Windcave

3D Secure FAQ

Version 1.0

Copyright

Proprietary Notice

Windcave

Document Revision Information and Amendments

All amendments are to be identified, and the manual updated, noting the amendment on this amendment page.

Version	Date	Section	Revision Information	Amended by
0.1	06/03/2025	All	Document Creation	NW
0.2	07/03/2025	All	Common and Less Common Response Codes added, plus other additional edits.	SJ
0.3	13/03/2025	4	Added FAQs section	NW
0.4	01/04/2025	All	Review and update order	NW
1.0	02/04/2025	All	Published Version	NW

Windcave

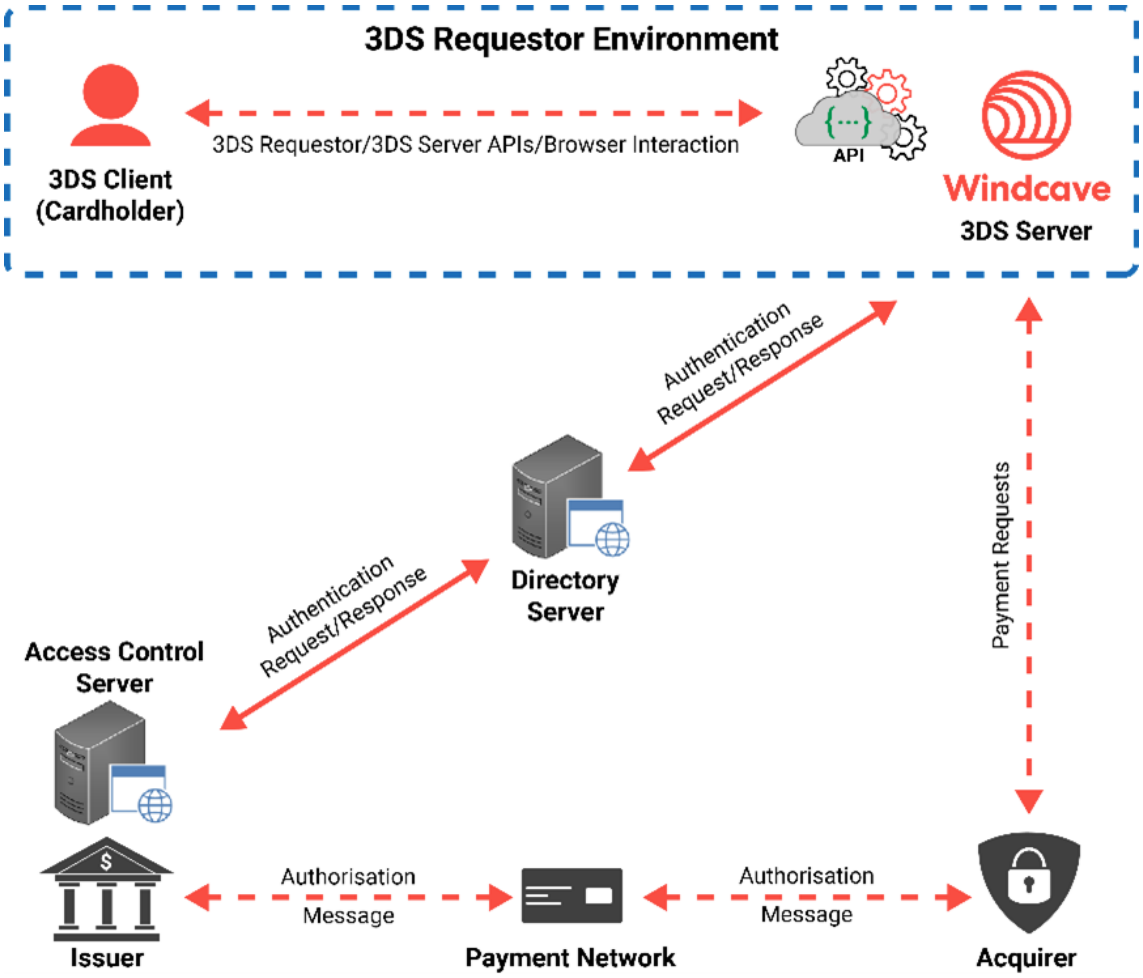
Contents

1 3D Secure

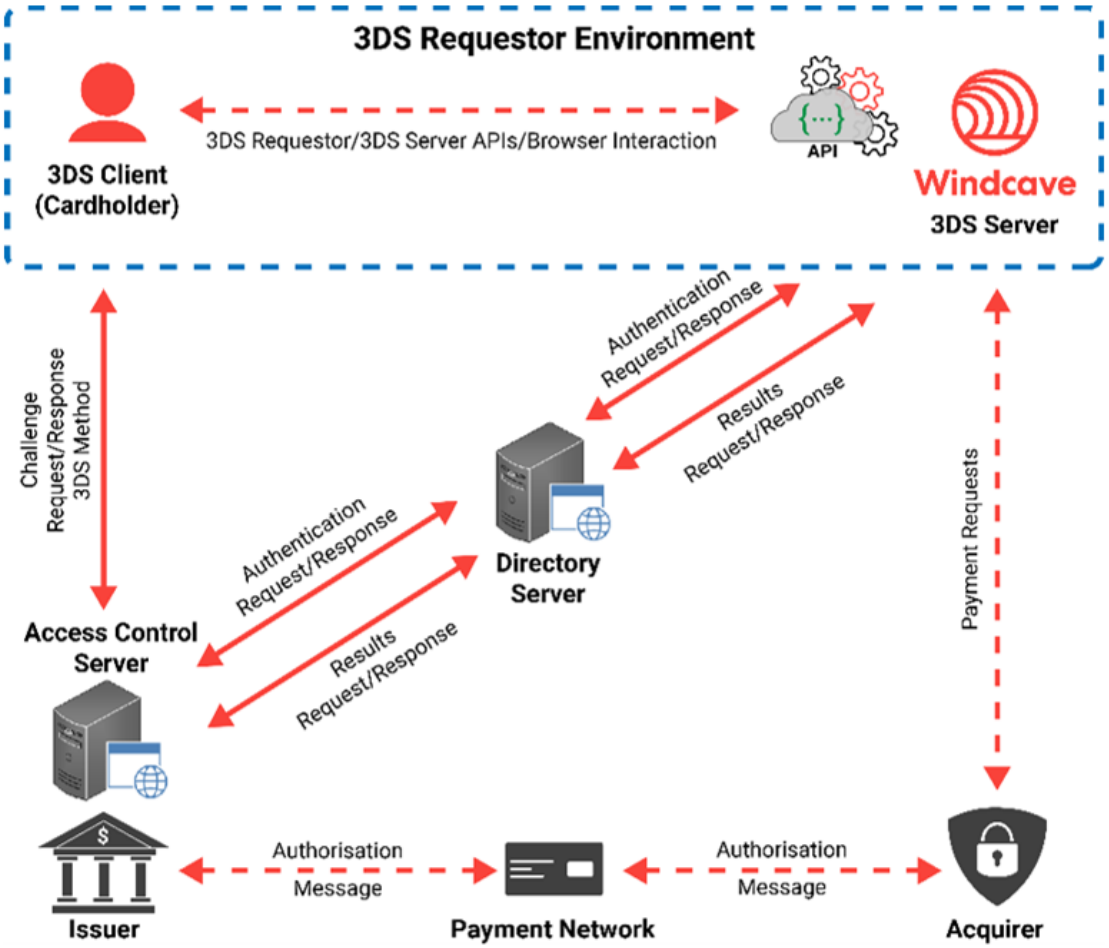
3D Secure (3DS) is an authentication tool designed to combat fraudulent online payment transactions while minimizing the friction needed for card holder authentication, so that conversion rates can be maximized.

