Product Sheet

3D Secure (Apata)

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

3D Secure provides an extra layer of security for online credit and debit card payments

Note: 3D Secure is mandatory for e-commerce card transactions in the EU, UK, and certain Latin American and Asia-Pacific markets. Beyond mandates, there is also a financial implication: merchants will enforce 3DS to shift liability to the issuer and receive reduced interchange as a result.

3D Secure (Three Domain Structure) is a security protocol that helps to prevent fraud in e-commerce 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. You can 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.

Thredd use Apata as our 3D Secure service provider. Apata and Thredd provide a real-time 3D Secure enrolment and authentication service. 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 Apata at: https://apata.com/.

Features

Configurable Authentication

- Multiple authentication types available including:
  - One-Time Password (OTP) via email or SMS
  - Behavioural Biometrics
  - Knowledge Based Authentication
  - Strong Customer Authentication (SCA) methods like Biometric and Out of Band authentication
- Solution is fully supported by Visa and Mastercard.

Full Coverage

- Full global coverage.
- Configurable rules.
- PSD2 SCA exemptions support including TRA (Transaction Risk Analysis), Low value Payment (LVP) and Secure Corporate Payment exemption.
- Seamless integration managed through a set of SOAP and RESTful APIs.

Real-time

- Real-time 3D Secure enrolment and authentication using Apata and Thredd.
- Compliant with the Second Payment Services Directive (PDS2).

Benefits

Business Facing

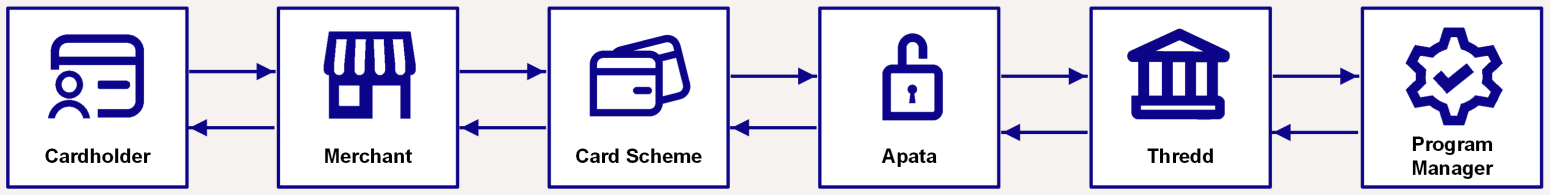
- Increase Customer Trust – 3D Secure adds an extra layer of security for online transactions, reducing fraud risk.
- Enhanced Conversion Rates – with customer preferred & frictionless experiences.
- Improve Fraud Prevention – authenticating cardholders, greatly minimizing the chances of unauthorized transactions.
- Reduce Chargebacks – leads to fewer chargebacks by validating legitimate transactions.
- Enable Scale & Growth – 3D Secure is globally recognized and accepted by online merchants, making it the easiest way to authenticate card transactions.

