EMULATION (WITHOUT REDIRECTION)

ONLINE PAYMENT

Nom de fichier: Monetico_Paiement_Internet_Emulation_v2.1
Numéro de version: 2.1
Date: 2017-07-04

Confidential

Document title: Monetico Payment Emulation Without Redirection (Online Payment)
Filename: Monetico_Internet_Payment_Emulation_v2.1
Version number: 2.1
Date: 2017-07-04

The Desjardins products and services described in this document are the exclusive property of Desjardins Financial Group and all associated logos and taglines are trademarks of Desjardins Financial Group. All other trademarks mentioned in this document as well as the corresponding copyrights belong to their respective owners.

The information provided in this document is confidential and for the exclusive use of Desjardins Group and its partners. Any reproduction or distribution in whole or in part without the written permission of Desjardins Financial Group is strictly prohibited.

Web site: **www.desjardins.com**

TABLE OF CONTENTS

1 Introduction

1.1 About this document

The objective of this document is to present the technical aspects of integrating the Monetico online payment solution in emulation mode (without redirection) with your merchant website.

1.2 Target audience

This document is intended for the technical resources that are responsible for integrating the Monetico online payment solution.

1.3 Terminology

The following table contains a lexicon of certain terms used in this document.

Term used	**Desjardins term**
cancellation	purchase cancellation, preauthorization reversal
CC	payment card
« phonie »	telephone call for authorization
authorization	authorization, preauthorization
payment capture	preauthorization completion
code société	merchant number
recrédit	refund
TPE - Terminal de Paiement Électronique	EPT – Electronic Payment Terminal
TPEV – TPE virtuel	VEPT – virtual EPT
buyer, customer, client	online shopper

2 Emulation service

2.1 Description

The objective of the VEPT (Virtual Electronic Payment Terminal) online emulation service is to allow merchants to securely process online payment transactions. The Monetico payment server validates the payment card information, authorizes the payment and automatically returns the authorization result to the merchant's application.

The merchant's application dialogs directly with the Monetico payment server. Messages are exchanged in secure mode (TLS encryption) thus ensuring the confidentiality of the information provided by the merchant.

In order to certify the data exchanged, a seal is calculated on all the data sent by the merchant to the Monetico server using a standard function (IETF RFC2104). This seal is integrated in the data provided and verified by our servers for every payment.

2.2 Merchant security key

A security key specific to each Electronic Payment Terminal (EPT), designed to certify the data exchanged between the merchant's server and the secure Monetico payment server, is essential in order to be able to use the VEPT emulation service. A link for downloading that security key is sent by our Support Centre to the merchant.

The merchant can ask for the generation of a new key, from time to time or on the occasion of events such as going into production, changing host, changing service provider etc. The merchant is responsible for keeping the key secure and confidential, using the best tools available in their environment.

The security key is represented externally by 40 hexadecimal characters (e.g.

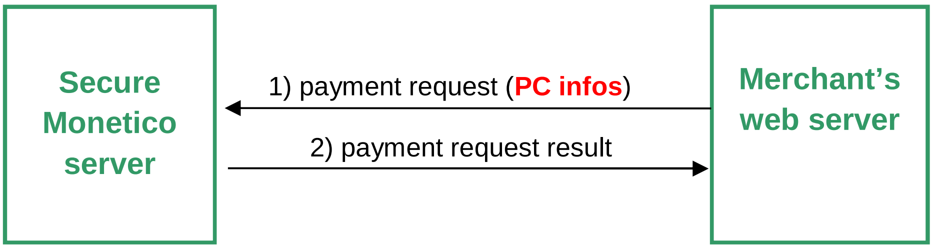
`0123456789ABCDEF0123456789ABCDEF01234567`).

The external representation must be converted into a 20-byte string (operational representation) before use.

2.3 Protocol

2.3.1 If the customer's card is not 3DSecure

The following diagram describes the exchanges between the merchant's web server and the secure Monetico server:

