

# Monetico Paielement

**Paielement sécurisé sur Internet**

**Documentation Technique**  
**Page de paiement**



# SOMMAIRE

<b>1</b>	<b>Mise en place de l'interface de paiement</b>	<b>4</b>
1.1	Introduction	4
1.2	Mode d'affichage du formulaire de paiement	5
1.3	Personnalisation du formulaire de paiement Monetico Paiement	6
1.4	Clé de sécurité commerçant	6
1.5	Spécifications des messages échangés	7
1.5.1	Rappel de la cinématique	7
1.5.2	Interface « Aller »	8
1.5.3	Interface « Retour »	21
<b>2</b>	<b>Aides à l'installation</b>	<b>34</b>
2.1	Passer un TPE en production	34
2.2	Foire aux questions	34
2.3	Les problèmes les plus fréquents	39
2.3.1	Problème de calcul du sceau de sécurité	39
2.3.2	Le commerçant ne peut pas être identifié	40
2.3.3	La commande a déjà été traitée.	41
2.3.4	La date de validité de la commande est dépassée.	41
2.3.5	Le mode de paiement utilisé est non disponible.	41
<b>3</b>	<b>Assistance technique</b>	<b>42</b>
<b>4</b>	<b>Annexes</b>	<b>43</b>
4.1	Contraintes générales de codage HTML des champs	43
4.2	Contrainte d'encodage	44
4.3	Calcul du sceau MAC	44
4.3.1	Exemples de chaînes permettant le calcul du sceau	45
4.4	Détail du document JSON « contexte_commande »	48
4.4.1	Généralités et exclusions	48
4.4.2	Détail de l'objet « billing »	49
4.4.3	Détail de l'objet « shipping »	49
4.4.4	Détail de l'objet « shoppingCart »	50
4.4.5	Détail de l'objet « client »	51
4.4.6	Description des attributs	52
4.5	Détail du document JSON « authentification »	63
4.5.1	Détail de l'objet « details »	63
4.5.2	Description des attributs	63
4.5.3	Exemple	67
4.6	La gestion du protocole d'authentification 3DSecure	67
4.6.1	La notification serveur à serveur du résultat du paiement - interface « Retour »	67
4.7	URL des services	73
4.7.1	L'environnement de test dit « sandbox »	73
4.7.2	En Production	73
4.8	Spécificités Cofidis	73
4.8.1	Redirection automatique	73



## 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 Mode d'affichage du formulaire de paiement

La page de paiement Monetico Paiement s'affiche suite à une redirection du payeur depuis le site marchand. On parle de « page déportée » car le payeur quitte le site marchand et y reviendra à la fin du paiement.

La page de paiement, à la charte Monetico Paiement, contient l'ensemble des informations liées au paiement (informations concernant le commerçant, le paiement, ...) :

- 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

Commerçant	Demonstration Monetico Services CM (MODEMO)
Référence	E0727092410
Montant	129,95 EUR

Montant de la transaction : 129,95 EUR

Numéro de carte bancaire

Date d'expiration Mois  / Année

Nom du titulaire de la carte

Code de vérification  [Qu'est-ce que c'est ?](#)

Monetico Paiement garantit la confidentialité et la sécurité de vos données.

Les symboles : indiquent que la transaction est sécurisée.

## 1.3 Personnalisation du formulaire de paiement Monetico Paiement

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 dédiés](https://www.monetico-paiement.fr/fr/piloter-suivre/parametrage/page-de-paiement.html) (<https://www.monetico-paiement.fr/fr/piloter-suivre/parametrage/page-de-paiement.html>).

## 1.4 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'événements 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).

## 1.5 Spécifications des messages échangés

### 1.5.1 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 <sup>1</sup>	Serveur de paiement de Monetico Paiement
L'internaute peut imprimer (ou sauvegarder) cette page <sup>1</sup>	
Le serveur propose à l'internaute de revenir sur le site du commerçant via un lien hypertexte <sup>1</sup>	
S'il suit ce lien, l'internaute quitte le serveur de paiement et revient sur le site du commerçant <sup>1</sup>	
Le serveur du commerçant adapte son dialogue en fonction du résultat de paiement reçu	Site web du commerçant

<sup>1</sup> 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.

## 1.5.2 Interface « Aller »

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.

### 1.5.2.1 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 » (4.7.1).

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. Être 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	7 caractères alphanumériques
Valeur(s) possible(s)	[A-Za-z0-9]{7}
Exemple	1234567

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

Champ	date
Présence	Obligatoire
Description	Date de la commande
Format	JJ/MM/AAAA:HH:MM:SS
Valeur(s) possible(s)	
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	Igue
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

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

<b>Champ</b>	<b>societe</b>
<b>Présence</b>	Obligatoire
<b>Description</b>	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.
<b>Format</b> <b>Valeur(s) possible(s)</b>	Chaine de caractères générée à la création de votre contrat
<b>Exemple</b>	maSociete

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

<b>Champ</b>	<b>mail</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	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 vers le marchand en fin de paiement n'est pas possible.
<b>Format</b> <b>Valeur(s) possible(s)</b>	255 caractères maximum ^.\+@.\+.\+.\$
<b>Exemple</b>	monclient@mondomain.com

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

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

<b>Champ</b>	<b>3dsdebrayable</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	Permet de forcer le débrayage de 3DSecure Attention, ce forçage engendre un risque important de refus d'autorisation de la banque émettrice.
<b>Format</b> <b>Valeur(s) possible(s)</b>	0 : pas de débrayage du protocole 3DSecure 1 : débrayage du protocole 3DSecure
<b>Exemple</b>	0

