

TECHNICAL SPECIFICATIONS

Strong Customer Authentication (3D Secure)



Euronet Merchant Services Payment Institution Single Member S.A.
1 Sachtouri & Poseidonos Ave., 176 74 Kallithea, Athens, Greece
Authorised as a Payment Institution by the Bank of Greece under Law 4537/2018

www.epayworldwide.gr



History of Changes

Date	Version	Changes
03/06/2019	1.0	Original version
10/07/2019	1.0.1	Change in the possible values of the RecurringInd parameter and various improvements
30/07/2019	1.0.2	<ul style="list-style-type: none">Section 4: New parameters added to the request message (shipping address data, billing address data, cardholder data)Addition of Section 5 (3D-Secure Wrapper Test Cases)
23/09/2019	1.0.3	<ul style="list-style-type: none"><UserAgent> parameter is now set to (M)andatory and <RecurPurchaseDate>, <RecurFreq>, <RecurEnd> parameters to (C)onditionalDescription and Type enrichment of the following parameters: BillAddrCity, BillAddrCountry, BillAddrLine1, BillAddrLine2, BillAddrLine3, BillAddrPostCode, BillAddrState, ShipAddrCity, ShipAddrCountry, ShipAddrLine1, ShipAddrLine2, ShipAddrLine3, ShipAddrPostCode, ShipAddrState, CardholderName, Email, HomePhone, MobilePhone
02/01/2020	1.0.4	<p>Description and format enrichment of the following parameters:</p> <ul style="list-style-type: none">o Descriptiono BrowserIPo Navigator_languageo Navigator_javaEnabledo Navigator_jsEnabledo Screen_colorDeptho Screen_heighto Screen_widtho TimezoneOffseto UserAgento BrowserAccept
20/07/2020	1.0.5	Section 4: Update of the parameters description: BillAddrCountry, BillAddrLine1, BillAddrPostCode, BillAddrState, ShipAddrCity, ShipAddrCountry, ShipAddrLine1, ShipAddrPostCode, ShipAddrState, CardholderName, Email, HomePhone, MobilePhone, WorkPhone
26/10/2020	1.0.6	Section 4: Update of the parameters description to Ticketing Web Service: BillAddrState, ShipAddrState, HomePhone, MobilePhone, WorkPhone



History of Changes

Date	Date	Date
08/02/2021	1.0.7	Section 4: Update of the parameters description: Navigator_language, Description
26/07/2021	1.0.8	Section 5: Update of test cases with new cards
01/03/2022	2.0	Service rebranding to epay eCommerce
20/09/2023	2.1	Addition of the parameter "ChallengeInd" and change to the possible values of the parameter "MessageCategory"



Contents

1.	Introduction	4
2.	General Architecture	5
3.	Details for the Creation of a Test Account	7
4.	Strong Customer Authentication through 3D-Secure Wrapper	8
5.	3D-Secure Wrapper Test Cases	27



1. Introduction

This document describes the development required for the strong authentication of a card holder debiting their card on a website. This is the so-called “3D Secure Version 2” or “EMV 3D-Secure” process supported through the “Visa Secure” and “Mastercard Identity Check” services; it has to be executed prior to any card debiting attempt initiated by the holder on a company’s website.

More specifically, where a company uses “Web Service” for card debits (see relevant Euronet Merchant Services specification) made by card holders through the company’s website, the process described herein should be implemented.

3D-Secure requires the card details (number and expiry date) which are either entered by the user on the company’s website, or alternative the company sends a “token” obtained at an earlier stage using the Euronet Merchant Services Tokenization service (see relevant Euronet Merchant Services specifications).

In the sections below detailed information is provided on the following:

- **Section 2 → General Architecture:**
Description of the 3D-Secure general architecture.
- **Section 3 → Details on the creation of a Test Account:**
The details required to be sent to Euronet Merchant Services in order to create a *test account* and perform test transactions.
- **Section 4 → Strong Customer Authentication through 3D-Secure Wrapper:**
Description of the 3D-Secure process and of the calls required for strong customer authentication.
- **Section 5 → 3D-Secure Wrapper Test Cases:**
Description of test cases to be executed in order to check the 3D Secure process

2. General Architecture

The following diagrams show the general architecture for executing a transaction following the 3D Secure process. There are two alternatives:

A) Use of the card's actual details

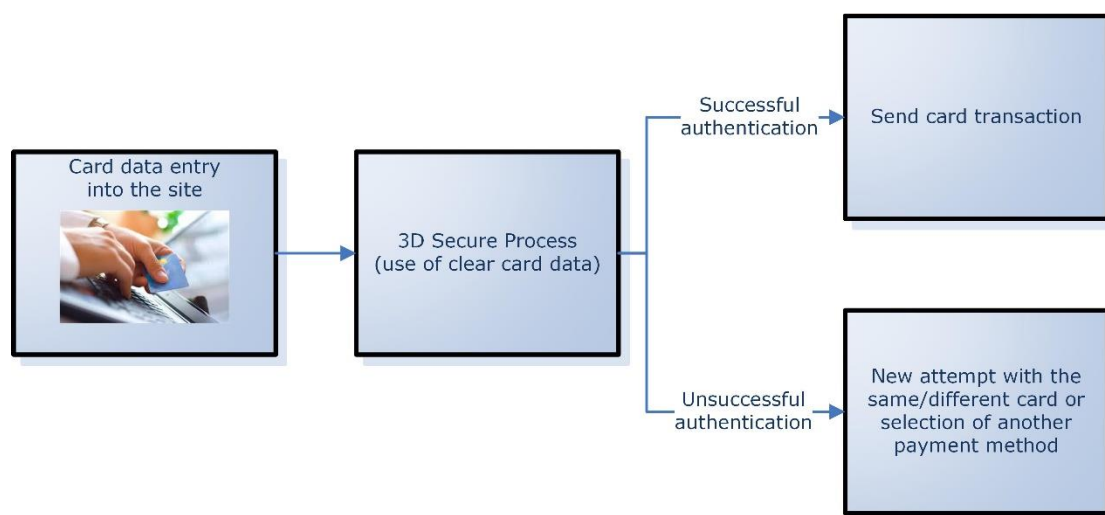


Diagram 2.1: General architecture – use of clear card

As shown in the above diagram:

1. The user enters their card details on the company's website (card number, expiry date, CVV2)
2. 3D Secure is executed; the card details (number and expiry date - see next section) are included
3. Provided the process is successfully completed, the sale or pre-authorisation transaction is sent or the user is prompted to try again using the same or a different card.

