Monetico Paiement

Paiement sécurisé sur Internet

Demande de paiement par API

EURO INFORMATION

SOMMAIRE

1 Introduction

1.1 Principe

Le but du service de demande de paiement par API « paymentservice » via Internet est de permettre aux commerçants de traiter leurs paiements VàD (Vente à Distance) de façon sécurisée via Internet. Le serveur sécurisé Monetico paiement effectue la vérification de la validité des informations bancaires transmises avant d'accorder l'autorisation de paiement et confirme automatiquement le résultat de la demande de paiement à l'application du commerçant.

L'application du commerçant dialogue directement avec le serveur sécurisé Monetico Paiement. Les échanges se passent en mode sécurisé : l'usage de HTTPS ainsi que le protocole de sécurisation des échanges TLS V1.2 garantissant la confidentialité des informations fournies par le commerçant.

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

1.2 Protocole 3D Secure

L'authentification des porteurs de cartes bancaires lors d'un acte de paiement se fait par le biais du protocole 3D Secure. Celui-ci permet de s'assurer que la personne ayant saisie 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.

Historiquement, cette phase d'authentification était basée sur la version 1 du protocole sécurisé de communication entre les différents acteurs 3D Secure. Courant de l'année 2019, la version 2.1 de ce protocole 3D Secure est entrée en application. Celle-ci est maintenant la version du protocole 3D Secure par défaut. En Octobre 2022, le protocole 3D Secure V1 sera définitivement obsolète.

L'interface de demande de paiement fournie par la plateforme Monetico Paiement prend en compte les différentes versions du protocole 3D Secure afin de fournir une séquence de flux unifiée.

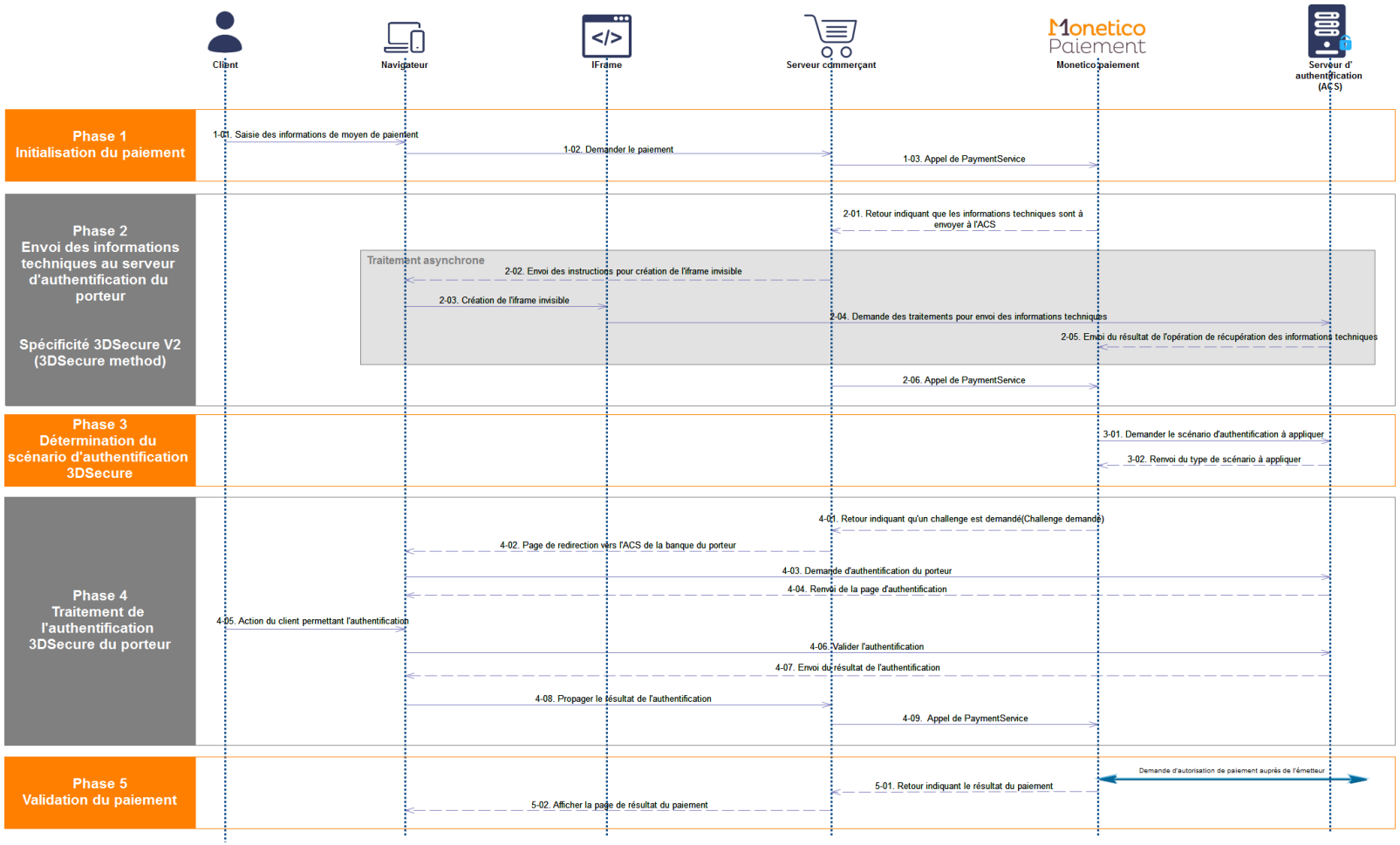
1.3 Organisation du document

Le document est découpé en plusieurs sections :

- La section « 2 Scénario de paiement » donne les principes généraux du service de demande de paiement par API et les différents échanges de flux devant être effectués.
- La section « 3 Spécifications des messages vers la plateforme Monetico paiement » se focalise sur les échanges techniques entre le serveur du commerçant et la plateforme Monetico paiement
- La section « 4 Traitement du retour du service de paiement lorsqu'une action est demandée au commerçant » se concentre sur les traitements devant être effectués par le serveur commerçant en fonction des retours effectués par la plateforme Monetico paiement. En particulier, une préconisation d'implémentation est proposée pour les échanges entre le serveur commerçant et le serveur d'authentification (ACS) de la banque du porteur.
- La section « 5 Annexes » aborde différents points donnant des informations supplémentaires

2 Scénario de paiement

Le diagramme ci-dessous décrit le scénario d'une demande de paiement. En orange, les étapes obligatoires. En gris, les étapes facultatives dépendantes du scénario d'authentification du porteur (3D Secure) devant être appliqué sur le paiement.



Phase 1 : Initialisation du paiement

Descriptif des échanges

- 1-01 : le client saisit ses informations de carte de paiement
- 1-02 : le client valide sa saisie.
- 1-03 : une requête au service de demande de paiement par API est effectué

Retour(s) possible(s)

- La carte de paiement demande une authentification via le protocole 3D Secure V2 :
  - La banque de client souhaite recevoir les informations de l'environnement technique du client
    la prochaine étape à prendre en compte : **Phase 2 : Envoi des informations techniques au serveur d'authentification du porteur**
  - La banque de client ne souhaite pas recevoir les informations de l'environnement technique du client
    la prochaine étape à prendre en compte : **Phase 3 : Détermination du scénario d'authentification 3D Secure**

Intégration à réaliser

Intégration	Etapes
Actions à réaliser côté serveur marchand	étape 1-03
Actions à réaliser côté Javascript	-

Phase 2 : Envoi des informations techniques au serveur d'authentification du porteur

Descriptif des échanges

- 2-01 : le retour du service de demande de paiement par API indique que les informations techniques sont à envoyer au serveur d'authentification du porteur
- De 2-02 à 2-05 : un appel au service de réception des informations techniques du serveur d'authentification du porteur est effectué
- 2-06 : une requête au service de demande de paiement par API est effectué pour signaler que l'envoi des informations techniques a été effectué

Retour(s) possible(s)

La prochaine étape à prendre en compte : **Phase 3 : Détermination du scénario d'authentification 3D Secure**

Intégration à réaliser

Intégration	Etapes
Actions à réaliser côté serveur marchand	étape 2-01
Actions à réaliser côté Javascript	étapes 2-02 et 2-03

Phase 3 : Détermination du scénario d'authentification 3D Secure

Descriptif des échanges

- 3-01 : le serveur d'authentification du porteur est contacté
- 3-02 : En retour, celui-ci indique le type de scénario d'authentification 3D Secure à réaliser

Retour(s) possible(s)

En fonction du retour du serveur d'authentification du porteur, l'étape suivante change :

- La carte du porteur est éligibile à l'authentification 3D Secure et l'émetteur demande une authentification du porteur
  la prochaine étape à prendre en compte : **Phase 4 : Traitement de l'authentification 3D Secure du porteur**
- La carte du porteur n'est pas éligibile à l'authentification 3D Secure ou l'émetteur ne demande pas d'authentification du porteur
  la prochaine étape à prendre en compte : **Phase 5 : Validation du paiement**

Intégration à réaliser

Intégration	Etapes
Actions à réaliser côté serveur marchand	-
Actions à réaliser côté Javascript	-

Phase 4 : Traitement de l'authentification 3D Secure du porteur

Descriptif des échanges

- 4-01 : le retour de Service de demande de paiement par API indique que l'authenfication du porteur est à effectuer
- 4-02 : Redirection vers le serveur d'authentification de la banque du porteur
- De 4-03 à 4-07 : Etapes pour l'authentification du porteur de la carte de paiement
- 4-08 : Redirection vers le serveur du commerçant
- 4-09 : une requête au service de demande de paiement par API est effectué pour envoyer le résultat de l'authentification

Retour(s) possible(s)

La prochaine étape à prendre en compte : **Phase 5 : Validation du paiement**

Intégration à réaliser

Intégration	Etapes
Actions à réaliser côté serveur marchand	étapes 4-01 et 4-09
Actions à réaliser côté Javascript	-

Phase 5 : validation du paiement

Descriptif des échanges

- 5-01 : le retour de Service de demande de paiement par API indique la résultat du paiement
- 5-02 : la page de résultat du paiement est affichée

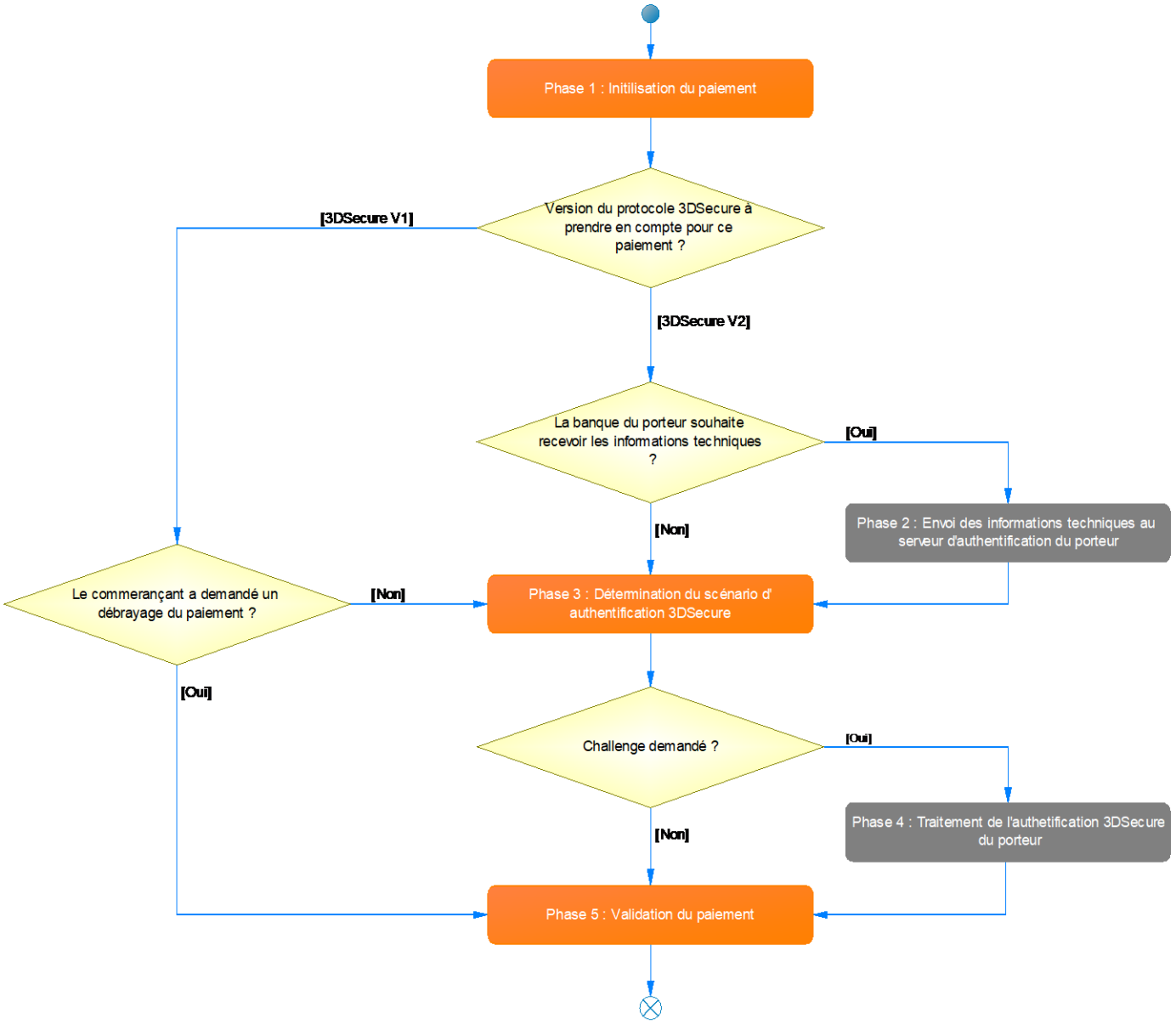
Retour(s) possible(s)

