3D Secure Guide

RDX with OTP, Biometric, In-App and KBA Authentication

Version: 1.5
20 May 2022

Global Processing Services ltd.
6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Support Email: ops24@globalprocessing.com

Support Phone: +442037409682

Documentation queries: docs@globalprocessing.com

Publication number: 3DS-RDX-BI-1.5-20.05.2022

Copyright

Contents

1. About This Document

This document describes the 3D Secure RDX (Realtime Data eXchange) Biometric, Knowledge Based Authentication (KBA) and In-App Out Of Band (OOB) authentication service and how to integrate this service with GPS.

Target Audience

This document is intended for GPS clients (Program Managers) who are interested in integrating the 3D Secure RDX 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 SOAP and REST-based web services to connect to GPS.

What's Changed?

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

1.1. 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 RDX Project.

For information on the 3D Secure API, see Using the 3D Secure API

1.2. Related Documents

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

Document	Description
Web Services Guide	Provides details of the GPS Web Services API and includes a section on 3D Secure web services.
EHI Guide	Provides details of the GPS External Host Interface (EHI).
Smart Client Guide	Describes how to use the GPS Smart Client to manage your account.

Other Guides

Refer to the table below for other relevant documents.

Document	Description
Cardinal 3D Secure User Guide	Specification and 3D secure configuration rules when using the Cardinal Portal to set up the rules and policies for your program.

GPS also provide training on how to use the Cardinal Portal. For details, please contact your 3DS project manager.

2. 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 and Mastercard and is branded as *Verified by Visa / Visa Secure* and *Mastercard SecureCode / Mastercard Identity Check* respectively.

GPS 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 GPS 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

2.1. Authentication Types

GPS 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). GPS 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 GPS 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 GPS.
- **Out of Band (OOB) authentication**. Cardinal sends an authentication request to GPS 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 GPS.

  Note: OOB is currently not available. Please check with your 3DSecure Implementation Manager before integrating this method.

- **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. GPS

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 GPS together with the cardholder's answer. GPS compares the answer returned by Cardinal to the answer stored in the GPS 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 channel[1]. If Biometrics is being used for authentication, this secondary verification is obtained via Biometric data[2]. 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:

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.

[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 GPS/Cardinal development roadmap.

SCA must be in place by **March 2022** for UK issued cards, and across most of the EEA this date was from **January 1st, 2021**. It is already being enforced for other electronic transactions.

Note: For details of deadline extensions for other EEA countries and SCA requirements in other regions, please contact your Issuer.

2.2. Parties Involved in 3D Secure

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

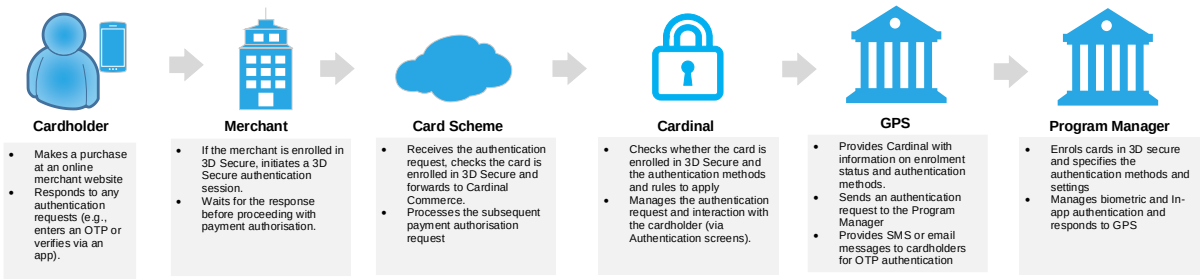


Figure 1: Flowchart of Parties involved 3D Secure

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 or OTP Email. GPS provides an option to auto-enrol the cards in your program, see Card Auto Enrolment. Alternatively, you can do this using the GPS web services 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 screens[3]. 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 and the 3D Secure authentication request.

[3] 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.

Card Scheme

Visa or Mastercard 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 GPS 3D Secure service. They receive 3D Secure authentication requests from the Card Schemes and check their database for the 3D Secure rules you have configured in the Cardinal Portal for cards in this BIN range[4].

If 3D Secure authentication is required, they send a request to GPS for the types of authentication supported by the card. They provide 3D Secure Authentication screens to the cardholder. See Screens.

- If OTP SMS is selected, then Cardinal generates the OTP and sends it to GPS. They provide the cardholder with relevant screens and messages.
- If Biometric or In-App is selected, then Cardinal provides the cardholder with relevant screens and messages and sends GPS 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 GPS for verification.

GPS

GPS manages the communication with Cardinal and the Program Manager. During an authentication session, GPS sends Cardinal a list of the authentication types for which the card is registered[5]. Cardinal can use these details to present the available authentication methods to the cardholder.

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

- For OTP SMS, GPS receives the OTP from Cardinal and sends the OTP to the cardholder's mobile phone. See Appendix 2: OTP Message Templates.
- For OTP Email, GPS receives the OTP from Cardinal and sends an email with the OTP to the cardholder. See Appendix 2: OTP Message Templates.
- For KBA, Cardinal sends the cardholder's security question answer to GPS. GPS compares the answer to the details held in the GPS database and returns a response to Cardinal.
- For Biometric and In-App, GPS notifies your systems of a request to start an authentication session. Your systems manage the cardholder authentication via your

[4] 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.

[5] 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.

smart phone application and return a response to GPS. GPS notify Cardinal of the result.

Program Manager

As a GPS Program Manager, you must sign up for the 3D Secure RDX service with GPS 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 the GPS web services API to enrol your cards in the 3D Secure service and request to register in GPS 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 web services to send GPS 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 GPS and send verification results to GPS. See Using the GPS 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 GPS, 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 GPS.

2.3. Cardholder Authentication Flows

This section provides a description of the message flow between parties in an authentication session.

2.3.1. Authentication using OTP

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

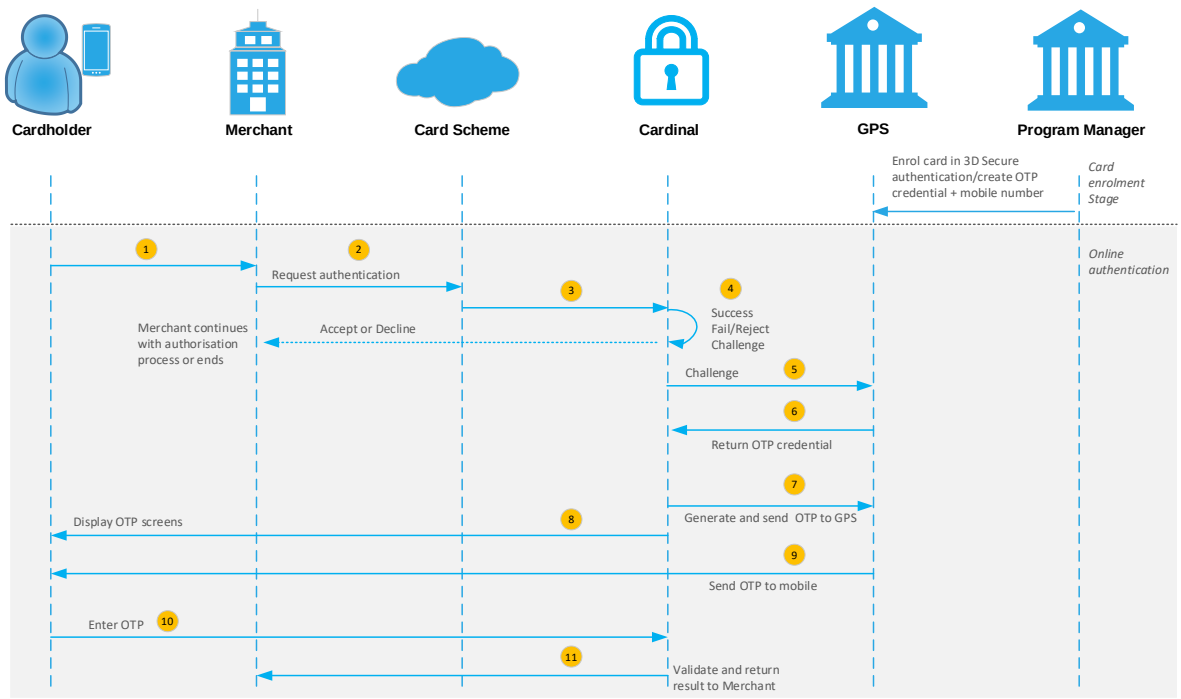


Figure 2: 3D Secure Authentication Process – Using RDX and OTP

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).
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 GPS in real-time to query the types of authentication the card is registered for (e.g., Biometric, OTP SMS or KBA).
6. GPS 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 web services API and on the default types set up for your cards).[6]
7. Cardinal generates the OTP and sends it to GPS in real-time.
8. Cardinal displays the OTP screens to the cardholder.
9. GPS 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.

[6] We configure the sub-BIN range to a default main authentication method and a fallback method. See **Setup Options** in Client Information.

