this to send the authentication result to Thredd.

14.1 Initiating a Biometric Session

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

See the example below:

Thredd Request

```
{ "Pubtoken": 812561666,
  "GPSInitiateActionID": "ade509f0-7ea8-43a4-8c07-6c5e17076987",
  "MessageVersion3DS": "1.0.2",
  "Credential": {
    "Id": "000000000000000000000000000000669",
    "Type": "BIOMETRIC",
    "Text": "TEST_BIOMETRIC_OTP_VALUE"
  },
  "ChannelCreated": "GA",
  "MerchantInfo": {
    "AcquirerID": "5555555",
    "MerchantID": "12345678",
    "MerchantName": "Amazon",
    "MerchantURL": "https://www.amazon.com",
    "MerchantCategoryCode": null,
    "MerchantCountryCode": "UK",
    "MerchantAppRedirectURL": "merchantScheme://appName?transID=b2385523-a66c-4907ac3c-91848e8c0067"
  },
  "TransactionInfo": {
    "TransactionTimeStamp": "2020-08-17T10:35:32.061Z",
    "TransactionAmount": 1000,
    "TransactionCurrency": "826",
    "TransactionExponent": 2
  }
}
```

Notes

Thredd token of the card to authenticate:

```
{ "Pubtoken": 812561666,
```

The last digits are the credential Id for this card 669:

```
"Id": "000000000000000000000000000000669",
```

Merchant and transaction details. You can optionally configure your app to confirm any of these details during the Biometric authentication:

```
"MerchantName": "Amazon",
MerchantURL": "https://www.amazon.com",
"MerchantCategoryCode": null,
"MerchantCountryCode": "UK",
"MerchantAppRedirectURL": "merchantScheme://appName?transID=b2385523-a66c-4907ac3c-91848e8c0067"
```

```
"TransactionTimeStamp": "2020-08-17T10:35:32.061Z",
"TransactionAmount": 1000,
"TransactionCurrency": "826",
"TransactionExponent": 2
```

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



Your Response

Upon receipt of a request, your systems should return a 200-HTTP response code.

Note: Thredd does not resend the request if the 200-HTTP response to the [NotifyInitiateAction](#) request is not received. The authentication session will time out if Thredd does not receive your [NotifyValidate](#) request. See [Validation Timeout](#).

When your systems receive the [NotifyInitiateAction](#) request, you can optionally use the Thredd OAuth server to validate the token, to confirm it is from Thredd. See [Validating the Token \(optional\)](#)

The customer should then be prompted 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.

Validating the Token (optional)

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

```
Authorization: Bearer eyJh-
bGciOiJSUzI1NiIsImt-
pZCI6IjE5ODI3Q0E4M0NEMkNGNUUzMTAxMUVBQkQ0N0ZDNTg4RkMyRjQ3RTIiLCJ0eXAiOiJh-
dCtqd3QiLCJ4NXQiOiJHwUo4cUR6U3oxNHhBUjZyMUh-
fRm-
lQd3ZSLUki-
fQ.eyJ0eXkiOiJlZ2M1MzZk-
sImV4cCI6MTYwNzU0NzZk30SwiaXNzI-
joi-
aHR0cHM6Ly9vYXV0aHVi-
dC5n-
bG9iYWx-
wcm9jZXRz-
aW5nLm5ldCI6ImF1ZCI6WyJyZWh-
hcGkiLCJmaXJi-
aW9tZXRy-
aWNh-
cGkiXSwiY2x-
pZW50X2lkIjoizmlyYmlyIiwic2NvcGUlOiJyY2xpZW50X3ZhbG1kYXRlIiwiaWF0Ij0iLCJ0eXkiOiJlZ2M1MzZk-
bJ41QF1LZyqxaRMZWAUxurXJwIWRG2wtC0Q1KFzVPbZhpwKAwJvQTIymJFhryEvRUGTQqM61Nwu_Dnsx8H-Jpi7_0PjQk4MaAhqFv6MEgDMHvxUZ2_Q6vYj_-
h2rRDunHjBvhvA55-yGLdqxeHRtNvHJQCsaVZHDLBngUpeFpWcwrhbK1SYbN1G1f1YBm5aAX_YDwpWt4p_M6w7TAYJZQvc4Hi_NqAZwUOY7x01-
hVD69onUmd74k6nt0ncowGgC3naWQieqcVMd3B1kCannYZfL1XMhSxeN_XqWtjKTK3WmavYj6vrv
```

You can optionally verify the token (check that it is valid and active) using the OAuth introspect API endpoint. See [Using the Thredd OAuth Server](#).

Note: The token expires after 4 hours (14400 seconds).

14.2 Notifying Thredd of the Result of the Biometric Session

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

API Endpoints

UAT: <https://vcasuat.globalprocessing.net/api/v1/NotifyValidate>

Production:

PRDZ: <https://p0ivcas.globalprocessing.net/api/v1/NotifyValidate>

PRD1: <https://p1ivcas.globalprocessing.net/api/v1/NotifyValidate>

PRD2: <https://p2ivcas.globalprocessing.net/api/v1/NotifyValidate>

See the example JSON message below:

Your Request

```
{"Pubtoken":987654321,
"ProgMgrCode":"ABC",
"GPSInitiateActionID":"e459b9d8-9703-43a4-bf71-9426fc235c25",
"PMReferenceID":"637441368856932254",
"Status":"SUCCESS",
"Error":null}
```



Notes

Thredd token of the card that was authenticated:

```
{"Pubtoken":987654321,
```

The result of your authentication: SUCCESS, STEPUP, FAILURE, FAILWITHFEEDBACK or ERROR:

```
"Status":"SUCCESS",
```

Thredd Response

```
{
  "Pubtoken":987654321,
  "GPSInitiateActionID":"e459b9d8-9703-43a4-bf71-9426fc235c25",
  "PMReferenceID":"637441368856932254",
  "Status":"SUCCESS",
  "Error":{
    "ReferenceNumber":"","
    "Description":"","
    "Message":""}
}
```

If the cardholder authenticates successfully, you must return the status of SUCCESS. If the cardholder was unable to use the requested authentication method (e.g., Biometric/In-App) you can use the STEPUP status to trigger the fallback option configured for the card (Note that STEPUP will only work if your cards have been enrolled for a fallback option, such as, OTP SMS).

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

If there was any error in your request (e.g., invalid JSON format or incorrect details), Thredd will return details of the error.

Thredd returns the result to Cardinal. For a successful authentication, the transaction proceeds to authorisation. For a failed or timed out authentication, Cardinal will show the Fail with Feedback screen.

Validation Timeout

When Thredd sends the [NotifyInitiateAction](#) message to your system, Thredd expects to receive back a [NotifyValidate](#) response from your system within the validation timeout period (default is 30 seconds and is configurable up to 900 seconds)¹.

If Thredd does not receive the [NotifyValidate](#) response within this period, the authentication session times out. In this case, Cardinal will show the Fail with Feedback screen to the cardholder.

¹ This period starts from when Thredd sends the [NotifyInitiateAction](#) message up to receiving the [NotifyValidate](#).



15 Using Delegated SMS API

The delegated SMS API enables you to receive the 3DS OTP (One-time-password) code from Thredd during the 3D Secure authentication session, allowing you to send the OTP code to the cardholder.

. Thredd provides you with a request in the [DelegatedOTPNotification](#) endpoint containing details of the transaction, the merchant and the OTP. You send a response back to Thredd in order to acknowledge that you received the OTP.

Note: You must acknowledge the request as successful request with a 200 status response within a 10 second timeframe.

Prerequisites

To use the Delegated SMS API, you must first do the following:

- Contact your Thredd Account Manager asking to use this service.
- Supply your [DelegateOTPnotification](#) endpoints for UAT and Production environments.
- Ensure that your firewalls allow Thredd IP addresses. See [Authorising Thredd IP Addresses](#).
- Nominate and share with Thredd the product you're going to test with in UAT and Production environments.
- Enrol cards with OTP SMS credentials to use the Delegated SMS API.

Notification Signature

Note: The verification of the notification signature is optional, though Thredd recommends that you use it.

The notifications JSON body are signed using SHA256withRSA. The signature is included in the [X-Thredd-Signature](#) HTTP header. You can use the public key to verify the authenticity and integrity of the notification.