Le paiement est finalisé et la résultat du paiement est renvoyé : il n'y a pas d'étape suivante.

Intégration à réaliser

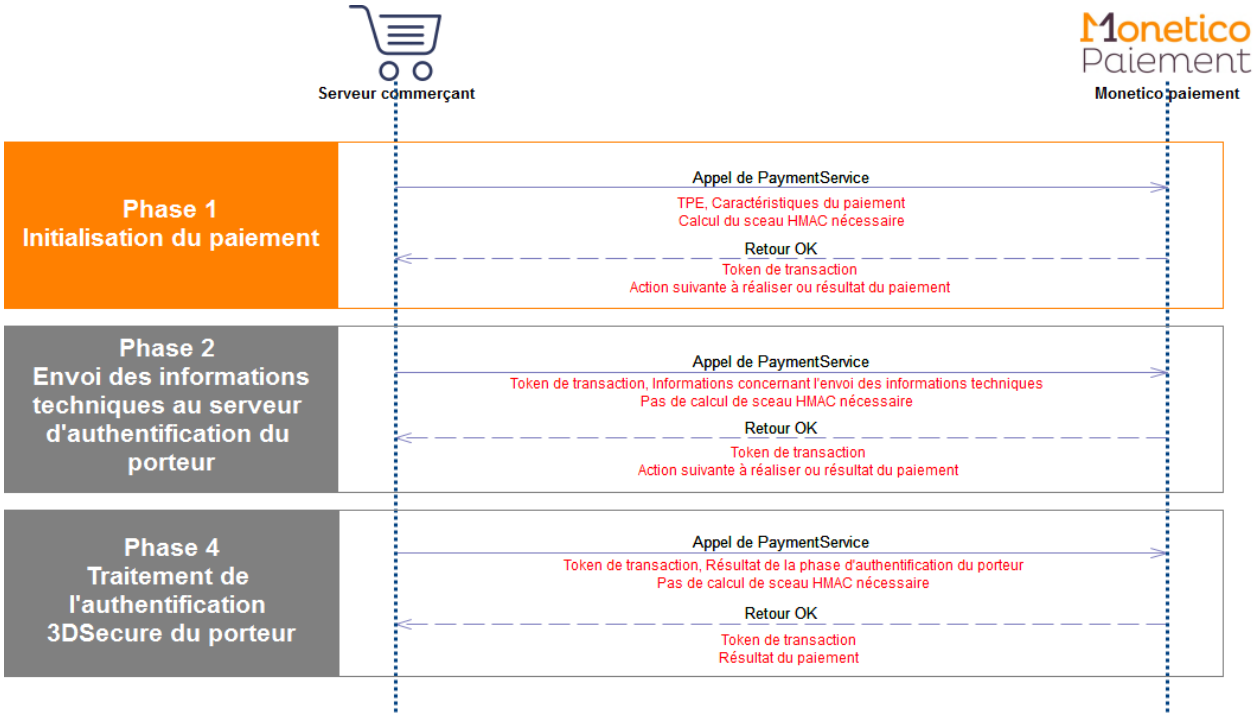
Intégration	Etapes
Actions à réaliser côté serveur marchand	étapes 5-01 et 5-02
Actions à réaliser côté Javascript	-

En résumé, l'enchainement des étapes d'un paiement se déroule de la manière suivante :



3 Spécifications des messages vers la plateforme Monetico paiement

Pour réaliser un paiement, de 1 à 3 échanges maximum entre le serveur du commerçant et le service de demande de paiement par API sont à prendre en compte. Le nombre d'échanges dépend du scénario du paiement :



Lors de la phase d'initialisation (Phase 1)

- En entrée : le TPE, les caractéristiques du paiement doivent être fournies
  Un calcul de sceau HMAC est nécessaire.
- En sortie : un token de transaction ainsi que l'action suivante à réaliser ou le résultat du paiement sont fournis. Le token de transaction sert pour tous les appels suivants pour ce paiement. L'action suivante permet d'indiquer au commerçant la suite du traitement à réaliser

Une fois que l'envoi des informations techniques au serveur d'authentification du porteur a été réalisé (phase 2)

- En entrée : le token de transaction et les informations concernant l'envoi des informations techniques doivent être fournis
  Aucun calcul de sceau HMAC est nécessaire.
- En sortie : un token de transaction, ainsi que l'action suivante à réaliser ou le résultat du paiement, sont fournis.

Une fois que la phase d'authentification du porteur a été effectuée (phase 4)
• En entrée : le token de transaction et le résultat de la phase d'authentification du porteur doivent être fournis Aucun calcul de sceau HMAC est nécessaire. • En sortie : un token de transaction, ainsi que l'action suivante à réaliser ou le résultat du paiement, sont fournis.

3.1 Sécurité des échanges

Les informations de la demande de paiement sont envoyées au serveur Monetico Paiement par un message HTTPS, en utilisant le protocole de sécurisation des échanges **TLS V1.2** uniquement.

3.2 Format des échanges

L'application du commerçant doit émettre une requête HTTP de type **POST** à destination du service de demande de paiement par API sur les serveurs de la banque.

Cette requête doit contenir certaines informations en en-tête, et son corps consiste en un document au format **JSON/UTF-8**.

3.3 Calcul du sceau HMAC

3.3.1 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 sécurisé Monetico Paiement, est indispensable pour utiliser le service de demande de paiement par API. Un lien permettant de télécharger cette clé de sécurité depuis le tableau de bord est envoyé par notre centre de support au commerçant.

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

La clé de sécurité est représentée de façon externe par 40 caractères hexadécimaux (par exemple : `0123456789ABCDEF0123456789ABCDEF01234567`). Cette représentation externe doit être convertie en une chaîne de 20 octets (représentation opérationnelle) avant utilisation.

3.3.2 Principe du calcul du sceau

Le sceau, à mettre dans le header 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 l'intégralité du corps de la requête HTTP.

Remarque : Les espaces, tabulations, ou retours à la ligne figurant dans le corps de la requête doivent être pris en compte pour le calcul du sceau MAC.

Un exemple de calcul de sceau MAC :

```
POST /test/paymentservice.cgi HTTP/1.1
Content-Type:application/json
MAC:3BB2E1BFE87A72380B2455C2F1C80D784DC02346
Host:payment-api.e-i.com
Accept-Encoding:gzip,
deflate
Connection:keep-alive
{
   "merchant_configuration":{
      "point_of_sale":"9000001",
      "version":"3.0",
      "language":"FR",
      "configuration":"emulation3d"
   },
   "order":{
      "date":"2019-09-11T18:29:10",
      "customer":{
         "mail":"customer@mail.com"
      },
      "context":{
         "billing":{
            "addressLine1":"7 rue du verger",
            "city":"Illkirch",
            "postalCode":"67400",
            "country":"FR"
         }
      }
   },
   "payment":{
      "transaction_initiator":"cardholder",
      "reference":"dfb44bc6-9d45-42e8-85a6-b98c2ab627a6",
      "payment_mean":{
         "account_number":"0000010000000002",
         "cvx":"123",
         "cardholdername":"Jean Dupont",
         "scheme":"VISA",
         "default_scheme":true,
         "expiry_date":"2035-12"
      },
      "amount":{
         "value":10001,
         "currency":"EUR",
         "exponent":2
      }
   }
}
```

En rouge, le MAC calculé en utilisant la clé décrite en section 3.3.1
En vert, un exemple des données à utiliser pour le calcul du sceau mac.

3.4 Environnements mis à disposition

3.4.1 Environnement de test (« sandbox »)

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

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

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

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

- https://payment-api.e-i.com/test/paymentservice.cgi

Le numéro de carte de paiement pilote le scénario joué pour un paiement. Le tableau suivant présente les numéros de carte de paiement à utiliser dans l'environnement « sandbox » pour les différents scénarii disponibles :

			3D Secure V2	
Numéro	**Scénario**	**Réseau carte**	**Paiement accepté**	**Paiement refusé**
1	La carte n'est pas enrôlée au 3D Secure	Visa	0000010000000021	0000010000000022
		Mastercard	0000030000000021	0000030000000022
2	L'authentification est effectuée avec succès sans challenge	Visa	0000010000000023	0000010000000024
		Mastercard	0000030000000023	0000030000000024
3	L'authentification est effectuée avec succès avec challenge	Visa	0000010000000025	0000010000000026
		Mastercard	0000030000000025	0000030000000026
4	L'authentification n'a pas pu être complétée (problème technique ou autre)	Visa		0000010000000027
		Mastercard		0000030000000027
5	Une tentative d'authentification a bien été effectuée. L'authentification n'a pas pu se faire mais une preuve a été générée (CAVV)	Visa	0000010000000028	
		Mastercard	0000030000000028	
6	L'authentification a échouée sans challenge	Visa		0000010000000029
		Mastercard		0000030000000029
7	L'authentification a échouée avec challenge	Visa		0000010000000030
		Mastercard		0000030000000030
8	L'authentification a été refusée par l'émetteur	Visa		0000010000000031
		Mastercard		0000030000000031

3.4.2 Environnement de production

Vous devez faire une demande auprès de l'assistance technique (voir Annexe 5.1) pour faire passer votre TPE en production.

Une fois le passage en production effectué, vous pourrez vous adresser au serveur de production, disponible à l'adresse suivante :

- https://payment-api.e-i.com/paymentservice.cgi

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

3.5 Appels au service de demande de paiement par API

3.5.1 Phase 1 : Initialisation du paiement

Lors de la phase d'initialisation du paiement, les données transmises doivent être inclure le calcul du sceau HMAC.

3.5.1.1 Les données d'en-tête

Les données attendues sont les suivantes :

Champ	Content-Type
Présence	Obligatoire
Description	Précise le format des échanges
Format Valeur(s) possible(s)	application/json; charset=utf-8

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(s)	f97861e0f3e296b7eece2cfd86dc46c43ac88049

3.5.1.2 Les données du corps

Lors de la phase d'initialisation du paiement, les caractéristiques du paiement doivent être fournies en entrée du service. Le corps de la requête est un document au format JSON/UTF-8. Il contient les informations suivantes :

Champ JSON	Type JSON	Présence	Détails
merchant_configuration	Objet	Obligatoire	lien
order	Objet	Obligatoire	lien
payment	Objet	Obligatoire	lien
authentication	Objet	Conditionnelle	lien

3.5.1.2.1 Objet « merchant_configuration »

L'objet « merchant_configuration » contient la configuration commerçant liée au contrat.