2.3.2. Authentication using Biometrics or In-App OOB

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

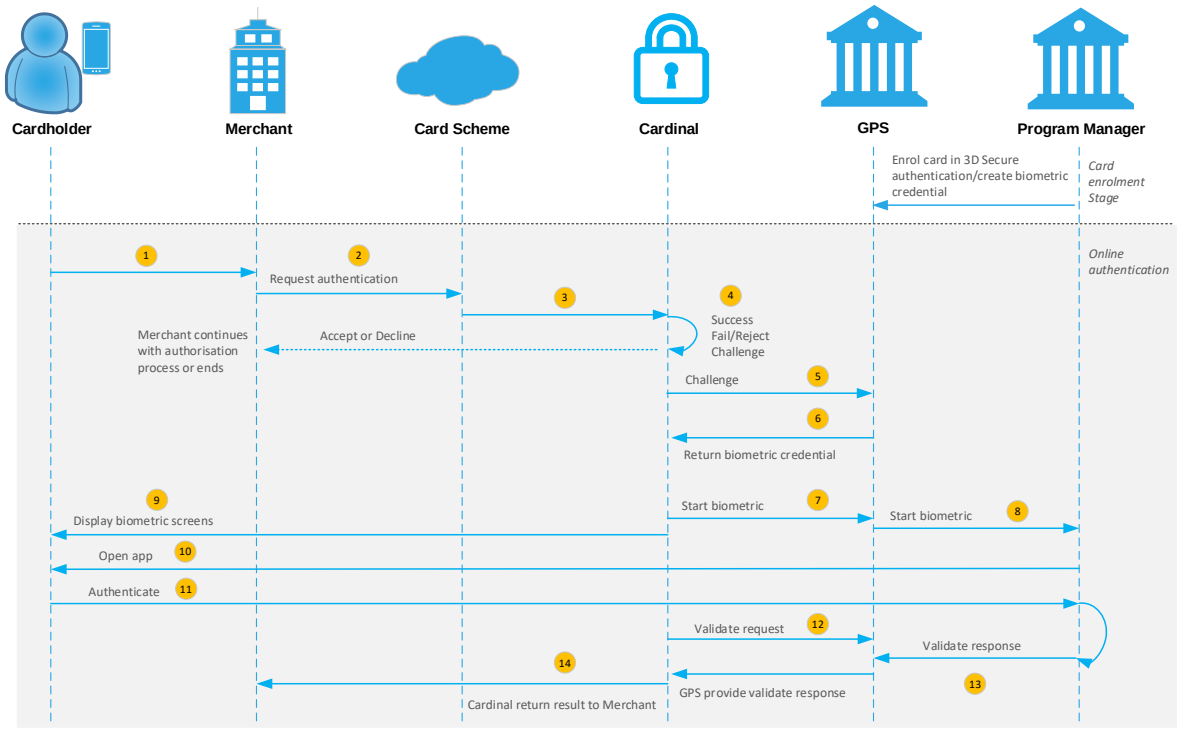


Figure 3: 3D Secure Authentication Process – Using RDX and Biometrics

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. GPS replies to Cardinal with Biometric as the type of authentication (based on what you registered the card for using the web services API and on the default types set up for your cards).[7]
7. Cardinal calls GPS to start the Biometric authentication.
8. GPS sends a message to your RDX service endpoint, to start authenticating using Biometric. (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.

[7] We configure the sub-BIN range to a default main authentication method and a fallback method. See **Setup Options** in Client Information.

11. The cardholder authenticates using your smart phone app (e.g., by scanning their fingerprint or face using their smart device). Your systems should return the result of the Biometric authentication to GPS.
12. Cardinal sends a validate request to GPS.
13. GPS waits for your validate response and sends the results back to Cardinal.
14. Cardinal returns the results to the merchant.

Note: Out of Band (OOB) authentication is currently not available. Please check with your 3DSecure Implementation Manager before integrating this method.

2.3.3. Authentication using KBA

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

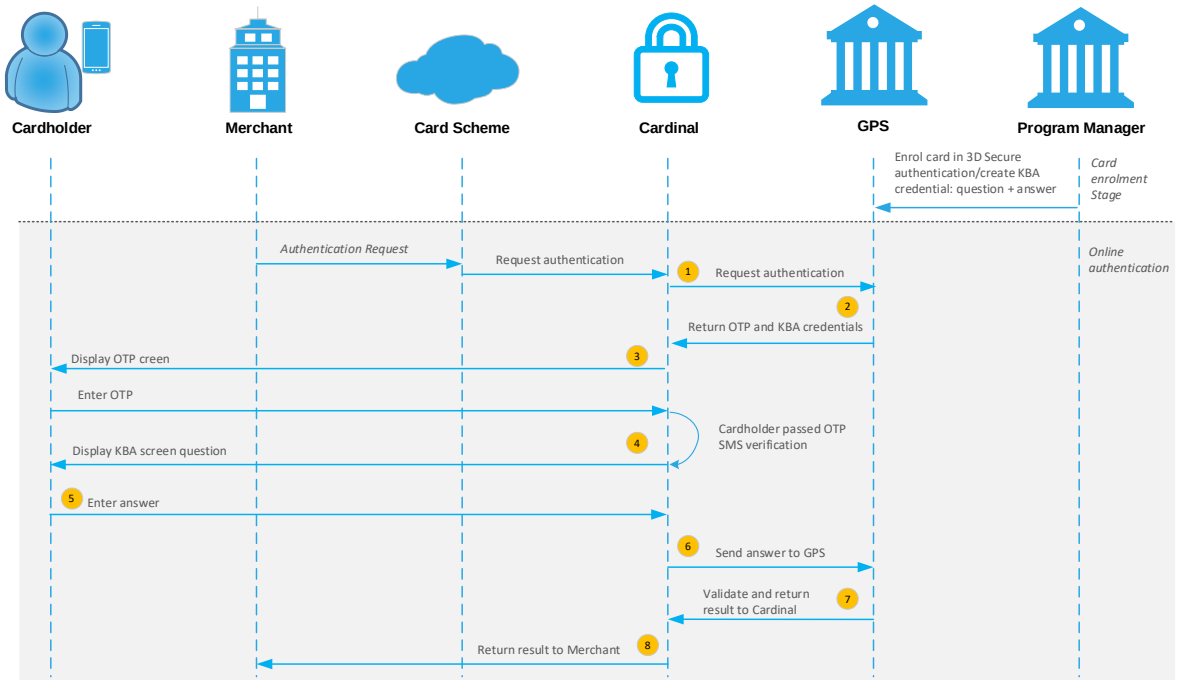


Figure 4: 3D Secure Authentication Process – Using RDX and KBA

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 GPS in real-time to query the types of authentication the card is registered for (e.g., OTP SMS and KBA).
2. GPS replies to Cardinal with the OTP and KBA authentication types. For KBA, GPS 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 GPS 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 GPS, together with the KBA answer.
7. GPS compares the answer returned from Cardinal to the answer stored in the GPS database[8]. GPS sends the combined OTP and KBA validation results back to Cardinal.
8. Cardinal returns the results to the merchant.

2.3.4. What happens after authentication?

Once 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.)

GPS validates the 3DS key for a Mastercard transaction (for Visa, Visa generates the key and validates it).

Depending on your External Host Interface (EHI) mode, GPS 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 How to Access the Cardinal Portal.

[8] When GPS receives the answer from Cardinal it is immediately encrypted using a hashing algorithm and compared to the hashed answer value stored in the GPS database.

3. 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.

3.1. Overview of Steps

You must have the RDX service set up prior to implementing Biometrics or In-App authentication. A project starts once Cardinal Commerce have received your requirements. You should allow 10-12 weeks for a typical project. (This timeline includes both RDX and biometric setup and assumes you have already developed the customer smart device application you will be using to provide Biometric/In-App authentication.)

Figure 3 below provides an overview of the steps in a typical project.

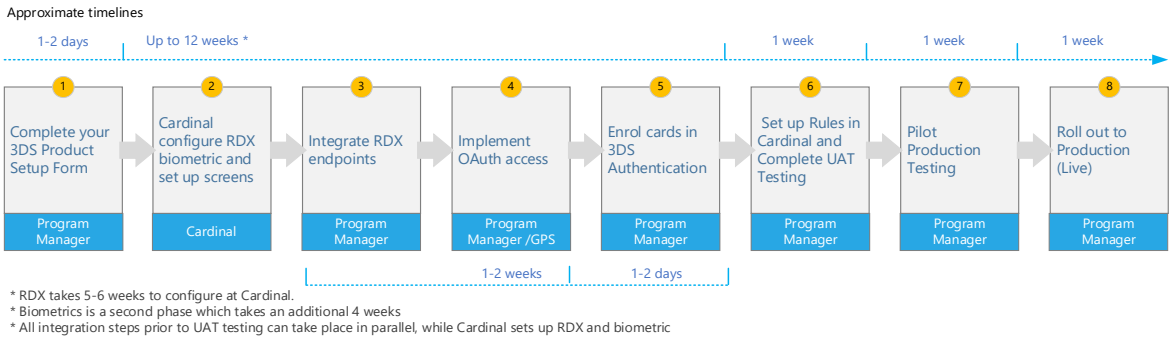


Figure 5: Steps in a 3D Secure RDX Project

Refer to the table below.

#	Step/Action	Approximate time needed
1	**Complete your 3DS Product Setup Form (PSF)** Your GPS 3DS project manager can help you complete this form.	Allow 1-2 days. A *Statement of Work* must be completed between GPS and Cardinal.
2	**Cardinal sets up your 3D Secure account** Cardinal configures your 3D secure settings, Portal access and customised authentication screens.	Allow up to 12 weeks for Cardinal to configure both RDX and biometric.
3	**Integrate the 3D Secure RDX endpoints** Provide GPS with your API endpoints and a list of permitted IP addresses for using the services.	Allow 1-2 weeks for GPS to configure the API endpoints and enable access for your IP addresses.

#	Step/Action	Approximate time needed
	Develop the functionality to receive and process 3D Secure messages using the 3DSecure SOAP and REST API.	
4	**Implement OAuth access** GPS sets up your OAuth access and provides you with details to access the GPS 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** GPS activates a single card product in the Staging environment, so you can enrol a few cards for Staging UAT testing. You can enrol your cards and specify the types of authentication using the 3D Secure RDX Web service (Ws_AddUpDelCredentials)	It takes 1-2 hours for GPS to activate the card product. Allow 1-2 hours to enrol cards in the GPS Staging UAT environment and run authentication tests. See step 6. Then repeat in Pilot production. See step 7.
6	**Complete Staging/UAT testing** Once RDX and biometric are configured, GPS and Cardinal release the project into the Staging UAT environment for you to test. You can now create your 3D Secure rules and policies in the Cardinal Staging Portal.	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. Allow a week to complete the Staging UAT testing.
7	**Complete pilot Production testing** GPS and Cardinal set up your cards in the Production environment: • GPS activates a single card product in the Production environment, so you can enrol a few cards for pilot testing. • You provide Cardinal with your pilot cards to be enrolled at the Scheme. • Create your 3D Secure rules and policies in the Cardinal Production Portal.	The full pilot testing phase takes around 1-2 weeks: • Allow a week for GPS 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 web service Ws_AddUpDelCredentials) and for pilot card testing.

#	Step/Action	Approximate time needed
	• Cardinal contacts the Scheme to set your pilot cards live with a Cardinal URL[9].	
8	**Roll out to Production (Live)** Notify GPS once you have completed your pilot testing. GPS configures your card products for 3D Secure. You need to enrol all your live cards in 3D Secure and register them for your supported authentication types (e.g., Biometric or OTP SMS). GPS also offer an auto-enrolment option. See Card Auto Enrolment. Notify GPS that you have completed enrolment. Cardinal contacts the Card Scheme to set your card BIN ranges live (For Mastercard). For Visa, Cardinal supplies the card range files for the issuer to load at the Visa Directory Server.	Allow a week to 10 days to complete the roll-out at the Card Scheme and to enrol your cards.

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

3.1.1. Step 1: Complete your 3DS Product Setup Form

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

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

- Client Information
- Cardinal Access
- Screens

Each of these tabs is described in further detail below.