<b>Champ</b>	<b>ThreeDSecureChallenge</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	Souhait commerçant concernant le challenge 3DSecure
<b>Format</b> <b>Valeur(s) possible(s)</b>	« 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 (paiement express), le souhait « challenge_mandated » sera systématiquement utilisé.
<b>Exemple</b>	challenge_preferred

<b>Champ</b>	<b>libelleMonetique</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	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. <b>NB</b> : Le nombre de caractères pris en compte est dépendant de la banque du porteur

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

Champ	<b>libelleMonetiqueLocalite</b>
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. <b>NB</b> : Le nombre de caractères pris en compte est dépendant de la banque du porteur
Format	<i>ville\code postal\code pays</i>
Valeur(s) possible(s)	<ul style="list-style-type: none"> <li><i>ville</i> : [-A-Za-z0-9 ]+</li> <li><i>code postal</i> : [-A-Z a-z0-9]*</li> <li><i>code pays</i> : [A-Za-z]{3} conformément à la norme ISO 3166-1 alpha-3</li> </ul> <p>Format global attendu : [-A-Za-z0-9 ]+[-A-Z a-z0-9]*[A-Za-z]{3}</p> <p>Longueur maximum attendue : 32 caractères</p>
Exemple	Strasbourg\67000\FRA Strasbourg\FRA

Champ	<b>desactivemoyenpaiement</b>
Présence	Optionnelle
Description	Permet de ne pas afficher un ou plusieurs moyens de paiement alternatifs sur la page de paiement.
Format	3xcb, 4xcb, 5-10-12xcb, loan, paylater, paypal, lyfpay
Valeur(s) possible(s)	
Exemple	paypal

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

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

<b>Champ</b>	<b>protocole</b>
<b>Présence</b>	Optionnelle Nécessite la souscription à un moyen de paiement alternatif
<b>Description</b>	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).
<b>Format</b>	3xcb, 4xcb, 5-10-12xcb, loan, paylater, paypal, lyfpay
<b>Valeur(s) possible(s)</b>	
<b>Exemple</b>	lyfpay

<b>Champ</b>	<b>url_notification</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	URL utilisée pour effectuer les différentes notifications de résultat
<b>Format</b>	2048 caractères maximum. Doit être une URL valide.
<b>Valeur(s) possible(s)</b>	
<b>Exemple(s)</b>	<a href="https://www.interface-retour-monetico.com/exemple.cgi">https://www.interface-retour-monetico.com/exemple.cgi</a>

<b>Champ</b>	<b>mail_notification_ok</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	Adresse(s) email utilisée(s) suite à l'envoi d'une notification de résultat en succès Maximum 10 adresses séparées par un point-virgule
<b>Format</b>	^(.+@.+\.+;?){1,10}\$
<b>Valeur(s) possible(s)</b>	
<b>Exemple(s)</b>	monclient@mondomaine.com;monclient2@mondomaine.com

<b>Champ</b>	<b>mail_notification_err</b>
<b>Présence</b>	Optionnelle
<b>Description</b>	Adresse(s) email utilisée(s) suite à l'envoi d'une notification de résultat en erreur Maximum 10 adresses séparées par un point-virgule
<b>Format</b>	^(.+@.+\.+;?){1,10}\$
<b>Valeur(s) possible(s)</b>	
<b>Exemple(s)</b>	monclient@mondomaine.com;monclient2@mondomaine.com

### 1.5.2.2 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	<b>nbrech</b>
Présence	Optionnelle en cas de paiement fractionné
Description	Nombre d'échéances pour cette commande
Format	2, 3 ou 4.
Valeur(s) possible(s)	
Exemple	3

Champ	<b>dateech[N]</b> (N =1, 2, 3 ou 4)
Présence	Optionnelle en cas de paiement fractionné
Description	Date de la Nième échéance
Format	JJ/MM/AAAA
Valeur(s) possible(s)	
Exemple	24/05/2019
Champ	<b>montantech[N]</b> (N =1, 2, 3 ou 4)
Présence	Optionnelle en cas de paiement fractionné
Description	Montant TTC de la Nième échéance
Format	Un nombre entier
Valeur(s) possible(s)	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

### 1.5.2.3 Informations propres au paiement pré-autorisation

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

### 1.5.2.4 Informations propres aux moyens de paiement COFIDIS

Dans le cadre des paiements Cofidis 3xCB, 4xCB, 5-10-12xCB, Loan et Paylater 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	<b>civiliteclient</b>
Présence	Optionnelle
Description	Civilité du client.
Format	MR / MME / MLLE
Valeur(s) possible(s)	
Exemple	MR

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

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

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

Champ	<b>complementadressesclient</b>
Présence	Optionnelle
Description	Complément d'adresse
Format	.{1,50}
Valeur(s) possible(s)	
Exemple	Appartement B

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

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

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

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

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

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

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

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

## 1.5.2.5 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="igue" 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>
```

## 1.5.2.6 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="igue" 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>
```

