Desjardins

Monetico Paiement

GUIDE D'INTÉGRATION

PAIEMENT EN LIGNE

Nom de fichier : Monetico_Paiement_Internet_Guide_Intégration_v2.01
Numéro de version : 2.01
Date : 2018-02-23

Confidentiel

Titre du document : Paiement sur Internet – Guide d'intégration
Nom de fichier : Monetico_Paiement_Internet_Guide_Intégration_v2.01
Numéro de version : 2.01
Date : 2018-02-23

Site Web : www.desjardins.com

TABLE DES MATIÈRES

1 Introduction

1.1 À propos de ce document

L'objectif de ce document est de présenter les aspects techniques de l'intégration de la solution de paiement en ligne Monetico Desjardins avec votre site commerçant.

1.2 Public cible

Ce document a été rédigé principalement à l'intention des ressources techniques responsables de l'intégration de la solution de paiement en ligne Monetico.

1.3 Terminologie

Le tableau suivant contient un lexique de certains termes utilisés dans le présent document.

Terme utilisé	Terme Desjardins
annulation	annulation d'achat, renversement de préautorisation
appel « phonie »	appel pour autorisation
autorisation	préautorisation
capture de paiement	conclusion de préautorisation
carte bancaire	carte de crédit
chiffre vérificateur	code de vérification
code société	numéro de marchand
commerçant	Marchand
email, mail	Courriel
emails jetables	liste noire (« black list »)
environnement de validation	environnement de test
interface retour	Confirmation
mise en recouvrement	compensation, conclusion de préautorisation,
paiement différé	paiement de préautorisation
paiement en attente	paiement en attente
paiement immédiat	Paiement d'achat
première échéance	premier versement
recrédit	remboursement
remise	dépôt
société	entreprise
TPE - Terminal de Paiement Électronique	TPV Terminal Point de Vente; mode de paiement
TPE virtuel (web)	mode de paiement

2 Mise en place de l'interface de paiement

2.1 Interfaces

L'intégration de la solution de paiement Monetico avec votre site commerçant consiste à mettre en place deux interfaces dans votre système informatique :

- Interface « Aller » : sert à la génération d'un formulaire de demande de paiement sécurisé par un sceau, qui accompagnera votre client lorsque vous le redirigez vers le serveur de paiement de Monetico
- Interface « Retour » : sert à la réception de la confirmation du paiement que Monetico envoie après chaque demande de paiement

Le travail d'intégration nécessite des compétences avancées en programmation :

- recevoir et contrôler des paramètres en méthode POST
- manipuler des chaînes de caractères
- utiliser une fonction ou une classe conforme à la norme RFC2104 implémentant le HMAC SHA1 ou MD5
- sauvegarder le contexte de paiement en fichier ou base de données
- suivre le déroulement pas à pas d'un programme dans un outil de débogage ou en programmant des traces.

À titre d'information, des exemples de ces deux interfaces vous seront fournis avec la documentation, dans les langages de programmation les plus courants (PHP, VB.NET, C#.NET, ASP, Python, Ruby, Java et C++). Vous trouverez ces exemples sur le site de Monetico à l'adresse :
https://assistance.monetico.ca/paiement-en-ligne/forfait-classique
Vous pourrez utiliser ces exemples comme point de départ, mais vous devrez les modifier selon les spécificités de votre environnement et de votre application. En particulier, le stockage des clés devra être revu pour exploiter les meilleurs outils de confidentialité disponibles dans votre environnement.

2.2 Clé de sécurité commerçant

Une clé de sécurité, propre à chaque Terminal de Paiement Électronique (TPE), destinée à certifier les données échangées entre le serveur du commerçant et le serveur de paiement sécurisé de Monetico, est indispensable pour utiliser le service de paiement. Un lien, permettant de télécharger cette clé de sécurité, est envoyé par courriel au commerçant.

Le commerçant peut demander la régénération d'une nouvelle clé, périodiquement ou à l'occasion d'évènements tels qu'une mise en production, un changement d'hébergeur, un changement de prestataire, etc. Il est de la responsabilité du commerçant de conserver cette clé de façon sûre et confidentielle en exploitant les meilleurs outils disponibles dans son environnement.

La clé de sécurité est représentée de façon externe par 40 caractères hexadécimaux (par exemple : `0123456789ABCDEF0123456789ABCDEF01234567`).
Cette représentation textuelle doit être convertie en une chaîne binaire de 20 octets (représentation opérationnelle) avant utilisation. Référez-vous aux exemples de code pour de plus amples informations.

L'ancienne clé reste reconnue par le système lors de la génération d'une nouvelle clé. C'est une utilisation avec succès de la nouvelle clé (en environnement de test, en environnement de production) qui viendra définitivement invalider l'ancienne (pour l'environnement respectif).

2.3 Spécifications des messages échangés

2.3.1 Rappel du flux des échanges

Action	Intervenant
Le serveur commerçant obtient l'accord de l'internaute sur la chose et le prix	**Site web du commerçant**
Le serveur du commerçant rassemble les données du paiement à effectuer …	**Interface « Aller » sur le serveur du commerçant**
… puis crée le formulaire de paiement scellé	
… puis met en page ce formulaire de paiement à destination de l'internaute	
L'internaute clique sur le bouton correspondant au formulaire de paiement …	
… et accède au serveur de paiement	**Serveur de paiement de la banque**
Le serveur bancaire vérifie la validité du sceau et entame le dialogue de paiement avec l'internaute	
L'internaute dialogue avec le serveur bancaire et paye (ou ne paye pas) par carte bancaire	
Le serveur bancaire renvoie un résultat de paiement scellé au serveur du commerçant sur son interface « Retour »	
Le serveur du commerçant vérifie la validité du sceau …	**Interface « Retour » sur le serveur du commerçant**
… puis prend en compte le résultat de paiement …	
… puis renvoie un accusé de réception au serveur bancaire	
Le serveur affiche à l'internaute le résultat du paiement[1]	**Serveur de paiement de la banque**
L'internaute peut imprimer (ou sauvegarder) cette page[1]	
Le serveur propose à l'internaute de revenir sur le site du commerçant via un lien hypertexte[1]	
S'il suit ce lien, l'internaute quitte le serveur de paiement et revient sur le site du commerçant[1]	
Le serveur du commerçant adapte son dialogue en fonction du résultat de paiement reçu	**Site web du commerçant**

[1] Le retour automatisé vers le site marchand sans action complémentaire de l'utilisateur est disponible en option.
Dans ce cas : le serveur de paiement de la banque va produire une page redirigeant le porteur sur l'URL appropriée au résultat de la demande d'autorisation. Le ticket de paiement est envoyé par mail.

2.3.2 Interface « Aller »

2.3.2.1 Création du formulaire

Les paramètres du terminal et les données de la commande sont regroupés en un formulaire HTML scellé afin de transmettre la demande de paiement au serveur de Monetico via le fureteur du client. Les champs à fournir dans le formulaire sont fournis dans le tableau ci-dessous :

Champs	Description	Remarque
version	Version du système de paiement utilisée	**Version actuelle** `3.0`
TPE	Numéro de TPE Virtuel du commerçant. Taille : 7 caractères	**Exemple :** `1234567`
date	Date de la commande au format `JJ/MM/AAAA:HH:MM:SS`	**Exemple :** `05/12/2006:11:55:23`

montant	Montant total incluant les taxes de la commande formaté de la manière suivante :
	• Un nombre entier
	• Un point décimal (optionnel)
	• Un nombre entier de *n* chiffres : *n* étant le nombre maximal de décimales de la devise (optionnel)
	• Une devise sur 3 caractères alphabétiques ISO4217 (CAD)
		Exemples : `62.73CAD`
		`10CAD`
		`1024CAD`

reference	Référence unique de la commande. Taille : 12 caractères alphanumériques maximum	**Exemple :** `ABERTYP00145`
texte-libre	Zone de texte libre. Taille : 3200 caractères maximum	
mail	Adresse courriel de l'internaute	
lgue	Code langue Taille : 2 caractères	**Valeurs possibles :** `FR` `EN`
societe	Code alphanumérique permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité	**Ce code est fourni par nos services.** **Exemple :** `monSite1`
url_retour	URL par laquelle l'acheteur revient sur la page d'accueil de la boutique	
url_retour_ok	URL par laquelle l'acheteur est redirigé sur le site du commerçant suite à un paiement accepté	**Attention : à ne pas confondre avec l'URL de l'interface « Retour », aussi appelée URL de confirmation des paiements**
url_retour_err	URL par laquelle l'acheteur revient sur le site du commerçant suite à un paiement refusé ou en cliquant sur le bouton « abandonner »	
MAC	Sceau issu de la certification des données Taille : 40 caractères hexadécimaux	
options	Liste des options utilisées (peut être vide).	**Exemple :**

	Chaque option est séparée des autres par un caractère '&'. Si l'option a une valeur, le nom est séparé de la valeur par le caractère '='.	**opttest=abc&optbis=123**

Liste des options possibles :

Options	Description	Remarque
aliascb	Alias de la carte de crédit d'un client en cas de souscription de l'option « paiement express » Format : [a-zA-Z0-9]{1,64}	**Exemple :** **aliascb=client1**
forcesaisiecb	Permet de forcer la saisie d'une carte de crédit en cas de souscription de l'option « paiement express »	**Exemple :** **forcesaisiecb=1**
3dsdebrayable	Permet de forcer le débrayage de 3DSecure	**Exemple :** 3dsdebrayable=1

Remarque :
Lorsque le nom ou la valeur de l'option est incorrect, la demande de paiement est interrompue et un message d'erreur, indiquant que le formulaire est erroné, est affiché sur la page.