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

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.
Visa BID	Your issuer's Visa Business Identifier (BID).
Mastercard Primary ICA Number	Your issuer's primary ICA, as registered with Mastercard.
Mastercard Company Name (Issuer)	Your issuer's Company Name, as registered with Mastercard.
Mastercard Company ID (CID)	Your issuer's Company ID, as registered with Mastercard.
GPS Programme Manager ID	Your GPS 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. **Note**: You need to make a copy of the **Screens** tab and provide the text for the Screens in each additional language you want supported.
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.
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.
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.

Field	Description
Setup Options (provide details for **Test** and **Production** separately)	
Default authentication	Select the default authentication type to support all sub-BIN ranges. Options are: • Biometric • SMS OTP • KBA • OUTOFBAND[10] • ALL[11] 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.
Fallback authentication	Select the fallback authentication type to support all sub-BIN ranges. Options are: • SMS OTP • KBA • OUTOFBAND[10] • ALL • None 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.
Enable SMS OTP auto enrolment	Options are: *NO:* all cards must be enrolled for OTP SMS and the mobile number must be registered using Ws_AddUpDelCredentials. *YES - Initial Load*: GPS enrol the existing cards to the OTP SMS credential. GPS use the phone number linked to the card (i.e., the phone number supplied when the card was created or updated).

[10] OUTOFBAND is currently not available. Please check with your 3DSecure Implementation Manager before integrating this method.
[11] *ALL* includes Biometric and OTP, but not KBA. If GPS returns ALL, then during the online transaction the cardholder is shown a screen showing all available options and can select their preferred authentication method.

Field	Description
	YES - Continuous: Same as Initial load, however any future cards created will also have their phone numbers automatically registered for 3D Secure in the same way.
Enable KBA auto enrolment	No auto-enrolment for KBA on new cards. This is available for replacement cards. See Card Renewals and Credential Auto-enrolment.
Enable Biometric auto enrolment	Options are: *NO*: All cards must be enrolled for Biometric using Ws_AddUpDelCredentials. *YES - Initial Load*: GPS creates a Biometric credential for all existing cardholders. YES - Continuous: Same as Initial load, however any future cards created will also have Biometric credentials created the same way.
Biometric validation timeout	The period (in seconds) you have to respond to a request for Biometric validation before the system times out[12]. The maximum is 900 seconds. This is the time from when we notify you to start authentication, up to your validation response.
NotifyInitiateAction endpoint	The endpoint GPS should use to send you the Biometric validation request. (Implemented using the (NotifyInitiateAction API. See Initiating a Biometric Session.)
OAuth IP Address	Provide details of the IP addresses you want GPS to allow to use the GPS OAuth server.
Do you need Introspection credentials? (Optional)	Select *Yes* or *No*. If you select *Yes*, GPS will generate the credentials that will be used to validate the Token.
Bin Ranges Low and **Bin Ranges High**	
Provide the whole range (16 digit) of the Sub-BIN or BIN. If you do not own the whole BIN, please provide the SUB-BIN range.	
Staging testing cards /Staging product ID	

[12] 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
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).*

Cardinal Access

Please provide GPS 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 via a VPN to their office IP address. Any attempt to access Cardinal from a non-registered IP address will result in the page not being displayed.

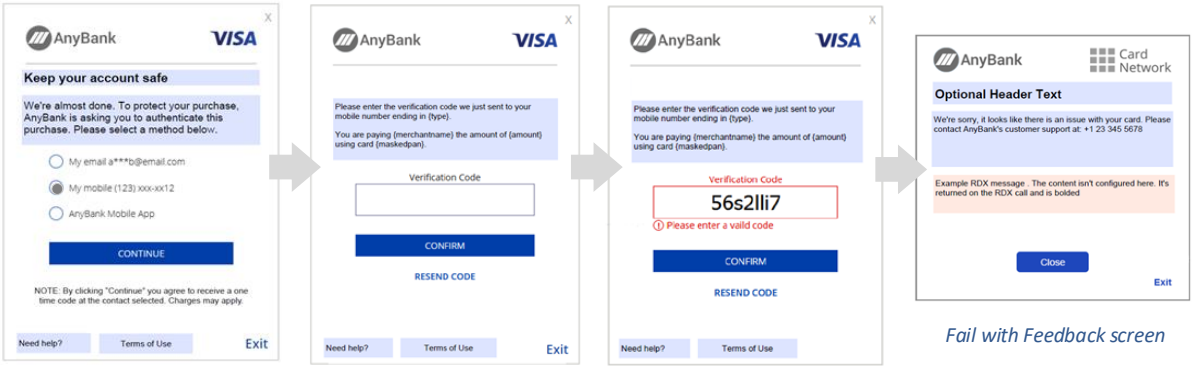
Please provide details of the administrator users who need to access the Cardinal Portal. GPS can set up role-based access for your users to the following Cardinal Portal applications: Customer Service Application, Rules Application, Reporting Application and Admin Application.

Note: Any users GPS 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).*

Screens

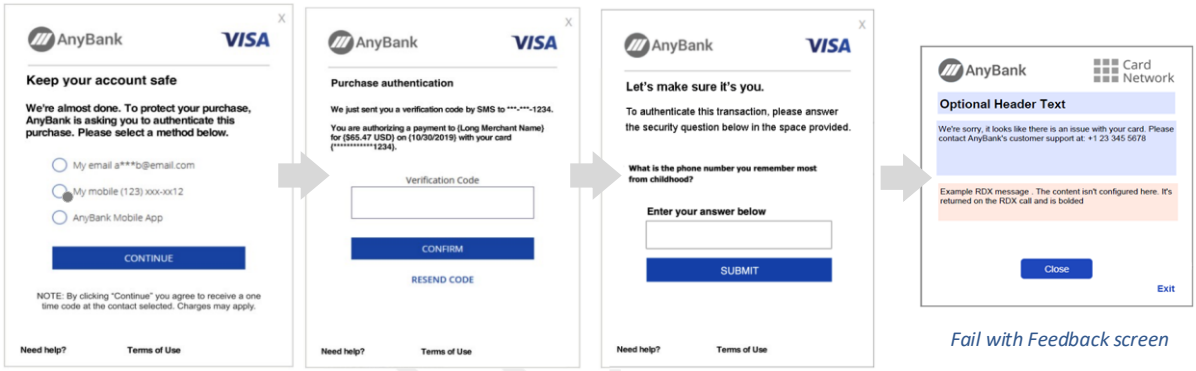
You can customise the logo and text that appears on the 3D Secure Authentication screens during an authentication *challenge* session. If you support more than one language, you need to provide the text translation for the screens. See the examples below for authentication by *One-time Password (OTP)*.



Optional Choice screen *Verification screen* *OTP validation* *Fail with Feedback screen*

Figure 6: 3D Secure Authentication Screens - for OTP

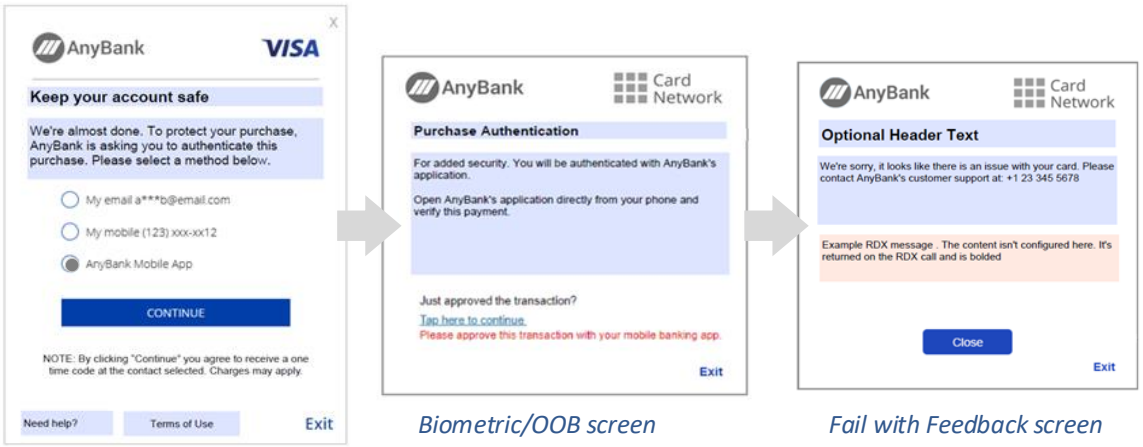
See the examples below for *KBA* + OTP authentication.



Optional Choice screen *OTP Verification screen* *KBA Verification screen* *Fail with Feedback screen*

Figure 7: 3D Secure Authentication Screens – for KBA and OTP

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



Optional Choice screen *Biometric/OOB screen* *Fail with Feedback screen*

Figure 8: 3D Secure Authentication Screens - for Biometric

For more details on text field customisation, refer to the instructions in the *3DS Product Setup Form (PSF).*

Language Support

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

You must specify language support in your *3DS Product Setup Form*. You must specify a default language. You can specify additional languages and provide the translated text you want to use for each language.

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

The screen text limit is 350 characters.

KBA Language Support

If you support more than one language, you can provide translations for the GPS 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: GPS cannot use a different language to what is configured as the language with Cardinal for your BIN/sub-BINs.

OTP SMS Text Support

For OTP SMS messages (sent by GPS 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 GPS 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 (for details, see the **Create Card** web service in the *Web Services Guide*). Below is an example of the OTP SMS message, in French:

Figure 9: OTP SMS Message Example

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

3.1.2. Step 2: Cardinal Configure 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.

3.1.3. Step 3: Integrate RDX Endpoints

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

Setting up Firewall Permissions

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

You must provide GPS 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 GPS systems (in both UAT staging and Production).
- The IP addresses you will use for sending API messages to GPS (in both UAT staging and Production).
- The IP addresses you will use for OAuth (in both UAT staging and Production) to be authorised at GPS.

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

Implementing the Biometrics API

Please provide GPS 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 GPS, using the NotifyValidate API. See Notifying GPS of the result of the Biometric Session.

3.1.4. Step 4: Implement OAuth Access

You must authenticate against the GPS 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 GPS.

For details, see Using the GPS OAuth Server.

3.1.5. Step 5: Enrol your cards in 3D Secure

You can enrol your cards in 3D Secure using the GPS 3D Secure RDX Enrolment web service (Ws_AddUpDelCredentials). Your request must include the GPS *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: GPS 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.

GPS saves the card enrolment record in our database.

Card Auto Enrolment

If you are migrating existing cards to 3D Secure, GPS can automatically enrol all your cards in the 3D Secure RDX service: you can request auto-enrolment by specifying the authorisation types to auto-enrol on your *3DS Product Setup Form*. See Step 1: Complete your 3DS Product Setup Form.