## 1.5.2.7 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>
```

## 1.5.2.8 Exemple de formulaire de paiement propres aux moyens de paiement COFIDIS

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

## 1.5.2.9 Calcul du sceau du formulaire

Pour réaliser le calcul du sceau MAC, il faut se reporter à la [section dédiée](#).

## 1.5.3 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 15 secondes pour répondre comme décrit au chapitre 1.5.3.2.2, page 33. 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](#).

### 1.5.3.1 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	<p>Chaîne de caractères</p> <p>payetest : paiement accepté (en « sandbox » uniquement)  paiement : paiement accepté (en Production uniquement)  Annulation : paiement refusé  attente_partenaire : paiement en attente d'une validation par le partenaire externe</p> <p>En paiement fractionné, pour les mises en recouvrement automatique des échéances de rang &gt; 1 :</p> <p>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)</p>
Complément	<p>En cas de paiement refusé, une autorisation ultérieure pourra encore être délivrée pour la même référence.</p> <p>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.</p> <p>Le code « attente_partenaire » peut être signe de spécificités (voir 9.9.1)</p>
Exemple	paiement

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

Champ	TPE
Description	Numéro de votre TPE virtuel
Format Valeur(s) possible(s)	<p>7 caractères alphanumériques  [A-Za-z0-9]{7}</p>
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 <b>HORS</b> 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

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

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

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

<b>Champ</b>	<b>issuer</b>
<b>Description</b>	Fournisseur du titre restaurant
<b>Format</b>	SODEXO
<b>Valeur(s) possible(s)</b>	GROUPEUP
	NATIXIS (pour les cartes BIMPLI)
<b>Complément</b>	Champ présent uniquement si brand est égale à CO
<b>Exemple</b>	SODEXO

<b>Champ</b>	<b>soldecompte</b>
<b>Description</b>	Solde du compte du payeur
<b>Format</b>	Un nombre entier
<b>Valeur(s) possible(s)</b>	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}
<b>Complément</b>	Champ présent uniquement si brand est égale à CO

<b>Exemple</b>	95.25EUR
----------------	----------

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

<b>Champ</b>	<b>authentification</b>
<b>Description</b>	Document JSON/UTF-8 encodé en base 64 contenant les informations liées à l'authentification du client notamment pour 3DSecure.
<b>Complément</b>	<a href="#">Lien</a> vers la structure du document.

Champ	usage
Description	Précise le type de carte utilisée pour réaliser la transaction
Format	credit : carte de crédit ou à débit différé
Valeur(s) possible(s)	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	particulier : compte d'un particulier
Valeur(s) possible(s)	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	oui
Valeur(s) possible(s)	non
Exemple	oui

Champ	motifrefus
Description	Motif du refus de la demande de paiement
Format	<b>Appel Phonie</b> : la banque du client demande des informations complémentaires
Valeur(s) possible(s)	<b>Refus</b> : la banque du commerçant ou du client refuse d'accorder l'autorisation <b>Interdit</b> : la banque du commerçant ou du client refuse d'accorder l'autorisation <b>filtrage</b> : la demande de paiement a été bloquée par le paramétrage de filtrage que le commerçant a mis en place dans son Module Prévention Fraude <b>scoring</b> : la demande de paiement a été bloquée par le paramétrage de scoring que le commerçant a mis en place dans son Module Prévention Fraude <b>3DSecure</b> : 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	<b>Refus banque</b> : la banque du client ou du commerçant refuse d'accorder l'autorisation
Valeur(s) possible(s)	<b>Refus emetteur</b> : la banque du client refuse d'accorder l'autorisation

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

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

<b>Champ</b>	<b>bincb</b>
<b>Description</b>	Code BIN de la banque du porteur de la carte de paiement
<b>Format</b>	Le format dépend de la longueur du numéro de carte :
<b>Valeur(s) possible(s)</b>	<ul style="list-style-type: none"> <li>- 8 chiffres pour les numéros de cartes ayant une longueur de 16 chiffres ou plus</li> <li>- 6 chiffres suivis de 2 caractères 'X' pour les numéros de carte ayant une longueur de moins de 16 chiffres</li> </ul>
<b>Exemple</b>	12345678 123456XX
<b>Complément</b>	Uniquement en cas de souscription du module prévention fraude

<b>Champ</b>	<b>hpancb</b>
<b>Description</b>	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)
<b>Complément</b>	Uniquement en cas de souscription du module prévention fraude

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

<b>Champ</b>	<b>originetr</b>
<b>Description</b>	Code pays de l'origine de la transaction
<b>Format</b>	Norme ISO 3166-1

<b>Complément</b>	Uniquement en cas de souscription du module prévention fraude
-------------------	---

<b>Champ</b>	<b>montantech</b>
<b>Description</b>	Montant de l'échéance en cours
<b>Complément</b>	Uniquement dans le cas du paiement fractionné

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

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

<b>Champ</b>	<b>filtragecause</b>
<b>Description :</b>	Numéros des types de filtres bloquant le paiement (cf. tableau « Retours Module Prévention Fraude – détails » <a href="#">ci-dessous</a> )
<b>Format</b>	1 : Adresse IP
<b>Valeur(s) possible(s)</b>	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
<b>Complément</b>	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.

<b>Champ</b>	<b>filtragevaleur</b>
<b>Description</b>	Données ayant engendré le blocage
<b>Complément</b>	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.

<b>Champ</b>	<b>filtrage_etat</b>
<b>Description</b>	Indique, s'il est présent uniquement, que le filtrage est en mode « information ». information : Mode information du filtrage
<b>Complément</b>	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.

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

<b>Champ</b>	<b>cbmasquee</b>
<b>Description</b>	Le numéro de carte tronqué en conformité avec PCI DSS
<b>Format</b>	Le format dépend de la longueur du numéro de carte :
<b>Valeur(s) possible(s)</b>	<ul style="list-style-type: none"> <li>- 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</li> <li>- 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</li> </ul>