The process for checking the signature is as follows:

Step 1: Receive the Notification

You receive a JSON notification from Thredd which includes the X-Thredd-Signature header. See the following example:

```
X-Thredd-Signature:
k=I0SqfG1jT-fn_oIeFAypGC66PduPP08XioSKM1ZNoEc,
s=452ad9892d5687bd660eac27428a9301bc363f3db875f8307da25e9b0a231556
```

Step 2: Extract the Signature Info

From the X-Thredd-Signature header, extract the key ID, designated **k** in the header (which tells you which key was used). Then extract the signature, designated **s** in the header (the actual digital signature).

Step 3: Get the Public Key

Use the JWKS Endpoint URL to download a JSON file with the public key included. The following table describes the endpoint URLs you need for each environment.

Environment	JWKS Endpoint URL
UAT	https://keystore.directory.sandbox.threddid.com/906d9a03-836e-4af0-b500-f84ef48247d3/aae5943b-f6ab-4e0a-bb7f-7ddb75c1685a/application.jwks
Production	https://keystore.directory.threddid.com/cf253304-8bbb-44ff-938c-89fd11e9651a/e5a5116a-2de3-4265-9d0a-c0b5bca94c34/application.jwks



Note: The JWKS Endpoint URL is publicly accessible and may need to be whitelisted on the program manager's side, depending on your network security policies. JWKS Endpoint URLs are static and idempotent; they remain unchanged even when certificates are renewed at Thredd's side.

Step 4: Find the Matching Key

Browse the JWKS file for the key with the same kid (key ID). This is the public key that matches the one Thredd used to sign the message.

```
{
  "keys": [
    {
      "kty": "RSA",
      "use": "sig",
      "x5c": [
        "MIIGCzCCBP0gAwIBAgIUJb-
hB6Wa8zD/ikJQik+cRrLZv39cwDQYJKoZIhvcNAQELBQAw-
bTElMAkGA1UEBhMCR0IxBGjAYBgNVBAoTEVRocmVkJZCBVSYBMaW1p-
dGVkMRk-
wFwYDVQQLExBUaHJlZGQgRG1yZWNoY3J5MSswJQYDVQQLEx5UaHJlZGQgU2FuZGJveCBJc3N1aW5nIENBIC0gRzEwHh-
cNMjUwNTI4MDgxNDAwLWw-
cNMjYwNjI3MDgxNDAwLWwB8MQswCQYDVQGEwJHQjEPMA0GA1UEChMgdGhyZWRkMS0wKwYDVQQLExQ5MDZkOWEwMy04MzZlLTRhZjAtYjUwMC1mODRlZjQ4MjQ3ZDMxLTAr-
BgNVBAMTJGFhZTU5NDNiLWY2YWI0NGUwYS1iYjd-
mLTdkZGI3NWwMxNjg1YTCCASIdQYJKoZIhvcNAQEBBQADg-
gEPADCCAQoCg-
gEBAIv5KG+6xPHvcIa2j60WaP0CTrB+9EmgL6DsXtMrdM2WRGUjr062Cbecp-
m00UkxTRjuRRAvDGgcFJG2w3y/GBfgk-
m5A2ZaeFxLOx-
siPcettkWy5zxRjr0swje-
wryHPfyJSAUyA1WX/2JG3g/wWQ5b-
cIORzwt4Vjh7UgV4/d6Wvd3zHu5L2y3BaIUHD+NJJ1B2F3o6+2B/f4XXRjLLhvtIx-
a5o2P-
pod-
w7h4ANv/7tEw8+gYdg3kQhiSV1dL9KtH4qve-
hwXvT1Nh1DvXpaHfDeFEGWSDj/t61DudEuXkGZQjMy1fWIL6-
faF40F9b1yn-
2960v1+VWKDW1SZ3vx566YkCAwEAAaOCAPiWg-
gKOMA4GA1UdDwEB/wQEAwIDuDAMBGNVHRMBAF8EAJAAMB0GA1UdDgQWBBAhKBAbt-
prg1-
fakQadWbcJx8b-
jCjAfbgNVHSMEGDAWgBR7BUKY6bZcNSiIjOCnSgEqeKM-
foDBABg-
grBgEFBQcBAQQ0MDIwMAYIKwYBBQUHMAGGJGh0dHA6Ly9vY3NwLnBraS5zYW5kYm94LnRocmVkJZG1kLmNvbTA/BGNVHR8EODA2MDSgMqAwhi5odHRwOi8vY3JsLnBraS5z-
YW5kYm94LnRocmVkJZG1kLmNvbS9p-
c3N1ZXIuY3JsMIIBqQYDV0gBIIBoDCCAzwg-
gGYBg-
srBgEEAYO6L3EBAjCCAYCwg-
gFCBg-
grBgEFBQcCAjCCATQMg-
gEwVGh-
pcyBDZXJ0aWZpY2F0ZSBp-
cyBzb2x1-
bHkgZm9yIHVzZSB3aXR0IFRocmVkJZCBVSYBMaW1p-
dGVkIGFuZCBvdGh1-
ciBwYXJ0aWw-
cGF0aw5nIG9yZ2FuaXNh-
dGlvb-
nMg-
dXNpb-
mcgVGhyZWRkIFVLIEx-
pbWl0ZWQgc2Vydm-
ljZXMsIGFzIHBy-
b3ZpZGVkIGJ5IHRoZSBidXNpb-
mVzcyBm-
cm9tIHRp-
bWUg-
dG8g-
dGltZS4gSXRzIHJlY2Vp-
cHQsIHBvc3N1-
c3Np-
b24g-
```



```

b3Ig-
dXN1IGNvb-
nN0aXR1dGVzIGFjY2VwdGFuY2Ug-
b2Yg-
dGh1IFRocmVkb2VudHMg-
dGVkIENl-
cnRpZm-
ljYXR1IFBvbG1jeSBhb-
mQgcmVsYXR1ZCBk-
b2N1bWVudHMg-
dGh1-
cmVp-
bjA/Bg-
grBgEFBQCcARYz-
aHR0cDovL3Jl-
cG9z-
aXRvcnkucGt-
pLnNhb-
mRib3gudGhyZWRkaWQuY29tL3BvbG1-
jaWVzMA0GCsQGSib3DQEBcwUAA4IBAQCvBltk3i6XaOPpIo88ar/9JdUZBTlAWkOmUyCNJfZ1id-
bX9t-
nTs0xbAx-
fueD4nR67x03XTN4EDNzj05F6+hr6k3wHarGf0ZKk59hv+ox31Z6U3AjqCCjKVZh8QbY/3j59sF5r/s03D44o-
gDxJB1hgDDSRb-
fCDU7PGhBxxHIVm17Yp-
bXKq7/0qZB70r/VkFt3Unu3xkIC06p-
g+PdiJAP2gNXKM0HPd3Jsqx4AMFSjz80z-
sKEiMVTko+C9q7eBE/bk7MhQjkS7iKhgCLcxuX0Guh0xjEeCE7NBQvYQ+z5Lbh/yHQ1lPtWGCvjyisoh0bWkDnaWWSbhBSsmsE9xROveE"
  ],
  "n": "im_kob7rE8e9whraPo5Zo_QJ0sH70SaAvo0xe0yt0zZZGBS0vTrYJt5ymY45STFNG05FEC8MaBycUkbbDfL8YF-CSb-
kDZlP4XEs7GyI9x622RZjnPFEmvSzCN7CvIc9_I1IBTIDVZf_YkbeD_BZD1twg5HPC03hW0HtSBXj93pZV3fMe7kvbLcFohQcP40knUHYXejr7YH9_hddEksuG-
0jFrmjY-mh3DuHgA2__u0TDz6Bh2DeRCGJJWV0v0q0fiq96HBe9PU2HU09e1od8N4UQZZIOP-3rU050S5eQZ1CMzLV9Ygvp9oXjQX1vXKfb3rS-X5VYoNaVJne_
HnrpiQ",
  "e": "AQAB",
  "kid": "I0SqfG1jT-fn_oIeFAypGC66PduPP08XioSKM1ZNoEc",
  "x5u": "https://keystore.directory.sandbox.threddid.com/906d9a03-836e-4af0-b500-f84ef48247d3/aae5943b-f6ab-4e0a-bb7f-
7ddb75c1685a/ndqXpdRi_k46QLcLP7CmvJSKZx7VfFuc52J8G2kSiGc.pem",
  "x5t#S256": "ndqXpdRi_k46QLcLP7CmvJSKZx7VfFuc52J8G2kSiGc",
  "x5dn": "CN=aae5943b-f6ab-4e0a-bb7f-7ddb75c1685a,OU=906d9a03-836e-4af0-b500-f84ef48247d3,O=thredd,C=GB"
}
]
}

```

Step 5: Verify the Signature

Use your programming language's library to verify the signature. Check that the signature is valid for the JSON body you received, using the public key in the JWKS JSON file.