Auto-enrol options include:

- *None*: there is no auto-enrolment. You will need to do this using Ws_AddUpDelCredentials.
- *Initial load*: GPS creates the authentication type credentials (e.g., *OTP SMS* or *BIOMETRIC*) for all existing cards. For OTP SMS, GPS 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 Ws_AddUpDelCredentials.
- *Continuous*: Same as Initial load, however any future cards created (using the Card Create (Ws_CreateCard) web service will also have their credentials automatically registered for 3D Secure in the same way. Applying any changes to credentials for existing cards must be done using Ws_AddUpDelCredentials.

GPS auto-enrols the card in the *default* main and *fallback* authentication types set for your card product. For OTP SMS, GPS 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 Step 1: Complete your 3DS Product Setup Form.

3.1.6. Step 6: Complete Staging/UAT Testing

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

Set up Rules in the Cardinal Portal

GPS 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 GPS a list of IP addresses you want to add to the authorised access list in Cardinal.

How to Access the Cardinal Portal

You can log in at:

Staging: https://identifiportalstaging.cardinalcommerce.com/home/dashboard

Live: https://centinelportal.cardinalcommerce.com/

See the example below:

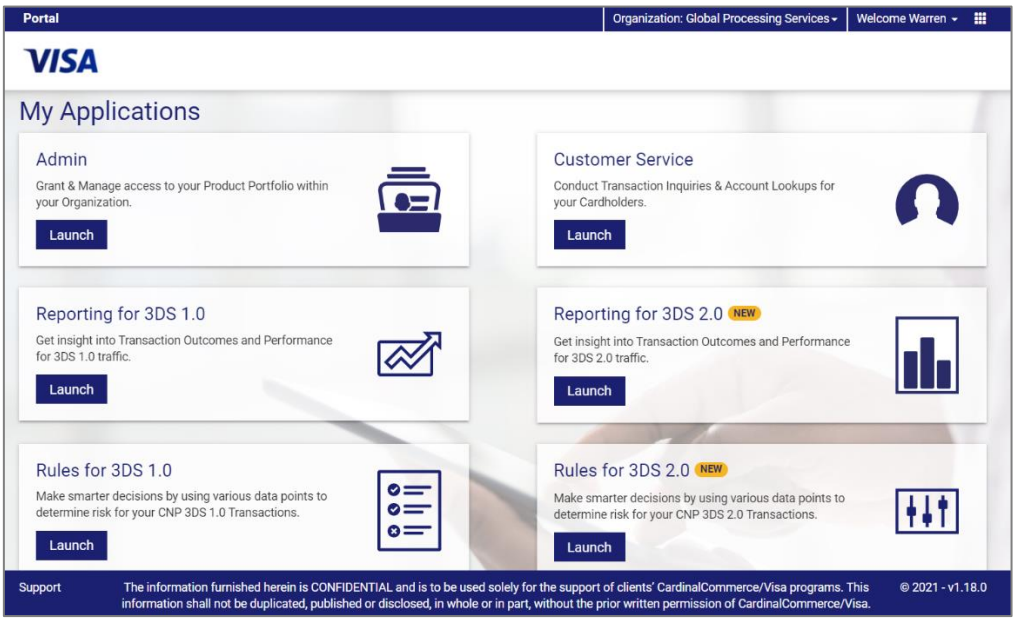


Figure 10: Cardinal Portal

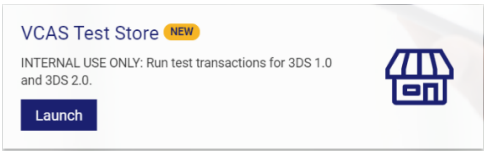
In the Cardinal Portal, create your 3D Secure policy and set up the rules required to trigger *Success*, *Fail/Reject* or *Challenge* outcomes. You should complete rules for both 3DS 1.0 and 3DS 2.0. For details, see Appendix 1: Cardinal 3D Secure Rules.

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

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:

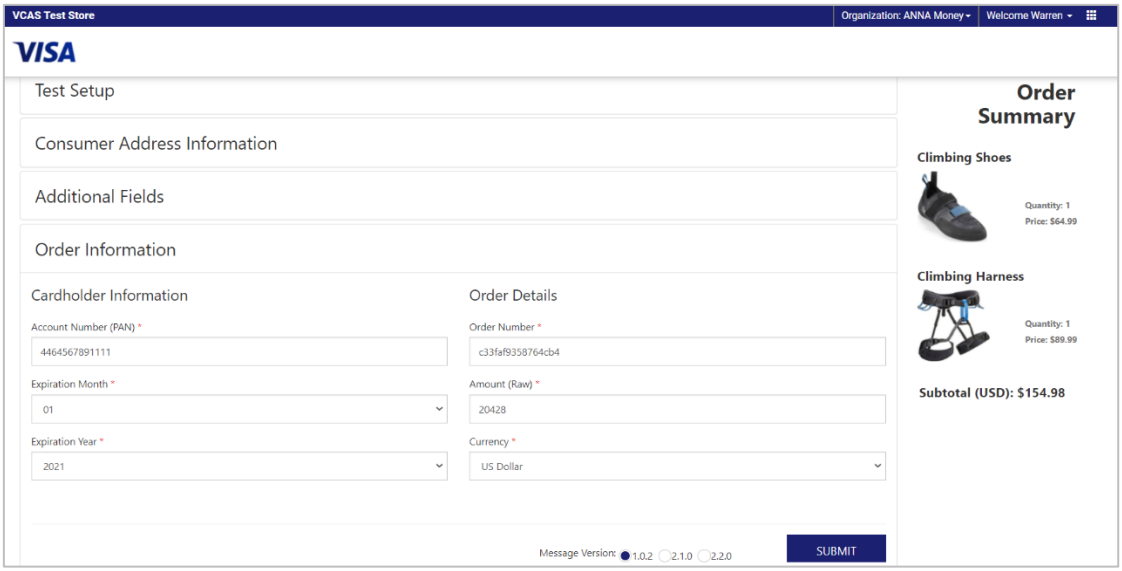


Figure 11: VCAS Test Store

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. OTP messages will not be sent to your mobile number (since this is not supported in the Staging/UAT environments). You will be able to complete the simulation of the Biometric authentication.

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,

3.1.7. Step 7: Complete Pilot Production Testing

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

- GPS 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.

You can register the cards for the supported 3D Secure authentication types using the 3D Secure RDX web service (Ws_AddUpDelCredentials).

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/email addresses?
    - For Biometric/In-App authentication, is your smart device application correctly handling the authentication process and reporting the result to GPS?
    - 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 GPS 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 if it is required for your program.

3.1.8. Step 8: Roll out to Production (Live)

Notify GPS 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, GPS 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.

3.2. Upgrading from Batch to RDX

If you are currently using the Cardinal Batch service, you will need to upgrade to the Cardinal Real-time data exchange (RDX) service in order to support Strong Customer Authentication.

GPS is currently in the process of migrating customers using the legacy Batch service to RDX. You should have received an email from your 3DS project manager about this.

The upgrade process is as follows:

1. Contact your 3DS project manager to request an upgrade from GPS batch to RDX.
2. Integrate the new RDX web service (Ws_AddUpDelCredentials) and then follow steps 5-7 described in Overview of Steps.
3. When you are ready to go live, book one of the available weekly upgrade slots for migration from batch to RDX. Confirm whether you want GPS to auto-enrol your cards or whether you will do this via web services.
4. GPS 3DS project manager will send you the planned upgrade dates and timeline.
5. On the day of the upgrade GPS will activate your product for RDX. While the upgrade is taking place, you should not use any of the legacy batch API web services.
6. All cards are then enrolled (either using auto-enrolled by GPS or you must do this via web services).
7. Cardinal switches the BINs to RDX at 4pm UK time. (Cards must be enrolled by this time or any card transactions made using them will be declined.)

3.3. Authorising GPS IP Addresses

The following GPS IP addresses must be authorised on your firewall to enable OAuth and RDX API communication to support Biometric/In-App authentication:

Live Server (Primary)

URL	Server name	IP	Components
https://vcasp.globalprocessing.net	GPS-BLH-RDX	195.40.85.53 195.40.85.40	GPS.VCAS.RDX.API
https://oauth.globalprocessing.net	GPS-BLH-RDX	195.40.85.53 195.40.85.40	GPS.Identity.Api

Live Server (Secondary AKA Disaster Recovery)

URL	Server name	IP	Components
vcasdr.globalprocessing.net	GPS-BLH-RDX-02	80.65.249.136	GPS.VCAS.RDX.API
oauthdr.globalprocessing.net	GPS-BLH-RDX-02	80.65.249.136	GPS.Identity.Api

UAT Server

URL	IP	Components
https://oauthuat.globalprocessing.net	3.9.27.216	GPS.VCAS.RDX.API
https://oauthuat.globalprocessing.net	3.9.27.216	GPS.Identity.Api

4. Using the 3D Secure API

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

- Using the Card Enrolment API
- Using the Biometric/In-App Authentication API
- Using the GPS OAuth Server

4.1. Using the Card Enrolment API

To enrol your cards in 3D Secure and to register the card for different authentication types (e.g., OTP SMS, KBA and Biometric), use the 3D Secure (Ws_AddUpDelCredentials) web service API. This is a SOAP-based web service, which requires sending your request as an XML message. This web service is described in detail in the *GPS Web Services Guide*.