<b>Exemple</b>	12345678*****12 123456*****123
<b>Complément</b>	Présent systématiquement pour les paiements par carte. Absent pour les paiements sans saisie de carte sur la page Monetico Paiement (Paypal ...)

<b>Champ</b>	<b>modepaiement</b>
<b>Description</b>	Moyen de paiement utilisé
<b>Format</b>	CB, paypal, 1euro, 3xcb, 4xcb, 5-10-12xcb, loan, paylater, lyfpay
<b>Valeur(s) possible(s)</b>	
<b>Complément</b>	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

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

<b>Champ</b>	<b>statutDébrayageAuthentification</b>
<b>Description :</b>	Indique le statut de débrayage de l'authentification du porteur
<b>Format</b> <b>Valeur(s) possible(s)</b>	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
<b>Complément</b>	Uniquement si les options de débrayage par montant ou formulaires sont activées.

<b>Champ</b>	<b>nomcartesequestree</b>
<b>Description :</b>	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
<b>Format</b> <b>Valeur(s) possible(s)</b>	[0-9A-Za-z_,\.\- ]{1,20}
<b>Complément</b>	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%2e75EU
R&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&
&numauto=010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E
0F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbma
squee=12345678*****90&modepaiement=CB&authentication=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%2e75EU
R&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0
4&texte-libre=LeTexteLibre&code-
retour=paiement&cvx=oui&vld=1208&brand=VI&
numauto=010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0
F2C2CADBFC1C00B004B7C45&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=70156D2CFF27A9B8AAE5AFE590D9CFCAAF9BDC&  
texte-libre=Ceci+est+un+test%2c+ne+pas+tenir+compte%2e&code-  
retour=Annulation&cvx=oui&vld=0912&brand=MC&motifrefus=filtrage&moti  
frefusautorisation=-  
&originecb=FRA&bincb=12345678&hpancb=764AD24CFABBB818E8A7DC61D4D6B4B  
89EA837ED&ipclient=10%2e45%2e166%2e76&originetr=inconnue&filtragecau  
se=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%2e75EU  
R&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b0  
4&texte-libre=LeTexteLibre&code-  
retour=paiement&cvx=oui&vld=1208&brand=VI&  
numauto=010101&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0  
F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbenr  
egistree=1&nomcartesequestree=VISA%20CIC&cbmasquee=12345678\*\*\*\*\*90&  
modepaiement=CB&authentification=[ewoJIn \(...\) KfQo=](#)

### 1.5.3.2 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](#).

#### 1.5.3.2.1 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.

### 1.5.3.2.2 Spécificités pour l'environnement de test dit « sandbox »

Afin de garantir la conformité de votre implémentation ainsi que la gestion correcte de tout nouveau paramètre futur envoyé par Monetico Paiement, un champ ayant un nom et une valeur aléatoires est généré et ajouté automatiquement à l'interface « Retour » pour chaque paiement.

Ce champ aléatoire est présent uniquement pour les paiements réalisés dans l'environnement de test dit « sandbox ».

Pour calculer le sceau MAC, référez-vous à la [documentation en annexe](#).

### 1.5.3.3 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	<code>version=2&lt;LF&gt;</code> <code>cdr=0&lt;LF&gt;</code>
Non	<code>version=2&lt;LF&gt;</code> <code>cdr=1&lt;LF&gt;</code>

**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 Aides à l'installation

### 2.1 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).

### 2.2 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%2e75EUR&reference=ref0001&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-libre=LeTexteLibre&code-retour=Annulation&cvx=oui&vld=1208&brand=VI&status3ds=1&motifrefus=Refus&originecb=FRA&bincb=12345678&hpancb=74E94B03C22D786E0F2C2CADBFC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbmasquee=12345678*****90&modepaiement=CB&authentication=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%2e75EUR&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=12754C03C22D786E0F2C2CADBFC1C00A25df6322&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbmasquee=12345678*****90&modepaiement=CB&authentication=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.

## 2.3 Les problèmes les plus fréquents

### 2.3.1 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 ».

#### 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.

### 2.3.2 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. »

#### 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 crédit

#### 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.

### 2.3.3 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.

### 2.3.4 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

### 2.3.5 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.

### 3 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](mailto:centrecom@e-i.com)
  - CIC : [centrecom@e-i.com](mailto: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.

## 4 Annexes

### 4.1 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	&	<code>&amp;amp;</code>
Signe inférieur	<	<code>&amp;lt;</code>
Signe supérieur	>	<code>&amp;gt;</code>
Guillemets	"	<code>&amp;quot;</code> ou <code>&amp;#x22;</code>
Apostrophe	'	<code>&amp;#x27;</code>

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).

## 4.2 Contrainte d'encodage

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

Tous les encodages ou décodages des paramètres de nos échanges doivent suivre la RFC 3986.

## 4.3 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

Pour vos appels à nos services, par exemple en phase « Aller » de l'appel à la page de paiement, le sceau doit prendre en compte tous les paramètres envoyés — valorisés ou non — **reconnus par la plateforme**, et uniquement ceux-ci.

Pour les réponses de nos services (interface « Retour »), il est important d'intégrer dans votre vérification du sceau **tous les paramètres envoyés par notre serveur**, y compris ceux que votre serveur n'utilise pas ou ne connaît pas. Pour rappel, le nom et la valeur de chaque paramètre devront être décodés en respectant les spécifications de la RFC 3986 avant d'être intégrés à ce calcul.

Ex : si un paramètre contient la chaîne « %2B » dans son nom ou sa valeur, il faudra décoder cette chaîne pour obtenir le caractère « + » avant d'effectuer le calcul du sceau.

### 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](#).

### 4.3.1 Exemples de chaînes permettant le calcul du sceau

#### 4.3.1.1 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"
  }
}
```



