Monetico Paiement

Paiement sécurisé sur Internet

Documentation Technique

EURO INFORMATION

SOMMAIRE

1 Mise en place de l'interface de paiement

1.1 Introduction

L'intégration de la plate-forme de paiement Monetico Paiement dans la cinématique de paiement par carte de paiement sur votre site consiste à mettre en œuvre deux interfaces dans votre système d'information :

- Interface « Aller » : génération d'un formulaire de demande de paiement, sécurisé par un sceau, qui accompagnera votre client lorsque vous le redirigez sur notre plate-forme de paiement
- Interface « Retour » : réception de la confirmation du paiement que nous envoyons après chaque demande de paiement

Le travail à réaliser 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 RFC2104 implémentant le HMAC SHA1
- 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.

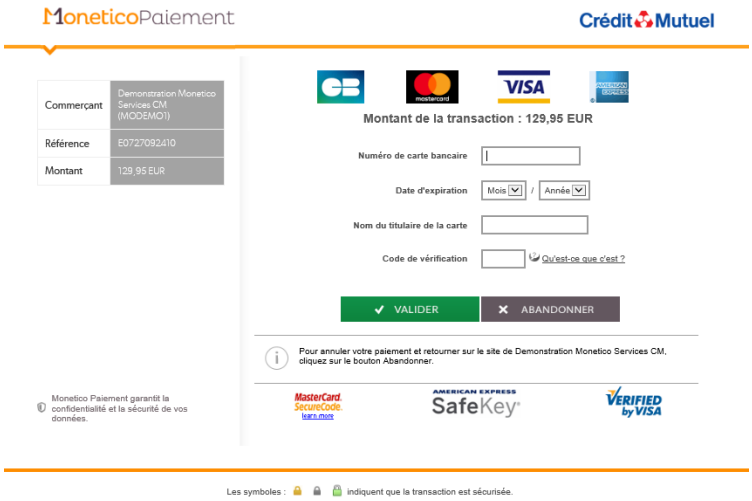
A titre d'information, des exemples de ces deux interfaces vous sont fournis avec la documentation, dans les langages de programmation les plus courants (PHP, C#.NET, Python, Ruby, Java et C++).

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.

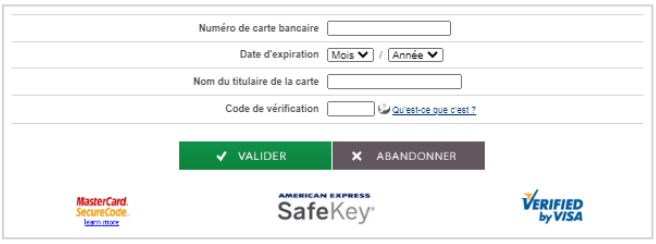
1.2 Modes d'affichage du formulaire de paiement

La page de paiement Monetico Paiement peut être affichée de 2 façons différentes :

- affichage en « page complète » : la page de paiement, à la charte Monetico Paiement, contient l'ensemble des informations liées au paiement (informations concernant le commerçant, le paiement, …).



- affichage en « page épurée » : la page de paiement Monetico Paiement contient uniquement les informations permettant la saisie des informations de cartes de paiement. Cette intégration est à privilégier si vous souhaitez conserver un tunnel de vente unifiée incluant également l'acte de paiement.



1.2.1 Affichage en « page complète »

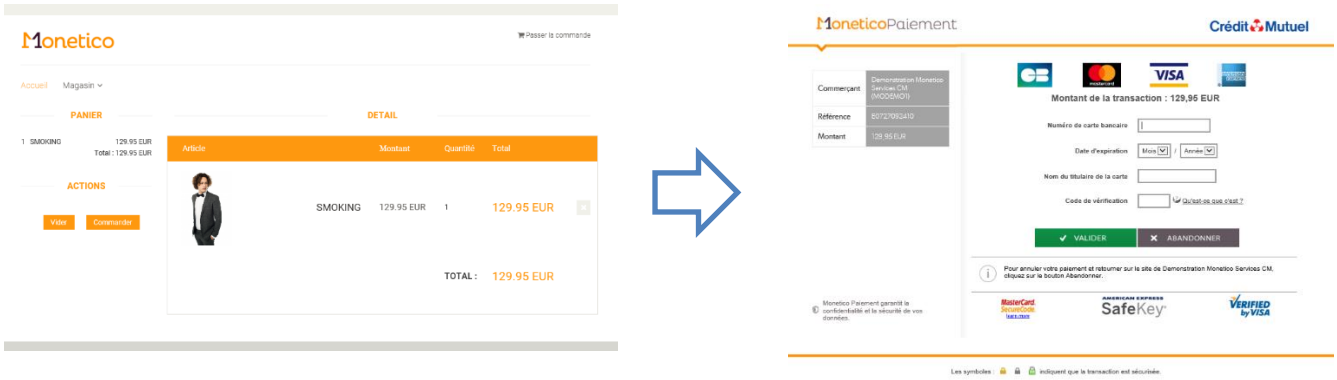
Dans ce mode, la page de paiement Monetico Paiement est affichée avec tous ses éléments :

- une entête et un pied de page avec les logos Monetico Paiement et bancaires
- les détails du paiement
- les réseaux de carte disponibles
- les champs de saisie des informations de carte

L'affichage en page complète est recommandé :

- si vous souhaitez rassurer votre client : les logos Monetico Paiement et de la banque sont visibles. L'URL sécurisée est également un élément de réassurance.
- si vous préférez une séparation claire entre votre site web et la page de paiement

Ci-dessous un exemple d'intégration en mode page complète : à la fin du processus de commande, votre client est redirigé vers la page de paiement Monetico Paiement afin de payer.



1.2.2 Affichage en « page épurée »

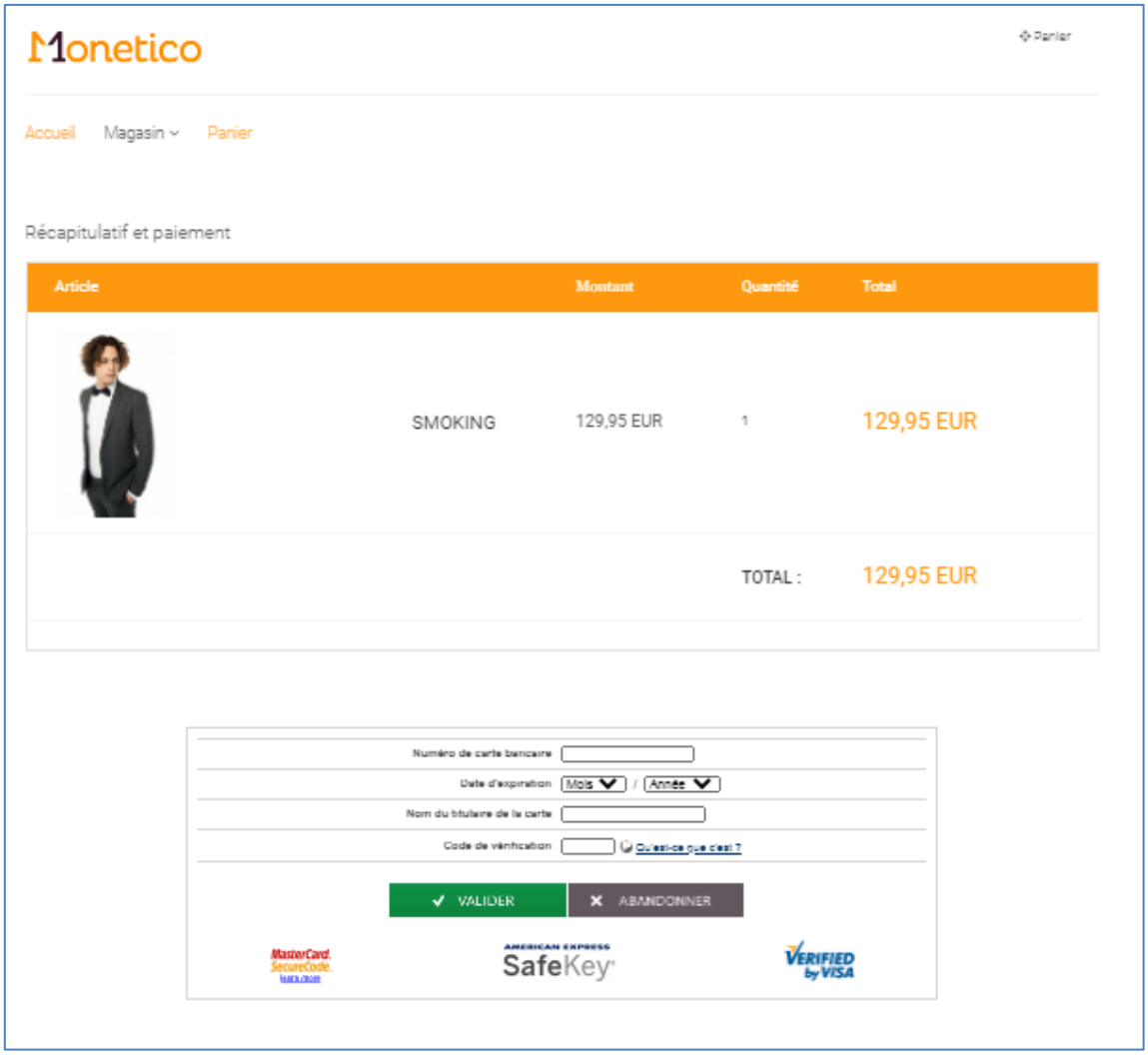
Dans ce mode, la page de paiement Monetico Paiement est affichée avec le minimum d'éléments requis :

- les champs de saisie des informations de carte

Ce mode est recommandé :

- si le processus de paiement est intégré à votre site web ou application mobile de manière à proposer un parcours homogène et court

Ci-dessous un exemple d'intégration en mode page épurée : votre client reste sur votre site mais saisit des informations de carte de paiement directement sur le formulaire sécurisée Monetico Paiement.



Au cours du processus de paiement, lorsqu'une nouvelle page doit être affichée (processus 3DSecure ou résultat du paiement), vous pouvez choisir le comportement de la page de paiement Monetico Paiement :

- la nouvelle page est affichée dans une page différente : votre client quitte votre site web ou votre application mobile
- la nouvelle page est affichée dans la zone réservée de votre site web (iframe) ou de votre application mobile (webview)

Ce comportement doit être choisi au moment de la configuration de l'option page épurée.

1.2.3 Personnalisation du formulaire de paiement Monetico Paiement

Quel que soit le mode d'affichage choisi, des options de personnalisation des éléments graphiques (couleurs des bordures, couleurs de fond, couleurs de polices, logos, bandeaux, boutons …) sont disponibles afin que le parcours d'achat soit visuellement le plus homogène possible.

Vous trouverez plus de détail sur la personnalisation de la page de paiement sur le site de Monetico Paiement dédiée (https://www.monetico-paiement.fr/fr/piloter-suivre/parametrage/page-de-paiement.html).

1.3 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 Monetico Paiement, est indispensable pour utiliser le service de paiement par carte de paiement. 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.

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).

1.4 Spécifications des messages échangés

1.4.1 Rappel de la cinématique

Action	Intervenant
Le serveur commerçant obtient l'accord de l'internaute sur sa commande	**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 …	
… accède au serveur de paiement (par une redirection depuis le site du marchand ou sans quitter la page du marchand)	**Serveur de paiement de Monetico Paiement**
Le serveur Monetico Paiement vérifie la validité du sceau et entame le dialogue de paiement avec l'internaute	
L'internaute dialogue avec le serveur Monetico Paiement et paye (ou ne paye pas) par carte de paiement	
Le serveur Monetico Paiement 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 de paiement	
Le serveur affiche à l'internaute le résultat du paiement[1]	**Serveur de paiement de Monetico Paiement**
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 Monetico Paiement 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.

1.4.2 Interface « Aller »

1.4.2.1 Différentes intégrations de la page de paiement

1.4.2.1.1 Intégration avec redirection vers une nouvelle page

Le formulaire de paiement doit être implémenté à l'aide d'une balise HTML « form » au sein du site web :

```
<form method="post" name="Nom" target="_top" action="https://p.monetico-services.com/paiement.cgi">
    <input type="hidden" name="parametre1" value="value1">
    …
</form>
```

La valeur du champ name ci-dessus est un exemple sans influence sur le comportement de l'application.

1.4.2.1.2 Intégration directe dans le site commerçant

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

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

Les valeurs des champs id et name ci-dessus 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

Remarque : comme spécifié dans le paragraphe 1.4.2.3 Informations propres au mode d'intégration « page épurée », le mode d'affichage doit être positionné à « iframe ».

1.4.2.2 Paramètres acceptés par la page de paiement

Les paramètres du terminal et les données de la commande sont regroupées en un formulaire HTML scellé afin de transmettre la demande de paiement au serveur Monetico Paiement via le navigateur du client.

Utilisez uniquement les champs cités dans ce paragraphe 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.

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. Ces informations sont uniquement affichées sur votre environnement de test dit « sandbox » (9.8.1).

Les champs obligatoires doivent tous être fournis lors de l'appel et doivent respecter les contraintes techniques listées ci-dessous.
Les champs facultatifs peuvent

1. Ne pas être fournis
2. Etre fournis vides
3. Ou bien si fournis valorisés, doivent respecter les contraintes listées ci-dessous.

Les champs qu'il est possible de fournir dans le formulaire sont listés ci-dessous.

Champ	**TPE**
Présence	Obligatoire
Description	Numéro de votre TPE virtuel
Format **Valeur(s) possible(s)**	7 caractères alphanumériques [A-Za-z0-9]{7}
Exemple	1234567

Champ	**version**
Présence	Obligatoire
Description	Version du système de paiement utilisée
Format **Valeur(s) possible(s)**	Uniquement la valeur « 3.0 »
Exemple	3.0

Champ	**date**
Présence	Obligatoire
Description	Date de la commande
Format **Valeur(s) possible(s)**	JJ/MM/AAAA:HH:MM:SS
Exemple	24/05/2019:10:00:25

Champ	**montant**
Présence	Obligatoire
Description	Montant TTC de la commande
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR

Champ	**reference**
Présence	Obligatoire
Description	Référence unique de la commande.
Format Valeur(s) possible(s)	^[\x20-\x7E]{1,50}$ Il est conseillé de n'envoyer que 12 caractères alphanumériques afin de conserver cette référence dans le détail la remise sur votre banque à distance.
Exemple	REF7896543

Champ	**lgue**
Présence	Obligatoire
Description	Code langue. Détermine la langue d'affichage de la page de paiement.
Format Valeur(s) possible(s)	Choix parmi : DE EN ES FR IT JA NL PT SV
Exemple	FR

Champ	**MAC**
Présence	Obligatoire
Description	Sceau issu de la certification de données envoyées au système de paiement.
Format Valeur(s) possible(s)	40 caractères hexadécimaux [0-9a-f]{40}
Exemple	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Champ	**contexte_commande**
Présence	Obligatoire
Description	Informations relatives à la commande : détail du panier, adresses d'expédition, de facturation et contexte technique. Description détaillée dans l'annexe 9.5
Format Valeur(s) possible(s)	Données au format JSON - UTF-8 encodées en base 64.