Customer Facing

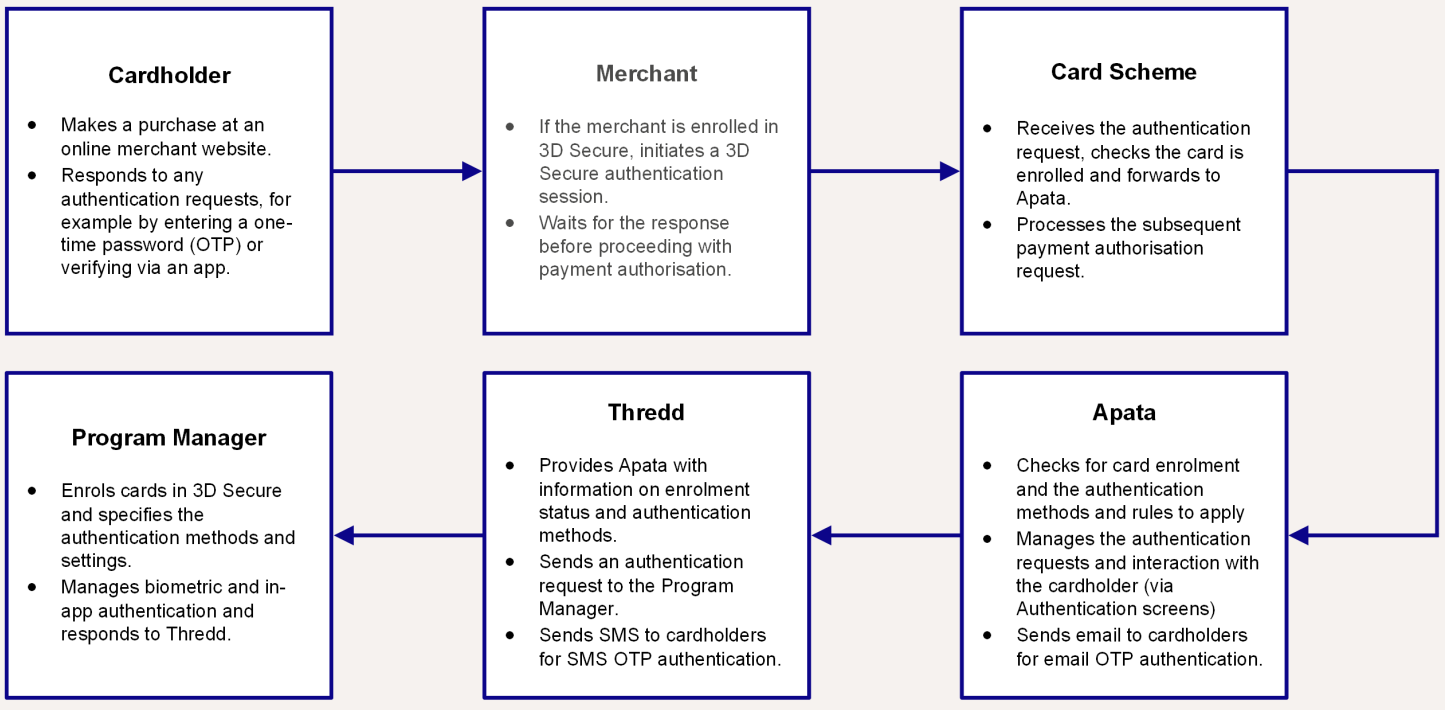
- Greater security protection when making e-commerce transactions.
- A more streamlined purchasing experience.
- Enhanced control through a choice of authentication methods.
- Seamless authentication for merchants that customers have white-listed.

How it works?