Champ JSON	Type JSON	Présence	Détails
point_of_sale	Chaîne	Obligatoire	lien
version	Chaîne	Obligatoire	lien
language	Chaîne	Obligatoire	lien
configuration	Chaîne	Obligatoire	lien

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

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

Champ	language
Présence	Obligatoire
Description	Code langue
Format Valeur(s) possible(s)	Choix parmi : DE EN ES FR IT JA NL PT SV
Exemple(s)	FR

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

3.5.1.2.2 Objet « order »

L'objet « order » véhicule les informations liées à la commande.

Champ JSON	Type JSON	Présence	Détails
date	Chaîne	Obligatoire	lien
customer	Objet	Optionnelle	lien
context	Objet	Obligatoire	lien

Champ	date
Présence	Obligatoire
Description	Date et heure locale de la demande
Format Valeur(s) possible(s)	Du type AAAA-MM-JJTHH:mm:SS 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
Exemple(s)	2019-07-09T10:52:25

3.5.1.2.2.1 Objet « customer »

L'objet « customer » permet de véhiculer des informations liées à votre client.

Champ JSON	Type JSON	Présence	Détail
mail	Chaîne	Conditionnelle	lien
ip_address	Chaîne	Optionnelle	lien

Champ	**mail**
Présence	Optionnelle
Description	Email du client réalisant la transaction, permet au porteur de recevoir son ticket de paiement à l'adresse indiquée.
Format **Valeur(s) possible(s)**	255 caractères maximum ^.+@.+\..+$
Exemple(s)	monclient@mondomaine.com

Champ	**ip_address**
Présence	Optionnelle
Description	Adresse IP du client réalisant la transaction.
Format **Valeur(s) possible(s)**	0-255.0-255.0-255.0-255
Exemple(s)	10.20.30.40

3.5.1.2.2.2 Objet « context »

3.5.1.2.2.2.1 Généralités et exclusions

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

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

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 cadre de la commande, il faut la fournir. Exemple(s) : 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	Type JSON	Présence	Détail
billing	Objet	Obligatoire	lien
shipping	Objet	Obligatoire si applicable	lien
shoppingCart	Objet	Optionnelle	lien
client	Objet	Optionnelle	lien
browser	Objet	Obligatoire si applicable	lien

3.5.1.2.2.2 Détail de l'objet « billing »

L'objet « billing » contient les informations liées à l'adresse de facturation.

Champ JSON	Type JSON	Présence	Détail
civility	Chaîne	Optionnelle	lien
name	Chaîne	Optionnelle	lien
firstName	Chaîne	Optionnelle	lien
lastName	Chaîne	Optionnelle	lien
middleName	Chaîne	Optionnelle	lien
address	Chaîne	Optionnelle	lien
addressLine1	Chaîne	Obligatoire	lien
addressLine2	Chaîne	Optionnelle	lien
addressLine3	Chaîne	Optionnelle	lien
city	Chaîne	Obligatoire	lien

postalCode	Chaîne	Obligatoire	lien
country	Chaîne	Obligatoire	lien
stateOrProvince	Chaîne	Obligatoire si applicable	lien
countrySubdivision	Chaîne	Optionnelle	lien
email	Chaîne	Optionnelle	lien
phone	Chaîne	Optionnelle	lien
mobilePhone	Chaîne	Optionnelle	lien
homePhone	Chaîne	Optionnelle	lien
workPhone	Chaîne	Optionnelle	lien

3.5.1.2.2.2.3 *Détail de l'objet « shipping »*

L'objet « shipping contient les informations liées à l'adresse de livraison.

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

3.5.1.2.2.2.4 *Détail de l'objet « shoppingCart »*

L'objet « shoppingCart » porte les informations du panier du client.

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

3.5.1.2.2.2.4.1 Détail de l'objet « shoppingCartItems »

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

3.5.1.2.2.5 Détail de l'objet « client »

L'objet « client » contient les informations sur le client.

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

3.5.1.2.2.6 Description des attributs

Attribut	accountAge
Description	Date de création du compte client sur le site commerçant.
Format	Chaîne
Restrictions	Du type AAAA-MM-JJ avec AAAA = année sur 4 chiffres, MM = mois sur 2 chiffres, JJ = jour sur deux chiffres (ISO 8601)

Attribut	addCardNbLast24Hours
Format	Entier
Description	Nombre de tentatives d'ajout carte du client sur le site commerçant durant les 24 dernières heures.

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

Attribut	addressLine1
Description	Adresse du client (numéro, rue)
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

Attribut	addressLine2
Description	Complément de l'adresse du client
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

Attribut	addressLine3
Description	Complément de l'adresse du client
Format	Chaîne
Restrictions	Jusqu'à 50 caractères

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attribut	quantity

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

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

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

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

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

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

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

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

3.5.1.2.2.7 Détail de l'objet « browser »

L'objet « browser » véhicule les informations sur le navigateur du client.

Champ JSON	Type JSON	Présence	Détail
accept_header	Chaîne	Obligatoire	lien
java_enabled	Booléen	Obligatoire	lien
language	Chaîne	Obligatoire	lien
color_depth	Entier	Obligatoire	lien
screen_height	Entier	Obligatoire	lien
screen_width	Entier	Obligatoire	lien
timezone	Entier	Obligatoire	lien
user_agent	Chaîne	Obligatoire	lien

Attribut	accept_header
Description	Contenu du header HTTP « Accept » envoyé par le porteur au serveur du commerçant
Format	Chaîne
Restrictions	Jusqu'à 2048 caractères

Attribut	java_enabled
Description	Résultat de l'exécution de la fonction JavaScript « navigator.javaEnabled() » par le navigateur du porteur
Format	Booléen

Attribut	language
Description	Propriété « navigator.language » du navigateur du porteur
Format	Chaîne

Attribut	color_depth
Description	Valeur représentant le nombre de bits par pixel pour l'affichage d'images. Propriété « screen.colorDepth » du navigateur du porteur
Format	Entier

Attribut	screen_height
Description	Valeur représentant la hauteur de l'écran du porteur en pixels. Propriété « screen.height » du navigateur du porteur
Format	Entier

Attribut	screen_width
Description	Valeur représentant la largeur de l'écran du porteur en pixels. Propriété « screen.width » du navigateur du porteur
Format	Entier

Attribut	timezone
Description	Valeur représentant la différence en minutes entre l'heure UTC et l'heure locale du porteur Résultat de l'exécution de la fonction JavaScript « Date.getTimezoneOffset()» par le navigateur du porteur
Format	Entier

Attribut	user_agent
Description	Contenu du header HTTP « User-Agent » envoyé par le porteur au serveur du commerçant
Format	Chaîne
Restrictions	Jusqu'à 2048 caractères

3.5.1.2.3 Objet « payment »

L'objet « payment » véhicule des informations liées au moyen de paiement utilisé pour la réalisation de la commande ainsi que les particularités liées notamment au mode de paiement.

Champ JSON	Type JSON	Présence	Détail
transaction_initiator	Chaîne	Obligatoire	lien
reference	Chaîne	Obligatoire	lien
comment	Chaîne	Optionnelle	lien
payment_mean	Objet	Obligatoire	lien
amount	Objet	Obligatoire	lien
payment_options	Objet	Optionnelle	lien
instalment_payment	Objet	Conditionnelle	lien
preauthorisation_payment	Objet	Conditionnelle	lien

Champ	**transaction_initiator**
Présence	Obligatoire
Description	Indique qui est à l'origine de la transaction. Cette information est nécessaire dans le cas de la DSP2
Format **Valeur(s) possible(s)**	cardholder : le porteur de la carte est présent lors de l'acte d'achat et peut donc s'authentifier. merchant : le porteur de la carte n'est pas présent et ne peut donc pas s'authentifier. Par exemple, lors des recouvrements des récurrences ultérieures, suite au paiement initial, pour un paiement récurrent.
Exemple(s)	cardholder

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. Sur une même journée, il ne peut pas y avoir deux paiements avec la même référence (sur un TPE donné).
Exemple(s)	REF7896543

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

3.5.1.2.3.1 Objet « payment_mean »

Champ JSON	Type JSON	Présence	Détail
wallet_id	Chaîne	Optionnelle	lien
hpan	Chaîne	Optionnelle	lien
name	Chaîne	Optionnelle	lien
account_number	Chaîne	Conditionnelle	lien
expiry_date	Chaîne	Conditionnelle	lien
cardholdername	Chaîne	Conditionnelle	lien
birth_date	Chaîne	Conditionnelle	lien
cvx	Chaîne	Conditionnelle	lien
scheme	Chaîne	Conditionnelle	lien
default_scheme	Booléen	Conditionnelle	lien

Champ	**wallet_id**
Présence	Optionnelle Nécessite la mise en place de l'option « paiement express » ou « one-click » sur le contrat Monetico paiement. Se rapprocher du support pour plus d'informations.
Description	Identifiant du wallet client
Format **Valeur(s) possible(s)**	De 1 à 64 caractères alphanumériques [a-zA-Z0-9]{1,64}
Exemple(s)	monClientRef001

Champ	**hpan**
Présence	Optionnelle Nécessite la mise en place de l'option « paiement express » ou « one-click » sur le TPE
Description	HPAN de la carte de paiement d'un client tel que renvoyé par Monetico Paiement. Permet de spécifier la carte à utiliser dans le cas où le wallet client contient plusieurs cartes bancaires.
Format **Valeur(s) possible(s)**	[A-Z0-9]{40}
Exemple(s)	428992D011D60A2E2ACB068842FB6BAECD5EAF7D

Champ	**name**
Présence	Optionnelle
Description	Nom qui a été assignée à la carte de paiement et qui sera visible par exemple lors de la consultation du wallet par le client.
Format **Valeur(s) possible(s)**	[0-9A-Za-z_,\.\-]{1,20}
Exemple(s)	VISA CIC

Champ	**account_number**
Présence	Obligatoire si le champ « wallet_id » n'est pas fourni.
Description	Numéro de la carte du porteur
Format Valeur(s) possible(s)	[0-9]{13,19}
Exemple(s)	1234567890123456

Champ	**cardholdername**
Présence	Obligatoire si le champ « account_number » est fourni
Description	Nom du porteur figurant sur la carte
Format Valeur(s) possible(s)	^[\x20-\x7E]{2,45}$
Exemple(s)	Jean Dupont

Champ	**birth_date**
Présence	Optionnelle
Description	Date de naissance présente sur certaines cartes bancaires
Format Valeur(s) possible(s)	AAAA-MM-JJ
Exemple(s)	1974-05-26

Champ	**expiry_date**
Présence	Optionnelle
Description	Date d'expiration de la carte de paiement
Format Valeur(s) possible(s)	AAAA-MM
Exemple(s)	2024-12

Champ	**cvx**
Présence	Obligatoire si la carte de paiement dispose d'un cryptogramme visuel.
Description	Cryptogramme visuel de la carte de paiement du porteur
Format Valeur(s) possible(s)	[0-9]{3,4}
Exemple(s)	123

Champ	**scheme**
Présence	Obligatoire si le champ « account_number » est fourni
Description	Nom du réseau à utiliser pour le paiement
Format Valeur(s) possible(s)	CB VISA MASTERCARD AMEX UPI PRIVATIVE
Exemple(s)	CB

Champ	**default_scheme**
Présence	Obligatoire si le champ « account_number » est fourni
Description	Indique si le réseau de paiement utilisé pour le paiement est celui par défaut ou si le client a sélectionné le réseau de paiement.
Format Valeur(s) possible(s)	true : si le réseau qui doit être utilisé est celui par défaut false : dans tous les autres cas

Exemple(s)	true

3.5.1.2.3.2 Objet « amount »

Montant de la demande de paiement.