B) Use of a token

In this case the Euronet Merchant Services "Tokenization" service has been used and the company has stored a "token" that corresponds to a card, the details of which have been stored in Euronet Merchant Services. The 3D Secure process is thus executed, using the token value and not the actual card details.

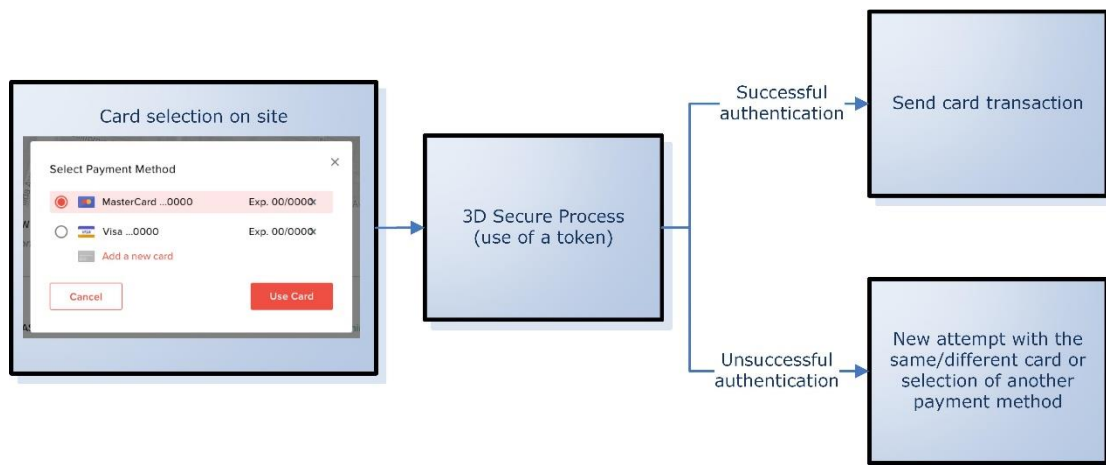


Diagram1.2: General architecture – use of a token

As shown in the above diagram:

1. The user selects the card to be debited from a list of masked card details. The company only knows the token and the masked card details acquired through the Euronet Merchant Services "Tokenization" service.
2. The 3D Secure process is thus executed using the token, not the actual card details (see next section).
3. Provided the process is successfully completed, the sale or pre-authorisation transaction is sent or the user is prompted to try again using the same or a different card.



3. Details for the Creation of a Test Account

The information to be sent to Euronet Merchant Services in order for the necessary technical information to be provided (*test account*) for test transactions is as follows (all is required):

- **Details of the technical manager**
 - Name of the technical manager
 - Telephone of the technical manager
 - Email address of the technical manager
 - Company where the technical manager is employed
- **Details of the merchant owning the system:**
 - Distinctive Title of the merchant owning the system
 - Tax Registration Number of the merchant owning the system
 - Domain name of the merchant's live site
- **Technical data:**
 - **IP address**: IP address of the server from which calls will be made

The *test account* details provided by Euronet Merchant Services, once the above information is sent, are as follows:

- AcquirerID
- MerchantID
- User
- Password

Information on the usefulness of the above details is provided in the following sections.



4. Strong Customer Authentication through 3D-Secure Wrapper

The 3D Secure process should precede any sale or pre-authorisation transaction made by the card holder on the company's website. This process, however, is not called prior to any refund or settlement transactions.

The process is executed by calling the Web Service ("3D-Secure Wrapper") presented below. The URL to which calls are sent is:



<https://paycenter.piraeusbank.gr/services/Wrapper3DSecure.aspx>





Caution!

- The amount and currency used in the 3D Secure process should be identical to those in the sale or pre-authorisation transaction that follows.
- The response timeout is 60 sec.
- The Web Service call should be made through the Server. **Cross-origin HTTP requests via scripts are not allowed.**

The Web Service request and response parameters are described below, followed by a diagram of the algorithm to be used. If there is an indicator **M (Mandatory)**, the parameter must have a value.

REQUEST PARAMETERS		
Parameter name	Description	Type
AcquirerID (M)	The acquirer id. Provided by Euronet Merchant Services.	String (up to 5 characters)
MerchantID (M)	The merchant ID. Provided by Euronet Merchant Services.	Integer
User (M)	User name. Provided by Euronet Merchant Services.	String (up to 50 characters)
Password (M)	User password <u>encrypted using the MD5 hashing algorithm</u> . Provided by Euronet Merchant Services (in non-encrypted form).	String (up to 50 characters)
RequestType (M)	Request type (see diagram below). Possible values: <ul style="list-style-type: none">▪ EnrollmentRequestInit▪ EnrollmentRequestContinue▪ PAREsValidationRequest	String

MerchantReference (M)	<p>Unique reference code of the transaction, used in all 3D-Secure Wrapper and Transaction Web Service requests, regarding the particular transaction.</p> <ul style="list-style-type: none"> “MerchantReference” accepts Greek and Latin uppercase and lowercase alphanumeric characters, spaces and the following special characters: /:_().,+ - Generated by the company’s system, it is a unique identifier of the transaction. <u>Even if the transaction is not approved, it is not possible to use the same MerchantReference value in the next attempt.</u> 	String (up to 50 characters)
PurchAmount	The transaction amount with an integer value formed by removing the decimal separator (e.g. for EUR 100.25 the value 10025 should be sent). A value is required here when RequestType=EnrollmentRequestInit and messageCategory ≠02 (see description of the messageCategory parameter below).	Long
Exponent	Number of decimals in the amount. A value is required where purchAmount should have a value.	Integer
Currency	The ISO 4217 currency code of the transaction (3-digit numerical value). E.g. 978 for the Euro. A value is required where purchAmount should have a value.	Integer
Description	<p>Description of the purchase (brief description of the products/service involved in the purchase). Maximum length is 125 characters.</p> <p>The parameter accepts Latin uppercase and lowercase alphanumeric characters, spaces and the following special characters: /:_().,+ -</p> <div>  Note: Most Issuers do not display this description. </div>	String (up to 125 characters)
Pan	Card number or token value. A value is required when RequestType=EnrollmentRequestInit.	String (up to 19 numeric digits)
Expiry	<p>The card expiry date in YYMM format.</p> <ul style="list-style-type: none"> When RequestType=EnrollmentRequestInit and the pan contains an actual card number, a value is required in expiry. 	String (4 digits)

