Monetico
Paiement

Secure payment over the Internet

Technical documentation

EURO
INFORMATION

CONTENTS

1 Setting up the payment interface

1.1 Introduction

Integrating the Monetico Paiement payment platform in the bank card payment process on your site consists in implementing two interfaces in your information system:

- "Request" interface: generation of a payment request form, secured with a seal, which will accompany your customer when you direct them to our payment platform
- "Response" interface: receipt of payment confirmation that we send after every payment request

The work to be carried out requires advanced programming skills:

- to receive and control settings in POST method
- to handle character strings
- to use a function or a class compliant with RFC2104 implementing HMAC SHA1
- to save the payment context in a file or database
- to monitor the step-by-step sequence of a program in a debugging tool or by programming traces.

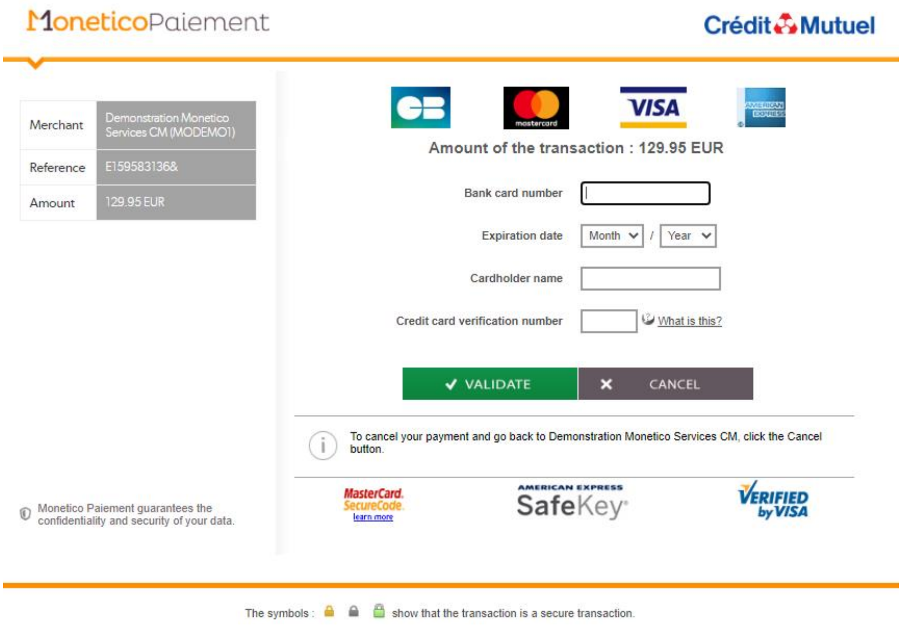
For information, examples of these two interfaces are provided with the documentation, in the most common programming languages (PHP, C#.NET, Python, Ruby, Java and C++).

You can use these examples as a starting point, but you will have to modify them according to your environment and your application. In particular, storage of keys needs to be reviewed to exploit the best confidentiality tools available in your environment.

1.2 Payment form display modes

Monetico Paiement offers two display modes for the payment form:

- “Full form” display: the payment page has Monetico Paiement branding and graphical chart and contains all the information of the payment (information concerning merchant, payment …).



Merchant	Demonstration Monetico Services CM (MODEMO1)
Reference	E1595831368
Amount	129.95 EUR

Monetico Paiement guarantees the confidentiality and security of your data.

Amount of the transaction : 129.95 EUR

Bank card number

Expiration date Month / Year

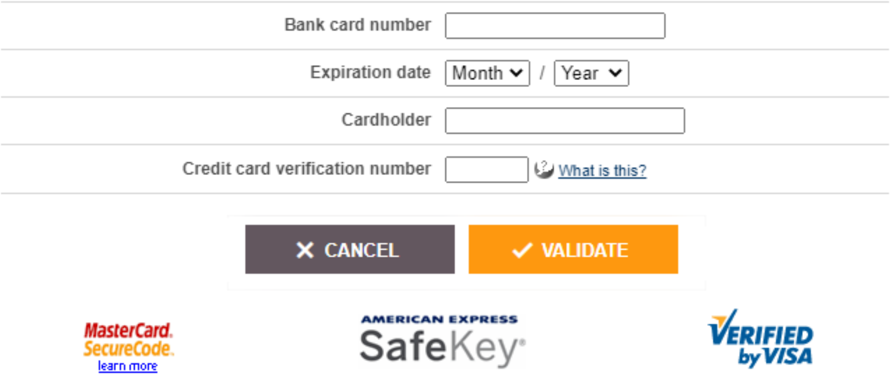
Cardholder name

Credit card verification number What is this?

To cancel your payment and go back to Demonstration Monetico Services CM, click the Cancel button.

The symbols : 🔒 🔒 🔒 show that the transaction is a secure transaction.

- “Minimalist form” display: the payment page only contains fields concerning the bank card information. This display should be preferred over the “full form” if you are looking for a more efficient and optimized integration of the payment functionality into you sales tunnel.



Bank card number

Expiration date Month / Year

Cardholder

Credit card verification number What is this?

1.2.1 “Full form” display

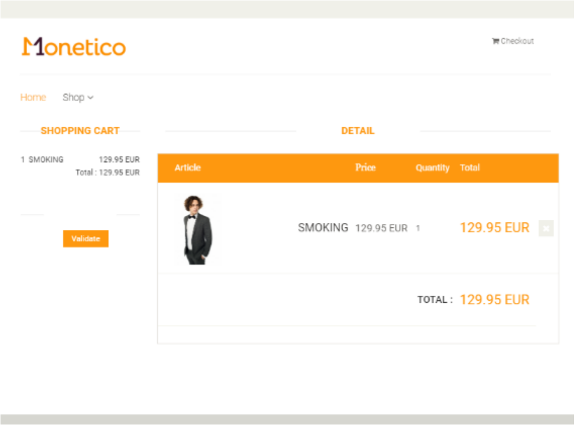
In this mode, the Monetico Paiement payment page is fully displayed with all the elements:

- a header and a footer with the Monetico Paiement and bank logos
- the details concerning the payment
- the available schemes
- the input fields for card information

The full display mode is recommended:

- if you want to reassure the customer : the logo Monetico Paiement and the logo of the bank are easily visible. The secured URL is also an element of reassurance.
- if a clear separation between your web site and the payment page is preferred.

As an example of the web integration: at the end of your checkout process, your customer is redirected to the page Monetico Paiement in order to pay his order.



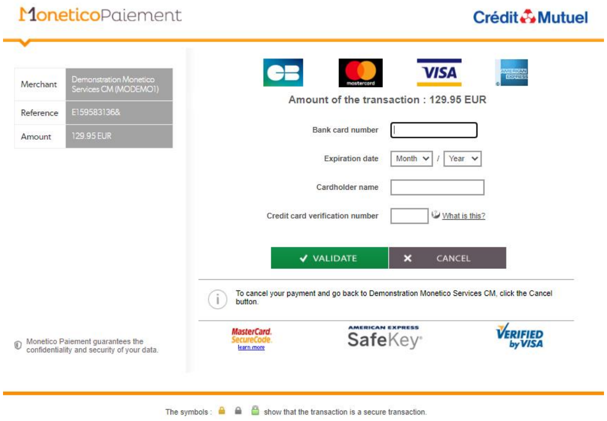
SHOPPING CART

1 SMOKING 129.95 EUR
Total : 129.95 EUR

DETAIL

Article	Price	Quantity	Total
SMOKING	129.95 EUR	1	129.95 EUR

TOTAL : 129.95 EUR



Merchant	Demonstration Monetico Services CM (MODEMO1)
Reference	E1595831368
Amount	129.95 EUR

Amount of the transaction : 129.95 EUR

Bank card number
Expiration date Month / Year
Cardholder name
Credit card verification number What is this?

To cancel your payment and go back to Demonstration Monetico Services CM, click the Cancel button.

Monetico Paiement guarantees the confidentiality and security of your data.

The symbols : 🔒 🔒 🔒 show that the transaction is a secure transaction.

1.2.2 “Light form” display

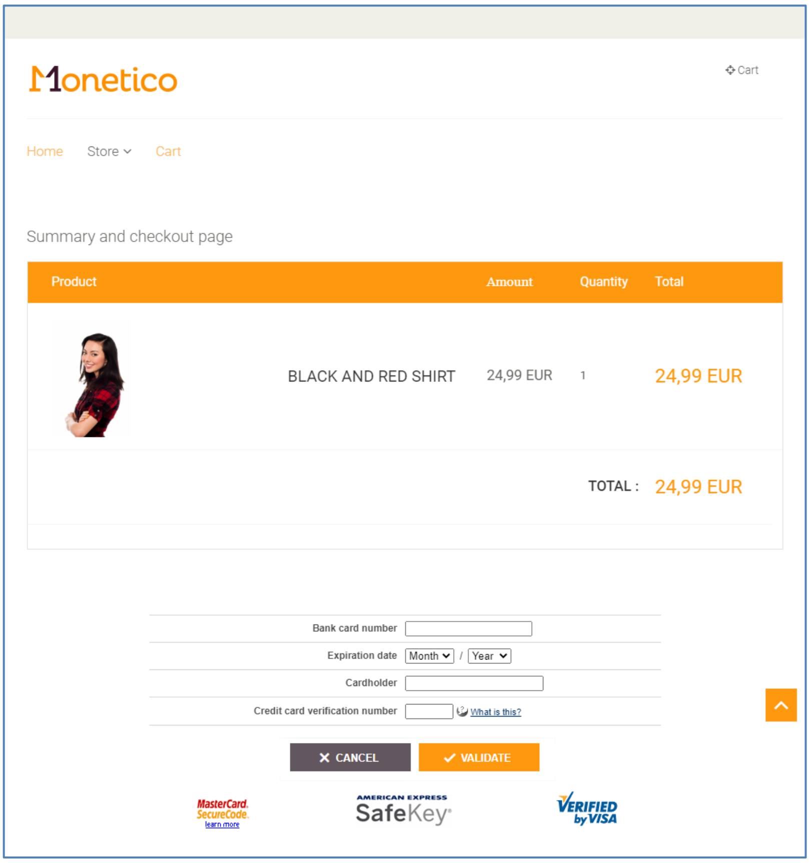
In this mode, the Monetico Paiement payment page is displayed with only required elements:

- the input fields for card information

The “Light form” mode is recommended:

- if the payment process is included in your web site or mobile application in order to have a coherent and shorter order check out.

As an example of the web integration: your customer stays on your web site and fills his bank card information directly on the Monetico Paiement secured page



Summary and checkout page

Product		Amount	Quantity	Total
	BLACK AND RED SHIRT	24,99 EUR	1	24,99 EUR
			TOTAL :	24,99 EUR

Bank card number	
Expiration date	Month / Year
Cardholder	
Credit card verification number	What is this?

During the payment process, when a new page must be displayed (3DSecure process or payment result), it is possible to choose the behavior of the Monetico Paiement page:

- The new page is displayed in a different page : your client leaves your web site or mobile application
- The new page is displayed on the reserved area on your web site (iframe) or mobile application (webview).

You have to choose your preferred behavior during the setup of the « light form » option.

1.2.3 Graphical customization of the Monetico Paiement payment form

Regardless of the chosen display mode, graphical customization options (borders colors, background colors, font colors, logos, headers, buttons …) are available to ensure that the purchasing process is as uniform as possible.

Find more details on the payment page on Monetico paiement web site (https://www.monetico-paiement.fr/fr/piloter-suivre/parametrage/page-de-paiement.html).

1.3 Merchant security key

A security key, specific to each POS, intended to certify the data exchanged between the merchant's server and the Monetico Paiement secure payment server, is required for using the bank card payment service. A link to download this security key is sent by our support centre to the merchant.

You may request for a new key to be regenerated, periodically or for events such as a production launch, a change of web host, a change of service provider, etc.
It is the merchant's responsibility to keep this key safe and confidential by using the best tools available in their environment.

The security key is represented externally by 40 hexadecimal characters (for example: `0123456789ABCDEF0123456789ABCDEF01234567`).
This external representation must be converted into a string of 20 bytes (operational representation) prior to use.

The former key will still be recognised by the system when generating a new key. Successful use of the new key (in a test environment, in a production environment) will definitively invalidate the former key (for the relevant environment).

1.4 Specifications of messages exchanged

1.4.1 Reminder of the process

Action	Participant
The merchant's server gets the web user's consent regarding the item and the price	**Merchant website**
The merchant's server collects the payment data...	**"Request" interface on the merchant's server**
… then creates the sealed payment form	
… then formats this payment form for the web user	
The web user clicks on the button corresponding to the payment form...	
… and accesses the payment server	**Payment server of the bank**
The bank server verifies the validity of the seal and begins the payment dialogue with the web user	
The web user dialogues with the bank server and pays (or doesn't pay) by bank card	
The bank server returns a sealed payment result to the merchant's server on their "Response" interface	
The merchant's server verifies the seal's validity...	**"Response" interface on the merchant's server**
… then takes into account the payment result …	
… then returns acknowledgement of receipt to the bank server	
The server shows the payment result to the web user[1]	**Bank payment server**
The web user can print (or save) this page[1]	
The server asks the web user if they want to return to the merchant's site via a link[1]	
It the customer follows this link, they will quit the payment server and return to the merchant's site[1]	
The merchant's site adapts its dialogue depending on the payment result received	**Merchant's web site**

[1] Automatic return to the merchant's site without any additional action by the user is available as an option. In this case, the Monetico Paiement server will produce a page redirecting the card holder to the relevant URL depending on the result of the authorisation request. The payment receipt is sent by email.

1.4.2 “Request" interface

1.4.2.1 Different integrations of the payment page

1.4.2.1.1 Integration with redirection to a new page

The payment form must be implemented using the HTML tag « form » in the merchant website page:

```
<form method="post" name="Name" target="_top" action="https://p.monetico-services.com/paiement.cgi">
      <input type="hidden" name="parameter1" value="value1">
      …
</form>
```

The value given for the field “name” above is just an example that has no effect on the application execution.

1.4.2.1.2 Direct integration on the merchant website pages

The merchant web site integrates the request to Monetico Paiement payment page using the HTML form « iframe »:

```
<iframe id="idPaymentFrame" name="namePaymentFrame" src="…" ></iframe>
```

The values given for the fields “id” and “name” above are just examples that have no effect on the application execution.

The field “src” must be built according to the description below:

https://p.monetico-services.com/paiement.cgi?parameter1=value1&parameter2=value2

Remark: as specified in section 1.4.2.3 Information specific to « light form » display mode, the display mode parameter must have the value « iframe ».

1.4.2.2 *Creation of the form*

The terminal settings and the order data are grouped together in a sealed HTML form in order to send the payment request to the Monetico Paiement server via the customer's browser.

Use only the fields mentioned in this paragraph when calling the payment page. The use of non-listed fields may results in errors when accessing the payment page: this access will be considered illegitimate.

When the name or the value of the option is incorrect, the payment request is interrupted and an error message, indicating that the form is incorrect, is shown on the page. This information is only displayed on your test environment known as "sandbox" (9.8.1).

The mandatory fields must all be provided in the call and must comply with the technical restrictions listed below.

Optional fields

1. May not be provided
2. May be provided empty
3. Or, if provided with a value, they must comply with the restrictions listed below.

The fields that may be provided in the form are listed below.

Field	**TPE**
Presence	Mandatory
Description	Number of your virtual POS
Format **Possible value(s)**	7 alphanumerical characters [A-Za-z0-9]{7}
Example	1234567

Field	**version**
Presence	Mandatory
Description	Version of payment system used
Format **Possible value(s)**	Only the value "3.0"
Example	3.0

Field	**date**
Presence	Mandatory
Description	Date of the order
Format **Possible value(s)**	DD/MM/YYYY:HH:MM:SS
Example	24/05/2019:10:00:25

Field	**montant**
Presence	Mandatory
Description	Amount of the order including tax
Format **Possible value(s)**	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR

Field	**reference**
Presence	Mandatory
Description	Unique order reference
Format **Possible value(s)**	^[\x20-\x7E]{1,50}$ It is advised to only send a maximum of 12 alphanumerical characters in order to keep this reference in your remote bank collections details.
Example	REF7896543

Field	**lgue**
Presence	Mandatory
Description	Language code. Determines the display language of the payment page or the iFrame page.
Format **Possible value(s)**	Choice from: DE EN ES FR IT JA NL PT SV
Example	FR

Field	MAC
Presence	Mandatory
Description	Seal resulting from the certification of data sent to the payment system.
Format Possible value(s)	40 hexadecimal characters [0-9a-f]{40}
Example	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Field	contexte_commande
Presence	Mandatory
Description	Information concerning the order: detail of basket, shipping and invoicing addresses and technical context. Detailed description in appendix 9.5
Format Possible value(s)	Data in JSON - UTF-8 format encoded in base64.

