Desjardins

Monetico
Payment

INTEGRATION GUIDE

(ONLINE PAYMENT)

Filename: Monetico_Internet_Payment_Integration_Guide_v2.01
Version no.: 2.01
Date: 2018-02-23

Confidential

Document title: Monetico Payment Integration Guide (Online Payment)
Filename: Monetico_Internet_Payment_Integration_Guide_v2.01
Version number: 2.01
Date: 2018-02-23

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 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
« 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
buyer, customer, client	online shopper

2 Installation of payment interface

2.1 Interfaces

The integration of the Monetico Payment solution with your merchant website involves the implementation of two interfaces in your IT system.

- “Outward” interface: for generation of a payment request form, secured by a seal, that will accompany your client while you redirect them to the Monetico payment server.
- “Return” interface: for receipt of a payment confirmation, that Monetico sends after every payment request

The integration work required calls for advanced programming skills:

- receipt and checking of parameters using the POST method
- handling of character strings
- use of functions or classes compliant with the RFC2104 standard implementing HMAC SHA1 or MD5
- saving of the payment context in a file or a database
- tracking of processing progress step by step in a debugging tool or by programming traces

For your information, examples of these two interfaces are supplied to you with the documentation, in the most common programming languages (PHP, VB.NET, C#.NET, ASP, Python, Ruby, Java and C++). You will find these examples on the Monetico site at:
https://assistance.monetico.ca/en/online-payment/classic-package

You may use these examples as the starting point. However, they must be modified according to the specific characteristics of your environment and application. In particular, the storage of keys must be reviewed in order to use the best confidentiality tools available in your environment.

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 payment service. A link for downloading that security key is sent by email 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`).

This textual representation must be converted into a 20-byte binary string

(operational representation) before use. Please refer to the code examples for more information.

The old key remains recognized by the system when a new key is generated. It is the successful use of the new key (in the test or production environment) that invalidates the old key in that environment..

2.3 Specifications of exchanged messages

2.3.1 Message flow summary

Action	Entity involved
The merchant sever obtains the online shopper's agreement on the goods or services purchased and the price	**Merchant website**
The merchant server collects the payment data …	**Merchant server « Outgoing » interface**
… then creates the sealed payment form	
… and formats a payment page for the online shopper	
The online shopper clicks the payment form button …	
… and accesses the payment server	**Monetico payment server**
The Monetico server validates the seal and initiates the payment dialogue with the online shopper	
The online shopper dialogues with the Monetico server and pays (or doesn't pay) by credit card	
The Monetico server returns a sealed payment result to the merchant server on its « Return » interface.	
The merchant server validates the seal …	**Merchant server « Return » interface**
… then examines the payment result …	
… and returns an acknowledgement to the Monetico server	
The Monetico server displays the payment result for the online shopper [1]	**Monetico payment server**
The online shopper can print (or save) this page[1]	
The server allows the online shopper to return to the merchant website via a hypertext link [1]	
If the online shopper clicks the link, they will leave the Monetico server and return to the merchant website [1]	
The merchant website adapts its dialogue according to the payment result obtained	**Merchant website**

2.3.2 « Outgoing » interface

2.3.2.1 Form creation

The parameters of the terminal and the order data are combined in a sealed HTML

[1] Automated return to the merchant website without further action is available as an option. In this case: the Monetico server will produce a page redirecting the cardholder to the appropriate URL according to the authorization request result. The payment receipt is sent by email.

form in order to transmit the payment request to the Monetico server via the customer's browser. The fields to be completed in the form are shown in the table below.

Field	Description	Comment
version	Version of the payment system used	Current version 3.0
TPE	Merchant’s 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) An ***n***-digit integer where ***n*** is the maximum number of decimals for the currency (optional) A currency in three ISO4217 alphabetical characters (CAD)	Examples: 62.73CAD 10CAD 1024CAD
reference	<u>Unique</u> order reference. Size: 12 alphanumeric characters maximum	Example: ABERTYP00145
texte-libre	Free text area. Size: 3200 characters maximum	
mail	Online shopper’s email address	
lgue	Language code Size: 2 characters	Possible values: FR EN
societe	Alphanumeric code to enable the merchant to use the same virtual EPT for different sites (separate configurations) relating to the same activity	The code is supplied by us. Example: mySite1
url_retour	URL that enables the buyer to go back to the merchant website’s home page	Important: do not confuse these with the “Return” interface URL, also called the payment confirmation URL
url_retour_ok	URL with which the buyer goes back to the merchant’s website following an accepted payment.	
url_retour_err	URL with which the buyer goes back to the merchant’s website following a declined Payment or by clicking on the “Quit” button	
MAC	Seal from the data certification Size: 40 hexadecimal characters	
options	List of options used (can be empty)	**Example:**
	Options are separated from each other by an ‘&’. If the option has a value, its name is separated from its value with ‘=’	**opttest=abc&optbis=123**

List of options:

Options	Description	Comment
aliascb	Alias of the customer's credit card in case of express payment option subscription. Format: [a-zA-Z0-9]{1,64}	**Example:** **aliascb=client1**
forcesaisiecb	Force a customer to enter their credit card in case of express payment option subscription	**Example:** **forcesaisiecb=1**
3dsdebrayable	Allows the forcing of 3DSecure disengagement	**Example:** 3dsdebrayable=1

Note:
When an option's name or value is incorrect, the payment request is aborted and an error message displayed, indicating that the form was not properly completed.

Please refer to the « General Documentation » guide for information about Express Payment.

2.3.2.2 Example of payment form in HTML

```
<form action="https://p.monetico-services.com/paiement.cgi"
        method="post" id="PaymentRequest">
        <input type="hidden" name="version" value="3.0" />
        <input type="hidden" name="TPE" value="1234567" />
        <input type="hidden" name="date" value="16/04/2013:15:25:38" />
        <input type="hidden" name="montant" value="0.01CAD" />
        <input type="hidden" name="reference" value=" yourRF12345" />
        <input type="hidden" name="MAC" value="ca66baf34e37db1a184d05cbcd1ca3a53e1cc045" />
        <input type="hidden" name="url_retour"
            value="http://url.retour.com/ko.cgi?order_ref=yourRF12345" />
        <input type="hidden" name="url_retour_ok"
            value="http://url.retour.com/ok.cgi?order_ref=yourRF12345" />
        <input type="hidden" name="url_retour_err"
            value="http://url.retour.com/err.cgi?order_ref=yourRF12345" />
        <input type="hidden" name="lgue" value=«EN» />
        <input type="hidden" name="societe" value="mySite1" />
        <input type="hidden" name="texte-libre" value="This is a test" />
        <input type="hidden" name="mail" value="onlineshopper@email.com" />
        <input type="submit" name="bouton" value="Credit Card Payment" />
</form>
```

2.3.2.3 Example of payment form in HTML (with Disengageable 3DSecure)

This example describes the second way to implement the Disengageable 3DSecure function (please refer to the Merchant Control Panel for details of the first method).

