Paylane 3-D Secure Guide

For PayLane Merchants

Created by: PayLane IT Crew / 2007-11-28

Last modification: 2011-08-12

Saved by: Jan Makulec

Table of contents

1. What is 3-D Secure

3-D Secure is a technical solution that allows authentication of cardholders performing internet (e-commerce) transactions. It provides additional security for both cardholders and merchants by requiring cardholders to authenticate and approve transactions on the websites of their banks. Various authentication solutions (like passwords, SMS codes, one time PINs, token OTC) may be used, depending on the card issuer (cardholder's bank).

3-D Secure solution is offered by Visa under the name of *Verified by Visa*, by MasterCard under the name of *MasterCard SecureCode*. Other card schemes have also adopted 3-D Secure (like JCB *J/Secure*) or are preparing to offer it.

2. Benefits of 3-D Secure

3-D Secure brings a number of very strong benefits for banks, cardholders, acquirers and merchants.

Banks (issuers of cards) are protected against fraudulent transactions performed by people who obtained card details of bank's cardholders. The cardholder is thus protected against card details theft that can result in fraudulent charges using the card, even if it is in the possession of the cardholder.

Acquirers and merchants are protected against chargebacks that result from fraudulent transactions. If transactions are performed using 3-D Secure issuing banks (on the basis of obtaining additional authorization from the cardholder) are not allowed to issue chargebacks with reason codes of fraud or lack of authorization origin.

To encourage banks to implement 3-D Secure for their customers card schemes (both Visa and MasterCard) have set a rule that the party which does NOT implement 3-D Secure (when other parties do) takes the responsibility in case of a dispute. This rule includes card issuers (e.g. banks). What is very important in this protection scheme is the fact that even if the issuing bank does not participate in 3-D Secure and transaction is not authenticated by 3-D Secure mechanisms the merchant who charges the cardholder (performing the 3-D Secure pre-check of the card) is still fully protected against fraud/lack of authorization chargebacks.

What is also worth mentioning is the fact that cardholders' confidence in the merchant's payment collection (and Internet payments in general) is increased when transactions are performed with 3-D Secure. Cardholder that has

3-D Secure enabled for their card will most likely choose merchants that have implemented 3-D Secure, to achieve additional protection of their card details. This alone gives the opportunity to increase merchant's customer base and thus brings more sales and money.

3. How 3-D Secure works?

3-D Secure, as the name suggests, engages three sides (or domains) in the authentication process. The three domains are:

- Acquirer Domain (the commerce)
- Issuer Domain (bank issuing the credit card)
- Interoperability Domain (credit card organization)

The three parties communicate with each other, passing information required to authenticate the cardholder and authorize the payment.

4. 3-D Secure implementation at PayLane

PayLane provides services which significantly simplify 3-D Secure Authentication process from merchant's point of view. All acquirer-issuer communication is handled by PayLane. Merchants are only required to:

1. Initiate the 3-D Secure Authentication
2. Redirect the customer to PayLane page
3. Handle incoming postback message from PayLane
4. Perform or decline the sale, depending on authentication result

3-D Secure Authentication is initiated by merchant who checks if the card is enrolled in 3-D Secure (is eligible for 3-D Secure Authentication). PayLane provides an appropriate method in PayLane Direct web service to facilitate this check (see 4.2).

Depending on the check, 2 different scenarios may occur:

1. Card is not eligible for 3-D Secure Authentication
   In this scenario, merchant stops 3-D Secure Authentication process and performs ordinary sale (see 4.4).
2. Card is eligible for 3-D Secure

Merchant proceeds with 3-D Secure Authentication (see 4.3). Depending on authentication result, sale is performed or declined (see 4.4).

4.1. Requirements

Using PayLane's 3-D Secure implementation has following technical requirements:

- Web services integration
- Ability to redirect users to page on another server
- Ability to handle POST requests

4.2. PayLane Direct

4.2.1. checkCard3dSecureEnrollment

When the customer supplies his credit card data and confirms the order, merchant initiates 3-D Secure transaction by checking cardholder participation in 3-D Secure using `checkCard3dSecureEnrollment` method.

Detailed information about `checkCard3dSecureEnrollment` method, including list of parameters and return values, can be found in *PayLane Direct System* document, available from PayLane.

4.3. PayLane Secure

4.3.1. Redirecting to PayLane Secure

After successful enrollment check using PayLane Direct, it is required to redirect user to PayLane Secure webpage

(`paylane_url` returned by `checkCard3dSecureEnrollment` method).

This will initiate the process of 3-D Secure authentication. User will be redirected to his issuing bank page and asked to provide authentication data (depends on the issuer, usually password).

After that, PayLane will check the answer from bank and return the result to merchant page (`back_url`) using *postback* mechanism (see below).