	<ul style="list-style-type: none"> When RequestType=EnrollmentRequestInit and the pan contains an epay eCommercetoken, no value is sent. 	
MD	The content of this parameter will be returned through POST in the company's termURL (see parameter description below). It should contain ASCII characters numbered from 0x20 to 0x7E, excluding "<" and ">". If additional data is required, Base64 encoding is necessary. The final size of the parameter should be up to 254 bytes. It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (up to 254 bytes)
Lang	ISO 639-1 language code corresponding to the language used on the company's website. E.g. el for Greek, en for English. It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (2 characters)
TermURL	The company's URL to which the user is returned following the authentication process in their bank (see diagram below). A value is required when RequestType=EnrollmentRequestInit.	String
Pares	It may be assigned a value when RequestType= PAREsValidationRequest. If the company received a value in the pares parameter when returning to the TermURL, this value is sent here.	String
Cres	It may be assigned a value when RequestType= PAREsValidationRequest. If the company received a value in cres parameter when returning to the TermURL, this value is sent here.	String
ThreeDSMethodNotificationURL	<p>The company's URL called under certain conditions during the 3D Secure process, in order for a subsequent call to 3D Secure wrapper to follow (see diagram below). A value is required when RequestType=EnrollmentRequestInit.</p> <div>  Caution! It is recommended that its value be generated dynamically and the MerchantReference value is included as a parameter (in the query string), so that there is a unique element to establish the link to the transaction upon return (e.g. https://www.test.gr?ref=abcd where 'abcd' is the </div>	String

	MerchantReference value of the transaction)	
ThreeDSCompInd	<p>A value is sent only when RequestType=EnrollmentRequestContinue (see diagram below).</p> <ul style="list-style-type: none"> ▪ "Y": Sent only when the wrapper call with RequestType=EnrollmentRequestContinue follows the company's threeDSMethodNotificationURL call. ▪ "N": Sent only when the wrapper call with RequestType=EnrollmentRequestContinue is made without prior call of the company's threeDSMethodNotificationURL (TIMEOUT) 	String
PanMode	For future use; no value is sent.	String
MessageCategory	The value " Payment " is always sent and only when RequestType=EnrollmentRequestInit.	String
ChallengeWindowSize	<p>Desirable window size for card holder authentication. Potential values:</p> <ul style="list-style-type: none"> ▪ W250H400: 250x400 ▪ W390H400: 390x400 ▪ W500H600: 500x600 ▪ W600H400: 600x400 ▪ FullScreen: Full screen <p>A value is required only when RequestType=EnrollmentRequestInit.</p>	String
BrowserIP	<p>The browser's IP. Values accepted IPv4 e.g. 1.12.123.255 or IPv6 e.g. 2011:0db8:85a3:0101:0101:8a2e:0370:7334</p> <p>A value is required only when RequestType=EnrollmentRequestInit.</p>	String
Navigator_language	<p>Value representing the browser language as defined in IETF BCP47. Obtained from navigator.language HTML property.</p> <p>A value is required only when RequestType=EnrollmentRequestInit.</p>	String (up to 10 characters)
Navigator_javaEnabled	<p>Value representing the ability of the cardholder browser to execute Java. Obtained from the navigator.javaEnabled property. Accepted values: true/false</p> <p>A value is required only when RequestType=EnrollmentRequestInit.</p>	String
Navigator_jsEnabled	<p>Value representing the ability of the cardholder browser to execute JavaScript. Accepted values: true/false</p> <p>A value is required only when RequestType=EnrollmentRequestInit.</p>	String

Screen_colorDepth	Value representing the bit depth of the color palette for displaying images, in bits per pixel. Obtained from Cardholder browser using the screen.colorDepth property. Accepted values: 1, 4, 8, 15, 16, 24, 32, 48. A value is required only when RequestType=EnrollmentRequestInit.	String (1-2 characters)
Screen_height	Total height of the Cardholder's screen in pixels. Obtained from the screen.height property. A value is required only when RequestType=EnrollmentRequestInit.	String (1-6 numeric characters)
Screen_width	Total width of the cardholder's screen in pixels. Obtained from the screen.width property. A value is required only when RequestType=EnrollmentRequestInit.	String (1-6 numeric characters)
TimezoneOffset	Time-zone offset in minutes between UTC and the cardholder browser local time. Note that the offset is positive if the local time zone is behind UTC and negative if it is ahead. Value is returned from the getTimezoneOffset() method. Examples: If UTC -5 hours, TimezoneOffset=300 or +300. If UTC +5 hours, TimezoneOffset=-300. A value is required only when RequestType=EnrollmentRequestInit.	String (1-5 characters)
UserAgent	Exact content of the HTTP user-agent header. If the total length of the User-Agent sent by the browser exceeds 2048 characters, the system truncates the excess portion. A value is required only when RequestType=EnrollmentRequestInit.	String (max. 2048 characters)
BrowserAccept	Value of the accept header field (response types acceptable by the browser). If the total length of the accept header sent by the browser exceeds 2048 characters, the system truncates the excess portion. A value is required only when RequestType=EnrollmentRequestInit.	String (max. 2048 characters)
BillAddrCity	Billing address city The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (up to 50 characters)

BillAddrCountry	ISO 3166-1 numeric country code, corresponding to Billing address country. E.g. 300 for Greece. It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (3 numeric digits)
BillAddrLine1	Additional line 1 of the billing address The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (up to 50 characters)
BillAddrLine2	Additional line 2 of the billing address The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (up to 50 characters)
BillAddrLine3	Additional line 3 of the billing address The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (up to 50 characters)
BillAddrPostCode	Post code of the billing address The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.	String (up to 16 characters)
BillAddrState	ISO 3166-2 country subdivision code without the country name code, corresponding to Billing address State (if applicable). Below are the values for the administrative regions in Greece A Eastern Macedonia and Thrace B Central Macedonia C Western Macedonia D Epirus E Thessaly F Ionian Islands G Western Greece H Central Greece I Attica J Peloponnese	String (max. 3 characters)



	<p>K Northern Aegean L Southern Aegean M Crete</p> <p>It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	
ShipAddrCity	<p>Shipping address city</p> <p>The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (up to 50 characters)
ShipAddrCountry	<p>ISO 3166-1 numeric country code, corresponding to Shipping address country. E.g. 300 for Greece. It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (3 numeric digits)
ShipAddrLine1	<p>Additional line 1 of the shipping address</p> <p>The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (up to 50 characters)
ShipAddrLine2	<p>Additional line 2 of the shipping address</p> <p>The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit</p>	String (up to 50 characters)
ShipAddrLine3	<p>Additional line 3 of the shipping address</p> <p>The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit</p>	String (up to 50 characters)
ShipAddrPostCode	<p>Post code of the shipping address</p> <p>The parameter contains only Greek or Latin lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (up to 16 characters)