This second method allows for more precise management of the disengagement process. Unlike the Control Panel that defines a general rule for your EPT, sending the option permits lowering the specification to the site code level.

Please note that sending the option takes priority over the Control Panel configuration. Thus, if the option indicates to disengage whereas the Control Panel specifies the opposite, disengagement will occur.

One can look at the Control Panel configuration as a general rule that can be waived by sending the option.

Below is an example of a form sent to the payment page. You will see that an option is sent in the options field as follows:

- 3dsdebrayable=1

Only the value 1 is accepted for this option.
.
Please note that this field is used in the calculation of the security seal.

```
<form action="https://p.monetico-services.com/paiement.cgi"
        method="post" id="PaymentRequest">
        <input type="hidden" name="version" value="3.0" />
        <input type="hidden" name="TPE" value="1234567" />
        <input type="hidden" name="date" value="16/04/2013:15:25:38" />
        <input type="hidden" name="montant" value="0.01CAD" />
        <input type="hidden" name="reference" value=" yourRF12345" />
        <input type="hidden" name="MAC" value="ca66baf34e37db1a184d05cbcd1ca3a53e1cc045" />
        <input type="hidden" name="url_retour_ok"
            value="http://url.retour.com/ok.cgi?order_ref=yourRF12345" />
        <input type="hidden" name="url_retour_err"
            value="http://url.retour.com/err.cgi?order_ref=yourRF12345" />
        <input type="hidden" name="lgue" value=«EN» />
        <input type="hidden" name="societe" value="mySite1" />
        <input type="hidden" name="texte-libre" value="This is a test" />
        <input type="hidden" name="mail" value="onlineshopper@email.com" />
        <input type="hidden" name="options" value="3dsdebrayable=1" />
        <input type="submit" name="bouton" value="Credit Card Payment" />
</form>
```

2.3.2.4 Form 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 information from the form:

```
<TPE>*<date>*<montant>*<reference>*<texte-libre>*
<version>*<lgue>*<societe>*<mail>*<nbrech>*<dateech1>*<montantech1>*<dat
eech2>*<montantech2>*<dateech3>*<montantech3>*<dateech4>*<montantech4>*<
options>
```

Example for a payment:

```
1234567*05/12/2006:11:55:23*62.73CAD*ABERTYP00145*FreeTextExample*3.0
*FR*mySite1*internaute@sonemail.ca**********
```

2.3.3 « Return » interface

After processing the payment request, the Monetico server directly informs the merchant server of the payment request result by sending an online HTTP request to the payment confirmation URL (“Return interface”). **This URL must be communicated to us upon implementation of the system via the email address support@desjardins.monetico-services.com.**

Note: The return interface is called **after each payment attempt** for a given order, so as to indicate the result. It may thus happen that the return interface receives several declined payment notifications followed by an accepted payment notification for the same order reference. If the customer does not complete the payment process right to the end, for example does not enter their credit card information, the Return interface is not called.

The Return interface allows itself 30 seconds to respond. A timeout is considered an error in the merchant return interface. When an error response is provided and the payment is accepted: a second call is performed (except for a call with immediate redirection to the merchant website).

2.3.3.1 Parameters returned by Monetico

The Return interface is called by the Monetico server with the POST method. The data sent by the Monetico server is described below:

Field	Description	Comment
MAC	Seal resulting from data certification	
date	Order authorization request date in format `DD/MM/YYY_a_HH:MM:SS`	
TPE	Merchant’s virtual EPT number	The Monetico server returns the data as received during the « Outgoing » payment phase.
montant	Order amount formatted as follows: An integer A decimal point (optional) An integer (optional) A currency in three ISO4217 alphabetical characters (`CAD`)	
reference	Unique order reference	
texte-libre	Free text area	
code-retour	The payment result, which may be one of the following: `payetest` payment accepted (TEST only)	In the event of a declined payment, a later authorization can still be delivered for the same reference.

cvx	paiement payment accepted (Production only) Annulation payment declined oui if the card verification number CVN (required for Visa and MasterCard cards) has been entered non else	
vld	Expiry date of the credit card used to make the payment	
brand	Card network code (2 alphabetical characters) AM American Express MC Mastercard VI Visa na not available	The ”na” value is always returned in the test environment.
status3ds	3DSecure exchange indicator: -1: the transaction was not done according to the 3DSecure protocol 1: the transaction was made according to the 3DS protocol and the risk level is low 2: the transaction could not be done according to the 3DSecure protocol, but the cardholder was authenticated by means of 3DSecure 3: the transaction was made according to the 3DS protocol and the risk level is high 4: the transaction was made according to the 3DS protocol and the risk level is very high	
numauto	Authorization number as supplied by the card issuer	Only if authorization was granted
motifrefus	Reason for authorization refusal: Appel phonie (Telephone call): the card issuer requests additional information. **Note: This function is not currently offered by Desjardins.** Refus (Decline) The card issuer declines authorization. Interdit (Prohibited) The card issuer declines authorization. Filtrage (blocked by Fraud Prevention Module as configured by the merchant) scoring: the payment request was blocked	Only if authorization was declined

