Desjardins

Monetico Paiement

PAGE INTÉGRÉE (IFRAME)

PAIEMENT EN LIGNE

Nom de fichier : Monetico_Paiement_Internet_Page_Intégrée_v2.0
Numéro de version : 2.0
Date : 2016-12-02

Confidentiel

Titre du document : Monetico Paiement Page Intégrée (iFrame)
Nom de fichier : Monetico_Paiement_Internet_Page_Intégrée_v2.0
Numéro de version : 2.0
Date : 2016-12-02

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 en mode page intégrée (iframe) 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, CB	carte de paiement, CP
chiffre vérificateur	code de vérification
code société	numéro de marchand
commerçant	Marchand
email, mail	Courriel
emails jetables	liste noire (« black list »)
émulation	sans redirection
environnement de validation	environnement de test
interface retour	confirmation
mise en recouvrement	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
ticket récapitulatif	relevé de transaction
TPE - Terminal de Paiement Électronique	TPV Terminal Point de Vente; mode de paiement
TPEV - TPE virtuel (web)	TPV virtuel

2 Page intégrée (iFrame)

2.1 Principe

Permettre aux commerçants de traiter leurs paiements de façon sécurisée via Internet sans sortir du tunnel de vente commerçant. Contrairement à la page de paiement Monetico, la page intégrée se fond dans le site Web du commerçant. Le serveur de paiement de Monetico effectue la vérification de la validité des informations de la carte de paiement transmises avant d'accorder l'autorisation de paiement et confirme automatiquement le résultat de la demande de paiement à l'application du commerçant.

Les échanges sont réalisés en toute sécurité (chiffrement TLS V1.0 et supérieur), garantissant la confidentialité des informations fournies par le commerçant.

Afin de certifier les données échangées, un sceau est calculé sur l'ensemble des données fournies par le commerçant au serveur Monetico, à l'aide d'une fonction standard (IETF RFC2104). Ce sceau est intégré aux données fournies et vérifié par nos serveurs à chaque paiement.

Vous bénéficiez d'un retour d'information immédiat sur votre serveur suite à chaque paiement effectué sur notre plate-forme, vous notifiant du succès ou de l'échec du paiement. En complément, nous pouvons également vous notifier par courriel du résultat de ces paiements.

2.2 Clé de sécurité commerçant

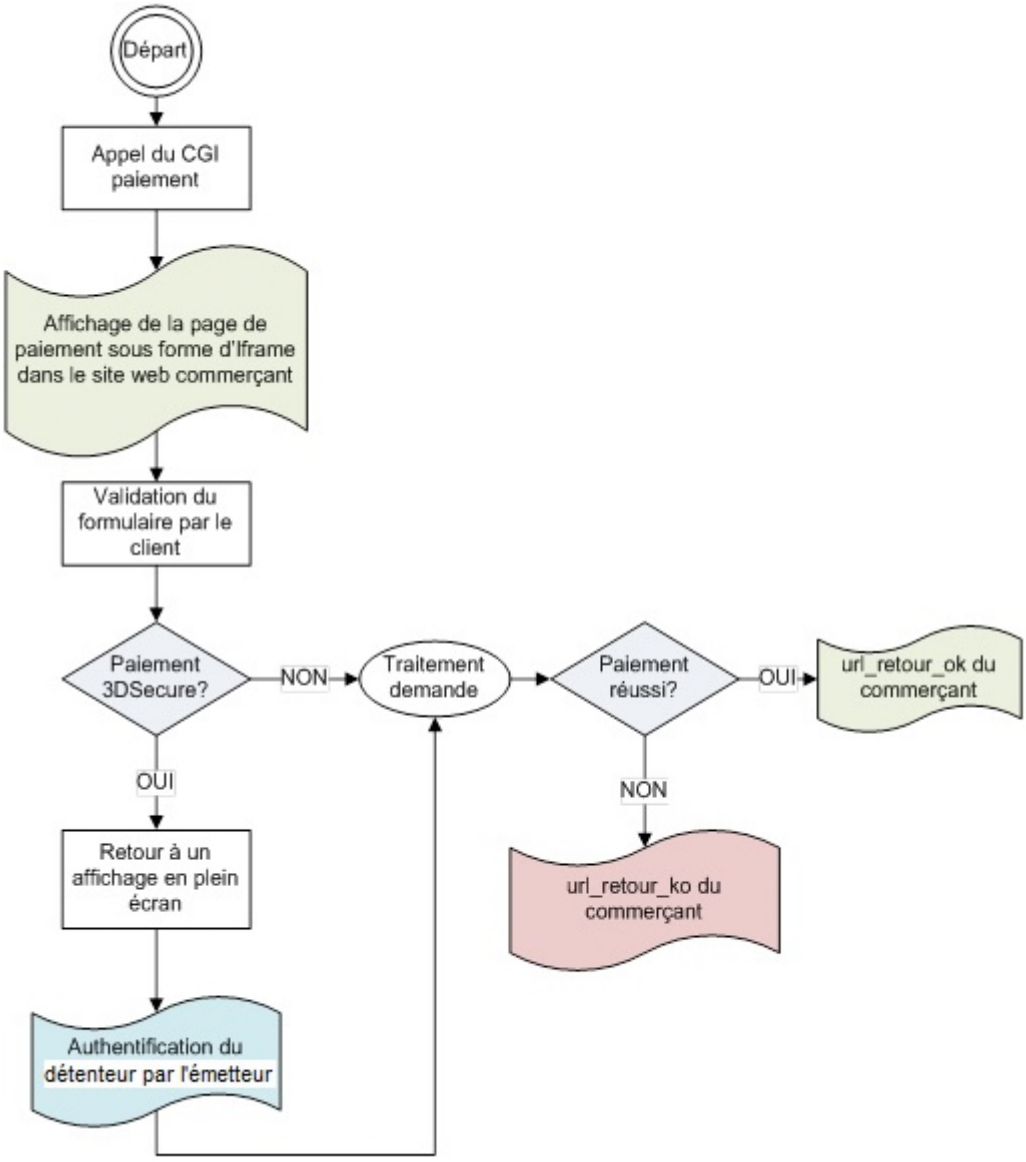
Une clé de sécurité, propre à chaque TPE, destinée à certifier les données échangées entre le serveur du commerçant et le serveur de paiement sécurisé de Monetico, est indispensable pour utiliser le service Monetico Paiement sous la forme de page intégrée. Un lien, permettant de télécharger cette clé de sécurité, est envoyé par notre centre de support 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 externe doit être convertie en une chaîne de 20 octets (représentation opérationnelle) avant utilisation.