ShipAddrState	<p>ISO 3166-2 country subdivision code without the country name code, corresponding to Shipping address State (if applicable).</p> <p>Below are the values for the administrative regions in Greece A Eastern Macedonia and Thrace B Central Macedonia C Western Macedonia D Epirus E Thessaly F Ionian Islands G Western Greece H Central Greece I Attica J Peloponnese K Northern Aegean L Southern Aegean M Crete</p> <p>It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (max. 3 characters)
CardholderName	<p>Name of the card holder</p> <p>The parameter contains only Latin (not Greek) lowercase & uppercase alphanumeric characters, space, or the following special characters /:_().,+ - It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (2-45 characters)
Email	<p>E-mail of the card holder</p> <p>The parameter shall meet requirements of Section 3.4 of IETF RFC 5322. It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (up to 254 characters)
HomePhone	<p>Home phone number of the card holder, in the following format country code number dash subscriber phone number, and length up to 3 digits dash up to 15 digits. e.g. 30-2103288000 for Greece</p> <p>List of assigned country codes in the following document. https://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_763.pdf</p> <p>It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	String (up to 19 characters)
MobilePhone	<p>Mobile number of the card holder, in the following format country code number</p>	String (up to 19 characters)

	<p>dash subscriber phone number, and length up to 3 digits dash up to 15 digits. e.g. 30-6972222222 for Greece</p> <p>List of assigned country codes in the following document. https://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_763.pdf</p> <p>It may be assigned a value only when RequestType=EnrollmentRequestInit.</p>	
WorkPhone	<p>Work phone number of the card holder, in the following format country code number dash subscriber phone number, and length up to 3 digits dash up to 15 digits. e.g. 30-2103288000 for Greece</p> <p>List of assigned country codes in the following document. https://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_763.pdf</p>	String (up to 19 characters)
RecurringInd	<p>It is only used in recurring transactions. It concerns the first transaction of a recurring payment (i.e. standing order), performed online by the card holder and is, therefore, preceded by the 3d-secure process. It is only sent when RequestType= EnrollmentRequestInit. Potential values:</p> <ul style="list-style-type: none"> ▪ R, for recurring transactions (transactions performed at regular intervals) ▪ C, for unscheduled recurring transactions (transactions performed at irregular intervals) <p><u>Unless the process concerns a recurring transaction, the parameter is omitted.</u></p>	String (1 character)
RecurPurchaseDate	<p>In recurring transactions, it contains the date of the first recurring transaction in YYYYMMDDHHMMSS format. It may only have a value when RequestType=EnrollmentRequestInit and provided that the RecurringInd has a value, too.</p>	String (14 characters)
RecurFreq	<p>In recurring transactions, it contains the recurrence frequency of the transaction (integer number of days). It may only have a value when RequestType=EnrollmentRequestInit and provided that the RecurringInd has a value, too.</p>	String (max. 4 characters)

RecurEnd	In recurring transactions (i.e. when RecurringInd=R or C), it contains the expiry date of the recurring debit in YYYYMMDD format. It may only have a value when RequestType=EnrollmentRequestInit and provided that the RecurringInd has a value, too.	String(8 characters)
ChallengeInd	The parameter is only used for transactions with card verification and use of strong authentication without charging the card. In this case the value to be sent is: 04	String

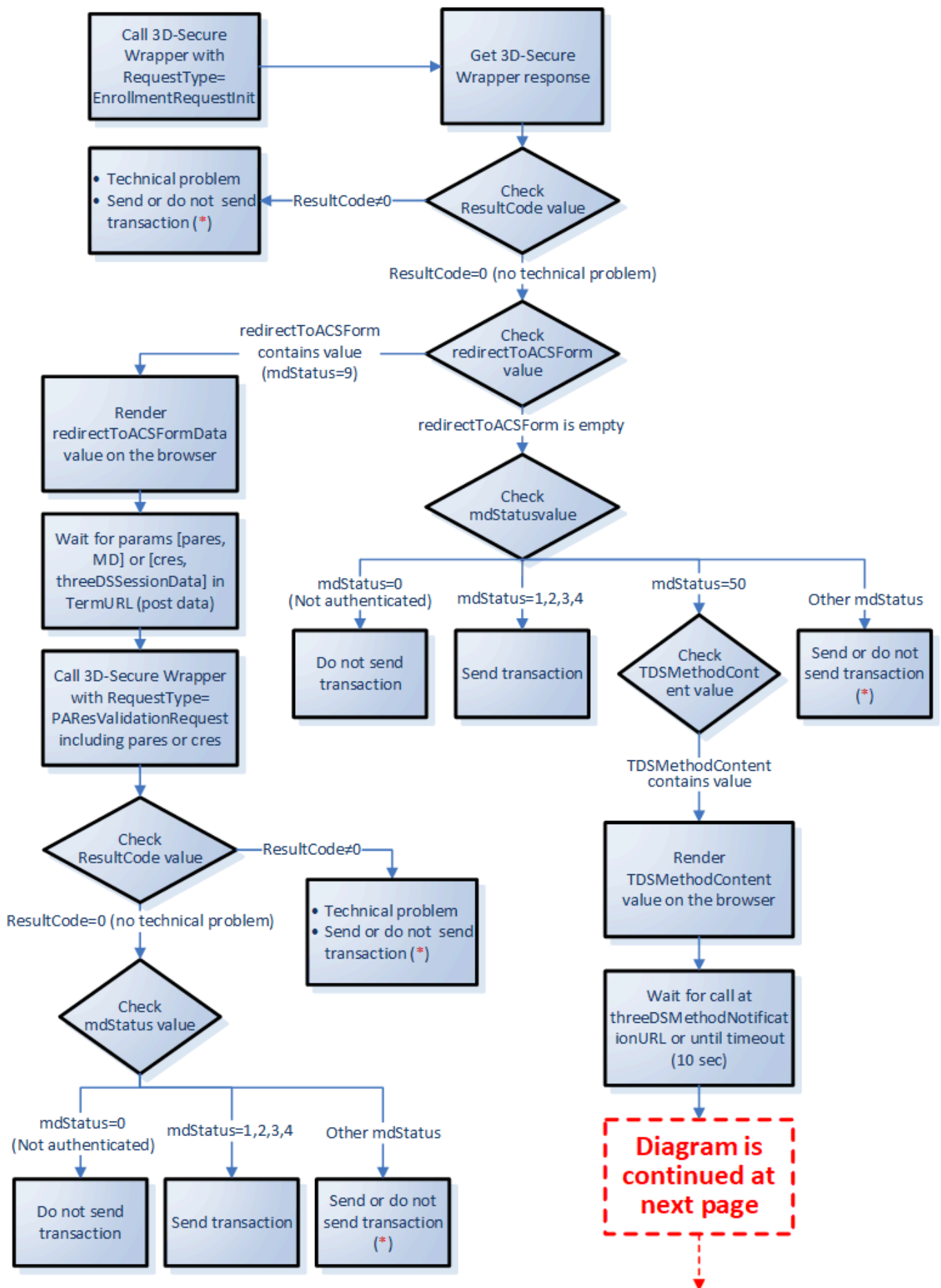
The parameters sent with the response are the following:

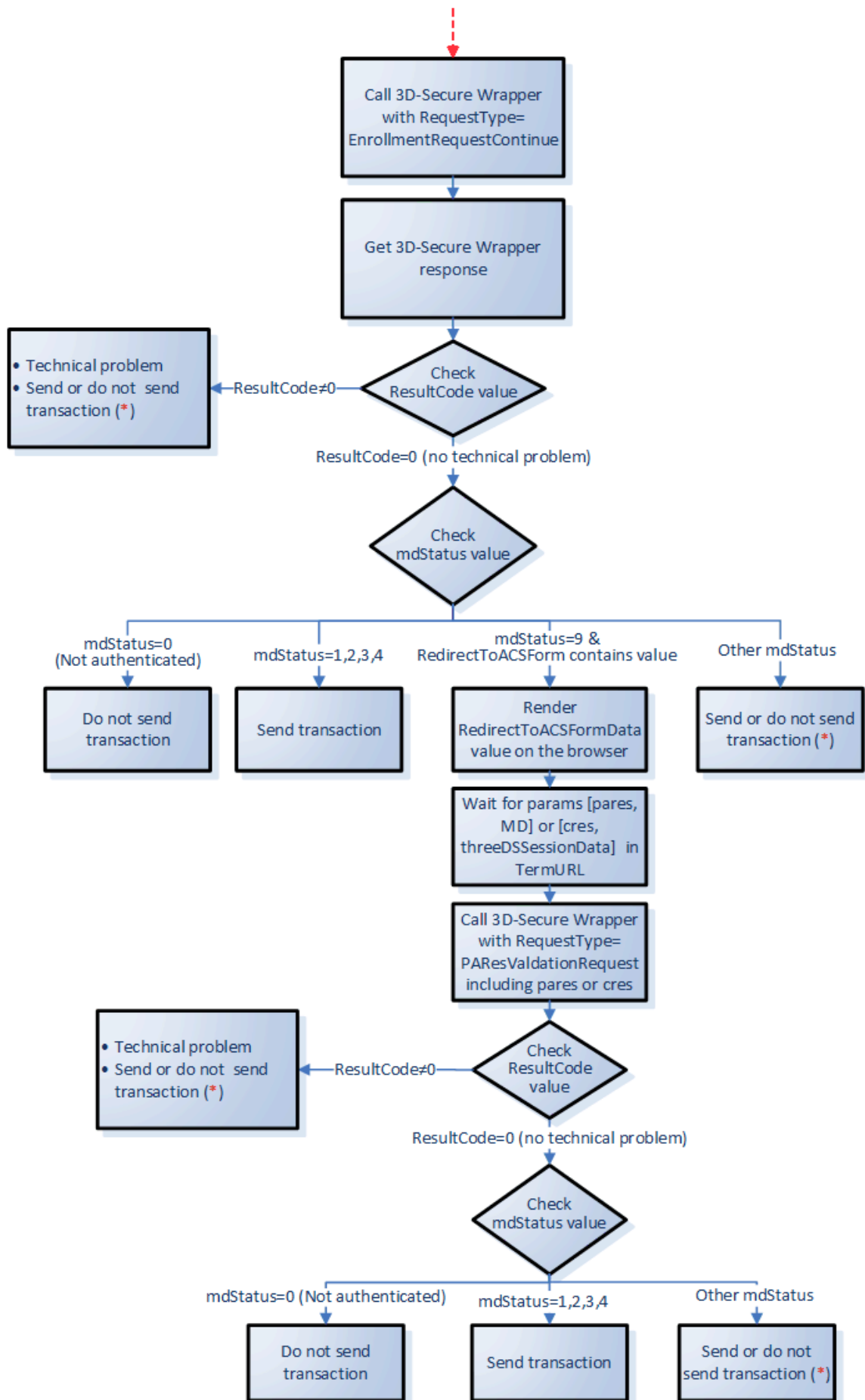
RESPONSE PARAMETERS		
Parameter name	Description	Type
AcquirerID (M)	The AcquirerID value sent with the request	String
MerchantID (M)	The MerchantID value sent with the request	Integer
User (M)	The User value sent with the request	String (up to 50 characters)
RequestType (M)	The RequestType value sent with the request	String
ResultCode (M)	<p>The request result code indicating whether a technical issue occurred during the call. Specifically:</p> <ul style="list-style-type: none"> ➡ Value = 0: No issue occurred and the remaining parameters have information on the 3D Secure process carried out. ➡ Value ≠ 0: There was an issue with the request data or another type of technical issue. The «ResultDescription» parameter contains the problem description. 	Integer
ResultDescription (M)	<p>The description corresponding to the «ResultCode» parameter value.</p> <div>  Note: This information is not recommended to be displayed to the user. </div>	String (up to 1024 characters)
SupportReferenceID (M)	<p>Reference id of the submitted request. It has a different value for each request.</p> <div>  Note: It is necessary to save the value, so that it can be used as a reference in the communication with Euronet Merchant Services, as required. </div>	Long integer
MerchantReference (M)	The MerchantReference value sent with the request.	String (up to 50 characters)
MdStatus (C)	<p>Unless there is some technical problem (ResultCode=0), it contains information on the call outcome during execution of the 3D Secure process. The actions which should follow in order for the process to be completed depend on this value (see diagram below). The possible values are:</p> <ul style="list-style-type: none"> ➡ 0: Not authenticated ➡ 1: Fully authenticated 	String