	by the scoring configuration that the merchant specified in the 3DSecure Fraud Prevention Module: if the decline is linked to a negative 3DSecure authentication received from the the issuer of the cardholder's card.	
originecb	Country code of card issuer (ISO 3166-1 standard)	Only in case of subscription to Fraud Prevention Module
bincb	BIN code of the cardholder's credit card issuer	
hpancb	Irreversible hashing (HMAC-SHA1) of the credit card number used to make the payment (that uniquely identifies a credit card for a given merchant)	
ipclient	IP address of customer who performed the transaction	
originetr	Country code of transaction origin (ISO 3166-1)	
veres	3DSecure VERes state	In case of subscription to the Fraud Prevention Module and the 3DSecure option
pares	3DSecure PARes state	
montantech	Amount of the current instalment	Only for a split payment.
filtragecause	Number of filter type that blocked the payment (see « Fraud Prevention Module – Details » table below) 1: IP address 2: Card number 3: BIN of the card 4: Country of the card 5: Country of the IP 6: Consistency between country of the card / country of the IP 7: Email black list 8: Amount limitation for a credit card during a specified period 9: Number of transactions limitation for a credit card during a specified period 11: Number of transactions limitation for an alias during a specified period 12: Amount limitation for an alias during a specified period 13: Amount limitation for an IP address during a specified period 14: Number of transactions limitation for an IP address during a specified period 15: Card testers 16: Limitation of number of alias per credit	**Only if payment has been blocked by Fraud Prevention Module.** **If multiple filters are blocking, they are all returned and separated by '-'.** **Causes and corresponding values are given in the same order.**

	card	
filtragevaleur	Data that caused the payment blockage	
cbenregistree	Boolean indicating whether the card has been saved under a given alias: : 1: the customer has entered a credit card and it has been saved under the given alias 0: all other cases	**Only in case of express payment subscription**
cbmasquee	The first 6 and the last 4 digits of the credit card, separated by asterisks (*). only during the recording of the credit card	**Only in case of express payment subscription.** **Example:** 123456******7890

Fraud Prevention Module – Details

The payment blocking system is based on nine customizable filters that can be configured via the Control Panel. Each filter is based on a specific criterion such as customer's IP address, email address, credit card issuer country…

Filter type	Analysis criteria	Returned value (blockage cause)	Comment
1	IP address	Customer's IP address	
2	Card number	Hashing of the customer's credit card number	Works only for payment by credit card
3	Card BIN	BIN of the customer's credit card	
4	Country of the card	Country of the customer's credit card	
5	Country of the IP	Country of the customer's IP	
6	Match of country of the card / country of the IP	Country of the credit card Country of the IP	Works only for payment by credit card
7	Email black list	Domain name of the customer's email	
8	Amount limitation for a card during a specified period	Amount accumulated in ($) by the credit card over the given period	Works only for payment by credit card
9	Trans. limitation for a card during a specified period	Number of accumulated payments by the credit card over the given period	
11	Trans. limitation for an alias during a specified period	Number of accumulated payments by the alias over the given period	Only in case of express payment subscription
12	Amount limitation for an alias during a specified period	Amount accumulated in ($) by the alias over the given period	
13	Amount limitation for an IP address during a specified period	Amount accumulated in ($) by the IP address over the given period	

14	Trans. limitation for an IP address during a specified period	Number of accumulated payments by the IP Address	
15	Cards testers	Number of accumulated trans. by the IP address over the given period (in minutes)	
16	Limitation number of alias by card	Aliases already associated with card used for the payment	Only in case of express payment subscription

Example of data sent by the Monetico payment server to the Return interface for a Purchase or Preauthorization payment:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75CA
D&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=010101
&originecb=CAN&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B0
04B7C45&ipclient=127%2e0%2e0%2e1&originetr=CAN&veres=Y&pares=Y
```

Example of data sent by the Monetico payment server to the Return interface for a payment blockage by the Prevention Fraud module

```
TPE=9000001&date=05%2f10%2f2011%5fa%5f15%3a33%3a06&montant=1%2e01CAD
&reference=P1317821466&MAC=70156D2CFF27A9B8AAE5AFEBE590D9CFCAAF9BDC&
texte-libre=Ceci+est+un+test%2c+ne+pas+tenir+compte%2e&code-
retour=Annulation&cvx=oui&vld=0912&brand=MC&status3ds=-
1&motifrefus=filtrage&originecb=CAN&bincb=513283&hpancb=764AD24CFABB
B818E8A7DC61D4D6B4B89EA837ED&ipclient=10%2e45%2e166%2e76&originetr=i
nconnue&veres=&pares=&filtragecause=4-&filtragevaleur=CAN-
```

Example of data sent by the Monetico payment server to the Return interface for a payment with the express payment option

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75CA
D&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=010101
&originecb=CAN&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B0
04B7C45&ipclient=127%2e0%2e0%2e1&originetr=CAN&cbenregistree=1&cbmas
quee=123456******7890
```

Note:
Country values returned are based on the ISO 3166-1 alpha-3 standard.

2.3.3.2 Seal validation

The confirmation message received is sealed by a MAC seal calculated by the Monetico payment server together with the merchant security key assigned to your payment terminal.

A seal validation function must be implemented in the “Return” interface to ensure that there is no falsification of the data contained in the confirmation message of the payment received.

To do this, the function must recalculate the MAC code associated with the message and compare it with that transmitted in the message. If the two codes are identical, the information received is reliable (integrity of the information and authentication of the issuer).

The MAC is calculated using an encryption hashing function combined with a secret key in accordance with the RFC 2104 specifications.

This function will generate the seal from the data to certify and the merchant’s Production security key.

The data to be certified is presented in the form of a concatenation in a specific order of the information sent by the Monetico server:

```
<TPE>*<date>*<montant>*<reference>*<texte-libre>*3.0*<code-
retour>*<cvx>*<vld>*<brand>*<status3ds>*<numauto>*<motifrefus>*<o
riginecb>*<bincb>*<hpancb>*<ipclient>*<originetr>*<veres>*<pares>
*
```

All the fields must be taken into consideration when calculating the MAC even if they are not provided in the response.

Example: if you are subscribed to the Fraud Prevention module and the 3DSecure option and the payment is accepted:

```
1234567*05/12/2006_a_11:55:23*62.75CAD*ABERTYP00145*LeTexteLibre*
3.0*paiement*oui*1208*VI*1*010101**FRA*010101*74E94B03C22D786E0F2
C2CADBFC1C00B004B7C45*127.0.0.1*FRA*Y*Y*
```

Example: if you are not subscribed to the Fraud Prevention module and the payment is accepted:

```
1234567*05/12/2006_a_11:55:23*10CAD*ABERTYP00145*
LeTexteLibre*3.0*paiement*oui*1208*VI*1*010101*********
```

2.3.3.3 Receipt acknowledgement creation

The response sent by the “Return” interface to the Monetico payment server must be one of the two messages presented in the table below, depending solely on the verification of the MAC seal received without taking into account the value of the payment return code, provided that this value is a valid one for the return code field.

