DirectLink with 3-D Secure

Table of contents

1. 3-D Secure v1.0

1.1 Introduction

1.2 3-D transaction flow via DirectLink

1.2.1 Extra request parameters

1.2.2 Additional return fields

1.2.3 Comments

2. 3-D Secure v2.0 (Available as of April 2019)

2.1 Introduction

2.2 3-D transaction flow via DirectLink

2.2.1 Extra request parameters

2.2.2 Additional return fields

2.2.3 Comments

1. 3-D Secure v1.0

1.1 Introduction

Version 1 of this guide will be unpublished by April 2019

The 3-D Secure protocol enables the cardholder to be identified during the purchasing process. The cardholder needs to be connected to the Internet during the identification process. Thus 3-D Secure does not work for call centre or recurring payments.

Visa has implemented the 3-D Secure protocol under the name Verified By Visa, MasterCard under the name SecureCode, JCB under the name J-Secure and American Express under the name SafeKey.

The principle of the integration of DirectLink with 3-D Secure is to initiate a payment in DirectLink mode and end it in e-Commerce mode if a cardholder authentication is requested.

This document describes the integration of the 3-D Secure protocol in DirectLink. For further information on DirectLink or e-Commerce, go to DirectLink or e-Commerce documentation.

1.2 3-D transaction flow via DirectLink

The transaction flow involves the following steps:

1. You send us a DirectLink request for the transaction, containing a number of additional parameters (cf. Extra request parameters).
2. Our system receives the card number in your request and checks online whether the card is registered in the VISA/MasterCard /JCB/AmEx directory (registered means that identification is possible for the card number, i.e. the card is a 3-D Secure card).
3. If the cardholder is registered, the answer to the DirectLink request contains a specific payment status and html code that has to be returned to the customer to start the identification process (cf. Additional return fields). The block of html code will automatically start the identification process between the cardholder (customer) and his issuing bank.
4. The cardholder identifies himself on the issuing bank's page.
5. Our system receives the identification response from the issuer.
6. If the identification was successful, our system will submit the actual financial transaction to the acquirer.
7. You receive the result of the global identification and online authorisation process via e-Commerce mode feedback channels.

Comments:

- Whether the liability shift applies or not depends on your acquirer contract. Therefore, we recommend you to check the terms and conditions with your acquirer.
- If the cardholder is not registered (in step 3), you will receive the standard DirectLink XML response containing the result of the online authorisation process.
- To receive the exact payment status/error codes (in step 7), you need to implement the online or offline post-sale feedback as described in the e-Commerce documentation.

1.2.1 Extra request parameters

Apart from the standard DirectLink parameters, you also need to send the following information:

Field	Description
FLAG3D	Fixed value: 'Y' Instructs our system to perform 3-D Secure identification if necessary.

For more information, go to Transaction Feedback.

1.2.2 Additional return fields

If the cardholder is not registered, the normal DirectLink response is returned. If the cardholder is registered, the following (additional) fields will be returned:

Field	Description
STATUS	New value: “46” (waiting for identification)
HTML_ANSWER	BASE64 encoded html code to be added in the html page returned to the customer. This tag is added as a child of the <ncresponse> global XML tag. The field HTML_Answer field contains HTML code that has to be added in the html page returned to the customer's browser. This code will automatically load the issuer bank identification page in a pop-up in the main window, depending on the WIN3DS parameter value. To avoid any interference between the html tags included in the content of the HTML_ANSWER XML tag, with the rest of the XML returned as a response to the DirectLink request, the HTML_ANSWER content is BASE64 encoded by our system before returning the response. Consequently, this must be BASE64 DEcoded before it is included in the html page sent to the cardholder.

1.2.3 Comments

Test Cards

You can use the following test cards to simulate a 3-D Secure registered card in our test environment:

Brand	Card number	Expiry date	Password
VISA	4000000000000002	Any date in the future	11111
MasterCard	5300000000000006	Any date in the future	11111
American Express	371449635311004	Any date in the future	11111

Incorrect identification

If a transaction is blocked due to incorrect identification, the transaction result will be:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2. 3-D Secure v2.0 (Available as of April 2019)

2.1 Introduction

In 2013, the European Commission published a proposal for the revised version of the Payment Services Directive, known as PSD2 to simplify payment processing and create the rules and regulations for payment services in the EU and there began the need for new version of 3-D Secure, v2.1.
The biggest change is that you, as a merchant, are asked to share more data: issuers are hungry for data points to improve the accuracy of their decision ultimately leading to a frictionless scenario, but you are the ones on the front line capturing the data.

The 3DS v2 approach to risk evaluation is more effective, but requires the entire ecosystem to change, allowing you to push the data through to the issuer.

2.2 3-D transaction flow via DirectLink

The transaction flow involves the following steps:

1. You send us a DirectLink request for the transaction, containing a number of additional parameters.

These parameter can be devised to three sets:

a. Mandatory parameters that need to be captured in the payment page where the cardholder is entering the card details.