	<ul style="list-style-type: none"> ➡ 2: Not enrolled ➡ 3: Not enrolled cache (not used any more) ➡ 4: Attempt ➡ 5: U received ➡ 6: Error received (from Directory or ACS server) ➡ 9: Pending ➡ 50: Interim status during the execution of 3D Secure (see diagram below) ➡ 80: Skip device case ➡ 91: Network error ➡ 92: Directory error (read timeout) ➡ 93: Configuration error ➡ 94: Merchant input error ➡ 95: No directory found for PAN/cardtype ➡ 96: No version 2 directory found for PAN/cardtype ➡ 99: System error 	
MdErrorMsg (C)	MdStatus description (up to 128 characters)	String
EnrollmentStatus (C)	<p>Enrollment status. Contains a value when RequestType=PAResValidationRequest and is an informative field (not used <u>anywhere</u>). The potential values are:</p> <ul style="list-style-type: none"> ➡ Y: Authentication Available ➡ N: Cardholder not participating ➡ U: Unable to authentication 	String
AuthenticationStatus (C)	<p>Authentication status. Contains a value when RequestType=PAResValidationRequest and is an informative field (not used <u>anywhere</u>). The potential values are:</p> <ul style="list-style-type: none"> ➡ Y: Authentication Successful ➡ N: Authentication failed ➡ U: Authentication could not be performed ➡ A: Attempts processing performed ➡ R: Authentication rejected 	String
Eci (C)	<p>Electronic Commerce Indicator. Its value should be included when Transaction Web Service is called for the execution of the transaction (Eci parameter). If no ECI value is returned by 3D Secure wrapper, the following default values must be sent to the Transaction Web Service:</p> <ul style="list-style-type: none"> ➡ For Visa: 07 ➡ For Mastercard: 00 	String

Cavv (C)	Cardholder Authentication Value. Its value should be included when Transaction Web Service is called for the execution of the transaction (Cavv parameter)	String
Xid	ID of the request returned through the 3D Secure process. Its value should be included when Transaction Web Service is called for the execution of the transaction (Xid parameter)	String
PAResVerified (C)	Indicates whether signature verification during messaging for the execution of the 3D Secure process was successful or not. Potential values: True/False. This is an informative field and its value is not used <u>anywhere</u> .	String
Protocol (C)	Authentication protocol version used during authentication. Possible values: 1 and 2. Its value should be included when Transaction Web Service is called for the execution of the transaction (Protocol parameter)	String
TDSMethodContent (C)	Raw html for browser rendering. May contain a value when RequestType=EnrollmentRequestInit (see diagram below)	String
RedirectToACSFormData (C)	Raw html for browser rendering. It may contain a value when RequestType=EnrollmentRequestInit or RequestType=EnrollmentRequestContinue (see diagram below)	String
DsTransID (C)	Directory server transaction id. Its value should be included when Transaction Web Service is called for the execution of the transaction (DsTransID parameter)	String

The following diagram shows the algorithm for executing the 3D Secure process, followed by a text describing the process and the required calls.





Caution!



(*): In such cases, authentication has not been successfully completed. If, however, the company does decide to send the transaction, the Issuing bank may reject it. If the Issuer eventually approves the transaction and this transaction is disputed, the company shall be liable and no coverage shall be provided.

The process and controls carried out are as follows:

1. 3D-Secure Wrapper call with **RequestType=EnrollmentRequestInit**
2. The value of Result Code parameter is checked:
 - 2.1 If it is not 0, this means that a technical issue has occurred and the company will decide whether to send the transaction or not (*).
 - 2.2 If it is 0, the value of the **redirectToACSFormData** parameter of the response is checked:
 - 2.1.1 If the **redirectToACSFormData** parameter has a value, then:
 - ➡ Rendering of the **redirectToACSFormData** content on the browser (raw html). At this point the user may need to proceed to an authentication process (i.e. enter the One Time Password sent to their mobile phone or be authenticated using their fingerprint on their mobile phone).
 - ➡ Waiting for data through post on **TermURL** (sent when 3D Secure wrapper was first called):
 - Either a value will be sent through post data to the "**pares**" parameter and the content of the **md** parameter of the first 3D Secure wrapper call will be sent to "**md**" parameter
 - Or a value will be sent through post data to the "**cres**" parameter and the content of the md parameter of the first 3D Secure wrapper call will be sent to the "**threeDSSessionData**" parameter
 - ➡ 3D-Secure Wrapper call with:
 - **RequestType= PAREsValidationRequest**
 - **MerchantReference:** the value which had been used in the first 3D Secure wrapper call
 - **pares** the value of the pares parameter sent to TermURL or **cres** the value of cres sent to TermURL (one of the two parameters will be sent to TermURL)
 - ➡ The value of Result Code parameter is checked:
 - If it is not 0, this means that a technical issue has occurred and the company will decide whether to send the transaction or not (*).
 - If it is 0, the parameter value of the **mdStatus** response is checked:

- ❖ If mdStatus=0 (unsuccessful authentication), no transaction is sent and an informative message is displayed to the user.
- ❖ If mdStatus=1, 2, 3 or 4, the transaction is sent using the Transaction Web Service. Caution: the values of **Eci** , **Cavv**, **Xid**, **protocol**, **dsTransID** parameters of the 3D Secure wrapper in the 3D Secure wrapper response should be sent and the same **MerchantReference** should be used.
- ❖ If mdStatus has a different value, the 3D Secure process has not been completed and the company should decide whether to send the transaction or not (*).

2.1.2 If the **redirectToACSFormData** parameter has no value, then:

➡ The value of the response **mdStatus** parameter is checked:

- If mdStatus=0 (unsuccessful authentication), no transaction is sent and an informative message is displayed to the user.
- If mdStatus=1, 2, 3 or 4, the transaction is sent using the Transaction Web Service. Caution: the values of **Eci** , **Cavv**, **Xid**, **protocol**, **dsTransID** parameters of the 3D Secure wrapper in the 3D Secure wrapper response should be sent and the same **MerchantReference** should be used.
- If mdStatus has a value other than 0, 1, 2, 3, 4 and 50, the 3D Secure process has not been completed and the company should decide whether to send the transaction or not (*).
- If mdStatus=50, then:
 - ❖ Rendering of the **TDSMethodContent** content on the browser (raw html).
 - ❖ Waiting for a call to **threeDSMethodNotificationURL** (sent with the first 3D-Secure Wrapper call).
 - ❖ If data is sent to threeDSMethodNotificationURL or there is a **10 sec** waiting time (in which case a timeout is assumed), 3D-Secure wrapper is called with **RequestType=EnrollmentRequestContinue** and with the same MerchantReference value used in the first 3D-Secure wrapper call
 - ❖ The value of Result Code parameter is checked:
 - If it is not 0, this means that a technical issue has occurred and the company will decide whether to send the transaction or not (*).
 - If it is 0, the value of the **mdStatus** response parameter is checked:
 - If mdStatus=0 (unsuccessful authentication), no transaction is sent and an informative message is displayed to the user.