1.1 High-level overview

Frictionless Authentication overview diagram



Challenge Authentication overview diagram



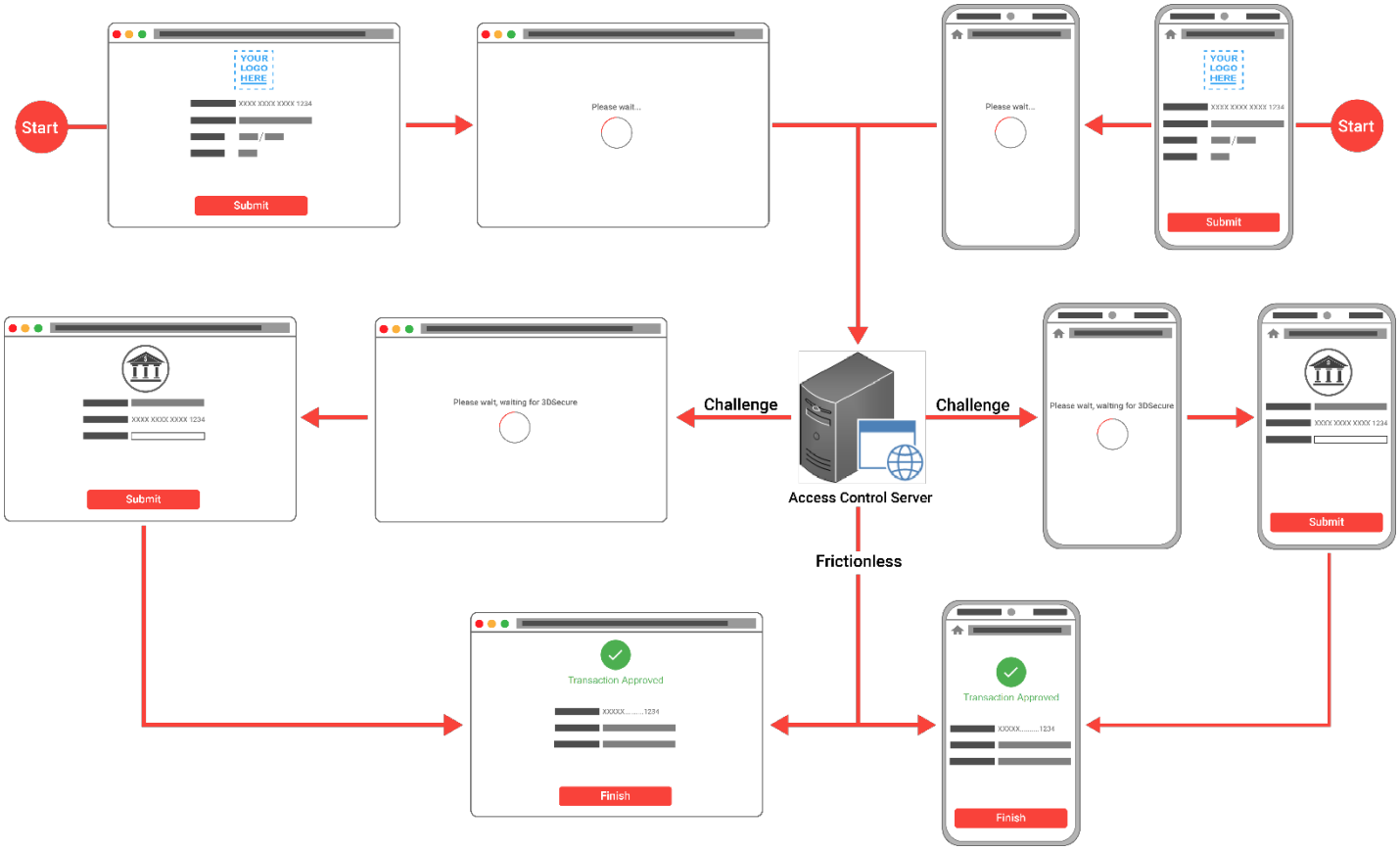
2 Understanding 3D Secure

3D Secure aims to provide a seamless authentication experience by enhancing data sharing between merchants and card issuers in a non-intrusive manner, and by supporting modern authentication methods such as two-factor authentication via SMS one time password, banking app or biometrics.

2.1 Authentication

2.1.1 Browser-Based Authentication

Browser-Based authentication embeds the 3D Secure challenge into an iFrame. This iFrame is located in the payment checkout so to the cardholder it appears as though they have not left the payment page. Below is an example of the 3D Secure browser-based authentication user experience for PC and Mobile.



2.1.2 Out of Band Authentication

OOB or Out of Band Authentication is a method that issuers can use to authenticate 3D Secure challenge. It allows issuers to process the authentication outside of the cardholder's browser interface, for example the 3DS challenge triggers a push notification via a mobile banking app for the issuer to authenticate the payment, then the cardholder is prompted to approve the payment via this app.

2.1.3 3RI

3RI (3DS Requestor Initiated) is a type of authentication where the customer is not actively participating in the transaction. An example of this is merchant-initiated transactions.

3RI is essentially back-end rebilling that follows a prior authentication via the front end (i.e. a website, loading card onto an app). Once the payment method is authenticated, the 3RI feature can be incorporated within future billing cycles, triggering 3DS authentication requests without requiring the customer to re-enter their payment details.