2.3.2.2 Liste de champs propres au mode de paiement fractionné

Les champs suivants sont spécifiques au mode de paiement fractionné :

Champs	Description	Remarque
nbrech	Nombre d'échéances pour cette commande (entre 2 et 4 maximum)	**Exemple :** 4
dateech1	Date de la première échéance au format JJ/MM/AAAA La première échéance correspond à la date de la commande.	**Exemple :** 25/04/2008
montantech1	Montant TTC de l'échéance formaté de la manière suivante : • Un nombre entier • Un point décimal (optionnel) • Un nombre entier de *n* chiffres : *n* étant le nombre maximal de décimales de la devise (optionnel) • Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, GBP, CHF, etc.)	**Exemples :** 62.73EUR 10GBP 1024USD
dateech[N] (N entre 2 et 4)	Date de la Nième échéance au format JJ/MM/AAAA	**Exemple :** 05/06/2008
montantech[N] (N entre 2 et 4)	Montant TTC de la Nième échéance formaté de la manière suivante :	**Exemples :** 62.73EUR 10GBP 1024USD

	• Un nombre entier • Un point décimal (optionnel) • Un nombre entier de *n* chiffres : *n* étant le nombre maximal de décimales de la devise (optionnel) • Une devise sur 3 caractères alphabétiques ISO4217 (`EUR`, `USD`, `GBP`, `CHF`, etc.)	

Remarque :

- Pour pouvoir utiliser ces champs, votre TPE doit être configuré pour accepter les paiements en N fois ;
- Tous ces champs sont optionnels : si vous ne les fournissez pas, les paramètres mis en place à la création de votre TPE seront pris en compte ;
- La somme des montants de chaque échéance doit être égale au montant de la commande ;
- Les montants doivent être dans la même devise ;
- Les échéances doivent être mensuelles.
- En cas d'expiration de CB avant la dernière échéance :
  - la commande peut être refusée ou :
  - les échéances suivant la date d'expiration peuvent être reportées sur la première échéance.

2.3.2.3 Liste de champs propres au paiement via partenaires

Le champ suivant est à ajouter dans le cas de l'intégration des boutons permettant de payer via un de nos partenaires (Paypal, 3xCB…) directement sur le site du commerçant (sans passer par la page de paiement) :

Champs	Description	Remarque
protocole	Mode de paiement via un partenaire souhaité	**Exemple :** `protocole=paypal`

Liste des valeurs possibles pour le champ "protocole" :

Valeur du champ	Partenaire
paypal	Paypal
1euro	Cofidis 1Euro
3xcb	Cofidis 3xCB
fivory	Fivory

Remarque :

- Pour pouvoir utiliser ces moyens de paiement, votre TPE doit être configuré en conséquence.

2.3.2.4 Exemple de formulaire de paiement en HTML

```
<form action="https://p.monetico-services.com/paiement.cgi"
      method="post" id="PaymentRequest">
      <input type="hidden" name="version" value="3.0" />
      <input type="hidden" name="TPE" value="1234567" />
      <input type="hidden" name="date" value="16/04/2013:15:25:38" />
      <input type="hidden" name="montant" value="0.01CAD" />
      <input type="hidden" name="reference" value=" votreRF12345" />
      <input type="hidden" name="MAC" value="ca66baf34e37db1a184d05cbcd1ca3a53e1cc045" />
      <input type="hidden" name="url_retour_ok"
         value="http://url.retour.com/ok.cgi?order_ref=votreRF12345" />
      <input type="hidden" name="url_retour_err"
         value="http://url.retour.com/err.cgi?order_ref=votreRF12345" />
      <input type="hidden" name="lgue" value="FR" />
      <input type="hidden" name="societe" value="monSite1" />
      <input type="hidden" name="texte-libre" value="Ceci est un test" />
      <input type="hidden" name="mail" value="internaute@email.com" />
      <input type="submit" name="bouton" value="Paiement Carte de credit" />
</form>
```

2.3.2.5 Exemple de formulaire de paiement fractionné en HTML

```
<form method="post" name="MoneticoFormulaire" 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="05/12/2006:11:55:23">
    <input type="hidden" name="montant" value="100EUR">
    <input type="hidden" name="reference" value="ABERTPY00145">
    <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
    <input type="hidden" name="url_retour"
        value="http://url.retour.com/ko.cgi?order_ref=votreRF12345">
    <input type="hidden" name="url_retour_ok"
        value="http://url.retour.com/ok.cgi?order_ref=votreRF12345">
    <input type="hidden" name="url_retour_err"
        value="http://url.retour.com/err.cgi?order_ref=votreRF12345">
    <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="nbrech" value="3">
    <input type="hidden" name="dateech1" value="05/12/2006">
    <input type="hidden" name="montantech1" value="50EUR">
    <input type="hidden" name="dateech2" value="25/01/2007">
    <input type="hidden" name="montantech2" value="25EUR">
    <input type="hidden" name="dateech3" value="25/02/2007">
    <input type="hidden" name="montantech3" value="25EUR">
    <input type="submit" name="bouton" value="Paiement CB">
</form>
```

2.3.2.6 Calcul du sceau du formulaire

Le sceau (à mettre dans le champ MAC) est calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.
Cette fonction générera le sceau à partir de données à certifier et de la clé de sécurité commerçant sous sa forme opérationnelle.
Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations du formulaire :

```
<TPE>*<date>*<montant>*<reference>*<texte-libre>*
<version>*<lgue>*<societe>*<mail>*<nbrech>*<dateech1>*<montantech
1>*<dateech2>*<montantech2>*<dateech3>*<montantech3>*<dateech4>*<
montantech4>*<options>
```

Exemple pour un paiement:

```
1234567*05/12/2006:11:55:23*62.73CAD*ABERTYP00145*ExempleTexteL
ibre*3.0*FR*monSite1*internaute@sonemail.ca**********
```

Exemple pour un paiement fractionné :

```
1234567*05/12/2006:11:55:23*62.73EUR*ABERTYP00145*ExempleTe
xteLibre*3.0*FR*monSite1*internaute@sonemail.fr*4*05/12/2006
*16.23EUR*05/01/2007*15.5EUR*05/02/2007*15.5EUR*05/03/2007*1
5.5EUR*
```

2.3.3 Interface « Retour »

Après avoir traité la demande de paiement, le serveur de Monetico informe directement le serveur du commerçant du résultat de la demande de paiement en émettant une requête HTTP en ligne, contenant le résultat de la demande de paiement, sur l'URL de confirmation des paiements (interface « Retour »). **Cet URL doit nous être indiquée au moment de la mise en place du système via l'adresse** support@desjardins.monetico-services.com.

Remarque : L'interface retour est appelée **après chaque tentative de paiement** d'une même commande, pour en indiquer le résultat. Il est donc possible que l'interface retour reçoive plusieurs notifications de paiements refusés puis une notification de paiement accepté pour une même référence de commande. Si le client ne poursuit pas le processus de paiement jusqu'au bout, par exemple s'il ne saisit pas les informations de sa carte de crédit, l'interface retour n'est pas appelée.

L'interface de retour dispose de 30 secondes pour répondre comme décrit au chapitre **Erreur ! Source du renvoi introuvable.**, page **Erreur ! Signet non défini.**. Le cas du dépassement de délai est interprété comme une erreur dans l'interface de retour marchand.
Lorsque qu'une réponse erronée est fournie et que le paiement est accepté : un second appel est réalisé (sauf cas réalisant une redirection immédiate sur le site marchand).