Champ	**societe**
Présence	Obligatoire
Description	Code alphanumérique permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité. Il s'agit de votre code société.
Format Valeur(s) possible(s)	Chaine de caractères générée à la création de votre contrat
Exemple	maSociete

Champ	**texte-libre**
Présence	Optionnelle
Description	Zone de texte libre. Est restituée notamment sur le tableau de bord.
Format Valeur(s) possible(s)	3200 caractères maximum
Exemple	Livraison relais colis rue des tourterelles

Champ	**mail**
Présence	Optionnelle (sauf pour page épurée → iFrame : obligatoire)
Description	Email du client réalisant la transaction, permet au porteur de recevoir son ticket de paiement à l'adresse indiquée. Si non fourni, la redirection automatique n'est pas activée.
Format Valeur(s) possible(s)	255 caractères maximum ^.+@.+\..+$
Exemple	monclient@mondomain.com

Champ	**url_retour_ok**
Présence	Optionnelle Si non fourni, l'URL configurée par défaut sur votre code société sera utilisée.
Format Valeur(s) possible(s)	2048 caractères maximum URL par laquelle l'acheteur revient sur le site du commerçant suite à un paiement accepté
Exemple	http://url.retour.com/ok.cgi?ref=REF001

Champ	url_retour_err
Présence	Optionnelle Si non fourni, l'URL configurée par défaut sur votre code société sera utilisée.
Format Valeur(s) possible(s)	2048 caractères maximum URL par laquelle l'acheteur revient sur le site du commerçant suite à un paiement refusé
Exemple	http://url.retour.com/ko.cgi?ref=REF001

Champ	3dsdebrayable
Présence	Optionnelle
Description	Permet de forcer le débrayage de 3DSecure
Format Valeur(s) possible(s)	0 : pas de débrayage du protocole 3DSecure 1 : débrayage du protocole 3DSecure
Exemple	0

Champ	ThreeDSecureChallenge
Présence	Optionnelle
Description	Souhait commerçant concernant le challenge 3DSecure
Format Valeur(s) possible(s)	« no_preference » : pas de préférence (choix par défaut) « challenge_preferred » : challenge souhaité « challenge_mandated » : challenge requis « no_challenge_requested » : pas de challenge demandé « no_challenge_requested_strong_authentication » : pas de challenge demandé – l'authentification forte du client a déjà été réalisée par le commerçant. « no_challenge_requested_trusted_third_party » : pas de challenge demandé – demande d'exemption car le commerçant est un bénéficiaire de confiance du client. «no_challenge_requested_risk_analysis » : pas de challenge demandé – demande d'exemption TRA (Transaction Risk Analysis). Nécessite une option spécifique sur le contrat du marchand. En cas de demande de séquestration d'une carte, le souhait « challenge_mandated » sera systématiquement utilisé.
Exemple	challenge_preferred

Champ	libelleMonetique
Présence	Optionnelle
Description	Permet, s'il est renseigné, de remplacer la partie « enseigne » dans le libellé du paiement « enseigne*localité » qui apparaît sur le relevé de compte du porteur. **NB :** Le nombre de caractères pris en compte est dépendant de la banque du porteur

Format **Valeur(s) possible(s)**	[A-Z a-z0-9]{1,32}
Exemple	MonCommerce

Champ	**libelleMonetiqueLocalite**
Présence	Optionnelle
Description	Permet, s'il est renseigné, de remplacer la partie « localité » dans le libellé du paiement « enseigne*localité » qui apparaît sur le relevé de compte du porteur. **NB :** Le nombre de caractères pris en compte est dépendant de la banque du porteur
Format **Valeur(s) possible(s)**	*ville**code postal**code pays* • *ville :* [-A-Za-z0-9]+ • *code postal* : [-A-Z a-z0-9]* • *code pays* : [A-Za-z]{3} conformément à la norme ISO 3166-1 alpha-3 Format global attendu : [-A-Za-z0-9]+\[-A-Z a-z0-9]*\[A-Za-z]{3} Longueur maximum attendue : 32 caractères
Exemple	Strasbourg\67000\FRA Strasbourg\\FRA

Champ	**desactivemoyenpaiement**
Présence	Optionnelle
Description	Permet de ne pas afficher un ou plusieurs moyens de paiement alternatifs sur la page de paiement.
Format **Valeur(s) possible(s)**	1euro, 3xcb, 4xcb, paypal, lyfpay, sofort ou giropay.
Exemple	paypal

Champ	**aliascb**
Présence	Optionnelle. Nécessite l'option « paiement express »
Description	Alias de la carte de paiement d'un client
Format **Valeur(s) possible(s)**	De 1 à 64 caractères alphanumériques [a-zA-Z0-9]{1,64}
Exemple	monClientRef001

Champ	**forcesaisiecb**
Présence	Optionnelle. Nécessite la souscription de l'option « paiement express »
Description	Permet de forcer la saisie d'une carte de paiement
Format **Valeur(s) possible(s)**	0 ou 1
Exemple	0

Champ	protocole
Présence	Optionnelle Nécessite la souscription à un moyen de paiement alternatif
Description	Mode de paiement via un partenaire souhaité. 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).
Format Valeur(s) possible(s)	1euro, 3xcb, 4xcb, paypal, lyfpay, sofort ou giropay.
Exemple	lyfpay

1.4.2.3 Informations propres au mode d'intégration « page épurée »

Champ	mode_affichage
Présence	Optionnelle
Description	Permet d'afficher un formulaire de paiement minimal dans une iframe sur les pages du site marchand ou une webview dans l'application mobile Nécessite la souscription à l'option « iframe »
Format Valeur(s) possible(s)	Uniquement la valeur « iframe »
Exemple	iframe

REM : Le champ mail devient obligatoire en mode d'intégration « page épurée ».

1.4.2.4 *Informations propres au paiement fractionné*

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.

Les règles ci-dessous doivent être respectées :

- 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.

Champ	**nbrech**
Présence	Optionnelle en cas de paiement fractionné
Description	Nombre d'échéances pour cette commande
Format **Valeur(s) possible(s)**	2, 3 ou 4.
Exemple	3

Champ	**dateech[N]** (N =1, 2, 3 ou 4)
Présence	Optionnelle en cas de paiement fractionné
Description	Date de la Nième échéance
Format **Valeur(s) possible(s)**	JJ/MM/AAAA
Exemple	24/05/2019
Champ	**montantech[N]** (N =1, 2, 3 ou 4)
Présence	Optionnelle en cas de paiement fractionné
Description	Montant TTC de la Nième échéance
Format **Valeur(s) possible(s)**	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	33.50EUR

1.4.2.5 Informations propres au paiement pré-autorisation

Champ	numero_dossier
Présence	Obligatoire dans le cas du paiement préautorisation
Description	Numéro de dossier
Format Valeur(s) possible(s)	12 caractères alphanumériques maximum
Exemple	20150901PRE1

1.4.2.6 Informations propres aux moyens de paiement COFIDIS

Dans le cadre des paiements Cofidis 3xCB et 4xCB, il est possible d'envoyer des informations concernant le client lors de la demande de paiement afin de pré-remplir le formulaire de demande sur le site partenaire. **Ces valeurs sont à encoder en hexadécimal avant d'être envoyées**.

La liste de ces informations est la suivante :

Champ	civiliteclient
Présence	Optionnelle
Description	Civilité du client.
Format Valeur(s) possible(s)	MR / MME / MLLE
Exemple	MR

Champ	nomclient
Présence	Optionnelle
Description	Nom du client.
Format Valeur(s) possible(s)	(^[a-zA-Záàâäãåçéèêëíìîïñóòôöõúùûüýÿ-]{1,50}$)
Exemple	Dupont

Champ	prenomclient
Présence	Optionnelle
Description	Prénom du client.
Format Valeur(s) possible(s)	(^[a-zA-Záàâäãåçéèêëíìîïñóòôöõúùûüýÿ-]{1,50}$)
Exemple	Thomas

Champ	adresseclient
Présence	Optionnelle
Description	Adresse du client
Format Valeur(s) possible(s)	.{1,100}
Exemple	20 rue des champs

Champ	complementadresseclient
Présence	Optionnelle
Description	Complément d'adresse
Format Valeur(s) possible(s)	.{1,50}
Exemple	Appartement B

Champ	codepostalclient
Présence	Optionnelle
Description	Code postal du client
Format Valeur(s) possible(s)	(^[a-zA-Z0-9]{1,10}$)
Exemple	67200

Champ	villeclient
Présence	Optionnelle
Description	Ville du client
Format Valeur(s) possible(s)	(^[a-zA-Z]{1,50}$)
Exemple	Strasbourg

Champ	paysclient
Présence	Optionnelle
Description	Pays du client
Format Valeur(s) possible(s)	(^[a-zA-Z]{2}$)
Exemple	FR

Champ	telephonefixeclient
Présence	Optionnelle
Description	Numéro de téléphone fixe du client
Format Valeur(s) possible(s)	(^[0-9]{2,20}$)

Exemple	0312345678
Champ	**telephonemobileclient**
Présence	Optionnelle
Description	Numéro de téléphone mobile du client
Format **Valeur(s) possible(s)**	(^[0-9]{2,20}$)
Exemple	0612345678

Champ	**departementnaissanceclient**
Présence	Optionnelle
Description	Département de naissance du client.
Format **Valeur(s) possible(s)**	(^[a-zA-Z]{1,50}$)
Exemple	67

Champ	**datenaissanceclient**
Présence	Optionnelle
Description	Date de naissance du client.
Format **Valeur(s) possible(s)**	(^[A-Za-z0-9]{8}$)
Exemple	19900103

Champ	**prescore**
Présence	Optionnelle
Description	Pré score Cofidis
Format **Valeur(s) possible(s)**	[0-9]
Exemple	1234567

1.4.2.7 Exemple de formulaire de paiement en HTML

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

1.4.2.8 Exemple de formulaire de paiement fractionné en HTML

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

1.4.2.9 Exemple de formulaire de paiement préautorisation en HTML

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

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

```
<form method="post" name="Monetico" target="_top" action="https://p.monetico-services.com/paiement.cgi">
    <input type="hidden" name="version" value="3.0">
    <input type="hidden" name="TPE" value="1234567">
    <input type="hidden" name="date" value="05/06/2019:11:55:23">
    <input type="hidden" name="montant" value="62.73EUR">
    <input type="hidden" name="reference" value=" REF003">
    <input type="hidden" name="numero_dossier" value="20150901PRE1">
    <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
    <input type="hidden" name="url_retour_ok" value="http://url.retour.com/ok.cgi?order_ref= REF003">
    <input type="hidden" name="url_retour_err" value="http://url.retour.com/err.cgi?order_ref= REF003">
    <input type="hidden" name="lgue" value="FR">
    <input type="hidden" name="societe" value="monSite1">
    <input type="hidden" name="texte-libre" value="ExempleTexteLibre">
    <input type="hidden" name="mail" value="internaute@sonemail.fr">
    <input type="hidden" name="civilite" value="4D52">
    <input type="hidden" name="nomclient" value="6C6163686F7563726F757465">
    <input type="hidden" name="prenomclient" value="63657374626F6E">
    <input type="hidden" name="adresseclient" value=" 72756520646573207361756369736573">
    <input type="submit" name="bouton" value="Paiement CB">
</form>
```

1.4.2.11 Calcul du sceau du formulaire

Pour réaliser le calcul du sceau MAC, il faut se reporter à la section dédiée.

1.4.3 Interface « Retour »

Après avoir traité la demande de paiement, le serveur Monetico Paiement informe directement le serveur du commerçant du résultat de la demande de paiement en émettant une requête HTTP(S) on-line, contenant le résultat de la demande de paiement, sur l'URL de confirmation des paiements (interface « Retour »). **Cette URL doit nous être indiquée au moment de la mise en place du système.**

L'interface retour est appelée **après chaque tentative de validation d'un paiement**, 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. 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 paiement), l'interface retour n'est pas appelée.

L'interface de retour dispose de 30 secondes pour répondre comme décrit au chapitre 1.4.3.3, page 35. 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).

Remarque à l'attention des commerçants migrant depuis une ancienne version du calcul du sceau

Les champs décrits ci-dessous ne sont valables que lorsque le sceau envoyé à l'interface « Aller » a été calculé selon la méthode décrite dans ce document. Pour les paiements créés en adéquation avec une version antérieure de cette documentation et du calcul, le retour sera conforme à ce qui y était décrit.

De même, le calcul du sceau à l'interface « Retour » est fait de la même façon que lors de l'interface « Aller » et donc selon l'ancien calcul pour les commandes initialisées avant la transition.

Ceci est notamment important pour les paiements fractionnés, où l'appel à l'interface « Retour » peut avoir lieu plusieurs jours après la réalisation du paiement pour les différentes échéances, laps de temps au cours duquel une migration vers l'utilisation du nouveau calcul de sceau peut avoir eu lieu. Des appels à l'interface retour des deux types pourraient donc coexister.

Pour référence, les champs précédemment renvoyés ainsi que l'ancienne méthode de calcul du sceau MAC pour l'interface « Retour » sont décrits en annexe.

