Product Sheet

3D Secure (Cardinal)

Reduce risk of fraud and give cardholders a more secure buying experience

Use 3D Secure in your payment programmes to protect online credit and debit card transactions, reduce the risk of fraud and give cardholders a more secure buying experience

3D Secure (Three Domain Structure), also known as 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 'Visa Secure' and 'Mastercard Identity Check' respectively.

Thredd use Cardinal Commerce as our 3D Secure service provider. Cardinal and Thredd provide a real-time 3D Secure enrolment and authentication service called Realtime Data eXchange (RDX). You can implement this service through Thredd to ensure that your cardholders are successfully enrolled and authenticated using 3D Secure. You can find out more about Cardinal at: https://www.cardinalcommerce.com/

Features

Configurable Authentication

- Multiple authentication types available including risk-based authentication (RBA), one-time password (OTP), and Strong Consumer Authentication (SCA) methods like biometric and out-of-band (OOB)
- Solution is fully supported by Visa and Mastercard

Full Coverage

- Full global coverage
- Configurable rules
- Configurable risk-based authentication (RBA) rules for a frictionless authentication approval decision, and challenge rules to trigger a request for further authentication

Real-time

- Real-time 3D Secure enrolment and authentication using Cardinal and Thredd Realtime Data eXchange (RDX)

Secure

- Compliant with the Second Payment Services Directive (PDS2)

Benefits

Business Facing

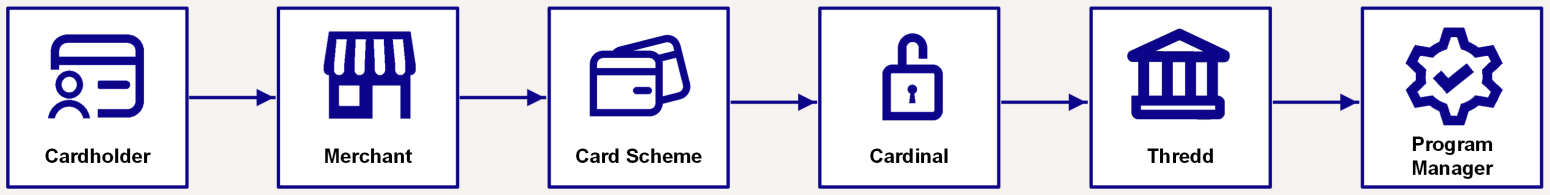
- Reduce the risk of fraud in online credit and debit card transactions
- Real-time 3D Secure enrolment and authentication using Cardinal and Thredd RDX
- Fully configurable authentication and challenge rules to suit your products and customers
- Peace of mind and reduced costs in achieving regulatory compliance
- Seamless integration managed through a set of SOAP and RESTful APIs

Customer Facing

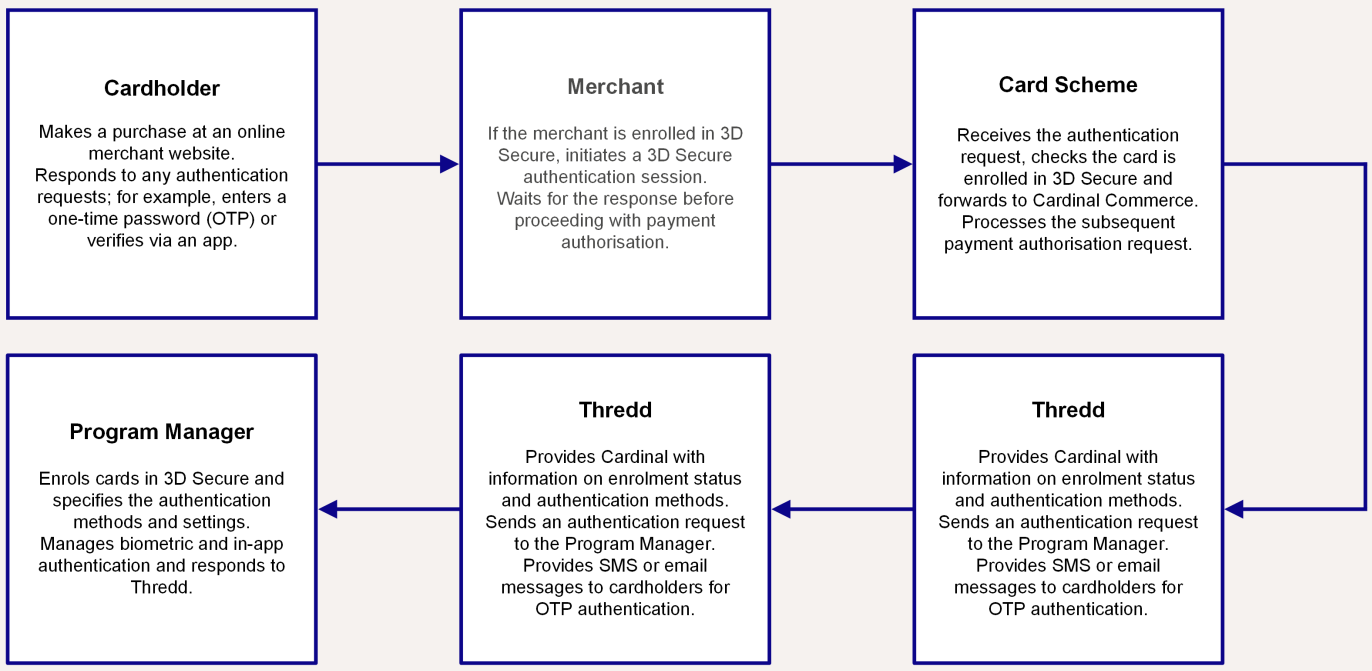
- Greater security protection when making e-commerce transactions
- A more streamlined purchasing experience
- Enhanced control through a choice of authentication methods, including one-time password (OTP), biometric and in-app authentication