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

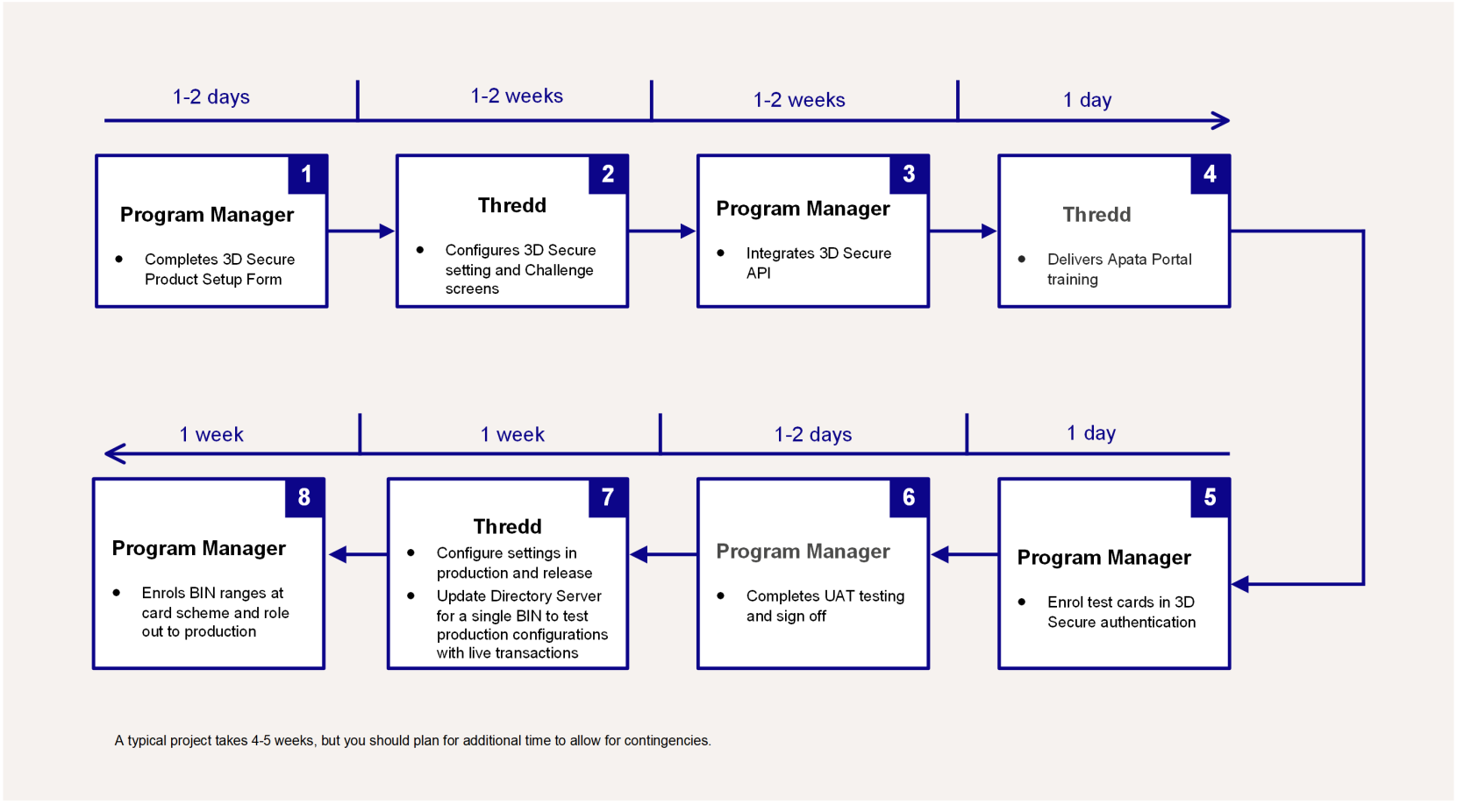


The role played by each party is explained in more detail below:



Setup At-a-Glance

The diagram below provides an overview of the steps in a 3D Secure project. A project starts once we have received your requirements. A typical project takes 4-5 weeks, but you should plan for additional time to allow for contingencies.



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. Thredd configures your challenge methods, challenge screens, card programs and setup in the UAT environment.
3. Integrate the 3D Secure API for Biometric/ Out of Band authentication (if applicable). Thredd will set up your oAuth access and provide you with credentials for the Thredd oAuth server.
4. Thredd provide your users with training on the Apata Portal.
5. Enrol your cards in 3D Secure. Thredd activates a single card product in the UAT environment, so you can enrol a few cards for UAT testing.
6. Complete UAT testing. Once 3D secure is configured, Thredd release the project into the UAT environment for you to test and sign off.
7. Complete pilot Production testing. Thredd sets up your 3D Secure configuration in the production environment. Updates the Directory Server for a single BIN to test production configurations with live transactions.
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.

   Note: If you are not self-issuing, your issuer must contact the Card Scheme to enrol the rest of your card ranges. Allow a week to 10 days to complete the roll-out at the Card Scheme and to enrol your cards.

FAQs

Q. Is 3D Secure mandatory for all cards?

Any cards that are issued in a 3D Secure mandated region are required to be enroled in 3D Secure.

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

Yes, you can use Thredd's auto-enrolment service to automatically enrol cards in 3D Secure.

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

Thredd provides flexible implementation options:

- *Initial load* – Thredd creates the authentication type credentials for all existing cards. Adding credentials for any future new cards or applying any changes to credentials for existing cards must be done manually using the enrolment API.
- *Continuous* – same as Initial load, however any future cards created 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 the enrolment API.

Q. Can I configure the rules used for processing 3D Secure transactions?

Yes, you can configure the rules for 3D Secure transaction processing using flexible Risk Profiles, which are set up in the Apata Portal.

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

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://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html
- 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 (Apata).

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

Apata 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 (Apata).

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

The EMVCo website provides detailed specifications for anyone implementing a 3D Secure project. This includes information not covered in the Thredd guides, such as authentication message flows between Issuer, ACS provider and merchant and specific internal message fields that may be passed or validated.

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.