Valid seal	Acknowledgement to be sent in text format

Yes	`version=2<LF>`
	`cdr=0<LF>`

No	`version=2<LF>`
	`cdr=1<LF>`

Note: <LF> represents a new line character.

When the Monetico server does not receive the acknowledgement for a validated seal, it sends an email alert to a monitored electronic mailbox specified by the merchant and then makes a second attempt.

This email contains a link allowing for the repetition of the request sent by the Monetico server via the GET method, a code for the error that occurred when calling the confirmation URL, and the acknowledgement sent by the merchant server.

For the test phase, the merchant must give us the address of a regularly monitored electronic mailbox. To go into Production, the merchant server must have sent an acknowledgement with a validated seal for the last three tests. This address must be emailed to our support centre at support@desjardins.monetico-services.com**.**

2.3.4 Address Verification System (AVS)

The solution supports acquirer Address Verification (AVS).
This service allows the issuer to verify the cardholder’s billing address and provides a validation result code. This code can be grouped into 5 categories as follows:

- “exact match”: Same address and same postal code
- "address match": Same address, postal code not validated
- "zip match": Same postal code, address not validated
- "no match": Address and postal code different
- address information not verified

The back-office allows a Monetico agent to activate (or not activate) the AVS service for a given merchant. By default, AVS is inactive.

If the AVS service is activated, the payment page requests input of the billing address of the credit card used (this address may differ from the delivery address).

If the AVS service is activated, the billing address of the credit card used must be provided by the merchant site in emulation mode.

If the AVS service is activated, the billing address of the credit card used for the payment can optionally entered for MOTO transactions. It is not mandatory.

If the AVS service is activated, the back office allows a Desjardins agent to configure the following behaviours for an approved transaction when the response contains the address verification result:

- approval if the authorization request response contains the « exact match », "address match" , "zip match" , "no match" or "Information non verified" status, the acceptor solution ends the transaction with the "approved" status.
- conditional decline: if the authorization request response contains the "no match" status, the acceptor automatically generates a reversal, whereas if the authorization request response contains the « exact match », "address match" or "zip match" status, the acceptor solution ends the transaction with the "approved" status.
- definitive decline: if the authorization request response contains the "address match" or "zip match" or "no match", the acceptor automatically generates a reversal.

The address validation status is shown in the merchant reports when available in the response returned by Monetico.

The address validation status is present in the response returned to the merchant site (in emulation mode) when available in the response returned by Monetico.

3 Requesting an authorization completion

3.1 Description

The objective of the Capture_Paiement (Payment Capture) service is to enable merchants to securely complete previously authorized payments via computer request.

This service can only be used with Electronic Payment Terminals (EPTs) configured in "Preauthorization payment" ("Paiement de préautorisation") mode.

In order to request an authorization completion, the merchant's application must make a request to the Monetico server's web capture service (via a HTTPS message) supplying certain information (order amount, date, reference, the virtual merchant EPT number, etc.) A seal must be calculated in order to certify the exchanged data.

In response to this request, the Monetico server returns the result of the capture request to the merchant's application: accepted or declined.

3.2 Call to Capture request service

3.2.1 Information to be provided

The merchant's application must issue a POST method request via a HTTPS message (TLS) to the Capture_Paiement service on the Monetico servers, containing the following fields:

Field	Description	Comment
version	Version of the payment system used	Current version 3.0
TPE	Virtual merchant EPT number Size: 7 characters	example: `1234567`
date	Date and time of the completion request In format `DD/MM/YYYY:HH:MM:SS`	Example: `05/12/2006:11:55:23`
date_commande	Order date in format `DD/MM/YYYY`	Example: `03/12/2006`
montant	Initial order amount	Format: - An integer - A decimal point (optional) - An integer (optional) - A currency in three ISO4217 alphabetical *characters (CAD)*
montant_a_capturer	Completion request amount	
montant_deja_capture	Amount already completed for this order	
montant_restant	Balance of the order after this requested completion	

		Examples: 62.73CAD 10CAD 1024CAD
reference	Order reference	Example: ABERTYP00145
texte-libre	Free text area Size: 3,200 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 with different sites (separate configurations) relating to the same activity	This code is supplied by our services. Example: mySite1
MAC	Seal from data certification Size: 40 hexadecimal characters	
stoprecurrence	Forces termination of recurrence for EPTs in recurrent payment	This parameter is optional
phonie	The value of this field is sent in the event of a telephone authorization .	This parameter is optional. **NB: This service is not currently offered by Desjardins.**

The fields of this request (except for the version and the amounts) must all be encoded in HTML. The encoding specifications are described at the end of this document.

3.2.2 Seal calculation

The seal (to be entered in the MAC field) must be calculated using an encryption hashing function combined with a secret key in accordance with the RFC 2104 specifications. The data to be certified is presented in the form of a concatenation in a specific order of the information from the form:

```
<TPE>*<date>*<montant_a_capturer><montant_deja_capture><montant_restant>*<reference>*<texte-libre>* <version>*<lgue>*<societe>*
```

3.2.3 Capture request examples

Example 1: partial completion of $62 for an initial order of $100.