DelegatedOTPNotification Example Request

The following is an example [DelegatedOTPNotification](#) request.

```

{
  "Pubtoken": 100111111,
  "DelegatedOtpId": "24b78815-7547-4768-b1f8-9a07ebbd3a3b",
  "MessageVersion3DS": "1.0.2",
  "Credential": {
    "Id": "000000000000000000000000000000002045695",
    "Type": "OTPSMS",
    "Text": "xxxxxxxxx6385"
  },
  "MerchantInfo": {
    "AcquirerID": "1234567",
    "MerchantID": "123456789",
    "MerchantName": "Test Merchant",
    "MerchantURL": "www.test.com",
    "MerchantCategoryCode": "2468",
    "MerchantCountryCode": "840",
    "MerchantAppRedirectURL": "merchantScheme://appName?transID=b2385523-a66c-4907ac3c-91848e8c0067"
  }
}

```



```
},
"TransactionInfo": {
  "TransactionTimeStamp": "2021-12-17 15:48:23.2877",
  "TransactionAmount": 1000,
  "TransactionCurrency": "826",
  "TransactionExponent": 2
},
"Passcode": "123456",
"MobileNumber": "+911234567890",
"MessageContent": "123456 is the One Time Password for purchase of GBP 10.00 at Test Merchant with card ending 6443 . Please use the One Time Password to complete the transaction."
}
```

A successful response returns a 200 status.

Note: For more information on the DelegatedOTPNotification endpoint fields, see [Appendix 6: DelegatedOTPNotification Fields](#).



16 Using the Thredd oAuth Server

You must authenticate against the Thredd oAuth server before you can use the 3D Secure RDX Biometric API services. The oAuth server provides you with a username (`client_ID`) and a secret password (`Client_secret`) that you will need to include in your API requests in order to access the RDX API services. You can also use the oAuth server to validate any API requests received from Thredd; Thredd will provide 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>

16.1 oAuth API Endpoints

Thredd provides two oAuth API endpoints:

- `token` - you can use this to obtain a token. Whenever you use the RDX 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 `NotifyInitiateAction` endpoint (to notify you of a request to initiate a Biometric/In-App session)

Thredd oAuth endpoints are listed below.

UAT:

Token endpoint: <https://oauthuat.globalprocessing.net/connect/token>

Introspect endpoint: <https://oauthuat.globalprocessing.net/connect/introspect>

Production:

Token endpoint: <https://p1ists.globalprocessing.net/connect/token>

Introspect endpoint: <https://p1ists.globalprocessing.net/connect/introspect>

16.1.1 oAuth User Credentials

Please check with your Thredd 3DS project manager for your `client_id` and `client_secret` to access the oAuth server.

16.1.2 oAuth Token Expiry

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

16.2 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 oAuth server returns a token, which you must include in any 3D Secure RDX requests.

Below are examples of an oAuth Token request and response.

Request

```
POST https://oauthuat.globalprocessing.net/connect/token
Accept: application/json
Content-Type: application/x-www-form-urlencoded
client_id=9d70c6bbad8ad202628222fc0f3fdd
&client_secret=a3d5566e8ca0d6da823eb7815c1c2b66
&grant_type=client_credentials
```

Response (Successful)

```
200 OK
```




17 Cardinal ADX

Cardinal Authentication Data Exchange (ADX) is an API used to send the authentication result of a transaction from the Visa Consumer Authentication Service (VCAS) to a third party, such as an issuer or other relevant entity.

Thredd leverages the Cardinal ADX API using our Event Delivery System (EDS), where you can create webhooks to return notification events.

The event type for Cardinal ADX is event code 114, which returns detailed information on the ADX Authentication Result event.

Note: For more information on how to create a webhook, see [Introduction to Webhooks](#).



17.1 Event Code 114 - Detailed Cardinal ADX Event

The 114 event code is used when Cardinal sends a detailed ADX Authentication Result event. This notification includes detailed information on the transaction, merchant, payment and cardholder.

After a webhook for event code 114 has been successfully set up, when Cardinal send a detailed ADX authentication result event, a notification response is sent from the Event Delivery Service to the URL specified in the webhook. See the below example of a response.

```
{
  "context": {
    "notificationId": "f47ac10b-58cc-4372-a567-0e02b2c3d479",
    "eventCode": 114,
    "eventVersion": "v1",
    "notificationTime": "2024-01-24T23:20:28Z"
  },
  "payload": {
    "webRequestId": "3479b99f-40b5-95c2-a73c-9e83b644f765",
    "dsTransactionId": "00ec043e-40b5-4ce4-95c2-9e83b644f412",
    "requestId": "0fe3b99f-8c52-41cf-a73c-0107fef56e3",
    "issuerOrgId": "5723c1870063ac1a9c3ab07c",
    "cavv": "AAIBASR0YAAAAN6vhACIdQ8DKJSL",
    "cavvHex": "0002010124746000000DEAF8400887500073512",
    "eci": "05",
    "messageVersion": "2.2.2",
    "authenticationResponse": "Y",
    "authenticationType": "OTP",
    "riskScore": "50",
    "transStatusReason": "01",
    "merchantChallengeIndicator": "NoPreference",
    "pubtoken": "123456789",
    "merchantInfo": {
      "acquirerId": "55554444",
      "acquirerCountryCode": "826",
      "merchantId": "12345678",
      "merchantName": "Ranier Expeditions",
      "merchantURL": "www.google.com",
      "merchantCategoryCode": "5734",
      "merchantCountryCode": "372"
    },
    "transactionInfo": {
      "transactionTimeStamp": "2024-03-21T20:55:49.000Z",
      "transactionAmount": 1000,
      "transactionCurrency": "840",
      "transactionExponent": 0,
      "transactionAmountUSD": 1248,
      "transactionType": "Purchase",
      "purchaseType": "GoodsOrService",
      "channel": "WEB",
      "flowStatus": "Fully Authenticated",
      "addressMatch": "Y",
      "ruleTriggered": "Low-Risk Rule",
      "merchantAdditionalData": {
        "shippingIndicator": "ShipToBillingAddress",
        "deliveryTimeFrame": "ElectronicDelivery",
        "deliveryEmailAddress": "user@user.com",
        "reorderItemsIndicator": "FirstTime",
        "preorderPurchaseIndicator": "MerchandiseAvailable",
        "preorderDate": "20240828",
        "giftCardAmount": 10000,
        "giftCardCurrency": "840",
        "giftCardCount": 1
      },
      "vcasPanStatus": "Active",
      "paymentInfo": {
        "cardNumber": "123456789098877655",
        "cardExpiryMonth": "01",
        "cardExpiryYear": "2028",
        "cardType": "Credit",
        "cardHolderName": "Johnny B Goode"
      }
    }
  }
}
```



```
    },
    "billingAddress": {
      "firstName": "Johnny",
      "middleName": "B",
      "lastName": "Goode",
      "address1": "123 Main Street",
      "address2": "Apartment 99",
      "address3": "NA",
      "locality": "Anytown",
      "region": "IA",
      "postalCode": "52227",
      "countryCode": "826"
    },
    "shippingAddress": {
      "firstName": "Johnny",
      "middleName": "B",
      "lastName": "Goode",
      "address1": "123 Main Street",
      "address2": "Apartment 99",
      "address3": "NA",
      "locality": "Anytown",
      "region": "IA",
      "postalCode": "52227",
      "countryCode": "826"
    },
    "consumerInfo": {
      "emailAddress": "user@user.com",
      "phoneNumber": "+14151231234",
      "mobileNumber": "+14151231234",
      "workNumber": "+14151231234"
    },
    "consumerWalletInfo": {
      "provider": "Apple",
      "walletAge": 10000,
      "paymentCardAge": 10000
    },
    "deviceInfo": {
      "userAgent": "Google Chrome",
      "ip": "123.567.22.980",
      "latitude": "38.8951",
      "longitude": "-77.0364",
      "browserAcceptHeader": "*/*",
      "browserJavaEnabled": "True",
      "browserJavascriptEnabled": true,
      "browserLanguage": "en-US",
      "browserColorDepth": "24",
      "browserScreenHeight": "960",
      "browserWidth": "1536",
      "browserTimeZone": "-330",
      "platform": "Android",
      "deviceModel": "Android",
      "operatingSystemName": "Marshmallow",
      "operatingSystemVersion": "1.2.3.4",
      "locale": "Denver",
      "advertisingId": "NA",
      "screenResolution": "1080x1920",
      "deviceName": "Android",
      "sdkAppId": "45a2fc4d-d95f-4709-9200-65129b772",
      "deviceExtendedData": "NA"
    },
    "riskProviderInfo": {
      "name": "Cardinal",
      "providerId": "45a2fc4d-d95f-4709-9200-65129b772jdiK",
      "deviceId": "x45e5ca957d4420d8d2cfbb98c6c3f84"
    },
    "mandatedRegion": "NONE",
    "challengeCancel": "01",
    "reasonCodes": {
      "risk": {
        "reasonCode": "Low-Risk",
        "reasonDescription": "Low-Risk"
      }
    }
  }
}
```



```
    },
    "stepUp": {
      "reasonCode": "Low-Risk",
      "reasonDescription": "Low-Risk"
    },
    },
    "initiateAction": {
      "reasonCode": "Low-Risk",
      "reasonDescription": "Low-Risk"
    },
    },
    "validate": {
      "reasonCode": "Low-Risk",
      "reasonDescription": "Low-Risk"
    }
  }
},
"additionalRiskResultInfo": {
  "riskIndicator": "01",
  "deviceIDVelocity": 0,
  "ipVelocity": 0
},
"exemptionInfo": {
  "merchantFraudRate": "1",
  "secureCorporatePayment": "N"
},
"extensionData": {
  "acsrba": {
    "status": "Success",
    "score": "950",
    "decision": "Not Low Risk",
    "reasonCode1": "A",
    "reasonCode2": "GG"
  },
  "emvPaymentToken": {
    "tokenRequestorId": "12345678910",
    "tokenStatusIndicator": "A",
    "tokenAdditionalData": {
      "tokenAdditionalDataVersion": "1.0",
      "tokenCharacteristics": "06"
    },
    "version": "1.0"
  },
  "dafExtension": {
    "authPayCredStatus": "Y",
    "authPayProcessReqInd": "01",
    "dafAdvice": "01",
    "version": "1.0"
  }
},
"threeRIInd": "01",
"threeDSRequestorPriorAuthenticationInfo": {
  "threeDSReqPriorAuthData": "NA",
  "threeDSReqPriorAuthMethod": "01",
  "threeDSReqPriorAuthTimestamp": "2028-08-28T10:23:31.490Z",
  "threeDSReqPriorRef": "NA"
}
}
```