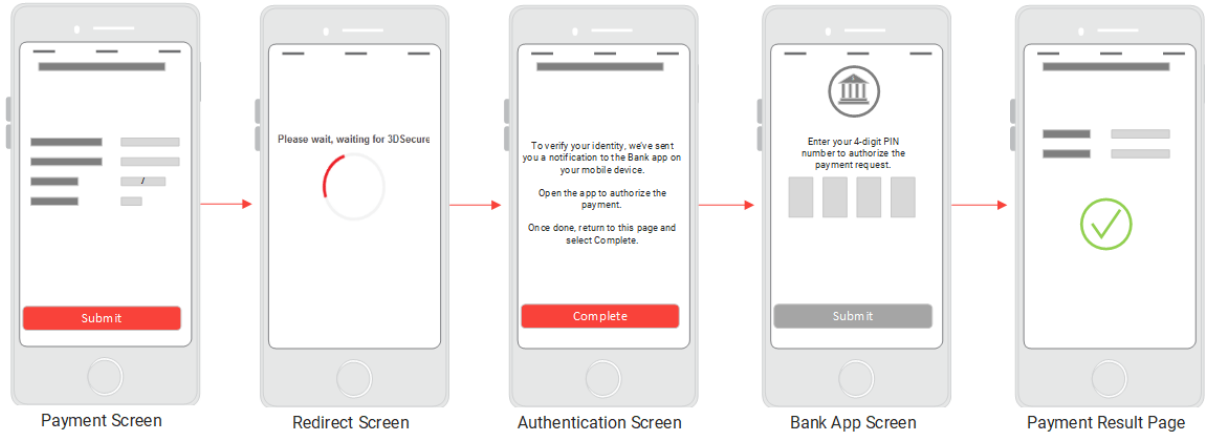
For more information on 3D Secure Authentication methods and information, please visit: https://www.windcave.com/developer-e-commerce-api-rest#3DS

2.2 Frictionless vs Challenge

A Frictionless flow is where no further authentication is required by the cardholder and payment will process as normal i.e. after entering payment details cardholder will be redirected to the transaction result page.

A Challenge flow is where the cardholder will be presented with a challenge (how this is done varies between issuers), this challenge will require the cardholder to further authenticate they are the owner of the account. Once authenticated the transaction will proceed as normal i.e. cardholder will be redirected to the transaction result page.

Below is an example of a Challenge flow:



2.3 Liability Shift

A liability shift refers to a change in who is responsible for covering the financial cost of a chargeback in the event that a payment turns out to be fraudulent.

The liability shift from 3DS protects merchants from chargebacks involving fraudulent use of a credit card, but it does not protect from chargebacks related to the merchant not providing the goods/services. If there is a dispute or chargeback from a cardholder for a transaction for fraudulent reasons (i.e. customer disputes that they made or authorized the payment) the merchant will not be liable for the dispute or chargeback costs, therefore will not have transaction funds taken from their account to be returned to the customer.

2.4 Strong Customer Authentication

Strong Customer Authentication (or SCA) is a payment regulation that makes transacting online more secure and helps reduce the risk of fraud. SCA is also known as two-factor authentication (2FA) or multi-factor authentication (MFA).

SCA requires a transaction to meet at least two of three components listed below:

	Knowledge Something your customer knows e.g. a PIN code or password
	Possession Something your customer has e.g. a credit card or electronic device
	Inherence Something your customer is e.g. a fingerprint or facial recognition

2.4.1 SCA Exemptions

SCA Exemptions only come into scope for businesses based in the UK or Europe and are part of the requirements of the PSD2 legislation, designed to minimize friction where possible.

Under this legislation an SCA exemption is a rule that allows a transaction to process without an SCA component.

These exemptions can be requested by the merchant or acquirer, in which case the liability will stay with the merchant/acquirer. If an exemption is not explicitly requested by the merchant/acquirer, the exemption will still be applied by the issuer to avoid SCA friction. In these scenarios, the liability remains with the issuer. Exemptions include:

1. Low-Value Transactions — Transactions under €30/£25
2. Fixed Amount Subscriptions — Recurring transactions (applicable after first payment)
3. Trusted Beneficiaries — Exemption list for trusted merchants
4. MOTO — Exempt as not considered as electronic payment types
5. Merchant-Initiated Transactions — Agreement is between the merchant and the customer

For more information on SCA and examples of SCA exemptions, please visit the Strong Customer Authentication section of our 3D Secure guide.

