Desjardins

Monetico Payment

INTEGRATED PAGE (IFRAME)

ONLINE PAYMENT

Nom de fichier: Monetico_Internet_Payment_Integrated_Page_v2.0
Numéro de version: 2.0
Date: 2016-12-02

Confidential

Document title: Monetico Payment Integrated Page (iFrame) Online Payment
Filename: Monetico_Internet_Payment_Integrated_Page_v2.0
Version number: 2.0
Date: 2016-12-02

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

TABLE OF CONTENTS

1 Introduction 5

1.1 About this document 5

1.2 Target audience 5

1.3 Terminology 5

2 Integrated page (iFrame) 6

2.1 Description 6

2.2 Merchant security key 6

3 Process flows 7

3.1 Screen sequence 7

3.2 Integrated page display 8

3.3 ACS redirection 9

3.4 Payment return 9

3.5 Payment requests 10

4 How it works 15

4.1 Integration with the merchant website 15

4.2 Payment validation 16

5 Integrated page characteristics 17

5.1 Display mode 17

5.2 Page customization 17

5.3 Email of the transaction record 17

5.4 Return to the merchant website 18

6 Appendices 19

6.1 General constraints for the HTML coding of fields 19

6.2 Specific constraints depending on the field 20

6.3 General constraints for URL field coding 21

6.4 3D-Secure mode 22

6.4.1 Description 22

6.4.2 How it works 22

6.4.3 3D-Secure glossary 24

7 Use of the service 25

7.1 Test environment 25

7.2 Production environment 25

7.3 Technical support 26

8 Installation aids 27

8.1 Most frequent problems _____ 27
8.1.1 Security seal calculation problem _____ 27
8.1.2 The merchant cannot be identified _____ 28
8.1.3 Your merchant's site was not identified _____ 28

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 integrated page (iFrame) mode 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, PC
« 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 Integrated page (iFrame)

2.1 Description

Enables merchants to securely process online payments without leaving the merchant's sales funnel. Contrary to the Monetico payment page, the integrated page blends with the merchant website. The Monetico payment server validates the payment card information transmitted before authorizing the payment and automatically confirms the payment request result to the merchant's application.

The exchanges are done securely (TLS V1.0 or higher encryption), 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.

For every payment performed on our platform, your server receives an immediate notification of the payment's success or failure. In addition, we can email the payment result to you.

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 Monetico's payment service in integrtaed page mode. 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.

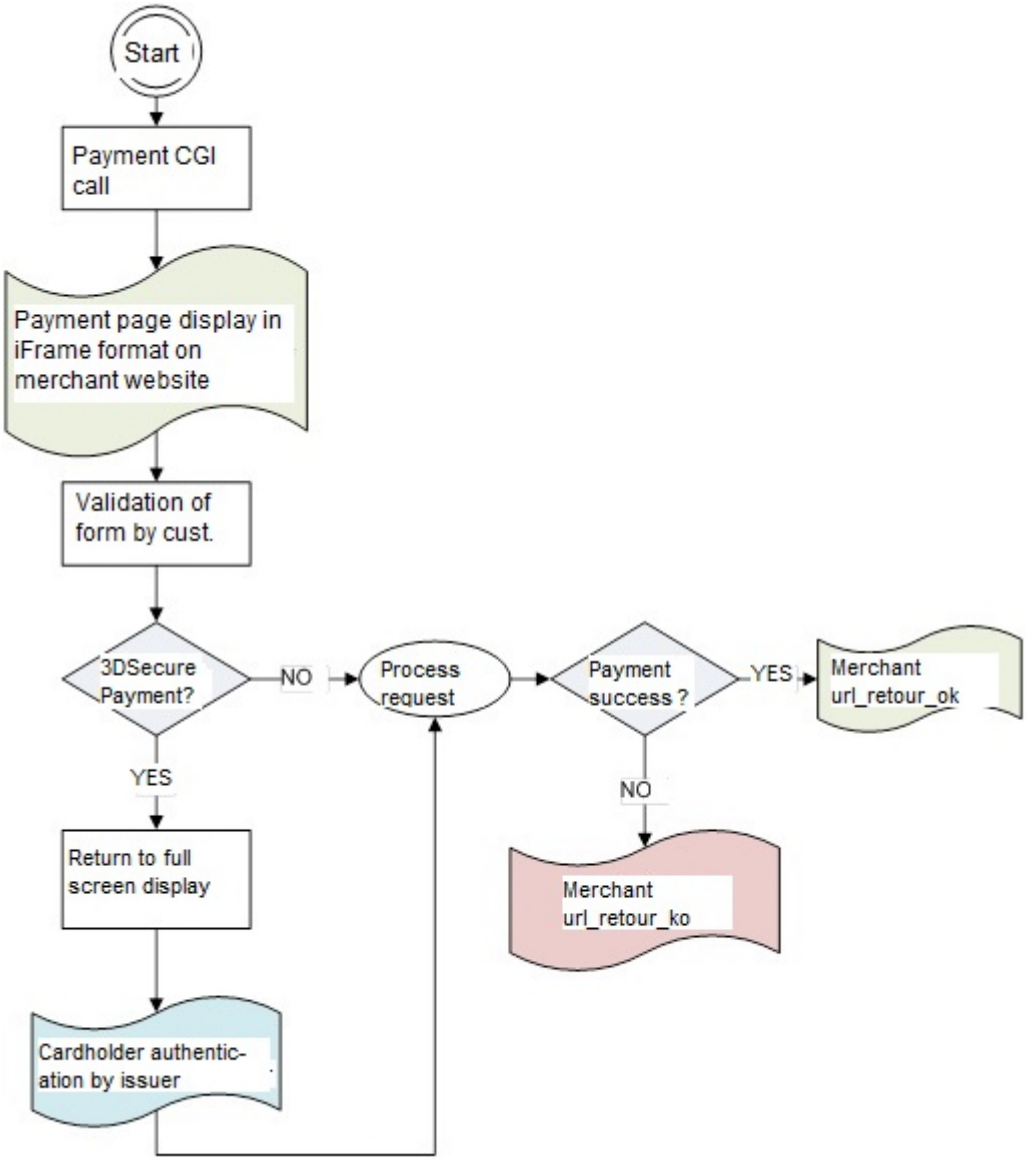
The security key is represented externally by 40 hexadecimal characters (e.g.