3 Cinématiques

3.1 Enchainement des écrans

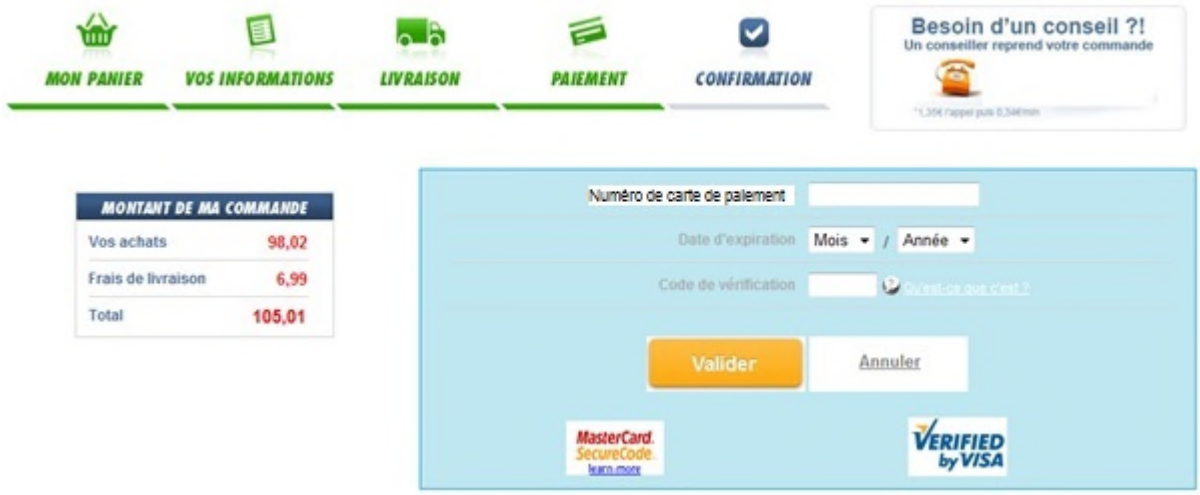


3.2 Affichage de la page intégrée

L'application Monetico Paiement affiche le formulaire de saisie dans le site web du commerçant en appliquant une personnalisation lui permettant de se fondre dans le site marchand.