Parameter	Description
browserAcceptHeader	Exact content of the HTTP accept headers as sent to the merchant from the Cardholder's browser.
browserColorDepth	Value representing the bit depth of the color palette for displaying images, in bits per pixel. Obtained from Cardholder browser using the screen color Depth property.
browserJavaEnabled	Boolean that represents the ability of the cardholder browser to execute Java. Value is returned from the navigator java Enabled property.
browserLanguage	Value representing the browser language as defined in IETF BCP47. Returned from navigator language property.
browserScreenHeight	Total height of the Cardholder's screen in pixels. Value is returned from the screen height property.
browserScreenWidth	Total width of the cardholder's screen in pixels. Value is returned from the screen width property.
browserTimeZone	Time difference between UTC time and the Cardholder browser local time, in minutes.
browserUserAgent	Exact content of the HTTP user-agent header.

Note: Please don't forget to calculate the parameters in your SHA signature.

b. Required additional parameters (cf. Extra request parameters)

c. Recommended parameters (list of parameters) that if sent will have a positive impact on transaction conversion rates. Based on the information contained in these parameters, a potential frictionless authentication flow may take place, where the cardholder won't need anymore to authenticate himself and therefore a quicker transaction completing is expected.

Our system receives the card number in your request and checks online whether the card is registered in the VISA/MasterCard/JCB/AmEx directory (registered means that identification is possible for the card number, i.e. the card is a 3-D Secure card).

2. Based on the schemes directory response and whether additional parameters in 1.c (Recommended parameters - list of parameters) above were provided (given if the cardholder is registered for 3-D Secure), two potential flows are expected if the cardholder is registered:

2.1. A frictionless flow: The cardholder doesn't physically need to authenticate themselves because the authentication took place in the background without their input. In this case, the liability shift is on the issuing bank.

2.2. A challenge flow: The cardholder needs to identify himself.

i. The answer to the DirectLink request contains a specific payment status and an html code that has to be returned to the customer to start the identification process (cf. Additional return fields). The block of html code will automatically start the identification process between the cardholder (customer) and his issuing bank.

ii. The cardholder identifies himself on the issuing bank’s page.

iii. Our system receives the identification response from the issuer.

iv. If the identification was successful, our system will submit the actual financial transaction to the acquirer.

3. You receive the result of the global identification and online authorisation process via e-Commerce mode feedback channels.

2.2.1 Extra request parameters

Apart from the standard DirectLink parameters, you also need to send the following information:

Field	Description
FLAG3D	Fixed value: ‘Y’ Instructs our system to perform 3-D Secure identification if necessary.
HTTP_ACCEPT	The Accept request header field in the cardholder browser, used to specify certain media types which are acceptable for the response. This value is used by the issuer to check if the cardholder browser is compatible with the issuer identification system. For example: Accept: */*
HTTP_USER_AGENT	The User-Agent request-header field in the cardholder browser, containing information about the user agent originating the request. This value is used by the issuer to check if the cardholder browser is compatible with the issuer identification system. For example: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
WIN3DS	Way to show the identification page to the customer. Possible values: • MAINW: display the identification page in the main window (default value). • POPUP: display the identification page in a pop-up window and return to the main window at the end. • POPIX: display the identification page in a pop-up window and remain in the pop-up window.
ACCEPTURL	URL of the webpage to show the customer when the payment is authorised. (or waiting to be authorised).
DECLINEURL	URL to which the customer is redirected if the maximum number of failed authorisation attempts has been reached (10 by default, but which can be changed in the Technical Information page, "Global transaction

Field	Description
	parameters" tab, "Payment retry" section).
EXCEPTIONURL	URL of the webpage to show the customer when the payment result is uncertain.
PARAMPLUS	Field to submit the miscellaneous parameters and their values that you wish to be returned in the post-sale request or final redirection.
COMPLUS	Field to submit a value you wish to be returned in the post-sale request or output.
LANGUAGE	Customer's language, for example: “en_US”
Optional	
TP	To change the layout of the "order_A3DS" page, you can send a template name/url with this parameter. (go to e-Commerce: Dynamic template).

For more information, go to Transaction Feedback.

2.2.2 Additional return fields

If the cardholder is not registered, the normal DirectLink response is returned. If the cardholder is registered, the following (additional) fields will be returned:

Field	Description
STATUS	New value: “46” (waiting for identification)
HTML_ANSWER	BASE64 encoded html code to be added in the html page returned to the customer. This tag is added as a child of the <ncresponse> global XML tag. The field HTML_Answer field contains HTML code that has to be added in the html page returned to the customer's browser. This code will automatically load the issuer bank identification page in a pop-up in the main window, depending on the WIN3DS parameter value. To avoid any interference between the html tags included in the content of the HTML_ANSWER XML tag, with the rest of the XML returned as a response to the DirectLink request, the HTML_ANSWER content is BASE64 encoded by our system before returning the response. Consequently, this must be BASE64 DEcoded before it is included in the html page sent to the cardholder.

2.2.3 Comments

Test Cards

You can use the following test card to simulate a 3-D Secure registered card in our test environment:

Frictionless Flow		
Brand	Card number	Expiry date

Frictionless Flow		
VISA	4186455175836497	Any date in the future
Mastercard	5137009801943438	Any date in the future
American Express	375418081197346	Any date in the future

Challenge Flow		
Brand	Card number	Expiry date
VISA	4874970686672022	Any date in the future
Mastercard	5130257474533310	Any date in the future
American Express	379764422997381	Any date in the future

Incorrect identification

If a transaction is blocked due to incorrect identification, the transaction result will be:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134