Field	societe
Presence	Mandatory
Description	Alphanumerical code allowing the merchant to use the same virtual POS for different sites (separate settings) relating to the same activity. This is your company code.
Format Possible value(s)	String of characters generated when creating your contract
Example	myCompany

Field	texte-libre
Presence	Optional
Description	Free text zone. Is notably reproduced on the dashboard.
Format Possible value(s)	3200 characters maximum
Example	Delivery to Rue des Tourerelles collection point

Field	**mail**
Presence	Optional
Description	Email address of the customer making the transaction. Allows the card holder to receive their payment receipt at the given address. If not provided, automatic redirection is not activated.
Format **Possible value(s)**	255 characters maximum ^.+@.+\..+$
Example	monclient@mondomain.com

Field	**url_return_ok**
Presence	Optional If not provided, the URL configured by default on your company code will be used.
Format **Possible value(s)**	2048 characters maximum URL through which the buyer returns to the merchant's site following accepted payment
Example	http://url.retour.com/ok.cgi?ref=REF001

Field	**url_return_err**
Presence	Optional If not provided, the URL configured by default on your company code will be used.
Format **Possible value(s)**	2048 characters maximum URL through which the buyer returns to the merchant's site following rejected payment
Example	http://url.retour.com/ko.cgi?ref=REF001

Field	**3dsdebrayable**
Presence	Optional
Description	To force disabling of 3D Secure
Format **Possible value(s)**	0: no disabling of the 3D Secure protocol 1: disabling of the 3D Secure protocol
Example	0

Field	**ThreeDSecureChallenge**
Presence	Optional
Description	Merchant's preference concerning the 3D Secure challenge
Format **Possible value(s)**	"no_preference": default choice "challenge_preferred" "challenge_mandated": challenge required "no_challenge_requested" "no_challenge_requested_strong_authentication": no challenge requested – the customer's strong authentication has already been performed by the merchant. "no_challenge_requested_trusted_third_party" : no challenge requested – request for exemption because the merchant is a trusted third party. "no_challenge_requested_risk_analysis": no challenge requested – request for exemption for a reason other than one already mentioned (for example: small amount) In the context of storing a card, the “challenge_mandated” wish will be systematically used.
Example	challenge_preferred

Field	**libelleMonetique**
Presence	Optional
Description	If filled in, replaces the "trade name" part in the "trade name*city" payment description which appears on the card holder's bank statement. **NB:** The number of characters considered depends on the card holder's bank
Format **Possible value(s)**	[A-Z a-z0-9]{1,32}
Example	MyShop

Field	libelleMonetiqueLocalite
Presence	Optional
Description	If filled in, replaces the "city" part in the "trade name*city" payment description which appears on the card holder's bank statement. **NB:** The number of characters considered depends on the card holder's bank
Format Possible value(s)	city\zip code\country code • city : [-A-Za-z0-9]+ • zip code : [-A-Z a-z0-9]* • country code : [A-Za-z]{3} following the ISO 3166-1 alpha-3 standard Global format global expected : [-A-Za-z0-9]+\[-A-Z a-z0-9]*\[A-Za-z]{3} Maximum length expected : 32 characters
Example	Strasbourg\67000\FRA Strasbourg\\FRA

Field	desactivemoyenpaiement
Presence	Optional
Description	Makes it possible to not display one or more alternative payment methods on the payment page.
Format Possible value(s)	1euro, 3xcb, 4xcb, paypal or lyfpay.
Example	paypal

Field	aliascb
Presence	Optional. Requires the "express payment" option
Description	Alias of the customer's bank card
Format Possible value(s)	From 1 to 64 alphanumerical characters [a-zA-Z0-9]{1,64}
Example	monClientRef001

Field	forcesaisiecb
Presence	Optional. Requires subscription to the "express payment" option
Description	Forces input of a bank card
Format Possible value(s)	0 : the card used for the previous payment is used for this payment 1 : the card information must be given again
Example	0

Field	**protocole**
Presence	Optional Requires subscription to an alternative payment method
Description	Payment method via a preferred partner. The following field must be added in the case of integrating buttons allowing payment via a partner (Paypal, 3xCB, etc.) directly on the merchant's site (without going via the payment page).
Format Possible value(s)	1euro, 3xcb, 4xcb, paypal or lyfpay.
Example	lyfpay

1.4.2.3 Information specific to “light form” display mode

Field	**mode_affichage**
Presence	Optional
Description	To display minimalist payment form which is recommended with an iframe integration on the merchant website or a webview integration in the merchant mobile application. Requires the "iframe" option
Format **Possible value(s)**	Only the value “iframe”
Example	iframe

1.4.2.4 Information specific to split payments

To be able to use these fields, your POS must be configured to accept payments in N instalments. All of these fields are optional: if you do not provide them, the settings configured when creating your POS shall be taken into account.

The rules below must be followed:

- The sum of the amounts of each instalment must be equal to the amount of the order;
- The amounts must be in the same currency;
- The instalments must be monthly.
- If the bank card expires before the final instalment:
  - the order may be rejected or:
  - the instalments after the expiry date may be added to the first instalment.

Field	**nbrech**
Presence	Optional in the case of split payment
Description	Number of instalments for this order
Format **Possible value(s)**	2, 3 or 4.
Example	3

Field	**dateech[N]** (N =1, 2, 3 or 4)
Presence	Optional in the case of split payment
Description	Date of the Nth instalment
Format **Possible value(s)**	DD/MM/YYYY
Example	24/05/2019

Field	**montantech[N]** (N =1, 2, 3 or 4)
Presence	Optional in the case of split payment
Description	Amount including tax of the Nth instalment
Format **Possible value(s)**	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	33.50EUR

1.4.2.5 Information specific to pre-authorised payments

Field	**numero_dossier**
Presence	Mandatory in the case of a pre-authorised payment
Description	Dossier number
Format **Possible value(s)**	12 alphanumerical characters maximum.
Example	20150901PRE1

1.4.2.6 Information specific to COFIDIS payments

As part of the partner COFIDIS 3xCB and 4xCB payments, it is possible to send customers' information when requesting payment in order to pre-fill the request form on the partner site. **These values must be encoded in hexadecimal before being sent.**

The list of this information is as follows:

Field	**civiliteclient**
Presence	Optional
Description	Customer's civility
Format **Possible value(s)**	MR / MME / MLLE
Example	MR

Field	**nomclient**
Presence	Optional
Description	Customer's name
Format **Possible value(s)**	(^[a-zA-Záàâäãåçéèêëíìîïñóòôöõúùûüýÿ-]{1,50}$)
Example	Dupont

Field	**prenomclient**
Presence	Optional
Description	Customer’s firstname
Format **Possible value(s)**	(^[a-zA-Záàâäãåçéèêëíìîïñóòôöõúùûüýÿ-]{1,50}$)
Example	Thomas

Field	adresseclient
Presence	Optional
Description	Customer’s address
Format Possible value(s)	.{1,100}
Example	20 rue des champs

Field	complementadresseclient
Presence	Optional
Description	Customer’s address additional information
Format Possible value(s)	.{1,50}
Example	Appartement B

Field	codepostalclient
Presence	Optional
Description	Customer’s zip code
Format Possible value(s)	(^[a-zA-Z0-9]{1,10}$)
Example	67200

Field	villeclient
Presence	Optional
Description	Customer’s city of residence
Format Possible value(s)	(^[a-zA-Z]{1,50}$)
Example	Strasbourg

Field	paysclient
Presence	Optional
Description	Customer’s country of residence
Format Possible value(s)	(^[a-zA-Z]{2}$)
Example	FR

Field	telephonefixeclient
Presence	Optional
Description	Customer’s landline phone
Format Possible value(s)	(^[0-9]{2,20}$)
Example	0312345678

Field	**telephonemobileclient**
Presence	Optional
Description	Customer’s mobile phone
Format **Possible value(s)**	(^[0-9]{2,20}$)
Example	0612345678

Field	**departementnaissanceclient**
Presence	Optional
Description	Customer’s geographic code of the entity of the country of birth
Format **Possible value(s)**	(^[a-zA-Z]{1,50}$)
Example	67

Field	**datenaissanceclient**
Presence	Optional
Description	Customer’s birth date
Format **Possible value(s)**	(^[A-Za-z0-9]{8}$)
Example	19900103

Field	**prescore**
Presence	Optional
Description	Cofidis pre-scoring
Format **Possible value(s)**	[0-9]
Example	1234567

1.4.2.7 Example of payment form in HTML

```
<form method="post" name="Monetico" target="_top" action="https://p.monetico-services.com/paiement.cgi">
        <input type="hidden" name="version" value="3.0">
        <input type="hidden" name="TPE" value="1234567">
        <input type="hidden" name="date" value="05/05/2019:11:55:23">
        <input type="hidden" name="montant" value="62.73EUR">
        <input type="hidden" name="reference" value="REF001">
        <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
        <input type="hidden" name="url_retour_ok" value="http://url.retour.com/ok.cgi?ref=REF001">
        <input type="hidden" name="url_retour_err" value="http://url.retour.com/ko.cgi?ref=REF001">
        <input type="hidden" name="lgue" value="FR">
        <input type="hidden" name="societe" value="monSite1">
        <input type=" hidden" name="contexte_commande" value=”ewoJI(…)KCX0KfQ==”>
        <input type="hidden" name="texte-libre" value="ExempleTexteLibre">
        <input type="hidden" name="mail" value="internaute@sonemail.fr">
        <input type="submit" name="bouton" value="Paiement CB">
</form>
```

1.4.2.8 Example of split payment form in HTML

```
<form method="post" name="Monetico" target="_top" action="https://p.monetico-services.com/paiement.cgi">
    <input type="hidden" name="version" value="3.0">
    <input type="hidden" name="TPE" value="1234567">
    <input type="hidden" name="date" value="05/05/2019:11:55:23">
    <input type="hidden" name="montant" value="100EUR">
    <input type="hidden" name="reference" value=" REF002">
    <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
    <input type="hidden" name="url_retour_ok" value="http://url.retour.com/ok.cgi?ref=REF002">
    <input type="hidden" name="url_retour_ko" value="http://url.retour.com/ko.cgi?ref=REF002">
    <input type="hidden" name="lgue" value="FR">
    <input type="hidden" name="societe" value="monSite1">
    <input type=" hidden" name="contexte_commande" value="ewoJI(…)KCX0KfQ==">
    <input type="hidden" name="texte-libre" value="ExempleTexteLibre">
    <input type="hidden" name="mail" value="internaute@sonemail.fr">
    <input type="hidden" name="nbrech" value="3">
    <input type="hidden" name="dateech1" value="05/05/2019">
    <input type="hidden" name="montantech1" value="50EUR">
    <input type="hidden" name="dateech2" value="05/06/2019">
    <input type="hidden" name="montantech2" value="25EUR">
    <input type="hidden" name="dateech3" value="05/07/2019">
    <input type="hidden" name="montantech3" value="25EUR">
    <input type="submit" name="bouton" value="Paiement CB">
</form>
```

1.4.2.9 Example of pre-authorised payment form in HTML

```
<form method="post" name="Monetico" target="_top" action="https://p.monetico-services.com/paiement.cgi">
    <input type="hidden" name="version" value="3.0">
    <input type="hidden" name="TPE" value="1234567">
    <input type="hidden" name="date" value="05/06/2019:11:55:23">
    <input type="hidden" name="montant" value="62.73EUR">
    <input type="hidden" name="reference" value=" REF003">
    <input type="hidden" name="numero_dossier" value="20150901PRE1">
    <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
    <input type="hidden" name="url_retour_ok" value="http://url.retour.com/ok.cgi?order_ref= REF003">
    <input type="hidden" name="url_retour_err" value="http://url.retour.com/err.cgi?order_ref= REF003">
    <input type="hidden" name="lgue" value="FR">
    <input type="hidden" name="societe" value="monSite1">
    <input type="hidden" name="texte-libre" value="ExempleTexteLibre">
    <input type="hidden" name="mail" value="internaute@sonemail.fr">
    <input type="submit" name="bouton" value="Paiement CB">
</form>
```

1.4.2.10 Exemple de formulaire de paiement propres aux moyens de paiement COFIDIS

```
<form method="post" name="Monetico" target="_top" action="https://p.monetico-services.com/paiement.cgi">
        <input type="hidden" name="version" value="3.0">
        <input type="hidden" name="TPE" value="1234567">
        <input type="hidden" name="date" value="05/06/2019:11:55:23">
        <input type="hidden" name="montant" value="62.73EUR">
        <input type="hidden" name="reference" value=" REF003">
        <input type="hidden" name="numero_dossier" value="20150901PRE1">
        <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
        <input type="hidden" name="url_retour_ok" value="http://url.retour.com/ok.cgi?order_ref= REF003">
        <input type="hidden" name="url_retour_err" value="http://url.retour.com/err.cgi?order_ref= REF003">
        <input type="hidden" name="lgue" value="FR">
        <input type="hidden" name="societe" value="monSite1">
        <input type="hidden" name="texte-libre" value="ExempleTexteLibre">
        <input type="hidden" name="mail" value="internaute@sonemail.fr">
        <input type="hidden" name="civilite" value="4D52">
        <input type="hidden" name="nomclient" value="6C6163686F7563726F757465">
        <input type="hidden" name="prenomclient" value="63657374626F6E">
        <input type="hidden" name="adresseclient" value=" 7275652064657320736175636973736573">
        <input type="submit" name="bouton" value="Paiement CB">
</form>
```

1.4.2.11 Calculation of form seal

For the MAC algorithm, refer to the dedicated section.

1.4.3 "Response" interface

After processing the payment request, the bank server directly informs the merchant's server of the result of the payment request by issuing an on-line HTTP(S) request containing the result of the payment request on the payment confirmation URL ("Response" interface). **This URL must be given to us at the time of setting up the system.**

The “Response” interface is called **after each payment attempt** for the same order to indicate the result. It is therefore possible that the Response interface will receive several notifications of rejected payments followed by notification of accepted payment for the same reference. If the customer does not pursue the payment process to the end, for example if they do not enter their bank card information, the Response interface is not called.

The Response interface has 30 seconds to reply, as described in chapter 1.4.3.3, page 36. If the time-frame is exceeded, the merchant's Response interface interprets this as an error.

When an incorrect response is given and the payment is accepted: a second call is made (unless there is immediate redirection to the merchant's site).

Note to merchants migrating from an older version of the seal calculation

The fields described below are only valid when the seal sent to the "Request" interface has been calculated according to the method described in this document. For payments created in accordance with an earlier version of this documentation and the calculation, the return will be in accordance with what was described therein.

Similarly, the calculation of the seal at the "Response" interface is done in the same way as at the "Request" interface and therefore according to the old calculation for commands initialized before the transition.

This is particularly important for split payments, where the call to the "Response" interface can take place several days after the payment is made for the various due dates, during which time a migration to the use of the new seal calculation may have taken place. Calls to the return interface of both types could therefore coexist.

For reference, the fields previously returned and the old method of calculating the MAC seal for the "Response" interface are described in the appendix.

1.4.3.1 Settings sent back by Monetico Paiement

The "Response" interface will be called by the bank server with the POST method. The data sent by the Monetico Paiement server is described below.