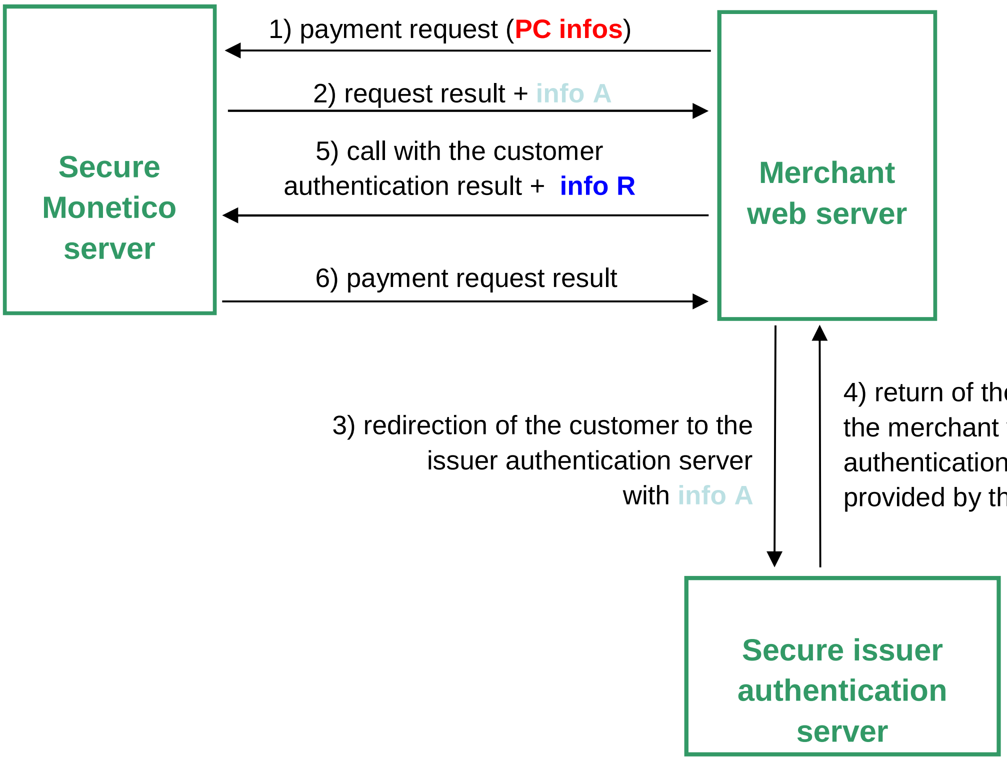


1. Payment request: The merchant's application sends a payment request to the Monetico server (call to the VEPT emulation service)

2. The Monetico server return the payment request result to the merchant's application: payment approved or payment declined.

2.3.2 If the customer's card is 3DSecure

The following diagram describes the exchanges between the merchant's web server, the secure Monetico server and the card issuer authentication server:


Secure Monetico server
1) payment request (PC infos)
2) request result + info A
5) call with the customer authentication result + info R
6) payment request result
Merchant web server
3) redirection of the customer to the issuer authentication server with info A
4) return of the customer to the merchant website after authentication + info R provided by the issuer
Secure issuer authentication server

1. Payment request: The merchant's application sends a payment request to the Monetico server (first call to the VEPT emulation service)

2. The Monetcio server returns to the merchant application a complementary cardholder authentication request, containing card issuer secure authentication server address as well as information (A) to send to it.

3. The merchant application redirects the customer to their card issuer's authentication server for cardholder authentication (by providing elements (A) returned by the Monetico in step 2).

4. Following authentication, the customer is redirected to the merchant website with the card issuer's secure authentication server response (R).

5. The merchant web server then submits the customer authentication result (R) to the Monetico server, as provided by the cardholder's card issuer (second call to the VEPT emulation service).

6. The Monetico server returns the payment result to the merchant application: payment approved or payment declined.

3 Specifications of exchanged messages

3.1 Step 1: first call to VEPT emulation

The payment request information is sent to the Monetico server by a HTTPS (TLS) message. The merchant application must issue a POST method request to the VEPT emulation service on the Monetico servers, containing the following fields:

Fields	Description	Note
version	Payment system version used	**Current version** 3.0
TPE	Merchant virtual EPT number Size: 7 characters	**Example:** 1234567
Date	Order date in format DD/MM/YYYY:HH:MM:SS	**Example:** 05/12/2006:11:55:23
montant	Total order amount including taxes formatted as follows: An integer A decimal point (optional) A 2-digit integer (optional) A 3 alphabetic character currency (ISO4217) (CAD)	**Examples:** 62.73CAD 10CAD 1024CAD **Note: Rounding is automatically done if there are than 2 decimal places.**
reference	Unique order reference Size: 12 alphanumeric characters maximum	**Example:** ABERTYP00145
texte-libre	Free text area Size: 3200 characters maximum	
lgue	Language code (upper case) Size: 2 characters	FR or EN
societe	Alphanumeric code to enable the merchant to use the same virtual EPT for different sites (separate configurations) relating to the same activity	**This code is provided by our services.** **Example:** mySite1
MAC	Seal from the data certification Size: 40 hexadecimal characters	
numero_carte	Cardholder card number	**Ex:** 1234567890123456
annee_validite	Card expiry date (year) Size: 4 digits	**Example:** 2008
mois_validite	Card expiry date (month) Size: 2 digits	**Example:** 08
cvx	Cardholder card visual cryptogram	**Example:** 123 **This parameter is optional for certain cards**
phonie	The value of this field will be returned in the case of call for authorization	**This parameter is optional (This function is not currently**

		supported by Desjardins)
Mail	Online shopper's email	**Ex: dupont@yahoo.ca**
Options	List of options used (can be empty) Options are separated from each other by an '&'. If the option has a value, its name is separated from its value with '='	**Example:** `clientip=10.20.30.40&detailrefus=1`

3.1.1 Call for authorization ("Phonie")

It is possible that an authorization request be declined for a « phonie » type reason (amount too great, authorization centre congestion, etc.). It could therefore require the merchant to manually (telephone, fax) contact the cardholder's authorization centre with the cardholder's account number and the amount to obtain an authorization number for this transaction.
Note: This function is not currently supported by Desjardins.

3.1.2 List of possible options

Options	Description	Note
aliascb	Alias of the customer's payment card in case of express payment option subscription. Format: [a-zA-Z0-9]{1,64}	**Example:** `aliascb=client1`
clientip	Customer IP address Format: 0-255.0-255.0-255.0-255	**Example:** `clientip=10.20.30.40`
detailrefus	If activated in the case of decline: allows distinguishing the different decline causes in a dedicated field. Authorized values: 0: option inactive (default value) 1: option active	**Example:** `detailrefus=0`

Note: When the option name or value is not part of those defined, the option is ignored.