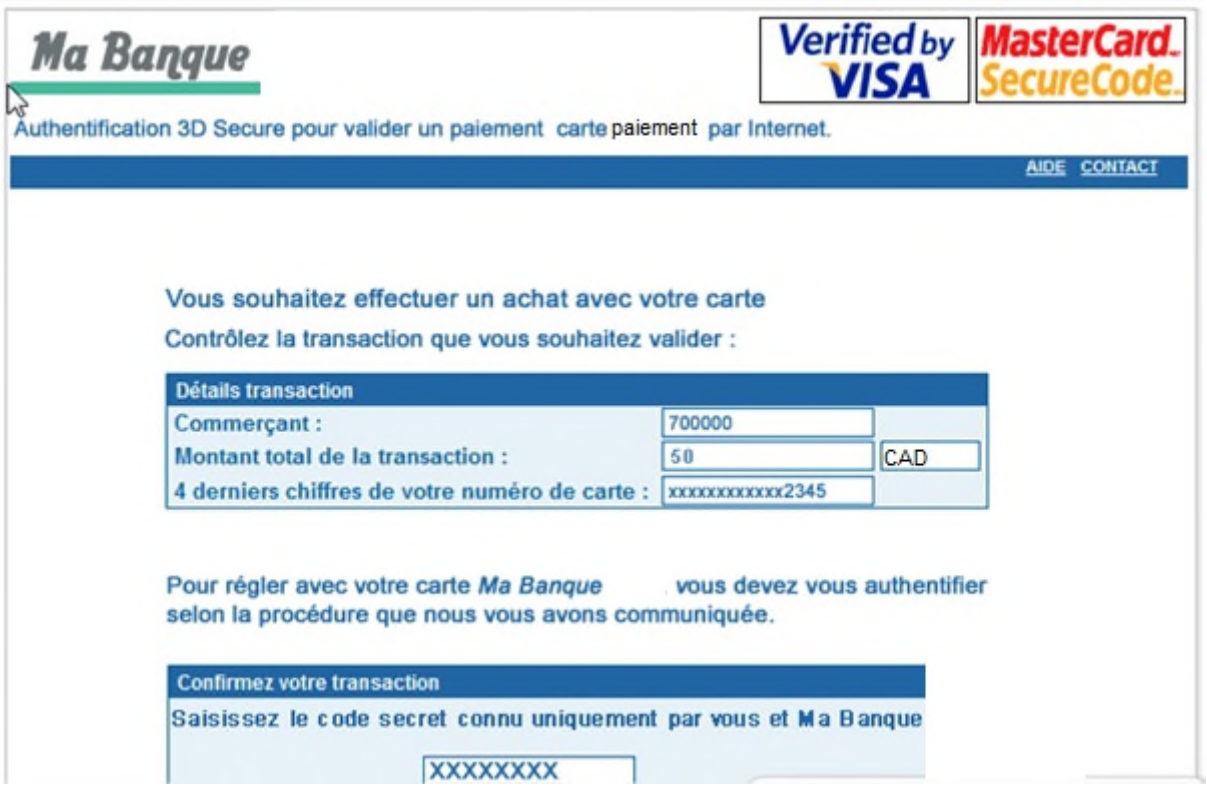
Dans le cas d'un paiement non 3DSecure :

Dans le cas d'un paiement 3DSecure :



3.3 Redirection ACS

Dans le cas d'un paiement 3DSecure, l'application Monetico Paiement reviendra sur un affichage classique avant de rediriger le client vers le système d'authentification de l'émetteur de sa carte:



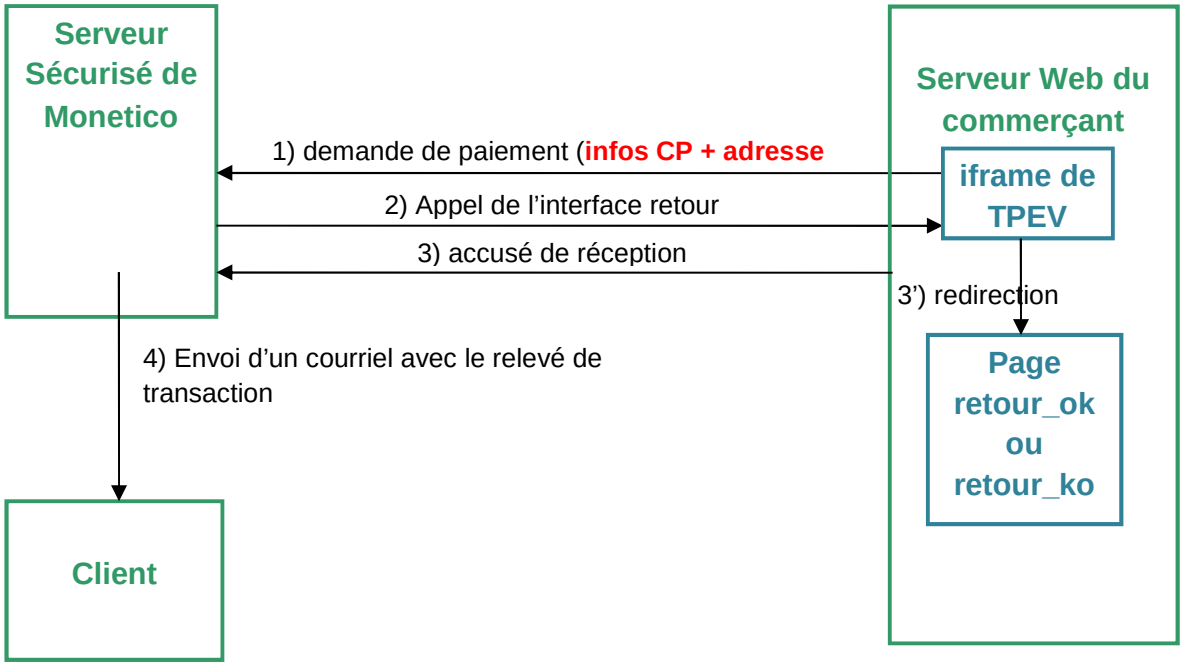
3.4 Retour paiement

Un exemple de page de retour du commerçant présentant le résultat du paiement au détenteur.

3.5 Demandes de paiement

3.5.1 Si la carte du client n'est pas 3DSecure

Le schéma suivant décrit les échanges entre le serveur Web du commerçant et le serveur sécurisé Monetico :



1. Demande de paiement : saisie des informations cartes sur la page intégrée au site marchand.

2. Le serveur Monetico informe directement le système informatique du commerçant du résultat de la demande de paiement en émettant une requête http(s) sur l'adresse de confirmation des paiements (en d'autres termes, **le serveur Monetico appelle l'interface « Retour »** placée sur la machine du commerçant).
   Vous devez nous indiquer cette adresse URL au moment de la mise en place du système et en cas de changement (modification de nom de domaine ou de répertoire).