How it works?

During the 3D Secure authentication session, several parties are involved in exchanging data, as shown in the following diagram:

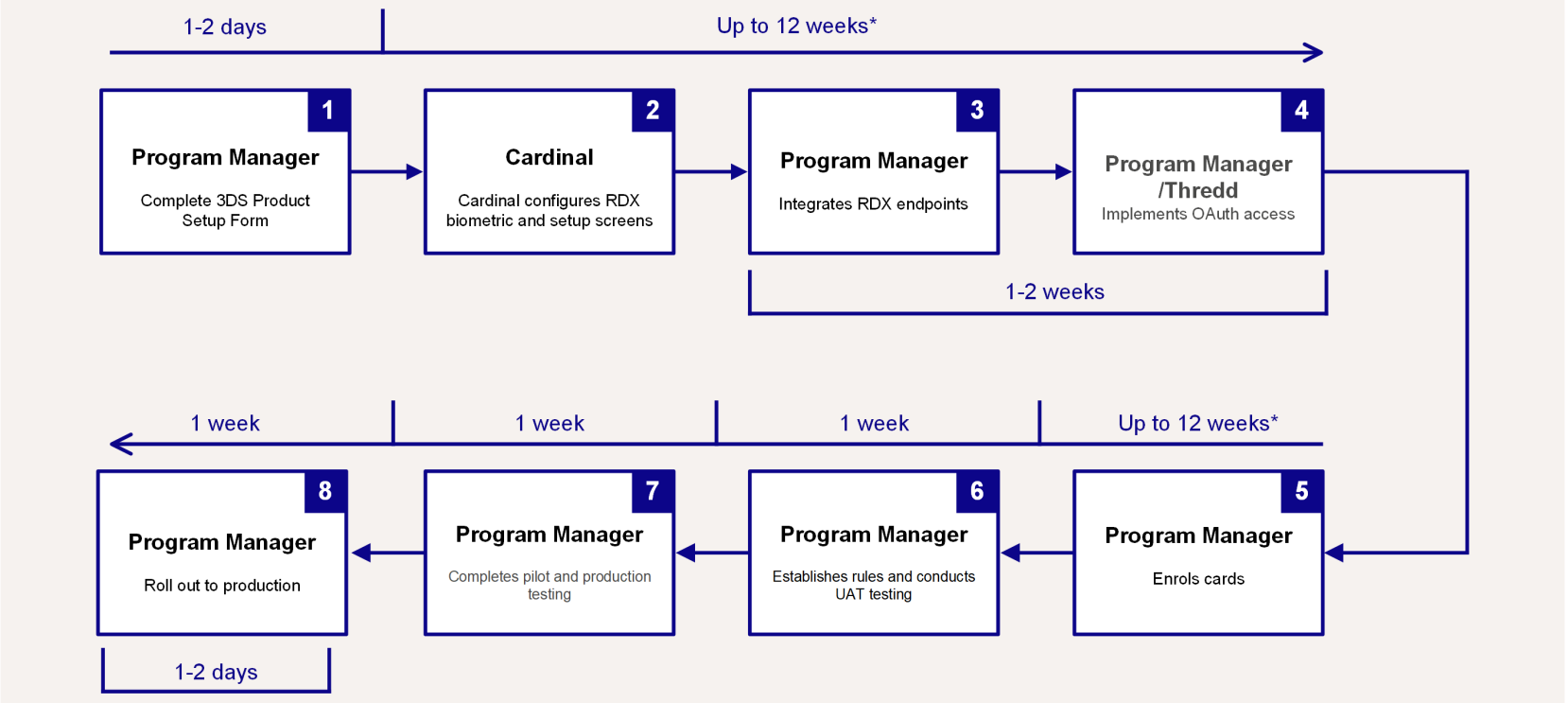


The role played by each party is explained in more detail below:



Setup At-a-Glance

The diagram below provides an overview of the steps in a typical Biometric/In-App project. You must have the RDX service set up prior to implementing Biometrics or In-App authentication.



Note: All time-lines are approximate.

These steps are explained in more detail below:

1. Complete your 3DS Product Setup Form (PSF). Your Thredd 3DS project manager can help you complete this form.
2. Cardinal sets up your 3D Secure account. Cardinal configures your 3D Secure settings, portal access and customised authentication screens.

   Note: RDX takes 5-6 weeks to configure at Cardinal. Biometric is a second phase which takes an additional 4 weeks. All integration steps prior to UAT testing can take place in parallel, where Cardinal sets up RDX and Biometric.
3. Integrate the 3D Secure RDX endpoints. Provide Thredd with your API endpoints and a list of permitted IP addresses for using the services. Develop the functionality to receive and process 3D Secure messages using the 3D Secure SOAP and REST API.
4. Implement OAuth access. Thredd sets up your OAuth access and provides you with details to access the Thredd OAuth server. Test that you can access the OAuth server in staging and production.
5. Enrol your cards in 3D Secure. Thredd activates a single card product in the Staging environment, so you can enrol a few cards for Staging UAT testing. You can enrol your cards and specify the types of authentication using the 3D Secure RDX Web service (Ws_ AddUpDelCredentials).
6. Complete Staging/UAT testing. Once RDX and biometric are configured, Thredd 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.
7. Complete pilot Production testing. Thredd and Cardinal set up your cards in the Production environment.Thredd activates a single card product in the Production environment, so you can enrol a few cards for pilot testing. You provide Cardinal with your pilot cards to be enrolled at the Scheme. You create your 3D Secure rules and policies in the Cardinal Production Portal. Cardinal contacts the Scheme to set your pilot cards live with a Cardinal URL.