3 3D Secure and Payline

Transactions recorded in Payline provide valuable 3D Secure information as shown below:

Field	Description
Cavv	Cardholder Authentication Verification Value Code displayed when processed via Visa, MasterCard, Amex or Discover to prevent fraudulent transactions. If the **Cavv** and **RecoPreProc** are the **only** fields displayed on the 3DSecure tab then the transaction was not 3DS but will have been ApplePay, GooglePay or similar Payment Method with equivalent authentication check – see the Payment Method for confirmation.
ReCoPreProc	Response Code Pre-Processing Code giving information on pre-processing (i.e., before Authorization request) such as 3DSecure authentication. **3D0000** = UCAF = 210 i.e. not authenticated **3D0100** = UCAF = 211 i.e. authenticated **3D0200** = UCAF = 212 i.e. authenticated **3D0500** = ECI = 05 i.e. authenticated **3D0600** = ECI = 06 i.e. authenticated **3D0700** (Visa) = ECI = 07 i.e. not authenticated **3D0700** (MasterCard) = UCAF = 217 i.e. authenticated, MIT 3RI *UCAF (Universal Cardholder Authentication Field - MasterCard terminology) and ECI (Electronic Commerce Indicator - Visa terminology) are also known as SLI – Security Level Indicators* **3DE0** = E0 is returned when Windcave fails to receive a response back from the ACS within the timeout period (determined by the ACS and out of Windcave's control). Note this may be up to 10 minutes or more. **3DEB** = EB may indicate an issue involving currency or country code. Please raise to Windcave Support to investigate. **3DEC** = EC may indicate an issue related to the MCC (Merchant Category Code). Please raise with Windcave Support to investigate. **3DEN** = EN may indicate an issue at the ACS with an individual Authentication request (i.e. for that individual transaction). Please ask Card Holder to attempt again. **3DEP** = indicates an error in the comms from the Scheme's Directory Server to Windcave and Windcave are required by the 3DSv2 protocol to decline, regardless of the authentication result at the ACS. Please ask Card Holder to attempt again. **3DEV** = EV indicates that a 3DS v2 authentication request was sent to the DC/ACS but it did ***not*** pass authentication. Check the **3DSecure tab** for the **Transaction Status Reason Details** for explanation for the decline. **3DGU** = GU indicates an unauthenticated transaction where 3DS v2 request was not sent i.e. the card BIN range does not support 3DS v2.
Xid	*Obsolete Transaction ID* *3DS v2 now uses ACS, DS and Server transaction fields – see below for details*
Using User MPI Data	This indicates that the merchant is using an external MPI/3DS Server and then submit a transaction to us with 3DSecure details they have received from their external 3DSecure provider. Windcave does not recommend this but does support it for Rest API.
Message Category	Indicates the message category **NPA** = Non-payment authentication – a $0 authentication for a Validate transaction to load a card into an App (or similar) for rebilling and trigger a Challenge despite the low amount. It does not guarantee a Challenge, but it increases the **PA** = Payment authentication – the more typical 3DS authentication for a purchase transaction or pre-authorisation