3.1.3 Fields specific to instalment payment

Fields	Description	Note
nbrech	Number of payments for this order (between 2 and 4 maximum)	**Example:** `4`
dateech1	Date of the first instalment in format `DD/MM/YYYY` The first payment corresponds to the order date.	**Example:** `25/04/2008`

montantech1	The total payment amount including taxes formatted as follows:
	An integer
	A decimal point (optional)
		Examples: `62.73CAD`
		`10CAD`
		`1024CAD`

	A 2-digit integer (optional) A 3 alphabetic character currency (ISO4217) (CAD)	***Note: Rounding is automatically done if there are than 2 decimal places.**
dateech[N] (N between 2 and 4)	Date of the Nth instalment in format DD/MM/YYYY	**Example:** 05/06/2008
montantech[N] (N between 2 and 4)	Nth payment amount including taxes formatted as follows: An integer A decimal point (optional) A 2-digit integer (optional) A 3 alphabetic character currency (ISO4217) (CAD)	**Examples:** 62.73CAD 10CAD 1024CAD ***Note: Rounding is automatically done if there are more than 2 decimal places**

Note:

- In order to use these fields, your EPT must be configured to accept instalment payments.
- All these fields are mandatory
- The sum of the instalment payments must be equal to the order amount.
- The amounts must be in the same currency.
- The payments must be monthly

3.1.4 Seal calculation

The seal (to enter in the MAC field) is calculated using an encryption hashing function combined with the secret key in accordance with the RFC 2104 specifications.

This function will generate the seal from the data to certify and the merchant's security key in its operational form.

The data to certify is presented in the form of a concatenation in a specific order of the form information:

```
<TPE>*<date>*<montant>*<reference>*<texte-libre>*
<version>*<lgue>*<societe>*<mail>*<nbrech>*<dateech1>*<monta
ntech1>*<dateech2>*<montantech2>*<dateech3>*<montantech3>*<d
ateech4>*<montantech4>*<options>
```

Example for a traditional payment:

```
1234567*05/12/2006:11:55:23*62.73CAD*ABERTYP00145*FreeText
Example*3.0*EN*mySite1*onlineshopper@theiremail.ca*********
*
```

Example for an instalment payment:

```
1234567*05/12/2006:11:55:23*62.73CAD*ABERTYP00145*FreeTex
tExample*3.0*EN*mySite1*onlineshopper@theiremail.ca*4*05/1
2/2006*16.23CAD*05/01/2007*15.50CAD*05/02/2007*15.50CAD*05
/03/2007*15.50CAD*
```

3.1.5 Traditional payment request esample

```
POST /emulation3ds.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent: AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 301

          version=3.0
          &TPE=1234567
          &date=05%2F12%2F2006%3A11%3A55%3A23
          &montant=62.73CAD
          &reference=ABERTPY00145
          &texte-libre=FreeTextExample
          &lgue=EN
          &societe=mySite1
          &mail=onlineshopper@theiremail.ca
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
          &numero_carte=1234567890123456
          &annee_validite=2008
          &mois_validite=08
          &cvx=123
```

3.1.6 Instalment request payment example (in 2 instalments)

```
POST /emulation3ds.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent: AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 392

          version=3.0
          &TPE=1234567
          &date=05%2F12%2F2006%3A11%3A55%3A23
          &montant=100CAD
          &reference=ABERTPY00145
          &texte-libre=FreeTextExample
          &lgue=EN
          &societe=mySite1
          &mail=onlineshopper@theiremail.ca
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
          &numero_carte=1234567890123456
          &annee_validite=2008
          &mois_validite=08
          &cvx=123
          &nbrech=2
          &dateech1=05%2F12%2F2006
          &montantech1=20CAD
          &dateech2=12%2F01%2F2007
          &montantech2=80CAD
```

3.1.7 Payment request response

VEPT emulation returns an XML format message to the merchant (refer to the "XML return message" parararagraph for a description of the message tags.

The return message <cdr> tag will determine the subsequent processing to be performed:

<cdr> value	Subsequent processing	Return message example
0	The payment was declined. It is not necessary to perform steps 2 and 3 because the card used is not enrolled in	<xml> <cdr>0</cdr> <version>2.0</version> <reference>reference1</reference> <veres>N</veres>

	3DSecure	<originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
1	The payment was approved. It is not necessary to perform steps 2 and 3 because the card used is not enrolled in 3DSecure	<xml> <cdr>1</cdr> <version>2.0</version> <reference>reference1</reference> <aut>658745</aut> <veres>N</veres> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
2	The card used to pay the transaction is enrolled in 3DSecure. The process must continue at Step 2	<xml> <cdr>2</cdr> <version>2.0</version> <reference>reference1</reference> <md>B8AAFC7A508DA43FA5AFC474CE71A67697EED</md> <veres>Y</veres> <urlacs>http://url-acs-client/acs.cgi</urlacs> <pareq>IT8ubu+5z4YupUCOEHKsbiPep8UzIAcPKJEjpwGlzD8H0iGQRauaas 9dX65ghj321rty63ffhg632r65ghj321rty63ffhMLODtyghjEHKsbiPep8U zIAcPKJEjpwGlzD8HEHKsbiPep8UzIAcPKJEjpwGlzD8HrypeUCOE HKsbiPdfg5jh8353213ert5ezerAcPKJEjpwGlzD8H0iGQRauaas9dX6 5ghjEjpwGlzD8HEHep8UzIAcPKJKJEjpwGlzghetrzerzteer </pareq> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
< 0	The emulation request encountered an error. (Refer to the « XML return message – List of XML return code values » section)	<xml> <cdr>-2</cdr> <version>2.0</version> <reference>reference1</reference> </xml>