1.4.3.1 Paramètres renvoyés par Monetico Paiement

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

Champ	code-retour
Description	Le résultat du paiement
Format Valeurs possibles	Chaine de caractères payetest : paiement accepté (en « sandbox » uniquement) paiement : paiement accepté (en Production uniquement) annulation : paiement refusé En paiement fractionné, pour les mises en recouvrement automatique des échéances de rang > 1 : paiement_pf[N] : paiement accepté de l'échéance N (N entre 2 et 4) Annulation_pf[N] : paiement refusé définitivement de l'échéance N (N entre 2 et 4)
Complément	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 « sandbox ». Si ce code est présent lors d'un paiement en production, il s'agit d'une anomalie.
Exemple	paiement

Champ	MAC
Description	Sceau issu de la certification de données envoyées au système de paiement.
Format Valeur(s) possible(s)	40 caractères hexadécimaux [A-F]{40}
Exemple	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Champ	TPE
Description	Numéro de votre TPE virtuel
Format Valeur(s) possible(s)	7 caractères alphanumériques [A-Za-z0-9]{7}
Exemple	1234567

Champ	**montant**
Description	Montant TTC de la commande
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR
Complément	Uniquement dans le cas des modes de paiement **HORS** préautorisation

Champ	**montantestime**
Description	Montant TTC estimé de la commande
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR
Complément	Uniquement dans le cas du mode de paiement préautorisation

Champ	**reference**
Description	Référence unique de la commande.
Format Valeur(s) possible(s)	50 caractères alphanumériques maximum
Exemple	REF7896543

Champ	**texte-libre**
Description	Zone de texte libre fournie lors de la phase « Aller »
Format Valeur(s) possible(s)	3200 caractères maximum
Exemple	Livraison relais colis rue des tourterelles

Champ	**date**
Description	Date de la demande d'autorisation de la commande
Format Valeur(s) possible(s)	JJ/MM/AAAA_a_HH:MM:SS
Exemple	24/05/2019_a_10:00:25

Champ	**cvx**
Description	Indique si le cryptogramme visuel a été saisi lors de la transaction.
Format Valeur(s) possible(s)	oui: si le cryptogramme visuel a été saisi non: sinon
Exemple	oui

Champ	**vld**
Description	Date de validité de la carte de paiement utilisée pour effectuer le paiement
Format Valeur(s) possible(s)	MMAA
Exemple	1019

Champ	**brand**
Description	Code réseau de la carte sur 2 positions alphabétiques parmi.
Format Valeur(s) possible(s)	AM American Express CB GIE CB MC Mastercard VI Visa na Non disponible
Complément	La valeur « na » est systématiquement retournée dans l'environnement de test
Exemple	VI

Champ	**numauto**
Description	Numéro d'autorisation tel que fourni par la banque émettrice.
Format Valeur(s) possible(s)	Chaine de caractère
Complément	Uniquement dans le cas où l'autorisation a été accordée
Exemple	000002

Champ	**authentification**
Description	Document JSON/UTF-8 encodé en base 64 contenant les informations liées à l'authentification du client notamment pour 3DSecure.
Complément	Lien vers la structure du document.

Champ	**usage**
Description	Précise le type de carte utilisée pour réaliser la transaction
Format **Valeur(s) possible(s)**	credit : carte de crédit ou à débit différé debit : carte de débit prepaye : carte prépayée inconnu : impossible de déterminer le type de carte
Exemple	credit

Champ	**typecompte**
Description	Précise le type de compte associé à la carte de paiement
Format **Valeur(s) possible(s)**	particulier : compte d'un particulier commercial : compte d'un professionnel inconnu : impossible de déterminer le type de compte
Exemple	particulier

Champ	**ecard**
Description	Explicite si la carte utilisée pour le paiement est virtuelle ou non
Format **Valeur(s) possible(s)**	oui non
Exemple	oui

Champ	**motifrefus**
Description	Motif du refus de la demande de paiement
Format **Valeur(s) possible(s)**	**Appel Phonie** : la banque du client demande des informations complémentaires **Refus** : la banque du commerçant ou du client refuse d'accorder l'autorisation **Interdit** : la banque du commerçant ou 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 la banque du porteur
Complément	Uniquement dans le cas où la demande de paiement a été refusée

Champ	**motifrefusautorisation**
Description	Motif du refus détaillé de la demande d'autorisation
Format **Valeur(s) possible(s)**	**Refus banque** : la banque du client ou du commerçant refuse d'accorder l'autorisation **Refus emetteur** : la banque du client refuse d'accorder l'autorisation

	Refus critique : la banque du client refuse d'accorder l'autorisation. Contrairement au « Refus banque » et au « Refus emetteur » ce refus est définitif. **Refus repli VADS** : la banque du client refuse d'accorder l'autorisation et requiert une authentification du client. **Refus temporaire** : la demande d'autorisation a été refusée mais pourrait être retentée. **Refus technique** : la demande d'autorisation a été refusée en raison d'un problème technique. **Refus autres** : autre motifs de refus. **Refus test** : simulation d'un test de refus d'autorisation en environnement de validation.
Complément	Uniquement dans le cas où la demande d'autorisation a été refusée

Champ	**originecb**
Description	Code pays de la banque émettrice de la carte de paiement
Format **Valeur(s) possible(s)**	Norme ISO 3166-1
Complément	Uniquement en cas de souscription du module prévention fraude

Champ	**bincb**
Description	Code BIN de la banque du porteur de la carte de paiement
Format **Valeur(s) possible(s)**	Le format dépend de la longueur du numéro de carte : - 8 chiffres pour les numéros de cartes ayant une longueur de 16 chiffres ou plus - 6 chiffres suivis de 2 caractères 'X' pour les numéros de carte ayant une longueur de moins de 16 chiffres
Exemple	12345678 123456XX
Complément	Uniquement en cas de souscription du module prévention fraude

Champ	**hpancb**
Description	Hachage irréversible (HMAC-SHA1) du numéro de la carte de paiement utilisée pour effectuer le paiement (identifiant de manière unique une carte de paiement pour un commerçant donné)
Complément	Uniquement en cas de souscription du module prévention fraude

Champ	**ipclient**
Description	Adresse IP du client ayant fait la transaction
Complément	Uniquement en cas de souscription du module prévention fraude

Champ	**originetr**
Description	Code pays de l'origine de la transaction
Format	Norme ISO 3166-1

Complément	Uniquement en cas de souscription du module prévention fraude

Champ	**montantech**
Description	Montant de l'échéance en cours
Complément	Uniquement dans le cas du paiement fractionné

Champ	**numero_dossier**
Description	Numéro de dossier pour les TPE en pré autorisation
Format **Valeur(s) possible(s)**	12 caractères alphanumériques maximum
Exemple	20150901PRE1

Champ	**typefacture**
Description	Type de facture à générer pour les TPE en pré autorisation
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format **Valeur(s) possible(s)**	preauto

Champ	**filtragecause**
Description :	Numéros des types de filtres bloquant le paiement (cf. tableau « Retours Module Prévention Fraude – détails » ci-dessous)
Format **Valeur(s) possible(s)**	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 : Email jetable 8 : Limitation en montant pour une CB sur une période donnée 9 : Limitation en nombre de transactions pour une CB 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 CB
Complément	Uniquement dans le cas d'un filtrage du paiement ou si le mode information est activé. Si plusieurs filtres bloquent le paiement, ceux-ci sont séparés par des tirets. Les causes et les valeurs correspondantes étant dans le même ordre.

Champ	filtragevaleur
Description	Données ayant engendré le blocage
Complément	Uniquement dans le cas d'un filtrage du paiement ou si le mode information est activé. Si plusieurs filtres bloquent le paiement, ceux-ci sont séparés par des tirets. Les causes et les valeurs correspondantes étant dans le même ordre.

Champ	filtrage_etat
Description	Indique, s'il est présent uniquement, que le filtrage est en mode « information ». information : Mode information du filtrage
Complément	Uniquement dans le cas d'un filtrage du paiement ou si le mode information est activé. Si plusieurs filtres bloquent le paiement, ceux-ci sont séparés par des tirets. Les causes et les valeurs correspondantes étant dans le même ordre.

Champ	cbenregistree
Description	Booléen indiquant si la carte a été enregistrée sous un aliascb donné
Format Valeur(s) possible(s)	1 : Le client a saisi une carte de paiement et elle a été enregistrée sous l'aliascb envoyé 0 : Tous les autres cas
Complément	Uniquement en cas de souscription de l'option paiement express

Champ	cbmasquee
Description	Le numéro de carte tronqué en conformité avec PCI DSS
Format Valeur(s) possible(s)	Le format dépend de la longueur du numéro de carte : - 8 premiers et 2 derniers chiffres de la carte de paiement du client, séparés par des étoiles pour les numéros de carte ayant une longueur de 16 chiffres ou plus - 6 premiers chiffres, 6 étoiles, le reste des chiffres de la carte de paiement du client pour les numéros de carte ayant une longueur de moins de 16 chiffres
Exemple	12345678******12 123456******123
Complément	Présent systématiquement pour les paiements par carte. Absent pour les paiements sans saisie de carte sur la page Monetico Paiement (Paypal …)

Champ	modepaiement
Description	Moyen de paiement utilisé
Format Valeur(s) possible(s)	CB, paypal, 1euro, 3xcb, 4xcb, lyfpay, sofort ou giropay
Complément	Dans le cas d'un paiement à l'aide du wallet ApplePay, la valeur sera CB et la paramètre « wallet » indiquera le nom du wallet

Champ	**wallet**
Description	Nom du wallet utilisé pour le paiement, uniquement dans le cas d'un paiement ApplePay
Format **Valeur(s) possible(s)**	applepay

Champ	**statutDebrayageAuthentification**
Description :	Indique le statut de débrayage de l'authentification du porteur
Format **Valeur(s) possible(s)**	0 : débrayage non demandé 1 : débrayage accordé -1 : débrayage non accordé en raison du type de carte de paiement -2 : débrayage non accordé en raison des options du paiement
Complément	Uniquement si les options de débrayage par montant ou formulaires sont activées.

Champ	**nomcartesequestree**
Description :	Nom qui a été assigné à la carte de paiement et qui sera visible par exemple lors de la consultation du wallet par le client
Format **Valeur(s) possible(s)**	[0-9A-Za-z_,\.\-]{1,20}
Complément	Uniquement si un nom a été associé à la carte lors de son enregistrement

Retours Module Prévention Fraude – Détails

La fonctionnalité de filtrage des paiements s'appuie sur un ensemble de neuf filtres, librement paramétrables sur le tableau de bord (nouvelle version). Chacun de ces filtres agit sur un critère spécifique, comme l'adresse IP du client, son adresse email, le pays de sa carte de paiement…

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	Email jetable	Nom de domaine de l'adresse email du client	
8	Limitation en montant pour une CB sur une période donnée	Montant cumulé en euros (€) 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 CB sur une période donnée	Nombre de transactions cumulées sur la période donnée associée 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 associée 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 euros (€) sur la période donnée associé à l'alias du client	
13	Limitation en montant par IP sur une période donnée	Montant cumulé en euros (€) 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 associée à l'adresse IP du client	
15	Testeurs de cartes	Nombre de transactions cumulées sur la période donnée associée à l'adresse IP du client	
16	Limitation en nombre d'alias par CB	Les alias déjà associés à la carte utilisée pour le paiement	Uniquement en cas de souscription de l'option paiement express

Exemple de données envoyées par le serveur Monetico Paiement à l'interface « Retour » pour un paiement immédiat, différé, partiel ou récurrent :

TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1208&brand=VI&
&numauto=010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbmasquee=12345678******90&modepaiement=CB&authentification=ewoJIn(…)KfQo=

Exemple de données envoyées par le serveur Monetico Paiement à l'interface « Retour » pour la première échéance d'un paiement fractionné :

TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1208&brand=VI&
numauto=010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&

montantech=20EUR&cbmasquee=12345678******90&modepaiement=CB&authentification=ewoJIn(…)KfQo=

Exemple de données envoyées par le serveur Monetico Paiement à l'interface « Retour » pour un blocage d'un paiement immédiat par le MPF:

TPE=1234567&date=05%2f10%2f2011%5fa%5f15%3a33%3a06&montant=1%2e01EUR&reference=P1317821466&MAC=70156D2CFF27A9B8AAE5AFEBE590D9CFCAAF9BDC&texte-libre=Ceci+est+un+test%2c+ne+pas+tenir+compte%2e&code-retour=Annulation&cvx=oui&vld=0912&brand=MC&motifrefus=filtrage&motifrefusautorisation=-&originecb=FRA&bincb=12345678&hpancb=764AD24CFABBB818E8A7DC61D4D6B4B89EA837ED&ipclient=10%2e45%2e166%2e76&originetr=inconnue&filtragecause=4-&filtragevaleur=FRA-&cbmasquee=12345678******90&modepaiement=CB&authentification=bnVsbAo=

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

TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1208&brand=VI&numauto=010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbenregistree=1&nomcartesequestree=VISA%20CIC&cbmasquee=12345678******90&modepaiement=CB&authentification=ewoJIn(…)KfQo=

1.4.3.2 Validation du sceau

Le message de confirmation reçu est scellé par un **sceau MAC** qui a été calculé par le serveur de paiement Monetico Paiement 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**, se référer à la documentation en annexe.

1.4.3.2.1 Spécificités pour les paiements fractionnés

Notamment, les appels à l'interface retour pour les échéances des paiements fractionnés seront tous scellés avec la méthode de calcul utilisée lors de la création du paiement ; il convient donc de prévoir un mécanisme de repli gérant l'ancien calcul du sceau pour les paiements fractionnés réalisés avant votre implémentation de la méthode décrite dans ce document pour lesquels nous réaliserions un appel à votre interface retour.

1.4.3.3 Création de l'accusé de réception

La réponse renvoyée par l'interface « Retour » au serveur de paiement Monetico Paiement 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 Monetico Paiement 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 Monetico Paiement, 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 l'adresse d'une boîte aux lettres électronique régulièrement relevée. Pour passer en production, le serveur commerçant doit avoir renvoyé un accusé de réception avec un sceau validé pour les trois derniers tests.

2 Demander la mise en recouvrement d'une demande de paiement

2.1 Présentation

Le but du service « capture_paiement » est de permettre aux commerçants de mettre en recouvrement, par requête informatique et de manière sécurisée, les paiements qui ont été préalablement autorisés.

Ce service peut être utilisé avec les modes de paiement suivants :

- paiement différé
- paiement partiel
- paiement fractionné (pour la première échéance uniquement)
- paiement récurrent (selon la configuration choisie)

Pour demander une mise en recouvrement, l'application du commerçant doit faire appel au service web de capture du serveur Monetico Paiement (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 Monetico Paiement retourne le résultat de la demande de capture à l'application du commerçant : capture acceptée ou capture refusée.