- If mdStatus=1, 2, 3 or 4, the transaction is sent using the Transaction Web Service. Caution: the values of **Eci** , **Cavv**, **Xid**, **protocol**, **dsTransID** parameters of the 3D Secure wrapper in the 3D Secure wrapper response should be sent and the same **MerchantReference** should be used.
- If mdStatus has a value other than 0, 1, 2, 3, 4 and 9, the 3D Secure process has not been completed and the company should decide whether to send the transaction or not (*).
- If mdStatus=9 and **redirectToACSForm** has a value, then:
 - ➡ Rendering of the **redirectToACSForm** content on the browser (raw html). At this point the user may need to proceed to an authentication process (i.e. enter the One Time Password sent to their mobile phone or be authenticated using their fingerprint on their mobile phone).
 - ➡ Waiting for data through post on TermURL (sent when 3D Secure wrapper was first called):
 - Either a value will be sent through post data to the "**pares**" parameter and the content of the **md** parameter of the first 3D Secure wrapper call will be sent to "**md**" parameter
 - Or a value will be sent through post data to the "**cres**" parameter and the content of the md parameter of the first 3D Secure wrapper call will be sent to the "**threeDSSessionData**" parameter
 - ➡ 3D-Secure Wrapper call with:
 - **RequestType= PResValidationRequest**
 - **MerchantReference:** the value which had been used in the first 3D Secure wrapper call
 - **pares** the value of the pares parameter sent to TermURL or **cres** the value of cres sent to TermURL (one of the two parameters will be sent to TermURL)
 - ➡ The value of Result Code parameter is checked:
 - If it is not 0, this means that a technical issue has occurred and the company will decide whether to send the transaction or not (*).
 - If it is 0, the parameter value of the **mdStatus** response is checked:
 - If mdStatus=0 (unsuccessful authentication), no transaction is sent and an informative message is displayed to the user.
 - If mdStatus=1, 2, 3 or 4, the transaction is sent using the Transaction Web Service. Caution: the values of **Eci**, **Cavv**, **Xid**, **protocol**, **dsTransID**

parameters of the 3D Secure wrapper in the 3D Secure wrapper response should be sent and the same **MerchantReference** should be used.

- If mdStatus has a different value, the 3D Secure process has not been completed and the company should decide whether to send the transaction or not (*).



Caution!

- (*): In such cases, authentication has not been successfully completed. If, however, the company does decide to send the transaction, the Issuing bank may reject it. If the Issuer eventually approves the transaction and this transaction is disputed, the company shall be liable and no coverage shall be provided.
- If the ECI parameter has no value and the company decides to send a transaction (Transaction Web Service call), the following default values must be submitted to Transaction Web Service:
 - ➡ For Visa: Eci=07
 - ➡ For Mastercard: Eci=00
- When the authentication process is initiated for a transaction, all 3D Secure wrapper calls and any Transaction Web Service call should have a **common MerchantReference value**. In the next transaction, however, a different MerchantReference value should be used (even if the process involves the same order, the payment of which is repeated due to a failure in the first time)
- The amount and currency used in the 3D Secure process (PurchAmount, Exponent, Currency parameters of the "Wrapper3DSecure service") should match those to be used in the Transaction Web Service (Amount and CurrencyCode parameters)



5. 3D-Secure Wrapper Test Cases

Below follows a list of the test cases to be executed in order to check the implementation of the 3D Secure process. In every test case:

- 1) The process described in this document should be performed using the details listed below
- 2) Depending on the result of the 3D Secure process and provided that the transaction is to be sent (see previous Section), the Transaction Web Service should be called with the same card details, same Merchant Reference, same amount and same currency. Moreover, when the Transaction Web Service is called:
 - The CVV2 parameter (for sales and preauthorisations) must have the value '123'.
 - In preauthorisations, the ExpirePreauth parameter must have the value '30'
 - The Installments parameter must have the value '0'



Test Case 1 - MDSTATUS=50/1 FRICTIONLESS

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	4908455555555557
Expiry if a sale transaction is to follow (RequestType=SALE)	xx10 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx11 where xx the last 2 digits of a future year
Authentication Type	Frictionless



Final response parameters:

Parameter	Value
ResultCode	0
MdStatus (intermediate/ final)	50/ 1
AuthenticationStatus	Y
ECI	05
Protocol	2



Company application actions:

- Transaction submission using Transaction Web Service



Test Case 2 - MDSTATUS=50/0 FRICTIONLESS

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	5194991111111113
Expiry if a sale transaction is to follow (RequestType=SALE)	xx01 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx02 where xx the last 2 digits of a future year
Authentication Type	Frictionless



Final response parameters:

Parameter	Value
ResultCode	0
MdStatus (intermediate/ final)	50/0
AuthenticationStatus	N
ECI	00
Protocol	2



Company application actions:

- The authentication was unsuccessful and the transaction should not be submitted



Test Case 3 - [MASTERCARD] MDSTATUS=50/* CHALLENGE-MULTIPLE

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	5194992222222229
Expiry if a sale transaction is to follow (RequestType=SALE)	xx01 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx02 where xx the last 2 digits of a future year
Authentication Type	Challenge



Final response parameters:

Parameter	Value
Challenge = YES	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 1
AuthenticationStatus	Y
ECI	02
Protocol	2
Company application actions:	
Transaction submission using Transaction Web Service	

Parameter	Value
Challenge = ATTEMPT	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 4
AuthenticationStatus	A
ECI	01
Protocol	2
Company application actions:	
Transaction submission using Transaction Web Service	

Parameter	Value
Challenge = NO	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 0
AuthenticationStatus	N
ECI	00
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
-----------	-------

Challenge = REJECTED	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 0
AuthenticationStatus	R
ECI	00
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = UNAVAILABLE	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 5
AuthenticationStatus	U
ECI	00
Protocol	2
Company application actions:	
The 3D Secure process has not been completed and the company should decide whether to send the transaction or not	



Test Case 4 - [VISA] MDSTATUS=50/* CHALLENGE-MULTIPLE

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	4908456666666663
Expiry if a sale transaction is to follow (RequestType=SALE)	xx05 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx06 where xx the last 2 digits of a future year
Authentication Type	Challenge



Final response parameters:

Parameter	Value
Challenge = YES	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 1
AuthenticationStatus	Y
ECI	05
Protocol	2

Company application actions:

Transaction submission using Transaction Web Service

Parameter	Value
Challenge = ATTEMPT	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 4
AuthenticationStatus	A
ECI	06
Protocol	2

Company application actions:

Transaction submission using Transaction Web Service

Parameter	Value
Challenge = NO	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 0
AuthenticationStatus	N
ECI	-
Protocol	2

Company application actions:

The authentication was unsuccessful and the transaction should not be submitted

Parameter	Value
-----------	-------

Challenge = REJECTED	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 0
AuthenticationStatus	R
ECI	-
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = UNAVAILABLE	
ResultCode	0
MdStatus (intermediate/ final)	50/9/ 5
AuthenticationStatus	U
ECI	-
Protocol	2
Company application actions:	
The 3D Secure process has not been completed and the company should decide whether to send the transaction or not	