3.2 Step 2: Customer authentication phase

In the case of the payment card being 3DSecure, the merchant must redirect the customer, using a POST method form, to the card issuer authentication server's URL (provided in tag <urlacs>). The form must contain the following fields:

Field	Description
PaReq	retrieved as is from tag <pareq> from the Step 1 return message
MD	retrieved as is from tag <md> from the Step 1 XML return message
TermUrl	Merchant site return URL after customer authentication by the card issuer's authentication server. The return URL must be a complete URL (e.g. http://merchant.return-URL.com).

Form example:

```
<form name="formulaire" action="http://url-acs-client/acs.cgi" method="post">
        <input type="hidden" name="PaReq"
                        value="IT8ubu+5z4YupUCOEHKsbiPep8UzIAcPKJlzD8H0iGQRauaas9dX65ghj321rt
                        y63ffhg632r65ghj321rty63ffhMLODrtyghjEHKsbiPep8UzIAcPKJEjpwGlzD8HEHKsbiP
                        ep8UzIAcPKJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213587ert5ezer">
        <input type="hidden" name="TermUrl" value="http://merchant.return-URL.com">
        <input type="hidden" name="MD" value=" B8AAFC7A508DA43FA5AFC474CE71A67697EED">
        <input type="submit" value="Click here to authenticate yourself on your card issuer's server">
</form>
```

When clicking on the form's Submit button, the customer arrives on their card issuer's authentication server and authenticates themself.

3.2.1 Card issuer response

The card issuer's authentication server builds an authentication result and submits it to the URL provided in field « TermURL » of the form (the customer is thus again on the merchant site). It is an http POST request with the following parameters:

Field	Description
PaRes	Customer authentication request result
MD	Unique order identification data

Return example:

```
pares=FDG8p5z4YupUCOEHKsbiPep8UzIAcPKJEjpwGlzD8H0iGQRauaas9dX65ghj321rty63ffhg632r
65ghj321rthDio+5kn2Pep8UzIAcPKJEjpwGlzD8HEHKsbiPep8UzIAcPKJEjpwGlzD8HrypeUCOEHKsb
```

```
iPdfg5jh8353213ert5ezerAcPKJEjpwGlzD8H0iGQRauaas9dX65ghjEjpwGlzD8HEHep8UzIAcPKJKJEj
pwGlzghetrzewQ/xc45fr=&md=B8AAFC7A508DA43FA5AFC474CE71A67697EED
```

The information contained in this return message will be used to perform a second call to the EPT emulation service.

3.3 Step 3: second call to VEPT emulation

The merchant must make a second call to the VEPT emulation service, providing the card issuer's authentication result as is.

Field	Description
PaRes	Retrieved as is from « pares » of the return http request in step 2
MD	Retrieved as is from « md » of the return http request in step 2

The VEPT emulation then performs the authorization request and returns to the merchant an XML format message containing the payment result (payment approved or payment declined).

3.3.1 Request example

```
POST /emulation3ds.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent: AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 317

        PaRes=
        FDG8p5z4YupUCOEHKsbiPep8UzIAcPKJEjpwGlzD8H0iGQRauaas9dX65ghj321rty
        63ffhg632r65ghj321rthDio%2B5kn2Pep8UzIAcPKJEjpwGlzD8HEHKsbiPep8UzIAcP
        KJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213ert5ezerAcPKJEjpwGlzD8H0iGQR
        auaas9dX65ghjEjpwGlzD8HEHep8UzIAcPKJKJEjpwGlzghetrzewQ%2Fxc45fr%3D
        &MD= B8AAFC7A508DA43FA5AFC474CE71A67697EED
```

Notes:

The PaRes field to return to the Monetico server may contain non alphanumeric characters ('=', '+', '/'). They must therefore be encoded in RFC 1738 format (i.e. '%3D', '%2B', '%2F' respectively).

The preceding examples intentionally use a PaRes field with a reduced data size. Normally the PaRes field has a data size of approximately 4KB.

3.3.2 Return message

VEPT emulation returns an XML format message to the merchant (refer to the “XML return message” parararagraph for a description of the message tags.

The return message’s <cdr> tag contains the customer authentication result and the payment authorization result:

<cdr> value	Subsequent processing	Return message example
0	The payment was declined. The decline reason may be due to cardholder authentication failure (pares=N) or payment authorization decline (pares=Y)	<xml> <cdr>0</cdr> <version>2.0</version> <reference>reference1</reference> <veres>Y</veres> <pares>N</pares> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
1	The payment was approved	<xml> <cdr>1</cdr> <version>2.0</version> <reference>reference1</reference> <aut>658745</aut> <veres>Y</veres> <pares>Y</pares> <originecb>CAN</originecb> <hpancb>74E94B03C22D786E0F2C2CADBFC1C00B004B7C45</hpancb> </xml>
< 0	The emulation request encountered an error. (Refer to the « XML return message – List of XML return codes values » section)	<xml> <cdr>-2</cdr> <version>2.0</version> <reference>reference1</reference> <veres>Y</veres> <pares>Y</pares> </xml>

3.4 XML return message

Below is a description of the XML return message tags that are returned to the merchant:

The following section describes the case where the « detailrefus » option is not used. If this option was used (i.e. « detailrefus=1 » was sent, please refer to the "Case where option « detailrefus » is activated" section.