#### 4.3.1.2 Phase retour

Paie ment immé diat, différé, partiel ou récurrent avec inscription au module préven tion fraude et à l'option 3D Secure

TPE=1234567\*authentification=[ewoJln\(...\)](#)KfQo=\*bincb=12345678\*brand=VI\*cbmasquee=12345678\*  
 \*\*\*\*\*90\*code-  
 retour=paie ment\*cvx=oui\*date=05/12/2006\_a\_11:55:23\*ecard=non\*hpancb=74E94B03C22D786E0F2  
 C2CADBFC1C00B004B7C45\*ipclient=127.0.0.1\*modepaiement=CB\*montant=62.75EUR\*numauto=0  
 10101\*originecb=FRA\*originetr=FRA\*reference=ABERTYP00145\*texte-  
 libre=LeTexteLibre\*typecompte=inconnu\*usage=credit\*version=3.0\*vld=1208

Paie ment fractionné avec inscription au module préven tion fraude et à l'option 3D Secure

TPE=1234567\*authentification=[ewoJln\(...\)](#)KfQo=\*bincb=12345678\*brand=VI\*cbmasquee=12345678\*  
 \*\*\*\*\*90\*code-  
 retour=paie ment\*cvx=oui\*date=05/12/2006\_a\_11:55:23\*ecard=non\*hpancb=74E94B03C22D786E0F2  
 C2CADBFC1C00B004B7C45\*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

Paie ment bloqué par le module préven tion fraude avec l'option 3D Secure

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=C  
 B\*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

Paie ment avec l'option paie ment express et inscription au module préven tion fraude et à l'option 3D Secure

TPE=1234567\*authentification=[ewoJln\(...\)](#)KfQo=\*bincb=12345678\*brand=VI\*cbenregistree=1\*cbmas  
 quee=12345678\*\*\*\*\*90\*code-  
 retour=paie ment\*cvx=oui\*date=05/12/2006\_a\_11:55:23\*ecard=non\*hpancb=74E94B03C22D786E0F2  
 C2CADBFC1C00B004B7C45\*ipclient=127.0.0.1\*modepaiement=CB\*montant=62.75EUR\*nomcartese  
 questree=VISA  
 CIC\*numauto=010101\*originecb=FRA\*originetr=FRA\*reference=ABERTYP00145\*texte-  
 libre=LeTexteLibre\*typecompte=inconnu\*usage=credit\*version=3.0\*vld=1208

## 4.4 Détail du document JSON « contexte\_commande »

### 4.4.1 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
<b>billing</b>	Adresse de facturation	Obligatoire	<a href="#">lien</a>
<b>shipping</b>	Adresse de livraison	Obligatoire si applicable	<a href="#">lien</a>
<b>shoppingCart</b>	Panier client	Optionnelle	<a href="#">lien</a>
<b>client</b>	Informations client	Optionnelle	<a href="#">lien</a>

#### 4.4.2 Détail de l'objet « billing »

Champ JSON	Présence	Type JSON	Détail
civility	Optionnelle	Chaîne	<a href="#">lien</a>
name	Optionnelle	Chaîne	<a href="#">lien</a>
firstName	Optionnelle	Chaîne	<a href="#">lien</a>
lastName	Optionnelle	Chaîne	<a href="#">lien</a>
middleName	Optionnelle	Chaîne	<a href="#">lien</a>
address	Optionnelle	Chaîne	<a href="#">lien</a>
addressLine1	Obligatoire	Chaîne	<a href="#">lien</a>
addressLine2	Optionnelle	Chaîne	<a href="#">lien</a>
addressLine3	Optionnelle	Chaîne	<a href="#">lien</a>
city	Obligatoire	Chaîne	<a href="#">lien</a>
postalCode	Obligatoire	Chaîne	<a href="#">lien</a>
country	Obligatoire	Chaîne	<a href="#">lien</a>
stateOrProvince	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
countrySubdivision	Optionnelle	Chaîne	<a href="#">lien</a>
email	Optionnelle	Chaîne	<a href="#">lien</a>
phone	Optionnelle	Chaîne	<a href="#">lien</a>
mobilePhone	Optionnelle	Chaîne	<a href="#">lien</a>
homePhone	Optionnelle	Chaîne	<a href="#">lien</a>
workPhone	Optionnelle	Chaîne	<a href="#">lien</a>

#### 4.4.3 Détail de l'objet « shipping »

Champ JSON	Présence	Type JSON	Description
civility	Optionnelle	Chaîne	<a href="#">lien</a>
name	Optionnelle	Chaîne	<a href="#">lien</a>
firstName	Optionnelle	Chaîne	<a href="#">lien</a>
lastName	Optionnelle	Chaîne	<a href="#">lien</a>
address	Optionnelle	Chaîne	<a href="#">lien</a>
addressLine1	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
addressLine2	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
addressLine3	Optionnelle	Chaîne	<a href="#">lien</a>
city	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
postalCode	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
country	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
stateOrProvince	Obligatoire si applicable	Chaîne	<a href="#">lien</a>
countrySubdivision	Optionnelle	Chaîne	<a href="#">lien</a>
email	Optionnelle	Chaîne	<a href="#">lien</a>
phone	Optionnelle	Chaîne	<a href="#">lien</a>
shipIndicator	Optionnelle	Chaîne	<a href="#">lien</a>
deliveryTimeframe	Optionnelle	Chaîne	<a href="#">lien</a>
firstUseDate	Optionnelle	Chaîne	<a href="#">lien</a>
matchBillingAddress	Optionnelle	Booléen	<a href="#">lien</a>