See the example below:

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
<soapenv:Header>
  <hyp:AuthSoapHeader>
     <hyp:strUserName>*******</hyp:strUserName>
     <hyp:strPassword>*******</hyp:strPassword>
   </hyp:AuthSoapHeader>
  </soapenv:Header>
  <soapenv:Body>
    <hyp:Ws_AddUpDelCredentials>
      <hyp:WSID>14012021141223</hyp:WSID>
      <hyp:IssCode>GPS</hyp:IssCode>
      <hyp:PublicToken>123456789</hyp:PublicToken>
      <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>
```

GPS token of the card to enrol in 3D Secure

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

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>GPS</IssCode>
    <ActionCode>000</ActionCode>
    <PublicToken>123456789</PublicToken>
    <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 GPS 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 GPS to store[13]. 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] Answers are stored in hash-encoded format in the GPS database. Answers are case-sensitive; for example, '*London*' would be hash-encrypted differently from '*london*' or '*LONDON*'.

4.2. 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:

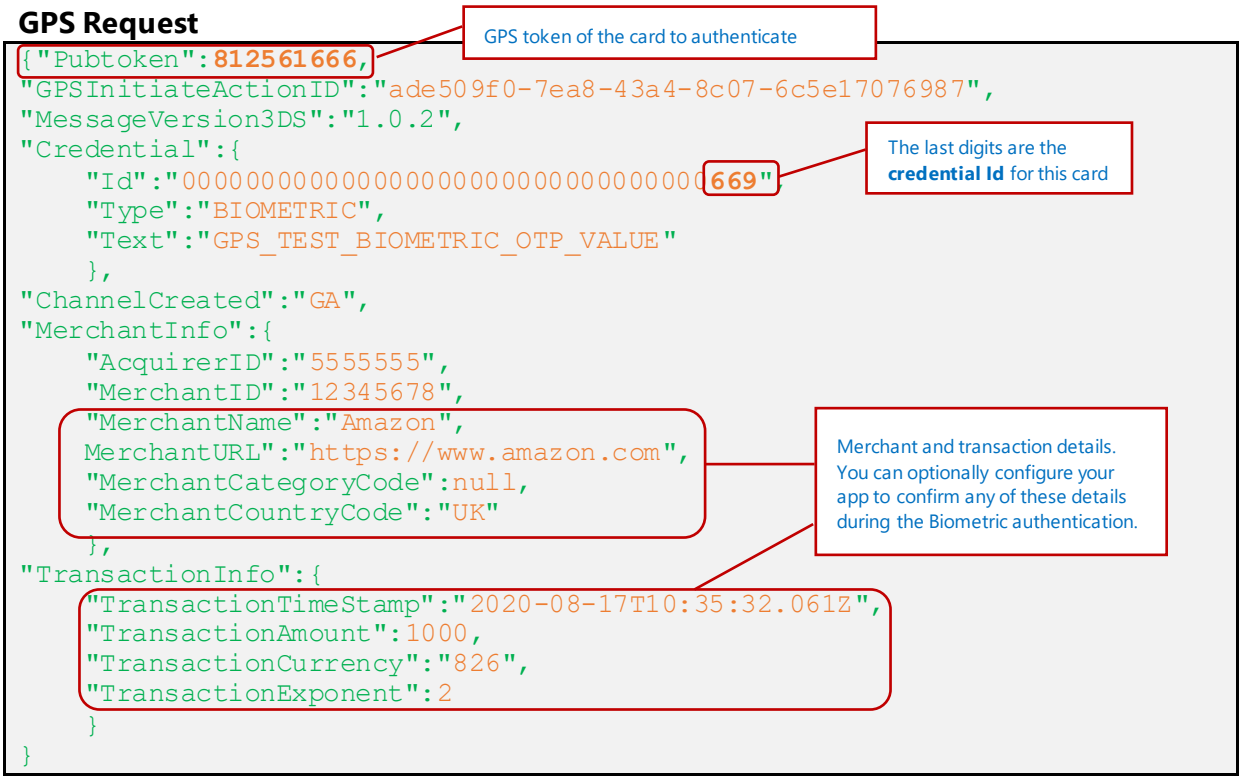
- NotifyInitiateAction – sent by GPS to notify you to set up an authentication session
- NotifyValidate – you use this to send the authentication result to GPS.

4.2.1. Initiating a Biometric Session

When GPS 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 Step 1: Complete your 3DS Product Setup Form).

See the example below:

GPS Request




```
{"Pubtoken":812561666,
"GPSInitiateActionID":"ade509f0-7ea8-43a4-8c07-6c5e17076987",
"MessageVersion3DS":"1.0.2",
"Credential":{
    "Id":"00000000000000000000000000000669",
    "Type":"BIOMETRIC",
    "Text":"GPS_TEST_BIOMETRIC_OTP_VALUE"
    },
"ChannelCreated":"GA",
"MerchantInfo":{
    "AcquirerID":"5555555",
    "MerchantID":"12345678",
    "MerchantName":"Amazon",
    MerchantURL":"https://www.amazon.com",
    "MerchantCategoryCode":null,
    "MerchantCountryCode":"UK"
    },
"TransactionInfo":{
    "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 Request Fields.

Your Response

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

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

When your systems receive the NotifyInitiateAction request, you can optionally use the GPS OAuth server to validate the token, to confirm it is from GPS. See Validating the Token.

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)

GPS passes the bearer token in the header of the NotifyInitiateAction request, as shown in the example below.

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjE5ODI3Q0E4M0NEMkNGNUUzMTAxMUVBQkQ0N0ZDNTg4RkM
yRjQ3RTIiLCJ0eXAiOiJhdCtqd3QiLCJ4NXQiOiJHWUo4cUR6U3oxNHhBUjZyMUhfRmlQd3ZSLU
kifQ.eyJuYmYiOjE2MDc1MzM1NzksImV4cCI6MTYwNzU0Nzk3OSwiaXNzIjoiaHR0cHM6Ly9vYX
V0aHVhdC5nbG9iYWxwcm9jZXNzaW5nLm5ldCIsImF1ZCI6WyJyZHhhcGkiLCJmaXJiaW9tZXRya
WNhcGkiXSwiY2xpZW50X2lkIjoiZmlyYmlvIiwic2NvcGUiOlsiY2xpZW50X3ZhbGlkYXRlIiwi
ZmlyYmlvbWV0cmljYXBpIl19.owfqYt7Rf6zHMLY2HT3j0RH7Lti05oWkp-
bJ41QF1LZyqxaRMZWJAUxuRXJwIWrG2wtC0Q1KFzVPbZhpwKAwJvQTIymJFhryEvRUGTQqM61Nw
u_Dnsx8H-Jpi7_0PjQk4MaAhqFv6MEgDMHvxUZ2_Q6vYj_-h2rRDunHjBvhvA55-
yGLdqxeHRtNvHJQCsaVZHdLBngUpeFpWcvrbhk1SYbNlGlflYBm5aAX_YDwpWt4p_M6w7TAYJZQ
vc4Hi_NqAZwUOY7xOlhVD69onUmd74k6nt0ncowGgC3naWQieqcVMd3B1kCAnnYZfLlXMhSxeN_
XqWtjKTK3WMavYj6vrw
```

You can optionally verify the token (check that it is valid and active) using the OAuth introspect API endpoint. See Using the GPS OAuth server.

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

4.2.2. Notifying GPS of the Result of the Biometric Session

When authentication is complete, you must use the NotifyValidate REST API to send the authentication outcome to GPS.

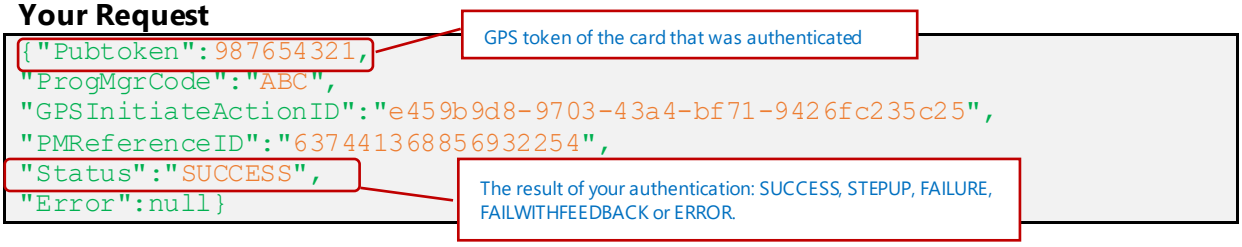
API Endpoints

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

Production: https://vcasp.globalprocessing.net/api/v1/NotifyValidate

See the example JSON message below:

Your Request




```
{"Pubtoken":987654321,
"ProgMgrCode":"ABC",
"GPSInitiateActionID":"e459b9d8-9703-43a4-bf71-9426fc235c25",
"PMReferenceID":"6374413688569322 54",
"Status":"SUCCESS",
"Error":null}
```

GPS Response

```
{"Pubtoken":987654321,
"GPSInitiateActionID":"e459b9d8-9703-43a4-bf71-9426fc235c25",
"PMReferenceID":"6374413688569322 54",
"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), GPS will return details of the error.

GPS 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 GPS sends the NotifyInitiateAction message to your system, GPS 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). [14]

If GPS 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.

4.3. Using the GPS OAuth Server

You must authenticate against the GPS 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 GPS; GPS 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 GPS 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

4.3.1. OAuth API Endpoints

GPS 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 GPS sends to your NotifyInitiateAction endpoint (to notify you of a request to initiate a Biometric/In-App session)

GPS OAuth endpoints are listed below.

UAT:

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

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

[14] This period starts from when GPS sends the NotifyInitiateAction message up to receiving the NotifyValidate.

Production:

Token endpoint: https://oauth.globalprocessing.net/connect/token

Introspect endpoint: https://oauth.globalprocessing.net/connect/introspect

4.3.2. OAuth User Credentials

Please check with your GPS 3DS project manager for your **client_id** and **client_secret** to access the OAuth server.

4.3.3. OAuth Token Expiry

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

4.3.4. OAuth Token Request Example

You can retrieve an OAuth access token from the GPS OAuth server using the private credentials (client_id and client_secret) provided to you by GPS. 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=9d70c6bbad8ad20262828222fc0f3fdd
&client_secret=a3d5566e8ca0d6da823eb7815c1c2b66
&grant_type=client_credentials
```

Response (Successful)

```
200 OK
```


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjZhNjdmOWEzZTA1OTM0ZWZjOT
UzYmY1ZjI1ZjVkMDMyIiwidHlwIjoiSldUIn0.eyJuYmYiOjE1ODI1NDExMTYsImV4cCI6MTU4M
jU0NDcxNiwiaXNzIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NDQzMzYiLCJhdWQiOlsiaHR0cHM6Ly9s
b2NhbGhvc3Q6NDQzMzYvcmVzb3VyY2VzIiwicmR4YXBpIiwicmVsYXlhcGkiXSwiY2xpZW50X2l
kIjoidmNhcyIsInNjb3BlIjpbImNsaWVudF92YWxpZGF0ZSIsInJkeGFwaSIsInJlbGF5YXBpIl
19.Lh5Mp0Qa82QVMzs4ylmzbB9W9Qk4qiVcODewvOq3N1_JmspKyYyhOilVj8KxNxPjiKVYnFA2
hDWtlKO16l8aL1oEkBky1h4haQuqtPWaUdNirWVDs99R1VqCh3wYmYZmNHNseJvEVIrd__HQ7kT
JLGO7NkebPc_QM6rTB2qfYI9nax6JQnMrk72cDzeorwUlxSf2G6p49kpgyhNJooHfptWlRtV6JW
UPUVEC7oNEfYnbfjVhSUyF5_11HHi_2r0zLhFIdPH7fSUXzl8OOOCMqUvSedaAJN6SRIEnTiE5i
sjIMJG3T4pymqUcc6ujm3upB9UStaBXMelp7Rom7LVqQ",
    "expires_in": 3600,
    "token_type": "Bearer",
    "scope": "client_validate rdxapi relayapi"
}
```


The GPS OAuth server supports basic HTTP status codes. See the table below:

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

When your Client application has obtained the access token, it must be passed on every request made to the GPS RDX service. The access token is included in the standard Authorization header of the HTTP request.