Field	code-retour
Description	Payment result
Format Possible values	Character string payetest: accepted payment (in "sandbox" only) paiement: accepted payment (in Production only) annulation: rejected payment For split payments, for automatic collection of tier > 1 instalments: paiement_pf[N]: payment of instalment N (N between 2 and 4) accepted Annulation_pf[N]: payment of instalment N (N between 2 and 4) definitively rejected
Addition	In the event of a rejected payment, later authorisation may be issued for the same reference. The "payetest" code is only sent for payments made in the "sandbox" environment. If this code is present during a payment in production, this is an error.
Example	1

Field	MAC
Description	Seal resulting from the certification of data sent to the payment system.
Format Possible value(s)	40 hexadecimal characters [A-F]{40}
Example	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Field	TPE
Description	Number of your virtual POS
Format Possible value(s)	7 alphanumerical characters [A-Za-z0-9]{7}
Example	1234567

Field	**montant**
Description	Amount of the order including tax
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR
Addition	Only for a POS **NOT** in pre-authorisation

Field	**montantestime**
Description	Estimated amount of the order including tax
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR
Addition	Only for a POS in pre-authorisation

Field	**reference**
Description	Unique order reference
Format Possible value(s)	50 alphanumerical characters maximum.
Example	REF7896543

Field	**texte-libre**
Description	Free text zone provided during the "Out" phase
Format Possible value(s)	3200 characters maximum
Example	Delivery to Rue des Tourerelles collection point

Field	**date**
Description	Date of the order authorisation request
Format Possible value(s)	DD/MM/YYYY_at_HH:MM:SS
Example	24/05/2019:10:00:25

Field	cvx
Description	Indicates whether the visual cryptogram was entered during the transaction.
Format Possible value(s)	yes: if the visual cryptogram was entered no: otherwise
Example	yes

Field	vld
Description	Date of validity of the credit card used to make the payment
Format Possible value(s)	MMYY
Example	1019

Field	brand
Description	Network code of the card in 2 alphanumerical positions from:
Format Possible value(s)	AM American Express CB GIE CB MC Mastercard VI Visa na Not available
Addition	The "na" value is always returned in the test environment
Example	VI

Field	numauto
Description	Authorisation number as provided by the issuing bank.
Format Possible value(s)	Character string
Addition	Only if authorisation was given
Example	000002

Field	authentification
Description	Document JSON/UTF-8 encoded in base64 containing the information related to customer authentication, notably for 3D Secure.
Addition	Link to the document structure.

Field	**usage**
Description	Specifies the type of card used for the transaction
Format **Possible value(s)**	credit: credit card or deferred debit card debit: debit card prepaye: prepaid card inconnu: impossible to determine the type of card
Example	credit

Field	**typecompte**
Description	Specifies the type of account associated with the bank card
Format **Possible value(s)**	particulier: personal bank account commercial: business bank account inconnu: impossible to determine the type of account
Example	personal

Field	**ecard**
Description	Explains whether the card used for the payment is virtual or not
Format **Possible value(s)**	yes no
Example	yes

Field	**motifrefus**
Description	Reason for rejection of payment request
Format **Possible value(s)**	**Appel Phonie**: the customer's bank requests additional information **Refus**: the merchant's or customer's bank refuses to grant authorisation **Interdit**: the merchant's or customer's bank refuses to grant authorisation **filtrage**: the payment request was blocked by the filter setting that the merchant set up in their Fraud Prevention Module **scoring**: the payment request was blocked by the scoring setting that the merchant set up in their Fraud Prevention Module **3DSecure**: if the rejection is related to negative 3D Secure authentication received by the card holder
Addition	Only if the payment request was rejected

Field	**motifrefusautorisation**
Description	Reason for rejection of authorisation request
Format **Possible value(s)**	**Refus banque** : the merchant's or customer's bank refuses to grant authorisation **Refus emetteur** : the customer's bank refuses to grant authorisation **Refus critique** : the customer's bank refuses to grant authorisation. Unlike “Refus banque“ and “Refus emetteur”, this refusal is final.

	Refus repli VADS : the customer's bank refuses authorisation and requires client authentication **Refus temporaire** : authorisation temporarily refused, the payment could be retried **Refus technique** : authorisation refused because of a technical problem **Refus autres** : Other authorization refusal reason **Refus test** : Simulation test of authorisation refusal in validation environment
Addition	Only if the authorisation request was rejected

Field	**originecb**
Description	Country code of the bank issuing the bank card
Format **Possible value(s)**	ISO 3166-1
Addition	Only in the event of subscribing to the fraud prevention module

Field	**bincb**
Description	BIN code of the credit card holder's bank
Format **Possible value(s)**	The format depends on the card number length : - 8 digits when the card number length is 16 digits or more - 6 digits followed by 2 letters ‘X’ when the card number length is less than 16 digits
Example	12345678 123456XX
Addition	Only in the event of subscribing to the fraud prevention module

Field	**hpancb**
Description	One-way hashing (HMAC-SHA1) of the credit card number used to make the payment (unique way to identify a credit card for a given merchant)
Addition	Only in the event of subscribing to the fraud prevention module

Field	**ipclient**
Description	IP address of the customer that made the transaction
Addition	Only in the event of subscribing to the fraud prevention module

Field	**originetr**
Description	Source country code of the transaction
Format	ISO 3166-1
Addition	Only in the event of subscribing to the fraud prevention module

Field	**montantech**

Description	Amount of the instalment in progress
Addition	Only in the case of a split payment

Field	**numero_dossier**
Description	Dossier number for POS in pre-authorisation
Format **Possible value(s)**	12 alphanumerical characters maximum.
Example	20150901PRE1

Field	**typefacture**
Description	Type of invoice to generate for POS in pre-authorisation
Addition	Only for a POS in pre-authorisation
Format **Possible value(s)**	preauto

Field	filtragecause
Description:	Numbers of the types of filters blocking the payment (see "Fraud Prevention Module Response – details table" below)
Format Possible value(s)	1: IP address 2: Card number 3: Card BIN 4: Country of the card 5: Country of the IP 6: Consistency between country of the card / country of the IP 7: Disposable email 8: Amount restriction for a bank card over a given period 9: Restriction of number of transactions for a bank card over a given period 11: Restriction of number of transactions per alias over a given period 12: Amount restriction per alias over a given period 13: Amount restriction per IP over a given period 14: Restriction of number of transactions per IP over a given period 15: Card testers 16: Restriction of number of aliases per bank card
Addition	Only in the event of a payment filter or if the information mode is enabled. If several filters block the payment, they are separated with hyphens. The causes and corresponding values are in the same order.

Field	filtragevaleur
Description	Data that caused the block
Addition	Only in the event of a payment filter or if the information mode is enabled. If several filters block the payment, they are separated with hyphens. The causes and corresponding values are in the same order.

Field	filtrage_etat
Description	Indicates, only if present, that the filter is in "information" mode. information: Filter information mode
Addition	Only in the event of a payment filter or if the information mode is enabled. If several filters block the payment, they are separated with hyphens. The causes and corresponding values are in the same order.

Field	cbenregistree
Description	Boolean indicating whether the card has been registered under a given card alias (aliascb)
Field	1: The customer entered a bank card and it has been registered under the card alias (aliascb) sent 0: All other cases,
Addition	Only in the event of subscription to the express payment option

Field	cbmasquee
Description	The card number truncated as indicated by PCI DSS
Field	The format depends on card number length : - First 8 digits and 2 last digits of the customer's bank card, separated with stars when the card number length is 16 digits or more - First 6 digits, followed by 6 stars and the last remaining digits of the customer's bank card when the card number length is less than 16 digits
Example	12345678******12 123456******123
Addition	Always returned for payments using payment cards on Monetico Paiement. Not returned otherwise (Paypal …)

Field	modepaiement
Description	Payment method used
Format Possible value(s)	Bank card paypal 1euro 3xcb 4xcb audiotel

Field	statutDebrayageAuthentification
Description	Indicates the disabling status of the cardholder authentication
Format Possible value(s)	0 : The disabling was not requested 1 : The disabling was granted -1 : The disabling was not granted due to the type of bank card -2 : The disabling was not granted due to payment options
Addition	Only if the authentication disabling options are enabled.

Fraud Prevention Module Response – Details

The payment filtering function rests on a set of nine filters which can be freely configured on the dashboard (new version). Each of these filters acts on a specific criterion, such as the customer's IP address, their email address, the country of their bank card, etc.

Number of filter type	Analysis criterion	Value returned as blocking reason	Note
1	IP address	Customer's IP address	
2	Card number	Hash of the customer's card	Only for card payments
3	Card BIN	BIN of the customer's card	
4	Country of the card	Country of the customer's card	
5	Country of the IP	Country of the customer's IP	
6	Consistency between country of the card / country of the IP	Country of the customer's card # country of the customer's IP	Only for card payments
7	Disposable email	Domain name of the customer's email address	
8	Amount restriction for a bank card over a given period	Cumulative total in euros (€) over the given period associated with the customer's card	Only for card payments
9	Restriction of number of transactions for a bank card over a given period	Cumulative number of transactions over the given period associated with the customer's card	
11	Restriction of number of transactions per alias over a given period	Cumulative number of transactions over the given period associated with the customer's alias	Only in the event of subscription to the express payment option
12	Amount restriction per alias over a given period	Cumulative total in euros (€) over the given period associated with the customer's alias	
13	Amount restriction per IP over a given period	Cumulative total in euros (€) over the given period associated with the customer's IP address	
14	Restriction of number of transactions per IP over a given period	Cumulative number of transactions over the given period associated with the customer's IP address	
15	Card testers	Cumulative number of transactions over the given period associated with the customer's IP address	
16	Restriction of number of aliases per bank card	The aliases already associated with the card used for the payment	Only in the event of subscription to the express payment option

Example of data sent by the Monetico Paiement server to the "Response" interface for immediate, partial or recurrent payment:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EU
R&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&
&numauto=010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F
2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&authen
tification=ewoJIn(…)KfQo=
```

Example of data sent by the Monetico Paiement server to the "Response" interface for the first instalment of a split payment:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EU
R&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&
numauto=010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2
C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&
montantech=20EUR&authentification=ewoJIn(…)KfQo=
```

Example of data sent by the Monetico Paiement server to the "Response" interface for blocking of an immediate payment by the FPM:

```
TPE=9000001&date=05%2f10%2f2011%5fa%5f15%3a33%3a06&montant=1%2e01EUR
&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=FRA&bincb=513283&hpancb=764AD24CFABB
B818E8A7DC61D4D6B4B89EA837ED&ipclient=10%2e45%2e166%2e76&originetr=i
nconnue&veres=&pares=&filtragecause=4-&filtragevaleur=FRA-
```

Example of data sent by the Monetico Paiement server to the "Response" interface for a payment with the express payment option:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EU
R&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&numauto=010101&originecb=F
RA&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45&ipcl
ient=127%2e0%2e0%2e1&originetr=FRA&cbenregistree=1&cbmasquee=123456*
*****7890&authentification=ewoJIn(…)KfQo=
```

1.4.3.2 Validation of seal

The confirmation message received is sealed by a **MAC seal** calculated by the Monetico Paiement payment server using the merchant security key allocated to your payment terminal.

A seal validation function must be implemented in the "Response" interface to ensure that the data contained in the message confirming payment received was not tampered with.

For this, the function must re-calculate the **MAC** code associated with the message and compare it to the one sent in the message: if both codes are the same, the information received is reliable (integrity of information and authentication of the issuer).

To calculate the **MAC**, refer to the documentation in appendix.

1.4.3.2.1 Split payment specificity

In particular, calls to the "Response" interface for installment due dates will all be sealed with the calculation method used when the payment was created; it is therefore necessary to provide a fallback mechanism to manage the old calculation of the seal for installment payments made before your implementation of the method described in this document for which we would make a call to your "Response" interface.

1.4.3.2.2 Test environment known as “sandbox” specificity

In order to guarantee your implementation and the right management of every new parameter sent by Monetico Paiement, a field which name and content are random is generated and automatically added to the “Response” interface for every payment.

This random field is only present for payments made in the test environment known as “sandbox”.

To calculate the **MAC**, refer to the documentation in appendix.

1.4.3.3 Creation of the acknowledgement of receipt

The reply sent back by the "Response" interface to the Monetico Paiement payment server must be one of the two messages presented in the table below, dependant only on verification of the MAC seal received, without taking into account the value of the payment feedback-code, as soon as this value is in the list of values listed for the feedback-code (code-retour) field.

Validated seal	Acknowledgement of receipt to send back in text format

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

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

Note: `<LF>` corresponds to a line break

When the Monetico Paiement server does not receive the acknowledgement of receipt for a validated seal, it sends a warning mail to a monitoring email box provided by the merchant and makes a second attempt.

This email contains a link making it possible, via the GET method, to repeat the request issued by the Monetico Paiement server, an error code encountered during the URL confirmation call and the acknowledgement of receipt returned by the merchant's server.

From the test phase, the merchant must give us the address of an email box that is regularly checked. To move into production, the merchant's server must have returned an acknowledgement of receipt with a validated seal for the last three tests.

2 Request collection of a payment request

2.1 Presentation

The purpose of the "capture_paiement" service is to allow merchants to collect, by secure computerised request, payments which have been previously authorised.

This service can be used with the following payment methods:

- deferred payment
- partial payment
- split payment (for the first instalment only)
- recurrent payment (depending on the configuration chosen)

To request collection, the merchant's application must call the capture web service of the Monetico Paiement system (via HTTPS message), providing a certain amount of information (the amount of the order, its date, its reference, the number of the merchant's virtual POS, etc.). A seal must be calculated to certify the data exchanged.

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

2.2 Call to the capture request service

2.2.1 Information to supply

The merchant's application must issue a request in POST method via HTTPS message using the TLS V1.2 secure exchange protocol only, to the "capture_paiement" service on the Monetico Paiement servers, containing the following fields:

Field	**TPE**
Presence	Mandatory
Description	Number of your virtual POS
Format Possible value(s)	7 alphanumerical characters [A-Za-z0-9]{7}
Example	1234567

Field	**version**
Presence	Mandatory
Description	Version of payment system used
Format Possible value(s)	Only the value "3.0"
Example	3.0

Field	**date**
Presence	Mandatory
Description	Date and time of the capture request
Format Possible value(s)	DD/MM/YYYY:HH:MM:SS
Example	24/05/2019:10:00:25

Field	**date_commande**
Presence	Mandatory
Description	Date of the order in the format
Format Possible value(s)	DD/MM/YYYY
Example	24/05/2019

Field	montant
Presence	Mandatory
Description	Amount of the initial order including tax
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR

Field	montant_a_capturer
Presence	Mandatory
Description	Amount of the capture request including tax
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR

Field	montant_deja_capture
Presence	Mandatory
Description	Amount including tax corresponding to the amount already captured on this order
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR

Field	montant_restant
Presence	Mandatory
Description	Amount including tax corresponding to the balance of the order after the capture currently requested
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR

Field	reference
Presence	Mandatory
Description	Reference of the order.
Format Possible value(s)	50 alphanumerical characters maximum. [a-zA-Z0-9]{1,50}
Example	REF7896543

Field	lgue
Presence	Mandatory
Description	Language code in upper case
Format Possible value(s)	DE EN ES FR IT JA NL PT SV [A-Z]{2}
Example	FR

Field	societe
Presence	Mandatory
Description	Alphanumerical code allowing the merchant to use the same virtual POS for different sites (separate settings) relating to the same activity
Format Possible value(s)	Alphanumerical
Example	myCompany

Field	MAC
Presence	Mandatory
Description	Seal resulting from the certification of data sent to the payment system.
Format Possible value(s)	40 hexadecimal characters [A-Fa-f]{40}
Example	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Field	stoprecurrence
Presence	Optional
Description	Forces recurrence to stop for the POS in recurrent payment.
Format Possible value(s)	yes: stop recurrence
Example	yes

Field	numero_dossier
Presence	Optional
Description	Pre-authorisation dossier number
Addition	Only for a POS in pre-authorisation
Format Possible value(s)	12 alphanumerical characters
Example	20150901PRE1

Field	facture
Presence	Optional
Description	Type of invoice to generate
Addition	Only for a POS in pre-authorisation
Format Possible value(s)	preauto noshow
Example	noshow

Field	phonie
Presence	Optional
Description	The value of this field will be returned in the event of a phone call
Format Possible value(s)	yes

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

Note: It is possible for an authorisation request to be rejected for a "phone call" type reason (amount too high, authorisation centre busy, etc.).
It may then be necessary for the merchant to make a manual request (telephone, fax) to the authorisation centre of the card holder, which will send back the bank details and the sum, and an authorisation number for this transaction.

2.2.2 Calculation of seal

To calculate the MAC seal, refer to the dedicated section.

2.2.3 Examples of capture requests

Example 1: partial collection of €62 for an initial order of €100

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=100.00EUR
        &montant_a_capturer=62.00EUR
        &montant_deja_capture=0EUR
        &montant_restant=38.00EUR
        &reference=ABERTPY00145
        &lgue=FR
        &societe=monSite1
        &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

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

This capture can only take place if your POS is configured in Partial Payment, Recurrent Payment or Split Payment and if the first instalment is for 62.00EUR If successful, a further capture for a sum of €38 is still possible.

Example 2: full collection for an order of €100

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=100.00EUR
        &montant_a_capturer=100.00EUR
        &montant_deja_capture=0EUR
        &montant_restant=0EUR
        &reference=ABERTPY00145
        &lgue=FR
        &societe=monSite1
        &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

The 2 amounts must be the same

This capture can take place if your POS is configured in Partial Payment, Recurrent Payment or Deferred Payment. If successful, no later capture is possible.

2.3 Response of the capture request

2.3.1 Returned information

In response to the capture request, the merchant's application receives a message of acknowledgement from the Monetico Paiement server. This message is a "text/plain" MIME document specifying the result of the capture.

It contains the following fields separated by a character CHR (10) which corresponds to a line break.

Field	cdr
Description	Return code indicating the result of the capture
Format Possible value(s)	1: capture accepted 0: capture rejected -1: error

Field	lib
Description	Detailed description stating the nature of the return code
Format Possible value(s)	See below for the list of possible descriptions

Field	version
Description	Version number of the acknowledgement message
Format Possible value(s)	Only "1.0"

Field	reference
Description	Reference of the order

Field	aut
Description	Payment authorisation number if accepted

Field	phonie
Description	Authorisation rejected for "phone call" type reason
Addition	This field is only present if the "phonie" field was present and filled in during the calling request

Field	montant_estime
Description	Initial amount of the pre-authorisation request
Addition	Only for a POS in pre-authorisation
Format	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	62.73EUR

Field	date_autorisation
Description	Date on which the invoice was pre-authorised
Addition	Only for a POS in pre-authorisation
Format	YYYYA-MM-DD
Example	2019-06-26

Field	montant_debite
Description	Amount actually collected from the invoice
Addition	Only for a POS in pre-authorisation
Format	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	62.73EUR

Field	date_debit
Description	Date on which the collection was made
Addition	Only for a POS in pre-authorisation
Format	YYYYA-MM-DD
Example	26/06/2019

Field	numero_dossier
Description	Number of the dossier which has just been collected
Addition	Only for a POS in pre-authorisation
Format Possible value(s)	12 alphanumerical characters maximum.
Example	20150901PRE1

Field	**type_facture**
Description	Type of invoice that was just produced
Format **Possible value(s)**	preauto noshow
Example	noshow

The list of values available for the description is given in the following table:

cdr	lib	description	note
1	**paiement accepte**	The bank authorisation was issued and collection made	
1	**commande annulee**	The cancellation order was taken into account and the order was cancelled	
1	**recurrence stoppee**	The request to definitively cancel renewal was taken into account	**Only in Recurrent Payment**
0	**commande non authentifiee**	The reference does not correspond to an order	**Verify the reference and date_commande settings**
0	**commande expiree**	The date of the order exceeds the authorised time-frame (+/- 24 hours)	
0	**commande grillee**	The maximum number of attempts to enter the card details was reached (3 attempts allowed)	**The order is no longer accepted by the bank server**
0	**autorisation refusee**	The bank authorisation was not issued	**The capture was not performed**
0	**annulation refusee**	The authorisation cancellation was rejected	**The cancellation was not performed**
0	**la commande est deja annulee**	The order was cancelled during a previous capture	**No request will be accepted for this order**
0	**paiement deja accepte**	An authorisation request has already been issued 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: immediate payment, because the collection is automatic**
-1	**la demande ne peut aboutir**	The capture request is incorrectly formulated	**Verify the settings sent**
-1	**montant errone**	One of the amounts transmitted is incorrectly formatted	**Verify the 4 amount settings**
-1	**commercant non identifie**	The settings to identify the reatil website are incorrect	**Verify the company, language and POS (societe, lgue and TPE) fields**
-1	**traitement en cours**	The order is currently being processed	
-1	**date erronee**	The date does not comply with the required format	**Verify the date setting**
-1	**autre traitement en cours**	Another transaction is being processed with the same reference	**Repeat the request**
-1	**indisponibilite temporaire du service**	Service not available during maintenance operations (NWH)	**Repeat the request at the end of the maintenance**
-1	**probleme technique**	A technical problem occurred	**Repeat the request**

2.3.2 Specificity of the pre-authorisation payment mode

It is only possible to perform one capture of the initial request, partial or total.

2.3.3 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 recurrence cancellation