String used for calculation of the seal:

```
1234567*05/12/2006:11:55:23*62.00CAD0CAD38CAD*ABERTYP00145*FreeTextExample*3.0*FR*mySite1*
```

Request:

```
POST /capture_paiement.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: 307

          version=3.0
          &TPE=1234567
          &date=05%2F12%2F2006%3A11%3A55%3A23
          &date_commande=03%2F12%2F2006
          &montant=100.00CAD
          &montant_a_capturer=62.00CAD
          &montant_deja_capture=0CAD
          &montant_restant=38.00CAD
          &reference=ABERTPY00145
          &texte-libre=FreeTextExample
          &lgue=EN
          &societe=mySite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

The sum of the 3 amounts must be equal to the initial order amount

Example 2: total completion of an order of $100

String used for calculation of the seal:

```
1234567*05/12/2006:11:55:23*100.00CAD0CAD0CAD*ABERTYP00145*
FreeTextExample*3.0*FR*mySite1*
```

Request:

```
POST /capture_paiement.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: 305

          version=3.0
          &TPE=1234567
          &date=05%2F12%2F2006%3A11%3A55%3A23
          &date_commande=03%2F12%2F2006
          &montant=100.00CAD
          &montant_a_capturer=100.00CAD
          &montant_deja_capture=0CAD
          &montant_restant=0CAD
          &reference=ABERTPY00145
          &texte-libre=FreeTextExample
          &lgue=EN
          &societe=mySite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

The 2 amounts must be identical

3.3 Capture request response

3.3.1 Information returned

In response to the capture request, the merchant's application receives an acknowledgment message from the Monetico server. The message is a "text/plain" MIME type document that specifies the result of the capture.

It contains the following fields separated by a CHR(10) character:

Field	Description	Comment
version	Version number of the acknowledgement message	Current version. 1.0
reference	Order reference	Example: ABERTYP00145
cdr	Return code indicating the result of the completion	Possible values: 1: completion accepted 0: completion declined -1: error
lib	Detailed message specifying the nature of the return code	See below for list of possible messages
aut	Payment authorization number if the completion has been accepted	
phonie	Authorization declined for a "phone call" type reason	This field is only present if the Phone field is present and was included in the calling request **NB: This function is not currently offered by Desjardins.**

If cdr differs from 1 the completion was not successful.

The following table contains the list of possible messages.

cdr	Message	Description	Comment
1	**paiement accepte**	The authorization has been given and the completion has been done	
1	**commande annulee**	The cancellation request has been taken into account and the order has been cancelled	
1	**recurrence stoppee**	The request for permanent cancellation of renewal was taken into account	Only for recurring payment .
0	**commande non authentifiee**	The reference does not match an order	Check the reference and date_commande parameters
0	**commande expiree**	The order date has exceeded the permitted time delay(+/- 24h)	
0	**commande grillee**	The maximum number of attempts to enter the card number has been reached (three attempts allowed)	The order is no longer accepted by the payment server
0	**autorisation refusee**	The authorization is declined	The completion was not done
0	**la commande est deja annulee**	The order was cancelled at a previous request	No request will be accepted for this order

0	**paiement deja accepte**	A request for authorization has already been given for this order	
-1	**signature non valide**	The MAC signature is invalid	
-1	**verification echouee (mode de paiement)**	The payment method is not compatible with this request	For example: Purchase payment, since completion is done automatically
-1	**la demande ne peut aboutir**	The capture request is formulated incorrectly	Check the parameters sent
-1	**montant errone**	One of the amounts sent is incorrectly formatted	Check the four amount parameters
-1	**commercant non identifie**	The parameters used to identify the merchant website are not correct	Check fields societe, lgue and TPE
-1	**traitement en cours**	The order is being processed	
-1	**date erronee**	The date is not in the required format	Check the date parameter
-1	**autre traitement en cours**	Another transaction is being processed for the same reference	Repeat the request
-1	**probleme technique**	A technical problem has occurred	Repeat the request

3.3.2 Examples of messages returned

- Case of accepted capture

```
version=1.0
reference=000000000145
cdr=1
lib=paiement
accepte
aut=123456
```

- Case of accepted cancellation

```
version=1.0
reference=000000000145
cdr=1
lib=commande
annulee
aut=123456
```

- Case of declined authorization without the telephone authorization field provided

```
version=1.0
reference=000000000145
cdr=0
lib=autorisation refusee
```

- Case of declined authorization for reason of telephone call with telephone field completed with “yes”

```
version=1.0
reference=000000000145
cdr=0
```

```
lib=autorisation
refusee
phonie=yes
```

- Case of declined authorization for other reason with telephone field completed with “yes”

```
version=1.0
reference=000000000145
cdr=0
lib=autorisation refusee
```

- Case of declined completion prior to authorization request

```
version=1.0
reference=000000000145
cdr=0
lib=commande non authentifiee
```

- Case of error

```
version=1.0
reference=00000
0000145 cdr=-1
lib=commercant non identifie
```

4 Requesting a payment cancellation

4.1 Payment cancellation

In the event that the merchant has requested a payment but does not wish to complete it (goods not available, customer cancelled the order, etc.) they can notify the Monetico server of the cancellation of their payment request.

To do this, they request the capture service as described in the previous section, specifying the amount to be cancelled and the balance amount as 0CAD.

Example: cancelling an order with an initial amount of $100

String used for calculation of the seal:

```
1234567*05/12/2006:11:55:23*0CAD0CAD0CAD*ABERTYP00145*Exemp
leTexteLibre*3.0*FR*mySite1*
```