`0123456789ABCDEF0123456789ABCDEF01234567`).

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

3 Process flows

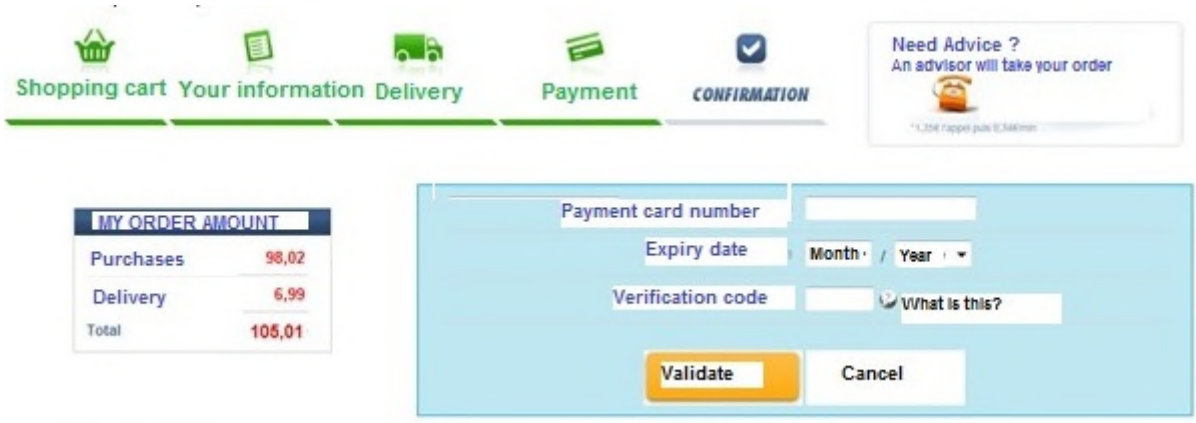
3.1 Screen sequence



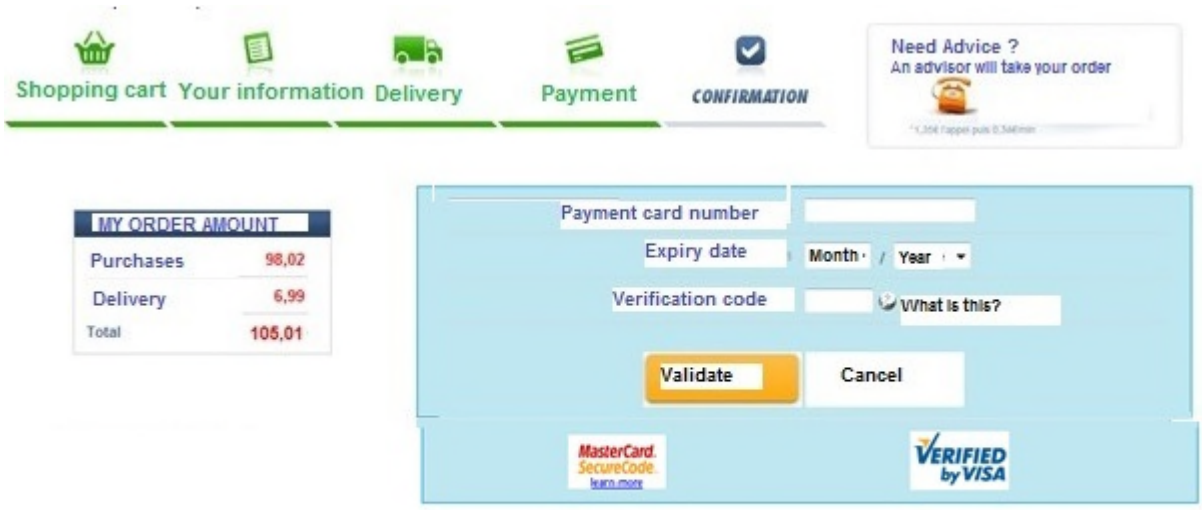
3.2 Integrated page display

The Monetico payment application displays the customized input form that blends with the merchant website.