2.3.3.1 Paramètres renvoyés par Monetico

L'interface « Retour » sera appelée par le serveur de Monetico avec la méthode POST. Les données envoyées par le serveur de Monetico sont décrites ci-dessous :

Champs	Description	Remarque
MAC	Sceau résultant de la certification des données	
date	Date de la demande d'autorisation de la commande au format JJ/MM/AAAA_a_HH:MM:SS	
TPE	Numéro de TPE Virtuel du commerçant	**Le serveur de Monetico renvoie ici les données telles qu'elles ont été reçues lors de la phase « Aller » du paiement**
montant	Montant de la commande formaté de la manière suivante : Un nombre entier Un point décimal (optionnel) Un nombre entier (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (CAD)	
reference	Référence unique de la commande	
texte-libre	Zone de texte libre	

code-retour	Le résultat du paiement, parmi : `payetest` paiement accepté (en TEST uniquement) `paiement` paiement accepté (en Production uniquement) `Annulation` paiement refusé	**En cas de paiement refusé, une autorisation ultérieure pourra encore être délivrée pour la même référence.** **Le code « payetest » n'est envoyé que pour des paiements effectués dans l'environnement de test. Si ce code est présent lors d'un paiement en production, il s'agit d'une anomalie.**
cvx	`oui` si le code de vérification CVV2 (obligatoire pour les cartes Visa et MasterCard) a été saisi `non` sinon	
vld	Date d'expiration de la carte de crédit utilisée pour effectuer le paiement	

brand	Code réseau de la carte sur 2 positions alphabétiques parmi.
	`AM` `American Express`
	`MC` `Mastercard`
	`VI` `Visa`
	`na` `Non disponible`
		La valeur « na » est systématiquement retournée dans l'environnement de test.

status3ds	Indicateur d'échange 3DSecure : `-1` : la transaction ne s'est pas faite selon le protocole 3DSecure `1` : la transaction s'est faite selon le protocole 3DS et le niveau de risque est faible `2` : la transaction ne peut pas se faire selon le protocole 3DSecure, le détenteur a cependant été authentifié par le biais de 3DSecure `3` : la transaction s'est faite selon le protocole 3DS et le niveau de risque est élevé `4` : la transaction s'est faite selon le protocole 3DS et le niveau de risque est très élevé	
numauto	Numéro d'autorisation tel que fourni par l'institution émettrice	**Uniquement dans le cas où l'autorisation a été accordée**

motifrefus	Motif du refus de la demande de paiement : Appel Phonie : l'émetteur de la carte de crédit du client demande des informations complémentaires **N.B. Cette fonctionnalité n'est actuellement pas offerte par Desjardins** Refus : l'émetteur de la carte de crédit du client refuse d'accorder l'autorisation Interdit : l'émetteur de la carte de crédit du client refuse d'accorder l'autorisation Filtrage : la demande de paiement a été bloquée par le paramétrage de filtrage que le commerçant a mis en place dans son Module Prévention Fraude scoring : la demande de paiement a été bloquée par le paramétrage de scoring que le commerçant a mis en place dans son Module Prévention Fraude 3DSecure : si le refus est lié à une authentification 3DSecure négative reçue de l'émetteur de la carte du détenteur	**Uniquement dans le cas où la demande de paiement a été refusée.**
originecb	Code pays de l'institution émettrice de la carte de crédit (norme ISO 3166-1)	**Uniquement en cas de souscription du module prévention fraude**
bincb	Code BIN de l'institution émettrice du détenteur de la carte de crédit	
hpancb	Hachage irréversible (HMAC-SHA1) du numéro de la carte de crédit utilisée pour effectuer le paiement (identifiant de manière unique une carte de crédit pour un commerçant donné)	
ipclient	Adresse IP du client ayant fait la transaction	
originetr	Code pays de l'origine de la transaction (norme ISO 3166-1)	
veres	Etat 3DSecure du VERes	**En cas de souscription du module prévention fraude et de l'option 3Dsecure**
pares	Etat 3DSecure du PARes	
montantech	Montant de l'échéance en cours	**Uniquement dans le cas du paiement fractionné.**

filtragecause	Numéros des types de filtres bloquant le paiement (cf. tableau « Retours Module Prévention Fraude – détails » ci-dessous) 1 : Adresse IP 2 : Numéro de carte 3 : BIN de carte 4 : Pays de la carte 5 : Pays de l'IP 6 : Cohérence pays de la carte / pays de l'IP 7 : Courriel jetable 8 : Limitation en montant pour une carte de crédit sur une période donnée 9 : Limitation en nombre de transactions pour une carte de crédit sur une période donnée 11 : Limitation en nombre de transactions par alias sur une période donnée 12 : Limitation en montant par alias sur une période donnée 13 : Limitation en montant par IP sur une période donnée 14 : Limitation en nombre de transactions par IP sur une période donnée 15 : Testeurs de cartes 16 : Limitation en nombre d'alias par carte de crédit	**Uniquement dans le cas d'un filtrage du paiement. Si plusieurs filtres bloquent le paiement, ceux-ci sont séparés par des tirets. Les causes et les valeurs correspondantes étant dans le même ordre.**
filtragevaleur	Données ayant engendrées le blocage	
cbenregistree	Booléen indiquant si la carte a été enregistrée sous un aliascb donné : 1 : Le client a saisi une carte de crédit et elle a été enregistré sous l'aliascb envoyé 0 : Tous les autres cas	**Uniquement en cas de souscription de l'option paiement express**
cbmasquee	6 premiers et 4 derniers chiffres de la carte de crédit du client, séparés par des étoiles, uniquement lors de l'enregistrement de la carte de crédit	**Uniquement en cas de souscription de l'option paiement express.** **Exemple :** 123456******7890

Retours Module Prévention Fraude (MPF) – Détails

La fonctionnalité de filtrage des paiements s'appuie sur un ensemble de neuf filtres, librement paramétrable sur le tableau de bord. Chacun de ces filtres agit sur un critère spécifique, comme l'adresse IP du client, son adresse courriel, le pays de l'émetteur de sa carte de crédit…

Numéro du type de filtre	Critère d'analyse	Valeur retournée comme raison du blocage	Remarque
1	Adresse IP	Adresse IP du client	
2	Numéro de carte	Hash de la carte du client	Fonctionne uniquement pour les paiements par carte
3	BIN de carte	Bin de la carte du client	
4	Pays de la carte	Pays de la carte du client	
5	Pays de l'IP	Pays de l'IP du client	
6	Cohérence pays de la carte / pays de l'IP	Pays de la carte # Pays de l'adresse IP du client	Fonctionne uniquement pour les paiements par carte
7	Courriel jetable	Nom de domaine de l'adresse courriel du client	
8	Limitation en montant pour une carte de crédit sur une période donnée	Montant cumulé en dollars ($) sur la période donnée associé à la carte du client	Fonctionne uniquement pour les paiements par carte
9	Limitation en nombre de transactions pour une carte de crédit sur une période donnée	Nombre de transactions cumulées sur la période donnée associé à la carte du client	
11	Limitation en nombre de transactions par alias sur une période donnée	Nombre de transactions cumulées sur la période donnée associé à l'alias du client	Uniquement en cas de souscription de l'option paiement express
12	Limitation en montant par alias sur une période donnée	Montant cumulé en dollars ($) sur la période donnée associé à l'alias du client	
13	Limitation en montant par IP sur une période donnée	Montant cumulé en dollars ($) sur la période donnée associé à l'adresse IP du client	
14	Limitation en nombre de transactions par IP sur une période donnée	Nombre de transactions cumulées sur la période donnée associé à l'adresse IP du client	
15	Testeurs de cartes	Nombre de transactions cumulées sur la période donnée associé à l'adresse IP du client	
16	Limitation en nombre d'alias par carte de crédit	Les alias déjà associés à la carte utilisée pour le paiement	Uniquement en cas de souscription de l'option paiement express Fonctionne uniquement pour les paiements par carte

Exemple de données envoyées par le serveur de paiement de Monetico à l'interface « Retour » pour un paiement d'achat ou de préautorisation :

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

Exemple de données envoyées par le serveur de paiement de Monetico à l'interface « Retour » pour un blocage d'un paiement d'achat par le Module Prévention Fraude:

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

Exemple de données envoyées par le serveur de paiement de Monetico à l'interface « Retour » pour un paiement avec l'option paiement express :

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

Remarque :
Les pays sont désignés par leur code ISO de trois lettres selon la norme ISO 3166-1 alpha-3.