```
version=1.0
reference=000000000145
cdr=1
lib=recurrence stoppee
aut=123456
```

- Case of authorisation rejected without the phone field supplied

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

- Case of an authorisation rejected for phone call reason with the phone field set to "yes"

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

- Case of an authorisation rejected with the phone field set to "yes"

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

- Case of a capture refused before the authorisation request

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

- Case of error

```
version=1.0
reference=000000000145
cdr=-1
lib=commercant non identifie
```

- Case of accepted capture in pre-authorisation

```
version=1.0
reference=000000000145
cdr=1
lib=paiement accepte
aut=123456
montant_estime=10EUR
date_autorisation=2019-05-20
montant_debite=5EUR
date_debit=2019-05-30
numero_dossier=doss123456
type_facture=preauto
```

- Case of accepted cancellation in pre-authorisation

```
version=1.0
reference=000000000145
cdr=1
lib=commande annulee
aut=123456
montant_estime=1.01EUR
date_autorisation=21/05/2019
numero_dossier=1011
type_facture=preauto
```

3 Request cancellation of payment/recurrence

3.1 Payment cancellation

If the merchant has requested a payment and does not want to collect payment (goods not available, customer changed their mind, etc.), they can inform the Monetico Paiement server to abort their payment request.

For this, they will call the capture service as described in the previous chapter, specifying the amount to capture and the amount outstanding at 0EUR.

Example: cancel an order for an initial amount of €100

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=100.00EUR
          &montant_a_capturer=0EUR
          &montant_deja_capture=0EUR
          &montant_restant=0EUR
          &reference=ABERTPY00145
          &lgue=FR
          &societe=monSite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

The fields “montant_a_capturer” (amount to capture) and “montant_restant” (outstanding amount) must be equal to 0

The field “montant_deja_capture” (amount already captured) must correspond to the payment record

This capture can take place if your POS is configured in Partial Payment or Deferred Payment. If successful, no later capture is possible.

3.2 Cancellation of recurrence

If the merchant does not want to continue automatic subscription renewals, they can inform the Monetico Paiement server of the cessation of payment recurrence.

For this, they will call the capture service as described in the previous chapter, specifying the amount to capture and the amount outstanding at 0EUR and setting the “stoprecurrence” field to “OUI”.

Example: cancel recurrence of an order with an initial sum.

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: 318

          version=3.0
          &TPE=1234567
          &date=05%2F12%2F2006%3A11%3A55%3A23
          &date_commande=03%2F12%2F2006
          &montant=100.00EUR
          &montant_a_capturer=0EUR
          &montant_deja_capture=0EUR
          &montant_restant=0EUR
          &stoprecurrence=OUI
          &reference=ABERTPY00145
          &lgue=FR
          &societe=monSite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

The fields “montant_a_capturer” (amount to capture) and “montant_restant” (outstanding amount) must be equal to 0

The field “montant_deja_capture” (amount already captured) must correspond to the payment record

This capture can take place if the POS is configured in Recurrent Payment. If successful, the order will not be renewed.

4 Request an additional invoice for pre-authorisation

Once the payment has been collected, the additional invoice request is made via the 3D Secure emulation service.

For more details, refer to the technical documentation for this.

5 Refund service

5.1 Presentation

The purpose of the "recredit_paiement" service is to allow merchants to refund their customers some or the full amount of their purchase, securely, over the Internet.

To request a refund, the merchant's application must call the refund web service of the Monetico Paiement system (via HTTPS message), providing a certain amount of information (the amount of the refund, its date, its reference, the number of the merchant's virtual POS, etc.). A seal must be calculated to certify the data exchanged.

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

5.2 Call to the refund service

5.2.1 Information to supply

The merchant's application must issue a request in POST method via HTTPS message using the TLS V1.2 secure exchange protocol only, to the "recredit_paiement" service on the Monetico Paiement servers, containing the following fields:

Field	**TPE**
Presence	Mandatory
Description	Number of your virtual POS
Format Possible value(s)	7 alphanumerical characters [A-Za-z0-9]{7}
Example	1234567

Field	**version**
Presence	Mandatory
Description	Version of payment system used
Format Possible value(s)	Only the value "3.0"
Example	3.0

Field	**date**
Presence	Mandatory
Description	Date and time of the refund request
Format Possible value(s)	DD/MM/YYYY:HH:MM:SS
Example	24/05/2019:10:00:25

Field	**date_commande**
Presence	Mandatory
Description	Date of the order
Format Possible value(s)	DD/MM/YYYY
Example	24/05/2019

Field	**date_remise**
Presence	Mandatory
Description	Date on which the payment was collected
Format Possible value(s)	DD/MM/YYYY
Example	24/05/2019

Field	**num_autorisation**
Presence	Mandatory
Description	Authorisation number returned by the bank's server at the time of the payment request
Example	123456

Field	**montant**
Presence	Mandatory
Description	Amount of the initial order including tax
Format **Possible value(s)**	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Example	95.25EUR

Field	**montant_recredit**
Presence	Mandatory
Description	Amount to refund including tax
Format **Possible value(s)**	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}

Field	**montant_possible**
Presence	Mandatory if the parameter **montant_deja_recredite** is not provided Optional otherwise
Description	Maximum refund amount including tax permitted for the authorisation number provided
Format **Possible value(s)**	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Addition	If a refund has already been made with this authorisation number, it must be deducted by the merchant. For example, for an order of €100, if €10 had already been refunded, the next refund would have a "montant_possible" amount of €90.
Example	95.25EUR

Field	**montant_deja_recredite**
Presence	Mandatory if the parameter **montant_possible** is not provided Optional otherwise
Description	Amount successfully refunded
Format Possible value(s)	A whole number A decimal point (optional) A whole number with 2 figures (optional) A currency with 3 alphabetical characters as per ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Addition	If this authorisation number has successful refunds, they must be provided. For example, if this authorisation number had refunds of €10, the next refund request would have a "montant_deja_recredite" of €10.
Example	95.25EUR

Field	**reference**
Presence	Mandatory
Description	Reference of the order.
Format Possible value(s)	50 alphanumerical characters maximum. [a-zA-Z0-9]{1,50}
Example	REF7896543

Field	**lgue**
Presence	Mandatory
Description	Language code in upper case
Format Possible value(s)	DE EN ES FR IT JA NL PT SV [A-Z]{2}
Example	FR

Field	**societe**
Presence	Mandatory
Description	Alphanumerical code allowing the merchant to use the same virtual POS for different sites (separate settings) relating to the same activity
Format Possible value(s)	Alphanumerical
Example	myCompany

Field	**MAC**
Presence	Mandatory
Description	Seal resulting from the certification of data sent to the payment system.
Format Possible value(s)	40 hexadecimal characters [A-Fa-f]{40}
Example	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Field	**numero_dossier**
Presence	Optional
Description	Pre-authorisation dossier number
Addition	Only for a POS in pre-authorisation
Format Possible value(s)	12 alphanumerical characters
Example	20150901PRE1

Field	**facture**
Presence	Optional
Description	Type of invoice to generate
Addition	Only for a POS in pre-authorisation
Format Possible value(s)	preauto noshow complementaire
Example	noshow

5.2.2 Credit card and ApplePay Wallet special case

For payments made using a credit card or ApplePay Wallet, it is possible to make a refund without providing the authorization number “num_autorisation” and the collect date “date_remise”. In this case, the refund is perform on the whole order, and the parameters “montant_possible” and “montant_deja_recredite” needs to be adapted.

5.2.3 Calculation of seal

To calculate the MAC, refer to the documentation in appendix.

5.2.4 Control of the IP and limit on the number of refunds

For security reasons, refund requests can only be issued from servers with an IP address known by our services. In addition, each IP address is limited daily in the number of refund requests it is authorised to make.

Before being able to make refund requests in the production environment, you therefore need to send an email to technical support (see chapter 7 Technical support) with the list of IP addresses to authorise, as well as the maximum number of daily refunds for each of them.

5.2.5 Example of a refund request

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

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=100.00EUR
          &montant_recredit=32.00EUR
          &montant_possible=100EUR
          &reference=ABERTPY00145
          &lgue=FR
          &societe=monSite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

If successful, a refund for a maximum sum of €68 is still possible.

Example 2: full refund for an order of €100

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=100.00EUR
          &montant_recredit=100EUR
          &montant_possible=100EUR
          &reference=ABERTPY00145
          &lgue=FR
          &societe=monSite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

Exemple 3 : full refund for an order of €100 payed by card

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
          &montant=100.00EUR
          &montant_recredit=100EUR
          &montant_deja_recedite=0EUR
          &reference=ABERTPY00145
          &lgue=FR
          &societe=monSite1
          &MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

5.3 Response of the refund request

5.3.1 Returned information

In response to the refund request, the merchant's application receives a message of acknowledgement from the Monetico Paiement server. This message is a "text/plain" MIME document specifying the result of the refund.

It contains the following fields separated by a character CHR (10) which corresponds to a line break.

Field	**cdr**
Description	Return code indicating the result of the refund
Format **Possible value(s)**	0: refund completed <0: error

Field	**lib**
Description	Detailed description stating the nature of the return code
Format **Possible value(s)**	See below for the list of possible descriptions

Field	**version**
Description	Version number of the acknowledgement message
Format **Possible value(s)**	Only "1.0"

Field	**reference**
Description	Reference of the order

Field	**numero_dossier**
Description	Number of the dossier which has just been refunded
Addition	Only for a POS in pre-authorisation
Format **Possible value(s)**	12 alphanumerical characters maximum.
Example	20150901PRE1

Field	**type_facture**
Description	Type of invoice that was just made
Format **Possible value(s)**	preauto noshow complementaire
Example	noshow

The list of values available for the description is given in the following table:

cdr	lib	Description	Note
0	**recredit effectue**	The refund request has been accepted	
-1	**recredit refuse**	The refund request has not been accepted	
-30	**Commercant non identifie**	The settings to identify the merchant site are incorrect	**Verify the company, POS and language (societe, TPE and lgue) fields**
-31	**signature non validee**	The MAC signature is invalid	
-32	**recredit non autorise**	Your POS is not authorised to perform refunds	**Contact technical support**
-33	**demande de recredit expiree**	The refund date exceeds the authorised time-frame (+/- 24 hours)	**Verify the date setting**
-34	**montant de recredit errone**	The amount to refund is incorrect	**Verify the montant_recredit setting**
-35	**Les montants transmis sont incorrects**	The amounts transmitted are not in phase with those of the bank server	**Verify the montant_recredit and montant_possible fields**
-36	**le maximum de recredit a été atteint**	The maximum number of refunds for your POS has been reached	
-37	**la commande est inexistante**	The order does not exist	**Verify that the fields identifying the order are correct**
-38	**la commande ne peut pas donner lieu a un recredit**	The order has not yet been paid, no refund can be made	
-39	**le paiement est inexistant**	An authorisation request has already been issued 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 does not correspond to the currency of the order	**Verify the devise (currency) setting**
-43	**parametres invalides**	One or more settings do not comply with the required format	**Verify the length of the fields and the format of dates**
-44	**autre traitement en cours**	Another transaction is being processed with the same reference; this may be a process other than a recredit_paiement	**Repeat the request**
-45	**verification carte echouee**	The card status does not allow the transaction (stolen, opposed, …)	
-46	**la commande est deja entierement recreditee**	The payment is already entirely refunded	**Check that the amount parameters of the request is correct**
-47	**plusieurs traitements ont ete trouves**	It was not possible to determine which Cofidis payment has to be refunded due to a missing payment reference	**Check the parameter ref_remise**
-48	**echec du recredit, recredit potentiellement partiel**	The PayPal refund was partially done	**Check that the amount parameters of the request is correct**

-49	**AMEX est désactivé pour ce commercant**	A refund is requested on a payment associated to an EPT with no AMEX configuration (AMEX have probably been removed from the EPT)	
-50	**numero d'autorisation et date de remise sont a fournir ensemble**	The authorization number or the collect date is missing.	**Check the parameters num_autorisation and date_remise**
-51	**le recredit global n'est pas permis pour cette commande**	« Global Refund » is not possible on this order, please provide the authorisation number and the collect date	**Provide the parameters num_autorisation and date_remise**
-52	**le montant deja recredite est incorrect**	The already refunded amount you provided is incorrect	**Check the parameter montant_deja_recredite**

5.3.2 Examples of messages returned

- Case of accepted refund

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

- Case of error