In the case of a non 3DSecure payment:

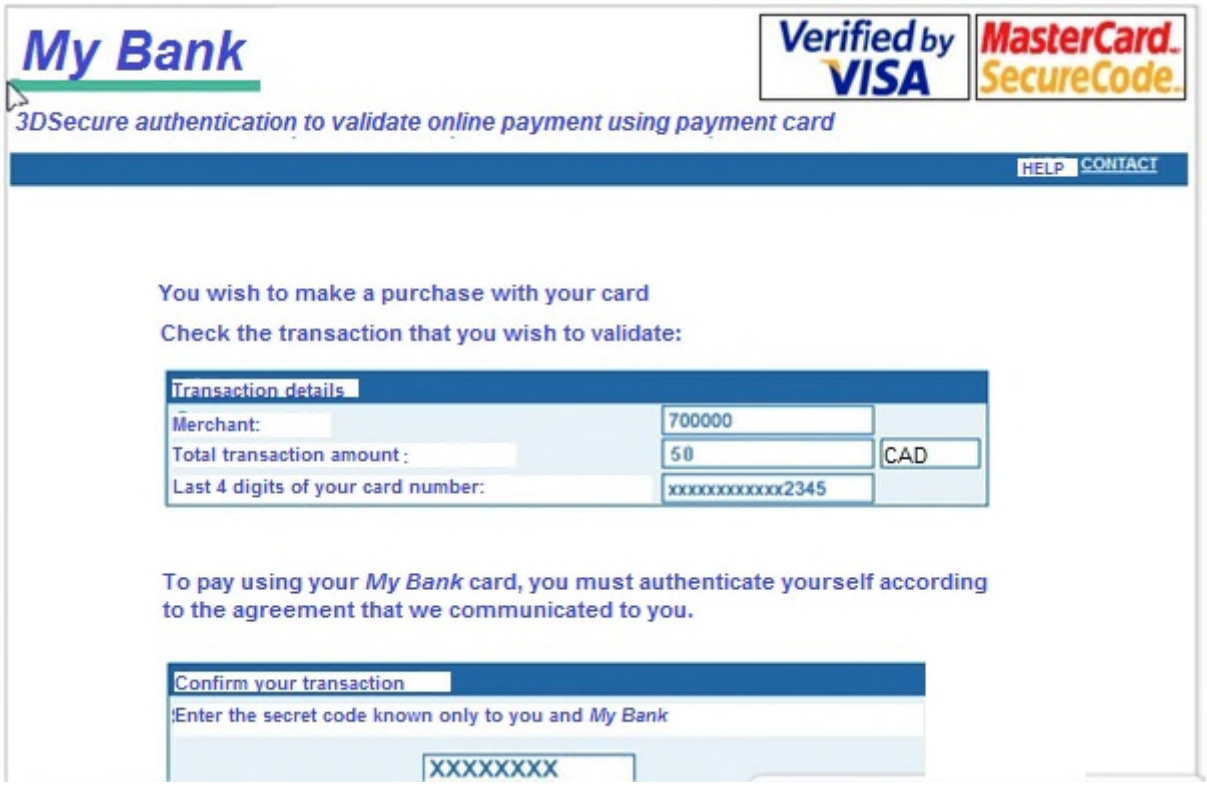


In the case of a 3DSecure payment:



3.3 ACS redirection

In the case of a 3DSecure payment, the Monetico Payment application will revert to a traditional display before redirecting the customer to their card issuer's authentication system.