Note: For more information on how to create a webhook for event code 114, see [Webhook Event Codes](#).



18 Additional 3D Secure Considerations

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

18.1 Support for 3D Secure Versions

EMV 3D Secure 2.1 and 2.2 are Card Scheme (payment network) versions for Visa/Mastercard and Discover, as well as smaller networks that use the Mastercard Network Exchange (MNE), such as STAR and Pulse. Thredd and Cardinal Commerce support both versions.

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

Thredd and Cardinal are ready with Visa EMV 3DS 2.1 and 2.2

Thredd and Cardinal support ProtectBuy 3DS 2.1 and 2.2

Note: Visa and Mastercard discontinued support for 3DS 1.0 in October 2022. 3DS 2.1 to be discontinued by card networks in September 2024.

See Appendix 1: Cardinal 3D Secure Rules.

18.1.1 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.

18.1.2 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 the [Cardinal Commerce Website > EMV® 3-D Secure v2.1 vs v2.2: What issuers need to know](#).

18.2 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 Thredd API / Cards API) and as described below:

Type	Description
RBA	Risk-Based authentication (done via Cardinal). The authentication decision is done based on the Cardinal rule's engine, which generate a risk score, based on factors such as country, IP address, merchant category, transaction type and amount. Note: Cardinal automatically enrolls your cards in this service. You do not need to do this via Thredd API or the Cards API.
OTPSMS	OTP SMS authentication. Cardinal 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



Type	Description
	screen to authenticate.
BIOMETRIC	Biometric authentication. Cardinal 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. Cardinal 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.
KBA	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?' Note: KBA is combined with OTP SMS, to meet the two-factor requirement for Strong Customer Authentication (SCA).



Appendix 1: Cardinal 3D Secure Rules

You can use the Cardinal Portal to create rules to trigger a success, reject/fail or challenge outcome on the Cardinal system, based on factors such as the transaction amount, the type of transaction, the merchant category code (MCC), the merchant country, IP address, IP country, Risk score and shipping method. The process is as follows:

1. Create rules for processing of 3D Secure transactions in Cardinal. See [Creating Rules](#).
2. Create a policy and add the required rules. See [Creating Policies](#).
3. Save your policy and select the card BIN ranges the policy applies to.
4. Repeat steps 1 and 3 for any additional rule in the policy.
5. Repeat step 3 for any additional sub-BIN/BIN ranges.
6. If you are using Compliance Manager, then set up any additional rules required for PSD2 and SCA. See [Creating Policies in Compliance Manager](#).

Creating Rules

To create a rule:

1. On the Cardinal Portal dashboard, in the **EMV 3DS Rules Manager** box, click **Launch**.
2. From the menu, select **Rules > Write New Rule**.

Provide a name and configure your rule. Your rule should include the conditions which trigger a specific authentication outcome. See [Rule Outcomes](#).

The example below shows a simple rule to approve transactions for less than 30 USD where the country is UK:

Figure 13: Cardinal Rule Editor

3. Click **Save Rule**.
4. Create the additional rules you require to trigger other outcomes.

You need to save the rule and publish it before adding it to the policy and saving the policy.

Rule Outcomes

Rule outcomes can be one of the following:

Field	Description
Success	The authentication request is Approved. Frictionless authentication approval is provided, and the card can proceed to payment authorisation.



Field	Description
Rejected	The authentication request is rejected. In this case Cardinal will show the status you configured for a rejected transaction. See Authentication Status .
Challenge	Cardinal do cardholder authentication, based on the authentication types the card is enrolled for.
Fail	The authentication request fails. The merchant can attempt payment using a different method.
Fail with Feedback	The authentication request fails with feedback. The response provides the reason for the failure. The message provided depends on what you have filled in the Fail with Feedback screen template in the 3DS Product Setup Form (PSF).

Authentication Status

Cardinal can display the following status values for the result or authentication transaction:

Status	Description
Y	Successful Authentication
N	Failed Authentication
NF	Not Authenticated with Feedback
A	Attempts
MC	Merchant Cancelled
CC	Cardholder Cancelled
I	Incomplete
U	Unavailable

Creating Policies

Your rules should now be added to a 3D Secure policy.

To create a new policy:

1. From the menu, select **Policies > Build New Policy**.
2. In the **Policy Editor** screen, click **Add Rule**.

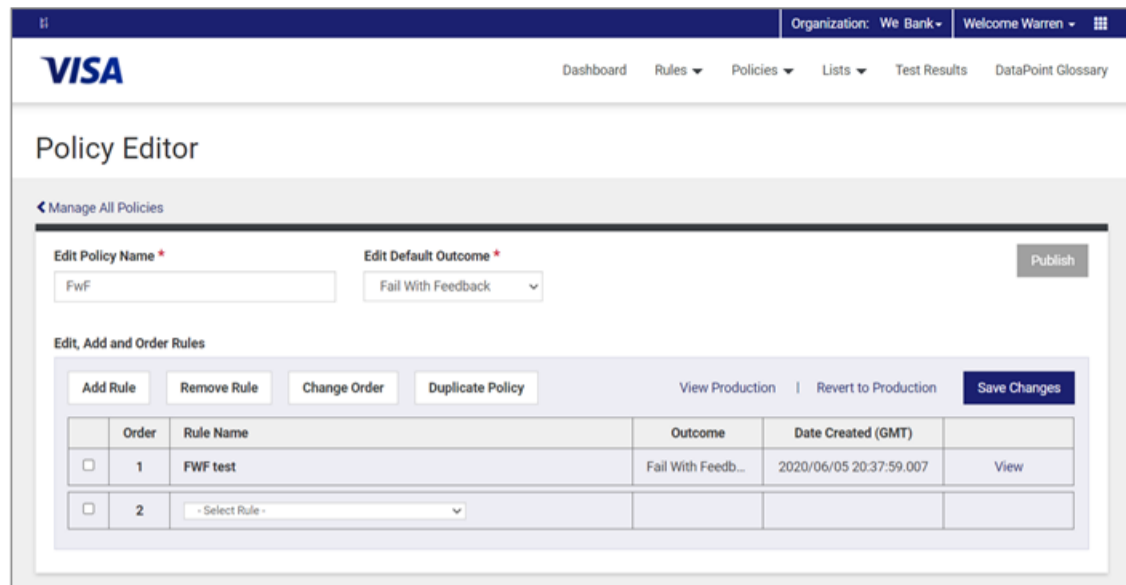


Figure 14: Cardinal Policy Editor

3. Add the rules you previously configured.
4. If you have more than one rule, to change the order of a rules, select the order and click **Change Order**. Then drag and drop the rule in the required order.
5. When you are finished, click **Save Changes**.
6. To publish the policy and link it to a Sub-BIN/BIN range (depending on what have you requested to be configured in Cardinal), click **Publish**.
7. Under **Available BIN Ranges**, select the BINs if they are not already selected.
8. Click **Publish** and **Yes Publish**.