3. Le système informatique du commerçant accuse réception de la confirmation du paiement.

   En pratique, l'interface « Retour » est chargée de recevoir la requête de confirmation du paiement, d'en extraire les différentes informations et de répondre au serveur Monetico par un accusé de réception.
   Les informations reçues par l'interface « Retour » permettent de déterminer la commande concernée, ainsi que le résultat de la demande de paiement. Cela permet au serveur du commerçant d'effectuer des traitements spécifiques :

- Vérifier que le montant et la référence correspondent au règlement d'une commande enregistrée en attente de paiement
- Mettre à jour le statut de la commande dans les bases de données
- Envoyer un courriel de confirmation au commerçant et/ou à l'acheteur
- Etc.

Attention : la commande doit être persistante dans le système commerçant (fichier, base de données) dès le début du processus et ne doit pas être détruite même après un premier avis de refus de paiement.

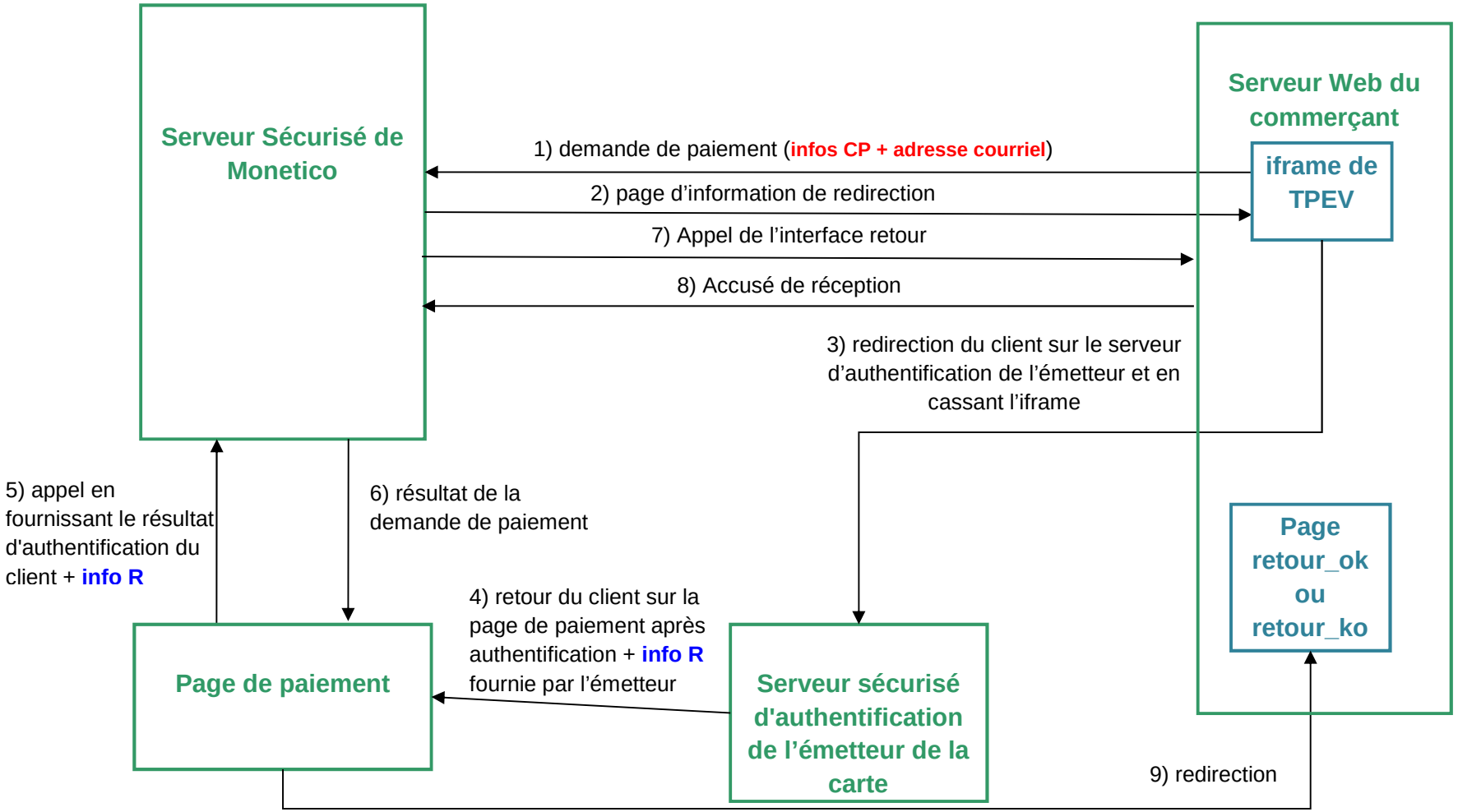
En effet, un refus peut être suivi d'un accord (l'interface « Retour » peut donc être appelée plusieurs fois pour une même commande), par exemple en cas d'erreur de saisie ou de plafond CP atteint ; l'acheteur peut donc vouloir utiliser une autre carte pour effectuer son paiement.