2.3.3.2 Validation du sceau

Le message de confirmation reçu est scellé par un sceau MAC qui a été calculé par le serveur de paiement de Monetico à l'aide de la clé de sécurité commerçant attribuée à votre terminal de paiement.

Une fonction de validation du sceau doit être implémentée dans l'interface « Retour » pour s'assurer qu'il n'y a pas eu de falsification des données contenues dans le message de confirmation du paiement reçu.

Pour cela, la fonction doit recalculer le code MAC associé au message et le comparer à celui transmis dans le message : si les deux codes sont identiques, l'information reçue est fiable (intégrité des informations et authentification de l'émetteur).

Pour calculer le MAC il faut utiliser une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.
Cette fonction générera le sceau à partir de données à certifier et de la clé de sécurité commerçant sous sa forme opérationnelle.
Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations envoyées par le serveur de Monetico :

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

Exemple si vous êtes inscrit au module prévention fraude et à l'option 3DSecure et le paiement est accepté :

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

2.3.3.3 Création de l'accusé de réception

La réponse renvoyée par l'interface « Retour » au serveur de paiement de Monetico doit être un des deux messages présentés dans le tableau ci-dessous, dépendant seulement de la vérification du sceau MAC reçu, sans tenir compte de la valeur du code-retour de paiement, dès lors que cette valeur fait partie de la liste des valeurs énumérées pour le champ code-retour.

Sceau validé	Accusé de réception à renvoyer au format texte
Oui	`version=2<LF>` `cdr=0<LF>`
Non	`version=2<LF>` `cdr=1<LF>`

Remarque : **<LF>** correspond à un saut de ligne

Lorsque le serveur de Monetico ne reçoit pas l'accusé de réception pour un sceau validé, il envoie un courriel d'alerte sur une boîte aux lettres électronique de surveillance indiquée par le commerçant et refait une seconde tentative.

Ce courriel contient un lien permettant de rejouer via la méthode GET la requête émise par le serveur de Monetico, un code de l'erreur rencontrée lors de l'appel de l'url de confirmation et l'accusé de réception renvoyé par le serveur commerçant.

Dès la phase de test, le commerçant doit nous fournir une adresse courriel régulièrement vérifiée. Pour passer en production, le serveur commerçant doit avoir renvoyé un accusé de réception avec un sceau validé pour les trois derniers tests. Acheminer cette adresse à notre centre de support support@desjardins.monetico-services.com

2.3.4 Vérification d'adresse « AVS »

La solution supporte le service de vérification d'adresse (AVS) acquéreur.
Ce service permet à l'émetteur de vérifier l'information concernant l'adresse de facturation d'un titulaire de carte et fournit un code de résultat de validation.
Ce code peut être découpé en 5 catégories :

- "exact match": Même adresse et même code postal
- "address match": Même adresse, code postal non validé
- "zip match": Même code postal, adresse non validée
- "no match" : Adresse et code postal différents
- Informations d'adresse non vérifiées

Le back-office permet à un agent Desjardins d'activer ou non le service AVS pour un commerçant donné, par défaut, la valeur est à « inactif ».

Si le service AVS est activé, la page de paiement demande la saisie de l'adresse de facturation de la carte de crédit utilisée (cette adresse peut différer de l'adresse de livraison).

Si le service AVS est activé, l'adresse de facturation reliée à la carte de crédit utilisée pour le paiement doit être fournie par le site commerçant en mode émulation.

Si le service AVS est activé, l'adresse de facturation reliée à la carte de crédit utilisée pour le paiement peut optionnellement être saisie lors des transactions MOTO. Il n'est pas obligatoire.

Si le service AVS est activé, le back-office permet à un agent Desjardins de configurer les comportements suivants lors d'une transaction approuvée, lorsque la réponse contient le résultat de la vérification d'adresse :

- approbation: si la réponse à la demande d'autorisation contient le statut « exact match », "address match" , "zip match" , "no match" ou "Information non vérifiée", la solution accepteur termine la transaction avec le statut "approuvée".
- refus conditionnel : si la réponse à la demande d'autorisation contient le statut "no match", la solution accepteur génère automatiquement un renversement; alors que si la demande d'autorisation contient le statut « exact match », "address match" ou "zip match", la solution accepteur termine la transaction avec le statut "approuvée".
- refus strict: si la réponse à la demande d'autorisation contient le statut "address match" ou "zip match" ou "no match", la solution accepteur génère automatiquement un renversement.

Le statut de validation de l'adresse est visualisable dans les rapports du commerçant lorsque disponible dans la réponse retournée par Desjardins.

Le statut de validation de l'adresse est présent dans la réponse retournée au site du commerçant (en mode émulation) lorsque disponible dans la réponse retournée par Desjardins.

3 Demander la conclusion d'une autorisation

3.1 Présentation

Le but du service Capture_Paiement est de permettre aux commerçants de conclure, par requête informatique et de manière sécurisée, les autorisations qui ont été préalablement effectuées.

Ce service peut être uniquement être utilisé avec les TPE configurés en mode « paiement de préautorisation ».

Pour demander une conclusion d'autorisation, l'application du commerçant doit faire appel au service web Capture_Paiement du serveur de Monetico (via un message HTTPS), en fournissant un certain nombre d'informations (le montant de la commande, sa date, sa référence, le numéro du TPE virtuel du commerçant, etc.). Un sceau doit être calculé pour certifier les données échangées.

En réponse à cette demande, le serveur de Monetico retourne le résultat de la demande de capture à l'application du commerçant, soit acceptée ou refusée.

3.2 Appel au service de demande de capture

3.2.1 Les informations à fournir

L'application du commerçant doit émettre une requête en méthode POST par un message HTTPS (TLS), à destination du service Capture_Paiement sur les serveurs de Monetico, contenant les champs suivants :

Champs	Description	Remarque
version	Version du système de paiement utilisée	**Version actuelle** `3.0`
TPE	Numéro de TPE Virtuel du commerçant Taille : 7 caractères	**exemple :** `1234567`
date	Date et heure de la demande de conclusion au format `JJ/MM/AAAA:HH:MM:SS`	**Exemple :** `05/12/2006:11:55:23`
date_commande	Date de la commande au format `JJ/MM/AAAA`	**Exemple :** `03/12/2006`
montant	Montant de la commande initiale	**Format :** - **Un nombre entier** - **Un point décimal (optionnel)**
montant_a_capturer	Montant de la demande de conclusion	
montant_deja_capture	Montant correspondant au montant déjà conclu sur cette commande	

montant_restant	Montant correspondant au solde de la commande après la conclusion présentement demandée	**- Un nombre entier (optionnel)** **- Une devise sur 3 caractères alphabétiques ISO4217 (CAD)** **Exemples : 62.73CAD** **10CAD** **1024CAD**
reference	Référence de la commande	**Exemple : ABERTYP00145**
texte-libre	Zone de texte libre Taille : 3200 caractères maxi.	
lgue	Code langue (en majuscules) Taille : 2 caractères	**FR ou EN**
societe	Code alphanumérique permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité	**Ce code est fourni par nos services.** **Exemple : monSite1**
MAC	Sceau issu de la certification des données Taille : 40 caractères hexadécimaux	
stoprecurrence	Force la fin de la récurrence pour les TPE en paiement récurrent.	**Ce paramètre est optionnel.**
phonie	La valeur de ce champ sera renvoyée en cas d'appel phonie	**Ce paramètre est optionnel.** **N.B. Cette fonctionnalité n'est actuellement pas offerte par Desjardins**

Les champs de cette requête (sauf la version et les montants) doivent tous être encodés en HTML. Les spécifications d'encodage sont décrites en fin de document.

3.2.2 Calcul du sceau

Le sceau (à mettre dans le champ MAC) doit être calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104. Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations du formulaire :

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

3.2.3 Exemples de requête de capture

Exemple 1 : conclusion partielle de 62 $ pour une commande initiale de 100 $

Chaîne utilisée pour le calcul du sceau :

```
1234567*05/12/2006:11:55:23*62.00CAD0CAD38CAD*ABERTYP00145*Exemp
leTexteLibre*3.0*FR*monSite1*
```

Requête :

```
POST /capture_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 307

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&date_commande=03%2F12%2F2006
&montant=100.00CAD
&montant_a_capturer=62.00CAD
&montant_deja_capture=0CAD
&montant_restant=38.00CAD
&reference=ABERTPY00145
&texte-libre=ExempleTexteLibre
&lgue=FR
&societe=monSite1
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

La somme des 3 montants doit être égale au montant initial de la commande

Exemple 2 : conclusion totale d'une commande de 100 $

Chaîne utilisée pour le calcul du sceau :

```
1234567*05/12/2006:11:55:23*100.00CAD0CAD0CAD*ABERTYP00145*Exemp
leTexteLibre*3.0*FR*monSite1*
```

Requête :

```
POST /capture_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 305

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

Les 2 montants doivent être identiques

3.3 Réponse de la demande de capture

3.3.1 Les informations retournées

En réponse à la demande de capture, l'application du commerçant reçoit un message d'acquittement de la part du serveur de Monetico. Ce message est un document de type MIME « text/plain » précisant le résultat de la conclusion.