```
version=1.0
reference=000000000145
cdr=-31
lib=the amounts transmitted are incorrect
```

- Case of accepted refund in pre-authorisation

```
version=1.0
reference=000000000145
cdr=0
lib=recredit completed
aut=353683
date_recredit=2019-05-21
montant_recredit=1EUR
numero_dossier=1010
type_facture=preauto
```

6 Summary file

The information we send to your feedback interface can also be provided to you in a consolidated manner via a summary file.

Sending this file or suspending this file is configured from your dashboard[2]. The settings that you can customise are:

- frequency of sending: daily, weekly or monthly,
- preferred order statuses: Recorded, Rejected, Failed, Paid, Cancelled,
- the file format you wish to receive: CVS or XML
- the type of sending: email or ftp,
- the configuration for sending the email or ftp.

The file sent to you contains the following fields:

Field	Description	Comment
1	POS number	
2	Date of collection	format YYYY-MM-DD
3	Reference of the order	as provided by the merchant
4	Order status: according to the preferred status selection made by the merchant	AN: you have cancelled the payment request AU: payments successfully recorded and pending collection GR: order cancelled following 4 unsuccessful attempts PA: the payment has been authorised and collected PP: partial payment recorded and pending collection RE: the payment authorisation was not granted
5	Date of the payment request	format YYYY-MM-DD
6	Time of the payment request	format hh:mm:ss
7	Amount including tax of the transaction formatted in the following way: - A whole number - A decimal point (optional) - A whole number (optional)	
8	Currency of the transaction	in 3 alphanumerical characters as per ISO4217 (EUR, USD, GBP, CHF, etc.)
9	Authorisation number as provided by the issuing bank	Only if authorisation was given

[2] A help page helps you to find the configuration best suited to your needs.

10	Collection of the acknowledgement of receipt from the merchant's feedback interface	OK: your feedback interface provided a valid acknowledgement of receipt NOK: your feedback interface did not provide a valid acknowledgement of receipt
11	Archiving reference	Only in the event of subscribing to the fraud prevention module
12	Type of card	AM: American Express CB: Carte Bancaire MC: Mastercard VI: Visa Only in the event of subscribing to the fraud prevention module
13	Date of validity of the card	format `MMYY` Only in the event of subscribing to the fraud prevention module
14	Presence of the visual cryptogram	yes no Only in the event of subscribing to the fraud prevention module
15	Free text as provided by the merchant	
16	3DS status	-1: the transaction did not take place according to the 3D Secure protocol and the risk of non-payment is high 1: the transaction took place according to the 3DS protocol and the risk of non-payment is low 4: the transaction took place according to the 3DS protocol and the risk of non-payment is high
17	Card number alias	One-way hashing (HMAC-SHA1) of the bank card number Only in the event of subscribing to the fraud prevention module
18	Card BIN	BIN code of the card holder's bank Only in the event of subscribing to the fraud prevention module
19	Origin of the card	Country code of the bank issuing the bank card as per ISO 3166-1 Only in the event of subscribing to the fraud prevention module

20	IP address of the customer that made the transaction	Only in the event of subscribing to the fraud prevention module
21	Origin of the transaction	Country code as per ISO 3166-1 Only in the event of subscribing to the fraud prevention module

7 Installation aids

7.1 Put a POS in production

You must aks the technical support service (see chapter 7) to put your POS in production.

Before this, the last three test payments made in the past seven days must have sent back a valid acknowledgement of receipt (authorisation request accepted and response to CGI2).

7.2 FAQs

Can the payment page be customised?

Yes, it is possible to customise the look of the payment page by adding this option to your contract. It is possible to change the colours, images and buttons.

How to display my logo on your payment page?

You must send the technical support service an email with either the URL or an image representing your logo, or the logo as an attachment. This image must be provided in GIF format and be 120x120 pixels maximum.

What is the maximum time for my customer to make the payment (enter the card number) following an order on my site?

The web user has 45 minutes from the time they reach the payment page to enter their bank card information. After this, any input will be rejected.

How many attempts do they have to enter their bank card number?

The maximum number of payment attempts is 4.

Where can the card numbers for tests be found?

On the payment page, you will see a flashing "TEST" icon; if you click on this, a window opens presenting different test card numbers. All you need to do is select one of the cards and the payment page form is filled in automatically.

There are several test cards simulating the different possible payment scenarios.

Which languages does the payment page manage?

- French
- English
- German
- Spanish
- Italian
- Dutch
- Portuguese
- Swedish
- Japanese

Can we receive an email for every payment request?

A notification may be sent by email every time an authorisation request is made (an authorisation request is made if the bank card number is validated). This option must be activated by contacting the technical support service (see chapter 7).

Can a payment be refunded?

Yes, for this you need to request the "refund" option from your sales rep. This function is then available on the merchant's dashboard.

What do the different "URL_RETOUR" in the settings refer to?

- url_retour_ok: corresponds to the link (allowing the buyer to return to a page in your shop) displayed at the bottom of our payment page if the payment is accepted
- url_retour_err: corresponds to the link (allowing the buyer to return to a page in your shop) displayed at the bottom of our payment page if the payment is rejected, or the first time the payment page is displayed.

You must not confuse these URLs with the "Response" interface URL.

What is the "CGI2 confirmation URL"?

This URL is the one for your "Response" interface. Its role is to receive the payment confirmation message issued by the Monetico Paiement server.

Where is the "CGI2 confirmation URL" configured?

This URL is entered in our databases; you must give it to us during the solution installation phase. You must also inform us of any change of address of your "Response" interface (by contacting the technical support service - see chapter 7).

What do I do if I get a "CGI2 NOT OK" error?

You first have to make the following verifications:

- Is the address of the "Response" interface you provided valid?
- Is this address accessible on your server from the exterior?
- Is the port of your "Response" interface either 80 (http) or 443 (https)? Our payment server can only address these two ports.

If the problem persists, please make the following extra verifications:

- the processing time between feedback from our server and sending of your acknowledgement of receipt must not take too long (less than 30 seconds)
- no redirection must be made when receiving the payment return code
- The format of the acknowledgement of receipt sent back must correspond to the format required for a valid seal.

How to interpret the meaning of the error code indicated in the email sent back in the event of an incorrect acknowledgement of receipt?

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

Why does my "CG12 confirmation URL" receive different return codes for the same reference?

Your customers have 4 attempts to enter their bank information for the same reference within a maximum time-frame of 45 minutes.

After each attempt, we send the result to your confirmation URL. Therefore, you may receive several rejection notifications ("Cancellation" return code) before receiving a possible payment notification ("payment" return code) for the same reference.

Example of a process with several confirmation URL calls:

A customer pays for reference ref0001but does not receive a payment authorisation with the bank card they are using.

Our server will send a rejection notification:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&reference=ref0001&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-libre=LeTexteLibre&code-retour=Annulation&cvx=oui&vld=1208&brand=VI&status3ds=1&motifrefus=Refus&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&&authentification=ewoJIn(…)KfQo=
```

The customer can attempt to pay again and uses their second bank card to pay for reference ref0001. This time, payment is accepted.

Our server will send a payment notification:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f12%3a15%3a33&montant=62%2e75EUR&reference=ref0001&MAC=f4562a2c18d86cfdbaf646016c202e89945841&texte-libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1210&brand=VI&status3ds=1&numauto=010101&originecb=FRA&bincb=010101&hpancb=12754C03C22D786E0F2C2CADBFC1C00A25df6322&ipclient=127%2e0%2e0%2e1&originetr=FRA&&authentification=ewoJIn(…)KfQo=
```

How to modify the default payment schedule of my split payments?

When your POS is in split payment, it is configured to comply with a default payment schedule that you defined when subscribing to your contract.

You can define a specific payment schedule for each order to override the default payment schedule of your POS.

This payment schedule must comply with the following restrictions:

- a number of instalments between 2 and 4 (nbrech setting)
- the sum of the instalments is equal to the sum of the order (montantech1, montantech2, montantech3, montantech4 settings)
- the instalment dates are one month apart (dateech1, dateech2, dateech3, dateech4 settings).

How to calculate the date of my instalments?

The instalment dates must be one month apart.

The duration of one month does not correspond to a precise number of days but to the duration between two same days in a calendar month or otherwise the closest possible date.

Examples:

If your first instalment date is 01/01/2010, the second instalment will be 01/02/2010, the third 01/03/2010 and the fourth 01/04/2010.

If your first instalment date is 31/01/2010, the second instalment will be 28/02/2010, the third 31/03/2010 and the fourth 30/04/2010.

If your first instalment date is 30/01/2012, the second instalment will be 29/02/2012, the third 30/03/2012 and the fourth 30/04/2012.

If you do not follow this system for calculating the instalment dates, you will get the error message "the form data is incorrect".

I received the error Code 0 in the email sent back for incorrect acknowledgement

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

I get the message "This POS is closed" when requesting payment on the TEST server?

The TEST POS that are not used for a rolling 15-day period are automatically closed by our services. They are not, however, deleted: you can use the reopen TEST POS function by connecting to your dashboard.

Is it possible to have one POS for several sites?

Yes, but to do this you need to request this in advance from your sales rep. The different sites have to have the same activity. As the configuration is specific for each site, you will need to send us all the information (return URLs, address of the "Response" interface, logo, etc.).

Can we get a payment statement file?

This can be provided by your bank; you can contact your sales rep.

7.3 The most frequent problems

7.3.1 Problem calculating the security seal

Error message on the payment page

"The information transmitted by your merchant has an invalid signature: The security level requested has not been reached. Our server is not able to process the payment request concerning your order".

Capture request error message

```
version=1.0
reference=<your reference>
cdr=-1
lib=signature not valid
```

Refund request error message

```
version=1.0
reference=<your reference>
cdr=-31
lib=signature not valid
```

Possible causes

- the form you have sent us does not contain all of the information required
- the MAC seal algorithm is incorrect
- the MAC seal algorithm was completed with an incorrect key

Resolution

Carefully follow the path described below. At the end of each step in which you have made changes to your implementation, perform new payment tests. If they are not successful, move to the next step.

Attention: do not skip a step!

Step 1: check that all variables sent in the form are present, spelt correctly, use the correct upper or lower case and comply with any restrictions on the format and characters authorised.

Step 2: check that you have avoided the errors inherent to certain fields:

- does the value of the **MAC** version correspond to a string of 40 hexadecimal characters (authorised values: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F)?
- is the value of the **version** variable 3.0?
- does the value of the **date** variable follow the format DD/MM/YYYY:HH:MM:SS?
- is the value of the **reference** variable a string that only contains letters (without accents) and numbers with a maximum of 12 characters?
- is the **texte-libre** variable spelt correctly, respecting the case and with the hyphen ('-') character and not the underline ('_') character?

Step 3: check that the string on which you are calculating the MAC seal respects the previously described formalism.

Be particularly attentive to the fact that the data used must be the same as the data you provide in the payment form; the best way of doing this is to store the different information in advance and then to use this to calculate the MAC seal and to build the form. Otherwise, entering data on the fly may lead to differences between the data used to calculate the seal and the data used to build the form (for example, for the date field, there may be a difference of a few seconds).

Step 4: check that you are using the right security key:

- you must use the last key given to you by our services,
- check that the key corresponds to your seal calculation algorithm (SHA1 or MD5),
- Contact our support service to validate together that you are using the right key and to validate that the version of your form ("version" field) corresponds to the version configured in our system.

If, despite all of these verifications, you still get this error message, the problem lies in integrating our solution in your information system.

We do not control every aspect of the wide diversity of languages and specificities linked to the environment used for the implementation of our payment solution and consequently, we cannot provide more extensive personalised support.

7.3.2 The merchant cannot be identified

Error message on the payment page

"Your merchant's site was not identified by our server. We are not able to process the payment request concerning your order" ”

Capture request error message

```
version=1.0
reference=<your reference>
cdr=-1
lib=merchant not identified
```

Refund request error message

```
version=1.0
reference=<your reference>
cdr=-30
lib=Merchant not identified
```

Possible causes

- the POS number is incorrect or missing
- the company code is incorrect or missing
- the language code is incorrect or missing
- the IP address of the merchant's server is not authorised to make a refund

Resolution

Check that “TPE”, “societe” and “lgue” variables are present, spelt correctly, use the correct upper or lower case and comply with any restrictions on the format and characters authorised.

7.3.3 The order has already been processed.

Error message

"Your order has already been processed."

Possible causes

You have supplied an order reference that has already been used in a previous transaction.

Resolution

You need to generate a new unique order reference.

7.3.4 The validity date of the order has expired.

Error message

"The validity date of your order has expired."

Possible causes

- either the order reference has been in the payment process for too long (usually more than one hour)
- or the order form was created too long ago, usually more than 12 hours ago

Resolution

- test a form updated with a new order reference
- test a new form and verify the system date of your server

7.3.5 The payment method used is not available.

Error message

"Payment method not available."

Possible causes

- either there is a syntax error in the form submitted
- or the merchant has not subscribed to the payment method

Resolution

Check that the variables in the form are spelt correctly, use the correct upper or lower case and comply with any restrictions on the format and characters authorised.

Check that you are not using a payment method other than the one to which you have subscribed.

7.3.6 The order cannot be authenticated

Error message

```
version=1.0
reference=<your reference>
cdr=0
lib=order not authenticated
```

Possible causes

- the reference is incorrect or missing
- the order date is incorrect or missing

Resolution

Check that the reference and date_commande variables are present in the form, spelt correctly, use the correct upper or lower case and comply with any restrictions on the format and characters authorised.

Check that the capture order has been authorised or registered on the date that you enter

7.3.7 The amounts are incorrect

Error message