4. Envoi d'un email au client résumant la transaction effectuée

3'. Redirection vers la page retour_ok ou retour_ko du commerçant selon le résultat du paiement

2.5.2 Si la carte du client est 3DSecure

Le schéma suivant décrit les échanges entre le serveur Web du commerçant, le serveur sécurisé Monetico et le serveur sécurisé d'authentification de l'émetteur de la carte du détenteur :



1. Demande de paiement : vérification de la participation au protocole 3DSecure de la carte saisie sur la page intégrée au site marchand.

2. Le serveur Monetico retourne une page de redirection vers le serveur sécurisé d'authentification de l'émetteur de la carte du détenteur.

3. Redirection du client vers le serveur d'authentification de l'émetteur de sa carte en revenant à un affichage classique.

4. Après authentification, le client est redirigé vers la page de paiement accompagné de la réponse (R) du serveur sécurisé d'authentification de l'émetteur de la carte du détenteur.

5. La page de paiement soumet alors au serveur Monetico le résultat (R) d'authentification du client, tel qu'il a été fourni par l'émetteur de la carte du détenteur.

6. Le serveur Monetico retourne le résultat du paiement à la page de paiement : paiement approuvé ou paiement refusé.

7. Le serveur Monetico informe directement le système informatique du commerçant du résultat de la demande de paiement en émettant une requête http(s) sur l'adresse de confirmation des paiements (en d'autres termes, **le serveur Monetico appelle l'interface « Retour »** placée sur la machine du commerçant).
   Vous devez nous indiquer cette adresse URL au moment de la mise en place du système et en cas de changement (modification de nom de domaine ou de répertoire).

8. Le système informatique du commerçant accuse réception de la confirmation du paiement.

   En pratique, l'interface « Retour » est chargée de recevoir la requête de confirmation du paiement, d'en extraire les différentes informations et de répondre au serveur Monetico par un accusé de réception.
   Les informations reçues par l'interface « Retour » permettent de déterminer la commande concernée, ainsi que le résultat de la demande de paiement. Cela permet au serveur du commerçant d'effectuer des traitements spécifiques :

   - Vérifier que le montant et la référence correspondent au règlement d'une commande enregistrée en attente de paiement
   - Mettre à jour le statut de la commande dans les bases de données
   - Envoyer un courriel de confirmation au commerçant et/ou à l'acheteur
   - Etc.

   Attention : la commande doit être persistante dans le système commerçant (fichier, base de données) dès le début du processus et ne doit pas être détruite même après un premier avis de refus de paiement.

En effet, un refus peut être suivi d'un accord (l'interface « Retour » peut donc être appelée plusieurs fois pour une même commande), par exemple en cas d'erreur de saisie ou de plafond CP atteint ; l'acheteur peut donc vouloir utiliser une autre carte pour effectuer son paiement.

9. La page de paiement redirige alors vers la page retour_ok ou retour_ko du commerçant selon le résultat de la demande.

4 Fonctionnement

4.1 Intégration au site marchand

Le site marchand intègre l'appel à Monetico Paiement à l'aide d'une balise HTML « iframe » au sein de la boutique:

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

Les valeurs des champs id et name sont des exemples sans influence sur le comportement de l'application.

Le champ « src » doit être valorisé sous la forme :

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

Utilisez uniquement les champs cités ci-dessous lors de vos appels à la page de paiement. L'emploi de champs non référencés pourrait amener un blocage lors de l'accès à la page de paiement, cet accès étant considéré comme non légitime.

Les paramètres à renseigner sont :

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 TTC de la commande formatée de la manière suivante : Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres* (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (`CAD`)	**Exemples :** `62.73CAD` `10CAD` `1024CAD` ***Attention : un arrondi est effectué automatiquement s'il y a plus de 2 décimales.**
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 email de l'internaute	**Exemple :** `email@e.ca`
lgue	Code langue Taille : 2 caractères	**Valeurs possibles :** `FR` `EN`
societe	Code alphanumérique permettant au	**Ce code est fourni par**

	commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité	**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 revient sur le site du commerçant suite à un paiement approuvé	**Attention : à ne pas confondre avec l'URL de l'interface « Retour », aussi appelée URL de confirmation des paiements**
url_retour_ko	URL par laquelle l'acheteur revient sur le site du commerçant suite à un paiement refusé	
MAC	Sceau issu de la certification des données Taille : 40 caractères hexadécimaux	
options	Liste des options utilisées (peut être vide). 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 '='.	**Exemple : `opttest=abc&optbis=123`**
mode_affichage	Paramètres permettant d'activer l'affichage sous forme l'iframe	**Pour activer l'iframe : `iframe`**

Attention, toutes ces valeurs devront être « URL encodés » (voir **Annexes, 6.3**), ainsi par exemple :

mail=email@e.ca
url_retour_ok=http://www.monsiteweb.com/paiement/retourOK.html

Deviendront :

mail=email%40e.ca

url_retour_ok=http%3A%2F%2Fwww.monsiteweb.com%2Fpaiement%2FretourOK.html

Cet encodage doit se faire après le calcul du sceau de sécurité.

4.2 Validation du paiement

Lorsque le client valide ou abandonne le paiement, l'application Monetico Paiement revient sur un affichage classique et redirige le client vers la page url_retour_ok ou url_retour_ko, qui devra alors réafficher une page complète (c'est-à-dire avec les bandeaux, entêtes et autres éléments de navigation du site) au détenteur.