8. Roll out to Production (Live). Notify Thredd once you have completed your pilot testing. Thredd configures your card products for 3D Secure. You need to enrol all your live cards in 3D Secure and register them for your supported authentication types (e.g. Biometric or OTP SMS). Thredd also offers an auto-enrolment option. Notify Thredd 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.

FAQs

Q. How does the 3DS authentication affect authorisation?

3DS authentication happens before payment authorisation. If the cardholder passes authentication, the transaction is sent to Thredd for authorisation: either Thredd or your systems authorise, depending on whether the card balance is maintained by Thredd or on your systems. If the cardholder does not pass 3DS authentication, the transaction will not reach Thredd for authorisation.

Q. What regulations are relevant to Biometric authentication?

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

- PSD2. For details, see https://ec.europa.eu/commission/presscorner/detail/en/memo_15_5793
- SCA guidelines. For details, see: https://www.visa.co.uk/partner-with-us/payment-technology/strong-customer-authentication.html

Q. What Biometric options can I use?

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

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

Yes, the dynamic OTP SMS or OTP email message can be configured in a language other than English. Note that only one language can be configured at a time. You need to provide the translation for the OTP message. For more information, see the 3D Secure Guide.

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

Cardinal supports EMV 3D Secure protocol versions 2.1.0 and 2.2.0.

Q. Is documentation available?

For more information, see the 3D Secure Guide.

Q. Where can I find out more?

To discuss implementing 3DS in your Thredd deployment, contact your Account Manager.

Contact Us

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

Thredd Ltd.

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.