Champ JSON	Type JSON	Présence	Détail
value	Entier	Obligatoire	lien
currency	Chaîne	Obligatoire	lien
exponent	Entier	Obligatoire	lien

Champ	**value**
Présence	Obligatoire
Description	Montant TTC de la commande exprimé dans sa plus petite fraction. Par exemple pour un montant de 199,24 euros, on indiquera ici 19924
Format **Valeur(s) possible(s)**	Un nombre entier [0-9]+
Exemple(s)	12345

Champ	**currency**
Présence	Obligatoire
Description	Code alphabétique de la devise utilisée.
Format **Valeur(s) possible(s)**	[A-Z]{3,4}
Exemple(s)	EUR

Champ	**exponent**
Présence	Obligatoire
Description	Exposant de la devise au sens de la norme ISO 4217
Format **Valeur(s) possible(s)**	Nombre entier
Exemple(s)	2 (pour l'euro EUR)

3.5.1.2.3.3 Objet « payment_options »

Champ JSON	Type JSON	Présence	Détails
merchant_identification	Objet	Optionnelle	lien
special_payment_mode	Chaîne	Optionnelle	lien

Champ	**special_payment_mode**
Présence	Optionnelle
Description	Facilité de paiement proposée par des partenaires. Nécessite la souscription d'une option.
Format **Valeur(s) possible(s)**	[A-Z a-z0-9]{1,32}
Exemple(s)	OPC23

3.5.1.2.3.3.1 *Objet « merchant_identification »*

Cet objet permet, s'il est renseigné, de personnaliser le libellé du paiement (format « enseigne*localite ») apparaissant sur le relevé de compte bancaire du porteur.

Champ JSON	Type JSON	Présence	Détails
name	Chaine	Obligatoire conditionné	lien
locality	Chaine	Obligatoire conditionné	lien

Champ	**name**
Présence	Obligatoire si l'objet « merchant_identification » est fourni sans le champ « locality »
Description	Permet, s'il est renseigné, de remplacer la partie « enseigne » dans le libellé du paiement (format « enseigne*localité ») apparaissant sur le relevé de compte du porteur. **NB :** Le nombre de caractères pris en compte est dépendant de la banque du porteur
Format **Valeur(s) possible(s)**	[A-Z a-z0-9]{1,32}
Exemple(s)	MonCommerce

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

3.5.1.2.3.4 Objet « instalment_payment »

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 JSON	Type JSON	Présence	Détails
instalments	Tableau d'objets	Optionnelle	lien

Champ	instalments
Présence	Optionnelle Si non renseigné, la configuration par défaut mise en place sur le TPE sera prise en compte
Description	Pour un paiement fractionné, permet de spécifier le montant et la date de recouvrement des fractions

Format
Valeur(s) possible(s)
	Chaque élément du tableau est un objet de la forme suivante :
	`{`
	`"date":"date_au_format_AAAA-MM-JJ",`
	`"amount":{`
	`"value": montant_en_centimes`
	`}`
	`}`

Exemple(s)	`[`
	`{`
	`"amount":{`
	`"value":2500`
	`},`
	`"date":"2019-08-05"`
	`},`
	`{`
	`"amount":{`
	`"value":2500`
	`},`
	`"date":"2019-09-05"`
	`},`
	`{`
	`"amount":{`
	`"value":2500`
	`},`
	`"date":"2019-10-05`
	`},`
	`{`
	`"amount":{`
	`"value":2501`
	`},`
	`"date":"2019-11-05"`
	`}`
	`]`

3.5.1.2.3.5 Objet « preauthorisation_payment »

L'objet « preauthorisation_payment » est obligatoire dans le cas du paiement préautorisation. Dans les autres modes de paiement, cet objet n'est pas à utiliser.

Pour pouvoir utiliser ces champs, votre TPE doit être configuré pour accepter les paiements en pré-autorisation.

Champ JSON	Type JSON	Présence	Détails
invoice_type	Chaîne	Obligatoire	lien
file_number	Chaîne	Obligatoire	lien

Champ	**invoice_type**
Présence	Obligatoire
Description	Type de la facture qui vient d'être réalisée
Format **Valeur(s) possible(s)**	preauthorisation : Demande d'une facture de pré-autorisation classique additional_charges : Demande d'une facture complémentaire
Exemple(s)	preauthorisation

Champ	**file_number**
Présence	Obligatoire
Description	Numéro de dossier
Format **Valeur(s) possible(s)**	12 caractères alphanumériques maximum
Exemple(s)	20150901PRE1

3.5.1.2.4 Objet « authentication »

L'objet « authentication » porte les informations destinées à piloter le processus d'authentification du client. Sa présence est obligatoire sauf dans le cadre de la VPC.

Champ JSON	Type JSON	Présence	Détails
merchant_preference	Chaine	Optionnelle	lien
merchant_redirection_url	Chaine	Obligatoire	lien
challenge_window_size	Chaine	Obligatoire	lien
disable_authentication	Booléen	Optionnelle	lien

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

Champ	**merchant_redirection_url**
Présence	Obligatoire
Description	URL vers laquelle l'ACS va rediriger le porteur de carte une fois que l'authentification a été réalisée
Format **Valeur(s) possible(s)**	Format valide d'une url
Exemple(s)	https://www.mywebsite.com/authentication_result.cgi

Champ	**challenge_window_size**
Présence	Obligatoire
Description	Dimensions de la fenêtre de challenge 3D Secure (V2 uniquement) souhaitées par le commerçant (largeur puis hauteur)
Format **Valeur(s) possible(s)**	« 250x400 » « 390x400 » « 500x600 » « 600x400 » « full_screen »
Exemple(s)	500x600

Champ	**disable_authentication**
Présence	Optionnelle
Description	Permet de débrayer l'authentification 3D Secure quelle que soit la version du protocole. Si la valeur « true » est fournie, le champ **merchant_preference** est ignoré.
Format **Valeur(s) possible(s)**	Booléen
Exemple(s)	false

3.5.1.3 Exemple(s)


```
{
   "merchant_configuration":{
      "point_of_sale":"9000001",
      "version":"3.0",
      "language":"FR",
      "configuration":"emulation3d"
   },
   "order":{
      "date":"2019-09-06T17:23:44",
      "customer":{
         "mail":"customer@mail.com"
      },
      "context":{
         …
      }
   },
   "payment":{
      "transaction_initiator":"cardholder",
      "reference":"89e8b64c-513f-4d9d-8ff9-4520d10ef780",
      "payment_mean":{
         "account_number":"0000030000000005",
         "cvx":"123",
         "cardholdername":"Jean Dupont",
         "scheme":"MASTERCARD",
         "default_scheme":true,
         "expiry_date":"2035-12"
      },
      "amount":{
         "value":10001,
         "currency":"EUR",
         "exponent":2
      },
      "payment_options":{
         "merchant_identification":{
            "name":"MyWebSite"
         }
      }
   },
   "authentication":{
      "merchant_preference":"no_challenge_requested",
      "merchant_redirection_url":"https://www.mywebsite.com/authentication_result.cgi",
      "challenge_window_size":"500x600"
   }
}
```

3.5.1.4 Cinématique « en deux temps »

Il est possible pour le commerçant de séparer la phase 1 en deux appels distincts :

- Un premier appel (a) **avec calcul du sceau MAC**, qui contient toutes les informations décrites dans la section 3.5.1.2 en dehors des informations relatives au moyen de paiement.
- Un second appel (b) **sans calcul de sceau MAC**, qui contient les informations relatives au moyen de paiement.

3.5.1.4.1 Les données de corps pour l'appel (a)

Se référer à la section 3.5.1.2.

Pour les utilisations du SDK mobile Monetico :

Au choix :

- Ne pas fournir l'objet « payment_mean ».
- Fournir l'objet « payment_mean » avec uniquement le champ « wallet_id » afin de permettre la séquestration de la carte ou l'utilisation d'une carte séquestrée.

Pour les autres cas d'utilisation :

Ne pas fournir l'objet « payment_mean ».

3.5.1.4.2 Les données de corps pour l'appel (b)

Le corps de la requête contient les informations suivantes :

Champ JSON	Type JSON	Présence	Détails
payment_token	Chaîne	Obligatoire	lien
payment	Objet	Obligatoire	lien

Objet « payment » :

- Doit contenir uniquement l'objet « payment_mean ».
- Se référer à la section 3.5.1.2.3.1.

3.5.2 Phase 2 : envoi des informations techniques au serveur d'authentification

Une fois l'envoi des informations techniques au serveur d'authentification effectué (voir le paragraphe 4.1 La valeur du champ « step » est « technical_information_collecting » pour plus de détail sur le traitement à effectuer pour fournir les informations techniques au serveur d'authentification), la confirmation de cet envoi doit être fournie au service de paiement par API.

Lors de cet appel, le calcul de sceau HMAC n'est pas demandé.

3.5.2.1 Les données d'en-tête

Champ	Content-Type
Présence	Obligatoire
Description	Précise le format des échanges
Format Valeur(s) possible(s)	application/json; charset=utf-8

3.5.2.2 Les données du corps

Lors de la phase d'envoi des informations techniques au serveur d'authentification, la confirmation de l'envoi des informations techniques au serveur d'authentification doit être fournie.

Le corps de la requête est un document au format JSON/UTF-8. Il contient les informations suivantes :

Champ JSON	Type JSON	Présence	Détails
payment_token	Chaîne	Obligatoire	lien
authentication	Objet	Obligatoire	lien

Champ	payment_token
Description	Jeton unique lié à une demande de paiement devant être utilisé si des appels supplémentaires sont nécessaires pour finaliser la transaction.
Format Valeur(s) possible(s)	UUID (RFC 4122)
Exemple(s)	eb2294de-a864-4a1f-abda-1b568bf7ca9a

3.5.2.2.1 Objet « authentication »

Champ JSON	Type JSON	Présence	Détails
status	Chaine	Obligatoire	lien

Champ	status
Présence	Obligatoire
Description	Statut de l'authentification du porteur
Format Valeur(s) possible(s)	threedsmethod_requested
Exemple(s)	threedsmethod_requested

3.5.2.3 Exemple(s)


```
{
   "payment_token":"6d7514d9-58ac-4c8d-a213-26dfa3a4a410",
   "authentication":{
      "status":"threedsmethod_requested"
   }
}
```


3.5.3 Phase 4 : traitement de l'authentification 3D Secure du porteur

Une fois le processus d'authentification par de serveur d'authentification de la banque du porteur effectué (voir le paragraphe 4.2 Le retour effectué est « cardholder_authentication » pour plus de détail sur le traitement à effectuer pour appeler le serveur d'authentification), le résultat de l'authentification doit être fourni au service de demande de paiement par API.

Lors de cet appel, le calcul de sceau HMAC n'est pas demandé.

3.5.3.1 Les données d'en-tête

Champ	Content-Type
Présence	Obligatoire
Description	Précise le format des échanges
Format Valeur(s) possible(s)	application/json; charset=utf-8

3.5.3.2 Les données du corps

Le corps de la requête est un document au format JSON/UTF-8. Il contient les informations suivantes :

Champ JSON	Type JSON	Présence	Détails
payment_token	Chaîne	Optionnelle	lien
authentication	Objet	Obligatoire	lien

Champ	payment_token
Description	Jeton unique lié à une demande de paiement devant être utilisé si des appels supplémentaires sont nécessaires pour finaliser la transaction.
Format Valeur(s) possible(s)	UUID (RFC 4122)
Exemple(s)	eb2294de-a864-4a1f-abda-1b568bf7ca9a

3.5.3.2.1 Objet « authentication »

Champ JSON	Type JSON	Présence	Détails
details	Objet	Obligatoire	lien

3.5.3.2.2 Objet « details »

Champ	**details**
Présence	Obligatoire
Description	Résultat de l'authentification du porteur Pour le 3D Secure V2, la valeur du « cres », renvoyée par le serveur d'authentification, doit être fournie. Pour le SecurePlus (équivalent du 3D Secure V1 pour les cartes UnionPay), la valeur de l' « ACPRes », renvoyée par le serveur d'authentification, doit être fournie.
Format **Valeur(s) possible(s)**	Objet
Exemple(s)	Voir les exemples ci-dessous pour le détail

Champ JSON	Type JSON	Présence	Détails
cres	Chaine	Conditionnelle	**lien**
threeDSSessionData	Chaine	Conditionnelle	
ACPRes	Chaine	Conditionnelle	**lien**

Une fois le processus d'authentification réalisé (porteur authentifié ou non) par le serveur d'authentification de la banque (ACS), ce dernier soumet le résultat via un POST http à l'URL qui a lui été fournie précédemment. Cette URL est déterminée comme suit :

- 3D Secure V2 : il s'agit du champ «merchant_redirection_url » passé lors de l'appel effectué par la plateforme Monetico paiement au serveur d'authentification pour déterminer le scénario à effectuer (flux 3.02 du diagramme décrivant le scénario de paiement).
- SecurePlus : il s'agit du champ « frontUrl » du formulaire d'appel au serveur d'authentification.