Request:

```
POST /capture_paiement.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: 299

            version=3.0
            &TPE=1234567
            &date=05%2F12%2F2006%3A11%3A55%3A23
            &date_commande=03%2F12%2F2006
            &montant=100.00CAD
            &montant_a_capturer=0CAD
            &montant_deja_capture=0CAD
            &montant_restant=0CAD
            &reference=ABERTPY00145
            &texte-libre=FreeTextExample
            &lgue=EN
            &societe=mySite1
            &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

The amount to capture and the amount remaining must be = zero

The amount already captured must correspond to the order history

This capture can be made if your EPT is configured for Preauthorization payment. If successful, no subsequent completion can be done.

5 Refund (Recrédit) service

5.1 Description

The objective of the Récrédit_Paiement service (Refund service) is to enable merchants to securely refund their clients part of the amount of their purchase or the total amount of their purchase via the Internet.

In order to request a refund, the merchant's application must make a request using the "Recrédit" web service to the Monetico server (by means of a HTTPS message) supplying certain information (refund amount, date, reference, the virtual merchant EPT number, etc.). A seal must be calculated in order to certify the data exchanged.

In response to this request, the Monetico server returns the result of the refund request to the merchant's application: accepted or declined.

5.2 Refund service request

5.2.1 Information to be provided

The merchant's application must send a POST method request via an HTTPS (SSL V3) message to the Recredit_Paiement service on the Monetico servers, containing the following fields:

Field	Description	Comment
version	Version of the payment system used	Current version 3.0
TPE	Virtual merchant EPT number Size: 7 characters	example: 1234567
date	Date and time of the refund request in format DD/MM/YYYY:HH:MM:SS	Example: 05/12/2006:11:55:23
date_commande	Initial order date in format DD/MM/YYYY	Example: 03/12/2006
date_remise	Date on which the completion process was initiated in format DD/MM/YYYY	Example: 04/12/2006 This date will be the same as date_commande in the case of an EPT configured in Purchase payment mode
num_autorisation	Authorization number sent by Monetico server for the authorization request	Example: 1234A6
montant	Initial order amount	Format: - An integer - A decimal point (optional) - An integer (optional) - A currency in three ISO4217 alphabetical characters (CAD)
montant_recredit	Amount to be refunded	
montant_possible	Maximum refund amount authorized for the transaction	

		Examples: 62.73CAD 10CAD 1024CAD
reference	Reference of the order to be refunded	Example: ABERTYP00145
texte-libre	Free text area Size: 3200 characters maximum	
lgue	Language code (upper case) Size: 2 characters	FR, EN
societe	Alphanumeric code for internal use only to enable the merchant to use the same virtual EPT for different sites (separate configurations) relating to the same activity	The code is supplied by us. Example: mySite1
MAC	Seal from data certification Size: 40 hexadecimal characters	

Note: the "montant_possible" ("possible_amount")field is required for the merchant server and the Monetico server to be in synchronization.
If any amount has already been refunded under this authorization number, it must be deducted by the merchant. For example, **if** for a **$100** order, a refund of **$10** has already been made, the next refund will have a "*possible_amount*" value of **$90**.

5.2.2 Seal calculation

The seal (to enter in the MAC field) is calculated using an encryption hashing function combined with a secret key in accordance with the RFC 2104 specifications. The data to be certified is presented in the form of a concatenation in a specific order of the request information:

```
<TPE>*<date>*<montant_recredit><montant_possible>*
<reference>*<texte-libre>*<version>*<lgue>*<societe>*
```

5.2.3 IP and number of refunds control

For security reasons, refund requests can only be sent from servers with an IP address known to our services. In addition, every IP address is limited in the daily number of refund requests that it is authorized to carry out.

Before you can carry out refund requests in the Production environment, you must email us the list of IP addresses to be authorized as well as the maximum number of daily refunds for each IP address. Please send this information to support@desjardins.monetico-services.com.

For reasons of convenience, no controls are imposed for refund requests in the test environment.

5.2.4 Refund request example (Recrédit)

Example 1: partial refund of $32 for an order of $100

String used for calculation of the seal:

```
                        1234567*05/12/2006:11:55:23*32.00CAD100CAD*ABERTYP00145*
          FreeTextExample*3.0*FR*mySite1*
```

Request:

```
POST /recredit_paiement.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: 328

         version=3.0
         &TPE=1234567
         &date=05%2F12%2F2006%3A11%3A55%3A23
         &date_commande=03%2F12%2F2006
         &date_remise=04%2F12%2F2006
         &num_autorisation=1234A6
         &montant=100.00CAD
         &montant_recredit=32.00CAD
         &montant_possible=100CAD
         &reference=ABERTPY00145
         &texte-libre=FreeTextExample
         &lgue=EN
         &societe=mySite1
         &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

If successful, a refund of a maximum amount of $68 can still be made

Example 2: total refund of an order of $100

String used for calculation of the seal:

```
        1234567*05/12/2006:11:55:23*100CAD100CAD*ABERTYP00145*
        FreeTextExample*3.0*FR*mySite1*
```

Request:

```
        POST /recredit_paiement.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: 326

                version=3.0
                &TPE=1234567
                &date=05%2F12%2F2006%3A11%3A55%3A23
                &date_commande=03%2F12%2F2006
                &date_remise=04%2F12%2F2006
                &num_autorisation=1234A6
                &montant=100.00CAD
                &montant_recredit=100CAD
                &montant_possible=100CAD
                &reference=ABERTPY00145
                &texte-libre=FreeTextExample
                &lgue=EN
                &societe=mySite1
                &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

5.3 Refund request response

5.3.1 Information returned

In response to the refund request, the merchant's application receives an acknowledgment message from the Monetico server. The message is a "text/plain" MIME type document that specifies the refund result.

It contains the following fields separated by a CHR(10) character:

Field	Description	Comment
version	Version number of the acknowledgement message	Current version 1.0
reference	Order reference	Example: ABERTYP00145
cdr	Return code indicating the result of the refund	Possible values: 0: refund successful <0: error
lib	Message specifying the nature of the return code	See below for list of possible messages

The following table lists the possible messages:

cdr	Message	Description	Comment
0	**recredit effectue**	The refund request has been taken into account	
-1	**recredit refuse**	The refund request has not been taken into account	
-30	**Commercant non identifie**	The parameters used to identify the merchant website are incorrect	Check the societe, TPE and lgue parameters
-31	**signature non validee**	The MAC signature is invalid	
-32	**recredit non autorise**	Your EPT is not authorized to do refunds	Contact support@desjardins.monetico-services.com
-33	**demande de recredit expiree**	The refund date has exceeded the permitted time delay (+/- 24h)	Check the date parameter
-34	**montant de recredit errone**	The amount to refund is incorrect	Check the refund amount parameter
-35	**Les montants transmis sont incorrects**	The amounts sent are not in sync with those of the Monetico server	Check fields montant_recredit and montant_possible
-36	**le maximum de recredit a été atteint**	The maximum number of refund transactions for your EPT has been reached	
-37	**la commande est inexistante**	There is no such order	Check that the fields used to identify the order are correct
-38	**la commande ne peut pas donner lieu a un recredit**	The order has not been paid so no refund may be given	
-39	**le paiement est inexistent**	An authorization request has already been given for this order	
-40	**le montant total des recredits ne peut depasser le seuil**	The amount to refund is incorrect	
-41	**un probleme technique est survenu**	Technical problem	Repeat the request
-42	**la devise est incorrecte**	The currency transmitted is not the currency of the order	Check the currency parameter (devise)
-43	**parametres invalides**	One or more parameters are not in the required format	Check the length of the fields and the formats of dates
-44	**autre traitement en cours**	Another transaction is being processed for the same reference; the process may be other than recredit_paiement	Repeat the request

5.3.2 Examples of messages returned

- Case of accepted refund (recredit)