Il contient les champs suivants séparés par un caractère CHR (10) :

Champs	Description	Remarque
version	Numéro de version du message d'acquittement	**Version actuelle : `1.0`**
reference	Référence de la commande	**Exemple : `ABERTYP00145`**
cdr	Code retour indiquant le résultat de la conclusion	**Valeurs possibles :** **`1` : conclusion acceptée** **`0` : conclusion refusée** **`-1` : erreur**
lib	Libellé détaillé précisant la nature du code retour	**Voir ci-dessous pour la liste des libellés possibles**
aut	Numéro d'autorisation de la conclusion si celle-ci a été acceptée	
phonie	Autorisation refusée pour un motif du type « appel phonie »	**Ce champ n'est présent que si le champ « phonie » était présent et renseigné dans la requête appelante** **N.B. Cette fonctionnalité n'est actuellement pas offerte par Desjardins**

Si cdr est différent de 1, la conclusion n'a pas été effectuée.

La liste des valeurs disponibles pour le libellé (champ lib) est donnée dans le tableau suivant :

cdr	Libellés	Description	Remarque
1	**paiement accepte**	L'autorisation a été délivrée et la conclusion a été effectuée	
1	**commande annulee**	La demande d'annulation a été prise en compte et la commande a été annulée	
1	**recurrence stoppee**	La demande d'annulation définitive du renouvellement a été prise en compte	**Uniquement en Paiement Récurrent.**
0	**commande non authentifiee**	La référence ne correspond pas à une commande	**Vérifier les paramètres référence et date_commande**
0	**commande expiree**	La date de commande dépasse le délai autorisé (+/- 24h)	
0	**commande grillee**	Le nombre maximal de tentatives de fourniture de carte a été atteint	**La commande n'est plus acceptée par le serveur de**

		(3 tentatives sont acceptées)	**paiement**
0	**autorisation refusee**	L'autorisation n'a pas été délivrée	**La conclusion n'est pas effectuée**
0	**la commande est deja annulee**	La commande a été annulée lors d'une précédente requête	**Aucune requête ne sera acceptée sur cette commande**
0	**paiement deja accepte**	Une demande d'autorisation a déjà été délivrée pour cette commande	
-1	**signature non valide**	La signature MAC est invalide	
-1	**verification echouee (mode de paiement)**	Le mode de paiement n'est pas compatible avec cette requête	**Par exemple : le paiement d'achat, car la conclusion est faite automatiquement**
-1	**la demande ne peut aboutir**	La demande de capture est formulée de manière incorrecte	**Vérifier les paramètres envoyés**
-1	**montant errone**	Un des montants transmis est mal formaté	**Vérifier les 4 paramètres de montant**
-1	**commercant non identifie**	Les paramètres servant à identifier le site commerçant ne sont pas corrects	**Vérifier les champs societe, lgue et TPE**
-1	**traitement en cours**	La commande est en cours de traitement	
-1	**date erronee**	La date ne respecte pas le format requis	**Vérifier le paramètre date**
-1	**autre traitement en cours**	Une autre transaction est en cours de traitement sur la même référence	**Soumettre la demande à nouveau**
-1	**probleme technique**	Un problème technique est survenu	**Soumettre la demande à nouveau**

3.3.2 Exemples de messages retournés

- Cas d'une capture acceptée

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

- Cas d'une annulation acceptée

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

- Cas d'une autorisation refusée sans le champ phonie fourni

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

- Cas d'une autorisation refusée au motif d'appel phonie avec le champ phonie renseigné à « oui »

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

- Cas d'une autorisation refusée avec le champ phonie renseigné à « oui »

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

- Cas d'une conclusion refusée avant la demande d'autorisation

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

- Cas d'une erreur

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

4 Demander une annulation de paiement

4.1 Annulation de paiement

Dans le cas où le commerçant a demandé un paiement et qu'il ne souhaite pas conclure la transaction (marchandise non disponible, client qui s'est rétracté, etc.), il peut notifier le serveur de Monetico de l'abandon de sa demande de paiement.

Pour cela, il appellera le service de capture comme décrit dans le chapitre précédent, en spécifiant le montant à annuler et le montant restant à 0CAD.

Exemple : annuler une commande d'un montant initial de 100 $

Chaîne utilisée pour le calcul du sceau :

```
1234567*05/12/2006:11:55:23*0CAD0CAD0CAD*ABERTYP00145*ExempleTexteLibre*3.0*FR*monSite1*
```

Requête :

```
POST /capture_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 299

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

Le montant à capturer et le montant restant doivent être égaux à 0

Le montant déjà capturé doit correspondre à l'historique de la commande

Cette capture peut s'effectuer si votre TPE est configuré en Paiement de préautorisation. En cas de succès, aucune conclusion ultérieure n'est réalisable.

5 Le service de remboursement (recrédit)

5.1 Présentation

Le but du service Récrédit_Paiement est de permettre aux commerçants de rembourser leurs clients d'une partie ou de la totalité de leur achat, de façon sécurisée, via Internet.

Pour demander un remboursement, l'application du commerçant doit faire appel au service web de « recrédit » du serveur de Monetico (via un message HTTPS), en fournissant un certain nombre d'informations (le montant du remboursement, sa date, sa référence, le numéro du TPE virtuel du commerçant, etc.). Un sceau doit être calculé pour certifier les données échangées.

En réponse à cette demande, le serveur de Monetico retourne le résultat de la demande de remboursement à l'application du commerçant : acceptée ou refusée.

5.2 Appel au service de recrédit

5.2.1 Les informations à fournir

L'application du commerçant doit émettre une requête en méthode POST par un message HTTPS (SSL V3), à destination du service Recredit_Paiement sur les serveurs de Monetico, contenant les champs suivants :

Champs	Description	Remarque
version	Version du système de paiement utilisée	**Version actuelle** `3.0`
TPE	Numéro de TPE Virtuel du commerçant Taille : 7 caractères	**exemple :** `1234567`
date	Date et heure de la demande de remboursement au format `JJ/MM/AAAA:HH:MM:SS`	**Exemple :** `05/12/2006:11:55:23`
date_commande	Date initiale de la commande au format `JJ/MM/AAAA`	**Exemple :** `03/12/2006`
date_remise	Date à laquelle a eu lieu la conclusion au format `JJ/MM/AAAA`	**Exemple :** `04/12/2006.` **Cette date sera la même que date_commande dans le cas d'un TPE configuré en mode Paiement d'achat**
num_autorisation	Numéro d'autorisation renvoyé par le serveur de Monetico lors de la demande d'autorisation	**Exemple :** `1234A6`
montant	Montant de la commande initiale	**Format :** **- Un nombre entier** **- Un point décimal (optionnel)** **- Un nombre entier (optionnel)** **- Une devise sur 3 caractères**
montant_recredit	Montant à rembourser	
montant_possible	Montant du remboursement maximum autorisé pour la transaction	

		alphabétiques ISO4217 (CAD) **Exemples : 62.73CAD** **10CAD** **1024CAD**
reference	Référence de la commande à rembourser	**Exemple : ABERTYP00145**
texte-libre	Zone de texte libre Taille : 3200 caractères maximum	
lgue	Code langue (en majuscules) Taille : 2 caractères	**FR, EN**
societe	Code alphanumérique à usage interne uniquement permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité	**Ce code est fourni par nos services.** **Exemple : monSite1**
MAC	Sceau issu de la certification des données Taille : 40 caractères hexadécimaux	

Note : le champ « montant_possible » est nécessaire afin que le serveur commerçant et le serveur de Monetico soient synchronisés. Si un remboursement a déjà été effectué sur ce numéro d'autorisation, il doit être ajusté par le commerçant. Par exemple, pour une commande de 100 $, si un remboursement de 10 $ a déjà été effectué, le prochain remboursement présentera une valeur de « montant_possible » de 90 $.

5.2.2 Calcul du sceau

Le sceau (à mettre dans le champ MAC) est calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.
Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations de la requête :

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

5.2.3 Contrôle de l'IP et limite du nombre de remboursements

Pour des raisons de sécurité, les requêtes de remboursement ne peuvent être émises que depuis des serveurs avec une adresse IP connue de nos services. De plus, chaque adresse IP est limitée quotidiennement dans le nombre de requêtes de remboursement qu'elle est autorisée à effectuer.

Avant de pouvoir effectuer des requêtes de remboursement dans l'environnement de production, il vous faudra donc communiquer par courriel à support@desjardins.monetico-services.com la liste des adresses IP à autoriser, ainsi que le nombre de remboursements quotidiens maximum pour chacune d'entre elles.

Pour des raisons de commodité, aucun contrôle n'est effectué pour les requêtes de remboursement dans l'environnement de test.

5.2.4 Exemple de requête de remboursement (recrédit)

Exemple 1 : remboursement partiel de 32 $ sur une commande de 100 $

Chaîne utilisée pour le calcul du sceau :