2.2 Appel au service de demande de capture

2.2.1 Les informations à fournir

L'application du commerçant doit émettre une requête en méthode POST par un message HTTPS, en utilisant le protocole de sécurisation des échanges TLS V1.2 uniquement, à destination du service « capture_paiement » sur les serveurs de Monetico Paiement, contenant les champs suivants :

Champ	**TPE**
Présence	Obligatoire
Description	Numéro de votre TPE virtuel
Format Valeur(s) possible(s)	7 caractères alphanumériques [A-Za-z0-9]{7}
Exemple	1234567

Champ	**version**
Présence	Obligatoire
Description	Version du système de paiement utilisée
Format Valeur(s) possible(s)	Uniquement la valeur « 3.0 »
Exemple	3.0

Champ	**date**
Présence	Obligatoire
Description	Date et heure de la demande de capture
Format Valeur(s) possible(s)	JJ/MM/AAAA:HH:MM:SS
Exemple	24/05/2019:10:00:25

Champ	**date_commande**
Présence	Obligatoire
Description	Date de la commande au format
Format Valeur(s) possible(s)	JJ/MM/AAAA
Exemple	24/05/2019

Champ	**montant**
Présence	Obligatoire
Description	Montant TTC de la commande initiale
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR

Champ	**montant_a_capturer**
Présence	Obligatoire
Description	Montant TTC de la demande de capture
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR

Champ	**montant_deja_capture**
Présence	Obligatoire
Description	Montant TTC correspondant au montant déjà capturé sur cette commande
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR

Champ	**montant_restant**
Présence	Obligatoire
Description	Montant TTC correspondant au solde de la commande après la capture présentement demandée
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR

Champ	**reference**
Présence	Obligatoire
Description	Référence de la commande.
Format Valeur(s) possible(s)	50 caractères alphanumériques maximum [a-zA-Z0-9]{1,50}
Exemple	REF7896543

Champ	**lgue**
Présence	Obligatoire
Description	Code langue en majuscule
Format Valeur(s) possible(s)	DE EN ES FR IT JA NL PT SV [A-Z]{2}
Exemple	FR

Champ	**societe**
Présence	Obligatoire
Description	Code alphanumérique permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité
Format Valeur(s) possible(s)	Alphanumérique
Exemple	maSociete

Champ	**MAC**
Présence	Obligatoire
Description	Sceau issu de la certification de données envoyées au système de paiement.
Format Valeur(s) possible(s)	40 caractères hexadécimaux [A-Fa-f]{40}
Exemple	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Champ	**stoprecurrence**
Présence	Optionnelle
Description	Force la fin de la récurrence pour les TPE en paiement récurrent.
Format Valeur(s) possible(s)	oui : stopper la récurrence
Exemple	oui

Champ	**numero_dossier**
Présence	Optionnelle
Description	Numéro de dossier pré autorisation
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format Valeur(s) possible(s)	12 caractères alphanumériques
Exemple	20150901PRE1

Champ	**facture**
Présence	Optionnelle
Description	Type de facture à générer
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format Valeur(s) possible(s)	preauto noshow
Exemple	noshow

Champ	**phonie**
Présence	Optionnelle
Description	La valeur de ce champ sera renvoyée en cas d'appel phonie
Format Valeur(s) possible(s)	oui

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.

Remarque : Il est possible qu'une demande d'autorisation soit refusée pour un motif du type « appel phonie » (montant trop élevé, centre d'autorisation encombré, etc.).
Il peut alors être nécessaire pour le commerçant de faire une demande manuelle (téléphone, fax) au centre d'autorisation du porteur de la carte, qui communiquera en retour des coordonnées bancaires et du montant, un numéro d'autorisation pour cette transaction.

2.2.2 Calcul du sceau

Pour réaliser le calcul du sceau MAC, il faut se reporter à la section dédiée.

2.2.3 Exemples de requête de capture

Exemple 1 : recouvrement partiel de 62€ pour une commande initiale de 100€

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

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

Cette capture ne peut s'effectuer que si votre TPE est configuré en Paiement Partiel, Paiement Récurrent ou Paiement Fractionné et que la première échéance est de 62.00EUR. En cas de succès, une capture ultérieure d'un montant de 38€ est encore réalisable.

Exemple 2 : recouvrement total d'une commande de 100€

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

Les 2 montants doivent être identiques

Cette capture peut s'effectuer si votre TPE est configuré en Paiement Partiel, en Paiement Récurrent ou en Paiement Différé. En cas de succès, aucune capture ultérieure n'est réalisable.

2.3 Réponse de la demande de capture

2.3.1 Les informations retournées

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

Il contient les champs suivants séparés par un caractère CHR(10) qui correspond à un saut de ligne.

Champ	**cdr**
Description	Code retour indiquant le résultat de la capture
Format **Valeur(s) possible(s)**	1 : capture acceptée 0 : capture refusée -1 : erreur

Champ	**lib**
Description	Libellé détaillé précisant la nature du code retour
Format **Valeur(s) possible(s)**	Voir ci-dessous pour la liste des libellés possibles

Champ	**version**
Description	Numéro de version du message d'acquittement
Format **Valeur(s) possible(s)**	Uniquement « 1.0 »

Champ	**reference**
Description	Référence de la commande

Champ	**aut**
Description	Numéro d'autorisation du paiement si celui-ci a été accepté

Champ	**phonie**
Description	Autorisation refusée pour un motif du type « appel phonie »
Complément	Ce champ n'est présent que si le champ « phonie » était présent et renseigné dans la requête appelante

Champ	**montant_estime**
Description	Montant initial de la demande de pré autorisation
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	62.73EUR

Champ	**date_autorisation**
Description	Date à laquelle la facture a été pré autorisée
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format	AAAA-MM-JJ
Exemple	2019-06-26

Champ	**montant_debite**
Description	Montant effectivement recouvré lors de la facture
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	62.73EUR

Champ	**date_debit**
Description	Date à laquelle le recouvrement a été effectué
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format	AAAA-MM-JJ
Exemple	2019-06-26

Champ	**numero_dossier**
Description	Numéro du dossier qui vient d'être recouvré
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format Valeur(s) possible(s)	12 caractères alphanumériques maximum
Exemple	20150901PRE1

Champ	type_facture
Description	Type de la facture qui vient d'être réalisée
Format Valeur(s) possible(s)	preauto noshow
Exemple	noshow

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

cdr	lib	description	remarque
1	**paiement accepte**	L'autorisation de paiement a été délivrée et la mise en recouvrement 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 (3 tentatives sont acceptées)	**La commande n'est plus acceptée par le serveur bancaire**
0	**autorisation refusee**	L'autorisation bancaire n'a pas été délivrée	**La capture n'est pas effectuée**
0	**annulation refusee**	L'annulation de l'autorisation a été refusée	**L'annulation n'est pas effectuée**
0	**la commande est deja annulee**	La commande a été annulée lors d'une précédente capture	**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 immédiat, car le recouvrement est fait 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	**Réitérer la demande**
-1	**indisponibilite temporaire du service**	Service non disponible lors des opérations de maintenance en HNO	**Réitérer la demande en fin de maintenance**
-1	**probleme technique**	Un problème technique est survenu	**Réitérer la demande**

2.3.2 Spécificité du mode de paiement pré autorisation

Il n'est possible de réaliser qu'une seule capture de la demande initiale, partielle ou totale.

2.3.3 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 annulation de récurrence
  version=1.0
  reference=000000000145
  cdr=1
  lib=recurrence stoppee
  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 capture 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

- Cas d'une capture acceptée en pré autorisation

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

- Cas d'une annulation acceptée en pré autorisation

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

3 Demander une annulation de paiement/de récurrence

3.1 Annulation de paiement

Dans le cas où le commerçant a demandé un paiement et qu'il ne souhaite pas le mettre en recouvrement (marchandise non disponible, client qui s'est rétracté, etc.), il peut notifier le serveur Monetico Paiement 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 capturer et le montant restant à 0EUR.

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

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

Les champs « montant_a_capturer » et « montant_restant » doivent être égaux à 0

Le champ « montant_deja_capture » doit correspondre à l'historique de la commande

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

3.2 Annulation de récurrence

Si le commerçant ne souhaite pas poursuivre les renouvellements automatiques d'un abonnement, il peut notifier le serveur Monetico Paiement de l'abandon de la récurrence du paiement.

Pour cela, il appellera le service de capture comme décrit dans le chapitre précédent, en spécifiant le montant à capturer et le montant restant à 0EUR et le champ « stoprecurrence » à OUI.

Exemple : annuler la récurrence d'une commande d'un montant initial.

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: 318

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

Les champs « montant_a_capturer » et « montant_restant » doivent être égaux à 0

Le champ « montant_deja_capture » doit correspondre à l'historique de la commande

Cette capture peut s'effectuer si le TPE est configuré en Paiement Récurrent. En cas de succès, la commande ne sera plus renouvelée.

4 Demander une facture complémentaire pour la préautorisation

La demande de facture complémentaire une fois le paiement recouvré s'effectue via le service d'émulation 3DSecure.

Pour plus de détails, se référer à la documentation technique de ce service.

5 Le service de remboursement (recrédit)

5.1 Présentation

Le but du service « recredit_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 de Monetico Paiement (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 Monetico Paiement 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, en utilisant le protocole de sécurisation des échanges TLS V1.2 uniquement, à destination du service « recredit_paiement» sur les serveurs de Monetico Paiement, contenant les champs suivants :

Champ	**TPE**
Présence	Obligatoire
Description	Numéro de votre TPE virtuel
Format Valeur(s) possible(s)	7 caractères alphanumériques [A-Za-z0-9]{7}
Exemple	1234567

Champ	**version**
Présence	Obligatoire
Description	Version du système de paiement utilisée
Format Valeur(s) possible(s)	Uniquement la valeur « 3.0 »
Exemple	3.0

Champ	**date**
Présence	Obligatoire
Description	Date et heure de la demande de recrédit
Format Valeur(s) possible(s)	JJ/MM/AAAA:HH:MM:SS
Exemple	24/05/2019:10:00:25

Champ	**date_commande**
Présence	Obligatoire
Description	Date de la commande
Format Valeur(s) possible(s)	JJ/MM/AAAA
Exemple	24/05/2019

Champ	**date_remise**
Présence	Obligatoire
Description	Date à laquelle a eu lieu la mise en recouvrement
Format Valeur(s) possible(s)	JJ/MM/AAAA
Exemple	24/05/2019

Champ	num_autorisation
Présence	Obligatoire
Description	Numéro d'autorisation renvoyé par le serveur de la banque lors de la demande de paiement
Exemple	123456

Champ	montant
Présence	Obligatoire
Description	Montant TTC de la commande initiale
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Exemple	95.25EUR

Champ	montant_recredit
Présence	Obligatoire
Description	Montant TTC à recréditer
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}

Champ	montant_possible
Présence	Obligatoire si le champ **montant_deja_recredite** est absent Optionnel sinon
Description	Montant TTC de recrédit maximum autorisé pour le numéro d'autorisation fourni
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Complément	Si un remboursement a déjà été effectué sur ce numéro d'autorisation, il doit être décompté 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 €.
Exemple	95.25EUR

Champ	**montant_deja_recredite**
Présence	Obligatoire si le champ **montant_possible** est absent Optionnel sinon
Description	Montant TTC des recrédits réussit déjà effectués
Format **Valeur(s) possible(s)**	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Complément	Si des remboursements ont déjà été effectués sur ce numéro d'autorisation, ils doivent être renseignés 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_deja_recredite » de 10 €.
Exemple	95.25EUR

Champ	**reference**
Présence	Obligatoire
Description	Référence de la commande.
Format **Valeur(s) possible(s)**	50 caractères alphanumériques maximum [a-zA-Z0-9]{1,50}
Exemple	REF7896543

Champ	**lgue**
Présence	Obligatoire
Description	Code langue en majuscule
Format **Valeur(s) possible(s)**	DE EN ES FR IT JA NL PT SV [A-Z]{2}
Exemple	FR

Champ	**societe**
Présence	Obligatoire
Description	Code alphanumérique permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité
Format **Valeur(s) possible(s)**	Alphanumérique
Exemple	maSociete

Champ	MAC
Présence	Obligatoire
Description	Sceau issu de la certification de données envoyées au système de paiement.
Format Valeur(s) possible(s)	40 caractères hexadécimaux [A-Fa-f]{40}
Exemple	f97861e0f3e296b7eece2cfd86dc46c43ac88049

Champ	numero_dossier
Présence	Optionnelle
Description	Numéro de dossier pré autorisation
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format Valeur(s) possible(s)	12 caractères alphanumériques
Exemple	20150901PRE1

Champ	facture
Présence	Optionnelle
Description	Type de facture à générer
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format Valeur(s) possible(s)	preauto noshow complementaire
Exemple	noshow

5.2.2 Cas particulier des paiements par carte

Pour les paiements effectués avec une carte, il est possible de ne fournir ni la date de la remise « date_remise » ni le numéro de l'autorisation associé « num_autorisation ». Dans ce cas le remboursement sera effectué sur la commande en entier et il faudra adapter les champs « montant_possible » et « montant_deja_recredite » pour qu'ils correspondent à la commande.

5.2.3 Calcul du sceau

Pour calculer le sceau MAC, se référer à la documentation en annexe.

5.2.4 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 l'assistance technique (voir chapitre 7 Assistance technique) la liste des adresses IP à autoriser, ainsi que le nombre de remboursement quotidiens maximum pour chacune d'entre elles.

5.2.5 Exemple de requête de recrédit

Exemple 1 : recrédit partiel de 32€ sur une commande de 100€

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

En cas de succès, un recrédit d'un montant maximal de 68€ est encore réalisable.

Exemple 2 : recrédit total sur une commande de 100€

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

Exemple 3 : recrédit total sur une commande de 100€ payée par carte

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

5.3 Réponse de la demande de recrédit

5.3.1 Les informations retournées

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

Il contient les champs suivants séparés par un caractère CHR(10) qui correspond à un saut de ligne.