Example:

```
Authorization: Bearer XXXXXX_ACCESS_TOKEN_XXXXX
```

4.3.5. OAuth Introspect Example

GPS includes a token in the header of the request sent to your NotifyInitiateAction endpoint. You can optionally use the Introspect endpoint to validate this token (i.e., check that it is active). Below are examples of an OAuth Introspect request and response.

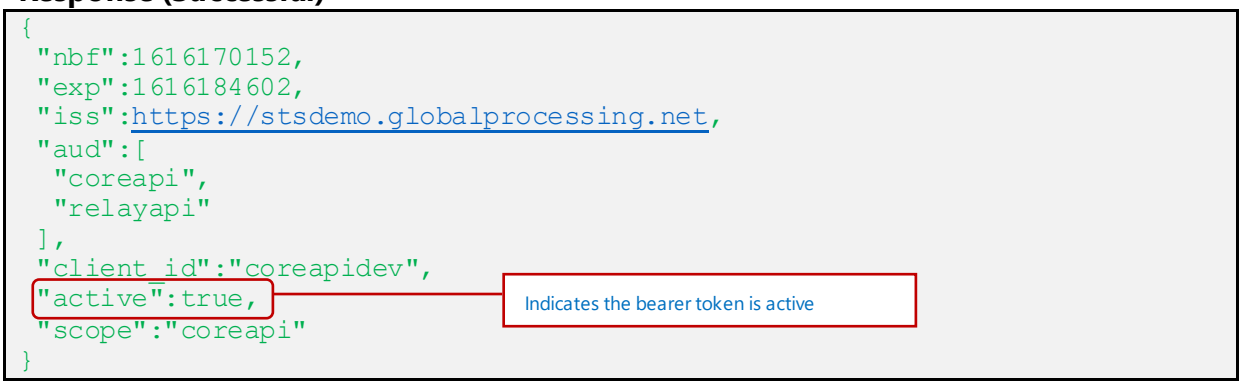
Request

```
POST https://oauthuat.globalprocessing.net/connect/introspect
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Key=eyJhbGciOiJSUzI1NiIsImtpZCI6IjE5ODI3Q0E4M0NEMkNGNUUzMTAxMUVBQkQ0N0ZDNTg
4RkMyRjQ3RTIiLCJ0eXAiOiJhdCtqd3QiLCJ4NXQiOiJHWUo4cUR6U3oxNHhBUjZyMUhfRmlQd3
ZSLUkifQ.eyJuYmYiOjE2MDc1MzM1NzksImV4cCI6MTYwNzU0Nzk3OSwiaXNzIjoiaHR0cHM6Ly
9vYXV0aHVhdC5nbG9iYWxwcm9jZXNzaW5nLm5ldCIsImF1ZCI6WyJyZHhhcGkiLCJmaXJiaW9tZ
XRyaWNhcGkiXSwiY2xpZW50X2lkIjoiZmlyYmlvIiwic2NvcGUiOlsiY2xpZW50X3ZhbGlkYXRl
IiwiZmlyYmlvbWV0cmljYXBpIl19.owfqYt7Rf6zHMLY2HT3j0RH7Lti05oWkp-
bJ41QF1LZyqxaRMZWJAUxuRXJwIWrG2wtC0Q1KFzVPbZhpwKAwJvQTIymJFhryEvRUGTQqM61Nw
u_Dnsx8H-Jpi7_0PjQk4MaAhqFv6MEgDMHvxUZ2_Q6vYj_-h2rRDunHjBvhvA55-
yGLdqxeHRtNvHJQCsaVZHdLBngUpeFpWcvrbhk1SYbNlGlflYBm5aAX_YDwpWt4p_M6w7TAYJZQ
vc4Hi_NqAZwUOY7xOlhVD69onUmd74k6nt0ncowGgC3naWQieqcVMd3B1kCAnnYZfLlXMhSxeN_
XqWtjKTK3WMavYj6vrw
```

Notes

- In the request body, the *Content-Type* should be **application/x-www-form-urlencoded**
- key = token (where the token is the bearer token value you received in the header of a NotifyIniateAction request from GPS.)
- The authorization header should be in the following format: Basic (hashed value). The hashed value needs to be resourceid:password and must be base64 encoded.

Response (Successful)



Response (Failure)

Notes

- The scope field indicates your application permissions. It is sufficient to check that the bearer token is active. You can optionally also check the scope.
- If you are using .net, GPS recommends using the Identity Model middleware software package. For more information, see https://identitymodel.readthedocs.io/en/latest/

4.4. Card Renewals and Credential Auto-enrolment

When an existing card is about to expire, you can renew the card using the Card Renew (Ws_Renew_Card) web service. For details, see the Web Services Guide > Card Renew.

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.

5. Additional 3D Secure Considerations

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

5.1. Support for 3D Secure Versions

3D Secure v1 and v2 are Card Scheme (Visa/MasterCard) versions. GPS and Cardinal Commerce support both versions. There are major differences between 3DS versions 1 and 2, and some minor differences between 2.1 and 2.2. GPS always ensure you have both versions, to cover all scenarios.

The versions are based on the Scheme's mandates to support PSD2.

GPS and Cardinal support Mastercard V1.0 and 2.1. Cardinal are working with Mastercard on the certification for 2.2; the mandate deadline is October 2022, however Cardinal will be certified by the end of 2021.

GPS and Cardinal are ready with Visa 1.0, 2.1 & 2.2

When setting up your 3D Secure rules on the Cardinal Portal, you should set these up on both v1 and v2 to ensure you support all merchants. See Appendix 1: Cardinal 3D Secure Rules.

Note: GPS recommends you set up rules on both versions, to ensure that you can support merchants on both v1 and v2.

5.1.1. 3D Secure v1

3DS v1 supports Strong Customer Authentication (SCA) compliance for PSD2. It also provides merchant fraud liability protection, but only until October 2021 for Visa Secure - 3DS1.

V1 is unpopular with consumers and causes issues for merchants. It dates to a time before smart phones.

The Card Schemes will start to decommission 3DS v1 from October 2021, and merchants will also lose the liability shift advantage.

5.1.2. 3D Secure v2

3DS v2 provides SCA compliance and merchant fraud liability protection. It provides support for Smart devices and a better customer experience.

It enables merchants to send additional information to the issuer. It supports the use of dynamic authentication through Biometrics and In-app authentication methods.

3DS v2 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.

5.2. Supported Authentication Types

Refer to the table below for details of the authentication types which GPS supports. The <Type> value is the name as used in the RDX web service (Ws_AddUpDelCredentials) 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 enrols your cards in this service. You do not need to do this via GPS web services.
OTPSMS	OTP SMS authentication. Cardinal generates a single-use One-Time Password (OTP). GPS 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.
BIOMETRIC	Biometric authentication. Cardinal sends a Biometric authentication request to GPS 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 GPS.
OUTOFBAND	In-App authentication. Cardinal sends the Out Of Band (OOB) authentication request to GPS 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 GPS. **Note**: OOB is currently not available. Please check with your 3DSecure Implementation Manager before integrating this method.
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? KBA may be combined with OTP SMS or OTP Email.

6. 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.

6.1. Creating Rules

To create a rule:

1. In the **Rules for 3DS 1.0** or **Rules for 3DS 2.0** box, click **Launch**. (You need to set up rules for both 1.0 and 2.0.)
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:

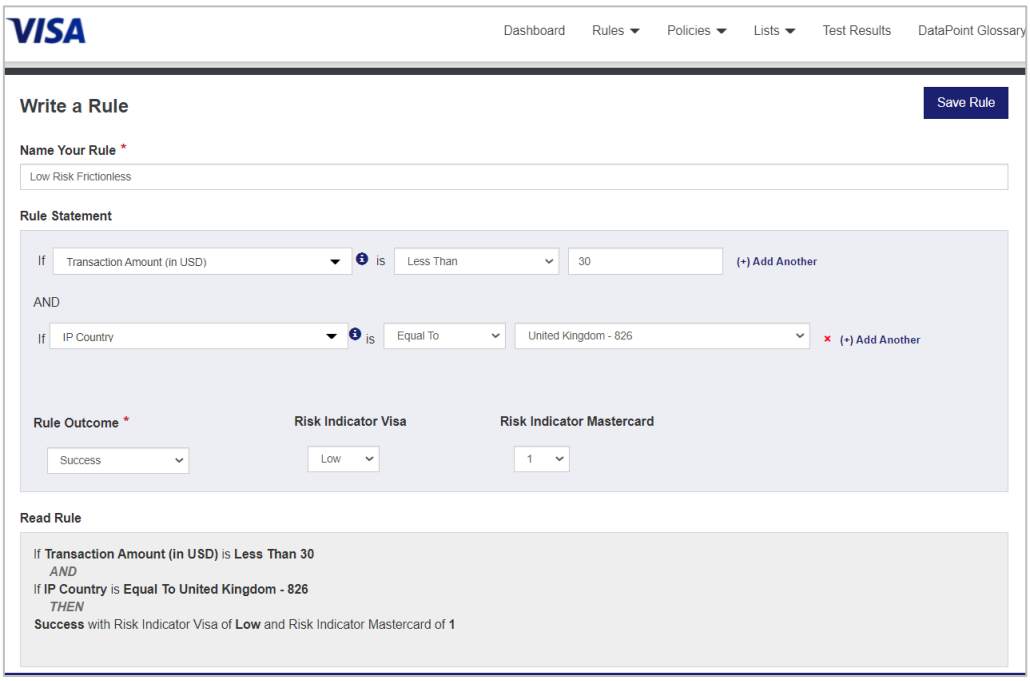


Figure 12: Cardinal Rule Editor

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.

6.1.1. 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.
Rejected[15]	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).

6.1.2. 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

[15] Relevant to 3DS 2.0 only.

Status	Description
U	Unavailable

6.2. 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**.