```
version=1.0
reference=<your reference>
cdr=-1
lib=amount error
```

Possible causes

- one of the amounts transmitted is incorrect
- the sum of the amounts is incorrect

Resolution

Check that the amount, amount_to_capture, amount_already_captured and amount_outstanding variables are present in the form, spelt correctly, use the correct upper or lower case and comply with any restrictions on the format and characters authorised.

Check that the sum of the values of the amount_to_capture, amount_already_captured and amount_outstanding variables is equal to the value of the amount variable for a collection.

Check that the values of the amount_to_capture and amount_outstanding variables are equal to 0EUR for a cancellation.

8 Technical support

Euro Information offers support in the general understanding of its solution:

- By email by writing to the **mailbox**
  - Crédit Mutuel: centrecom@e-i.com
  - CIC: centrecom@e-i.com
- By telephone by calling **0820 821 735**

However, Euro Information cannot provide support for technical integration issues related to its payment solution in the merchant information system.

9 Appendices

9.1 General constraints for HTML coding of the fields

All call request fields, except the version and amounts, must be coded in HTML before being formatted in the form (i.e. immediately after the MAC calculation).

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

Name	Symbol	Replacement
Ampersand	&	**&amp;**
Less than sign	<	**&lt;**
Greater than sign	>	**&gt;**
Double quotes	"	**&quot; or &#x22;**
Apostrophe	`	**&#x27;**

"HTML_ENCODE" functions (see IETF RFC1738) of the languages are perfectly suitable; they encode far more characters, typically everything which is not:

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

If, in the "text-libre" field, you use characters outside the printable ascii range (31<ascii<127), you must encode this field before any payment-related processing to avoid any problem calculating the MAC seal.

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

9.2 Encoding restriction

All non ASCII characters must be UTF-8 encoded.

Every encoding and decoding of our fields must respect the RFC 3986.

9.3 Calculation of MAC seal

The seal (to put in the MAC field) is calculated using a cryptographic hash function combined with a secret key in line with RFC 2104 specifications.
This function will generate a seal based on data to be certified and the merchant's security key in its operational form.

The data to be certified is structured:

- in the form of a sequence *Field_name=Field_value*,
- with the elements separated by a the "*" character,
- listed in alphabetical order

In calls to our services, the seal must take into account all the sent parameters, valorized or not, **recognized by the platform**, and exclusively these parameters.

For our services' responses ("Response" interface), you must include in your seal validation **all parameters sent by our server**, even the ones unknown or unused by your server. Please remember that the fields names and values must be decoded according to the RFC 3986 before the seal calculation step.

Ex: if a parameter contains a string « %2B » in its name or value, the string must be decoded as « + » in order to ensure a correct seal calculation.

Note:

The order used is based on the ASCII code. In addition, it is case sensitive:

- first, the numbers from 0 to 9,
- then, characters in UPPER CASE,
- lastly, characters in lower case.
- For special characters, refer to the ASCII table

9.3.1 Examples of strings to calculate the seal

9.3.1.1 "Out" phase

a) Order context

Example of the "contexte_commande" field:

```
{
   "billing":{
      "firstName":"Jérémy",
      "lastName":"Grimm",
      "addressLine1":"3 rue de l'église",
      "city":"Ostheim",
      "postalCode":"68150",
      "country":"FR"
   },
   "shipping":{
      "firstName":"Jérémy",
      "lastName":"Grimm",
      "addressLine1":"3 rue de l'église",
      "city":"Ostheim",
      "postalCode":"68150",
      "country":"FR",
      "email":"jerem68@hotmail.com",
      "phone":"+33-612345678",
      "shipIndicator":"billing_address",
      "deliveryTimeframe":"two_day",
      "firstUseDate":"2017-01-25",
      "matchBillingAddress":true
   },
   "client":{
      "email":"jerem68@hotmail.com",
      "phone":"+33-612345678",
      "birthCity":"Colmar",
      "birthPostalCode":"68000",
      "birthCountry":"FR",
      "birthdate":"1987-03-27"
   }
}
```

Therefore, after encoding in base64:

```
ewogICAiYmlsbGluZyI6ewogICAgICAiZmlyc3ROYW1lIjoiSsOpcsOpbXkiLAogICAgICAibGFzdE5hbWUiOiJHc
mltbSIsCiAgICAgICJhZGRyZXNzTGluZTEiOiIzIHJ1ZSBkZSBsJ8OpZ2xpc2UiLAogICAgICAiY2l0eSI6Ik9zdGhl
aW0iLAogICAgICAicG9zdGFsQ29kZSI6IjY4MTUwIiwKICAgICAgImNvdW50cnkiOiJGUiIKICAgfSwKICAgInNo
aXBwaW5nIjp7CiAgICAgICJmaXJzdE5hbWUiOiJKw6lyw6lteSIsCiAgICAgICJsYXN0TmFtZSI6IkdyaW1tIiwKIC
AgICAgImFkZHJlc3NMaW5lMSI6IjMgcnVlIGRlIGwnw6lnbGlzZSIsCiAgICAgICJjaXR5IjoiT3N0aGVpbSIsCiAgI
CAgICJwb3N0YWxDb2RlIjoiNjgxNTAiLAogICAgICAiY291bnRyeSI6IkZSIiwKICAgICAgImVtYWlsIjoiamVyZW0
2OEBob3RtYWlsLmNvbSIsCiAgICAgICJwaG9uZSI6IiszMy02MTIzNDU2NzgiLAogICAgICAic2hpcEluZGljYXR
vciI6ImJpbGxpbmdfYWRkcmVzcyIsCiAgICAgICJkZWxpdmVyeVRpbWVmcmFtZSI6InR3b19kYXkiLAogICAgI
CAiZmlyc3RVc2VEYXRlIjoiMjAxNy0wMS0yNSIsCiAgICAgICJtYXRjaEJpbGxpbmdBZGRyZXNzIjp0cnVlCiAgI
H0sCiAgICJjbGllbnQiOnsKICAgICAgImVtYWlsIjoiamVyZW02OEBob3RtYWlsLmNvbSIsCiAgICAgICJtb2JpbG
VQaG9uZSI6IiszMy02MTIzNDU2NzgiLAogICAgICAiYmlydGhDaXR5IjoiQ29sbWFyIiwKICAgICAgImJpcnRoU
G9zdGFsQ29kZSI6IjY4MDAwIiwKICAgICAgImJpcnRoQ291bnRyeSI6IkZSIiwKICAgICAgImJpcnRoZGF0ZSI6I
jE5ODctMDMtMjciCiAgIH0KfQ==
```

b) *Immediate payment*

TPE=1234567*contexte_commande=ewoJI(…)KCX0KfQ==*date=05/12/2006:11:55:23*dateech1=*dateech2=*dateech3=*dateech4=*lgue=FR*mail=internaute@sonemail.fr*montant=62.73EUR*montantech1=*montantech2=*montantech3=*montantech4=*nbrech=*options=*reference=ABERTYP00145*societe=monSite1*texte-libre=ExempleTexteLibre*version=3.0

c) *Split payment*

TPE=1234567*contexte_commande=ewoJI(…)KCX0KfQ==*date=05/12/2006:11:55:23*dateech1=05/12/2006*dateech2=05/01/2007*dateech3=05/02/2007*dateech4=05/03/2007*lgue=FR*mail=internaute@sonemail.fr*montant=62.73EUR*montantech1=16.23EUR*montantech2=15.5EUR*montantech3=15.5EUR*montantech4=15.5EUR*nbrech=4*options=*reference=ABERTYP00145*societe=monSite1*texte-libre=ExempleTexteLibre*version=3.0

9.3.1.2 Response phase

Simple payment with registration to the fraud prevention module and the 3D Secure option.

TPE=1234567*authentification=ewoJIn(…)KfQo=*bincb=010101*brand=VI*code-retour=paiement*cvx=oui*date=05/12/2006_a_11:55:23*ecard=non*hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45*ipclient=127.0.0.1*montant=62.75EUR*numauto=010101*originecb=FRA*originetr=FRA*reference=ABERTYP00145*texte-libre=LeTexteLibre*typecompte=inconnu*usage=credit*version=3.0*vld=1208

9.3.1.3 Capture service

TPE=1234567*date=05/12/2006:11:55:23*date_commande=05/12/2006*lgue=FR*montant=62.00EUR*montant_a_capturer=62.00EUR*montant_deja_capture=0EUR*montant_restant=38EUR*reference=ABERTYP00145*societe=monSite1*version=3.0

9.3.1.4 Cancellation of payment/recurrence service

Payment cancellation
TPE=1234567*date=05/12/2006:11:55:23*lgue=FR*montant_a_capturer=0EUR*montant_deja_capture=0EUR*montant_restant=0EUR*reference=ABERTYP00145*societe=monSite1*texte-libre=ExempleTexteLibre*version=3.0

Cancellation of recurrence
1234567*date=05/12/2006:11:55:23*lgue=FR*montant_a_capturer=0EUR*montant_deja_capture=0EUR*montant_restant=0EUR*reference=ABERTYP00145*societe=monSite1*texte-libre=ExempleTexteLibre*version=3.0

9.3.1.5 Refund service

TPE=1234567*date=05/12/2006:11:55:23*date_commande=05/12/2006*date_remise=05/12/2006*lgue=FR*montant=100.00EUR*montant_possible=100.00EUR*montant_recredit=32.00EUR*num_autorisation=000000*reference= ABERTYP00145*societe= monSite1*version=3.0

9.4 Old call to the “Response” interface

This section is only for merchants making the transition from the old MAC seal calculation to the new one and having to manage calls to the response interface for orders created before modification. It should be ignored in all other cases. It describes the fields returned and the calculation of the seal validating them, in the case of version 3.0.

9.4.1 Parameters returned by the bank

Fields	Description	Note
MAC	Seal resulting from certification of data	
date	Date of request of authorization of the order in the format `DD/MM/YYYY_a_HH:MM:SS`	
TPE	Virtual EPT merchant number	**The bank server sends here the data as received during the payment « Request» phase**
montant	TTC amount of the order formatted as follows: An integer A decimal point (optional) An integer (optional) A currency of 3 alphabetical characters ISO4217 (`EUR`, `USD`, `GBP`, `CHF`, etc.)	
reference	Unique order reference	
texte-libre	Free text field	
code-retour	The result of the payment, among: `payetest` payment accepted (in TEST only) `paiement` payment accepted (in Production only) `Annulation` payment declined In split payment, for automatic recovery of due dates of row > 1: `paiement_pf[N]` payment accepted of due date N (N between 2 and 4) `Annulation_pf[N]` payment declined permanently of the due date N (N between 2 and 4)	**In case of payment declined, a subsequent authorization can still be delivered for the same reference.** **The code « payetest » is sent only for payments made in the validation environment. If this code is present during a payment in production, there is an anomaly.**
cvx	`oui` if the visual cryptogram (required for Visa and MasterCard cards) was entered `non` otherwise	

vld	Validity date of the credit card used to make the payment	
brand	Network code of the card with 2 alphabetical positions in. AM American Express CB GIE CB MC Mastercard VI Visa na Not available	**The value « na » is systematically returned in the test environment.**
status3ds	3DSecure exchange indicator: -1 : the transaction was not done according to the 3DSecure protocol 1 : the transaction is done according to the 3DS protocol and the risk level is low 4 : the transaction is done according to the 3DS protocol and the risk level is very high	
numauto	Authorization number as provided by the issuer bank	**Only in case where authorization has been granted**
motifrefus	Reason for rejection of payment request : Appel phonie : the bank of the customer requests additional information Refus: the bank of the customer refuses to grant authorization Interdit: the bank of the customer refuses to grant authorization filtrage: the payment request has been blocked by the filter settings that the merchant has set in his Fraud Prevention Module scoring: the payment request has been blocked by the setting of scoring that the merchant has set in his Fraud Prevention Module 3DSecure: if the refusal is related to a negative 3DSecure authentication received from the bank of the holder	**Only if the payment request was rejected.**
originecb	Country code of the bank issuing the bank card (standard ISO 3166-1)	**Only in case of subscription of the fraud prevention module**
bincb	BIN code of the bank of the credit card holder	

hpancb	Irreversible hashing (HMAC-SHA1) of the credit card number used to make the payment (uniquely identifying a credit card for a given merchant)	
ipclient	IP address of the customer who performed the transaction	
originetr	Country code of the origin of the transaction (standard ISO 3166-1)	
veres	3DSecure status of the VERes	**In case of subscription of the fraud prevention module and the 3Dsecure option**
pares	3DSecure status of the PARes	
montantech	Amount of current due date	**Only in case of split payment**
filtragecause	Numbers of types of filters blocking payment (see table « Fraud Prevention Module Returns – details » below) 1: IP address 2: Card number 3: Card BIN 4: Country of the card 5: Country of the IP 6 : Consistency Country of the card / Country of the IP 7 : Disposable email 8 : Limitation in amount for a BC over a given period 9 : Limitation in number of transactions for a BC over a given period 11 : Limitation in number of transactions by alias over a given period 12 : Limitation in amount by alias over a given period 13 : Limitation in amount by IP over a given period 14 : Limitation in in number of transactions by IP over a given period 15 : Card testers 16 : Limitation in number of alias by BC	**Only in case of a payment filtering or if information mode is used.** **If multiple filters blocking the payment, they are separated by hyphens. The causes and corresponding values are in the same order.**
filtragevaleur	Data that generated the blocking	
filtrage_etat	Present in the response only if « information » mode is used. information : Information mode	

cbenregistree	Boolean indicating whether the card was registered under a given aliasbc: 1: The customer has entered a bank card and it was registered under the aliasbc sent 0: All other cases	**Only in case of subscription of the express payment option**
cbmasquee	First 6 and last 4 digits of the bank card of the customer, separated by stars, only during registration of the bank card	**Only in case of subscription of the express payment option.** **Example:** 123456******7890

modepaiement	Means of payment used
	`CB`
	`paypal`
	`1euro`
	`3xcb`
	`4xcb`
	`audiotel`	

Fraud Prevention Module Returns– Details

The feature of filtering of payments is based on a set of nine filters, freely configurable on the dashboard (new version). Each of these filters acts on specific criteria, such as the IP address of the customer, his email address, country of his bank card…

Filter type number	Analysis criteria	Value returned due to blocking	Note
1	IP address	IP address of the customer	
2	Card number	Hash of the customer card	Works only for payments by card
3	Card BIN	Bin of the customer card	
4	Country of the card	Country of the customer card	
5	Country of the IP	Country of the customer IP	
6	Consistency Country of the card / Country of the IP	Country of the card # Country of the IP address of the customer	Works only for payments by card
7	Disposable email	Name of the domain of the email address of the customer	
8	Limitation in amount for a BC over a given period	Cumulative amount in euros (€) over a given period associated with the customer card	Works only for payments by card
9	Limitation in number of transactions for a BC over a given period	Number of transactions accumulated over a given period associated with the customer card	
11	Limitation in number of transactions by alias over a given period	Number of transactions accumulated over a given period associated with the customer alias	Only in case of subscription of the express payment option
12	Limitation in amount by alias over a given period	Cumulative amount in euros (€) over a given period associated with the customer alias	
13	Limitation in amount by IP over a given period	Cumulative amount in euros (€) over a given period associated with the IP address of the customer	
14	Limitation in number of transactions by IP over a given period	Number of transactions accumulated over a given	

		period associated with the IP address of the customer	
15	Card testers	Number of transactions accumulated over a given period associated with the IP address of the customer	
16	Limitation in number of alias by BC	The alias already associated with the card used for payment	Only in case of subscription of the express payment option Works only for payments by card.

Example of data sent by the payment server of the bank to the « Response » interface for an immediate, deferred, partial or recurrent payment:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2
CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&ver
es=Y&pares=Y
```

Example of data send by the payment server of the bank to the « Response » interface for the first due date of a split payment:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2
CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&ver
es=Y&pares=Y&montantech=20EUR
```

Example of data sent by the payment server of the bank to the « Response » interface for a blockage of immediate payment by the MPF:

```
TPE=9000001&date=05%2f10%2f2011%5fa%5f15%3a33%3a06&montant=1%2
e01EUR&reference=P1317821466&MAC=70156D2CFF27A9B8AAE5AFEBE590D
9CFCAAF9BDC&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=FRA&bincb=513283&hpancb=764AD2
4CFABBB818E8A7DC61D4D6B4B89EA837ED&ipclient=10%2e45%2e166%2e76
&originetr=inconnue&veres=&pares=&filtragecause=4-
&filtragevaleur=FRA-
```

Example of data sent by the payment server of the bank to the « Response » interface for a payment with express payment option:

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2
CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbe
nregistree=1&cbmasquee=123456******7890
```

Note:

Countries are designated by their three letter iso code according to the standard ISO 3166-1 alpha-3.

9.4.2 Validation of the seal

The confirmation message received is sealed with a MAC seal that was computed by the payment server of the bank using the merchant security key assigned to your payment terminal.

A validation function of the seal must be implemented in the « Response » interface to ensure that there has been no falsification of data contained in the confirmation message of payment received.

For that, the function must recalculate the MAC code associated with the message and compare it to that transmitted in the message: if the two codes are identical, the information received is reliable (integrity of information and authentication of the issuer).