L'interprétation de ce retour est dépendante de la version du protocole 3D Secure car les données renvoyées diffèrent en fonction de la version du protocole qui a été utilisée.

3.5.3.2.2.1 3D Secure V2

Les paramètres suivants sont renvoyés par l'ACS :

Champ	Description
cres	Résultat de la requête d'authentification du client
threeDSSessionData	Donnée permettant d'identifier de manière unique un paiement

Exemple(s) de retour de l'ACS:

```
cres=
ewogICAiYWNzVHJhbnNJRCIgOiAiOGY4N2I3ZjQtZTUwMC00MDkwLThkZTItZmNlMjIwNDQ0MGNlIiwKIC
AgIm1lc3NhZ2VUeXBlIiA6ICJDUmVzIiwKICAgIm1lc3NhZ2VWZXJzaW9uIiA6ICIyLjEuMCIsCiAgICJ0
aHJlZURTU2VydmVyVHJhbnNJRCIgOiAiODI1ZTlmZmQtYjA0NS00YTgxLWIzYzItZDBmMzQ0MWMyNGZhIi
wKICAgInRyYW5zU3RhdHVzIiA6ICJZIgp9Cg==&threeDSSessionData=982e7b2c-941e-454e-a6ad-
400bf503d32b
```

Les informations de ce message vont être utilisées pour effectuer un appel du service de paiement par API. Il faut donc les remettre en forme et les transmettre au service de paiement.
Lors de l'appel au service de la plateforme Monetico paiement, les données suivantes sont obligatoires :

- « cres » : fourni par l'ACS
- « threeDSSessionData » si fourni par l'ACS

Les données suivantes sont facultatives:

- « payment_token »: Même valeur que celle retournée à la phase 1.

Exemple(s) pour l'appel au service de demande de paiement par API :

```
{
   "payment_token":"982e7b2c-941e-454e-a6ad-400bf503d32b",
   "authentication":{
      "details":{
         "cres":"ewogICAiYWNzVHJhbnNJRCIgOiAiOGY4N2I3ZjQtZTUwMC00MDkwLThkZTItZmN
lMjIwNDQ0MGNlIiwKICAgIm1lc3NhZ2VUeXBlIiA6ICJDUmVzIiwKICAgIm1lc3NhZ2VWZXJzaW9uIiA
6ICIyLjEuMCIsCiAgICJ0aHJlZURTU2VydmVyVHJhbnNJRCIgOiAiODI1ZTlmZmQtYjA0NS00YTgxLWI
zYzItZDBmMzQ0MWMyNGZhIiwKICAgInRyYW5zU3RhdHVzIiA6ICJZIgp9Cg==",
         " threeDSSessionData":"982e7b2c-941e-454e-a6ad-400bf503d32b"
      }
   }
}
```

3.5.3.2.2.2 SecurePlus

Les paramètres suivants sont renvoyés par l'ACS :

Champ	Description
ACPRes	Résultat de la requête d'authentification du client

Exemple(s) de retour de l'ACS:

ACPRes=%3CUPACPPay%3E%3CMsgRes%3E%3Cversion%3E5.0.0%3C%2Fversion%3E%3Cencoding%3EUTF-8%3C%2Fencoding%3E%3CcertId%3E69678957876%3C%2FcertId%3E%3CsignMethod%3E01%3C%2FsignMethod%3E%3CtxnType%3E79%3C%2FtxnType%3E%3CtxnSubType%3E10%3C%2FtxnSubType%3E%3CbizType%3E000301%3C%2FbizType%3E%3CaccessType%3E1%3C%2FaccessType%3E%3CacqInsCode%3E31310250%3C%2FacqInsCode%3E%3CmerId%3E0056246%3C%2FmerId%3E%3CorderId%3Eaa9ecde754a447ef808f%3C%2ForderId%3E%3CtxnTime%3E20221229224320%3C%2FtxnTime%3E%3CaccType%3E%3C%2FaccType%3E%3CaccNo%3E62228212XXXXXX17%3C%2FaccNo%3E%3CcurrencyCode%3E978%3C%2FcurrencyCode%3E%3CtxnAmt%3E501%3C%2FtxnAmt%3E%3CactivateStatus%3EY%3C%2FactivateStatus%3E%3CreqReserved%3E%3Cid%3Eb97faa5d67d14ba3864a68a225e07b13%3C%2Fid%3E%3C%2FreqReserved%3E%3Creserved%3Ee3Zjb2RlPTIwMjIxMjI5MjE0MzU0MTkyMzM2JmVjaT0wOX0%3D%3C%2Freserved%3E%3CrespCode%3E00%3C%2FrespCode%3E%3CrespMsg%3ESuccess%3C%2FrespMsg%3E%3C%2FMsgRes%3E%3CSignature%3E%3CSignatureValue%3EKe95bIEQzrds9UyQyJzJ2AqY%2FRkuwwW%2BEoYwtPKEjLIndQz8xGboaRbqRLws1VvaNC5YORWuEdawIAwYj2P9K7eLf%2FKnphAZPoKueVmkQhq%2FWu5q8E8cqyb5e748G0mMHEoNTVjjstRzUpdqqAfFpN0TEgPWlG%2FN6tzcm2dnHettK8K%2Fiv1YTa8rs8nLgSS4qZXPaTL%2Bn1XuuNV4nQrNH%2BdnOhamzWKauWpzM%2BzAnNczSqrgQkG5vBUGPD7WyL41emqCx0ej66Jh9%2FWXL9xZ7WecwiJZc3uuYxf4IbSGus50I7UJiow15fOuo0sWyYv7HrHuVWaArhBl1zipsHI11g%3D%3D%3C%2FSignatureValue%3E%3C%2FSignature%3E%3C%2FUPACPPay%3E

Les informations de ce message doivent être utilisées pour effectuer un appel du service de paiement par API. Il convient au préalable de les mettre en forme avant transmission. Lors de l'appel au service de la plateforme Monetico paiement, les données suivantes sont obligatoires :

- « ACPRes » : fourni par l'ACS du client qu'il faudra URL-Décodé puis l'encoder en Base 64 avant transmission au service de paiement par API.

Les données suivantes sont facultatives:

- « payment_token »: Même valeur que celle retournée à la phase 1.

Exemple(s) pour l'appel au service de demande de paiement par API :


```
{
   "payment_token":"982e7b2c-941e-454e-a6ad-400bf503d32b",
   "authentication":{
      "details":{
         "ACPRes":"PFVQQUNQUGF5PjxNc2dSZXM+PHZlcnNpb24+NS4wLjA8L3ZlcnNpb24+PGVuY29kaW5nPlVURi04PC9lbmNvZGluZz48Y2VydElkPjY5Njc4OTU3ODc2PC9jZXJ0SWQ+PHNpZ25NZXRob2Q+MDE8L3NpZ25NZXRob2Q+PHR4blR5cGU+Nzk8L3R4blR5cGU+PHR4blN1YlR5cGU+MTA8L3R4blN1YlR5cGU+PGJpelR5cGU+MDAwMzAxPC9iaXpUeXBlPjxhY2Nlc3NUeXBlPjE8L2FjY2Vzc1R5cGU+PGFjcUluc0NvZGU+MzEzMTAyNTA8L2FjcUluc0NvZGU+PG1lcklkPjAwNTYyNDY8L21lcklkPjxvcmRlcklkPjAwNTYyNDY8L21lcklkPjxvcmRlcklkPjxjxvcmRlcklkP
```

```
mFhOWVjZGU3NTRhNDQ3ZWY4MDhmPC9vcmRlcklkPjx0eG5UaW1lPjIwMjIxMjI5MjI0MzIwPC90eG5Ua
W1lPjxhY2NUeXBlPjwvYWNjVHlwZT48YWNjTm8+NjIyMjgyMTJYWFhYWFgxNzwvYWNjTm8+PGN1cnJlb
mN5Q29kZT45Nzg8L2N1cnJlbmN5Q29kZT48dHhuQW10PjUwMTwvdHhuQW10PjxhY3RpdmF0ZVN0YXR1c
z5ZPC9hY3RpdmF0ZVN0YXR1cz48cmVxUmVzZXJ2ZWQ+PGlkPmI5N2ZhYTVkNjdkMTRiYTM4NjRhNjhhM
jI1ZTA3YjEzPC9pZD48L3JlcVJlc2VydmVkPjxyZXNlcnZlZD5lM1pqYjJSbFBUSXdNakl4TWpJNU1qR
TBNelUwTVRreU16TTJKbVZqYVQwd09YMD08L3Jlc2VydmVkPjxyZXNwQ29kZT4wMDwvcmVzcENvZGU+P
HJlc3BNc2c+U3VjY2VzczwvcmVzcE1zZz48L01zZ1Jlcz48U2lnbmF0dXJlPjxTaWduYXR1cmVWYWx1Z
T5LZTk1YklFUXpyZHM5VXlReUp6SjJBcVkvUmt1d3dXK0VvWXd0UEtFakxJbmRRejh4R2JvYVJicVJMd
3MxVnZhTkM1WU9SV3VFZGF3SUF3WWoyUDlLN2VMZi9LbnBoQVpQb0t1ZVZta1FocS9XdTVxOEU4Y3F5Y
jVlNzQ4RzBtTUhFb05UVmpqc3RSelVwZHFxQWZGcE4wVEVnUFdsRy9ONnR6Y20yZG5IZXR0SzhLL2l2M
VlUYThyczhuTGdTUzRxWlhQYVRMK24xWHV1TlY0blFyTkgrZG5PaGFteldLYXVXcHpNK3pBbk5jelNxc
mdRa0c1dkJVR1BEN1d5TDQxZW1xQ3gwZWo2NkpoOS9XWEw5eFo3V2Vjd2lKWmMzdXVZeGY0SWJTR3VzN
TBJN1VKaW93MTVmT3VvMHNXeVl2N0hySHVWV2FBcmhCbDF6aXBzSEkxMWc9PTwvU2lnbmF0dXJlVmFsd
WU+PC9TaWduYXR1cmU+PC9VUEFDUFBheT4="
      }
   }
}
```


3.6 Retour du service de demande de paiement par API

3.6.1 Structure du retour du service

Le Service de demande de paiement par API retourne des informations au format JSON/UTF-8. Ce document comporte plusieurs parties.

Champ JSON	Type JSON	Présence	Détails
next_step	Objet	Conditionnelle	lien
merchant_configuration	Objet	Obligatoire	lien
payment	Objet	Obligatoire	lien
authentication	Objet	Obligatoire	lien
risk_management	Objet	Optionnelle	lien
payment_token	Chaîne	Obligatoire	lien
request_token	Chaîne	Obligatoire	lien
return_code	Entier	Obligatoire	lien

Champ	**payment_token**
Description	Jeton unique lié à une demande de paiement devant être utilisé si des appels supplémentaires sont nécessaires pour finaliser la transaction. Sa durée de validité est de 45 minutes.
Format Valeur(s) possible(s)	UUID (RFC 4122)
Exemple(s)	eb2294de-a864-4a1f-abda-1b568bf7ca9a

Champ	**request_token**
Description	Jeton unique généré à chaque appel à nos services. A fournir dans le cadre de vos demandes de support.
Format Valeur(s) possible(s)	UUID (RFC 4122)
Exemple(s)	918b9280-b7ca-47ee-9e0c-d006ef9c6b0c

Champ	**return_code**
Description	Code retour indiquant l'état du paiement.
Format Valeur(s) possible(s)	Liste complète des valeurs du champ « return_code » Les valeurs possibles varient en fonction de la phase du paiement.
Exemple(s)	1

3.6.1.1 Objet « next_step »

Cet objet permet de spécifier l'action suivante à réaliser par le commerçant : elle permet donc d'orienter la cinématique des échanges en fonction des différents scénarii possibles. Cet objet est retourné uniquement si une action doit être réalisée de votre part.