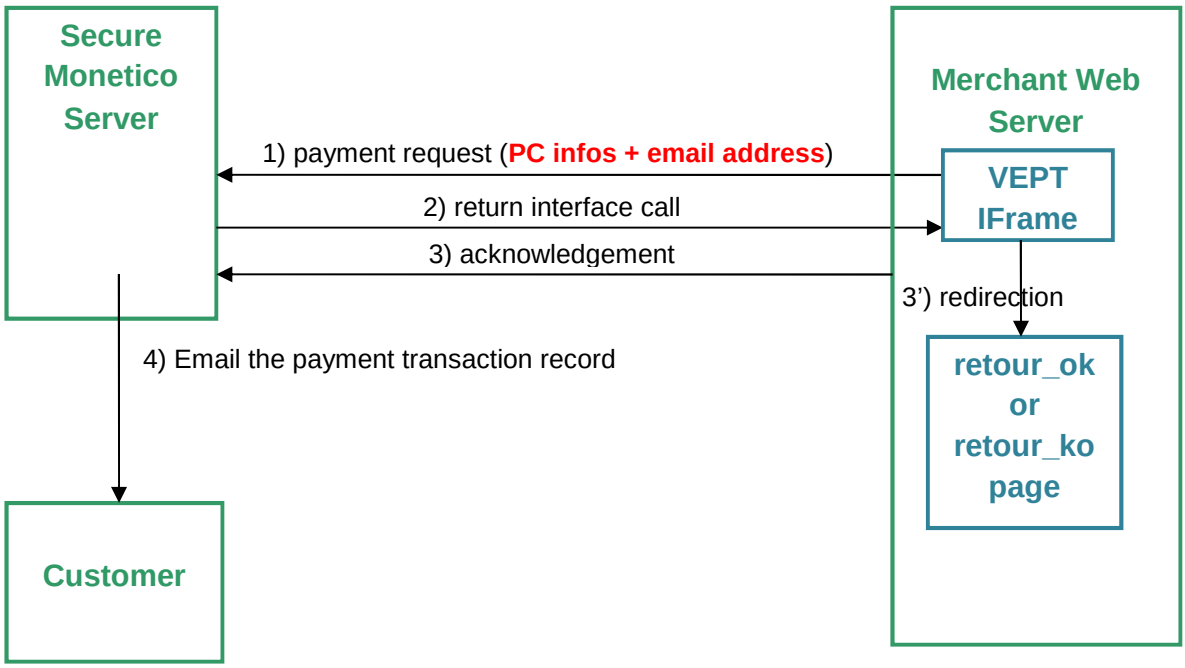
3.4 Payment return

Below is an example of a merchant return page presenting the payment result to the cardholder.

3.5 Payment requests

3.5.1 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: entry of the card information on the integrated page of the merchant website.

2. The Monetico server directly informs the merchant's IT system of the payment request result by issuing an http(s) request on the payment confirmation address (in other words, **the Monetico server calls the "Return" interface placed on the merchant's machine**).
   You must give us this URL address when the system is implemented and in case of change (domain name or directory modification).

3. The merchant's IT system acknowledges payment confirmation.

   In practice, the "Return" interface is responsible for receiving the payment confirmation request, extracting the various information from it and responding to the Monetico server via an acknowledgement.

   The information received by the "Return" interface allow for determination of the order concerned, as well as the payment request result. This allows the merchant server to perform specific processing:

   - Verify that the amount and reference correspond to a recorded order awating payment
   - Update the order status in the databases
   - Send a confirmation email to the merchant and/or the online shopper
   - Etc.

   NB: the order must be persistent in the merchant system (file, database) from the beginning of the process and must not be deleted even after a first payment decline notice.