#### 4.4.4 Détail de l'objet « shoppingCart »

Champ JSON	Présence	Type JSON	Description
giftCardAmount	Optionnelle	Nombre	<a href="#">lien</a>
giftCardCount	Optionnelle	Nombre	<a href="#">lien</a>
giftCardCurrency	Optionnelle	Chaîne	<a href="#">lien</a>
preOrderDate	Optionnelle	Chaîne	<a href="#">lien</a>
preorderIndicator	Optionnelle	Booléen	<a href="#">lien</a>
reorderIndicator	Optionnelle	Booléen	<a href="#">lien</a>
shoppingCartItems	Optionnelle	Tableau d'objets	<a href="#">lien</a>

##### 4.4.4.1 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	<a href="#">lien</a>
description	Optionnelle	Chaîne	<a href="#">lien</a>
productCode	Optionnelle	Chaîne	<a href="#">lien</a>
imageURL	Optionnelle	Chaîne	<a href="#">lien</a>
unitPrice	Obligatoire	Nombre	<a href="#">lien</a>
quantity	Obligatoire si applicable	Nombre	<a href="#">lien</a>
productSKU	Optionnelle	Chaîne	<a href="#">lien</a>
productRisk	Optionnelle	Chaîne	<a href="#">lien</a>

#### 4.4.5 Détail de l'objet « client »

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

#### 4.4.6 Description des attributs

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

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

<b>Attribut</b>	<b>addressLine1</b>
<b>Description</b>	Contient le numéro et le nom de la rue
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 50 caractères

<b>Attribut</b>	<b>addressLine2</b>
<b>Description</b>	Contient le numéro et le nom de la rue
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 50 caractères

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

<b>Attribut</b>	<b>authenticationMethod</b>
<b>Description</b>	Méthode d'authentification du client sur le site commerçant
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	« 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	<b>authenticationTimestamp</b>
Description	Date et heure UTC de l'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 (ISO 8601)

Attribut	<b>birthCity</b>
Description	Ville de naissance
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

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

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

Attribut	<b>birthdate</b>
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	<b>birthLastName</b>
Description	Nom de naissance
Format	Chaîne
Restrictions	Jusqu'à 45 caractères

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

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

<b>Attribut</b>	<b>city</b>
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 50 caractères
<b>Description</b>	Ville Peut contenir le CEDEX.

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

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

<b>Attribut</b>	<b>countrySubdivision</b>
<b>Description</b>	Code géographique de l'entité du pays
<b>Format</b>	Chaîne
<b>Restrictions</b>	ISO 3166-2
<b>Aide</b>	<a href="https://en.wikipedia.org/wiki/ISO_3166-2">https://en.wikipedia.org/wiki/ISO_3166-2</a> <a href="https://en.wikipedia.org/wiki/ISO_3166-2:FR">https://en.wikipedia.org/wiki/ISO_3166-2:FR</a>

Attribut	<b>deliveryTimeframe</b>
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	<b>description</b>
Description	Description d'un article.
Format	Chaîne
Restrictions	Jusqu'à 2048 caractères.

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

Attribut	<b>firstName</b>
Description	Prénom
Format	Chaîne
Restrictions	Jusqu'à 45 caractères

Attribut	<b>firstUseDate</b>
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	<b>giftCardAmount</b>
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

<b>Attribut</b>	<b>giftCardCount</b>
<b>Description</b>	Nombre de cartes cadeaux achetées
<b>Format</b>	Nombre
<b>Restrictions</b>	Nombre entier Maximum de 2 chiffres utiles

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

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

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

<b>Attribut</b>	<b>last24HoursTransactions</b>
<b>Format</b>	Entier positif ou nul
<b>Description</b>	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.

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

Attribut	<b>lastAccountModification</b>
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	<b>lastName</b>
Description	Nom de famille.
Format	Chaîne
Restrictions	Jusqu'à 45 caractères.

Attribut	<b>lastPasswordChange</b>
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	<b>lastYearTransactions</b>
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	<b>matchBillingAddress</b>
Description	Indique si les adresses d'expédition ou de facturation sont identiques.
Format	Booléen

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

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

<b>Attribut</b>	<b>name</b>
<b>Description</b>	Nom et prénom.
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 45 caractères

<b>Attribut</b>	<b>nationalIDNumber</b>
<b>Description</b>	Numéro d'une pièce d'identité.
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 255 caractères

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

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

<b>Attribut</b>	<b>postalCode</b>
<b>Description</b>	Code postal
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 10 caractères

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

<b>Attribut</b>	<b>preorderIndicator</b>
<b>Description</b>	Indique s'il s'agit d'une précommande.
<b>Format</b>	Booléen

<b>Attribut</b>	<b>priorAuthenticationMethod</b>
<b>Description</b>	Mécanisme utilisé pour l'authentification du porteur lors de son dernier paiement sur le site commerçant.
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	« 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

<b>Attribut</b>	<b>priorAuthenticationTimestamp</b>
<b>Description</b>	Date et heure UTC de la précédente authentification du client sur le site commerçant.
<b>Format</b>	Chaîne
<b>Restrictions</b>	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

<b>Attribut</b>	<b>productCode</b>
<b>Description</b>	Indique le type de produit.
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	« adult_content » : contenu pour adulte « coupon » : bon de réduction appliqué à la commande « default » : valeur par défaut (si aucun autre code ne convient) « electronic_good » : biens électroniques (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

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

<b>Attribut</b>	<b>productSKU</b>
<b>Description</b>	Identifiant que le commerçant donne à un article.
<b>Format</b>	Chaîne
<b>Restrictions</b>	Jusqu'à 255 caractères

<b>Attribut</b>	<b>quantity</b>
<b>Format</b>	Nombre
<b>Restrictions</b>	Nombre entier
<b>Description</b>	Exprime une quantité (par exemple un nombre d'articles)

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

<b>Attribut</b>	<b>shipIndicator</b>
<b>Format</b>	Chaîne
<b>Description</b>	Moyen d'expédition retenu.
<b>Valeurs possibles</b>	« digital_goods »: Biens numériques (pas d'expédition). « travel_and_event »: Transports ou événements (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.