3.4.1 Traditional case where option "detailrefus" is not activated

Balise	Description	Note
<cdr>	return code	Note that if <cdr> is not equal to 1, the payment was not completed
<version>	emulation return message version number	Current version 2.0 (3.0 if the anti-fraud module is activated)
<reference>	order reference	
<aut>	authorization number	<aut> only present if the payment was approved
<phonie>	authorization declined with reason "call for auth"	<phonie> only present if field "phonie" was present and populated in the calling request (This function not currently supported by Desjardins)
<veres>	3D-Secure enrollment result Y: card enrolled 3D-Secure N: card not enrolled 3D-Secure U: technical problem	
<pares>	customer authentication result on their card issuer's authentication server Y: customer authenticated N: customer not authenticated A: authentication was requested and the issuer assumes customer authentication U: not authenticated due to a technical problem	<pares> is only present if the merchant has performed a second call to EPT emulation following customer authentication

<pareq>	complete message to send as is to the card issuer's authentication server, for customer authentication	<pareq> is only present if <cdr> return code is equal to 2
<urlacs>	URL of the card issuer's authentication server	<urlacs> is only present if <cdr> return code is equal to 2
<md>	"Merchant Data": the merchant must provide this value as is to the card issuer's authentication server.	<md> is only present if <cdr> return code is equal to 2
<originecb>	Payment card issuer country code (ISO 3166-1 standard)	<originecb> is present if <cdr> is positive or nul
<hpancb>	Irreversible hashing (HMAC-SHA1) of the payment card number used for the payment (uniquely identifying a payment card for a given merchant)	<hpancb> is present if <cdr> is positive or nul
<filtrage>	Information relating to payment filtering	Only present when payment was blocked
<scoring>	Information relating to payment scoring	Only present when scoring is activated
<analyse>	Blockage details	A group present for each filter blocking the payment. Between the tags <filtrage> or <scoring>
<cause>	Numbers of the filter types blocking the payment (see "Fraud Prevention Module Return Details" below) 1: IP address 2: Card number 3: Card BIN 4: Card country 5: IP country 6: Card country / IP country consistency 7: Black list 8: Payment card amount limit for a given period 9: Payment card transaction limit for a given	Between tags <analyse>

	period 11: Transaction limit per alias for a given period 12: Amount limit per alias for a given period 13: Amount limit per IP for a given period 14: Transaction limit per IP for a given period 15: Card testers 16: Number of aliases per payment card limit	
<valeur>	Data causing the blockage	Between tags <analyse>
<couleur>	1: Green 2: Orange 3: Red	Between tags <scoring>
<action>	1: No action: traditional scenario 2: 3DS deactivation (only if Disengageable 3DS option) 3: 3DS forcing 4: Order decline	Between tags <scoring>

3.4.2 List of XML return code message values (tag <cdr>)

Valeur balise <cdr>	Description	Commentaire
0	Payment not completed	issuer authorization was not received
1	Payment completed	issuer authorization was received and the payment was completed.
2	Step 1 result for a 3DSecure enrolled card	the merchant must perform steps 2 and 3 for customer authentication
-1	Technical problem	technical problem, need to repeat the request
-2	Unidentified merchant	parameters to identify the merchant site are incorrect, check fields societe, lgue and TPE
-3	Order not authenticated	the MAC signature is invalid
-4	Payment card expired	the payment card expiry date is invalid
-5	Payment card number is erroneous	the payment card number is invalid
-6	Order expired	the order date is beyond the authorized delay (+/- 24h)
-7	Erroneous amount	the amount transmitted is incorrectly formatted or is equal to zero
-8	Erroneous date	the date transmitted is erroneous
-9	Erroneous CVX	the visual cryptogram transmitted is erroneous
-10	Payment already authorized	an authorization has already been provided for this payment request, the payment can still be completed
-11	Payment already completed	the payment for this order has already been completed
-12	Payment already cancelled	the order has been cancelled and cannot accept a new authorization request
-13	Processing	the order is being processed
-14	Order locked out	the maximum number of card entry attempts has been reached (3 attempts

		are allowed), the order is no longer accepted by the Monetico server
-15	Parameter error	the parameters transmitted to EPT emulation are erroneous
-16	3D-Secure authentication result error	the 3D-Secure authentication result transmitted to EPT emulation is invalid
-17	The instalment amount is erroneous	The instalment amount is incorrectly formatted. The sum of the instalments is not equal to the order amount.
-18	The instalment date is erroneous	One of the dates transmitted is incorrectly formatted. The difference between the dates is not one month
-19	The number of instalments is incorrect	The number of instalments must be between 2 and 4.
-20	The version sent is incorrect	The version must be equal to « 3.0 »
-21	The payment was blocked by filtering	The blockage reasons are present in tag « filtrage ».
-22	Confiscated payment card has expired	The date of the confiscated payment card has expired
-23	Le paiement a été bloqué par scoring	The blockage reasons are present in tag « scoring ».
-24	CVV not present	The CVV, which is mandatory, has not been provided
-25	EPT closed	The EPT used is closed
-26	AVS missing	« Address Verification System » : address not provided
-27	Payment card network not accepted	The payment card network is not accepted by Desjardins or by the merchant