Creating Policies in Compliance Manager

Compliance Manager is a Cardinal application which provides tools to identify transactions that require Strong Customer Authentication (SCA), and enables you to configure rules for handling these transactions. This option is mainly relevant to Issuers (BIN sponsors) in the European Economic Area (EEA) and in other regions who want to conform to the Second Payment Services Directive (PSD2). For more information, refer to the *VCAS Compliance Manager Portal User Guide*.

Note: You will need to request access to the Compliance Manager application as this is only relevant to PSD2 customers and is not provided automatically.

To create a new Compliance Manager policy:

1. From the Cardinal Portal dashboard, in the **Compliance Manager** box, click **Launch**.
2. In the Compliance Manager screen, click **Create a New Policy**.
3. Enter a name for this policy and click **Assign Card Ranges**. Then enter the card ranges that apply to this policy.
4. Switch on the rules which you want to apply to the policy and click **Save Policy**. See **Compliance Manager Rules**.

Compliance Manager Rules

Refer to the table below for details of available rules.

Rule	Description
Smart detection	If enabled, then Cardinal will use the origin of the issuing card and location of the merchant acquirer to determine whether is out of scope for Strong Customer Authentication (SCA), thereby providing a frictionless experience for 'one-leg-out' transactions.
Acquirer transaction risk analysis	If enabled, then any merchants that the Acquirer has flagged as exempt from SCA will not be included in the Cardinal SCA checks. You can also configure rules to customise this exemption, using criteria you define, such as for specific transaction amount thresholds or specific Merchant Category Codes that you want to apply.
Issuer transaction risk analysis	If enabled, enables you to set thresholds below which Cardinal will not apply SCA checks, based on transaction amount and risk score.



Compliance Manager Organization: UK LIMITED Welcome

VISA Dashboard Create a New Policy Change History

Compliance Manager

< Back To Dashboard

Name This Policy

Enter Policy Name Assign Card Ranges Save Policy

Smart Detection

This value-added service can be included to determine if the transaction is in or out of scope for Strong Customer Authentication (SCA)

Cardinal's Smart Detection can determine scope before the transaction is routed to SCA
Detecting the origin of the issuing card and location of the merchant site can provide a frictionless experience for 'One-leg-out' transactions.

More Information:

"One-leg-out" transactions <ul style="list-style-type: none">• EU cardholders shopping online at a merchant site based in Asia• US cardholders shopping online at a merchant site	"Two-legs-in" transactions <ul style="list-style-type: none">• After detecting when "two-legs-in", we'll generate a new value of MandatedRegion = EEA (European Economic Area)• This new field will be used through the Reporting Apps, Rules Apps, RDX, and ADX features
---	---

Acquirer Transaction Risk Analysis

Acquirers assess the risk of the transaction prior to running 3-D Secure and request frictionless authentication unless the transaction meets bypass conditions created below.

Support The information furnished herein is CONFIDENTIAL and is to be used solely for the support of clients' CardinalCommerce/Visa programs. This information shall not be duplicated, published or disclosed, in whole or in part, without the prior written permission of CardinalCommerce/Visa. © 2023 - v1.13.1

Figure 15: Compliance Manager Screen



Appendix 2: OTP Message Templates

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

OTP SMS

Note: If you are customising the text, Thredd recommend you keep your message brief. Otherwise, the message is split into multiple parts, which are sent separately.

Full template

The template can contain OTP, Card Number, Currency, Amount and Merchant Name:

```
@OTP is the One Time Password for purchase of @CUR @Amount at @MerchantName with card ending @CardNumber.  
Please use the One Time Password to complete the transaction.
```

Note: The *@CardNumber* is the last 4 digits of the card number.

If merchant information is not present

```
@OTP is the One Time Password for purchase of @CUR @Amount with card ending @CardNumber.  
Please use the One Time Password to complete the transaction.
```

If transaction information is not present

```
@OTP is the One Time Password for purchase at @MerchantName with card ending @CardNumber.  
Please use the One Time Password to complete the transaction.
```

If both transaction and merchant information are not present

The template can only contain the OTP and card number:

```
@OTP is the One Time Password for purchase with card ending @CardNumber.  
Please use the One Time Password to complete the transaction.
```



Appendix 3: Biometric/OOB Fields

This section provides details of the fields used in biometric/OOB [NotifyInitiateAction](#) and [NotifyValidate](#) message requests and responses.

NotifyInitiateAction Message Fields

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

Field	Description	Data type	Length	Status
Pubtoken	Thredd 9-digit public token linked to the card.	Number	Up to 9 characters	Required
GPSInitiateActionID	36-character unique identifier of the NotifyInitiateAction request.	String	36 characters	Required
MessageVersion3DS	3D Secure message version (e.g., 1.0.2).	String	Up to 8 characters	Required
Credential		Object		
ID	Unique credential identifier which Thredd generates during enrolment.	String	36 characters	Required
Type	<p>Credential type:</p> <ul style="list-style-type: none"> • BIOMETRIC • OUTOFBAND <p>SMSOTP is not sent to Program Managers; Thredd sends OTP messages directly to cardholders.</p> <p>Note: Please discuss with your Implementation Manager before implementing OOB authentication.</p>	String	ENUM	Required
Text	Credential value. For example, when type is OTPSMS value is "+447654123456" and when type is BIOMETRIC, value is "YOUR BANK MOBILE APP"	String	Up to 254 characters	Optional
ChannelCreated	<p>How the request was created:</p> <ul style="list-style-type: none"> • GA - Thredd auto-enrolment process. • PM -Program Manager calling Thredd Hyperion API Credential Call <p>Note: Thredd recommends you store credentials upon receiving the NotifyInitiateAction request.</p>	String	ENUM	Optional
MerchantInfo		Object		Optional
AcquirerID	Identifier of the merchant acquirer.	String	Up to 11 characters	Optional
MerchantID	Identifier of the merchant performing the	String	Up to 35	Optional



Field	Description	Data type	Length	Status
	purchase request.		characters	
MerchantName	Merchant name.	String	Up to 40 characters	Optional
MerchantURL	URL or name of the merchant's website or app. (Also known as the RequestorAppUrl field; this is optional data, which the merchant may provide)	String	Up to 2048 characters	Required
MerchantCategory Code	Category code describing the type of merchant business.	String	4 characters	Optional
MerchantCountry Code	Country code of the merchant. For 3DS1 transactions this value is the 2-letter format (e.g., US). For 3DS2 transactions this value is the 3-digit number format (e.g., 840).	String	Up to 3 characters	Optional
MerchantAppRedirectURL	The callback URL for the merchant's app, which your authentication app should use to enable the merchant app to redirect the cardholder back to the checkout page once they have authenticated. ¹ 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		Object		Optional
TransactionTime Stamp	Transaction timestamp in UTC, as per the ISO 8601 UTC specification (e.g., 2019-03-21T20:55:49.000Z).	String	24 characters	Optional
TransactionAmount	Transaction amount in minor currency units (e.g., 1000 for \$10.00).	Number	Up to 48 characters	Optional
TransactionCurrency	3-digit numeric ISO 4217 currency code.	String	3 characters	Optional
TransactionExponent	Exponent for formatting the given ISO 4217 currency code.	Integer	1 character	Optional