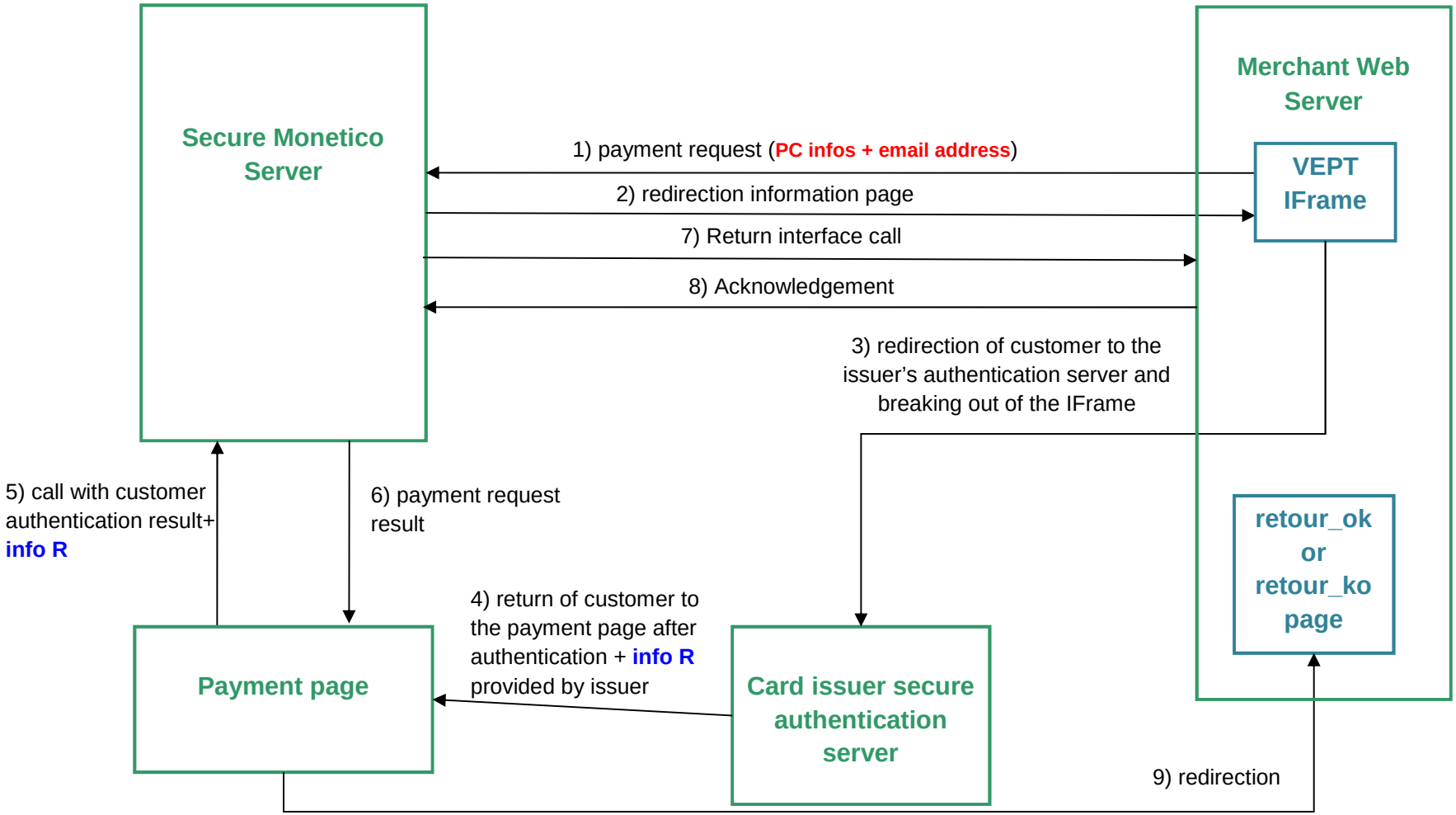
   In fact, a decline may be followed by an approval (the "Return" interface may thus be called several times for the same order), for example, in the case of an input entry error or a threshold reached error; the online shopper may therefore want to use another card to make the payment.

4. Email the customer a summary of the transaction performed

3'. Redirection to the merchant's retour_ok or retour_ko page according to the payment result

2.5.2 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 cardholder's card issuer secure authentication server:



1. Payment request: 3DSecure protocol participation verification for the card entered on the integrated page of the merchant website.

2. The Monetico server returns a redirecton page to the cardholder's card issuer's secure authentication server.

3. Redirection of customer to their card issuer's authentication server reverting to a traditional display.

4. Following authentication, the customer is redirected to the payment page together with the response (R) from the cardholder's card issuer's secure authentication server.

5. The payment page then submits the customer authentication result (R) as provided by the card issuer.

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

7. The Monetico server directly informs the merchant's IT system of the payment request result by issuing an http(s) request on the payment confirmation address (in other words, **the Monetico server calls the "Return" interface placed on the merchant's machine**).
   You must give us this URL address when the system is implemented and in case of change (domain name or directory modification).

8. The merchant's IT system acknowledges payment confirmation.

   In practice, the "Return" interface is responsible for receiving the payment confirmation request, extracting the various information from it and responding to the Monetico server via an acknowledgement.
   The information received by the "Return" interface allow for determination of the order concerned, as well as the payment request result. This allows the merchant server to perform specific processing:

   - Verify that the amount and reference correspond to a recorded order awating payment
   - Update the order status in the databases
   - Send a confirmation email to the merchant and/or the online shopper
   - Etc.

   NB: the order must be persistent in the merchant system (file, database) from the beginning of the process and must not be deleted even after a first payment decline notice.

   In fact, a decline may be followed by an approval (the "Return" interface may thus be called several times for the same order), for example, in the case of an input entry

error or a payment card threshold reached error; the online shopper may therefore want to use another card to make the payment.