```
1234567*05/12/2006:11:55:23*32.00CAD100CAD*ABERTYP00145*Exemp
leTexteLibre*3.0*FR*monSite1*
```

Requête :

```
POST /recredit_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 328

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&date_commande=03%2F12%2F2006
&date_remise=04%2F12%2F2006
&num_autorisation=1234A6
&montant=100.00CAD
&montant_recredit=32.00CAD
&montant_possible=100CAD
&reference=ABERTPY00145
&texte-libre=ExempleTexteLibre
&lgue=FR
&societe=monSite1
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

En cas de succès, un remboursement d'un montant maximal de 68 $ est encore réalisable.

Exemple 2 : remboursement total sur une commande de 100 $

Chaîne utilisée pour le calcul du sceau :

```
1234567*05/12/2006:11:55:23*100CAD100CAD*ABERTYP00145*Exemp
leTexteLibre*3.0*FR*monSite1*
```

Requête :

```
POST /recredit_paiement.cgi HTTP/1.0
```

```
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 326

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&date_commande=03%2F12%2F2006
&date_remise=04%2F12%2F2006
&num_autorisation=1234A6
&montant=100.00CAD
&montant_recredit=100CAD
&montant_possible=100CAD
&reference=ABERTPY00145
&texte-libre=ExempleTexteLibre
&lgue=FR
&societe=monSite1
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

5.3 Réponse de la demande de remboursement (recrédit)

5.3.1 Les informations retournées

En retour à la demande de remboursement, l'application du commerçant reçoit un message d'acquittement de la part du serveur de Monetico. Ce message est un document de type MIME « text/plain » précisant le résultat du remboursement.

Il contient les champs suivants séparés par un caractère CHR(10) :

Champs	Description	Remarque
version	Numéro de version du message d'acquittement	**Version actuelle** `1.0`
reference	Référence de la commande	**Exemple :** `ABERTYP00145`
cdr	Code retour indiquant le résultat du recrédit	**Valeurs possibles :** `0` **: recrédit effectué** `<0` **: erreur**
lib	Libellé précisant la nature du code retour	**Voir plus loin pour la liste des libellés possibles**

La liste des valeurs disponibles pour le libellé est donnée dans le tableau suivant :

cdr	Libellés	Description	Remarque

0	**recredit effectue**	La demande de remboursement a été prise en compte	
-1	**recredit refuse**	La demande de remboursement n'a pas été prise en compte	
-30	**Commercant non identifie**	Les paramètres servant à identifier le site commerçant ne sont pas corrects	**Vérifier les paramètres societe, TPE et lgue**
-31	**signature non validee**	La signature MAC est invalide	
-32	**recredit non autorise**	Votre TPE n'est pas autorisé à effectuer des remboursements	**Contacter support@desjardins.monetico-services.com**
-33	**demande de recredit expiree**	La date de remboursement dépasse le délai autorisé (+/- 24h)	**Vérifier le paramètre date**
-34	**montant de recredit errone**	Le montant à rembourser est incorrect	**Vérifier le paramètre montant_recredit**
-35	**Les montants transmis sont incorrects**	Les montants transmis ne sont pas synchronisés avec ceux du serveur de Monetico	**Vérifier les champs montant_recredit et montant_possible**
-36	**le maximum de recredit a été atteint**	Le nombre maximum de remboursement pour votre TPE a été atteint	
-37	**la commande est inexistante**	La commande n'existe pas	**Vérifier que les champs permettant d'identifier la commande sont corrects**
-38	**la commande ne peut pas donner lieu a un recredit**	La commande n'a pas encore été payée, aucun remboursement ne peut être effectué	
-39	**le paiement est inexistant**	Une demande d'autorisation a déjà été délivrée pour cette commande	
-40	**le montant total des recredits ne peut depasser le seuil**	Le montant à rembourser est incorrect	
-41	**un probleme technique est survenu**	Problème technique	**Réitérer la demande**
-42	**la devise est incorrecte**	La devise transmise ne correspond pas à la devise de la commande	**Vérifier le paramètre devise**
-43	**parametres invalides**	Un ou plusieurs paramètres ne respectent pas le format requis	**Vérifier la longueur des champs et le format des dates**
-44	**autre traitement en cours**	Une autre transaction est en cours de traitement sur la même référence ; cela peut être un autre traitement que recredit_paiement	**Réitérer la demande**

5.3.2 Exemples de messages retournés

- Cas d'un recrédit accepté

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

- Cas d'une erreur

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

6 Aides à l'installation

6.1 Passer un TPE en production

Vous devez faire une demande auprès de support@desjardins.monetico-services.com pour faire passer votre TPE en production. Au préalable, il faudra que les trois derniers paiements effectués en test aient renvoyé un accusé de réception valide.

6.2 Foire aux questions

Peut-on personnaliser la page de paiement ?

Oui. Veuillez vous référer au document « Monetico Paiement Personnalisation de la Page de Paiement ».

Comment afficher mon logo sur votre page de paiement ?
Vous devez nous transmettre par courriel à l'assistance technique soit l'URL d'une image représentant votre logo, soit le logo en pièce jointe. Cette image doit être au format GIF et d'une taille de 120x120 pixels maxi.

Quel est le temps maximum dont dispose mon client pour effectuer le paiement (saisie du numéro de carte) suite à une commande sur mon site ?
L'internaute dispose de 45 minutes, à partir de l'arrivée sur la page de paiement, pour saisir les informations relatives à sa carte bancaire. Au-delà de ce délai, toute saisie sera refusée.

Quel est le nombre d'essais pour saisir les numéros de carte bancaire ?
Le nombre d'essai maximum pour un paiement est de 4.

Où peut-on trouver des numéros de carte pour effectuer des tests ?
Sur la page de paiement, vous trouverez une icône clignotante « TEST » ; en cliquant sur cette icône, une fenêtre présentant différents numéros de carte de test s'ouvre. Il vous suffit alors de sélectionner l'une des cartes et le formulaire de la page de paiement se remplit automatiquement.
Vous disposez de plusieurs cartes de test :

- 2 cartes 16 pan : l'une pour provoquer un paiement accepté et l'autre pour provoquer un paiement refusé
- 2 cartes 15 pan (cartes étrangères) sur le même principe

Quelles sont les langues prises en charge par la page de paiement ?

- Français
- Anglais

Peut-on être prévenu par courriel pour chaque demande de paiement ?

Une notification peut être envoyée par courriel à chaque fois qu'une demande d'autorisation est effectuée (une demande d'autorisation est effectuée si le format du numéro de carte a été validé). Il faut demander l'activation de cette option en s'adressant à l'assistance technique (voir chapitre 7)

Comment connaitre le nom et l'adresse des détenteurs de carte ?

Nous ne disposons pas des informations relatives aux coordonnées de l'acheteur sur notre serveur de paiement ; en effet, le client ne saisit que les informations concernant sa carte bancaire (numéro, date d'expiration et cryptogramme visuel).
Il n'est pas prévu dans le cadre de notre solution de paiement que le commerçant puisse nous transmettre des informations sur le client. Nous ne proposons pas de moyen de déduire l'identité du porteur à partir des informations de la carte.

Peut-on re-créditer un paiement ?

Oui, pour cela il faut demander l'option « re-crédit » à votre conseiller commercial. Cette fonction est ensuite disponible sur le tableau de bord commerçant.

A quoi correspondent les différentes « URL_RETOUR » du paramétrage ?

- `url_retour` : correspond au lien affiché en bas de notre page de paiement, lorsqu'une erreur est commise dans l'appel à notre page de paiement (commande déjà payée, commande expirée, …), ce lien permet à l'acheteur de revenir sur une page de votre boutique.
- `url_retour_ok` : correspond au lien (permettant à l'acheteur de retourner sur une page de votre boutique) affiché en bas de notre page de paiement si le paiement est accepté
- `url_retour_err` : correspond au lien (permettant à l'acheteur de retourner sur une page de votre boutique) affiché en bas de notre page de paiement si le paiement est refusé, ou lors du premier affichage de la page de paiement.

Il ne faut pas confondre ces URL avec l'URL de l'interface « Retour ».

A quoi sert l'« URL de confirmation CGI2 » ?

Cette URL est celle de votre interface « Retour », dont le rôle est de recevoir le message de confirmation du paiement émis par le serveur banque.

Où doit-on paramétrer l'« URL de confirmation CGI2 » ?

Cette URL est renseignée dans nos bases ; vous devez nous la fournir lors de la phase de mise en place de la solution. Vous devez également nous notifier tout changement d'adresse de votre interface « Retour » (en vous adressant à l'assistance technique (voir chapitre 7)).

Que faire lorsque je rencontre une erreur « CGI2 NOT OK » ?

Vous devez tout d'abord effectuer les vérifications de base suivantes :

- L'adresse de l'interface « Retour » que vous nous avez fournie est-elle valide ?
- Cette adresse est-elle accessible sur votre serveur depuis l'extérieur ?
- Le port sur lequel s'adresser à votre interface « Retour » est-il bien 80 (http) ou 443 (https) ? En effet, notre serveur de paiement n'accepte de s'adresser qu'à ces deux ports

Si le problème persiste, veuillez effectuer les vérifications supplémentaires suivantes :

- le traitement entre le retour de notre serveur et votre envoi d'accusé de réception ne doit pas durer trop longtemps (moins de 30 secondes)
- il ne doit pas être fait de redirection à la réception du code retour paiement
- Le format de l'accusé de réception renvoyé doit correspondre au format attendu pour un sceau valide.

Comment connaître la signification du code d'erreur indiqué dans l'email renvoyé en cas d'accusé de réception incorrecte ?

Il s'agit de codes d'erreur propres au logiciel cURL. Leurs descriptions sont disponibles à l'adresse suivante :
http://curl.haxx.se/libcurl/c/libcurl-errors.html

Pourquoi mon « URL de confirmation CGI2 » reçoit-elle des codes retour différents pour une même référence ?

Vos clients ont droit 4 essais pour saisir leurs informations bancaires pour une même référence dans un délai maximum de 45 minutes.
Après chaque tentative, nous envoyons son résultat sur votre url de confirmation. Vous pouvez donc recevoir plusieurs notifications de refus (code retour « Annulation ») avant de recevoir une éventuelle notification de paiement (code retour « paiement ») pour une même référence.
Exemple d'une cinématique avec plusieurs appels de l'url de confirmation :
Un client souhaite payer la référence ref0001 mais n'obtient pas d'autorisation de paiement avec la carte bancaire qu'il utilise.
Notre serveur va envoyer une notification de refus :

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ref0001&MAC=e4359a2c18d86cf2e4b0e646016c202e
89947b04&texte-libre=LeTexteLibre&code-
retour=Annulation&cvx=oui&vld=1208&brand=VI&status3ds=1&motifr
efus=Refus&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0
F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA
&veres=Y&pares=Y
```