NotifyValidate Message Fields

Below are details of the fields in the [NotifyValidate](#) 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
Pubtoken	The 9-digit Thredd public token (must be copied from the NotifyInitiateAction request).	Number	9 characters	Required
GPSInitiateActionID	The unique identifier of the NotifyInitiateAction request (must be copied from the NotifyInitiateAction	String	36 character	Required

¹In 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
	request).			
PMReferenceID	Optional biometric or out of band validation reference for referencing purposes. Generated by the Program Manager.	String	Up to 36 characters	Optional
ProgMgrCode	Program Manager code for the issuer.	String	4 characters	Required
Status	<p>One of the following status values must be returned:</p> <ul style="list-style-type: none"> • SUCCESS - the cardholder was successfully authenticated • FAILURE - the cardholder could not be successfully authenticated. The cardholder will be shown the standard feedback message defined in Cardinal. • ERROR - used for any internal or technical failures • STEPUP - triggers your fallback authentication option (e.g., SMSOTP) • FAILWITHFEEDBACK - when authentication fails, this option allows you to display a customised feedback message to the cardholder, as sent in the error object. 	String	ENUM	Required
Error		Object		
Reference number	Program Manager reference number for the error. Used by Thredd for referencing purpose. Used for FAILURE, ERROR and FAILWITHFEEDBACK status.	String	Up to 15 characters	Optional
Description	Short description of the error. Used by Thredd for referencing purposes. Used for FAILURE, ERROR and FAILWITHFEEDBACK status.	String	Up to 50 characters	Optional
Message	A message that will be displayed to the cardholder. Used for FAILWITHFEEDBACK status.	String	Up to 100 characters	Optional

Thredd Response

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

Field	Description	Data type	Length	Mandatory / Optional
Pubtoken	Thredd 9-digit Thredd public token.	Number	9 characters	Required
GPSInitiateActionID	A unique identifier for each NotifyInitiateAction request.	String	36 character	Required
PMReferenceID	Optional biometric / out of band validation reference ID for referencing purposes.	String	Up to 36 characters	Optional
Status	The authentication status:	String	ENUM	Required



Field	Description	Data type	Length	Mandatory / Optional
	<ul style="list-style-type: none">• 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.			
Error		Object		
Reference number	Program Manager 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 100 characters	Optional



Appendix 4: 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 other languages, you can provide Thredd with your translated KBA questions. Any additional languages for your card products must also be configured for your BIN/sub-BINs at Cardinal. 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

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 RDX 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