To compute the MAC it is necessary to use a cryptographic hashing function in combination with a secret key adhering to the specifications of the RFC 2104.
This function will generate the seal from the data to certify and merchant security key in its operational form.
The data to be certified will be presented in the form of a concatenation in a specific order of information sent by the bank server:

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

Example if you are enrolled in the fraud prevention module and the 3DSecure option and the payment is accepted:

```
1234567*05/12/2006_a_11:55:23*62.75EUR*ABERTYP00145*LeTexteLibre*3.0*paiement*oui*1208*VI*1*010101**FRA*010101*74E94B03C22D786E0F2C2CADBFC1C00B004B7C45*127.0.0.1*FRA*Y*Y*
```

9.5 Detail of the JSON document "contexte_commande"

9.5.1 General points and exclusions

This field contains the information concerning the context of the order and is used during the "Out" phase.

This information is necessary to implement 3D Secure (2.X) and to fight fraud.

Note that operation in VPC mode is excluded from 3D Secure, therefore this information is not mandatory in this new mode of operation.

Up to four objects are present in the root of the document.

The presence column can be read as follows:

- Mandatory: this field / node must be provided
- Optional: this field does not have to be provided
- Mandatory if applicable: if the value exists in the context of the order, it must be provided. Example: stateOrProvince exists in the United States

In case some optional data is missing, sending an empty string or an empty object to the server is forbidden.
For a string, you can either:

- Ignore the field.
- Send the field with the *null* value.

For an object, you must ignore the field

Example:

```
"addressLine3":null
```

JSON field	Description	Presence	Detail
billing	Billing address	Mandatory	link
shipping	Shipping address	Mandatory if applicable	link
shoppingCart	Customer's cart	Optional	link
client	Customer information	Optional	link

9.5.2 Detail of the "billing" object

JSON field	Presence	JSON type	Detail
civility	Optional	String	link
name	Optional	String	link
firstName	Optional	String	link
lastName	Optional	String	link
middleName	Optional	String	link
address	Optional	String	link
addressLine1	Mandatory	String	link
addressLine2	Optional	String	link
addressLine3	Optional	String	link
city	Mandatory	String	link
postalCode	Mandatory	String	link
country	Mandatory	String	link
stateOrProvince	Mandatory if applicable	String	link
countrySubdivision	Optional	String	link
email	Optional	String	link
phone	Optional	String	link
mobilePhone	Optional	String	link
homePhone	Optional	String	link
workPhone	Optional	String	link

9.5.3 Detail of the "shipping" object

JSON field	Presence	JSON type	Description
civility	Optional	String	link
name	Optional	String	link
firstName	Optional	String	link
lastName	Optional	String	link
address	Optional	String	link
addressLine1	Mandatory if applicable	String	link
addressLine2	Mandatory if applicable	String	link
addressLine3	Optional	String	link
city	Mandatory if applicable	String	link
postalCode	Mandatory if applicable	String	link
country	Mandatory if applicable	String	link
stateOrProvince	Mandatory if applicable	String	link
countrySubdivision	Optional	String	link
email	Optional	String	link
phone	Optional	String	link
shipIndicator	Optional	String	link
deliveryTimeframe	Optional	String	link
firstUseDate	Optional	String	link
matchBillingAddress	Optional	Boolean	link

9.5.4 Detail of the "shoppingCart" object

JSON field	Presence	JSON type	Description
giftCardAmount	Optional	Number	link
giftCardCount	Optional	Number	link
giftCardCurrency	Optional	String	link
preOrderDate	Optional	String	link
preorderIndicator	Optional	Boolean	link
reorderIndicator	Optional	Boolean	link
shoppingCartItems	Optional	Table of items	link

9.5.4.1 Detail of the "shoppingCartItems" object

If the object “shoppingCart”, in this case, several fields are mandatory in the object “shoppingCartItems” and must be sent.

JSON field	Presence	JSON type	Description
name	Optional	String	link
description	Optional	String	link
productCode	Optional	String	link
imageURL	Optional	String	link
unitPrice	Mandatory	Number	link
quantity	Mandatory if applicable	Number	link
productSKU	Optional	String	link
productRisk	Optional	String	link

9.5.5 Detail of the "client" object

JSON field	Presence	JSON type	Description
civility	Optional	String	link
name	Optional	String	link
firstName	Optional	String	link
lastName	Optional	String	link
middleName	Optional	String	link
address	Optional	String	link
addressLine1	Optional	String	link
addressLine2	Optional	String	link
addressLine3	Optional	String	link
city	Optional	String	link
postalCode	Optional	String	link
country	Optional	String	link
stateOrProvince	Optional	String	link
countrySubdivision	Optional	String	link
email	Optional	String	link
birthLastName	Optional	String	link
birthCity	Optional	String	link
birthPostalCode	Optional	String	link
birthCountry	Optional	String	link
birthStateOrProvince	Optional	String	link
birthCountrySubdivision	Optional	String	link
birthdate	Optional	String	link
phone	Optional	String	link
nationalIDNumber	Optional	String	link
suspiciousAccountActivity	Optional	Boolean	link
authenticationMethod	Optional	String	link
authenticationTimestamp	Optional	String	link
priorAuthenticationMethod	Optional	String	link
priorAuthenticationTimestamp	Optional	String	link
paymentMeanAge	Optional	String	link
lastYearTransactions	Optional	String	link
last24HoursTransactions	Optional	String	link
addCardNbLast24Hours	Optional	String	link
last6MonthsPurchase	Optional	String	link
lastPasswordChange	Optional	String	link
accountAge	Optional	String	link
lastAccountModification	Optional	String	link

9.5.6 Description of attributes

Attribute	**accountAge**
Description	Date of creation of customer account on the merchant's site.
Format	String
Restrictions	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures (ISO 8601)
Attribute	**addCardNbLast24Hours**
Format	Whole
Description	Number of attempts to add the customer card on the retail website during the past 24 hours.

Attribute	**address**
Description	Customer's full address (number, street, additional information)
Format	String
Restrictions	Up to 255 characters

Attribute	**addressLine1**
Description	Contains the number and street name
Format	String
Restrictions	Up to 50 characters

Attribute	**addressLine2**
Description	Contains the number and street name
Format	String
Restrictions	Up to 50 characters

Attribute	**addressLine3**
Description	Any additional information concerning the address that is not entered in lines 1 and 2 of the address.
Format	String
Restrictions	Up to 50 characters

Attribute	**authenticationMethod**
Description	Method of authenticating the customer on the retail website.
Format	String
Possible values	"guest": no authentication "own_credentials": use of an account open on the retail website "federated_id": federated identity "issuer_credentials": identifiers supplied by the issuer "third_party_authentication" "fido": use of FIDO authentication

Attribute	**authenticationTimestamp**
Description	Date and UTC time of the customer's authentication on the retail website.
Format	String
Restrictions	Type YYYY-MM-DD**T**HH-mm-SS**Z** where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures, HH = time in 2 figures, mm = minutes in 2 figures, SS = seconds in two figures (ISO 8601)

Attribute	**birthCity**
Description	City of birth
Format	String
Restrictions	Up to 50 characters

Attribute	**birthCountry**
Description	Country of birth
Format	String
Restrictions	Country code in 2 characters as per ISO 3166-1 alpha-2

Attribute	**birthCountrySubdivision**
Description	Geographic code of the entity of the country of birth
Format	String
Restrictions	Follow ISO 3166-2.
Help	https://en.wikipedia.org/wiki/ISO_3166-2 https://en.wikipedia.org/wiki/ISO_3166-2:FR

Attribute	**birthdate**
Description	Birth date as per ISO 8601 format
Format	String
Restrictions	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ()

Attribute	**birthLastName**
Description	Birth name
Format	String
Restrictions	Up to 45 characters

Attribute	**birthPostalCode**
Description	Postal code of birthplace
Format	String
Restriction	Up to 10 characters

Attribute	**birthStateOrProvince**
Format	String
Restrictions	ISO 3166-2
Description	Geographic code of the state or province of birth (if applicable).
Help	https://fr.wikipedia.org/wiki/ISO_3166-2:US https://fr.wikipedia.org/wiki/ISO_3166-2:CA

Attribute	**city**
Format	String
Restrictions	Up to 50 characters
Description	City May contain the CEDEX.

Attribute	**civility**
Description	Civility
Format	String
Restrictions	Up to 32 alphabetical characters. No punctuation. Examples: "Mr, "Mrs"

Attribute	**country**
Description	Country code
Format	String
Restrictions	ISO 3166-1 alpha-2 / case sensitive (uppercase)

Attribute	**countrySubdivision**
Description	Geographic code of the entity of the country
Format	String
Restrictions	ISO 3166-2
Help	https://en.wikipedia.org/wiki/ISO_3166-2 https://en.wikipedia.org/wiki/ISO_3166-2:FR

Attribute	**deliveryTimeframe**
Description	Indicates the delivery time-frame for the order.
Format	String
Possible values	"same_day" "overnight" "two_day" "three_day" "long": more than three days "other" "none": no shipment

Attribute	**description**
Description	Description of an item.
Format	String
Restrictions	Up to 2048 characters.

Attribute	**email**
Format	String
Restrictions	Up to 254 characters. Must match the pattern “^.+@.+\..+$”
Description	Email

Attribute	**firstName**
Description	First name
Format	String
Restrictions	Up to 45 characters

Attribute	**firstUseDate**
Description	Date on which the shipping address was first used.
Format	String
Restrictions	ISO 8601 format Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ()

Attribute	**giftCardAmount**
Description	Amount used to buy gift cards / codes, expressed in the smallest unit of currency.
Format	Number
Restrictions	Whole number Maximum of 12 meaningful numbers

Attribute	**giftCardCount**
Description	Number of gift cards purchased
Format	Number
Restrictions	Whole number Maximum of 2 meaningful numbers

Attribute	**giftCardCurrency**
Format	String
Restrictions	3 alphabetical characters (e.g.: EUR). ISO 4217
Description	Currency of the gift card purchased

Attribute	**homePhone**
Description	Telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number
Example	The French number 05 12 34 56 78 will be written "+33-512345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribute	**imageURL**
Description	URL pointing to an image associated with an item.
Format	String
Restrictions	Up to 2000 characters.

Attribute	**last24HoursTransactions**
Format	Positive whole number or zero
Description	Number of transactions (completed or aborted) made by the customer with any payment method registered on the retail website in the past 24 hours.

Attribute	**last6MonthsPurchase**
Description	Number of purchases with this payment method in the past 6 months.
Format	Positive whole number or zero

Attribute	**lastAccountModification**
Description	Date of last modification of the customer account (including new billing address, new delivery address, new payment method registered).
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures () ISO 8601

Attribute	**lastName**
Description	Family name.
Format	String
Restrictions	Up to 45 characters.

Attribute	**lastPasswordChange**
Description	Date on which the customer changed their password or reset their account for the last time.
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures () ISO 8601

Attribute	**lastYearTransactions**
Format	Positive whole number or zero
Description	Number of transactions (completed or aborted) made by the customer with any payment method registered on the retail website in the past year.

Attribute	**matchBillingAddress**
Description	Indicates whether the shipping or billing addresses are the same.
Format	Boolean

Attribute	**middleName**
Description	Middle name(s)
Format	String
Restrictions	Up to 150 characters

Attribute	**mobilePhone**
Description	Mobile telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number
Example	The French mobile number 06 12 34 56 78 will be written "+33-612345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribute	**name**
Description	Last Name and First Name
Format	String
Restrictions	Up to 45 characters

Attribute	nationalIDNumber
Description	Number of piece of ID
Format	String
Restrictions	Up to 255 characters

Attribute	paymentMeanAge
Description	Date on which the card was added to the customer account (on the retail website).
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ISO 8601

Attribute	phone
Description	Telephone number
Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number
Example	The French number 05 12 34 56 78 will be written "+33-512345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribute	postalCode
Description	Post or zip code
Format	String
Restrictions	Up to 10 characters

Attribute	preOrderDate
Description	For a pre-order, date on which the goods will be available.
Format	Type YYYY-MM-DD where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures ISO 8601

Attribute	preorderIndicator
Description	Indicates whether it is a pre-order.
Format	Boolean

Attribute	priorAuthenticationMethod
Description	Customer's previous authentication method on the retail website.
Format	String
Possible values	"frictionless": ACS has made it possible to pay without challenge "challenge": The cardholder had to complete the challenge stage "AVS_verified": Verification of the cardholder address (AVS system) "other": Other authentication method

Attribute	priorAuthenticationTimestamp
Description	Date and UTC time of the customer's previous authentication on the retail website.
Format	String
Restrictions	Type YYYY-MM-DDTHH-mm-SSZ where YYYY = year in 4 figures, MM = month in 2 figures, DD = day in 2 figures, HH = time in 2 figures, mm = minutes in 2 figures, SS = seconds in two figures ISO 8601

Attribute	productCode
Description	Indicates the type of product.
Format	String
Possible values	"adult_content" "coupon" "default": default value (if no other code is suitable) "electronic_good": (not including software) "electronic_software" "gift_certificate" "handling_only": admin fees "service": service delivered to the customer "shipping_and_handling" "shipping_only" "subscription": to a website or other

Attribute	productRisk
Description	Indicates the level of risk related to a product.
Format	String
Possible values	"low" "normal" "high"

Attribute	productSKU
Description	Reference that the merchant gives an item.
Format	String
Restrictions	Up to 255 characters

Attribute	quantity
Format	Number

Restrictions	Whole number
Description	Expresses a quantity (e.g. a number of items)

Attribute	**reorderIndicator**
Description	"True" if, and only if, the customer has already made an identical order.
Format	Boolean

Attribute	**shipIndicator**
Format	String
Description	Chosen shipping method.
Possible values	"digital_goods": (no shipping). "travel_and_event": (no shipping). "billing_address": delivery to the billing address. "verified_address" Shipping to an address that has already been used. "another_address": Shipping to a new address. "pick-up": Shipping to a collection point. "other".

Attribute	**shoppingCartItems**
Description	Table containing the items in the cart.
Format	Table of items (type "shoppingCartItem")

Attribute	**stateOrProvince**
Description	Geographic code of the state or province (if applicable).
Format	String
Restrictions	ISO 3166-2
Help	https://fr.wikipedia.org/wiki/ISO_3166-2:US https://fr.wikipedia.org/wiki/ISO_3166-2:CA

Attribute	**suspiciousAccountActivity**
Description	Indicates whether the suspicious activities on the customer account have been reported by the merchant.
Format	Boolean

Attribute	**unitPrice**
Description	Amount expressed in the smallest unit of currency (for example, in centimes for the EURO)
Format	Number
Restrictions	Whole number Maximum of 12 meaningful numbers

Attribute	**workPhone**
Description	Work telephone number

Format	String
Restrictions	Up to 18 numerical characters with "+" as the first character, followed by the country code, a hyphen "-" and then the number
Example	The French number 05 12 34 56 78 will be written "+33-512345678"
Help	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

9.6 Detail of the JSON document "authentication"

This field contains the information concerning the card holder's authentication and is provided during the "Response" phase. If no authentication takes place (e.g. payment blocked upstream by the fraud prevention module, use of alternative payment methods such as COFIDIS), the field will always be returned but valued as null, i.e. bnVsbAo= once encoded.

JSON field	Description	Details
status	Result of authentication	link
protocol	Protocol used	link
version	Version of protocol	link
details	Details specific to the protocol and to the version	link

General information (status, protocol, version) is situated at the root of the JSON document. It is possible to base business processing on this information only, mainly by using the "status" field. The "details" field can provide a more in-depth analysis of the operation of the 3D Secure process.

9.6.1 Detail of the "details" object

JSON field	Description	Details
liabilityShift	Transfer of liability	link
VERes	Result contained in the VERes message	link
PARes	Result contained in the PARes message	link
ARes	Result contained in the ARes message	link
CRes	Result contained in the CRes message	link
merchantPreference	Merchant's preference	link
transactionID	ID of the transaction	link
status3DS	3D Secure 1.X exchange indicator	link
disablingReason	Reason for disabling 3D Secure	link

9.6.2 Description of attributes

Attribute	**status**
Description	Indicates the result of the authentication
Format	String
Possible values	• "authenticated": The authentication was successful. • "authentication_not_performed": The authentication could not be completed (technical or other problem). • "not_authenticated": The authentication failed. • "authentication_rejected": The authentication was rejected by the issuer. • "authentication_attempted": An authentication attempt took place. Authentication could not be completed but a proof was generated (CAVV) • "not_enrolled": The card is not enrolled for 3DS • "disabled": In the event of using the 3D Secure debrayable option

Attribute	protocol
Description	Protocol used for authentication
Format	String
Possible values	3DSecure

Attribute	version
Description	Version of protocol
Format	String
Possible values	1.0.2 2.1.0

Attribute	liabilityShift
Description	Indicates whether there is a transfer of liability to the issuing bank
Format	String
Possible values	"Y": The issuing bank is responsible for the risk. "N": The merchant is responsible for the risk. "NA": Impossible to determine, or not applicable.
Presence	For 3D Secure 2.X only.