Champ JSON	Type JSON	Présence	Détails
step	Chaine	Obligatoire	lien
recommended_implementation	Tableau d'objets	Obligatoire	lien
data	Chaine	Conditionnelle	lien
url	Chaine	Conditionnelle	lien

Champ	**step**
Présence	Obligatoire
Description	Descriptif du type d'action à réaliser de votre part
Format **Valeur(s) possible(s)**	• technical_information_collecting : dans le cadre du protocole 3D Secure V2, la collecte des informations techniques est à réaliser • cardholder_authentication : dans le cadre du protocole 3D Secure, le porteur de la carte doit maintenant effectuer la phase d'authentification (challenge)
Exemple(s)	technical_information_collecting
Champ	**recommended_implementation**
Présence	Obligatoire
Description	Recommandation d'implémentation pour réaliser l'action demandée. Si plusieurs valeurs sont retournées, le choix est laissé à l'appelant. De manière générale, il ne s'agit que d'une préconisation d'implémentation et l'appelant peut choisir d'autres moyens techniques de traiter ce retour.
Format **Valeur(s) possible(s)**	Plusieurs valeurs peuvent être retournée parmi : • redirect : une redirection vers l'url fournie dans le champ "url" en passant les données fournies dans le champ « data » doit être mise en place par le commerçant. • iframe : une iframe sur l'url fournie dans le champ "url" en passant les données fournies dans le champ « data » doit être mise en place par le commerçant. • invisible_iframe : une iframe invisible sur l'url fournie dans le champ "url" en passant les données fournies dans le champ « data » doit être mise en place par le commerçant.
Exemple(s)	["redirect", "iframe"]

Champ	**url**
Présence	Conditionnelle – Uniquement si l'action demandée au commerçant nécessite une url
Description	URL cible de l'action
Format **Valeur(s) possible(s)**	Format valide d'une url
Exemple(s)	https://url-acs-client/acs.cgi

3.6.1.1.1 Objet « data »

Chacun des champs présents dans cet objet sont à utiliser pour réaliser un traitement sur le serveur de commerçant. Le détail sur ce champ est précisé dans le paragraphe **3.6.2 Précisions sur les champs « code retour » et « next_step »**.

3.6.1.1.2 Exemple(s)


```
{
   …
   "next_step":{
      "data":{
         "MD":"6ee248c9-f73d-453a-8bf9-824e49b73524",
         "PaReq":"MDAwMDAzMDAwMDAwMDAwN3wyNDkwODA4OHx8fHx8fDA5MDAxNTd8TURBd01EQXd
NREF3TURBd01EQXdNRGN6TXpnPXxNQ19tZXJjaGFudHxQQTE5MDkwNjE1MTA0MDY5"
      },
      "recommended_implementation":[
         "redirect"
      ],
      "step":"cardholder_authentication",
      "url":" http://url-acs-client/acs.cgi"
   },
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   "return_code":2,
   …
}
```

3.6.1.2 Objet « merchant_configuration »

L'objet « merchant_configuration » retourné a la même structure que l'objet « merchant_configuration » passé par le commerçant en lors de l'initialisation du paiement.

3.6.1.3 Objet « payment »

Champ JSON	Type JSON	Présence	Détail
reference	Chaîne	Obligatoire	lien
status	Chaine	Obligatoire	lien
refusal_reason	Chaîne	Conditionnelle	lien
authorisation_refusal_reason	Chaîne	Conditionnelle	lien
payment_mean	Objet	Obligatoire	lien
amount	Objet	Obligatoire	lien
instalment_payment	Objet	Conditionnelle	lien
payment_options	Objet	Conditionnelle	lien
authorisation	Objet	Conditionnelle	lien

Champ	**status**
Description	Le statut du paiement
Présence	Obligatoire
Format **Valeur(s) possible(s)**	Statut du paiement : • created: statut initial du paiement • cardholder_authentication_pending: en attente d'authentification du porteur. • authorised: le paiement a été autorisé. • accepted : le paiement est accepté suite à une vérification de carte de paiement. • refused: le paiement est refusé. Voir les champs "refusal_reason" et "authorisation_refusal_reason" pour le détail. • captured: le paiement est capturé. • failed: le paiement est échoué suite à des problèmes techniques. Une nouvelle transaction doit être demandée. • too_many_attempts : Le nombre de tentatives de paiements maximum a été atteint. • cancelled : Le paiement a été annulé.
Exemple(s)	authorised

Champ	refusal_reason
Description	Si le statut du paiement est « refused », la raison du refus est décrite dans ce champ
Présence	Conditionnelle
Format Valeur(s) possible(s)	Une chaîne de caractères • authorisation_refused : Refusé suite à la demande d'autorisation du paiement • cardholder_authentication_failed : Refusé pour une authentification du porteur non aboutie • risk_detected : Refusé car un risque a été détecté sur ce paiement • AVS_no_match : Refusé car les informations AVS fournies n'ont pas été validées par l'émetteur. • CVV_no_match: Refusé car le CVV fourni n'a pu être validé par l'émetteur.
Exemple(s)	authorisation_refused

Champ	authorisation_refusal_reason
Description	Si la raison du refus est « authorisation_refused », le détail du refus est décrit dans ce champ
Présence	Conditionnelle
Format Valeur(s) possible(s)	Une chaîne de caractères • bank_refusal : la banque du commerçant ou du client refuse d'accorder l'autorisation • issuer_refusal : la banque du client refuse d'accorder l'autorisation • critical_refusal : la banque du client refuse d'accorder l'autorisation. Contrairement aux retours « bank_refusal » et « issuer_refusal », ce refus est définitif. • authentication_required : la banque du client refuse d'accorder l'autorisation et requière une authentification du client • temporary_refusal : la demande d'autorisation a été refusée mais pourrait être retentée • technical_refusal : la demande d'autorisation a été refusée en raison d'un problème technique • other_refusal : autre motifs de refus d'autorisation • sandbox_refusal : simulation d'un test de refus d'autorisation en environnement de validation
Exemple(s)	issuer_refusal

3.6.1.3.1 Objet « payment_mean »

Champ JSON	Type JSON	Présence	Détail
card_acquired	Booléen	Optionnelle	lien
wallet_id	Chaîne	Optionnelle	lien
hpan	Chaîne	Obligatoire	lien
name	Chaîne	Optionnelle	lien
cardholdername	Chaîne	Optionnelle	lien

birth_date	Chaîne	Optionnelle	lien
usage_code	Entier	Optionnelle	lien
account_type	Entier	Optionnelle	lien
origin	Chaîne	Optionnelle	lien
ecard	Booléen	Optionnelle	lien
scheme	Chaîne	Optionnelle	lien
expiry_date	Chaine	Optionnelle	lien
masked_account_number	Chaîne	Obligatoire	lien

Champ	**card_acquired**
Description	Indique si la carte de paiement a été séquestrée lors du paiement
Présence	Optionnelle
Format **Valeur(s) possible(s)**	true, false

Champ	**usage_code**
Description	Type de carte utilisée pour le paiement
Présence	Optionnelle
Format **Valeur(s) possible(s)**	• 1 : carte de crédit • 2 : carte de débit • 3 : autre
Exemple(s)	1

Champ	**account_type**
Description	Précise le type de compte associé à la carte de paiement
Présence	Optionnelle
Format **Valeur(s) possible(s)**	• 1 : carte de paiement d'un particulier • 2 : carte de paiement d'un professionnel • 4 : inconnu
Exemple(s)	1

Champ	**ecard**
Description	Indique si la carte utilisée est une carte virtuelle
Présence	Optionnelle
Format **Valeur(s) possible(s)**	true, false

Champ	**origin**
Description	Code pays de la carte de paiement
Présence	Optionnelle
Format	Norme ISO 3166-1 Deux lettres en majuscule
Exemple(s)	FR

Champ	**expiry_date**
Description	Optionnelle

Présence	Date d'expiration de la carte de paiement
Format **Valeur(s) possible(s)**	AAAA-MM
Exemple(s)	2024-12

Champ	**masked_account_number**
Description	Numéro de carte tronqué en conformité avec PCI-DSS
Présence	Obligatoire
Format **Valeur(s) possible(s)**	Le format dépend de la longueur du numéro de carte : - 8 premiers et 2 derniers chiffres de la carte de paiement du client, séparés par des étoiles pour les numéros de carte ayant une longueur de 16 chiffres ou plus - 6 premiers chiffres, 6 étoiles, le reste des chiffres de la carte de paiement du client pour les numéros de carte ayant une longueur de moins de 16 chiffres
Exemple(s)	12345678******12 123456******123

3.6.1.3.2 Objet « instalment_payment »

Cet objet est alimenté :

- soit par les informations transmises dans l'objet par le commerçant lors de l'appel au service
- soit par le paramétrage du TPE si aucune information n'a été fournie lors de l'appel au service

Champ JSON	Type JSON	Présence	Détails
instalments	Tableau d'objets	Optionnelle	lien

Champ	**instalments**
Présence	Optionnelle
Description	Pour un paiement fractionné, permet de spécifier le montant et la date de recouvrement des fractions

Format
Valeur(s) possible(s)
	Chaque élément du tableau est un objet de la forme suivante :
	`{`
	`"date":"date_au_format_AAAA-MM-JJ",`
	`"amount":{`
	`"value":`
	`montant_dans_la_plus_petite_fraction_de_la_devise`
	`}`
	`}`

Exemple(s)	`[`
	`{`
	`"amount":{`
	`"value":2500`
	`},`
	`"date":"2019-09-05"`
	`},`
	`{`
	`"amount":{`
	`"value":2500`
	`},`
	`"date":"2019-10-05"`
	`},`
	`{`
	`"amount":{`
	`"value":2500`
	`},`
	`"date":"2019-11-05"`
	`},`
	`{`
	`"amount":{`
	`"value":2501`
	`},`
	`"date":"2019-12-05"`
	`}`
	`]`

3.6.1.3.3 Objet « authorisation »

L'objet « authorisation » est retourné uniquement si la transaction a fait l'objet d'une demande d'autorisation. Si celui-ci est retourné, certains champs sont dans ce cas obligatoirement retournés.

Champ JSON	Type JSON	Présence	Détail
number	Chaîne	Obligatoire	lien
date	Chaîne	Obligatoire	lien

Champ	**number**
Description	Le numéro d'autorisation. Uniquement si le paiement a été accepté.
Présence	Optionnelle
Format **Valeur(s) possible(s)**	6 chiffres
Exemple(s)	123456

Champ	**date**
Description	La date d'autorisation. Uniquement si le paiement a été accepté.
Présence	Optionnelle
Format **Valeur(s) possible(s)**	AAAA-MM-JJ
Exemple(s)	2019-05-24

3.6.1.4 Objet « authentication »

Cet objet contient des informations relatives à l'authentification du porteur.

Champ JSON	Type JSON	Présence	Détails
status	Chaîne	Obligatoire	lien
protocol	Chaîne	Obligatoire	lien
version	Chaîne	Obligatoire	lien
details	Objet	Obligatoire	lien

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

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

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

3.6.1.4.1 Détail de l'objet « details »

L'objet« details » permet de réaliser une analyse plus fine du déroulé du processus d'authentification en fournissant des informations spécifiques au protocole et à la version d'authentification. Cet objet contient les spécificités liées à 3D Secure.

Champ JSON	Description	Détails
liabilityShift	Transfert de responsabilités	**lien**
ARes	Résultat contenu dans le message ARes	**lien**
CRes	Résultat contenu dans le message cres	**lien**
merchantPreference	Souhait du commerçant	**lien**
transactionID	Identifiant de la transaction	**lien**
status3DS	Indicateur d'échange 3D Secure	**lien**
disablingReason	Motif du débrayage de 3D Secure	**lien**

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

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

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

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

s

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

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

3.6.1.5 Objet « risk_management »

L'objet « risk_management » est retourné si le module antifraude est activé.