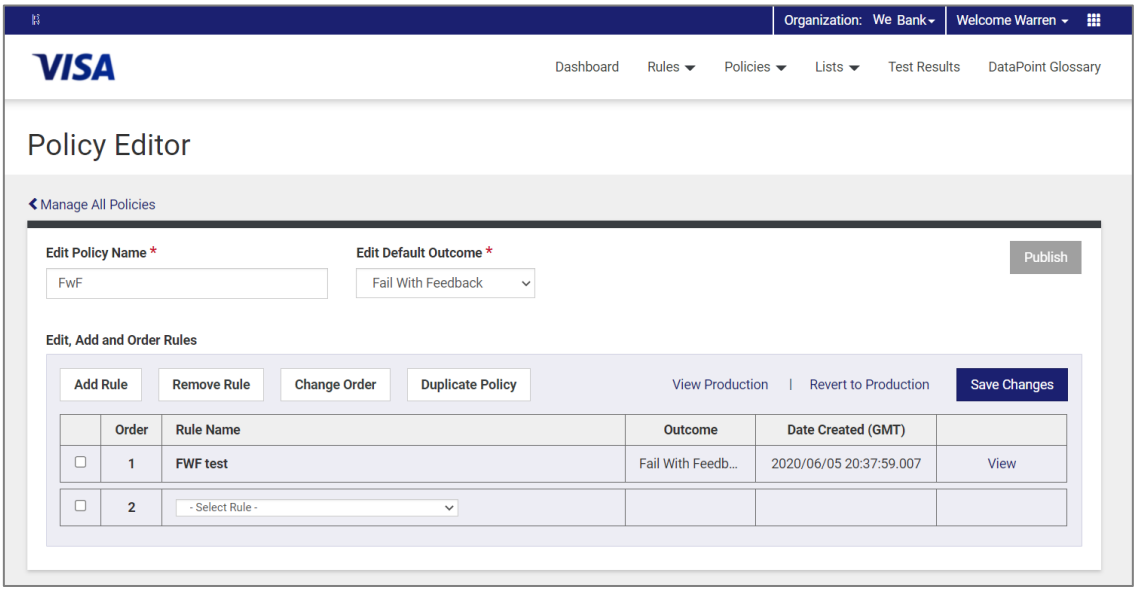
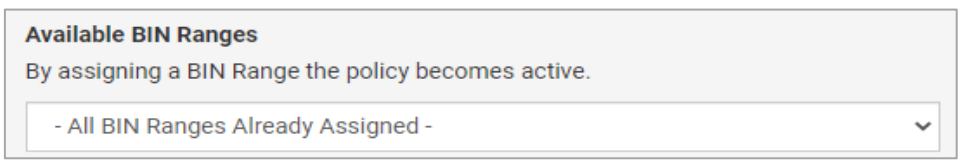


Figure 13: Cardinal Policy Editor

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**.

7. Appendix 2: OTP Message Templates

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

7.1. OTP SMS

Full template

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

```
English: @OTP is the 3DS OTP from card ending by @CardNumber with
@MerchantName for @CUR @Amount. Please use the OTP to complete the
transaction.]
```

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

If merchant information is not present

```
@OTP is the 3DS OTP from card ending by @CardNumber for @CUR @Amount.
Please use the OTP to complete the transaction.
```

If transaction information is not present

```
@OTP is the 3DS OTP from card ending by @CardNumber with @MerchantName.
Please use the OTP 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 3DS OTP from card ending by @CardNumber. Please use the OTP to
complete the transaction.
```

7.2. OTP Email

The details below are examples and can be configured.

Details in the Email header

Sender: Email account of the Program Manager

Subject: @ProgMgrCode - 3DS One Time Password

If merchant and transaction information is missing

```
The 3DS OTP is @OTP from card ending @XXXX. Please use the OTP to complete
the transaction.
```

If merchant and transaction information is present

```
The 3DS OTP is @OTP from card ending @CardNumber with @MerchantName for
@CUR @Amount. Please use the OTP to complete the transaction.
```

8. Appendix 3: Biometric/OOB Fields

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

8.1. NotifyInitiateAction Message Fields

Below are details of the fields in the NotifyInitiateAction request which GPS sends to your systems. For more information, see Initiating a Biometric Session.

Field	Description	Data type	Length	Status
Pubtoken	GPS 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 GPS generates during enrolment.	String	36 characters	Required
Type	Credential type: • BIOMETRIC • OUTOFBAND SMSOTP and EMAILOTP types are not sent to Program Managers; GPS sends OTPs directly to cardholders.	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	How the request was created: • GA - GPS auto-enrolment process. • PM -Program Manager calling GPS Hyperion API Credential Call **Note**: GPS recommends you store credentials upon receiving the *NotifyInitiateAction* request.	String	ENUM	Optional

Field	Description	Data type	Length	Status
MerchantInfo		Object		Optional
AcquirerID	Identifier of the merchant acquirer.	String	Up to 11 characters	Optional
MerchantID	Identifier of the merchant performing the purchase request.	String	Up to 35 characters	Optional
MerchantName	Merchant name.	String	Up to 40 characters	Optional
MerchantURL	URL or name of the merchant's website or app.	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
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

8.2. NotifyValidate Message Fields

Below are details of the fields in the NotifyValidate message which you should use to notify GPS of the result of the biometric/OOB session. For more information, see Notifying GPS of the Result of the Biometric Session.

Field	Description	Data type	Length	Status
Pubtoken	The 9-digit GPS 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 NotifyInitiateAction request).	String	36 character	Required
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	One of the following status values must be returned: • 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		

Field	Description	Data type	Length	Status
Reference number	Program Manager reference number for the error. Used by GPS for referencing purpose. Used for FAILURE, ERROR and FAILWITHFEEDBACK status.	String	Up to 15 characters	Optional
Description	Short description of the error. Used by GPS 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

8.2.1. GPS Response

Below are details of the GPS response to your NotifyValidate message:

Field	Description	Data type	Length	Mandatory / Optional
Pubtoken	GPS 9-digit GPS 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: • SUCCESS –the 3DS result was received before the timeout period • TIMEOUT – the 3DS result was received after the time out period • ERROR- In case of any internal technical failures • FAILURE - In case of any validation failures.	String	ENUM	Required

Field	Description	Data type	Length	Mandatory / Optional
Error		Object		
Reference number	Program Manager reference number for the error. Used by GPS for referencing purposes. Used for ERROR status only.	String	Up to 15 characters	Optional
Description	Short description of the error. Used by GPS for referencing purposes. Used for ERROR status only.	String	Up to 100 characters	Optional

9. 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 GPS 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?

9.1.1. Language Support for KBA Questions

If you offer your card products in other languages, you can provide GPS with your translated KBA questions. Any additional languages for your card products must also be configured for your BIN/sub-BINs at Cardinal. GPS 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.