You should preferably only enrol each card for one question. If you want to enrol a card for more than one question, then during the online authentication session Thredd will randomly choose one of the questions and pass this question to Cardinal in real-time for displaying to the cardholder. 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:Credentials>
```

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 5: 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.

Merchant
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 6: DelegatedOTPNotification Fields

Below are details of the fields in the [DelegatedOTPNotification](#) message fields, which you receive from Thredd. For an example request and response, see [Using Delegated SMS API](#).

Field	Description	Data type	Length	Status
Pubtoken	The 9-digit Thredd public token linked to the card.	Number	9 digits.	Required
DelegatedOtpId	The 36-character unique identifier of the NotifyInitiateAction request.	String	36 characters.	Required
MessageVersion3DS	The 3D Secure message version (For example, 1.0.2).	String	8 characters.	Required
Credential	Object that contains details on the credential.	Object		
Id	Unique credential identifier which Thredd generates during enrolment.	String	36 characters.	Required
Type	The credential type. This should be OTPSMS.	String	ENUM	Required
Text	The credential value. For example, when the type is OTPSMS, the value is +447654123456.	String	254 characters.	Required
MerchantInfo	Object that contains details of the merchant requesting the authentication.	Object		
AcquirerID	Identifier of the merchant acquirer.	String	11 characters.	Optional
MerchantID	Identifier of the merchant performing the purchase request.	String	35 characters.	Optional
MerchantName	The name of the merchant.	String	40 characters.	Optional
MerchantURL	The URL of the merchant's website, or the name of the merchant's app.	String	2048 characters.	Required
MerchantCategoryCode	The category code describing the type of merchant business.	String	4 characters.	Optional
MerchantCountryCode	Country code of the merchant. For 3DS1 transactions this value is the 2-letter format (For example, US). For 3DS2 transactions this value is the 3-digit number format (For example, 840).	String	3 characters .	Optional
MerchantAppRedirectURL	Note: The merchantappredirecturl field is used for app-based transactions and during in-app authentication only.	String	256 characters	Optional



Field	Description	Data type	Length	Status
	<p>The callback URL for the merchant's app. Your authentication app should use the callback URL for enabling the merchant app to redirect the cardholder back to the checkout page when they have authenticated.</p> <p>If this field is empty, your app does not need to initiate a callback to the merchant's app.</p>			
TransactionInfo	Provides details of the merchant requesting the transaction.	Object		
TransactionTimeStamp	The transaction timestamp in UTC, as per the ISO 8601 UTC specification (for example, 2019-03- 21T20:55:49.000Z).	String	24 characters.	Optional
TransactionAmount	The transaction amount in minor currency units (e.g., 1000 for \$10.00).	Number	48 characters.	Optional
TransactionCurrency	The 3-digit numeric ISO-4217 currency code.	String	3 characters.	Optional
TransactionExponent	The exponent for formatting the given ISO-4217 currency code.	String	1 character.	Optional
Passcode	The one time passcode (OTP) sent to the cardholder.	String	8 characters.	Required
MobileNumber	The cardholder's mobile number.	String	20 characters.	Required
MessageContent	The content of the message.	String	500 characters.	Required



General FAQs

This section provides answers to frequently asked questions.

Authentication and Biometric Regulations

Q. What regulations are relevant to Biometric authentication?

Biometric authentication is one of the methods for Strong Customer Authentication, which is covered in the following regulations:

- PSD2 Directive. For details, see https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
- Strong Customer Authentication guidelines. For details, see: <https://www.visa.co.uk/partner-with-us/payment-technology/strong-customer-authentication.html>

Q What were the deadlines for implementing 3D Secure with Biometric authentication?

For cards issued within the EEA (European Economic Area), the regional Card Scheme (payment network) deadline to have Strong Consumer (2 factor) authentication in place for 3D Secure was 31st December, 2020. Each country may have applied for its own deadline extension. For UK issued cards, the deadline was March 2022.

For other regions and countries please check with your issuer (if applicable) or Card Scheme (payment network).

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.

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

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

The rules you set up on the Cardinal Portal apply to both EMV 3DS 2.1 and 2.2. Both versions work with all the authentication types available within RDX (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 Secure RDX Project

Q. What are the steps in an RDX project?

For details, see [Steps in a 3D Secure Biometric/In-app Project](#).

Q. Do we need static IP addresses for oAuth calls?

The REST-based API endpoints that are used for Biometric authentication ([NotifyInitiateAction](#) and [NotifyValidate](#)) are secured with our oAuth security server (see [Using the Thredd oAuth Server](#)).

- Thredd only allow incoming requests from permitted IP addresses.
- For Thredd calls to your systems, we recommend you restrict access to permitted Thredd IP addresses. See [Authorising Thredd IP Addresses](#).



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 Biometric authentication?

Testing can start once Cardinal has completed building your screens and your configuration is released to the Staging environment, and you have successfully set up your 3D Secure configuration options and network connection.

Thredd provides a UAT environment, where you can use Cardinal's UAT simulator to test transactions. See [Completing Staging/UAT Testing](#).

Q. How do we test RDX Biometric 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 Thredd API ([Ws_CreateCard](#)) to create pilot cards in the production environment. For details, refer to the [Web Services Guide \(SOAP\)](#).
If you are using our Cards API, for similar create card functionality, see the [Cards API Website](#).
- Provide your 3DS project manager with the pilot card details you want them to submit to Cardinal. Cardinal will complete the Mastercard or Visa Card Scheme (payment network) forms to set your pilot cards to live on the Scheme's directory server.
- Thredd activate your products for RDX Biometric, and you enrol your cards in 3D Secure by calling the 3D Secure RDX web service ([Ws_AddUpDelCredentials](#)) or the [Create 3DS Credentials](#) Cards API. See [Using the Card Enrolment API](#).
- You need to set rules in the Cardinal Portal to challenge transactions, so transactions are authenticated. See [Cardinal Configuration of RDX Biometric and Screens](#).
- 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 Cardinal.

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

No, the Thredd CTS system does not have a connect to Cardinal and cannot be used for this purposes. 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 Cardinal Test Simulator. See [Using the Cardinal Test Simulator](#).

RDX 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 the Thredd API

Q. Which Thredd APIs do I use to enrol cards in 3D Secure?

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

Q. What is the Thredd API 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 RDX?

Yes, Thredd can auto-enrol your cards. There are two options, 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 the Smart Client application or the new Thredd Portal, such as a mobile phone number to use for OTP authentication.

Note: You still need to use the 3D Secure RDX 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 Biometric authentication).

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

You can use the RDX 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 web service returns an action code of 437.

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 unenrol a card from 3D Secure?

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

Note: Thredd does not unenrol cards on behalf of Program Managers. If your card status changes to any of the following: Card destroyed, Lost card, Stolen Card, the Program Manager will need to unenrol the respective cards. They can unenrol using: [Ws_AddUpDelCredentials](#) (SOAP) or the [3DS Credentials API](#) (REST).

Note: Please check with your 3DS project manager for unenrolment restrictions if you have *continuous auto-enrolment* 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>BIOMETRIC</hyp:Type>
    <hyp:Value>Biometric App</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 RDX 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**

In the [NotifyinitiateAction](#) web service this is 36 characters (Thredd adds leading zeros to the Credential ID as required by Cardinal). For example: **000000000000000000000000000000000000669**.



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 Web Services or 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., Biometric or In-App), then in your [NotifyValidate](#) response, you should set the message `status` field to STEPUP. See [Notifying Thredd of the Result of the Biometric Session](#).

This triggers the fallback solution (e.g., OTP SMS). (In the OTP SMS fallback scenario, Thredd sends the request to Cardinal, who generates the OTP and returns to Thredd for sending to the cardholder.)

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

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

During project implementation stage, you can customise the text that appears on the Cardinal Choice screen shown to cardholders: you specify this on the 3DS Product Setup Form; see [Cardinal Configuration of RDX Biometric and Screens](#). See the example below:

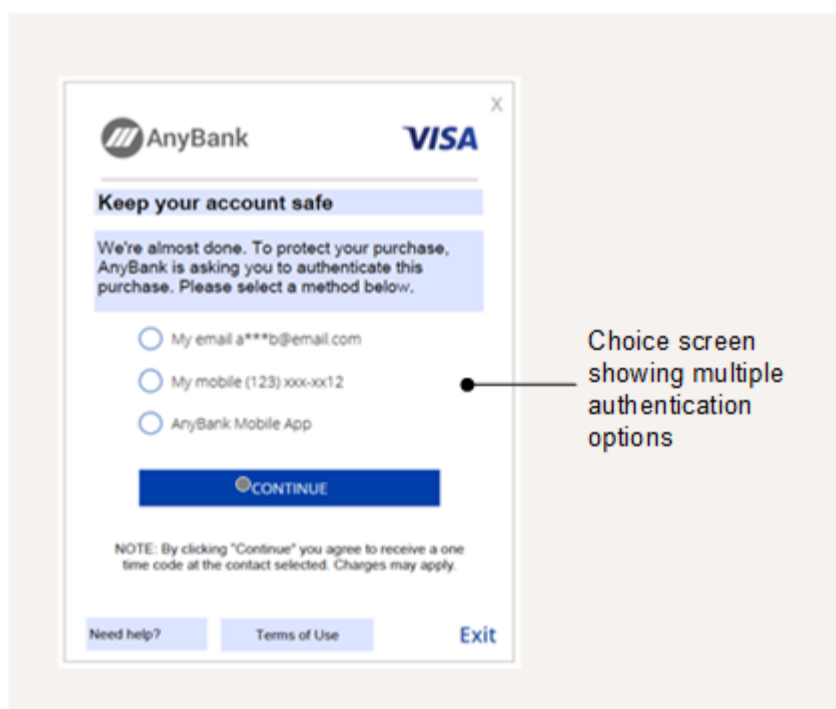


Figure 16: Choice Screen - where the user can select a method

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

Biometric and Out of Band (OOB) Authentication

Q. What does the Biometric/OOB screen look like?

The Biometric/OOB screen directs the cardholder to complete Biometric/In-App authentication through your customer smart device application. This option is triggered only if the authentication is set to Biometric and the card is enrolled for Biometric. See the example below:

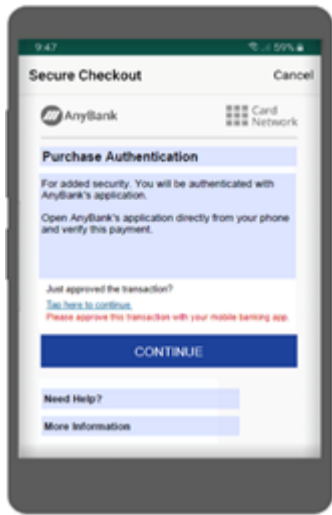


Figure 17: Biometric/OOB Authentication Screen

You can specify the text that appears on this screen using the 3DS Product Setup Form; see [Cardinal Configuration of RDX Biometric and Screens](#).

Q. How does a Biometrics/OOB session work?

Thredd can set up Biometric or OOB authentication as your default authentication type, with OTP SMS as the fallback type. If these types have been set up for your card program and the card has been enrolled in these types, then the cardholder is authenticated during a session using the default type or, if the default type cannot be used for any reason, the fallback type is provided.

Alternatively, if requested during the implementation phase, Cardinal can enable the Choice screen, where the cardholder chooses their preferred authentication type during the authentication session.

For details, see [Steps in a 3D Secure Biometric/In-app Project](#).

During an authentication session, a Biometric/OOB session works as follows:

1. If Biometric authentication is your default authentication type, Cardinal displays a message similar to the example in Figure 13. Alternatively, if you have requested to have the Choice screen for your customers, then the cardholder is shown the Choice screen and selects your smart device application (i.e., Biometric/OOB) as the authentication type (See Figure 12). A screen similar to the example in Figure 13 is then displayed.
2. When the cardholder selects Continue, Cardinal sends a message to Thredd and Thredd sends you the [NotifyInitiateAction](#) notification. You acknowledge the message. See [Initiating a Biometric Session](#).
3. Your Customer application manages the Biometric or In-App validation with the cardholder, on their smart device.