Attribute	VERes
Description	Verification of enrolment of a card for 3D Secure 1.X.
Format	String
Possible values	"Y": card enrolled for 3D Secure 1.X. "N": card not enrolled for 3D Secure 1.X. "U": Technical problem when verifying the card's eligibility
Presence	For 3D Secure 1.X only.

Attribute	PARes
Description	Result of 3D Secure authentication
Format	String
Possible values	"Y": Authentication successful. "U": Technical problem during authentication. "N": Authentication failed. "A": No authentication, but the card holder's bank is taking responsibility for the risk.
Presence	For 3D Secure 1.X only.

Attribute	ARes
Description	The ARes message is the ACS response from the issuer to the AReq message. It may indicate that the card holder has been authenticated or that an additional interaction between the card holder is necessary to complete the authentication. There is just one ARES message per transaction.
Format	String
Possible values	"Y": Authentication successful without challenge. "R": Authentication rejected by the issuer "C": Challenge requested. "U": The ACS did not respond correctly. "A": Authentication could not be completed but a proof was generated "N": Authentication failed without challenge.
Presence	For 3D Secure 2.X only.

Attribute	CRes
Description	The CRes message is the ACS response to the CReq message. It may indicate the card holder's result of authentication or, for a model based on an application, also indicate that additional interaction from the card holder is necessary to complete authentication.
Format	String
Possible values	"Y": Authentication successful after challenge. "N": Authentication failed after challenge.
Presence	For 3D Secure 2.X only.

Attribute	merchantPreference
Description	Indicates the merchant's preference concerning the 3D Secure 2.X authentication process. This is only a preference and it may not be approved by the issuing banks.
Format	String
Possible values	"no_preference": No preference expressed. "challenge_preferred": challenge desired. "challenge_mandated": challenge required. "no_challenge_requested": No challenge requested. "no_challenge_requested_strong_authentication": no challenge requested – the customer's strong authentication has already been performed by the merchant. "no_challenge_requested_trusted_third_party" : no challenge requested – request for exemption because the merchant is a trusted third party. "no_challenge_requested_risk_analysis": no challenge requested – request for exemption for a reason other than one already mentioned (for example: small amount)

Attribute	**transactionID**
Description	Unique ID related to the transaction.
Format	String / UUID (RFC 4122)
Possible values	UUID (RFC 4122)
Presence	For 3D Secure 2.X only.

Attribute	**status3DS**
Description	3D Secure 1.X exchange indicator
Format	Whole
Possible values:	-1: the transaction did not take place according to the 3D Secure protocol and the risk of non-payment is high 1: the transaction took place according to the 3DS protocol and the risk of non-payment is low 4: the transaction took place according to the 3DS protocol and the risk of non-payment is high
Presence	For 3D Secure 1.X only.

Attribute	**disablingReason**
Description	Only coupled with the disabling 3D Secure option. Indicates the disabling reason.
Format	String
Possible values	merchant: explicitly disabled by the merchant by sending the appropriate value in the form of the "Out" phase seuilnonatteint (threshold not reached): disabled because the amount of the transaction does not equal the amount configured by the merchant scoring: disabled for scoring reason
Presence	Only when authentication disabling has been performed.

9.6.3 Example

Below is an example of the JSON authentication document within the framework of 3D Secure 2.0.

```json
{
   "status":"authenticated",
   "protocol":"3DSecure",
   "version":"2.1.0",
   "details":{
      "liabilityShift":"Y",
      "ARes":"C",
      "CRes":"Y",
      "merchantPreference":"no_preference",
      "transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
   }
}
```

After base 64 encoding:

eyAgCiAgICJzdGF0dXMiOiJhdXRoZW50aWNhdGVkIiwKICAgInByb3RvY29sIjoiM0RTZWN1cmUiLAogICAid
mVyc2lvbiI6IjIuMS4wIiwKICAgImRldGFpbHMiOnsgIAogICAgICAibGlhYmlsaXR5U2hpZnQiOiJZIiwKICAgICAg
IkFSZXMiOiJDIiwKICAgICAgIkNSZXMiOiJZIiwKICAgICAgIm1lcmNoYW50UHJlZmVyZW5jZSI6Im5vX3ByZWZ
lcmVuY2UiLAogICAgICAidHJhbnNhY3Rpb25JRCI6IjU1NWJkOWQ5LTFjZjEtNGJhOC1iMzdjLTFhOTZiYzhiNj
AzYSIKICAgfQp9Cg==

9.7 Management of the 3D Secure authentication protocol

Authentication of bank card holders during an act of payment is realised via the 3D Secure protocol. This ensures that the person entering the bank card information on the payment page is legitimate for this purchase: they are asked to perform an additional action (enter a code, authentication via a mobile application, etc.) to authenticate them as the bank card holder.

Until now, this authentication phase was based on version 1 of the secure communication protocol between the different 3D Secure players.

In 2019, version 2.1 of this protocol will be applied. This new version will be the subject of a gradual upgrade throughout the second half of the year and probably into 2020. This means that, during this period, a transaction could take place with the 3D Secure V1 or the 3D Secure V2 protocol. The version of the protocol used will be defined depending on the holder's bank card: the issuing bank will decided which authentication version to use. These decisions depend partly on the BIN but not only.

In order to handle this transition period in the best possible way, you will find below some explanations regarding the impacts this will have on the Monetico Paiement platform.

It is important to note that as the networks (VISA, Mastercard, CB) are still finalising the specification of the standard, some information will change.

9.7.1 The payment request – "Request" interface

During the payment request, two settings are available to indicate the behaviour of the Monetico Paiement solution with regard to 3D Secure authentication:

- 3dsdebrayable: this field can disable any version of the 3D Secure protocol.
- ThreeDSecureChallenge: this field is specific to the 3D Secure V2 protocol.

Both fields can be provided during the payment request in order to ensure implementation of the required authentication behaviour, regardless of the version of protocol used for a payment.

The table below recommends which values to use depending on the preferred authentication scenario:

Preferred scenario	3dsdebrayable	ThreeDSecureChallenge
No preference	by choice	no_preference
Preferred authentication	0 or nothing	challenge_preferred
Authentication systematically requested	0 or nothing	challenge_mandated
No authentication requested	1	no_challenge_requested
No authentication requested, exemption type: strong authentication	1	no_challenge_requested_strong_authentication
No authentication requested, exemption type: trusted third party	1	no_challenge_requested_trusted_third_party
No authentication requested, exemption type: prior risk analysis carried out	1	no_challenge_requested_risk_analysis

Point of attention concerning the disabling option: if your POS is configured to be automatically disabled depending on the amount, any transaction for an amount less than the configured amount will be disabled: this equates to entering the value "3dsdebrayable" = 1 during a payment request.

9.7.2 Server-to-server notification of the payment result - "Response" interface

The table below indicates the different scenarios encountered and the values returned by the Monetico Paiement platform.

For each status, you will find the different scenarios that may lead to this status and examples of the value of the "authentication" field

Scenario	Status	Results
The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page.	**authenticated (link)**	link
The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page (frictionless). Transfer of liability differs depending on the preference expressed by the merchant: see the table on liability shift for details.	**authenticated (link)**	link
The 3D Secure protocol was completed. The card holder was authenticated by the issuing bank without formal authentication (no input of an authentication code for example)	**authentication_attempted (link)**	link
The 3D Secure protocol was started. The card holder's bank considered this payment to be risky and rejected authentication..	**not_authenticated (link)**	link
The 3D Secure protocol was started. Authentication of the card holder via the holding bank's ACS authentication page was requested, but it was not completed (several wrong entries of the authentication code, cancellation of authentication by the holder, etc.)	**not_authenticated (link)**	link
The 3D Secure protocol was started. Following a technical problem, it could not be completed.	**authentication_not_performed (link)**	link
The 3D Secure protocol was triggered but a technical problem occurred preventing the holder being authenticated by the issuer.	**authentication_not_performed (link)**	link
The 3D Secure protocol was started. The card holder's bank rejected the authentication.	**authentication_rejected (link)**	link
The card is not enrolled for the 3D Secure protocol.	**not_enrolled (link)**	link

Status	authenticated (link)
Scenario	The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page.

3DS v1 Response interface	{
	  "status":"authenticated",
	  "protocol":"3DSecure",
	  "version":"1.0.2",
	  "details":{
	    "VERes":"Y",
	    "PARes":"Y",
	    "status3ds":1
	  }
	}

3DS v2 Response interface	{
	  "status":"authenticated",
	  "protocol":"3DSecure",
	  "version":"2.1.0",
	  "details":{
	    "liabilityShift":"<See specific table>",
	    "ARes":"C",
	    "CRes":"Y",
	    "merchantPreference":"<preference expressed in Out phase>",
	    "transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	  }
	}

Status	authenticated (link)
Scenario	The 3D Secure protocol was completed The card holder was authenticated by the issuing bank via its ACS authentication page (frictionless). Transfer of liability differs depending on the preference expressed by the merchant: see the table on liability shift for details.
3DS v1 Response interface	Not applicable

3DS v2 Response interface	{
	  "status":"authenticated",
	  "protocol":"3DSecure",
	  "version":"2.1.0",
	  "details":{
	    "liabilityShift":"<See specific table>",
	    "ARes":"Y",
	    "merchantPreference":"<preference expressed in Out phase>",
	    "transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"

	`}` `}`
Status	**authentication_attempted (link)**
Scenario	The 3D Secure protocol was completed. The card holder was authenticated by the issuing bank without formal authentication (no input of an authentication code for example)

3DS v1 Response interface	`{`
	`"status":"authentication_attempted",`
	`"protocol":"3DSecure",`
	`"version":"1.0.2",`
	`"details":{`
	`"VERes":"Y",`
	`"PARes":"A",`
	`"status3ds":4`
	`}`
	`}`

3DS v2 Response interface	`{`
	`"status":"authenticated",`
	`"protocol":"3DSecure",`
	`"version":"2.1.0",`
	`"details":{`
	`"liabilityShift":"<See specific table>",`
	`"ARes":"C",`
	`"CRes":"Y",`
	`"merchantPreference":"<preference expressed in Out phase>",`
	`"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"`
	`}`
	`}`

Status	**not_authenticated (link)**
Scenario	The 3D Secure protocol was started. The card holder's bank considered this payment to be risky and rejected authentication.
3DS v1 Response interface	Not applicable

3DS v2 Response interface	`{`
	`"status":"not_authenticated",`
	`"protocol":"3DSecure",`
	`"version":"2.1.0",`
	`"details":{`
	`"liabilityShift":"<See specific table>",`
	`"ARes":"N",`
	`"merchantPreference":"<preference expressed in Out phase>",`
	`"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"`

	} }

Status	**not_authenticated (link)**
Scenario	The 3D Secure protocol was started. Authentication of the card holder via the holding bank's ACS authentication page was requested, but it was not completed (several wrong entries of the authentication code, cancellation of authentication by the holder, etc.)

3DS v1 Response interface	`{`
	`"status":"not_authenticated",`
	`"protocol":"3DSecure",`
	`"version":"1.0.2",`
	`"details":{`
	`"VERes":"Y",`
	`"PARes":"N",`
	`"status3ds":4`
	`}`
	`}`

3DS v2 Response interface	`{`
	`"status":"not_authenticated",`
	`"protocol":"3DSecure",`
	`"version":"2.1.0",`
	`"details":{`
	`"liabilityShift":"<See specific table",`
	`"ARes":"C",`
	`"CRes":"N",`
	`"merchantPreference":"<preference expressed in Out phase>",`
	`"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"`
	`}`
	`}`

Status	**authentication_not_performed (link)**
Scenario	The 3D Secure protocol was started. Following a technical problem, it could not be completed.

3DS v1 Response interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"U",
	"status3ds":4
	}
	}

3DS v2 Response interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"U",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_not_performed (link)**
Scenario	The 3D Secure protocol was triggered but a technical problem occurred preventing the holder being authenticated by the issuer.

3DS v1 Response interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"1.0.2",
	"details":{
	"VERes":"Y",
	"PARes":"U",
	"status3ds":4
	}
	}

3DS v2 Response interface	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<See specific table>",
	"ARes":"C",
	"CRes":"U",
	"merchantPreference":"<preference expressed in Out phase>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-

	1a96bc8b603a" } }

Status	**authentication_rejected (link)**
Scenario	The 3D Secure protocol was started. The card holder's bank rejected the authentication.
3DS v1 Response interface	Not applicable

3DS v2 Response interface	{
	"**status**":"authentication_rejected",
	"**protocol**":"3DSecure",
	"**version**":"2.1.0",
	"**details**":{
	"**liabilityShift**":"<See specific table",
	"**ARes**":"R",
	"**merchantPreference**":"<preference expressed in Out phase>",
	"**transactionID**":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**not_enrolled (link)**
Scenario	The card is not enrolled for the 3D Secure protocol.

3DS v1 Response interface	{
	"**status**":"not_enrolled",
	"**protocol**":"3DSecure",
	"**version**":"1.0.2"
	}

3DS v2 Response interface	{
	"**status**":"not_enrolled",
	"**protocol**":"3DSecure",
	"**version**":"2.1.0"
	}

To complete the tables above, below are the liability shift values depending on the different scenarios and statuses returned by Monetico Paiement.

9.7.2.1 Frictionless scenarios

Authentication of the card holder via the ACS of the issuing bank was completed.	Status	Liability Shift
Yes - Authentication via the ACS of the card holder's bank necessary	**authenticated**	Issuer
	not_authenticated	Transaction rejected
No - No authentication via the ACS of the card holder's bank necessary	**authenticated** (frictionless)	Merchant
	authentication_attempted (ARes = A)	Dependent on the network and type of card
	authentication_not_performed (ARes = U)	Dependent on the network and type of card
	authentication_rejected (ARes = R)	Transaction rejected
	not_enrolled	Merchant

9.7.2.2 Challenge scenarios

Authentication of the card holder via the ACS of the issuing bank was completed.	Status	Liability Shift
Yes - Authentication via the ACS of the card holder's bank necessary	**authenticated**	Issuer
	not_authenticated	Transaction rejected
No - No authentication via the ACS of the card holder's bank necessary	**authenticated** (frictionless)	Issuer
	authentication_attempted (ARes = A)	Dependent on the network and type of card
	authentication_not_performed (ARes = U)	Dependent on the network and type of card
	authentication_rejected (ARes = R)	Transaction rejected
	not_enrolled	Merchant

9.8 Service URL

9.8.1 The test environment, known as "sandbox"

The role of our test server is to allow you to validate your developments. Of course, all transactions made by our test payment server are fictive and do not lead to a real bank transaction.

To make payment requests in this environment, we provide you with test bank cards. They can be accessed by clicking the "Test Card" icon on the payment page.

The test environments are available at the following addresses:

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

- Capturing and refunding services:
  https://payment-api.e-i.com/test/capture_paiement.cgi
  https://payment-api.e-i.com/test/recredit_paiement.cgi

The test merchant dashboard allows you to manage and control payments made in the test environment. It is available at the following address:

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

9.8.2 In Production

After validating your developments and requesting the production launch of your POS from centrecom@e-i.com, you can contact the production server, available here:

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

- Capturing and refunding services:
  https://payment-api.e-i.com/capture_paiement.cgi
  https://payment-api.e-i.com/recredit_paiement.cgi

You can view payments made on your POS via the merchant dashboard at the following address:

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

We draw your attention to the fact that requests sent to the production server will be actual transactions.