DS Name	The name of the Scheme whose Directory Server routed the Authentication Request to the Issuer's Access Control Server.
ACS Transaction Id	Trace ID for the issuer's Access Control Server
DS Transaction Id	Trace ID for the scheme's Directory Server
Server Transaction Id	Trace ID for Windcave's own 3DS Server
3D Method Completed	Value here can be ignored for most purposes as completion of the "3DS Method" is not always required for the 3DS authentication. The "3DS Method" is a zero-pixel iFrame and is a requirement of the 3DS v2 specification (one of its main purposes is to fingerprint the card holder's device and browser details). The "3DS Method" may be part of but is not always critical to the 3DS authentication process. Y = Yes N = No U = Unknown
ACS Operator Id	Operator ID for issuer's Access Control Server (usually left blank)
ACS Reference Number	Identifies the Access Control Server by providing the reference of their EMV Letter Of Approval for 3DS v2
DS Reference Number	Identifies the Directory Server of the Scheme, and similar to above it is the official EMV reference authorising the use of that Directory Server for 3DS v2
3DSecure Version	The 3D Secure Version used for the transaction – Windcave uses the highest version supported in common for a given transaction by Windcave, the Scheme's Directory Server, the issuer's Access Control Server, and the card itself.
Authentication Type	Numeric Code – See Authentication Type Details (below) for more information
Authentication Type Details	Displays the Authentication type of the transaction. The Authentication type is determined by the issuer with their Access Control Server. Windcave have no control or visibility of this and we report the data we receive. Possible values may include: Dynamic = A challenge in the 3DS iFrame OOB (Out of Band) = A challenge outside of 3DS iframe e.g. bank app requests confirmation DeCoupled = Similar to OOB above, verifies and authenticates the customer's identity outside of their interaction with the website or app.
Authentication Method	Not currently in use
Transaction Status	Displays the status of the transaction using codes below: Y = Authenticated A = Authenticated via Stand In processing by the DS N = Not authenticated or account not verified U = Verification not confirmed R = Issuer is rejecting authorization C = this value is normally overwritten and so should not normally appear in Payline. If it is there, then it indicates there could be an issue with the messaging for that ACS. An issue of this type will usually be specific to the ACS and generally limited to 1 or a few transactions.
Transaction Status details	Displays further description from the transaction status code: Y = Authentication/Account Verification Successful A = Attempts Processing Performed (indicates it was Authenticated via Stand In processing by the Scheme's Directory Server) C = Challenge Required - this value is normally overwritten and so should not normally appear in PXMI. If it is there, then it indicates there could be an issue

	with the messaging for that ACS. An issue of this type will usually be specific to the ACS and generally limited to 1 or a few transactions.
Transaction Status Reason	Numeric Code – See Transaction Status Reason Details (below) for more information
Transaction Status Reason Details	Description of Transaction Status e.g. "Suspected Fraud", "Transaction not permitted to cardholder" etc
Challenge Cancellation Indicator	Numeric Code – See Challenge Cancellation Details (below) for more information
Challenge Cancellation Details	Description of Challenge Cancellation e.g. "Cardholder selected 'Cancel'", "Transaction Error" etc
Challenge indicator	Indicates the "challenge preference" that has been requested in the transaction. **Note**: the preference sent for a token-creating transaction would typically be 4 to increase the likelihood of Challenge. On the other hand, the preference for a one-off transaction would typically be 1. Codes used are **1, 2, 3** or **4**
Challenge indicator description	Displays the challenge indicator sent for this transaction: **1** = No preference **2** = No challenge requested (i.e. the preference is that there will NOT be a challenge) **3** = Challenge requested: Preference **4** = Challenge requested: Mandate
Cardholder Information	Shows the information shown to the cardholder (on the Windcave Result page for HPP integrations that display it, or available in the Rest API response for merchants to pull and display on their own result page) *Example for 3DS verification failure: "Please contact ABC bank on +64 1 234 567"*
Seconds for 3DSecure	Number of seconds used to complete 3D Secure authentication for the transaction
Seconds for challenge	Number of seconds used to complete the challenge part of the 3DS Secure authentication.

3.1 “Decline” Response Codes for 3DS

Please note, this is not an exhaustive list but covers the most common and some of the less common Response Codes that may be received when there is a decline related to 3DS

Response Code	Description
E0	E0 is retuned when Windcave fails to receive a response back from the ACS within the timeout period (determined by the ACS and out of Windcave’s control). Note that this can be up to 10 minutes or more.
EB	EB may indicate an issue involving currency or country code. Please raise to Windcave Support to investigate.
EC	EC may indicate, for a 3DS authentication with ReCoPreProc =3DEC, that there is an issue related to the Merchant Category Code. But if the ReCoPreProc has a different value, then this indicates it is unrelated to 3DS, and is more likely an issue with invalid CVC2/CVV2/CID code or similar – check “Acquirer” tab in transaction search for the Acquirer Response Text.
EN	EN is usually an issue at the issuer's ACS with that individual Authentication request (i.e. the individual transaction). It is not an issue related to the card itself, just that attempt. Please ask Card Holder to attempt again.
EP	EP indicates an error in the comms from the Scheme’s Directory Server to Windcave and Windcave are required by the 3DSv2 protocol to decline, regardless of the authentication result at the ACS. Please ask Card Holder to attempt again.
EV	EV indicates that a 3DS v2 authentication request was sent to the DC/ACS but did not pass authentication.
GU	GU indicates an unauthenticated transaction where 3DS v2 request was not sent i.e. the card BIN range does not support 3DS.
RC	RC with a 3Dsecure tab, then this generally means Card Holder has Chosen exit or cancel on ACS Challenge interface before really beginning the Challenge process. RC and there is no 3DSecure tab, then the card holder has cancelled on the Hosted Payment Page before clicking on the submit button so 3DS has not even been triggered
RY	RY usually indicates the Card Holder has cancelled after the Challenge has begun. Or it could be the ACS has had to cancel the Challenge for some reason. It could also be that the Challenge has failed in some way at the issuer's Access Control Server - Windcave has limited visibility, and no control, of this however sometimes it is indicated on 3DSecure tab by "Transaction Status Reason Details" = “ACS Technical issue”
01-99	A fully numeric response code (e.g. “51”, “54”, “05”) indicates that the transaction may have passed 3DS authentication successfully but the authorisation part of the transaction has then declined due to insufficient funds, incorrect expiry date, incorrect Cvv2 etc