4. When completed, you return the response to Thredd, using the [NotifyValidate](#) API endpoint. See [Notifying Thredd of the Result of the Biometric Session](#)
5. Thredd returns the response to Cardinal.

Further information on the Biometric call flow is described in the section [Cardholder Authentication Flows](#).

Note: Please discuss with your Implementation Manager before implementing OOB authentication.

Q. What Biometric options can we use?

This is entirely up to you, as your customer smart device application needs to implement the Biometric verification and the options you use must be supported on the end-user's device. Examples are: Face recognition, Fingerprint and Voice recognition.

Q. If we do not provide a [NotifyValidate](#) response, will Thredd automatically use the fallback option?

No, if Thredd does not receive the response, the transaction will time out after the configured timeout period.

Q. Why are we receiving a *FAILWITHFEEDBACK* status in the response to our [NotifyValidate](#) API call?

Thredd is expecting only one [notifyvalidate](#) API call per authentication session. If you make more than one [Notifyvalidate](#) API call for a single authentication session, only the first request will be processed; for any subsequent requests, you will receive a *FAILWITHFEEDBACK* response.



Q. Can we convert the default authentication type from Biometric to SMS OTP for cardholders who do not have a smart device?

If Thredd implemented auto-enrolment with Biometric as the main and SMS OTP as the fallback method, you have two options:

- Use either Web Services or Cards API, with [Delete](#) specified in the [Action](#) field to remove the Biometric Credential ID for this card. See [Using the Card Enrolment API](#).
- During an authentication session if the cardholder is not able to authenticate using Biometric, you can respond with the status STEPUP in your [NotifyValidate](#) response. In this case, the OTP SMS will be triggered. See [Notifying Thredd of the Result of the Biometric Session](#).

If the card has not been auto enrolled, you can use either Web Services or Cards API to add the required credentials to the card. See [Using the Card Enrolment API](#).

Language Support

Q. Can the OTP messages be displayed in more than one language?

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

Cardinal Portal

Q. How do I define and set up rules and policies for Risk Based Authentication (RBA)?

Risk Based Authentication (RBA) is an authentication method managed by Cardinal, based on their rule's engine.

You can use risk scores and the other data fields in the Cardinal Portal (such as transaction amount, IP address, merchant name or merchant country) in setting up the rules used by Cardinal. See [Appendix 1: Cardinal 3D Secure Rules](#).

The rule outcome when assessing a transaction can be:

- Success - the transaction is approved: frictionless authentication
- Fail/Fail with Feedback or Rejected - the transaction is declined.
 - Challenge - the cardholder is asked to verify their identity using an available authentication method.
 - Attempts - the transaction is approved as attempt without challenge. It could be triggered and identified as a risk concern to be reviewed.

For details, see [Rule Outcomes](#).

In the first two scenarios Cardinal completes authentication of the transaction. In the Challenge scenario, one of the other supported authentication types is used (e.g., Biometric/In-App or OTP SMS).

Note: Rules must be set up on the Cardinal Portal under both Rules 1.0 and Rules 2.0, to be applied for the 3DS transaction received from merchants enrolled in 3DS 1.0, 3DS 2.0, 3DS 2.1 & 3DS 2.2.

Q. How can I test transactions with Biometric authentication?

You can use Cardinal's UAT simulator to test transactions. The Test Simulator can be accessed on the Cardinal Portal. See [Completing Staging/UAT Testing](#).

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

Mastercard provides test cases for some 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, contact your 3DS project manager.

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

The Cardinal Compliance Manager app allows you to manage any PSD2 and Strong Customer Authentication (SCA) requirements and exemptions relating to cardholder authentication; Please refer to *Cardinal Compliance Manager Guide* for further information. 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. Do you 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 Cardinal in an optional [RequestorAppUrl](#) field which indicates the merchant's app URL. When initiating a biometric session, Thredd provides details to your systems in the [MerchantURL](#) field. For more information, see [Initiating a Biometric Session](#).

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

The CAVV/AAV is a cryptographic value which is included in the authorisation message request from the Merchant¹. 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, Visa, or Discover) validate this value. Card Scheme 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](#).

If Thredd was selected to validate and the CAVV/AAV is not valid or 3D secure was not passed / 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. Refer to the EMVCo guides for details.

¹The 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.



Troubleshooting

Q. Why are some cardholders not receiving the OTP?

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

- Network issue affecting the message transmission on the Thredd side
- 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

Q. How can I unblock a card that's been blocked on the Cardinal Portal?

Depending on your risk and fraud settings in the Cardinal Portal, a card may be blocked if the cardholder enters their OTP incorrectly three times during a 3D Secure session which uses One-Time Password (OTP) authentication. You can use the Thredd PANFinder application to look up the PAN associated with the Thredd public token for the card, and then unblock the card in the Cardinal Portal, in the **Customer Services application**: use the **Unblock card** feature and enter the full PAN.

The screenshot shows a web browser window with the URL <https://csr.cardinalcommerce.com/Account/Search>. The page header includes "Customer Service", "Organization:", "Welcome", and a "Reports" dropdown menu. The main content area is titled "Account Search" and features a form with the label "Enter Full Account Number" above a text input field. Below the input field is a blue button labeled "LOCATE ACCOUNT".

Figure 18: Unblocking a card using the Customer Services App



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.

Cardinal Commerce

3D Secure service provider.

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

Realtime Data Exchange (RDX)

3D Secure real-time API call to enroll a card in 3D Secure

Risk-Based Authentication (RBA)

The authentication decision is based on the risk rules configured for the service (i.e., rules you have configured in the Cardinal 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 legacy user interface for managing your account on the Thredd Thredd Platform. Smart Client is installed as a desktop application and requires a secure 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.

Thredd Portal

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



Document History

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

Version	Date	Description	Revised by
2.3	14/08/2025	Added support for Authentication using Delegated OTP. See Cardholder Authentication Flows .	JB
2.2	16/04/2025	Updates to the OTP message templates. See Appendix 2: OTP Message Templates .	WS
	11/02/2025	Added references to Thredd Portal, our new web application for managing your cards and transactions.	KD
	16/01/2025	Reinstated old IP addresses for PRD1 and PRD2 environments. See Authorising IP Addresses .	KD
	03/01/2025	Added a Note on 3D-Secure unenrolment in the General FAQs . Clarified explanations of enrolment and unenrolment (see Enrolling your Cards in 3D-Secure). Removed descriptions of upgrading from Batch to RDX.	KD
	21/12/2024	Updated URLs for service migration to the cloud environment. See Complete Pilot Production Testing, Using the Biometric In-App API and Using the Thredd OAuth Server .	KD
	13/11/2024	Updated the URL details for the Live Server (Primary). Removed URL details for the Live Server (Disaster Recovery). See Authorising IP Addresses . Updated one of the Production URLs for PRD1 and PRD2. See Authorising IP Addresses . Updated Producton URLs for OAuth API endpoints. See Using the OAuth Server . Updated the Producton URL for the NotifyValidate REST API. See Using the Biometric/In-App Authentication API	KD
	13/09/2024	Removed references to VPN.	WS
	02/09/2024	Added references to Discover Global Network.	PC
2.1	26/06/2024	Updated the company address .	PC
	21/03/2024	Updates to content and graphics to align with taxonomy updates on our documentation portal.	KD
2.0	22/08/2023	In the section PRD1 and PRD2 - Cloud Production Environments , updated the oAuth endpoint for PRD2 to p1ists.globalprocessing.net .	WS
	24/07/2023	Added details of when you might receive the <i>FAILWITHFEEDBACK</i> status in the response to a NotifyValidate API call. See the FAQs .	WS
	01/06/2023	Restructuring of guide topics. Updates to reflect changes to the Thredd 3DS Product Setup Form (PSF) and steps in a 3D Secure project. Added details of using the Cards API 3D Secure endpoints. Added details of using Compliance Manager.	WS
	31/05/2023	Updated Operations email address to be occ@thredd.com	MW
	27/04/2023	Guide rebrand to new company name and brand identity.	WS
	03/01/2023	Added additional IP addresses that need to be allowed for secure communication	WS



Version	Date	Description	Revised by
1.9		between Thredd and your systems when using one of our cloud production environments (PRD1 or PRD2). See Authorising Thredd IP Addresses .	
	12/12/2022	Guide updated to reflect that the OTOFBAND authentication type is now available. Note: Please discuss with your Implementation Manager before implementing this method.	WS
	08/12/2022	Added a note to indicate that your NotifyInitiateAction endpoint must resolve to a static IP address. See Steps in a 3D Secure Biometric/In-app Project .	WS
	06/12/2022	Removal of references to OTP Email, which is currently not supported.	WS
	01/12/2022	Updated the Copyright Statement.	MW
1.8	27/10/2022	Correction to the oAuth Introspect Example which shows how to validate a bearer token.	WS
	20/10/2022	New MerchantAppRedirectURL field added to the NotifyInitiateAction API. This field provides the callback URL to use to enable the merchant's app to redirect the cardholder back to their checkout page after completing the authentication session. See Appendix 3: Biometric/OOB Fields .	WS
	12/10/2022 21/09/2022	Fix to examples in Appendix 4: KBA Questions . Updated Thredd UAT IP addresses. See UAT Server . Added note about response time for NotifyInitiateAction response.	WS AL
1.7	12/08/2022	New guide layout and HTML version now available.	PC
1.6	18/07/2022	Added details of Dynamic Cardholder Verification (CVV) support to Supported Authentication Types .	WS
1.5	20/05/2022	Added new section with details of auto-enrolment of 3D Secure credentials when an expiring card is renewed resulting in a new card PAN. See Using the Card Enrolment API .	WS
1.4	08/03/2022 14/04/2022	Updates for the Out of Band (OTOFBAND) authentication method. Added notes to clarify that the OTOFBAND authentication type is not yet available. Correction: the bearer token in the header of the NotifyInitiateAction request, should be Authorization: Bearer.	WS
	31/01/2022	Addition of Knowledge Based Authentication (KBA). Removal of references to OTP Email, which is currently not supported.	WS
1.2	01/11/2021	Removed the port number from UAT URLs.	WS
1.1	30/09/2021	Address updates and update to Figure 4: 3D Secure Authentication Process Using RDX and Biometrics. New Appendix 3: Biometric/OOB Fields	WS
1.0	28/06/2021	First version - major rewrite and update.	WS
0.1	22/04/2021	Draft version	VAL



Contact Us

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

Thredd UK Ltd.

Company registration number 09926803

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

33 Kingsway

London

WC2B 6UF

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.