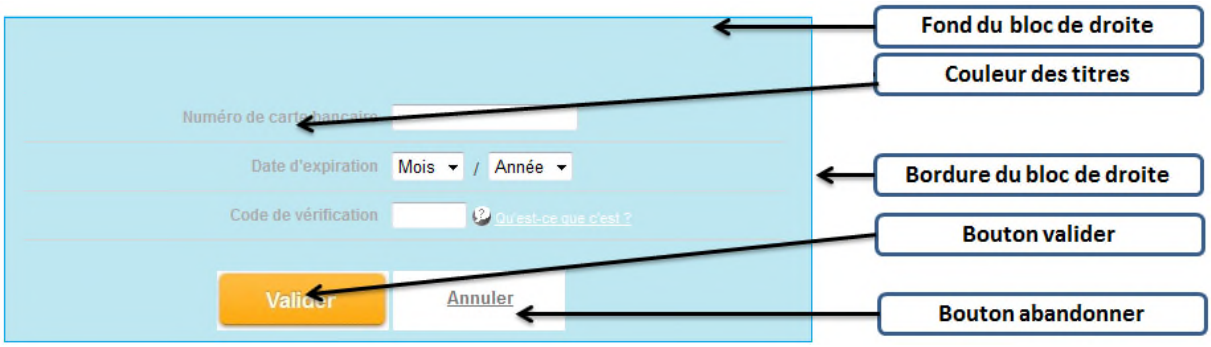
5 Spécificités de la page intégrée

5.1 Le mode d'affichage

Afin que le mode d'affichage intégré soit actif, l'appel à Monetico Paiement, le paramètre ***mode_affichage*** doit être valorisé à ***iframe*** sans quoi la page de paiement classique s'affichera sans personnalisation.

5.2 Personnalisation de la page

En mode de fonctionnement intégré, il est possible de personnaliser les éléments suivants :



Les boutons sont personnalisables sous forme d'image :

- Format gif
- Taille 128 x 25 pixels

Seule la couleur des différents éléments est personnalisable.

5.3 Envoi du relevé de transaction par courriel

Comme pour tous paiements, le client doit être informé du résultat du paiement par le Monetico Paiement. Dans le cadre du paiement par page de paiement intégrée, le relevé de transaction est envoyé directement au client par courriel. L'adresse courriel du client devient un paramètre obligatoire pour que le processus puisse se dérouler sous sa forme intégrée.

Le non-respect de cette règle impliquera une redirection vers la page de paiement sans application de la personnalisation affichant la page de paiement en plein écran.

5.4 Retour sur le site marchand

Lorsque la demande est traitée (refusée ou approuvée), la redirection sur le site marchand sera faite vers l'URL adaptée (cf. paramètres url_retour_ok et url_retour_ko) sans action complémentaire de l'utilisateur. L'affichage sous forme de page intégrée au site marchand ne sera pas conservé et les URLs de retour devront réafficher l'intégralité de la page du site marchand.

Il ne sera pas possible de placer plusieurs appels à une page de paiement intégrée car la première validée déclenchera une action entraînant potentiellement un changement de page.

6 Annexes

6.1 Contraintes générales de codage HTML des champs

Tous les champs de la requête d'appel, à l'exception de la version et du montant, 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 impérativement 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 » (cf. 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 ASCII 13 (CR et LF).

6.2 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**
référence	A-Z a-z 0-9	**12**
MAC	0-9 A-F a-f	**40**
lgue	A-Z	**2**
societe	A-Z a-z 0-9	**50**
texte-libre	Base 64	**3200**
numero_carte	0-9	**16**
annee_validite	0-9	**4**
mois_validite	0-9	**2**
cvx	0-9	**3**
phonie	A-Z a-z 0-9	**50**
mail		**50**
nbrech	2-4	**1**
dateechN		**50**
montantechN		**20**
option=clientip	0-255.0-255.0-255.0-255	**25**
mode_affichage=iframe	a-z	

6.3 Contraintes générales de codage URL des champs

Toutes les valeurs passées au CGI devront être URL encodés, avant l'envoi, comme précisé en 4.3. Les caractères à coder impérativement sont les codes ASCII de 0 à 127, réputés risqués :

Nom	Symbole	Remplacement
Signe Commercial	&	%26
Signe inférieur	<	%3C
Signe supérieur	>	%3E
Guillemets	"	%22
Apostrophe	'	%27
Arobase	@	%40

(Cette liste n'est pas exhaustive)

Les fonctions de type « urlencode **» des langages conviennent parfaitement,** elles encodent beaucoup plus de caractères, typiquement tout ce qui n'est pas :