3.4.3 Case where option “ detailrefus” is activated

Balise	Description	Note
<cdr>	return code	Note that if <cdr> is not equal to 1, the payment was not completed
<version>	emulation return message version number	Current version 2.0 (3.0 if the anti-fraud module is activated)
<reference>	order reference	
<aut>	authorization number	<aut> only present if the payment was approved
<phonie>	authorization declined with reason ”call for auth”	<phonie> only present if field “phonie” was present and populated in the calling request
<veres>	3D-Secure enrollment result Y: card enrolled 3D-Secure N: card not enrolled 3D-Secure U: technical problem	
<pares>	customer authentication result on their card issuer’s authentication server Y: customer authenticated N: customer not authenticated A: authentication was requested and the issuer assumes customer authentication U: not authenticated due to technical problem	<pares> is only present if the merchant has performed a second call to EPT emulation following customer authentication
<pareq>	complete message to send as is to the card issuer’s authentication server, for customer authentication	<pareq> is only present if <cdr> return code is equal to 2
<urlacs>	URL of the card issuer’s authentication server	<urlacs> is only present if <cdr> return code is equal to 2

<md>	"Merchant Data": the merchant must provide this value as is to the card issuer's authentication server.	<md> is only present if <cdr> return code is equal to 2
<originecb>	Payment card issuer country code (ISO 3166-1 standard)	<originecb> is present if <cdr> is positive or nul
<hpancb>	Irreversible hashing (HMAC-SHA1) of the payment card number used for the payment(uniquely identifying a payment card for a given merchant)	<hpancb> is present if <cdr> is positive or nul
<filtrage>	Information relating to payment filtering	Only present when payment was blocked
<scoring>	Information relating to payment scoring	Only present when scoring is activated
<analyse>	Blockage details	A group present for each filter blocking the payment Between the tags <filtrage> or <scoring>
<cause>	Numbers of the filter types blocking the payment (see “Fraud Prevention Module Return Details” below) 1: IP address 2: Card number 3: Card BIN 4: Card country 5: IP country 6: Card country / IP country consistency 7: Black list 8: Payment card amount limit for a given period 9: Payment card transaction limit for a given period 11: Transaction limit per alias for a given period 12: Amount limit per alias for a given period 13: Amount limit per IP for a given period 14: Transaction limit per IP for a given period 15: Card testers 16: Number of aliases per payment card limit	Between tags <analyse>
<valeur>	Data causing the blockage	Between tags <analyse>

<couleur>	1: Green 2: Orange 3: Red	Between tags <scoring>
<action>	1: No action: traditional scenario 2: 3DS deactivation (only if Disengageable 3DS option) 3: 3DS forcing 4: Order decline	Between tags <scoring>
<motifrefus>	Payment request decline reason: Appel Phonie: the card issuer requests additional information Refus: the card issuer declines authorization Interdit: the card issuer declines authorization filtrage: the payment request was blocked by filtering configuration that the merchant inplemented in their Fraud Prevention Module scoring: the payment request was blocked by scoring configuration that the merchant inplemented in their Fraud Prevention Module 3DSecure: if the decline is related to a negative 3DSecure authentication received from the cardholder's card issuer	Only in the case where the payment request was declined with cdr=0

3.4.4 List of XML return code messages (tag <cdr>)

Valeur balise <cdr>	Description	Commentaire
0	Payment not completed	issuer authorization was not received
1	Payment completed	issuer authorization was received and the payment was completed.
2	Step 1 result for a 3DSecure enrolled card	the merchant must perform steps 2 and 3 for customer authentication
-1	Technical problem	technical problem, need to repeat the request
-2	Unidentified merchant	parameters to identify the merchant site are incorrect, check fields societe, lgue and TPE
-3	Order not authenticated	the MAC signature is invalid
-4	Payment card expired	the payment card expiry date is invalid
-5	Payment card number is erroneous	the payment card number is invalid
-6	Order expired	the order date is beyond the authorized delay (+/- 24h)
-7	Erroneous amount	the amount transmitted is incorrectly formatted or is equal to zero
-8	Erroneous date	the date transmitted is erroneous
-9	Erroneous CVX	the visual cryptogram transmitted is erroneous
-10	payment already authorized	an authorization has already been provided for this payment request, the payment can still be completed
-11	Payment already completed	the payment for this order has already been completed
-12	Payment already cancelled	the order has been cancelled and cannot accept a new authorization request
-13	Processing	the order is being processed
-14	Order locked out	the maximum number of card entry attempts has been reached (3 attempts

		are allowed), the order is no longer accepted by the Monetico server
-15	Parameter error	the parameters transmitted to EPT emulation are erroneous
-16	3D-Secure authentication result error	the 3D-Secure authentication result transmitted to EPT emulation is invalid
-17	The instalment amount is erroneous	The instalment amount is incorrectly formatted. The sum of the instalments is not equal to the order amount.
-18	The instalment date is erroneous	One of the dates transmitted is incorrectly formatted. The difference between the dates is not one month
-19	The number of instalments is incorrect	The number of instalments must be between 2 and 4.
-20	The version sent is incorrect	The version must be equal to « 3.0 »
-22	Confiscated payment card has expired	The date of the confiscated payment card has expired
-24	CVV not present	The CVV, which is mandatory, has not been provided
-25	EPT closed	The EPT used is closed
-26	AVS missing	« Address Verification System » : address not provided
-27	Payment card network not accepted	The payment card network is not accepted by Desjardins or by the merchant

3.4.5 Fraud Prevention Module Return Details

The payment filtering function uses a set of nine filters that are completely configurable via the Control Panel (new version). Each of these filters relates to a specific criterion such as customer IP address or email address, the country of the customer's card, etc.