Le client à la possibilité de refaire une tentative de paiement et il utilise sa seconde carte bancaire pour payer la référence ref0001. Le paiement est cette fois-ci accepté.
Notre serveur va envoyer une notification de paiement :

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f12%3a15%3a33&montant=62%
2e75EUR&reference=ref0001&MAC=f4562a2c18d86cfdbaf646016c202e89
945841&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1210&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=010101&hpancb=12754C03C22D786E0F2C2
CADBFC1C00A25df6322&ipclient=127%2e0%2e0%2e1&originetr=FRA&ver
es=Y&pares=Y
```

J'ai l'erreur Code 0 dans l'email renvoyé en cas d'accusé de réception incorrecte ?
Votre url de confirmation n'a pas renvoyé l'accusé de réception attendu pour un sceau validé.

J'obtiens le message « Ce TPE est fermé » lors d'une demande de paiement sur le serveur de TEST ?
Les TPE de TEST non utilisés pendant 15 jours glissants sont automatiquement fermés par nos services. Ils ne sont cependant pas supprimés : vous pouvez utiliser la fonctionnalité de réouverture d'un TPE de TEST en vous connectant sur votre tableau de bord.

Peut-on avoir un TPE pour plusieurs sites ?
Oui, mais cela nécessite en amont une demande auprès de votre conseiller commercial. Il faut cependant que les différents sites répondent à la même activité. Le paramétrage étant spécifique pour chaque site, il vous faut nous transmettre toutes les informations (URLs de retour, adresse de l'interface « Retour », logo, etc.).

Peut-on obtenir un fichier relevé des paiements ?
Une telle prestation peut vous être fournie par votre banque ; vous pouvez vous adresser à votre conseiller commercial.

6.3 Les problèmes les plus fréquents

6.3.1 Problème de calcul du sceau de sécurité

Message d'erreur en page de paiement
« Les informations transmises par votre commerçant ont une signature non valide : Le niveau de sécurité exigé n'est pas atteint. Notre serveur n'est pas en mesure de traiter la demande de paiement relative à votre commande ».

Message d'erreur en requête de capture

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

Message d'erreur en requête de recrédit

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

Causes possibles

- le formulaire que vous nous avez envoyé ne contient pas toutes les informations requises

- le calcul du sceau MAC est erroné
- le calcul du sceau MAC est effectué avec une mauvaise clé

Résolution du problème
Suivez scrupuleusement le cheminement décrit ci-dessous ; à la fin de chaque étape où vous avez effectué des changements dans votre implémentation, effectuez de nouveaux tests de paiement. S'ils ne sont pas fructueux, passez à l'étape suivante.
Attention : ne sautez pas d'étape !

Etape 1 : vérifiez que toutes les variables envoyées dans le formulaire sont présentes, correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.

Etape 2 : vérifiez que vous avez réussi à éviter les erreurs inhérentes à certains champs particuliers :

- la valeur de la version MAC correspond-elle à une chaîne de 40 caractères hexadécimaux (valeurs autorisées : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) ?
- la valeur de la variable version correspond elle à 3.0 ?
- la valeur de la variable date est-elle bien au format JJ/MM/AAAA:HH:MM:SS ?
- la valeur de la variable reference est-elle bien une chaîne ne contenant que des lettres (non accentuées) et des chiffres pour une longueur maximale de 12 caractères ?
- la variable texte-libre est-elle correctement orthographiée, en respectant la casse et avec le caractère tiret ('-') et non le caractère souligné ('_') ?
-

Etape 3 : vérifiez que la chaîne sur laquelle vous calculez le sceau MAC respecte le formalisme décrit précédemment.

Soyez particulièrement attentif au fait que les données utilisées doivent être les mêmes que celles que vous fournissez dans le formulaire de paiement ; le meilleur moyen pour atteindre cet objectif est de stocker à l'avance les différentes informations, puis d'utiliser ce stockage pour le calcul du sceau MAC et pour la construction du formulaire. Au contraire, renseigner les données à la volée peut induire des différences entre celles utilisées pour le calcul du sceau et celles utilisées pour la construction du formulaire (par exemple, pour le champ date, il peut y avoir une différence de quelques secondes).

Etape 4 : vérifiez que vous utilisez la bonne clé de sécurité :

- vous devez utiliser la dernière clé qui vous a été fournie par nos services,
- vérifiez que la clé correspond à votre algorithme de calcul de sceau (SHA1 ou MD5),
- Contactez notre service de support afin de valider ensemble que vous utilisez bien la bonne clé, et afin de valider que la version de votre formulaire (champ « version ») correspond à la version paramétrée dans notre système.

Si malgré toutes ces vérifications vous obtenez toujours ce message d'erreur, le problème réside dans l'intégration de notre solution dans votre système d'information.
La grande diversité des langages et des spécificités liées à l'environnement utilisé pour l'implémentation de notre solution de paiement sont autant de paramètres dont nous ne maîtrisons pas tous les aspects et par conséquent, ils ne nous permettent pas de vous fournir un support personnalisé plus ample.

6.3.2 Le commerçant ne peut pas être identifié

Message d'erreur en page de paiement
« Le site de votre commerçant n'a pas été identifié par notre serveur. Nous ne sommes pas en mesure de traiter la demande de paiement relative à votre commande. »

Message d'erreur en requête de capture

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

Message d'erreur en requête de recrédit

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

Causes possibles
- le numéro de TPE est incorrect ou inexistant
- le code société est incorrect ou inexistant
- le code langue est incorrect ou inexistant
- l'adresse IP du serveur commerçant n'est pas autorisée à faire du recrédit

Résolution du problème
Vérifiez que les variables TPE, societe et lgue sont présents dans le formulaire, correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.

6.3.3 La commande a déjà été traitée

Message d'erreur
« Votre commande a déjà été traitée. »

Causes possibles
Vous avez fourni une référence de commande déjà utilisée lors d'une précédente transaction.

Résolution du problème

Vous devez générer une nouvelle référence de commande unique.

6.3.4 La date de validité de la commande est dépassée

Message d'erreur
« La date de validité de votre commande est dépassée. »

Causes possibles
- soit la référence de commande est en instance de paiement depuis un délai trop important (typiquement plus d'une heure)
- soit le formulaire de commande a été créé depuis un délai trop important, typiquement plus de 12 heures

Résolution du problème
- testez un formulaire mis à jour avec une nouvelle référence de commande
- testez un nouveau formulaire et vérifiez la date système de votre serveur

6.3.5 Le mode de paiement utilisé est non disponible

Message d'erreur
« Mode de paiement non disponible. »

Causes possibles
- soit il y a une erreur de syntaxe dans le formulaire soumis
- soit il s'agit d'un mode de paiement non souscrit par le commerçant

Résolution du problème
Vérifiez que les variables présentes dans le formulaire sont correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.
Vérifiez que vous n'employez pas un mode de paiement différent de celui que vous avez souscrit.