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

6.4 Explication du mode 3D-Secure

6.4.1 Principe

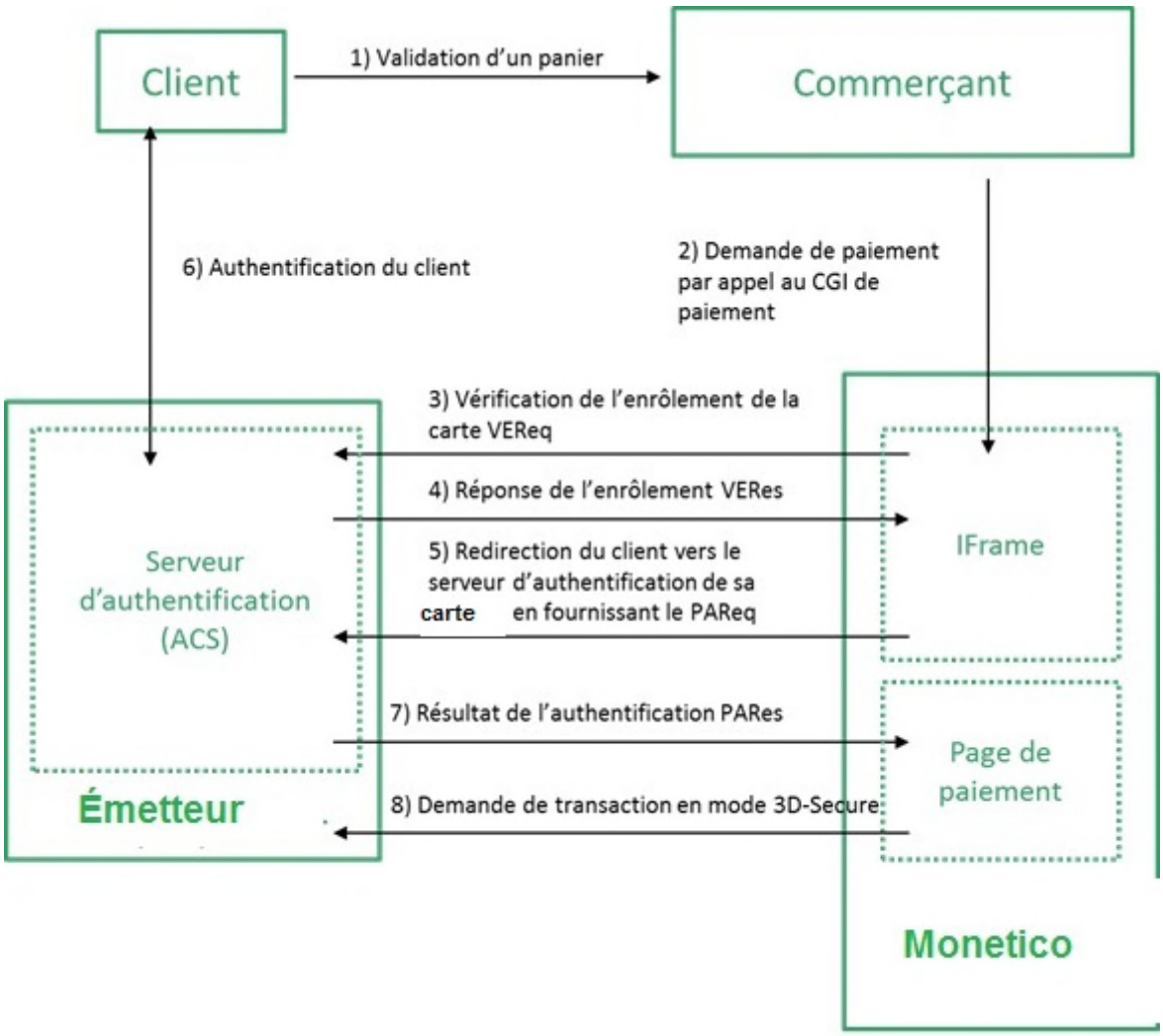
Afin de renforcer la sécurité des transactions sur internet, une nouvelle norme de sécurité existe : le 3D Secure. Elle a pour but de réduire les risques de fraude, grâce une procédure d'authentification du détenteur de la carte auprès de l'émetteur de sa carte.

Un objectif : diminuer les risques de fraude

Afin d'éviter qu'une transaction soit rejetée parce que le client conteste l'achat auprès de l'émetteur de sa carte, celle-ci vérifie désormais l'identité du client. En plus du numéro, de la date de validité et du cryptogramme, avec le système 3D Secure, le détenteur de la carte doit s'authentifier auprès de l'émetteur de sa carte en lui fournissant un code ou une information personnelle.

6.4.2 Fonctionnement

Voici le synoptique simplifié des échanges en mode 3DSecure :



Etape	Description
Etape 1	Le client valide son panier sur le site internet du commerçant.
Etape 2	Le site web du commerçant appel le CGI de paiement dans une iframe
Etape 3	Le serveur Monetico (l'iframe) envoie une requête de vérification d'enrôlement de la carte de paiement du client (VEReq) au serveur d'authentification de l'émetteur de la carte du détenteur (ACS).
Etape 4	Le serveur d'authentification de l'émetteur de la carte du détenteur soumet le résultat d'enrôlement (VERes) au serveur Monetico (l'iframe). Si la carte de paiement du client n'est pas enrôlée 3D-Secure, une demande d'autorisation est effectuée, et les étapes 4 à 9 sont ignorées.
Etape 5	L'iframe redirige le client sur le site de l'émetteur de sa carte en

	effectuant une requête d'authentification (PAReq).
Etape 6	L'ACS reçoit la requête d'authentification (PAReq).
Etape 6	L'ACS procède à l'authentification du client.
Etape 7	L'ACS soumet le résultat d'authentification du client (PARes) au serveur Monetico (page de paiement).
Etape 8	Le serveur Monetico effectue la demande d'autorisation en mode « 3D-Secure ».