Test Case 5 - [MASTERCARD] NO 3DS METHOD, CHALLENGE-MULTIPLE

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	5194993333333335
Expiry if a sale transaction is to follow (RequestType=SALE)	xx03 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx04 where xx the last 2 digits of a future year
Authentication Type	Challenge



Final response parameters:

Parameter	Value
Challenge = YES	
ResultCode	0
MdStatus (intermediate/ final)	9/ 1
AuthenticationStatus	Y
ECI	02
Protocol	2
Company application actions:	
Transaction submission using Transaction Web Service	

Parameter	Value
Challenge = ATTEMPT	
ResultCode	0
MdStatus (intermediate/ final)	9/ 4
AuthenticationStatus	A
ECI	01
Protocol	2
Company application actions:	
Transaction submission using Transaction Web Service	

Parameter	Value
Challenge = NO	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	N
ECI	00
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = REJECTED	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	R
ECI	00
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = UNAVAILABLE	
ResultCode	0
MdStatus (intermediate/ final)	9/ 5
AuthenticationStatus	U
ECI	00
Protocol	2
Company application actions:	
The 3D Secure process has not been completed and the company should decide whether to send the transaction or not	



Test Case 6 - NO 3DS METHOD, FRICTIONLESS, AUTHENTICATION STATUS = A

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	4020680000000098
Expiry if a sale transaction is to follow (RequestType=SALE)	xx10 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx11 where xx the last 2 digits of a future year
Authentication Type	Frictionless



Final response parameters:

Parameter	Value
ResultCode	0
MdStatus (intermediate/ final)	4
AuthenticationStatus	A
ECI	06
Protocol	2



Company application actions:

- Transaction submission using Transaction Web Service



Test Case 7 - NO 3DS METHOD, FRICTIONLESS, AUTHENTICATION STATUS U

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	4020680000000106
Expiry if a sale transaction is to follow (RequestType=SALE)	xx01 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx02 where xx the last 2 digits of a future year
Authentication Type	Frictionless



Final response parameters:

Parameter	Value
ResultCode	0
MdStatus (intermediate/ final)	5
AuthenticationStatus	U
ECI	-
Protocol	2



Company application actions:

- The 3D Secure process has not been completed and the company should decide whether to send the transaction or not



Test Case 8 – [VISA] NO 3DS METHOD, CHALLENGE-MULTIPLE

REQUIRED



Input parameters:

Parameter	Value
Currency	978
Pan	4020680000000114
Expiry if a sale transaction is to follow (RequestType=SALE)	xx01 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx06 where xx the last 2 digits of a future year
Authentication Type	Challenge



Final response parameters:

Parameter	Value
Challenge = YES	
ResultCode	0
MdStatus (intermediate/ final)	9/ 1
AuthenticationStatus	Y
ECI	05
Protocol	2
Company application actions:	
Transaction submission using Transaction Web Service	

Parameter	Value
Challenge = ATTEMPT	
ResultCode	0
MdStatus (intermediate/ final)	9/ 4
AuthenticationStatus	A
ECI	06
Protocol	2
Company application actions:	
Transaction submission using Transaction Web Service	

Parameter	Value
Challenge = NO	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	N
ECI	-
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = REJECTED	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	R
ECI	-
Protocol	2
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = UNAVAILABLE	
ResultCode	0
MdStatus (intermediate/ final)	9/ 5
AuthenticationStatus	U
ECI	-
Protocol	2
Company application actions:	
The 3D Secure process has not been completed and the company should decide whether to send the transaction or not	



Test Case 9 – [MASTERCARD] NO 3DS METHOD, CHALLENGE-MULTIPLE

OPTIONAL



Input parameters:

Parameter	Value
Currency	978
Pan	5194994444444441
Expiry if a sale transaction is to follow (RequestType=SALE)	xx01 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx02 where xx the last 2 digits of a future year
Authentication Type	Challenge



Final response parameters:

Parameter	Value
Challenge = YES	
ResultCode	0
MdStatus (intermediate/ final)	9/ 1
AuthenticationStatus	Y
ECI	02
Protocol	1

Company application actions:

Transaction submission using Transaction Web Service

Parameter	Value
Challenge = ATTEMPT	
ResultCode	0
MdStatus (intermediate/ final)	9/ 4
AuthenticationStatus	A
ECI	01
Protocol	1

Company application actions:

Transaction submission using Transaction Web Service

Parameter	Value
Challenge = NO	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	N
ECI	-
Protocol	1

Company application actions:

The authentication was unsuccessful and the transaction should not be submitted

Parameter	Value
Challenge = REJECTED	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	N
ECI	-
Protocol	1
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = UNAVAILABLE	
ResultCode	0
MdStatus (intermediate/ final)	9/ 5
AuthenticationStatus	U
ECI	-
Protocol	1
Company application actions:	
The 3D Secure process has not been completed and the company should decide whether to send the transaction or not	



Test Case 10 – [VISA] NO 3DS METHOD, CHALLENGE-MULTIPLE

OPTIONAL



Input parameters:

Parameter	Value
Currency	978
Pan	4908454444444446
Expiry if a sale transaction is to follow (RequestType=SALE)	xx01 where xx the last 2 digits of a future year
Expiry if a preauthorisation transaction is to follow (RequestType=AUTHORIZE)	xx02 where xx the last 2 digits of a future year
Authentication Type	Challenge



Final response parameters:

Parameter	Value
Challenge = YES	
ResultCode	0
MdStatus (intermediate/ final)	9/ 1
AuthenticationStatus	Y
ECI	05
Protocol	1

Company application actions:

Transaction submission using Transaction Web Service

Parameter	Value
Challenge = ATTEMPT	
ResultCode	0
MdStatus (intermediate/ final)	9/ 4
AuthenticationStatus	A
ECI	06
Protocol	1

Company application actions:

Transaction submission using Transaction Web Service

Parameter	Value
Challenge = NO	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	N
ECI	-
Protocol	1

Company application actions:

The authentication was unsuccessful and the transaction should not be submitted

Parameter	Value
Challenge = REJECTED	
ResultCode	0
MdStatus (intermediate/ final)	9/ 0
AuthenticationStatus	N
ECI	-
Protocol	1
Company application actions:	
The authentication was unsuccessful and the transaction should not be submitted	

Parameter	Value
Challenge = UNAVAILABLE	
ResultCode	0
MdStatus (intermediate/ final)	9/ 5
AuthenticationStatus	U
ECI	-
Protocol	1
Company application actions:	
The 3D Secure process has not been completed and the company should decide whether to send the transaction or not	