6.3.6 La commande ne peut pas être authentifiée

Message d'erreur

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

Causes possibles
- la référence est incorrecte ou inexistante
- la date de commande est incorrecte ou inexistante

Résolution du problème
Vérifiez que les variables reference et date_commande sont présentes dans le formulaire, correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.

Vérifiez que la référence de commande à capturer a bien été autorisée ou enregistrée à la date que vous fournissez

6.3.7 Les montants sont erronés

Message d'erreur

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

Causes possibles

- l'un des montants transmis est incorrect
- la somme des montants est incorrecte

Résolution du problème

Vérifiez que les variables montant, montant_a_capturer, montant_deja_capture et montant_restant sont présentes dans le formulaire, correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.
Vérifiez que la somme des valeurs des variables montant_a_capturer, montant_deja_capture et montant_restant est égale à la valeur de la variable montant pour une mise en recouvrement.

Vérifiez que les valeurs des variables montant_a_capturer et montant_restant sont égales à 0EUR pour une annulation.

7 Le fichier récapitulatif

Les informations que nous transmettons à votre interface « Retour » peuvent également être mises à votre disposition de manière consolidée via un fichier récapitulatif.

L'envoi de ce fichier, ou sa suspension, se paramètrent depuis votre tableau de bord[2]. Les paramètres que vous pouvez personnaliser sont :

- la fréquence d'envoi : quotidienne, hebdomadaire ou mensuelle,
- les états souhaités des commandes : Enregistré, Refusé, Grillé (Bloqué), Payé, Annulé,
- le format du fichier que vous souhaitez recevoir : CSV ou XML
- le type d'envoi : par courriel ou par FTP
- le paramétrage de l'envoi courriel ou FTP

Le fichier qui vous sera transmis contient les champs suivants :

Champ	Description	Commentaire
1	date de la conclusion	format AAAA-MM-DD
2	numéro de TPE virtuel	
3	référence de la commande	telle que fournie par le commerçant
4	état de la commande : selon la sélection effectuée par le commerçant sur la liste des états désirés	AN : vous avez annulé la demande de paiement AU : paiements enregistrés avec succès et en attente de conclusion GR : commande annulée suite à 4 tentatives infructueuses PA : le paiement a été autorisé et conclu PP : paiement partiel enregistré avec succès et en attente de conclusion (non supporté actuellement) RE : l'autorisation de paiement n'a pas été accordée
5	date de la demande de paiement	format AAAA-MM-DD
6	heure de la demande de paiement	format hh:mm:ss
7	Montant de la transaction formaté de la manière suivante : - Un nombre entier - Un point décimal (optionnel) - Un nombre entier (optionnel)	
8	Devise de la transaction	sur 3 caractères alphabétiques ISO4217 (CAD)
9	Numéro d'autorisation tel que fourni par l'institution émettrice	Uniquement dans le cas où l'autorisation a été accordée
10	Obtention de l'accusé de réception de l'interface retour du commerçant	OK : votre interface retour nous a fourni un AR valide NOK : votre interface retour ne nous a pas fourni d'AR valide
11	Référence d'archivage	Uniquement en cas de souscription du module prévention fraude

[2] Une page d'aide vous guide dans le paramétrage le plus adapté à votre besoin.

12	Type de carte	AM : American Express MC : Mastercard VI : Visa Uniquement en cas de souscription du module prévention fraude
13	date de validité de la carte	format MMAA Uniquement en cas de souscription du module prévention fraude
14	présence du cryptogramme visuel	oui non Uniquement en cas de souscription du module prévention fraude
15	texte libre tel que fourni par le commerçant	

8 Assistance technique

Desjardins propose une assistance à la compréhension générale de l'utilisation de sa solution :

- Par courriel : support@desjardins.monetico-services.com
- Par téléphone :
  Montréal et les environs : 514 397-4450
  Canada et États-Unis : 1 888 285-0015

Cependant, Desjardins n'offre qu'un soutien limité concernant les problématiques d'intégration technique de sa solution de paiement.

9 Annexes

9.1 Contraintes générales de codage HTML des champs

Tous les champs de la requête d'appel, à l'exception de la version et des montants, doivent être codés en HTML avant la mise en forme dans le formulaire (c'est à dire immédiatement après le calcul du MAC).

Les caractères à coder sont les codes ASCII de 0 à 127 réputés risqués :

Nom	Symbole	Remplacement
Signe Commercial	&	&amp;
Signe inférieur	<	&lt;
Signe supérieur	>	&gt;
Guillemets	"	" ou "
Apostrophe	'	&#x27;

Les fonctions de type « HTML_ENCODE » (norme IETF RFC1738) des langages conviennent parfaitement, elles encodent beaucoup plus de caractères, typiquement tout ce qui n'est pas :

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- abcdefghijklmnopqrstuvwxyz
- 0123456789
- _ . - (souligné, point, tiret)

Si vous utilisez dans le champ « texte-libre » des caractères hors de la plage ascii commune imprimable (31<ascii<127), vous devez coder ce champ avant tout traitement relatif au paiement pour éviter tout problème de calcul du sceau MAC.

Enfin, les champs ne doivent pas contenir les caractères ASCII 10 et 13 (CR et LF).

9.2 Contraintes particulières selon le champ

Champs	Contenu / format avant codage HTML	Taille maximale après codage HTML
tpe	A-Z a-z 0-9	**7**
version	3.0	**Fixe**
date		**50**
montant		**20**

reference	A-Z a-z 0-9	**12**
MAC	0-9 A-F a-f	**40**
lgue	A-Z	**2**
societe	A-Z a-z 0-9	**20**
texte-libre	Base 64	**3200**
URLs		**2048**
Mail		**255**
Nbrech	2-4	**1**
dateechN		**50**
montantechN		**20**
date_commande		**50**
montant_a_capturer		**20**
montant_deja_capture		**20**
montant_restant		**20**
phonie	**A-Z a-z 0-9**	**50**
num_autorisation		**10**
montant_recredit		**20**
montant_possible		**20**
stoprecurrence	**OUI**	**3**

9.3 URLs des services

9.3.1 L'environnement de test

Le rôle de notre serveur de test est de vous permettre de valider vos développements. Bien sûr, toutes les opérations effectuées par notre serveur de paiement de test sont fictives et ne débouchent sur aucun mouvement financier réel.

Pour effectuer des demandes de paiement dans cet environnement, nous mettons à votre disposition des cartes de crédit de test, accessibles en cliquant sur l'icône « Carte de Test » de la page de paiement.

Les environnements de test sont disponibles aux adresses suivantes :

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

Le tableau de bord commerçant de test vous permet de gérer et contrôler les paiements effectués dans l'environnement de test. Il est disponible à l'adresse suivante :

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

9.3.2 En Production

Après avoir validé vos développements et procédé à la demande de mise en production de votre TPE auprès de « support@desjardins.monetico-services.com », vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

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

Vous pouvez consulter les paiements opérés sur votre TPE via le tableau de bord commerçant disponible à l'adresse suivante :

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

Nous attirons votre attention sur le fait que les requêtes adressées au serveur de production seront des opérations réelles.

FIN DU DOCUMENT