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

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

<b>Attribut</b>	<b>suspiciousAccountActivity</b>
<b>Description</b>	Permet d'indiquer si des activités suspectes sur le compte du client ont été relevées par le commerçant.
<b>Format</b>	Booléen

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

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

#### 4.5 Détail du document JSON « authentication »

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
<b>status</b>	Résultat de l'authentification	<a href="#">lien</a>
<b>protocol</b>	Protocole utilisé	<a href="#">lien</a>
<b>version</b>	Version du protocole	<a href="#">lien</a>
<b>details</b>	Détails spécifiques au protocole et à la version	<a href="#">lien</a>

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.

##### 4.5.1 Détail de l'objet « details »

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

##### 4.5.2 Description des attributs

Attribut	status
<b>Description</b>	Indique le résultat de l'authentification
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	<ul style="list-style-type: none"> <li>« authenticated » : L'authentification est effectuée avec succès.</li> <li>« authentication_not_performed » : L'authentification n'a pas pu être complétée (problème technique ou autre).</li> <li>« not_authenticated » : L'authentification a échoué.</li> <li>« authentication_rejected » : L'authentification a été refusée par l'émetteur.</li> <li>« 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)</li> <li>« not_enrolled » : La carte n'est pas enrôlée au 3DS</li> <li>« disabled » : Dans le cas de l'usage de l'option 3DSecure débrayable</li> </ul>

<b>Attribut</b>	<b>protocol</b>
<b>Description</b>	Protocole utilisé pour l'authentification
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	3DSecure

<b>Attribut</b>	<b>version</b>
<b>Description</b>	Version du protocole
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	2.1.0 2.2.0

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

<b>Attribut</b>	<b>VERes</b>
<b>Description</b>	Vérification de l'enrôlement d'une carte à 3DSecure 1.X.
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	« 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
<b>Présence</b>	Dans le cadre de 3DSecure 1.X uniquement.

<b>Attribut</b>	<b>PARes</b>
<b>Description</b>	Résultat de l'authentification 3DSecure
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	« 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.
<b>Présence</b>	Dans le cadre de 3DSecure 1.X uniquement.

Attribut	<b>ARes</b>
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	Chaîne
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. « I » : Purement informationnel : accusé de réception signifiant que l'exemption demandée par le commerçant a bien été prise en compte.
Présence	Dans le cadre de 3DSecure 2.X uniquement.

Attribut	<b>CRes</b>
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	<b>merchantPreference</b>
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)

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

<b>Attribut</b>	<b>status3DS</b>
<b>Description</b>	Indicateur d'échange 3DSecure 1.X
<b>Format</b>	Entier
<b>Valeurs possibles :</b>	-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
<b>Présence</b>	Dans le cadre de 3DSecure 1.X uniquement.

<b>Attribut</b>	<b>disablingReason</b>
<b>Description</b>	Couplé à l'option de 3DSecure débrayable. Indique le motif du débrayage.
<b>Format</b>	Chaîne
<b>Valeurs possibles</b>	commerçant : 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
<b>Présence</b>	Lorsqu'un débrayage a été effectué uniquement.

### 4.5.3 Example

Ci-dessous un exemple de document JSON authentication 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 :

eyAgCiAglCJzdGF0dXMiOiJhdXRoZW50aWNhdGVkIiwKICAgInByb3RvY29sljoiM0RTZWN1cmUiLaogICAid  
mVyc2l2biil6ljluMS4wliwKICAgImRldGFpbHMiOnsIiwKICAgIAibGhYmlsaXR5U2hpZnQiOiJJZliwKICAgICAgl  
lkFSZXMiOiJDIiwKICAgICAglkNSZXMiOiJJZliwKICAgICAglm1cmNoYW50UHJlZmVyZW5jZSI6Im5vX3ByZWZ  
lc3VuY2UiLaogICAglCAidHJhbnNhY3Rpb25JRCl6ljU1NWJkOWQ5LTFjZjEtNGJhOC1iMzdlLTFlOTZiYzhinJ  
IyYSIKICAfQp9Cg==

## 4.6 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.

3D Secure est passé de la version 1 à la version 2 en 2019 et Monetico Paiement utilise actuellement la version 2.2.0.