Filter type number	Analysis criterion	Value returned as blockage reason	Note
1	IP address	Customer IP address	
2	Card number	Hash of customer card	Works only for card payments
3	Card BIN	Customer card BIN	
4	Card country	Customer card country	
5	IP country	Customer IP country	
6	Card country / IP country consistency	Customer card country # Customer IP address country	Works only for card payments
7	Black list	Customer email address domain name	
8	Payment card amount limit for a given period	Customer card cumulative amount in CAD over the given period	Works only for card payments
9	Payment card transaction limit for a given period	Customer card cumulative number of transactions over the given period	
11	Transaction limit per alias for a given period	Customer alias cumulative number of transactions over the given period	Only in the case of subscription to express payment option
12	Amount limit per alias for a given period	Customer alias cumulative amount in CAD over the given period	
13	Amount limit per IP for a given period	Customer IP address cumulative amount in CAD over the given period	
14	Transaction limit per IP for a given period	Customer IP address cumulative number of transactions over the given period	

15	Card testers	Customer IP address cumulative number of transactions over the given period	
16	Number of aliases per payment card limit	The aliases already associated with the payment card used	Only in the case of subscription to express payment option Works only for card payments.

4 Appendices

4.1 General requirements for the HTML coding of fields

All fields of the call request with the exception of the version and the amounts must be encoded in HTML before formatting in the form (i.e. immediately after the MAC calculation).

The characters to be encoded are ASCII codes from 0 to 127 which are deemed to be risky:

Name	Symbol	Replacement
Ampersand	&	**&amp;**
Less than	<	**&lt;**
Greater than	>	**&gt;**
Quotation marks	"	**&quot; or &#x22;**
Apostrophe	'	**&#x27;**

Functions of the "`HTML_ENCODE`" type (see IETF RFC1738 standard) of languages are perfectly suitable and encode many more characters, typically anything that is not:

- `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
- `abcdefghijklmnopqrstuvwxyz`
- `0123456789`
- `_ . -` (underscore, period, hyphen)

If you use characters outside the common printable ASCII range (31<ASCII<127) in field "`texte-libre`", you must encode the field before any payment-related processing to avoid problems while calculating the MAC seal.

Lastly, the fields must not contain ASCII characters 10 and 13 (CR and LF).

4.2 Specific requirements depending on the field

Fields	Contents / format before HTML encoding	Maximum size after HTML encoding
TPE	A-Z a-z 0-9	**7**
version	3.0	**Fixe**
date		**50**
montant		**20**
référence	A-Z a-z 0-9	**12**
MAC	0-9 A-F a-f	**40**
lgue	A-Z	**2**
societe	A-Z a-z 0-9	**50**
texte-libre	Base 64	**3200**
numero_carte	0-9	**16**
annee_validite	0-9	**4**
mois_validite	0-9	**2**
cvx	0-9	**3**
phonie	A-Z a-z 0-9	**50**
mail		**50**
nbrech	2-4	**1**
dateechN		**50**
montantechN		**20**
option=clientip	0-255.0-255.0-255.0-255	**25**
option=detailrefus	0-1	**1**