Champ JSON	Type JSON	Présence	Détail
monetico_fraud_prevention	Objet	Optionnelle	lien

3.6.1.5.1 Objet « monetico_fraud_prevention »

Champ JSON	Type JSON	Présence	Détail
filtering	Objet	Optionnelle	lien
scoring	Objet	Optionnelle	lien

3.6.1.5.2 Objets « filtering » et « scoring »

Champ JSON	Type JSON	Présence	Détail
analysis	Tableau d'objets	Optionnelle	lien
state	Chaîne	Obligatoire	lien
color	Chaîne	Optionnelle	lien
result	Chaîne	Obligatoire	lien

Champ	**analysis**
Description	Tableau d'objets contenant deux champs : • reason. La liste des valeurs en fourni en annexe. • value Ce tableau est fourni dans le cas de refus de paiement et fournit des couples de raisons de blocages.
Présence	Optionnelle
Format **Valeur(s) possible(s)**	Tableau

Exemple(s)	[
	{
	"reason":3,
	"value":"000001"
	},
	{
	"reason":8,
	"value":"100.0100EUR"
	},
	{
	"reason":4,
	"value":"FRA"
	}
	]

Champ	**state**
Description	La présence de ce champ permet d'indiquer que le retour du module antifraude est uniquement à caractère informatif et ne bloque en rien la commande.
Présence	Obligatoire
Format Valeur(s) possible(s)	information
Exemple(s)	information

Champ	**color**
Description	Code couleur du scoring indiquant la cinématique de paiement à enclencher.
Présence	Uniquement pour le scoring.
Format Valeur(s) possible(s)	green orange red
Exemple(s)	green

Champ	**result**
Description	Résultat du scoring ou du filtrage
Présence	Obligatoire
Format Valeur(s) possible(s)	Pour le filtrage : • blocked : commande bloquée par le système de filtrage. • authorized : commande autorisée par le système de filtrage Pour le scoring : • disable3DS : le calcul du scoring a déterminé que le processus 3D Secure doit être désactivé • force3DS : le calcul du scoring a déterminé que le processus 3D Secure doit être réalisé avec authentification du porteur en succès • decline : le paiement a été refusé suite au résultat de scoring
Exemple(s)	authorized

3.6.1.5.3 Exemple(s)

```
"risk_management":{
   "monetico_fraud_prevention":{
      "filtering":{
         "analysis":[
            {
               "reason":3,
               "value":"000001"
            },
            {
               "reason":8,
               "value":"100.0100EUR"
            },
            {
               "reason":4,
               "value":"FRA"
            }
         ],
         "result":"blocked",
         "state":"information"
      }
   }
}
```

3.6.2 Exemple(s) complet de retour du service

Un exemple de retour effectué lorsque le paiement a été accepté :


```
{
   "authentication":{
      "details":{
         "ARes":"A",
         "status3DS":4
      },
      "protocol":"3DSecure",
      "status":"authentication_attempted",
      "version":"2.1.0"
   },
   "merchant_configuration":{
      "configuration":"emulation3d",
      "language":"FR",
      "point_of_sale":"9000001",
      "version":"3.0"
   },
   "payment":{
      "amount":{
         "currency":"EUR",
         "exponent":2,
         "value":10001
      },
      "authorisation":{
         "date":"2019-09-06",
         "number":"000000"
      },
      "payment_mean":{
         "ecard":false,
         "expiry_date":"2035-12",
         "hpan":"C5F5A5ACAACB96129882D1A9DB9E1FBBED4FBE93",
         "masked_account_number":"000003******0007",
         "origin":"FR",
         "scheme":"MASTERCARD"
      },
      "payment_options":{
         "merchant_identification":{
            "name":"MyWebSite"
         }
      },
      "reference":"3a14f7c2-abf6-4be5-9759-1a25187f250e",
      "status":"captured"
   },
   "payment_token":"cc31528d-a881-4e29-bbba-f016fe2df1dc",
   "request_token":"083bcfe3-62a3-4400-a0b0-1e1a8ac95505",
   "return_code":1
}
```

3.6.3 Précisions sur les champs « code retour » et « next_step »

Le retour fait par le service va varier en fonction de l'étape suivante à prendre en compte par le commerçant. A l'issu de cette étape, les scénarii envisageables sont :

- L'étape suivante à réaliser est **Etape 2 : Envoi des informations techniques au serveur d'authentification du porteur**
  Dans ce cas, prendre en compte le retour décrit dans le paragraphe Retour du service lorsque l'étape suivante est « Etape 2 : Envoi des informations techniques au serveur d'authentification du porteur »
- L'étape suivante à réaliser est **Etape 4 : Traitement de l'authentification 3D Secure du porteur**
  Dans ce cas, prendre en compte le retour décrit dans le paragraphe Retour du service lorsque l'étape suivante est « Etape 4 : Traitement de l'authentification 3D Secure du porteur »
- L'étape **Etape 5 : Validation du paiement** a été réalisée
  Dans ce cas, prendre en compte le retour décrit dans le paragraphe Retour du service lorsque l'étape « Etape 5 : Validation du paiement » a été réalisée

3.6.3.1 Retour du service lorsque l'étape suivante est « Etape 2 : Envoi des informations techniques au serveur d'authentification du porteur »

Pour rappel, ce retour ne sera effectué que dans le cadre d'un protocole 3D Secure V2.

3.6.3.1.1 Le champ return_code

Dans le cas nominal, la valeur retournée pour ce champ est :

Valeur	Description	Commentaire
2	Une action est attendue par le commerçant. Se référer à l'objet « next_step » pour plus de détail.	Le commerçant doit maintenant effectuer les actions nécessaires pour envoyer les informations techniques au serveur d'authentification

Pour les cas d'erreur, les valeurs suivantes peuvent être renvoyées :

Valeur	Description	Commentaire
-1	Problème technique	Un problème technique est survenu : réitérer la demande
-2	Commerçant non identifié	Les paramètres servant à identifier le site commerçant ne sont pas corrects, vérifier les champs "configuration", "language" et "point_of_sale"
-3	Commande non authentifiée	La signature MAC est invalide
-4	CB expirée	La date de validité de la carte de paiement n'est pas valide
-5	Numéro de CB erroné	Le numéro de la carte de paiement n'est pas valide
-6	Commande expirée	La date de la commande dépasse le délai autorisé (+/- 24h)
-7	Montant erroné	Le montant transmis est mal formaté ou est égal à zéro
-8	Date erronée	La date transmise est erronée
-9	CVX erroné	Le cryptogramme visuel transmis est erroné
-10	Paiement déjà autorisé	Une autorisation a déjà été délivrée pour cette demande de paiement, il est toujours possible de mettre en recouvrement le paiement
-11	Paiement déjà accepté	Le paiement relatif à cette commande a déjà fait l'objet d'un recouvrement
-12	Paiement déjà annulé	Le paiement a été annulé : aucune opération ne peut plus être effectuée sur ce paiement.
-13	Traitement en cours	Le paiement est en cours de traitement
-14	Commande grillée	Le nombre maximal de tentatives de fourniture de carte a été atteint (3 tentatives sont acceptées), la commande n'est plus acceptée par le serveur bancaire
-15	Erreur paramètres	Les paramètres transmis sont erronés
-16	Erreur résultat d'authentification 3D-Secure	Le résultat d'authentification 3D Secure transmis est invalide
-17	Le montant des échéances est erroné	Le montant des échéances transmis est mal formaté. La somme des échéances n'est pas égale au montant de la commande.
-18	La date des échéances est erronée	L'une des dates transmise est mal formatée. La différence entre les dates n'est pas d'un mois.
-19	Le nombre d'échéance n'est pas correct	Le nombre d'échéance doit être compris entre 2 et 4.
-20	La version envoyée n'est pas correcte	La version doit être égale à « 3.0 »
-21	Le paiement a été bloqué par l'option de filtrage du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « filtering » de l'objet « risk_management ».
-22	CB séquestrée expirée	La date de la carte de paiement séquestrée utilisée est expirée
-23	Le paiement a été bloqué par l'option de scoring du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « scoring » de l'objet « risk_management ».
-24	CVV non présent	Le CVV n'a pas été fourni et est obligatoire
-25	TPE fermé	Le TPE utilisé est fermé. Uniquement retourné pour les paiements effectués dans l'environnement de test (sandbox)
-26	AVS manquant	Le TPE utilisé est configuré pour réaliser une vérification de l'adresse du porteur (Address Verification System) mais l'adresse n'a pas été fournie lors de l'appel.
-27	Réseau de la carte de paiement non accepté	Le réseau de la carte de paiement n'est pas accepté par la banque ou par le commerçant

3.6.3.1.2 Objet next_step

Champ JSON	Valeur
step	technical_information_collecting
recommended_implementation	invisible_iframe
data	Les données à envoyer
url	L'url à appeler

3.6.3.1.3 Exemple(s)

```
{
   …
   "next_step":{
      "data":{
         "threeDSMethodData":"eyJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIjoiaHR0cHM6Ly90c3QtcGF5bWVudC1hcGktZS1pLWNvbS5jbS1jaWMuZnIvdGVzdC9wYXltZW50c2VydmljZS5jZ2kiLCJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjFlM2I4ZWIwLTM3ZjMtNGM0Ny1iY2E4LWQwNTYzYzQ0ZDcwOCJ9Cg=="
      },
      "recommended_implementation":[
         "invisible_iframe"
      ],
      "step":"technical_information_collecting",
      "url":"https://payment-api-e-i-com.cm-cic.fr/test/acstest.cgi"
   },
   "return_code":2,
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   …
}
```

3.6.3.1.4 Traitement à réaliser par le commerçant suite à ce retour

Le traitement à réaliser par le commerçant est décrit dans le paragraphe spécifique 4.1 La valeur du champ « step » est « technical_information_collecting ».

3.6.3.2 Retour du service lorsque l'étape suivante est « Etape 4 : Traitement de l'authentification 3D Secure du porteur »

3.6.3.2.1 Le champ return_code

Dans le cas nominal, la valeur retournée pour ce champ est :

Valeur	Description	Commentaire
2	Une action est attendue par le commerçant. Se référer à l'objet « next_step » pour plus de détail.	Le commerçant doit maintenant effectuer les actions nécessaires pour envoyer les informations techniques au serveur d'authentification

Pour les cas d'erreur, les valeurs suivantes peuvent être renvoyées :

Valeur	Description	Commentaire
-1	Problème technique	Un problème technique est survenu : réitérer la demande
-6	Commande expirée	La date de la commande dépasse le délai autorisé (+/- 24h)
-10	Paiement déjà autorisé	Une autorisation a déjà été délivrée pour cette demande de paiement, il est toujours possible de mettre en recouvrement le paiement
-11	Paiement déjà accepté	Le paiement relatif à cette commande a déjà fait l'objet d'un recouvrement
-12	Paiement déjà annulé	Le paiement a été annulé : aucune opération ne peut plus être effectuée sur ce paiement.
-13	Traitement en cours	Le paiement est en cours de traitement
-14	Commande grillée	Le nombre maximal de tentatives de fourniture de carte a été atteint (3 tentatives sont acceptées), la commande n'est plus acceptée par le serveur bancaire
-15	Erreur paramètres	Les paramètres transmis sont erronés
-16	Erreur résultat d'authentification 3D-Secure	Le résultat d'authentification 3D Secure transmis est invalide
-21	Le paiement a été bloqué par l'option de filtrage du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « filtering » de l'objet « risk_management ».
-23	Le paiement a été bloqué par l'option de scoring du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « scoring » de l'objet « risk_management ».
-27	Réseau de la carte de paiement non accepté	Le réseau de la carte de paiement n'est pas accepté par la banque ou par le commerçant

3.6.3.2.2 Objet next_step

Champ JSON	Valeur
step	cardholder_authentication
recommended_implementation	redirect
data	Les données à envoyer
url	L'url à appeler

L'objet « data » est alimenté différemment en fonction de la version du protocole 3D Secure :

- 3DSecure V2 : les champs « threeDSSessionData » et « creq » sont renvoyés dans cet objet
  - Le champ « threeDSSessionData» permettra l'identification du paiement lors du retour du serveur d'authentification
  - Le champ « creq » contient les données à fournir au serveur d'authentification
- SecurePlus : le champ « ACPReq » est renvoyé dans cet objet, il contient les données à fournir au serveur d'authentification