#### 4.6.1 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 ( <a href="#">lien</a> )	<a href="#">lien</a>
Le protocole 3DSecure s'est finalisé Le porteur a été authentifié par la banque émettrice sans passer par sa page d'authentification ACS (frictionless).	authenticated ( <a href="#">lien</a> )	<a href="#">lien</a>

Le transfert de responsabilité est différent en fonction du souhait exprimé par le commerçant : voir le tableau sur le liability shift pour les détails.		
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)	<b>authentication_attempted</b> ( <a href="#">lien</a> )	<a href="#">lien</a>
Le protocole 3DSecure a été initié. La banque du porteur considère que ce paiement est risqué et refuse l'authentification.	<b>not_authenticated</b> ( <a href="#">lien</a> )	<a href="#">lien</a>
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, ...)	<b>not_authenticated</b> ( <a href="#">lien</a> )	<a href="#">lien</a>
Le protocole 3DSecure a été initié. Suite à un problème technique, il n'a pu aboutir.	<b>authentication_not_performed</b> ( <a href="#">lien</a> )	<a href="#">lien</a>
Le protocole 3DSecure s'est déclenché mais un problème technique est survenu empêchant l'authentification du porteur par l'émetteur.	<b>authentication_not_performed</b> ( <a href="#">lien</a> )	<a href="#">lien</a>
Le protocole 3DSecure a été initié. La banque du porteur refuse l'authentification.	<b>authentication_rejected</b> ( <a href="#">lien</a> )	<a href="#">lien</a>
La carte n'est pas enrôlée au protocole 3DSecure.	<b>not_enrolled</b> ( <a href="#">lien</a> )	<a href="#">lien</a>

<b>Status</b>	<b>authenticated</b> ( <a href="#">lien</a> )
<b>Scénario</b>	Le protocole 3DSecure s'est finalisé Le porteur a été authentifié par la banque émettrice via sa page d'authentification ACS.
<b>Interface retour 3DS v2</b>	<pre>{   "status": "authenticated",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique&gt;",     "ARes": "C",     "CRes": "Y",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

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

Interface retour 3DS v2	<pre>{   "status": "authenticated",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique&gt;",     "ARes": "Y",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>
Status	<b>authentication_attempted</b> ( <a href="#">lien</a> )
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	<pre>{   "status": "authenticated",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique&gt;",     "ARes": "C",     "CRes": "Y",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

Status	<b>not_authenticated</b> ( <a href="#">lien</a> )
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": "&lt;Voir tableau spécifique&gt;",     "ARes": "N",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

Status	<b>not_authenticated</b> ( <a href="#">lien</a> )
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	<pre>{   "status": "not_authenticated",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique",     "ARes": "C",     "CRes": "N",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

Status	<b>authentication_not_performed</b> ( <a href="#">lien</a> )
Scénario	Le protocole 3DSecure a été initié. Suite à un problème technique, il n'a pu aboutir.
Interface retour 3DS v2	<pre>{   "status": "authentication_not_performed",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique&gt;",     "ARes": "U",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

Status	<b>authentication_not_performed</b> ( <a href="#">lien</a> )
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	<pre>{   "status": "authentication_not_performed",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique&gt;",     "ARes": "C",     "CRes": "U",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

<b>Status</b>	<b>authentication_rejected (<a href="#">lien</a>)</b>
<b>Scénario</b>	Le protocole 3DSecure a été initié. La banque du porteur refuse l'authentification.
<b>Interface retour 3DS v2</b>	<pre>{   "status": "authentication_rejected",   "protocol": "3DSecure",   "version": "2.1.0",   "details": {     "liabilityShift": "&lt;Voir tableau spécifique ",     "ARes": "R",     "merchantPreference": "&lt;souhait exprimé phase Aller&gt;",     "transactionID": "555bd9d9-1cf1-4ba8-b37c-1a96bc8b603a"   } }</pre>

<b>Status</b>	<b>not_enrolled (<a href="#">lien</a>)</b>
<b>Scénario</b>	La carte n'est pas enrôlée au protocole 3DSecure.
<b>Interface retour 3DS v2</b>	<pre>{   "status": "not_enrolled",   "protocol": "3DSecure",   "version": "2.1.0" }</pre>

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.

#### 4.6.1.1 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	<b>authenticated</b>	Emetteur
	<b>not_authenticated</b>	Refus de la transaction
Non - Pas d'authentification via l'ACS de la banque du porteur	<b>authenticated (frictionless)</b>	Commerçant
	<b>authentication_attempted</b> (ARes = A)	Dépendant du réseau et du type de carte
	<b>authentication_not_performed</b> (ARes = U)	Dépendant du réseau et du type de carte
	<b>authentication_rejected</b> (ARes = R)	Refus de la transaction
	<b>not_enrolled</b>	Commerçant

#### 4.6.1.2 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	<b>authenticated</b>	Emetteur
	<b>not_authenticated</b>	Refus de la transaction
Non - Pas d'authentification via l'ACS de la banque du porteur	<b>authenticated</b> (frictionless)	Emetteur
	<b>authentication_attempted</b> (ARes = A)	Dépendant du réseau et du type de carte
	<b>authentication_not_performed</b> (ARes = U)	Dépendant du réseau et du type de carte
	<b>authentication_rejected</b> (ARes = R)	Refus de la transaction
	<b>not_enrolled</b>	Commerçant

## 4.7 URL des services

### 4.7.1 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.

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

- <https://p.monetico-services.com/test/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/>

### 4.7.2 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](mailto:centrecom@e-i.com), vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

- <https://p.monetico-services.com/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.**

## 4.8 Spécificités Cofidis

### 4.8.1 Redirection automatique

Dans le cadre d'un paiement Cofidis, sous certains protocoles (actuellement loan), il est possible qu'un paiement soit mis en attente d'une réponse de Cofidis.

Si la redirection automatique est demandée et qu'un tel scénario se produit, l'url de redirection qui sera utilisée sera l'url\_retour\_ok et le code-retour de l'interface retour est « attente\_partenaire ».