Champ	**cdr**
Description	Code retour indiquant le résultat du recrédit
Format **Valeur(s) possible(s)**	0 : recrédit effectué <0 : erreur

Champ	**lib**
Description	Libellé détaillé précisant la nature du code retour
Format **Valeur(s) possible(s)**	Voir ci-dessous pour la liste des libellés possibles

Champ	**version**
Description	Numéro de version du message d'acquittement
Format **Valeur(s) possible(s)**	Uniquement « 1.0 »

Champ	**reference**
Description	Référence de la commande

Champ	**numero_dossier**
Description	Numéro du dossier qui vient d'être remboursé
Complément	Uniquement dans le cas d'un TPE en pré autorisation
Format **Valeur(s) possible(s)**	12 caractères alphanumériques maximum
Exemple	20150901PRE1

Champ	**type_facture**
Description	Type de la facture qui vient d'être réalisée
Format **Valeur(s) possible(s)**	preauto noshow complementaire
Exemple	noshow

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

cdr	lib	Description	Remarque
0	**recredit effectue**	La demande de recrédit a été prise en compte	
-1	**recredit refuse**	La demande de recrédit 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 recrédits	**Contacter l'assistance technique**
-33	**demande de recredit expiree**	La date de recrédit dépasse le délai autorisé (+/- 24h)	**Vérifier le paramètre date**
-34	**montant de recredit errone**	Le montant à recréditer est incorrect	**Vérifier le paramètre montant_recredit**
-35	**Les montants transmis sont incorrects**	Les montants transmis ne sont pas en phase avec ceux du serveur bancaire	**Vérifier les champs montant_recredit et montant_possible**
-36	**le maximum de recredit a été atteint**	Le nombre maximum de recrédits 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 recrédit 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 recréditer 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**
-45	**verification carte echouee**	L'état de la carte ne permet plus d'opération (carte opposée, volée …)	
-46	**la commande est deja entierement recreditee**	La commande est entièrement recréditée.	**Vérifier la cohérence de la demande (paramètres d'appels) par rapport aux recrédits déjà effectués**
-47	**plusieurs traitements ont ete trouves**	Impossible de déterminer le paiement Cofidis à recréditer en raison de l'absence de la référence Cofidis	**Vérifier le paramètre ref_remise**
-48	**echec du recredit, recredit potentiellement partiel**	Le recrédit PayPal n'a pas réussi entièrement	**Vérifier la cohérence de la demande (paramètres d'appels)**

			par rapport aux recrédits déjà effectués
-49	**AMEX est désactivé pour ce commercant**	Un recredit sur une carte AMEX est effectué alors que l'option AMEX du TPE est désactivée	
-50	**numero d'autorisation et date de remise sont a fournir ensemble**	Il manque le numéro d'autorisation ou la date de remise	**Vérifier les champs num_autorisation et date_remise**
-51	**le recredit global n'est pas permis pour cette commande**	Il n'est pas possible de faire un recrédit global pour cette commande, veuillez fournir le numéro d'autorisation et la date de la remise	**Renseigner les champs num_autorisation et date_remise**
-52	**le montant deja recredite est incorrect**	Le montant déjà recrédité que vous avez fourni ne correspond pas à celui que nous avons calculer	**Vérifier le champ montant_deja_recredite**

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

- Cas d'un recrédit accepté en pré autorisation

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

6 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, Payé, Annulé,
- le format du fichier que vous souhaitez recevoir : CVS 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	Numéro de TPE	
2	Date de la mise en recouvrement	format AAAA-MM-DD
3	Référence de la commande	telle que fournie par le commerçant
4	Etat 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 recouvrement GR : commande annulée suite à 4 tentatives infructueuses PA : le paiement a été autorisé et mis en recouvrement PP : paiement partiel enregistré avec succès et en attente de recouvrement 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 TTC 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 (EUR, USD, GBP, CHF, etc.)

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

9	Numéro d'autorisation tel que fourni par la banque émetteur	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
12	Type de carte	AM : American Express CB : Carte Bancaire 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	
16	Statut 3DS	-1 : la transaction ne s'est pas faite selon le protocole 3DSecure et le risque d'impayé est élevé 1 : la transaction s'est faite selon le protocole 3DS et le risque d'impayé est faible 4 : la transaction s'est faite selon le protocole 3DS et le risque d'impayé est élevé
17	Alias du numéro de la carte	Hachage irréversible (HMAC-SHA1) du numéro de la carte de paiement Uniquement en cas de souscription du module prévention fraude
18	BIN de la carte	Code BIN de la banque du porteur de la carte de paiement Uniquement en cas de souscription du module prévention fraude
19	Origine de la carte	Code pays de la banque émettrice de la carte de paiement suivant la norme ISO 3166-1

		Uniquement en cas de souscription du module prévention fraude
20	Adresse IP du client ayant effectué la transaction	Uniquement en cas de souscription du module prévention fraude
21	Origine de la transaction	Code pays suivant la norme ISO 3166-1 Uniquement en cas de souscription du module prévention fraude

7 Aides à l'installation

7.1 Passer un TPE en production

Vous devez faire une demande auprès de l'assistance technique (voir chapitre 8) pour faire passer votre TPE en production.

Au préalable, il faudra que les trois derniers paiements effectués dans les sept derniers jours en test aient renvoyé un accusé de réception valide (demande d'autorisation acceptée et réponse au CGI2).

7.2 Foire aux questions

Peut-on personnaliser la page de paiement ?

Oui, il est possible au travers d'une option additionnelle à votre contrat de personnaliser le visuel de la page de paiement. Il est possible de changer les couleurs, les images et les boutons.

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 maximum.

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 de paiement. Au-delà de ce délai, toute saisie sera refusée.

Quel est le nombre d'essais pour saisir les numéros de carte de paiement ?

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 simulant les différents scénarios de paiement possibles

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

- Français
- Anglais
- Allemand
- Espagnol
- Italien
- Néerlandais
- Portugais
- Suédois
- Japonais

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 8)

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_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 Monetico Paiement.

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 8)).

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 de paiement qu'il utilise.

Notre serveur va envoyer une notification de refus :

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EU
R&reference=ref0001&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&tex
te-libre=LeTexteLibre&code-
retour=Annulation&cvx=oui&vld=1208&brand=VI&status3ds=1&motifrefus=R
efus&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2C2CADBFC
1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbmasquee=12345
678******90&modepaiement=CB&authentification=ewoJIn(…)KfQo=
```

Le client a la possibilité de refaire une tentative de paiement et il utilise sa seconde carte de paiement 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%2e75EU
R&reference=ref0001&MAC=f4562a2c18d86cfdbaf646016c202e89945841&texte
-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1210&brand=VI&status3ds=1&numauto=010101
&originecb=FRA&bincb=12345678&hpancb=12754C03C22D786E0F2C2CADBFC1C00
A25df6322&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbmasquee=12345678*
*****90&modepaiement=CB&authentification=ewoJIn(…)KfQo=
```

Comment modifier l'échéancier par défaut de mes paiements fractionnés ?

Lorsque votre TPE est en paiement fractionné, il est configuré pour respecter un échéancier par défaut que vous avez défini lors de la souscription de votre contrat.

Vous avez la possibilité de définir un échéancier propre à chaque commande afin de passer outre l'échéancier par défaut de votre TPE.

Cet échéancier doit respecter les contraintes suivantes :

- un nombre d'échéances compris entre 2 et 4 (paramètre nbrech)
- la somme des échéances est égale au montant de la commande (paramètres montantech1, montantech2, montantech3, montantech4)
- les dates d'échéances sont séparées d'une durée d'un mois (paramètres dateech1, dateech2, dateech3, dateech4).

Comment calculer la date de mes échéances ?

Les dates d'échéances doivent être séparées d'une durée d'un mois.

La durée d'un mois ne correspond pas à un nombre de jours précis mais à la durée entre deux mêmes jours d'un mois calendaire ou à défaut au jour le plus proche possible.

Exemples :

Si votre première échéance a pour date le 01/01/2010, la seconde échéance aura pour date le 01/02/2010, la troisième le 01/03/2010 et la quatrième le 01/04/2010.

Si votre première échéance a pour date le 31/01/2010, la seconde échéance aura pour date le 28/02/2010, la troisième le 31/03/2010 et la quatrième le 30/04/2010.

Si votre première échéance a pour date le 30/01/2012, la seconde échéance aura pour date le 29/02/2012, la troisième le 30/03/2012 et la quatrième le 30/04/2012.

Si vous ne respectez pas ce système de calcul pour les dates des échéances, vous obtiendrez le message d'erreur « les données du formulaire sont incorrectes ».

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.

7.3 Les problèmes les plus fréquents

7.3.1 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 des 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 variable **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.

7.3.2 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.

7.3.3 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.

7.3.4 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

7.3.5 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.

7.3.6 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

7.3.7 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.

8 Assistance technique

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

- Par courriel : en écrivant un message à la boîte aux lettres « **Commerce Electronique** »
  - Crédit Mutuel : centrecom@e-i.com
  - CIC : centrecom@e-i.com
- Par téléphone : en appelant le **0820 821 735**

Cependant, Euro Information n'assure pas de support concernant les problématiques d'intégration technique de sa solution de paiement dans le système d'information commerçant.

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 » (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 13 (CR et LF).

9.2 Contrainte d'encodage

Tous les caractères non-ASCII doivent être encodés en UTF-8.

9.3 Calcul du sceau MAC

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 sont structurées :

- sous une forme d'une suite *Nom_champ=Valeur_champ*,
- avec les éléments de la suite séparés par le caractère « * »,
- classés par ordre alphabétique

Le sceau doit prendre en compte tous les paramètres envoyés — valorisés ou non — reconnus par la plateforme, et uniquement ceux-ci.

Lors de la vérification du sceau sur l'interface « Retour », tous les paramètres envoyés sont pris en compte dans le calcul.

Remarque :

L'ordre utilisé est basé sur le code ASCII. Il est en outre sensible à la casse :

- d'abord les chiffres de 0 à 9,
- ensuite les caractères en MAJUSCULES,
- enfin les caractères en minuscules.
- Pour les caractères spéciaux se référer à la table ASCII.

9.3.1 Exemples de chaînes permettant le calcul du sceau

9.3.1.1 Phase « Aller »

a) Contexte commande

Exemple de champ « contexte_commande » :

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

Soit après encodage en base 64 :

ewogICAiYmlsbGluZyI6ewogICAgICAiZmlyc3ROYW1lIjoiSsOpcsOpbXkiLAogICAgICAibGFzdE5hbWUiOiJHcmltbSIsCiAgICAgICJhZGRyZXNzTGluZTEiOiIzIHJ1ZSBkZSBsJ8OpZ2xpc2UiLAogICAgICAiY2l0eSI6Ik9zdGhlaW0iLAogICAgICAicG9zdGFsQ29kZSI6IjY4MTUwIiwKICAgICAgImNvdW50cnkiOiJGUiIKICAgfSwKICAgInNoaXBwaW5nIjp7CiAgICAgICJmaXJzdE5hbWUiOiJKw6lyw6lteSIsCiAgICAgICJsYXN0TmFtZSI6IkdyaW1tIiwKICAgICAgImFkZHJlc3NMaW5lMSI6IjMgcnVlIGRlIGwnw6lnbGlzZSIsCiAgICAgICJjaXR5IjoiT3N0aGVpbSIsCiAgICAgICJwb3N0YWxDb2RlIjoiNjgxNTAiLAogICAgICAiY291bnRyeSI6IkZSIiwKICAgICAgImVtYWlsIjoiamVyZW02OEBob3RtYWlsLmNvbSIsCiAgICAgICJwaG9uZSI6IiszMy02MTIzNDU2NzgiLAogICAgICAic2hpcEluZGljYXRvciI6ImJpbGxpbmdfYWRkcmVzcyIsCiAgICAgICJkZWxpdmVyeVRpbWVmcmFtZSI6InR3b19kYXkiLAogICAgICAiZmlyc3RVc2VEYXRlIjoiMjAxNy0wMS0yNSIsCiAgICAgICJtYXRjaEJpbGxpbmdBZGRyZXNzIjp0cnVlCiAgICAgIH0sCiAgICAgICJjbGllbnQiOnsKICAgICAgImVtYWlsIjoiamVyZW02OEBob3RtYWlsLmNvbSIsCiAgICAgICJtb2JpbGVQaG9uZSI6IiszMy02MTIzNDU2NzgiLAogICAgICAiYmlydGhDaXR5IjoiQ29sbWFyIiwKICAgICAgImJpcnRoU G9zdGFsQ29kZSI6IjY4MDAwIiwKICAgICAgImJpcnRoQ291bnRyeSI6IkZSIiwKICAgICAgImJpcnRoZGF0ZSI6IjE5ODctMDMtMjciCiAgIH0KfQ==

b) *Paiement immédiat*

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

c) *Paiement fractionné*

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

9.3.1.2 Phase retour

Paiement immédiat, différé, partiel ou récurrent avec inscription au module prévention fraude et à l'option 3DSecure

TPE=1234567*authentification=ewoJIn(…)KfQo=*bincb=12345678*brand=VI*cbmasquee=12345678******90*code-retour=paiement*cvx=oui*date=05/12/2006_a_11:55:23*ecard=non*hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45*ipclient=127.0.0.1*modepaiement=CB*montant=62.75EUR*numauto=010101*originecb=FRA*originetr=FRA*reference=ABERTYP00145*texte-libre=LeTexteLibre*typecompte=inconnu*usage=credit*version=3.0*vld=1208

Paiement fractionné avec inscription au module prévention fraude et à l'option 3DSecure

TPE=1234567*authentification=ewoJIn(…)KfQo=*bincb=12345678*brand=VI*cbmasquee=12345678******90*code-retour=paiement*cvx=oui*date=05/12/2006_a_11:55:23*ecard=non*hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45*ipclient=127.0.0.1*modepaiement=CB*montant=62.75EUR*montantech=20EUR*numauto=010101*originecb=FRA*originetr=FRA*reference=ABERTYP00145*texte-libre=LeTexteLibre*typecompte=inconnu*usage=credit*version=3.0*vld=1208

Paiement bloqué par le module prévention fraude avec l'option 3DSecure

TPE=1234567*authentification=bnVsbAo=*bincb=12345678*brand=VI*cbmasquee=12345678******90*code-retour=Annulation*cvx=oui*date=05/12/2006_a_11:55:23*ecard=non*filtragecause=4-*filtragevaleur=FRA-*hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45*ipclient=127.0.0.1*modepaiement=CB*montant=62.75EUR*motifrefus=filtrage*motifrefusautorisation=-*numauto=010101*originecb=FRA*originetr=FRA*reference=ABERTYP00145*texte-libre=LeTexteLibre*typecompte=inconnu*usage=credit*version=3.0*vld=1208

Paiement avec l'option paiement express et inscription au module prévention fraude et à l'option 3DSecure

TPE=1234567*authentification=ewoJIn(…)KfQo=*bincb=12345678*brand=VI*cbenregistree=1*cbmasquee=12345678******90*code-retour=paiement*cvx=oui*date=05/12/2006_a_11:55:23*ecard=non*hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45*ipclient=127.0.0.1*modepaiement=CB*montant=62.75EUR*nomcartesequestree=VISA CIC*numauto=010101*originecb=FRA*originetr=FRA*reference=ABERTYP00145*texte-libre=LeTexteLibre*typecompte=inconnu*usage=credit*version=3.0*vld=1208

9.3.1.3 Service de capture

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

9.3.1.4 Service d'annulation de paiement/récurrence

Annulation de paiement

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

Annulation de récurrence

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

9.3.1.5 Service de remboursement

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

9.4 Ancien appel à l'interface « Retour »

Cette section ne s'adresse qu'aux commerçants effectuant la transition depuis l'ancien calcul de sceau MAC vers le nouveau et devant gérer des appels à l'interface retour pour des commandes créées avant celle-ci. Elle doit être ignorée dans tous les autres cas. Elle décrit les champs retournés et le calcul du sceau les validant, dans le cas d'une version 3.0.