9. The payment page then redirects to the retour_ok or retour_ko page depending on the payment request result.

4 How it works

4.1 Integration with the merchant website

The merchant website integrates the call to Monetico Payment using an HTML « iframe » tag within the online store:

```
<iframe id="idFramePaiement" name="nomFramePaiement" src="…" ></iframe>
```

The values of fields id and name are examples that have no effect on the application's behaviour.

The « src » field value must be of the following form:

https://p.monetico-services.com/paiement.cgi?parametre1=valeur1&parametre2=valeur2

Use only those fields specified below in your calls to the payment page. The use of any other fields could result in being unable to access the payment page because it would be considered as an illegitimate access.

The parameters to provide are:

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 more than 2 decimal places.

reference	Unique order reference Size: 12 alphanumeric characters maximum	**Example:** `ABERTYP00145`
texte-libre	Free text area Size: 3200 characters maximum	
mail	Online shopper's email address	**Example:** email@e.ca
lgue	Language code Size: 2 characters	`FR or EN`
societe	Alphanumeric code to enable the merchant to use the same virtual EPT for different sites (separate	**This code is provided by our services.** **Example:** `mySite1`

	configurations) relating to the same activity	
url_retour	URL by which the online shopper returns to the online store's home page	
url_retour_ok	URL by which the online shopper returns to the merchant website following an approved payment	**NB: not to be confused with the "Return" interface URL, also called "payment confirmation URL"**
url_retour_ko	URL by which the online shopper returns to the merchant website following a declined payment	
MAC	Seal from the data certification Size: 40 hexadecimal characters	
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`
mode_affichage	Parameters to activate display in iFrame form	**To activate the iframe:** iframe

NB: All values must be « URL encoded » (see **Appendix 6.3**), as for example:

mail=email@e.ca
url_retour_ok=http://www.mywebsite.com/payment/retourOK.html

will become:

mail=email%40e.ca

url_retour_ok=http%3A%2F%2Fwww.mywebsite.com%2Fpayment%2FretourOK.html

This encoding must be done after calculating the security seal.

4.2 Payment validation

When the customer validates or cancels payment, the Monetico Payment application reverts to the traditional display and redirects the customer to the url_retour_ok or url_retour_ko page, that will redisplay a complete page (i.e. with the banners, headers and other site navigation elements) to the cardholder.

5 Integrated page characteristics

5.1 Display mode

In order for the integrated display mode to be active, in the call to Monetico Payment, the parameter ***mode_affichage*** must be set to ***iframe,*** otherwise the traditional payment page will be displayed without customization.

5.2 Page customization

In integrated mode, it is possible to customize the following elements:

1. Background colour of the right block
2. Titles colour
3. Right block border colour
4. Validate button
5. Cancel button

The buttons are customizable as images:

- gif format
- size: 128 x 25 pixels

Only the colour of the various elements is customizable.

5.3 Email of the transaction record

As with all payments, the customer must be informed of the payment result by Monetico Payment. In the context of integrated payment page mode payments, the transaction record is emailed directly to the customer. The customer's email address is thus a mandatory parmameter in the integrated page mode.

Failure to comply with this rule will cause redirection to the full screen standard payment page without customization.

5.4 Return to the merchant website

When the request has been processed (declined or approved), redirection will occur to the appropriate URL (url_retour_ok or url_retour_ko) without any user action required. The integrated page form display on the merchant website will not be kept and the return URLs must redisplay the entire merchant website page.

It will not be possible to place multiple calls to an integrated payment page because the first one validated will trigger an action that potentially involves a page change.

6 Appendices

6.1 General constraints for the HTML coding of fields

All fields of the call request with the exception of the version and the amount 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	"	" or "
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 when calculating the MAC seal.

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

6.2 Specific constraints 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**
mode_affichage=iFrame	a-z	

6.3 General constraints for URL field coding

All values passed to the CGI must be URL encoded, before sending, as specified in Section 4.3. The characters that must be encoded are ASCII codes from 0 to 127 which are deemed to be risky:

Name	Symbol	Replacement
Ampersand	&	%26
Less than	<	%3C
Greater than	>	%3E
Quotation marks	"	%22
Apostrophe	'	%27
« At » sign	@	%40

(This list is not exhaustive)

Functions of the "urlencode" type of languages are perfectly suitable and encode many more characters, typically anything that is not:

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

6.4 3D-Secure mode

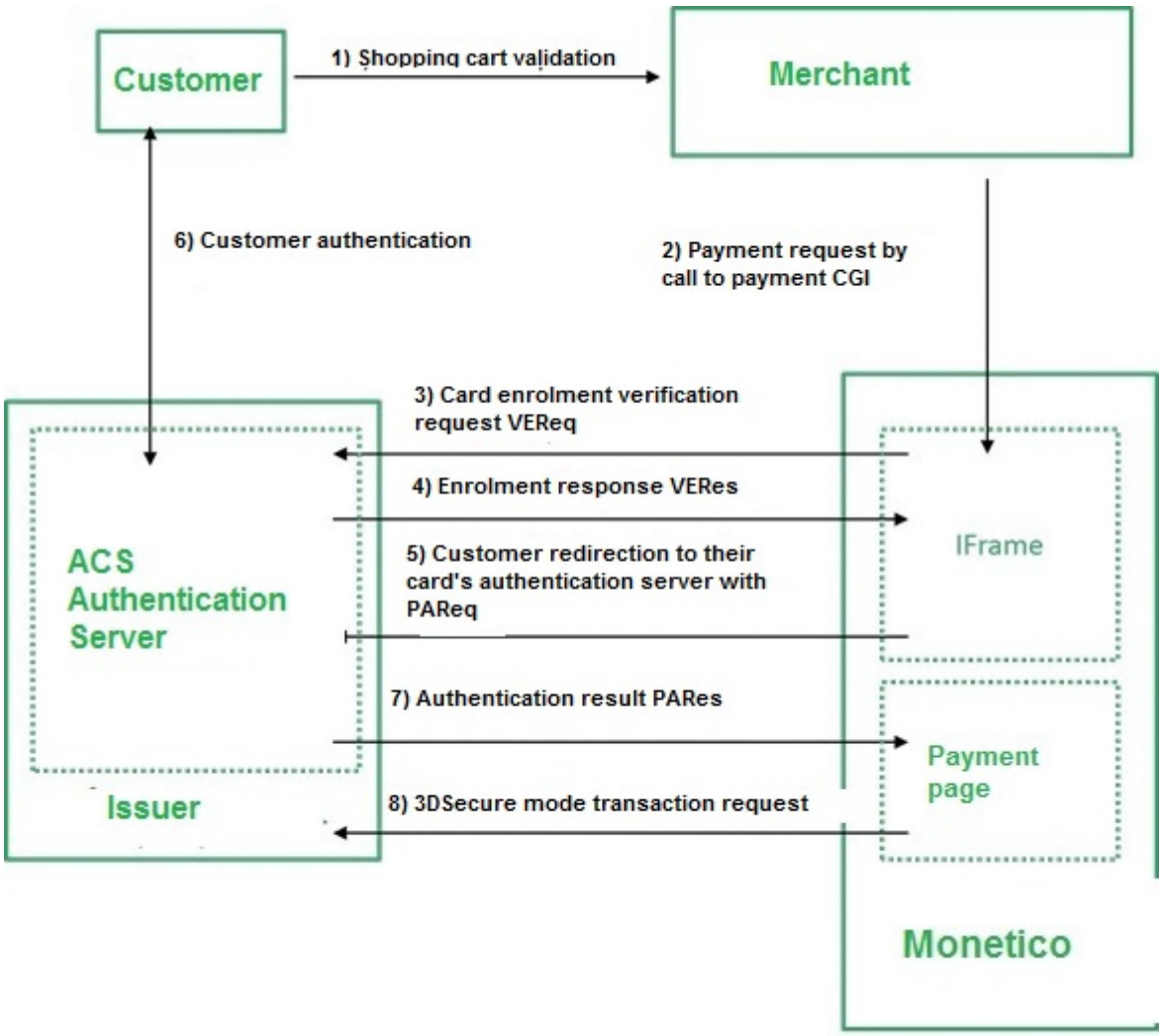
6.4.1 Description

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.

6.4.2 How it works

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



Step	Description
Step 1	The customer validates their shopping cart on the merchant's website.
Step 2	The merchant website calls the payment CGI in an iframe.
Step 3	The Monetico server (the iframe) sends a cardholder payment card enrolment verification request (VEReq) to the cardholder's card issuer's authentication server (ACS).
Step 4	The cardholder's card issuer's authentication server submits the enrolment verification result (VERes) to the Monetico server (the iframe). If the customer's payment card is not 3DSecure enrolled, an authorization request is performed and steps 4 to 9 are skipped.
Step 5	The iframe redirects the customer to their card issuer's website by performing an authentication request (PAReq).

Step 6	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 the Monetico server (payment page)
Step 8	The Monetico server performs the 3D-Secure mode authorization request.

6.4.3 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.