4.3 3D-Secure mode

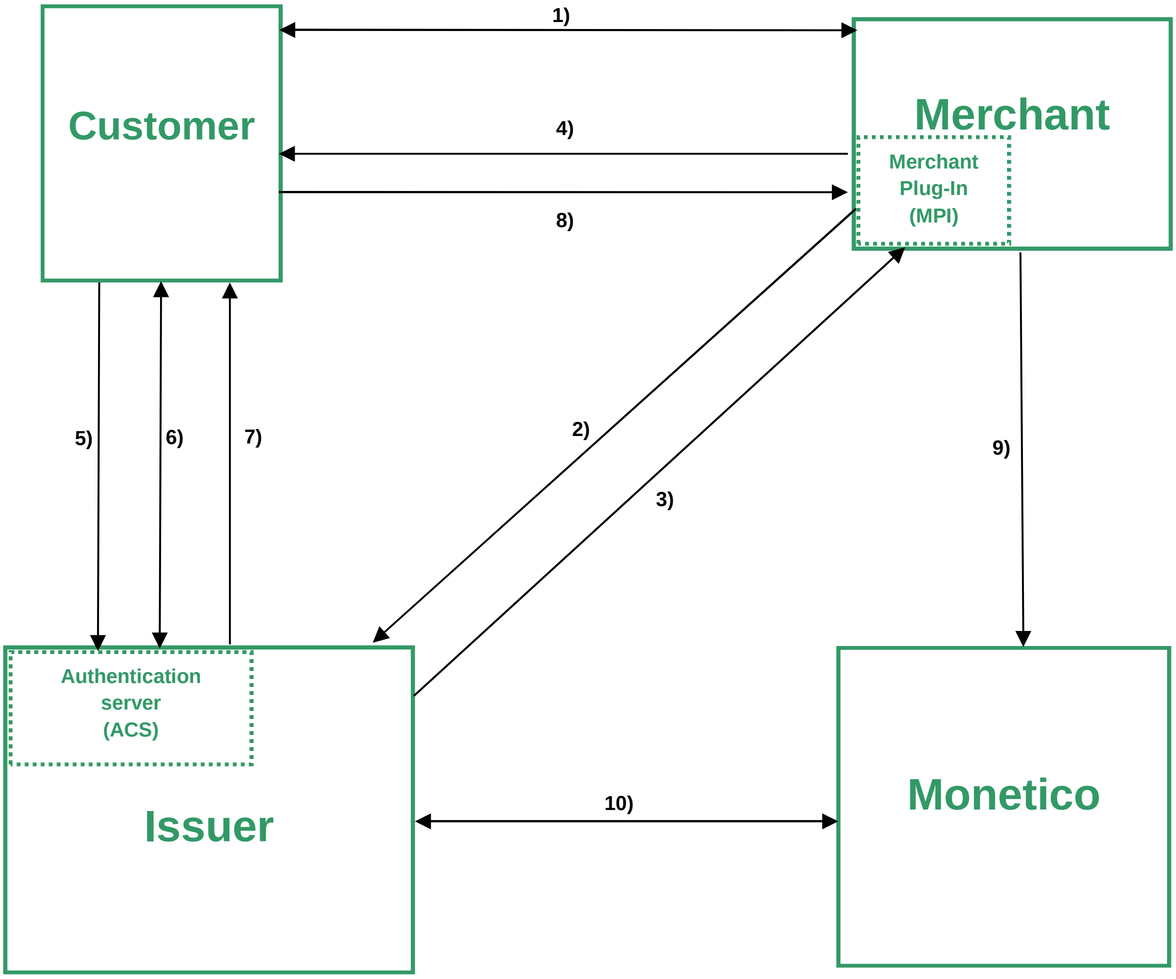
4.3.1 Description

In order to strengthen the security of Internet transactions, a new security standard is now in place: 3D Secure. It aims to reduce the risk of fraud, thanks to a cardholder authentication procedure by the card issuer.

The objective: to reduce the risk of fraud
In order to avoid having a transaction rejected because the customer contests the purchase with the card issuer, this procedure now verifies the customer's identity. In addition to card number, expiry date and cryptogram, with the 3D Secure system, the cardholder must authenticate themselves to their card issuer by providing a code or some personal information.

4.3.2 How it works

Below is a simplified summary of the message exchanges in 3D Secure mode:



Step	Description
Step 1	The customer makes their purchases on the merchant’s website and enters their payment card number, expiry date and visual cryptogram.
Step 2	The merchant plug-in (MPI) sends a customer payment card enrollment verification request (VEReq) to the card issuer’s authentication server (ACS).
Step 3	The card issuer’s authentication server submits the enrollment result (VERes) to MPI. If the customer’s payment card is not enrolled in 3Dsecure, an authorization request is performed, and steps 4 to 9 are skipped.
Step 4	The MPI sends an authentication request (PAReq) via the customer’s browser to the ACS.
Step 5	The ACS receives the authentication request (PAReq).
Step 6	The ACS proceeds to customer authentication.
Step 7	The ACS submits the customer authentication result (PARes) to MPI via the customer’s browser.
Step 8	The MPI receives the customer authentication result (PARes).
Step 9	The 3D-Secure mode authorization request has thus been performed.
Step 10	The transaction is performed.

4.3.3 3D-Secure glossary

Term	**Description**
ACS	3D-Secure secure authentication server.
VEReq	3D-Secure payment card enrollment verification request.
VERes	3D-Secure payment card enrollment verification result.
PAReq	Customer authentication request.
PARes	Customer authentication request result.
MPI	Merchant plug-in: software module to verify a payment card’s 3D-Secure enrollment and return the website address of the cardholder’s card issuer’s authentication server.

5 Use of the service

5.1 Test environment

The role of our test server is to enable you to test and validate your developments.

On the test server, the only card validation performed is on the card number structure. Nothing else is validated such as expiry date, black list, etc. that are applied on our production server.

Of course, all operations carried out by our test payment server are fictitious and do not result in any real financial transaction.

In order to test the different return codes provided by the Monetico server, several test card numbers are available that result in different authorization responses by the card issuer:

Card number	Authorization
0000 0100 0000 0001	**Card not enrolled in 3D-Secure declined**
0000 0100 0000 0002	**Card not enrolled in 3D-Secure approved**
0000 0100 0000 0003	**Card not enrolled in 3D-Secure call for authorization**
0000 0100 0000 0004	**Card enrolled in 3D-Secure not authenticated declined**
0000 0100 0000 0005	**Card enrolled in 3D-Secure authenticated approved**
0000 0100 0000 0006	**Card enrolled in 3D-Secure authenticated declined**

The test environments are available at the following address:

- https://p.monetico-services.com/test/emulation3ds.cgi

5.2 Production environment

After validating your developments and completing the request to support@desjardins.monetico-services.com to go into Production, you will be able to access the Production server, at the following address:

- https://p.monetico-services.com/emulation3ds.cgi

Please note that the payment requests sent to the Production server represent real financial transactions.

5.3 Technical support

Desjardins offers assistance for the overall understanding of the use of its solution:

- by email to support@desjardins.monetico-services.com
- by phone:
  Montreal area: 514-397-4450
  Canada and the US: 1-888-285-0015

However, Desjardins provides only limited support for any issues relating to the technical integration of its payment solution.

END OF DOCUMENT

.