Redirecting user to another web page may be handled in a number of ways:

- An ordinary link (`<a href=`…) may be presented with appropriate label (e.g. "Continue payment"). User clicks a link and is being redirected to PayLane Secure pages.
- Merchant application redirects user automatically by setting HTTP `Location` header. Webpage-generation solutions such as PHP offer appropriate functions to facilitate setting HTTP headers.
- A form, either visible, with labeled submit button ("Continue payment") or hidden, auto-submitted using Javascript.

We recommend displaying clear message about redirection to another page. This prevents users from becoming confused.

PayLane Secure pages were constructed according to all standards and recommendations from card organizations, with usability and ease of use in mind. This includes frameset form, placement of elements, information boxes etc.

4.3.2 Postback

While performing card enrollment check, merchant provides an URL where he wishes the results of 3-D Secure Authentication to be sent later (`back_url`). This URL should contain a webpage/script capable of receiving and processing HTTP POST requests from PayLane (postback). All sent POST fields are described in detail below.

Postback format

Field name	**Data type**	**Description**
`id_secure3d_auth`	integer (10)	ID of 3-D Secure Authentication. This ID is common to all 3-D Secure operations.
`correct`	integer (1)	„0" means failure, „1" means successful 3-D Secure Authentication. In case of failure, additional information is provided in `error_code` and `error_text` fields.
`error_code`	integer (3)	Error code. Empty if no error occurred. Error codes are always 3-digits long. For complete list of errors see the table below.
`error_text`	string	Textual description of error. Empty if no error occurred.

Postback error codes

Error code	Error text
501	Internal server error. Please try again later.
504	Service 3D Secure Authentication not accessible for this merchant account.
505	This merchant account is inactive.
721	Secure3d ID is not valid.
722	Authentication response message is not valid.
723	Secure3d ID not found.
724	3D Secure authentication was completed at [datetime] UTC.

4.4 Performing the sale

Sale should be performed when card was found not eligible for 3-D Secure Authentication or when authentication was performed and resulted in success.

Regardless of the situation it is required to provide `id_secure3d_auth` when performing `multiSale` using PayLane Direct.

That leaves a trail proving that merchant performed the sale "with 3-D Secure" even if card was not enrolled in 3-D Secure. It is important information in case of a dispute (chargeback).

5. Testing the implementation

To confirm compliance with 3-D Secure, there are several tests cases which must be executed. Test cases have a form of test credit card numbers. These test cases were prepared by Visa and contain all possible situations which may occur during 3-D Secure Authentication process.

Each test case is complemented with expected merchant reaction. For example: after successful authentication merchant is expected to proceed with the sale. Failed authentication should stop the process.

All cases are described shortly below:

No.	Test card number	Description	Expected reaction
3	4012001036275556	No response from Visa Directory Server	
4	4012001038443335	Cardholder not participating	Perform sale w/o 3-D Secure Authentication
5	4012001038488884	Unable to verify enrollment	
6	4012001036298889	Invalid response from Directory Server	
7	4012001036853337	Invalid ACS digital signature	
8	4012001036983332	Expired ACS signing certificate	
9	4012001037141112	Successful authentication via a 16-digit PAN	Perform sale
10	4005559876540	Successful Authentication via a 13-digit PAN	Perform sale
12	4012001037167778	Successful merchant attempt via 16-digit PAN	Perform sale
13	4012001037461114	Authentication Failure	Decline sale
14	4012001037484447	Authentication not available	
15	4012001037490006	Invalid Payer Authentication Response	

Note on cases: when it is impossible to ascertain if card participates in 3-D Secure (e.g. due to technical reasons on bank/card organizations side) it is up to merchant to decide whether to decline the sale or perform it without 3-D Secure Authentication. If merchant decides to perform the sale anyway, it is important to supply 3-D Secure Auth ID – it is a proof that the procedure was maintained and protects the merchant in case of dispute.

Note: PayLane system responds correctly to all test cases described above. Test accounts that are provided by PayLane to ease the integration process may be used to test 3-D Secure compliance.

Also please note that the test card numbers stated above vary depending on the acquiring bank. If in any doubts, please contact us directly to learn more.

Any questions? Please contact us:

Phone numbers:
UK phone: +44 2030 514075
Polish phone: +48 58 732 21 11
Fax: +48 58 668 31 46

E-mails:
General: info@paylane.com,
Sales: sales@paylane.com,
For Partners: partners@paylane.com,
Merchant Support: support@paylane.com

United Kingdom:
PayLane UK Ltd
46 Station Road
North Harrow, Middlesex HA2 7SE

Company No. 6493144
VAT ID GB991899439

Poland:
PayLane Sp. z o.o.
Arkonska Business Center
ul. Arkonska 6/A3, 80–387 Gdansk

NIP: 586-214-10-89
Regon: 220010531
KRS: 0000227278
Kapitał zakładowy: 60.000 PLN

Visit and follow us on:
Facebook: http://www.facebook.com/PayLane,
Twitter: http://twitter.com/PayLane,
LinkedIn: http://linkedin.com/company/paylane.