9.1.2. KBA Question Examples

Below is a code snippet example, showing the use of the KBA credential in the RDX Card enrolment web service (Ws_AddUpDelCredentials). 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>
 <KBA_Answer>Skoda</hyp:KBA_Answer>
 <KBA_AnswerOldValue></hyp:KBA_AnswerOldValue>
</hyp:Credential>
```

Example shows KBA ID with a Value of *4*. The answer stored in the GPS database will be *Skoda*.

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

Translated KBA Question Example

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

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

10. 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

11. Frequently Asked Questions

11.1.1. 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 are the deadlines for implementing 3D Secure with Biometric authentication?

For cards issued within the EEA (European Economic Area), the regional Card Scheme 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 has been extended until March 2022.

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

11.1.2. 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 GPS for authorisation: either GPS or your systems authorise, depending on whether the card balance is maintained by GPS or on your systems (EHI Mode 1,2,4 and 5).

If the cardholder does not pass 3DS authentication, the transaction will not reach GPS 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: V1 and V2. Version 1 is 1.0, version 2 is 2.1 and 2.2.

The rules you set up on the Cardinal Portal apply to both V1 and V2. Both versions work with all the authentication types available within RDX (OTP SMS, OTP email, Biometric/In App).

For more information, see Support for 3D Secure Versions.

11.1.3. 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, or can we use the VPN connection?

The REST-based API calls that are used for Biometric authentication (NotifyInitiateAction and NotifyValidate) are made outside of the existing VPN tunnel between GPS and your organisation. The endpoint is secured with our OAuth security server (see Using the GPS OAuth Server).

- GPS only allow incoming requests from permitted IP addresses.
- For GPS calls to your systems, we recommend you restrict access to permitted GPS IP addresses. See Authorising GPS IP Addresses.

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

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

Q. We are currently using Batch File processing. Can we start the Biometric project without upgrading to RDX?

No, if you need Biometric authentication, you must upgrade to RDX. For details, see Upgrading from Batch to RDX.

11.1.4. 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.

GPS provides a UAT environment, where you can use Cardinal's UAT simulator to test transactions. See Step 6: Complete Staging/UAT Testing.

Q. How do we test RDX Biometric in Production?

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

- You can use the Card Create web service (Ws_CreateCard) to create pilot cards in the production environment. For details, refer to the *GPS Web Services Guide*.
- 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 forms to set your pilot cards to live on the Scheme's directory server.
- GPS activate your products for RDX Biometric, and you enrol your cards in 3D Secure by calling the 3D Secure RDX web service (Ws_AddUpDelCredentials). See Using the Card Enrolment API.
- You need to set rules in the Cardinal Portal to challenge transactions, so transactions are authenticated. See Step 2: Set up Rules in the Cardinal Portal.
- 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.

11.1.5. RDX Card Enrolment

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

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

Note: If you are using the legacy Cardinal batch API calls, this does not support the RDX API Ws_AddUpDelCredentials. You can continue to use the legacy API (Ws_Insert3DSecureDetails, Ws_Update3DSecureDetails and Ws_Delete3DSecureDetails) until you are set up and your Sub BIN/BIN ranges are enrolled in RDX. See Upgrading from Batch to RDX.

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

The SOAP web services WSDL is available here:

https://ws-test.globalprocessing.ae:10000/hyperion_its/Service.asmx?WSDL

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

Yes, GPS can auto-enrol your cards. You must ensure that both existing and new cards have the information required for 3DSecure in Smart Client, such as a mobile phone number to use for OTP authentication.

Note that you still need to use the 3D Secure RDX web service (Ws_AddUpDelCredentials) to manage your cardholder records (e.g., to update the linked cardholder mobile phone number or delete a card from Biometric authentication).

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

In your 3DSecure enrolment request (using Ws_AddUpDelCredentials) you can 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>+5858585858588</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 web service (Ws_AddUpDelCredentials) and use the *Get* function to request the authentication methods for any enrolled card.

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, this is up to 8 characters. For example: **669**
In the NotifyinitiateAction web service this is 36 characters (GPS adds leading zeros to the Credential ID as required by Cardinal). For example: 000000000000000000000000000000000**669**.

11.1.6. Batch to RDX Upgrade

Q. What's the upgrade process from Batch to RDX?

For details of the upgrade process, see Upgrading from Batch to RDX.

Q. Can I use auto-enrolment?

Yes, you can ask GPS to auto-enrol your cards in RDX or do this for individual cards using Ws_AddUpDelCredentials web service.

Enrolment by the auto-enrolment or the web service needs to be completed before cardholders attempt online transactions. Auto-enrolment is far preferable in scenarios where new cardholders are likely to transact immediately, such as on creation of a virtual card.

Please contact your 3DS project manager to confirm the date and time for GPS to apply auto-enrolment for all the existing cards.

Q. How will the auto-enrolment from batch to RDX work?

GPS will select all cards already enrolled in 3DS OTP SMS via Batch File which have a mobile number (if any) and all live cards (not enrolled to 3DS from Card Creation WS) with Active status 00 and live. (i.e., all the existing 3DS customers) and ongoing enrolment process (new customers post implementation).

Auto-enrolment may take several hours, depending on the number of cards in your program.

Adding the auto enrolment for the Biometric capability typically is a separate project. First, we switch auto-enrolment for your cards to RDX with OTP SMS.

If you no longer want OTP SMS, on another separate date, we can switch this off after you have confirmed Biometric is working.

During the time of enrolling the cards from batch to RDX, there is no impact to transactions, but you cannot enrol any new cards using the batch file API Ws_Insert3DSecureDetails web service.

Q. What happens if the requested authentication type is not available?

If Cardinal contacts GPS to request a type of authentication where the cardholder is not able to authenticate using that method or where the method requested is not currently available (the card is not enrolled to this type of authentication), you return a response of *STEPUP* in your NotifyValidate call, and GPS will return the fallback method to Cardinal.[16]

Example:

Biometric requested, but only OTP via SMS is available for a card. Cardinal will generate the OTP which GPS will send to the cardholder's mobile number.

Q. Can certain cards be automatically excluded from RDX Biometric enrolment?

Example: can we exclude cardholders who don't have a smartphone.

Yes, you need to confirm the card sub-BIN ranges for which you want RDX Biometric.

At GPS, enrolment/auto-enrolment works based on sub-BIN ranges (8 digits) for the default and fallback authentication method (e.g., product level). Cardinal configuration works according to what you have requested to be configured at Cardinal as sub-BIN (8 digits) level or BIN level (6 digits).

If you want to include any previously excluded cards, you can do this via web services.

Q. Can we receive notification of auto-enrolments along with the enrolment IDs?

No, this is not possible. The Enrolment status is provided in the NotifyInitiateAction messages GPS sends to your systems. Enrolment status is listed in the ChannelCreated field. See Initiating a Biometric Session.

Q. How can we obtain a list of all auto-enrolled cards?

GPS will extract the Credential IDs after bulk auto-enrolment in RDX at the time of the upgrade and share it with you.

For any new auto-enrolled created card, you can use the RDX web service (Ws_AddUpDelCredentials) with the GET option to return details of the card's Credential IDs. See Using the Card Enrolment API.

11.1.7. 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 Step 1: Complete your 3DS Product Setup Form.

[16] The fallback option is triggered when the cardholder is unable to authenticate using their main authentication method.

The supported authentication types must then be added to the card using Ws_AddUpDelCredentials or, 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 GPS of the Result of the Biometric Session.

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

Q. Can we use Email OTP as a fallback authentication type?

Yes, if you are using the Cardinal RDX service. See OTP Email.

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 Screens. See the example below:

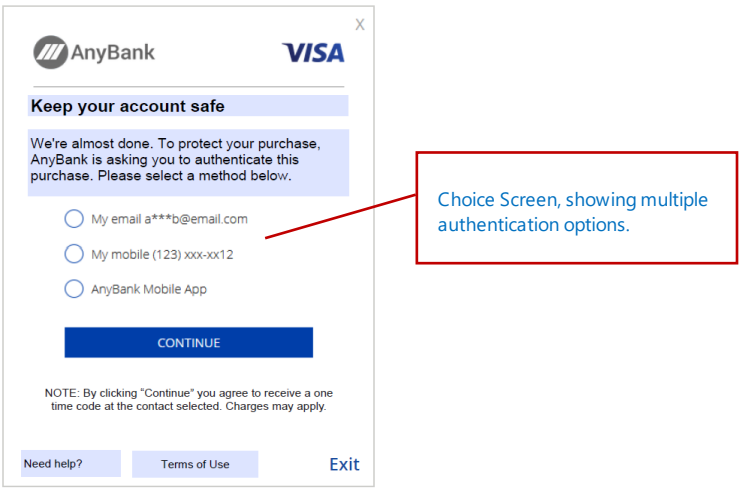


Figure 14: Choice Screen – where the user can select a method

To populate the options that appear on this screen, you need to register your cards for the required authentication types using Ws_AddUpDelCredentials or request auto-enrolment from your 3DS project manager.

11.1.8. 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:

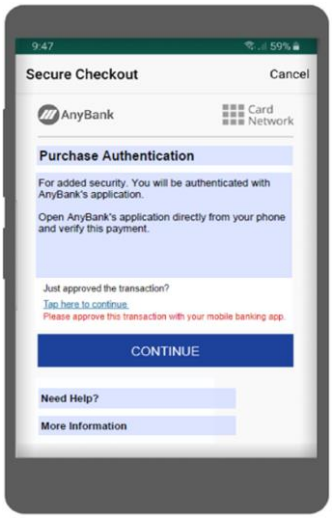


Figure 15: Biometric/OOB Authentication Screen

You can specify the text that appears on this screen using the *3DS Product Setup Form*; see Screens.

Q. How does a Biometrics/OOB session work?

GPS 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 RDX 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/OOP) 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 GPS and GPS 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 GPS, using the NotifyValidate API endpoint. See Notifying GPS of the Result of the Biometric Session
5. GPS returns the response to Cardinal.

Further information on the Biometric call flow is described in the section Authentication using Biometrics or In-App OOB.

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 GPS automatically use the fallback option?

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

Q. What authentication type should we use for OOB authentication?

Note: The OUTOFBAND authentication type is currently not available. Please use BIOMETRIC instead. Please check with your 3DSecure Implementation Manager before integrating this method.

If your Customer application supports an Out of Band (OOB) authentication method, such as In-App, then as a temporary solution (until OUTOFBAND is ready), you can enrol your cards in the BIOMETRIC authentication type. During an authentication session, when you receive the NotifyInitiateAction you should authenticate the cardholder using your App and then respond to GPS with the NotifyValidate results.

Note: To ensure a good customer journey, make sure you configure the screen text options so that the Cardinal Authentication screens display appropriate text to the cardholder.

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

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

- Use Ws_AddUpDelCredentials with '*Delete*' to remove the Biometric Credential ID for this card.
- 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 GPS of the Result of the Biometric Session.

If the card has not been auto enrolled, you can use Ws_AddUpDelCredentials to add the required credentials to the card.

11.1.9. 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. Please provide the translation for the OTP message. See Appendix 2: OTP Message Templates.

11.1.10. 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**[17]– 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, OTP SMS or OTP Email).

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 Step 6: Complete Staging/UAT Testing.

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

Mastercard provides test cases for some Issuer's Program Managers to verify the 3D secure authentication process under the PSD2 rules. If you have been contacted by your issuer to complete MC PSD2 test cases, contact your 3DS project manager.

[17] Rules 1.0 do not support Rejected.

12. Glossary

This section explains terms used in this document.

Term	Description
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 to check that the card is valid, and that the requested authorisation amount is available on the card.
BUSINESS IDENTIFIER (BID)	A business ID, which is unique to each Visa business customer.
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.
CARDINAL COMMERCE	3D Secure service provider.
CARDINAL PORTAL	Cardinal Commerce online account administration and rule configuration portal where customers can configure their 3D Secure service, view 3DS ecommerce transactions and run test transactions.
CARDHOLDER	Consumer or account holder who is provided with a card to enable them to make purchases.
CARD SCHEME	Card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.
EHI	External Host Interface. This is a GPS product providing clients either a real time feed or the ability to be involved in authorisations.
FRAUD LIABILITY PROTECTION	3D Secure transactions provide the online merchant with fraud liability protection.

Term	Description
FRICTIONLESS AUTHENTICATION	When a transaction is approved without requiring any manual input from the cardholder.
ICA	The Interbank Card Association Number (ICA) is a four-digit number assigned by MasterCard to a financial institution, third party processor, or other member to identify the member in transactions.
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	The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant Card Scheme.
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.
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.
ONE TIME PASSWORD (OTP)	A password that is valid for a single use only. During an authentication session (where the authentication type is with OTP SMS or OTP Email), the cardholder must enter this OTP to authenticate.
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.
PAN	The card's 16-digit permanent 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. All merchants who

Term	Description
	handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security
PRODUCT SETUP FORM (PSF)	A spreadsheet that provides details of your GPS account setup. The details are used to configure your GPS account.
PROGRAM MANAGER	A GPS customer who manages a card program. The Program Manager can create branded cards, load funds, and provide other card or banking services to their end customers.
PUBLIC TOKEN	The GPS 9-digit token is a unique reference for the PAN. This is used between GPS and clients to remove the need for GPS clients to hold actual PANs.
REALTIME DATA EXCHANGE (RDX)	3D Secure real-time API calls provided by Cardinal Commerce and GPS.
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).
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
SMART CLIENT	Smart Client is GPS's user interface for managing your account on the GPS Apex system. It is also called Smart Processor GPS. Smart Client is installed as a desktop application and requires a VPN connection to GPS systems in order to be able to access your account.
SOFT DECLINE	An issuer can use a soft decline if they receive a request from a merchant to authorise a payment, but they want to use authentication first.
STRONG CUSTOMER AUTHENTICATION (SCA)	Strong Customer Authentication (SCA) requires a combination of two factor 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).

Document History

Version	Date	Description	Revised by
0.1	22/04/2021	Draft version	VAL
1.0	28/06/2021	First version – major rewrite and update	WS
1.1	30/09/2021	Address updates and update to *Figure 3: 3D Secure Authentication Process Using RDX and Biometrics*. New Appendix 3: Biometric/OOB Fields	WS
1.2	01/11/2021	Removed the port number from UAT URLs.	WS
1.3	31/01/2022	Addition of Knowledge Based Authentication (KBA) Removal of references to OTP Email, which is currently not supported.	WS
1.4	08/03/2022 14/04/2022	Updates for the Out of Band (OUTOFBAND) authentication method. Added notes to clarify that the OUTOFBAND authentication type is not yet available. Correction: the bearer token in the header of the NotifyInitiateAction request, should be *Authorization: Bearer*	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 Card Renewals and Credential Auto-enrolment.	WS