```
version=1.0
reference=000000000145
cdr=0
lib=recredit effectue
```

- Case of error

```
version=1.0
reference=000000000145
cdr=-31
lib=les montants transmis sont incorrects
```

6 Installation aid

6.1 Putting an EPT into production

You must make a request to support@desjardins.monetico-services.com in order to put an EPT into Production. Before doing so, the last three payments performed in the Test environment must have returned valid acknowledgements.

6.2 Frequently Asked Questions

Can the payment page be customized?
Yes. Please refer to document “Monetico Payment – Payment Page Customization”.

How do I apply my logo to your payment page?
You must email us either the URL of an image representing your logo or the logo itself as an attachment. The image must be in GIF format and have a maximum size of 120x120 pixels.

How much time does my customer have to enter their credit card after ordering on my website?
The online shopper has 45 minutes from their arrival on the payment page to enter their credit card information. After that time has expired, no entry will be allowed.

How many tries are allowed for entry of the credit card information?
The maximum number of tries is 4.

Where can test card numbers be obtained?
On the payment page, you will see a blinking « TEST » icon. By clicking it, a window will display different test card numbers. When one of them is selected, the payment page form will automatically be populated. Below are the test cards available:

- two 16-digit cards: one of which causes a payment to be approved and the other will cause a decline
- two 15-digit cards (foreign cards): as above

What languages are supported by the payment page?

- French
- English

Is it possible to be advised by email of each payment request?
A notification can be emailed for each authorization request (an authorization request is performed if the card format has been validated). You must request activation of this option by contacting Technical Support.

How can I obtain the cardholder’s name and address?
We do not have the cardholder’s contact information on our payment server. In fact, the online shopper enters only their card information (card number, expiry date and

visual cryptogram). We do not envision having the merchant transmit this information to us in the context of our payment solution. Neither do we anticipate deducing the cardholder's identity from their card information.

Can a payment be refunded?

Yes, by requesting the Refund (or Re-credit) option from your account manager. The function would then be available on your Merchant Control Panel.

What do the different « URL_RETOUR » parameters mean?

- `url_retour`: corresponds to the link displayed at the bottom of our payment page, when an error is made in the call to our payment page (order already paid, order expired, etc.). This link allows the online shopper to return to your website.
- `url_retour_ok`: corresponds to the link (allows the online shopper to return to your website) displayed at the bottom of our payment page, if the payment is approved.
- `url_retour_err`: corresponds to the link (allows the online shopper to return to your website) displayed at the bottom of our payment page, if the payment is declined, or upon the first display of the payment page.

These URLs must not be confused with the « Return » interface URL.

What is the « CGI2 confirmation URL » used for?

This is your « Return » interface URL, whose role is to receive the payment confirmation message issued by the Monetico server.

Where is the « CGI2 confirmation URL » configured?

This URL is stored in our database. You must provide it to us when your solution is implemented. You must also notify us of any address change for your « Return » interface (by contacting Technical Support).

What do I do if I receive a « CGI2 NOT OK » error?

First, you must do the following basic checks:

- Is the « Return » interface that you provided us valid?
- Is this address externally accessible on your server?
- Is the port for addressing your « Return » interface 80 (http) or 443 (https)? Our server accepts only these two ports.

If the problem persists, please perform the following additional verifications:

- The processing between the return from our server and your acknowledgement must not take too long (less than 30 seconds)
- There must have been no redirection done upon receipt of the payment return code
- The format of the acknowledgement sent must be that expected for a valid seal.

How do I know the meaning of an error code in an email sent in case of an incorrect acknowledgement?

These error codes are specific to the cURL software. Their descriptions are available at: http://curl.haxx.se/libcurl/c/libcurl-errors.html

Why does my «CGI2 Confirmation URL » receive different return codes for the same reference?

Your customers have 4 tries to enter their card information for the same reference within a maximum delay of 45 minutes.

After each try, we send the result on your confirmation URL. So you could receive several decline notifications (return code « Cancellation ») before eventually receiving a payment notification (return code « Payment ») for the same reference.

Below is a sample scenario with several calls to the confirmation URL:

A customer wishes to pay for reference ref0001 but does not obtain authorization for the credit card used. Our server will send a decline notification:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2
e75EUR&reference=ref0001&MAC=e4359a2c18d86cf2e4b0e646016c202e89
947b04&texte-libre=LeTexteLibre&code-
retour=Cancellation&cvx=oui&vld=1208&brand=VI&status3ds=1&motif
refus=Refus&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0
F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&
veres=Y&pares=Y
```

The customer can try again, so uses a second credit card to pay reference ref0001. The payment is approved this time.

Our server will send a payment notification:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f12%3a15%3a33&montant=62%2
e75EUR&reference=ref0001&MAC=f4562a2c18d86cfdbaf646016c202e8994
5841&texte-libre=LeTexteLibre&code-
retour=payment&cvx=oui&vld=1210&brand=VI&status3ds=1&numauto=01
0101&originecb=FRA&bincb=010101&hpancb=12754C03C22D786E0F2C2CAD
BFC1C00A25df6322&ipclient=127%2e0%2e0%2e1&originetr=FRA&veres=Y
&pares=Y
```

I get error code 0 in the email returned for an incorrect acknowledgement?

Your confirmation URL did not send the expected acknowledgement for a validated seal.

I get the message « This EPT is closed » for a payment request on the TEST server?

The TEST TPEs that are unused for 15 consecutive days are automatically closed to our services. They are not, however, deleted. You can use the Reopen a TEST EPT function by logging on to your Merchant Control Panel.

Is it possible to have a EPT for multiple sites?

Yes, but first a request must be sent to your account manager. The different sites respond to the same activity. Since the configuration is specific to each site, you must transmit all the information to us (return URLs, « Return » interface address, logo, etc.)

Can a payment report file be obtained?

Such a report can be provided by your financial institution. Please contact your account manager.

6.3 The most common problems

6.3.1 Security seal calculation problem

Payment page error message

« The information sent by your merchant has an invalid signature: The required security level was not reached. Our server is unable to process the payment request for your order. »

error message in capture request

```
version=1.0
reference=<votre référence>
cdr=-1
lib=signature non valide
```

error message in recrédit request