4 Testing 3D Secure

3D Secure can be tested prior to rolling out.

Note: 3D Secure needs to be enabled on your REST username for testing – Please contact the Windcave sales to request this activation.

Once enabled on the REST user, the User Acceptance Testing (UAT) host can simulate the 3D Secure transaction process. This is triggered by using one of the below test cards at checkout:

Test Card Number	Expiry Date	CVC	3D Secure v2 Challenge Code
5588 8800 0007 7770	Any valid expiry date	Any 3 digits	123
4111 1111 1111 1111	12/25	Any 3 digits	Frictionless

5 FAQ's

Can I disable 3D Secure?

3D Secure may be mandatory for your eCommerce account; this is determined by the acquirer and any questions should be directed to your acquirer.

Although possible, it is not recommended to switch off 3DS as you will lose fraud liability coverage and will be liable for chargebacks. It is the decision of the acquirer on whether 3D Secure can be disabled for a merchant.
If accepted by the acquirer, you must:

1. Provide written confirmation of acceptance from the acquirer that 3DS will be disabled.
2. Provide written acceptance for full liability. The acquirer must provide this written confirmation direct to Windcave through the standard channels.

Can I disable 3D Secure for transactions under a certain amount (e.g. $80)?

Although possible, it is not recommended to switch off 3DS as you will lose fraud liability coverage and will be liable for chargebacks. It is the decision of the acquirer on whether 3D Secure can be disabled for a merchant.
If accepted by the acquirer, you must:

1. Have written confirmation of acceptance from the acquirer that 3DS will be disabled.
2. Have written acceptance for full liability for transactions under the specific amount before this change will be made. The acquirer must provide this specific confirmation direct to Windcave through the standard channels.

Why has a transaction has not processed through 3D Secure?

When viewing your transaction report, transactions which have not processed through 3DS will display as **Declined**. Through your Payline user, you can view the reason code / reason on the 3DS tab of the transaction.

If only a number of transactions are processing through 3DS, please check the type of transactions, e.g. some transaction types, i.e. MOTO, will not go through the 3DS process.

If multiple transactions are not processing through 3DS, please contact Windcave Support to ensure 3DS has been enabled.

Can I customize my 3D Secure page?

The 3D Secure user interface page is controlled by the individual issuer and cannot be customized by the merchant. However, custom integration is supported for merchant side 3D Secure - Please contact Windcave Support for more information.

Can I use 3D Secure for recurring payments or subscriptions?

Yes, for the initial transactions on set up, the transaction will be processed through 3D Secure. Future transactions will not be required to be processed through 3D Secure.

Please see section **3.2 3RI** of this guide for more information.

Are Gift Cards covered by 3D Secure?

Gift Cards may not be covered by 3DS, and some Gift Cards do not allow chargebacks.
User configurations set up by Windcave may allow Gift Cards to be skipped for 3DS.

Can I use an external MPI/3DS Server?

Windcave supports the use of an external MPI (Merchant Plugin Interface) / 3DS Server provided that all specified criteria and requirements are met. Please contact the Windcave Development support team for more information.

6 Contact Us

For further information or any queries, please contact Windcave Sales – sales@windcave.com

For help or assistance when using 3D Secure, please contact Windcave Support – Windcave | Contact

For any questions or issues while testing 3D Secure, please contact Windcave dev – devsupport@windcave.com and include your REST API username.