7 Use of the service

7.1 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 environment is available at the following address:

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

7.2 Production environment

After validating your developments you will be able to access the Production server, at the following address:

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

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

7.3 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

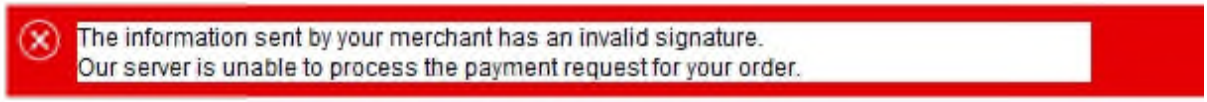
However, Desjardins provides only limited support for any issues relating to the merchant's technical integration of its payment solution.

8 Installation aids

8.1 Most frequent problems

8.1.1 Security seal calculation problem

Error message



Possible causes

- The form that you sent us does not contain all required information
- The MAC seal calculation is incorrect
- The MAC seal calculation was done using the wrong key
- The language code is incorrect or missing

Problem resolution

Follow the procedure below exactly. After each step where you have made changes in your implementation, perform new payment tests. If they still don't work, go to the next step.

NB: do not skip steps!

Step 1: verify that all the variables sent in the form are present, spelled correctly, respect the case and respect any possible restrictions regarding format or characters authorized. These variables are: TPE, date, montant, reference, texte-libre, version, lgue, societe, MAC, mail, nbrech, dateech1, montantech1, dateech2, montantech2, dateech3, montantech3, dateech4, montantech4, numero_carte, annee_validite, mois_validite, and cvx.

Step 2: verify that you have avoided errors that are inherent to certain specific fields:

- Is the MAC version value a 40-character hexadecimal string (authorized values: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F)?
- Is the version variable 3.0?
- Is the date variable format DD/MM/YYYY:HH:MM:SS?
- Is the reference variable a string containing only unaccented letters and digits and be a maximum length of 12 characters?
- Is the texte-libre variable correctly spelled and respects the case and uses the hyphen character ('-') and not the underline character ('_')?
-

Step 3: verify that the string for which you calculate the MAC respects the previously described criteria.

<TPE>*<date>*<montant>*<reference>*<texte-libre>*<version>*<lgue>*<societe>*

<mail>*<nbrech>*<dateech1>*<montantech1>*<dateech2>*<montantech2>*<dateech3>*<montantech3>*<dateech4>*<montantech4>*

Pay particular attention to the fact that the data used must be the same as that provided in the payment form. The best way to ensure this is to store the various information ahead of time, then use the stored version to calculate the MAC seal and for building the form (for example, for the date field, there could be a difference of several seconds).

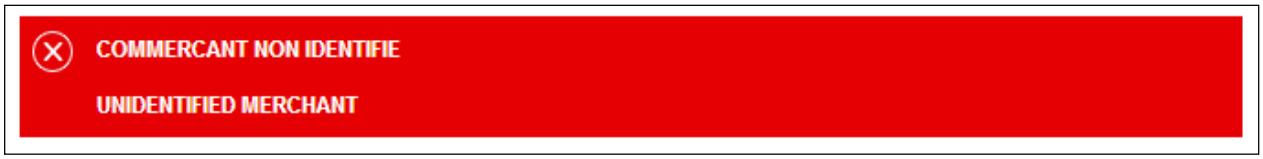
Step 4: Verify that you are using the correct security key:

- You must use the last key that we provided to you.
- Verify that the key matches your seal calculation algorithm (SHA1 or MD5),
- Contact our Technical Support to verify together that you are using the correct key

If, in spite of all these verifications, you still receive this error message, the problem is with your integration of our solution with your IT system. Due to the great variety of languages used and the specifics of the environment used to implement our payment solution that are too numerous for us to have expertise in all of them, we are unable to provide you with more detailed customized support.

8.1.2 The merchant cannot be identified

Error message



Possible causes

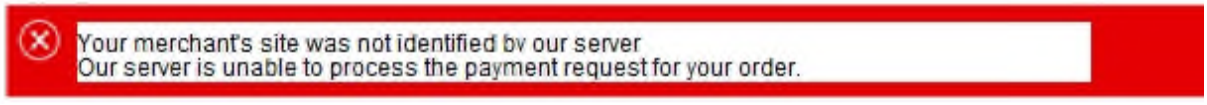
- The EPT number is incorrect or missing

Problem resolution

Verify that variables TPE, societe and lgue are present in the form, spelled correctly, respect the case and respect any possible restrictions regarding format or characters authorized.

8.1.3 Your merchant's site was not identified

Error message



Possible causes

- The company code is incorrect or inexistent

Problem resolution

Verify that variables TPE, societe and lgue are present in the form, spelled correctly, respect the case and respect possible restrictions regarding format and authorized characters.

END OF DOCUMENT