9.4.1 Champs retournés

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 la banque renvoie ici les données telles qu'elles ont été reçues lors de la phase « Aller » du paiement**
montant	Montant TTC 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 (`EUR`, `USD`, `GBP`, `CHF`, etc.)	
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 paiement fractionné, pour les mises en recouvrement automatique des échéances de rang > 1 : `paiement_pf[N]` paiement accepté de l'échéance N (N entre 2 et 4) `Annulation_pf[N]` paiement refusé définitivement de l'échéance N (N entre 2 et 4)	**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 validation. Si ce code est présent lors d'un paiement en production, il s'agit d'une anomalie.**

cvx	oui si le cryptogramme visuel (obligatoire pour les cartes Visa et MasterCard) a été saisi non sinon	
vld	Date de validité de la carte de paiement utilisée pour effectuer le paiement	
brand	Code réseau de la carte sur 2 positions alphabétiques parmi. AM American Express CB GIE CB 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 et le risque d'impayé est élevé 1 : la transaction s'est faite selon le protocole 3DS et le risque d'impayé est faible 4 : la transaction s'est faite selon le protocole 3DS et le risque d'impayé est élevé	
numauto	Numéro d'autorisation tel que fourni par la banque émettrice	**Uniquement dans le cas où l'autorisation a été accordée**

motifrefus	Motif du refus de la demande de paiement : Appel Phonie : la banque du client demande des informations complémentaires Refus : la banque du client refuse d'accorder l'autorisation Interdit : la banque 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 la banque du porteur	**Uniquement dans le cas où la demande de paiement a été refusée.**
originecb	Code pays de la banque émettrice de la carte de paiement (norme ISO 3166-1)	**Uniquement en cas de souscription du module prévention fraude**
bincb	Code BIN de la banque du porteur de la carte de paiement	
hpancb	Hachage irréversible (HMAC-SHA1) du numéro de la carte de paiement utilisée pour effectuer le paiement (identifiant de manière unique une carte de paiement 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	État 3DSecure du VERes	**En cas de souscription du module prévention fraude et de l'option 3Dsecure**
pares	État 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 : Email jetable 8 : Limitation en montant pour une CB sur une période donnée 9 : Limitation en nombre de transactions pour une CB 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 CB	**Uniquement dans le cas d'un filtrage du paiement ou si le mode information est activé. 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 engendré le blocage	
filtrage_etat	Indique, s'il est présent uniquement, que le filtrage est en mode « information ». information : Mode information du filtrage	
cbenregistree	Booléen indiquant si la carte a été enregistrée sous un aliascb donné : 1 : Le client a saisi une carte de paiement et elle a été enregistrée sous l'aliascb envoyé 0 : Tous les autres cas	**Uniquement en cas de souscription de l'option paiement express**

cbmasquee	Le numéro de carte tronqué en conformité avec PCI DSS. Le format dépend de la longueur du numéro de carte : - 8 premiers et 2 derniers chiffres de la carte de paiement du client, séparés par des étoiles pour les numéros de carte ayant une longueur de 16 chiffres ou plus - 6 premiers chiffres, 6 étoiles, le reste des chiffres de la carte de paiement du client pour les numéros de carte ayant une longueur de moins de 16 chiffres	**Uniquement en cas de souscription de l'option paiement express.** **Exemple :** 12345678******90
modepaiement	Moyen de paiement utilisé `CB, paypal, 1euro, 3xcb, 4xcb, lyfpay, sofort ou giropay`	
nomcartesequestree	Nom qui a été assigné à la carte de paiement lors de son enregistrement et qui sera visible par exemple lors de la consultation du wallet par le client	**Uniquement en cas de souscription de l'option paiement express.** **Exemple :** VISA CIC

Retours Module Prévention Fraude – Détails

La fonctionnalité de filtrage des paiements s'appuie sur un ensemble de neuf filtres, librement paramétrables sur le tableau de bord (nouvelle version). Chacun de ces filtres agit sur un critère spécifique, comme l'adresse IP du client, son adresse email, le pays de sa carte de paiement, …

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	Email jetable	Nom de domaine de l'adresse email du client	
8	Limitation en montant pour une CB sur une période donnée	Montant cumulé en euros (€) 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 CB sur une période donnée	Nombre de transactions cumulées sur la période donnée associée 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 associée 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 euros (€) sur la période donnée associé à l'alias du client	
13	Limitation en montant par IP sur une période donnée	Montant cumulé en euros (€) 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 associée à l'adresse IP du client	

15	Testeurs de cartes	Nombre de transactions cumulées sur la période donnée associée à l'adresse IP du client	
16	Limitation en nombre d'alias par CB	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 la banque à l'interface « Retour » pour un paiement immédiat, différé, partiel ou récurrent :

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2
C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&m
odepaiement=CB&veres=Y&pares=Y
```

Exemple de données envoyées par le serveur de paiement de la banque à l'interface « Retour » pour la première échéance d'un paiement fractionné :

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2
C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&m
odepaiement=CB&veres=Y&pares=Y&montantech=20EUR
```

Exemple de données envoyées par le serveur de paiement de la banque à l'interface « Retour » pour un blocage d'un paiement immédiat par le MPF:

```
TPE=9000001&date=05%2f10%2f2011%5fa%5f15%3a33%3a06&montant=1%2
e01EUR&reference=P1317821466&MAC=70156D2CFF27A9B8AAE5AFEBE590D
9CFCAAF9BDC&texte-
libre=Ceci+est+un+test%2c+ne+pas+tenir+compte%2e&code-
retour=Annulation&cvx=oui&vld=0912&brand=MC&status3ds=-
1&motifrefus=filtrage&originecb=FRA&bincb=12345678&hpancb=764A
D24CFABBB818E8A7DC61D4D6B4B89EA837ED&ipclient=10%2e45%2e166%2e
76&originetr=inconnue&modepaiement=CB&veres=&pares=&filtrageca
use=4-&filtragevaleur=FRA-
```

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

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&status3ds=1&numauto=
010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2
C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&m
odepaiement=CB&cbenregistree=1&nomcartesequestree=VISA%20CIC&c
bmasquee=12345678******90
```

Remarque :

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

9.4.2 Validation du sceau

Le message de confirmation reçu est scellé par un sceau MAC qui a été calculé par le serveur de paiement de la banque 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 la banque :

```
<TPE>*<date>*<montant>*<reference>*<texte-libre>*3.0*<code-
retour>*<cvx>*<vld>*<brand>*<status3ds>*<numauto>*<motifrefu
s>*<originecb>*<bincb>*<hpancb>*<ipclient>*<originetr>*<vere
s>*<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*62.75EUR*ABERTYP00145*LeTexteL
ibre*3.0*paiement*oui*1208*VI*1*010101**FRA*12345678*74E94B0
3C22D786E0F2C2CADBFC1C00B004B7C45*127.0.0.1*FRA*Y*Y*
```

9.5 Détail du document JSON « contexte_commande »

9.5.1 Généralités et exclusions

Ce champ contient des informations relatives au contexte de la commande et est utilisé lors de la phase « Aller ».

Ces informations sont nécessaires pour la mise en œuvre 3DSecure (2.X) et pour la lutte contre la fraude.

Attention, le fonctionnement en mode VPC étant exclu du 3DSecure, ces informations ne sont pas obligatoires dans ce mode de fonctionnement.

Jusqu'à 4 objets sont présents dans la racine du document.

La colonne présence peut être lue comme suit :

- Obligatoire : ce champ / nœud doit être fourni
- Optionnelle : ce champ peut ne pas être fourni
- Obligatoire si applicable : si la valeur existe dans le contexte de la commande, il faut la fournir. Exemple : stateOrProvince existe aux Etats-Unis

En cas d'absence de valorisation de données optionnelles, l'envoi d'une chaîne vide ou d'un objet vide est à proscrire.
Il faut :

- Dans le cas d'une chaîne vide, au choix :
  - ignorer ces données
  - leur assigner la valeur « null »
- Dans le cas d'un objet vide :
  Ignorer ces données

Exemple :