```
version=1.0
reference=<votre référence>
cdr=-31
lib= signature non validee
```

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

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.

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.

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 ou MD5),
- Contact our Technical Support to verify together that you are using the correct key and to validate that your form version (« version » field) matches that configured in our system.

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.

6.3.2 The merchant cannot be identified

Payment page error message

« Your merchant website cannot be identified by our server. We cannot process the payment request for your order. »

capture request error message

```
version=1.0
reference=<votre référence>
cdr=-1
lib=commercant non identifie
```

recrédit request error message

```
version=1.0
reference=<votre référence>
cdr=-30
lib= Commercant non identifie
```

Possible causes

- The EPT number is incorrect or inexistent
- The company code is incorrect or inexistent
- The language code is incorrect or inexistent
- The merchant server IP address is not authorized to do refunds

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.

6.3.3 The order has already been processed

Error message

« Your order has already been processed. »

Possible causes

You have provided an order reference that was used for a previous transaction.

Problem resolution

You must generate a new order reference that is unique.

6.3.4 The order validity date has expired

Error message

« The order validity date has expired. »

Possible causes

- either the order reference has been outstanding for too long (typically for more than one hour)
- or the order form was created too long ago, typically more than 12 hours.

Problem resolution

- Test a form updated with a new order reference
- Test a new form and check your server's system date

6.3.5 The payment mode used is unavailable

Error message

« Payment mode unavailable. »

Possible causes

- either there is a syntax error in the form submitted
- or it involves a payment mode that the merchant does not use

Problem resolution

Verify that variables in the form are spelled correctly, respect the case and respect possible restrictions regarding format and authorized characters

Verify that you are not using a payment mode to which you are not subscribed.

6.3.6 The order cannot be authenticated

Error message

```
version=1.0
reference=<votre référence>
cdr=0
lib=commande non authentifiee
```

Possible causes

- The reference is incorrect or inexistent
- The order date is incorrect or inexistent

Problem resolution

Verify that variables reference and date are present in the form, spelled correctly, respect the case and respect possible restrictions regarding format and authorized characters.
Verify that the order reference to be captured was really authorized or recorded on the date provided.

6.3.7 The amounts are incorrect

Error message

```
version=1.0
reference=<votre référence>
cdr=-1
lib=montant errone
```

Possible causes

- One of the transmitted amounts is incorrect
- The sum of the amounts is incorrect

Problem resolution

Verify that variables montant, montant_a_capturer, montant_deja_capture and montant_restant are present in the form, spelled correctly, respect the case and respect possible restrictions regarding format and authorized characters.
Verify that the sum of the values of variables montant_a_capturer, montant_deja_capture and montant_restant is equal to the value of montant for a preauthorization completion.
Verify that the values of variables montant_a_capturer and montant_restant are equal to zero for a cancellation.

7 Summary file

The information that we transmit to your Return interface can also be made available to you in a consolidated manner via a summary file.

The sending of this file or its suspension can be set up from your Control Panel[1]. You can customize the following parameters:

- the sending frequency: daily, weekly or monthly,
- the desired order states: Recorded, Declined, Blocked, Paid, Cancelled,
- the format of the file that you wish to receive: CSV or XML
- the transmission type: by email or by FTP
- the configuration of the email or FTP transmission.

The file transmitted to you contains the following fields:

Field	Description	Comment
1	completion date	format `YYYY-MM-DD`
2	virtual EPT number	
3	order reference	as supplied by the merchant

4	order state: according to the selection made by the merchant in the list of the requested states	AN: you have cancelled the payment request AU: successfully recorded payments awaiting completion GR: order cancelled after 4 failed attempts PA: the payment was authorized and completed PP: partial payment successfully stored and awaiting completion (not currently supported) RE: payment authorization was not granted
5	Date of payment request	format YYYY-MM-DD
6	Time of payment request	format hh:mm:ss
7	Transaction amount, formatted as follows: - An integer - A decimal point (optional) - An integer (optional)	
8	Currency of the transaction	In 3 alphabetical characters ISO4217 (CAD)
9	Authorization number as supplied by the card issuer	Only if authorization was granted
10	Acknowledgement receipt of merchant return interface	OK: your return interface submitted a valid acknowledgement to us NOK: your return interface failed to submit a valid acknowledgement to us
11	Archival reference	Only in case of subscription to Fraud Prevention Module
12	Card type	AM: American Express MC: Mastercard VI: Visa Only in case of subscription to Fraud Prevention Module
13	Card validity date	format MMYY Only in case of subscription to Fraud Prevention Module
14	Presence of visual cryptogram	oui non Only in case of subscription to Fraud Prevention Module
15	Free text as supplied by the merchant	

[1] A help page supports you with the configuration that best suits your needs.

8 Technical assistance

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.

9 Appendices

9.1 General requirements for the HTML encoding 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_ENCODED" 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).

9.2 Specific requirements depending on the field

Field	Content / format before HTML encoding	Maximum size after HTML encoding
TPE	A-Z a-z 0-9	7
version	3.0	Fixed
date		50
montant		20
reference	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	20
texte-libre	A-Z a-z 0-9	3200
URLs		2048

mail		255
brech	2-4	1
dateechN		50
montantechN		20
date_commande		50
montant_a_capture		20
montant_deja_capture		20
montant_restant		20
phonie	**A-Z a-z 0-9**	50
num_autorisation		10
montant_recredit		20
montant_possible		20
stoprecurrence	**YES**	3

9.3 Service URLs

9.3.1 Test environment

The role of our test server is to enable you to validate your developments. Of course, all operations carried out by our test payment server are fictitious and do not result in any real financial transaction.

For carrying out payment requests in this environment we provide test payment cards, that are accessible by clicking on the “Test card” icon on the payment page.

The test environments are available at the following addresses:

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

The test merchant Control Panel allows you to manage and control the payments carried out in the test environment. It is available at the following address:

- https://www.monetico-services.com/en/test/identification/default.cgi

9.3.2 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/paiement.cgi
- https://p.monetico-services.com/capture_paiement.cgi
- https://p.monetico-services.com/recredit_paiement.cgi

You can consult the payments performed on your EPT through the merchant Control Panel available at the following address:

- https://www.monetico-services.com/fr

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

END OF DOCUMENT