6.4.3 Glossaire 3D-Secure

Terme	Description
ACS	Serveur sécurisé d'authentification 3D-Secure.
VEReq	Requête pour la vérification de l'enrôlement d'une carte de paiement en 3D-Secure.
VERes	Résultat d'enrôlement d'une carte de paiement en 3D-Secure.
PAReq	Requête d'authentification du client.
PARes	Résultat de la requête d'authentification du client.
MPI	Plug-in marchand : module logiciel qui permet de vérifier l'enrôlement 3D-Secure d'une carte de paiement et de retourner l'adresse du site Web du serveur d'authentification de l'émetteur de la carte du détenteur.

7 Utilisation du service

7.1 En Test

Le rôle de notre serveur de test est de vous permettre de tester et de valider vos développements.

Sur ce serveur, le seul contrôle effectué est un contrôle de structure du numéro de carte. Il n'y a pas d'autres contrôles effectués : date d'expiration, contrôle du fichier des cartes en opposition, etc., comme cela existe sur notre serveur de paiement de production.

Bien sûr, aucun paiement accepté par notre serveur de paiement de test ne donne lieu à une mise en recouvrement.

Afin de tester les différents codes de retour du serveur Monetico, vous avez la possibilité d'utiliser plusieurs cartes de tests dont les autorisations sont différentes :

Numéro de carte	Autorisation
0000 0100 0000 0001	**Carte non enrôlée 3D-Secure avec autorisation refusée**
0000 0100 0000 0002	**Carte non enrôlée 3D-Secure avec autorisation approuvée**
0000 0100 0000 0003	**Carte non enrôlée 3D-Secure avec appel phonie**
0000 0100 0000 0004	**Carte enrôlée 3D-Secure non authentifiée avec autorisation refusée**
0000 0100 0000 0005	**Carte enrôlée 3D-Secure authentifiée avec autorisation approuvée**
0000 0100 0000 0006	**Carte enrôlée 3D-Secure authentifiée avec autorisation refusée**

L'environnement de test est disponible à l'adresse suivante :

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

7.2 En Production

Après avoir validé vos développements, vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

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

Nous attirons votre attention sur le fait que les requêtes de paiement adressées au serveur de production seront des paiements réels.

.

7.3 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 dans le système d'information commerçant.

8 Aides à l'installation

8.1 Les problèmes les plus fréquents

8.1.1 Problème de calcul du sceau de sécurité

Message d'erreur

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
- le code langue est incorrect ou inexistant

Résolution du problème

Suivez scrupuleusement le cheminement décrit ci-dessous ; à la fin de chaque étape pour laquelle 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. Ces variables sont : TPE, date, montant, reference, texte-libre, version, lgue, societe, MAC, mail, nbrech, dateech1, montantech1, dateech2, montantech2, dateech3, montantech3, dateech4, montantech4, numero_carte, annee_validite, mois_validite, et cvx

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

- la valeur 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/AA:HH:MM:SS ?
- la valeur de la variable référence 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 ('_') ?

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

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

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

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 :

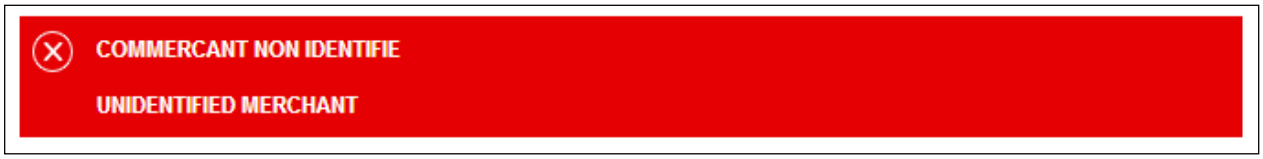
- vous devez utiliser la dernière clé qui vous a été fournie par nos services,
- vérifiez que la clé correspond à votre algorithme de calcul de sceau (SHA1 ou MD5),
- Contactez notre service de support et demandez-leur de valider avec vous que vous utilisez bien la bonne clé

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 utilisés 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.

8.1.2 Le commerçant ne peut pas être identifié

Message d'erreur



Causes possibles

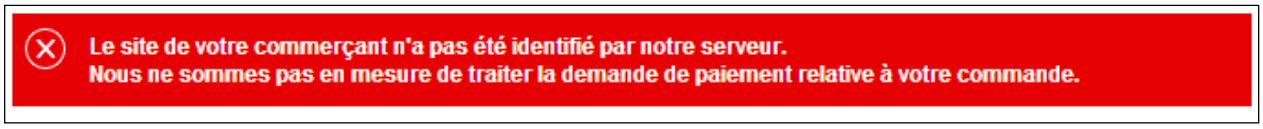
- le numéro de TPE est incorrect ou inexistant

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.

8.1.3 Le site de votre commerçant n'a pas été identifié

Message d'erreur



Causes possibles

- le code société est incorrect ou inexistant

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.

FIN DU DOCUMENT