```
"addressLine3":null
```

Champ JSON	Description	Présence	Détail
billing	Adresse de facturation	Obligatoire	lien
shipping	Adresse de livraison	Obligatoire si applicable	lien
shoppingCart	Panier client	Optionnelle	lien
client	Informations client	Optionnelle	lien

9.5.2 Détail de l'objet « billing »

Champ JSON	Présence	Type JSON	Détail
civility	Optionnelle	Chaîne	lien
name	Optionnelle	Chaîne	lien
firstName	Optionnelle	Chaîne	lien
lastName	Optionnelle	Chaîne	lien
middleName	Optionnelle	Chaîne	lien
address	Optionnelle	Chaîne	lien
addressLine1	Obligatoire	Chaîne	lien
addressLine2	Optionnelle	Chaîne	lien
addressLine3	Optionnelle	Chaîne	lien
city	Obligatoire	Chaîne	lien
postalCode	Obligatoire	Chaîne	lien
country	Obligatoire	Chaîne	lien
stateOrProvince	Obligatoire si applicable	Chaîne	lien
countrySubdivision	Optionnelle	Chaîne	lien
email	Optionnelle	Chaîne	lien
phone	Optionnelle	Chaîne	lien
mobilePhone	Optionnelle	Chaîne	lien
homePhone	Optionnelle	Chaîne	lien
workPhone	Optionnelle	Chaîne	lien

9.5.3 Détail de l'objet « shipping »

Champ JSON	Présence	Type JSON	Description
civility	Optionnelle	Chaîne	lien
name	Optionnelle	Chaîne	lien
firstName	Optionnelle	Chaîne	lien
lastName	Optionnelle	Chaîne	lien
address	Optionnelle	Chaîne	lien
addressLine1	Obligatoire si applicable	Chaîne	lien
addressLine2	Obligatoire si applicable	Chaîne	lien
addressLine3	Optionnelle	Chaîne	lien
city	Obligatoire si applicable	Chaîne	lien
postalCode	Obligatoire si applicable	Chaîne	lien
country	Obligatoire si applicable	Chaîne	lien
stateOrProvince	Obligatoire si applicable	Chaîne	lien
countrySubdivision	Optionnelle	Chaîne	lien
email	Optionnelle	Chaîne	lien
phone	Optionnelle	Chaîne	lien
shipIndicator	Optionnelle	Chaîne	lien
deliveryTimeframe	Optionnelle	Chaîne	lien
firstUseDate	Optionnelle	Chaîne	lien
matchBillingAddress	Optionnelle	Booléen	lien

9.5.4 Détail de l'objet « shoppingCart »

Champ JSON	Présence	Type JSON	Description
giftCardAmount	Optionnelle	Nombre	lien
giftCardCount	Optionnelle	Nombre	lien
giftCardCurrency	Optionnelle	Chaîne	lien
preOrderDate	Optionnelle	Chaîne	lien
preorderIndicator	Optionnelle	Booléen	lien
reorderIndicator	Optionnelle	Booléen	lien
shoppingCartItems	Optionnelle	Tableau d'objets	lien

9.5.4.1 Détail de l'objet « shoppingCartItems »

Si l'objet « shoppingCart » est envoyé, dans ce cas, certains champs doivent obligatoirement être renseignés dans l'objet « shoppingCartItems ».

Champ JSON	Présence	Type JSON	Description
name	Optionnelle	Chaîne	lien
description	Optionnelle	Chaîne	lien
productCode	Optionnelle	Chaîne	lien
imageURL	Optionnelle	Chaîne	lien
unitPrice	Obligatoire	Nombre	lien
quantity	Obligatoire si applicable	Nombre	lien
productSKU	Optionnelle	Chaîne	lien
productRisk	Optionnelle	Chaîne	lien

9.5.5 Détail de l'objet « client »

Champ JSON	Présence	Type JSON	Description
civility	Optionnelle	Chaîne	lien
name	Optionnelle	Chaîne	lien
firstName	Optionnelle	Chaîne	lien
lastName	Optionnelle	Chaîne	lien
middleName	Optionnelle	Chaîne	lien
address	Optionnelle	Chaîne	lien
addressLine1	Optionnelle	Chaîne	lien
addressLine2	Optionnelle	Chaîne	lien
addressLine3	Optionnelle	Chaîne	lien
city	Optionnelle	Chaîne	lien
postalCode	Optionnelle	Chaîne	lien
country	Optionnelle	Chaîne	lien
stateOrProvince	Optionnelle	Chaîne	lien
countrySubdivision	Optionnelle	Chaîne	lien
email	Optionnelle	Chaîne	lien
birthLastName	Optionnelle	Chaîne	lien
birthCity	Optionnelle	Chaîne	lien
birthPostalCode	Optionnelle	Chaîne	lien
birthCountry	Optionnelle	Chaîne	lien
birthStateOrProvince	Optionnelle	Chaîne	lien
birthCountrySubdivision	Optionnelle	Chaîne	lien
birthdate	Optionnelle	Chaîne	lien
phone	Optionnelle	Chaîne	lien
nationalIDNumber	Optionnelle	Chaîne	lien
suspiciousAccountActivity	Optionnelle	Booléen	lien
authenticationMethod	Optionnelle	Chaîne	lien
authenticationTimestamp	Optionnelle	Chaîne	lien
priorAuthenticationMethod	Optionnelle	Chaîne	lien
priorAuthenticationTimestamp	Optionnelle	Chaîne	lien
paymentMeanAge	Optionnelle	Chaîne	lien
lastYearTransactions	Optionnelle	Entier	lien
last24HoursTransactions	Optionnelle	Entier	lien
addCardNbLast24Hours	Optionnelle	Entier	lien
last6MonthsPurchase	Optionnelle	Entier	lien
lastPasswordChange	Optionnelle	Chaîne	lien
accountAge	Optionnelle	Chaîne	lien
lastAccountModification	Optionnelle	Chaîne	lien

9.5.6 Description des attributs

Attribut	**accountAge**
Description	Date de création du compte client sur le site commerçant.
Format	Chaîne
Restrictions	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres (ISO 8601)
Attribut	**addCardNbLast24Hours**
Format	Entier
Description	Nombre de tentatives d'ajout carte du client sur le site commerçant durant les 24 dernières heures.

Attribut	**address**
Description	Adresse complète du client (numéro, rue, complément)
Format	Chaîne
Restrictions	Jusqu'à 255 caractères

Attribut	**addressLine1**
Description	Contient le numéro et le nom de la rue
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

Attribut	**addressLine2**
Description	Contient le numéro et le nom de la rue
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

Attribut	**addressLine3**
Description	Toute information complémentaire d'adresse ne pouvant figurer dans les lignes 1 et 2 de l'adresse.
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

Attribut	**authenticationMethod**
Description	Méthode d'authentification du client sur le site commerçant
Format	Chaîne
Valeurs possibles	« guest » : pas d'authentification (invité) « own_credentials » : utilisation d'un compte ouvert sur le site commerçant « federated_id » : identité fédéré « issuer_credentials » : Identifiants fournis par l'émetteur « third_party_authentication » : authentification par un tiers « fido » : utilisation de l'authentification FIDO

Attribut	authenticationTimestamp
Description	Date et heure UTC de l'authentification du client sur le site commerçant.
Format	Chaîne
Restrictions	Du type AAAA-MM-JJ**T**HH:mm:SS**Z** avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres, HH = heure sur 2 chiffres, mm = minutes sur 2 chiffres, SS = secondes sur deux chiffres (ISO 8601)

Attribut	birthCity
Description	Ville de naissance
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

Attribut	birthCountry
Description	Pays de naissance
Format	Chaîne
Restrictions	Code pays sur 2 caractères suivant la norme ISO 3166-1 alpha-2

Attribut	birthCountrySubdivision
Description	Code géographique de l'entité du pays de naissance
Format	Chaîne
Restrictions	Suivre la norme ISO 3166-2
Aide	https://en.wikipedia.org/wiki/ISO_3166-2 https://en.wikipedia.org/wiki/ISO_3166-2:FR

Attribut	birthdate
Description	Date de naissance au format ISO 8601
Format	Chaîne
Restrictions	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres

Attribut	birthLastName
Description	Nom de naissance
Format	Chaîne
Restrictions	Jusqu'à 45 caractères

Attribut	birthPostalCode
Description	Code postal du lieu de naissance
Format	Chaîne
Restriction	Jusqu'à 10 caractères

Attribut	**birthStateOrProvince**
Format	Chaîne
Restrictions	ISO 3166-2
Description	Code géographique de l'état ou de la province de naissance (si applicable).
Aide	https://fr.wikipedia.org/wiki/ISO_3166-2:US https://fr.wikipedia.org/wiki/ISO_3166-2:CA

Attribut	**city**
Format	Chaîne
Restrictions	Jusqu'à 50 caractères
Description	Ville Peut contenir le CEDEX.

Attribut	**civility**
Description	Civilité
Format	Chaîne
Restrictions	Jusqu'à 32 caractères alphabétiques. Pas de ponctuation. Exemples: « M », « Mme »

Attribut	**country**
Description	Code pays
Format	Chaîne
Restrictions	Norme ISO 3166-1 alpha-2 / case sensitive (majuscule)

Attribut	**countrySubdivision**
Description	Code géographique de l'entité du pays
Format	Chaîne
Restrictions	ISO 3166-2
Aide	https://en.wikipedia.org/wiki/ISO_3166-2 https://en.wikipedia.org/wiki/ISO_3166-2:FR

Attribut	deliveryTimeframe
Description	Indique le délai d'expédition de la commande.
Format	Chaîne
Valeurs possibles	« same_day » : le jour même « overnight » : le lendemain « two_day » : deux jours « three_day » : trois jours « long » : plus de trois jours « other » : autre « none » : pas d'expédition

Attribut	description
Description	Description d'un article.
Format	Chaîne
Restrictions	Jusqu'à 2048 caractères.

Attribut	email
Format	Chaîne
Restrictions	Jusqu'à 254 caractères. Vérifie l'expression régulière « ^.+@.+\..+$ ».
Description	Courriel

Attribut	firstName
Description	Prénom
Format	Chaîne
Restrictions	Jusqu'à 45 caractères

Attribut	firstUseDate
Description	Date à laquelle l'adresse d'expédition a été utilisée pour la première fois.
Format	Chaîne
Restrictions	Format ISO 8601 Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres

Attribut	giftCardAmount
Description	Montant utilisé pour l'achat de cartes / codes cadeaux, exprimé dans la plus petite unité de la monnaie.
Format	Nombre
Restrictions	Nombre entier Maximum de 12 chiffres utiles

Attribut	giftCardCount
Description	Nombre de cartes cadeaux achetées
Format	Nombre
Restrictions	Nombre entier Maximum de 2 chiffres utiles

Attribut	giftCardCurrency
Format	Chaîne
Restrictions	3 caractères alphabétiques (exemple : EUR). Norme ISO 4217
Description	Devise de la carte cadeaux achetée

Attribut	homePhone
Description	Numéro de téléphone
Format	Chaîne
Restrictions	Jusqu'à 18 caractères numériques avec « + » comme premier caractère, suivi de l'indicatif pays, d'un tiret « - », puis du numéro
Exemple	Le numéro français 05 12 34 56 78 s'écrira « +33-512345678 »
Aide	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribut	imageURL
Description	URL pointant vers une image associée à un article.
Format	Chaîne
Restrictions	Jusqu'à 2000 caractères.

Attribut	last24HoursTransactions
Format	Entier positif ou nul
Description	Nombre de transactions (achevées ou abandonnées) du client avec n'importe quel moyen de paiement enregistrés sur le site commerçant durant les 24 dernières heures.

Attribut	last6MonthsPurchase
Description	Nombre d'achats avec ce moyen de paiement les 6 derniers mois.
Format	Entier positif ou nul

Attribut	lastAccountModification
Description	Date de la dernière modification du compte client (y compris nouvelle adresse de facturation, nouvelle adresse de livraison, nouveau moyen de paiement enregistré).
Format	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres Norme ISO 8601

Attribut	lastName
Description	Nom de famille.
Format	Chaîne
Restrictions	Jusqu'à 45 caractères.

Attribut	lastPasswordChange
Description	Date à laquelle le client a changé son mot de passe ou réinitialisé son compte pour la dernière fois.
Format	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres Norme ISO 8601

Attribut	lastYearTransactions
Format	Entier positif ou nul
Description	Nombre de transactions (achevées ou abandonnées) du client avec n'importe quel moyen de paiement enregistrés sur le site commerçant durant la dernière année.

Attribut	matchBillingAddress
Description	Indique si les adresses d'expédition ou de facturation sont identiques.
Format	Booléen

Attribut	middleName
Description	Deuxième prénom (et suivants)
Format	Chaîne
Restrictions	Jusqu'à 150 caractères

Attribut	**mobilePhone**
Description	Numéro de téléphone portable
Format	Chaîne
Restrictions	Jusqu'à 18 caractères numériques avec « + » comme premier caractère, suivi de l'indicatif pays, d'un tiret « - », puis du numéro
Exemple	Le numéro mobile français 06 12 34 56 78 s'écrira « +33-612345678 »
Aide	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribut	**name**
Description	Nom et prénom.
Format	Chaîne
Restrictions	Jusqu'à 45 caractères

Attribut	**nationalIDNumber**
Description	Numéro d'une pièce d'identité.
Format	Chaîne
Restrictions	Jusqu'à 255 caractères

Attribut	**paymentMeanAge**
Description	Date à laquelle la carte a été ajoutée sur le compte du client (sur le site commerçant).
Format	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres Nome ISO 8601

Attribut	**phone**
Description	Numéro de téléphone
Format	Chaîne
Restrictions	Jusqu'à 18 caractères numériques avec « + » comme premier caractère, suivi de l'indicatif pays, d'un tiret « - », puis du numéro
Exemple	Le numéro français 06 12 34 56 78 s'écrira « +33-612345678 »
Aide	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

Attribut	**postalCode**
Description	Code postal
Format	Chaîne
Restrictions	Jusqu'à 10 caractères

Attribut	**preOrderDate**
Description	Pour une précommande, date à laquelle la marchandise sera disponible.
Format	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres Norme ISO 8601

Attribut	**preorderIndicator**
Description	Indique s'il s'agit d'une précommande.
Format	Booléen

Attribut	**priorAuthenticationMethod**
Description	Mécanisme utilisé pour l'authentification du porteur lors de son dernier paiement sur le site commerçant.
Format	Chaîne
Valeurs possibles	« frictionless » : L'ACS a permis un paiement sans challenge « challenge » : Le porteur a dû compléter l'étape du challenge « AVS_verified » : Vérification de l'adresse du porteur (système AVS) « other » : Autre méthode d'authentification

Attribut	**priorAuthenticationTimestamp**
Description	Date et heure UTC de la précédente authentification du client sur le site commerçant.
Format	Chaîne
Restrictions	Du type AAAA-MM-JJTHH:mm:SSZ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres, HH = heure sur 2 chiffres, mm = minutes sur 2 chiffres, SS = secondes sur deux chiffres Norme ISO 8601

Attribut	**productCode**
Description	Indique le type de produit.
Format	Chaîne
Valeurs possibles	« adult_content » : contenu pour adulte « coupon » : bon de reduction appliqué à la commande « default » : valeur par défaut (si aucun autre code ne convient) « electronic_good » : biens éléctroniques (pas de logiciels) « electronic_software » : logiciels « gift_certificate » : cheque-cadeau « handling_only » : frais administratifs « service » : service rendu au client « shipping_and_handling » : frais d'expédition et administratifs « shipping_only » : frais d'expédition uniquement « subscription » : abonnement à un site web ou autre

Attribut	**productRisk**
Description	Indicateur du niveau de risque lié à un produit.
Format	Chaîne
Valeurs possibles	« low » : faible risque « normal » : risque moyen « high » : risque élevé

Attribut	**productSKU**
Description	Identifiant que le commerçant donne à un article.
Format	Chaîne
Restrictions	Jusqu'à 255 caractères

Attribut	**quantity**
Format	Nombre
Restrictions	Nombre entier
Description	Exprime une quantité (par exemple un nombre d'articles)

Attribut	**reorderIndicator**
Description	Vaut « true » si et seulement si le client a déjà passé une commande identique.
Format	Booléen

Attribut	**shipIndicator**
Format	Chaîne
Description	Moyen d'expédition retenu.
Valeurs possibles	« digital_goods »: Biens numériques (pas d'expédition). « travel_and_event »: Transports ou évènements (pas d'expédition). « billing_address »: Expédition sur l'adresse de facturation. « verified_address »: Expédition vers une adresse déjà utilisée. « another_address »: Expédition vers une nouvelle adresse. « pick-up » : Expédition vers un point relai. « other » Autre.

Attribut	**shoppingCartItems**
Description	Tableau contenant les articles présents dans le panier.
Format	Tableau d'objets (de type « shoppingCartItem »)

Attribut	**stateOrProvince**
Description	Code géographique de l'état ou de la province (si applicable).
Format	Chaîne
Restrictions	ISO 3166-2
Aide	https://fr.wikipedia.org/wiki/ISO_3166-2:US https://fr.wikipedia.org/wiki/ISO_3166-2:CA

Attribut	**suspiciousAccountActivity**
Description	Permet d'indiquer si des activités suspectes sur le compte du client on été relevées par le commerçant.
Format	Booléen

Attribut	**unitPrice**
Description	Montant exprimé dans la plus petite unité de la monnaie (par exemple en centimes pour le cas de l'EURO)
Format	Nombre
Restrictions	Nombre entier Maximum de 12 chiffres utiles

Attribut	**workPhone**
Description	Numéro de téléphone professionnel
Format	Chaîne
Restrictions	Jusqu'à 18 caractères numériques avec « + » comme premier caractère, suivi de l'indicatif pays, d'un tiret « - », puis du numéro Le numéro mobile français 05 12 34 56 78 s'écrira « +33-512345678 »
Aide	https://en.wikipedia.org/wiki/List_of_country_calling_codes https://en.wikipedia.org/wiki/E.123 https://en.wikipedia.org/wiki/E.164

9.6 Détail du document JSON « authentification »

Ce champ contient des informations relatives à l'authentification du porteur et est fourni lors de la phase « Retour ». Si aucune authentification n'a lieu (par exemple paiement bloqué en amont par le module prévention fraude, utilisation de moyens de paiement alternatifs tels que COFIDIS), le champ sera toujours renvoyé mais valorisé à null c'est-à-dire bnVsbAo= une fois encodé.

Champ JSON	Description	Détails
status	Résultat de l'authentification	lien
protocol	Protocole utilisé	lien
version	Version du protocole	lien
details	Détails spécifiques au protocole et à la version	lien

Les informations générales (status, protocol, version) sont situées à la racine du document JSON. Il est possible de baser son traitement métier uniquement sur ces informations en se basant principalement sur le champ « status ». Le champ « details » permet de réaliser une analyse plus fine du déroulé du processus 3DSecure.

9.6.1 Détail de l'objet « details »

Champ JSON	Description	Détails
liabilityShift	Transfert de responsabilités	lien
VERes	Résultat contenu dans le message VERes	lien
PARes	Résultat contenu dans le message PARes	lien
ARes	Résultat contenu dans le message ARes	lien
CRes	Résultat contenu dans le message CRes	lien
merchantPreference	Souhait du commerçant	lien
transactionID	Identifiant de la transaction	lien
status3DS	Indicateur d'échange 3DSecure 1.X	lien
disablingReason	Motif du débrayage de 3DSecure	lien

9.6.2 Description des attributs

Attribut	**status**
Description	Indique le résultat de l'authentification
Format	Chaîne
Valeurs possibles	• « authenticated » : L'authentification est effectuée avec succès. • « authentication_not_performed » : L'authentification n'a pas pu être complétée (problème technique ou autre). • « not_authenticated »: L'authentification a échoué. • « authentication_rejected »: L'authentification a été refusée par l'émetteur. • « authentication_attempted » : Une tentative d'authentification a bien été effectuée. L'authentification n'a pas pu se faire mais une preuve a été générée (CAVV) • « not_enrolled » : La carte n'est pas enrôlée au 3DS • « disabled » : Dans le cas de l'usage de l'option 3DSecure débrayable

Attribut	**protocol**
Description	Protocole utilisé pour l'authentification
Format	Chaîne
Valeurs possibles	3DSecure

Attribut	**version**
Description	Version du protocole
Format	Chaîne
Valeurs possibles	2.1.0 2.2.0

Attribut	**liabilityShift**
Description	Indique s'il y a transfert de responsabilités vers la banque émettrice
Format	Chaîne
Valeurs possibles	« Y » : La banque émettrice supporte le risque. « N » : Le marchand supporte le risque. « NA »: Impossible à déterminer ou non applicable.
Présence	Dans le cadre de 3DSecure 2.X uniquement.

Attribut	**VERes**
Description	Vérification de l'enrôlement d'une carte à 3DSecure 1.X.
Format	Chaîne
Valeurs possibles	« Y » : carte enrôlée 3DSecure 1.X. « N » : carte non-enrôlée 3DSecure 1.X. « U » : Problème technique lors de la vérification de l'éligibilité de la carte
Présence	Dans le cadre de 3DSecure 1.X uniquement.

Attribut	**PARes**
Description	Résultat de l'authentification 3DSecure
Format	Chaîne
Valeurs possibles	« Y » : Authentification réussie. « U » : Problème technique lors de l'authentification. « N » : Authentification échouée. « A » : Pas d'authentification mais la banque du porteur prend en charge le risque.
Présence	Dans le cadre de 3DSecure 1.X uniquement.

Attribut	ARes
Description	Le message ARes est la réponse ACS de l'émetteur au message AReq. Cela peut indiquer que le titulaire de la carte a été authentifié ou qu'une interaction supplémentaire entre le titulaire de la carte est nécessaire pour mener à bien l'authentification. Il n'y a qu'un seul message ARES par transaction.
Format	Chaine
Valeurs possibles	« Y » : Authentification réussie sans challenge. « R » : Authentification refusée par l'émetteur « C » : Challenge demandé. « U » : L'ACS n'a pas répondu correctement. « A » : L'authentification n'a pas pu se faire mais une preuve a été générée. « N » : Authentification échouée sans challenge.
Présence	Dans le cadre de 3DSecure 2.X uniquement.

Attribut	CRes
Description	Le message CRes est la réponse ACS au message CReq. Il peut indiquer le résultat de l'authentification du titulaire de carte ou, dans le cas d'un modèle basé sur une application, indiquer également qu'une interaction supplémentaire du titulaire de carte est nécessaire pour mener à bien l'authentification.
Format	Chaîne
Valeurs possibles	« Y » : Authentification réussie après challenge. « N » : Authentification échouée après challenge.
Présence	Dans le cadre de 3DSecure 2.X uniquement.

Attribut	merchantPreference
Description	Indique le souhait du commerçant concernant la cinématique de l'authentification 3DSecure 2.X. Il s'agit uniquement d'un souhait et ce dernier peut ne pas être approuvé par les banques émettrices.
Format	Chaîne
Valeurs possibles	« no_preference » : pas de préférence (choix par défaut) « challenge_preferred » : challenge souhaité « challenge_mandated » : challenge requis « no_challenge_requested » : pas de challenge demandé « no_challenge_requested_strong_authentication » : pas de challenge demandé – l'authentification forte du client a déjà été réalisée par le commerçant. « no_challenge_requested_trusted_third_party » : pas de challenge demandé – demande d'exemption car le commerçant est un bénéficiaire de confiance du client. «no_challenge_requested_risk_analysis » : pas de challenge demandé – demande d'exemption pour un autre motif que cité précédemment (par exemple : petit montant)

Attribut	**transactionID**
Description	Identifiant unique lié à la transaction.
Format	Chaîne / UUID (RFC 4122)
Valeurs possibles	UUID (RFC 4122)
Présence	Dans le cadre de 3DSecure 2.X uniquement.

Attribut	**status3DS**
Description	Indicateur d'échange 3DSecure 1.X
Format	Entier
Valeurs possibles :	-1 : la transaction ne s'est pas faite selon le protocole 3DSecure et le risque d'impayé est élevé 1 : la transaction s'est faite selon le protocole 3DS et le risque d'impayé est faible 4 : la transaction s'est faite selon le protocole 3DS et le risque d'impayé est élevé
Présence	Dans le cadre de 3DSecure 1.X uniquement.

Attribut	**disablingReason**
Description	Couplé à l'option de 3DSecure débrayable. Indique le motif du débrayage.
Format	Chaîne
Valeurs possibles	commercant : débrayage explicite par le commerçant via l'envoi de la valeur appropriée dans le formulaire de la phase « Aller » seuilnonatteint : débrayage car le montant de la transaction n'atteint pas le montant configuré par le commerçant scoring : débrayage sur motif de scoring

9.6.3 Exemple

Ci-dessous un exemple de document JSON authentification dans le cadre du 3DSecure v2.

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

Après encodage en base 64 :

```
eyAgCiAgICJzdGF0dXMiOiJhdXRoZW50aWNhdGVkIiwKICAgInByb3RvY29sIjoiM0RTZWN1cmUiLAogICAid
mVyc2lvbiI6IjIuMS4wIiwKICAgImRldGFpbHMiOnsgIAogICAgICAibGlhYmlsaXR5U2hpZnQiOiJZIiwKICAgICAg
IkFSZXMiOiJDIiwKICAgICAgIkNSZXMiOiJZIiwKICAgICAgIm1lcmNoYW50UHJlZmVyZW5jZSI6Im5vX3ByZWZ
lcmVuY2UiLAogICAgICAidHJhbnNhY3Rpb25JRCI6IjU1NWJkOWQ5LTFjZjEtNGJhOC1iMzdjLTFhOTZiYzhiNj
AzYSIKICAgfQp9Cg==
```

9.7 La gestion du protocole d'authentification 3DSecure

L'authentification des porteurs de cartes bancaires lors d'un acte de paiement se fait par le biais du protocole 3DSecure. Celui-ci permet de s'assurer que la personne ayant saisi les informations de cartes bancaires sur la page de paiement est légitime pour cet achat : il lui est demandé de réaliser une action supplémentaire (saisie d'un code, authentification via une application mobile, ...) permettant de l'authentifier en tant que porteur de la carte de paiement.

Jusqu'à présent, cette phase d'authentification était basée sur la version 1 du protocole sécurisé de communication entre les différents acteurs 3DSecure.

Courant de l'année 2019, la version 2.1 de ce protocole sera mise en application. Cette nouvelle version fera l'objet d'une montée en charge progressive tout au long du second semestre, qui devrait se prolonger vraisemblablement en 2020. Cela signifie que pendant cette période, une transaction pourra être effectuée avec le protocole 3DSecure V1 ou 3DSecure V2. La version du protocole utilisé sera définie en fonction de la carte de paiement du porteur : la banque émettrice décidera de la version de l'authentification à employer. Ces décisions reposent en partie sur le BIN mais pas uniquement.

Afin de traiter au mieux cette période de transition, vous trouverez ci-dessous des explications sur les impacts sur la plateforme Monetico Paiement.

Il est important de noter que les réseaux (VISA, Mastercard, CB) étant encore en cours de finalisation de la spécification de la norme, certaines informations sont susceptibles d'évoluer.

9.7.1 La demande de paiement – interface « Aller »

Lors de la demande de paiement, deux paramètres sont disponibles pour indiquer le comportement de la solution Monetico Paiement vis-à-vis de l'authentification 3DSecure :

- 3dsdebrayable : ce champ permet de débrayer l'authentification 3D quelle que soit la version.
- ThreeDSecureChallenge : ce champ est spécifique au protocole 3DSecure V2.

Les deux champs peuvent être fournis lors de la demande de paiement afin de s'assurer la mise en œuvre du comportement d'authentification souhaité, quelle que soit la version du protocole employé pour un paiement.

Le tableau ci-dessous préconise les valeurs à passer en fonction du scénario d'authentification souhaité :

Scénario souhaité	3dsdebrayable	ThreeDSecureChallenge
Pas de préférence	au choix	no_preference
Authentification souhaitée	0 ou rien	challenge_preferred
Authentification systématique demandée	0 ou rien	challenge_mandated
Pas d'authentification demandée	1	no_challenge_requested
Pas d'authentification demandée type d'exemption l'authentification forte	1	no_challenge_requested_strong_authentication
Pas d'authentification demandée type d'exemption tiers de confiance	1	no_challenge_requested_trusted_third_party
Pas d'authentification demandée type d'exemption analyse de risque préalable faite	1	no_challenge_requested_risk_analysis

Point d'attention concernant l'option de débrayage : si votre TPE est configuré pour un débrayage automatique par montant, toute transaction dont le montant est inférieur au montant paramétré sera débrayée: ceci équivaut à fournir la valeur « 3dsdebrayable » = 1 lors d'une demande de paiement.

9.7.2 La notification serveur à serveur du résultat du paiement - interface « Retour »

Le tableau ci-dessous vous indique les différents scénarii rencontrés et les valeurs retournées par la plateforme Monetico Paiement.

Pour chaque statut, vous trouverez les différents scénarii pouvant aboutir à ce statut et des exemples de valeur du champ « authentication »

Scénario	Status	Résultats
Le protocole 3DSecure s'est finalisé Le porteur a été authentifié par la banque émettrice via sa page d'authentification ACS.	**authenticated (lien)**	**lien**
Le protocole 3DSecure s'est finalisé Le porteur a été authentifié par la banque émettrice sans passer par sa page d'authentification ACS (frictionless). Le transfert de responsabilité est différent en fonction du souhait exprimé par le commerçant : voir le tableau sur le liabilty shift pour les détails.	**authenticated (lien)**	**lien**
Le protocole 3DSecure s'est finalisé. Le porteur a été authentifié par la banque émettrice sans authentification formelle (pas de saisie du code d'authentification par exemple)	**authentication_attempted (lien)**	**lien**
Le protocole 3DSecure a été initié. La banque du porteur considère que ce paiement est risqué et refuse l'authentification.	**not_authenticated (lien)**	**lien**
Le protocole 3DSecure a été initié. Une authentification du porteur via la page d'authentification ACS de la banque du porteur a été demandée mais celle-ci n'a pas aboutie (plusieurs saisies erronées du code d'authentification, annulation de l'authentification à l'initiative du porteur, ...)	**not_authenticated (lien)**	**lien**
Le protocole 3DSecure a été initié. Suite à un problème technique, il n'a pu aboutir.	**authentication_not_performed (lien)**	**lien**
Le protocole 3DSecure s'est déclenché mais un problème technique est survenu empêchant l'authentification du porteur par l'émetteur.	**authentication_not_performed (lien)**	**lien**
Le protocole 3DSecure a été initié. La banque du porteur refuse l'authentification.	**authentication_rejected (lien)**	**lien**
La carte n'est pas enrôlée au protocole 3DSecure.	**not_enrolled (lien)**	**lien**

Status	**authenticated (lien)**
Scénario	Le protocole 3DSecure s'est finalisé Le porteur a été authentifié par la banque émettrice via sa page d'authentification ACS.

Interface retour 3DS v2	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique>",
	"ARes":"C",
	"CRes":"Y",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}

Status	**authenticated (lien)**
Scénario	Le protocole 3DSecure s'est finalisé Le porteur a été authentifié par la banque émettrice sans passer par sa page d'authentification ACS (frictionless). Le transfert de responsabilité est différent en fonction du souhait exprimé par le commerçant : voir le tableau sur le liabilty shift pour les détails.

Interface retour 3DS v2	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique>",
	"ARes":"Y",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_attempted (lien)**
Scénario	Le protocole 3DSecure s'est finalisé. Le porteur a été authentifié par la banque émettrice sans authentification formelle (pas de saisie du code d'authentification par exemple)

Interface retour 3DS v2	{
	"status":"authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique",
	"ARes":"C",
	"CRes":"Y",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"

	<pre> } }</pre>

Status	**not_authenticated (lien)**
Scénario	Le protocole 3DSecure a été initié. La banque du porteur considère que ce paiement est risqué et refuse l'authentification.

Interface retour 3DS v2	<pre>{
	   "status":"not_authenticated",
	   "protocol":"3DSecure",
	   "version":"2.1.0",
	   "details":{
	      "liabilityShift":"<Voir tableau spécifique>",
	      "ARes":"N",
	      "merchantPreference":"<souhait exprimé phase Aller>",
	      "transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	   }
	}</pre>

Status	**not_authenticated (lien)**
Scénario	Le protocole 3DSecure a été initié. Une authentification du porteur via la page d'authentification ACS de la banque du porteur a été demandée mais celle-ci n'a pas aboutie (plusieurs saisies erronées du code d'authentification, annulation de l'authentification à l'initiative du porteur, ...)

Interface retour 3DS v2	{
	"status":"not_authenticated",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique",
	"ARes":"C",
	"CRes":"N",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_not_performed (lien)**
Scénario	Le protocole 3DSecure a été initié. Suite à un problème technique, il n'a pu aboutir.

Interface retour 3DS v2	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique>",
	"ARes":"U",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_not_performed (lien)**
Scénario	Le protocole 3DSecure s'est déclenché mais un problème technique est survenu empêchant l'authentification du porteur par l'émetteur.

Interface retour 3DS v2	{
	"status":"authentication_not_performed",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique>",
	"ARes":"C",
	"CRes":"U",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**authentication_rejected (lien)**
Scénario	Le protocole 3DSecure a été initié. La banque du porteur refuse l'authentification.

Interface retour 3DS v2	{
	"status":"authentication_rejected",
	"protocol":"3DSecure",
	"version":"2.1.0",
	"details":{
	"liabilityShift":"<Voir tableau spécifique ",
	"ARes":"R",
	"merchantPreference":"<souhait exprimé phase Aller>",
	"transactionID":"555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"
	}
	}

Status	**not_enrolled (lien)**
Scénario	La carte n'est pas enrôlée au protocole 3DSecure.

Interface retour 3DS v2	{
	"status":"not_enrolled",
	"protocol":"3DSecure",
	"version":"2.1.0"
	}

Pour compléter les tableaux ci-dessus, ci-dessous les valeurs du transfert de responsabilité (liability shift) en fonction des différents scénarii et des statuts renvoyés par Monetico Paiement.

9.7.2.1 Scénarii frictionless

Authentification du porteur via l'ACS de la banque émettrice a été effectuée	Status	Liability Shift
Oui - Authentification via l'ACS de la banque du porteur nécessaire	**authenticated**	Emetteur
	not_authenticated	Refus de la transaction
Non - Pas d'authentification via l'ACS de la banque du porteur	**authenticated** (frictionless)	Commerçant
	authentication_attempted (ARes = A)	Dépendant du réseau et du type de carte
	authentication_not_performed (ARes = U)	Dépendant du réseau et du type de carte
	authentication_rejected (ARes = R)	Refus de la transaction
	not_enrolled	Commerçant

9.7.2.2 Scénarii challenge

Authentification du porteur via l'ACS de la banque émettrice a été effectuée	Status	Liability Shift
Oui - Authentification via l'ACS de la banque du porteur nécessaire	**authenticated**	Emetteur
	not_authenticated	Refus de la transaction
Non - Pas d'authentification via l'ACS de la banque du porteur	**authenticated** (frictionless)	Emetteur
	authentication_attempted (ARes = A)	Dépendant du réseau et du type de carte
	authentication_not_performed (ARes = U)	Dépendant du réseau et du type de carte
	authentication_rejected (ARes = R)	Refus de la transaction
	not_enrolled	Commerçant

9.8 URL des services

9.8.1 L'environnement de test dit « sandbox »

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 bancaire réel.

Pour effectuer des demandes de paiement dans cet environnement, nous mettons à votre disposition des cartes de paiement 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 :

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

- Services de capture et de recrédit :
  https://payment-api.e-i.com/test/capture_paiement.cgi
  https://payment-api.e-i.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/

9.8.2 En Production

Après avoir validé vos développements et procédé à la demande de mise en production de votre TPE auprès de centrecom@e-i.com, vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

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

- Services de capture et de recrédit :
  https://payment-api.e-i.com/capture_paiement.cgi
  https://payment-api.e-i.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.