3.6.3.2.3 Exemple(s)

Exemple de retour pour un paiement s'effectuant selon le processus 3D Secure V2


```
{
   …
   "next_step":{
      "data":{
         "creq":"ew0KICAgImFjc1RyYW5zSUQiIDogIjI1ZjE5MjliLWUwZGItNGE0Yi04YTdjLWE
0MzBiNDI2MTdmZSIsDQogICAiY2hhbGxlbmdlV2luZG93Sl6ZSIgOiAiMDUiLA0KICAgIm1lc3NhZ2V
UeXBlIiA6ICJDUmVxIiwNCiAgICJtZXNzYWdlVmVyc2lvbiIgOiAiMi4xLjAiLA0KICAgInRocmVlRFN
TZXJ2ZXJUcmFuc0lEIiA6ICI0YzI2MjFjMy0xNjQ4LTRjNTEtODU5Zi1mNDEzYjc2MWJjZDMiDQp9DQo
",
         "threeDSSessionData":"NmVlMjQ4YzktZjczZC00NTNhLThiZjktODI0ZTQ5YjczNTI0"
      },
      "recommended_implementation":[
         "iframe",
         "redirect"
      ],
      "step":"cardholder_authentication",
      "url":"https://payment-api-e-i-com.cm-cic.fr/test/acstest.cgi"
   },
   "return_code":2,
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   …
}
```


Exemple de retour pour un paiement s'effectuant selon le processus SecurePlus


```
{
   …
   "next_step":{
      "data":{
         "ACPReq":"<UPACPPay><MsgReq><version>5.0.0</version><encoding>UTF-
8</encoding><certId>69798631478</certId><signMethod>01</signMethod><txnType>79</t
```

```
xnType><txnSubType>10</txnSubType><bizType>000301</bizType><accessType>1</accessT
ype><channelType>07</channelType><frontUrl>https://www.merchant-backend-
url.com</frontUrl><backUrl>https://www.merchant-backend-
url.com</backUrl><acqInsCode>31310250</acqInsCode><merId>0145992</merId><merCatCo
de>7372</merCatCode><merName>MerchantName</merName><merAbbr>MerchantNameAbbreviat
ion</merAbbr><orderId>30eba822f18745c2a0d2</orderId><txnTime>20221230190712</txnT
ime><accType></accType><accNo>62228212XXXXXX17</accNo><currencyCode>978</currency
Code><txnAmt>501</txnAmt><reqReserved><id>bb2ffdf634774f519dc050a85c794c03</id></
reqReserved><reserved><country>250</country><merUrl>https://www.merchant-url.com
</merUrl></reserved><customerInfo></customerInfo><encryptCertId></encryptCertId><
relTxnType>01</relTxnType><customerIp></customerIp></MsgReq><Signature><Signature
Value>oBifHROeSfPIOtUAKzxHu4veQlrr/pr9V6mIkBHvxWE+qz1766rga3rX9f3ZsAc4vzeSRupc2mN
Z7wDJIjvAjes7eg/7ACpiqtVgAVRMXmemPHe4Zckxe4Dj7mxPNp+SBHpzi/yQcAZCIe3Kt6heI2r7+d+B
9vLeiX+8Str+tDNdOkJj2mtdWdUH2f99B+q5+exckr3ZidLp3x0DVK2KJaqVg/KhpszqSvD09Q9/3WyqG
A2oiTVMHYZW6Pnyz9j0Xnoj3VvBJPtqOK3OdijnfjvR1XVw5HEg7zfrBgsEyrLeNxTOK6hTmRKTyF4gYO
NtC6Y7bg0DenHZIT9k7yXCGg==</SignatureValue></Signature></UPACPPay>"
      },
      "recommended_implementation":[
         "redirect"
      ],
      "step":"cardholder_authentication",
      "url":" http://url-acs-client/acs.cgi"
   },
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   "return_code":2,
   …
}
```


3.6.3.2.4 Traitement à réaliser par le commerçant suite à ce retour

Le traitement à réaliser par le commerçant est décrit dans le paragraphe spécifique 4.2 Le retour effectué est « cardholder_authentication ».

3.6.3.3 Retour du service lorsque l'étape « Etape 5 : Validation du paiement » a été réalisée

3.6.3.3.1 Le champ return_code

Dans le cas nominal, la valeur retournée pour ce champ est :

Valeur	Description	Commentaire
0	Paiement non effectué	L'autorisation bancaire n'a pas été délivrée : la demande d'autorisation a été refusée.
1	Demande d'autorisation acceptée	L'autorisation bancaire a été délivrée et la mise en recouvrement a été effectuée.

Pour les cas d'erreur, les valeurs suivantes peuvent être renvoyées :

Valeur	Description	Commentaire
-1	Problème technique	Un problème technique est survenu : réitérer la demande
-6	Commande expirée	La date de la commande dépasse le délai autorisé (+/- 24h)
-10	Paiement déjà autorisé	Une autorisation a déjà été délivrée pour cette demande de paiement, il est toujours possible de mettre en recouvrement le paiement
-11	Paiement déjà accepté	Le paiement relatif à cette commande a déjà fait l'objet d'un recouvrement
-12	Paiement déjà annulé	Le paiement a été annulé : aucune opération ne peut plus être effectuée sur ce paiement.
-13	Traitement en cours	Le paiement est en cours de traitement
-14	Commande grillée	Le nombre maximal de tentatives de fourniture de carte a été atteint (3 tentatives sont acceptées), la commande n'est plus acceptée par le serveur bancaire
-15	Erreur paramètres	Les paramètres transmis sont erronés
-16	Erreur résultat d'authentification 3D-Secure	Le résultat d'authentification 3D Secure transmis est invalide
-21	Le paiement a été bloqué par l'option de filtrage du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « filtering » de l'objet « risk_management ».
-22	CB séquestrée expirée	La date de la carte de paiement séquestrée utilisée est expirée
-23	Le paiement a été bloqué par l'option de scoring du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « scoring » de l'objet « risk_management ».

3.6.3.3.2 Objet next_step

L'objet « next_step » n'est pas retourné dans ce cas.

3.6.3.3.3 Exemple(s)


```
{
   "authentication":{
      "details":{
         "CRes":"Y",
         "ARes":"C",
         "status3DS":1,
      },
      "protocol":"3DSecure",
      "status":"authenticated",
      "version":"2.1.0"
   },
   "merchant_configuration":{
      "configuration":"emulation3d",
      "language":"FR",
      "point_of_sale":"9000001",
      "version":"3.0"
   },
   "payment":{
      "amount":{
         "currency":"EUR",
         "exponent":2,
         "value":10001
      },
      "authorisation":{
         "date":"2019-09-06",
         "number":"000000"
      },
      "payment_mean":{
         "ecard":false,
         "expiry_date":"2035-12",
         "hpan":"C5F5A5ACAACB96129882D1A9DB9E1FBBED4FBE93",
         "masked_account_number":"000003******0007",
         "origin":"FR",
         "scheme":"MASTERCARD"
      },
      "reference":"3a14f7c2-abf6-4be5-9759-1a25187f250e",
      "status":"captured"
   },
   "payment_token":"cc31528d-a881-4e29-bbba-f016fe2df1dc",
   "request_token":"083bcfe3-62a3-4400-a0b0-1e1a8ac95505",
   "return_code":1
}
```

3.6.3.3.4 Traitement à réaliser par le commerçant suite à ce retour

Le résultat de la demande de paiement a été fourni par la plateforme Monetico paiement : le commerçant peut maintenant faire son traitement métier en fonction du retour fourni (paiement accepté ou non).

3.7 Appel de l'interface « retour » du commerçant

Attention : Cette section concerne uniquement les transactions effectuées via le SDK mobile Monetico Paiement.

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 crédit), l'interface retour n'est pas appelée.

L'interface de retour dispose de 30 secondes pour répondre comme décrit au chapitre 3.7.2. 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).

Le calcul du sceau à l'interface « Retour » est fait en utilisant la nouvelle méthode de calcul du sceau.

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

3.7.1 Paramètres renvoyés par Monetico Paiement

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

Champ	**code-retour**
Description	Le résultat du paiement
Format Valeurs possibles	Chaine de caractères payetest : paiement accepté (en « sandbox » uniquement) paiement : paiement accepté (en Production uniquement) annulation : paiement refusé En paiement fractionné, pour les mises en recouvrement automatique des échéances de rang > 1 : paiement_pf[N] : paiement accepté de l'échéance N (N entre 2 et 4) Annulation_pf[N] : paiement refusé définitivement de l'échéance N (N entre 2 et 4)
Complément	En cas de paiement refusé, une autorisation ultérieure pourra encore être délivrée pour la même référence. Le code « payetest » n'est envoyé que pour des paiements effectués dans l'environnement « sandbox ». Si ce code est présent lors d'un paiement en production, il s'agit d'une anomalie.
Exemple	paiement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Champ	**motifrefus**
Description	Motif du refus de la demande de paiement
Format **Valeur(s) possible(s)**	**Appel Phonie** : la banque du client demande des informations complémentaires **Refus** : la banque du client refuse d'accorder l'autorisation **Interdit** : la banque du client refuse d'accorder l'autorisation **filtrage** : la demande de paiement a été bloquée par le paramétrage de filtrage que le commerçant a mis en place dans son Module Prévention Fraude **scoring** : la demande de paiement a été bloquée par le paramétrage de scoring que le commerçant a mis en place dans son Module Prévention Fraude **3DSecure** : si le refus est lié à une authentification 3DSecure négative reçue de la banque du porteur
Complément	Uniquement dans le cas où la demande de paiement a été refusée

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

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

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

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

Champ	**originetr**
Description	Code pays de l'origine de la transaction
Format	Norme ISO 3166-1
Complément	Uniquement en cas de souscription du module prévention fraude

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

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

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

Champ	**filtragecause**
Description :	Numéros des types de filtres bloquant le paiement (cf. tableau « Retours Module Prévention Fraude – détails » ci-dessous)
Format **Valeur(s) possible(s)**	1 : Adresse IP 2 : Numéro de carte 3 : BIN de carte 4 : Pays de la carte 5 : Pays de l'IP 6 : Cohérence pays de la carte / pays de l'IP 7 : Email jetable 8 : Limitation en montant pour une CB sur une période donnée 9 : Limitation en nombre de transactions pour une CB sur une période donnée 11 : Limitation en nombre de transactions par alias sur une période donnée 12 : Limitation en montant par alias sur une période donnée 13 : Limitation en montant par IP sur une période donnée 14 : Limitation en nombre de transactions par IP sur une période donnée 15 : Testeurs de cartes 16 : Limitation en nombre d'alias par CB
Complément	Uniquement dans le cas d'un filtrage du paiement ou si le mode information est activé. Si plusieurs filtres bloquent le paiement, ceux-ci sont séparés par des tirets. Les causes et les valeurs correspondantes étant dans le même ordre.

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

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

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

Champ	**cbmasquee**
Description	Le numéro de carte tronqué en conformité avec PCI DSS
Format Valeur(s) possible(s)	Le format dépend de la longueur du numéro de carte : - 8 premiers et 2 derniers chiffres de la carte de paiement du client, séparés par des étoiles pour les numéros de carte ayant une longueur de 16 chiffres ou plus - 6 premiers chiffres, 6 étoiles, le reste des chiffres de la carte de paiement du client pour les numéros de carte ayant une longueur de moins de 16 chiffres
Exemple	12345678******12 123456******123
Complément	Uniquement en cas de souscription de l'option paiement express et lors de l'enregistrement de la carte

Champ	**modepaiement**
Description	Moyen de paiement utilisé
Format Valeur(s) possible(s)	CB paypal 1euro 3xcb 4xcb audiotel

Retours Module Prévention Fraude – Détails

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

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

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

TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&refer
ence=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-
libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1208&brand=VI&
&numauto=010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADB
FC1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&
authentification=ewoJIn(…)KfQo=

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

TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&refer
ence=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-
libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1208&brand=VI&
numauto=010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADBF
C1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&
montantech=20EUR&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=9000001&date=05%2f10%2f2011%5fa%5f15%3a33%3a06&montant=1%2e01EUR&refere
nce=P1317821466&MAC=70156D2CFF27A9B8AAE5AFEBE590D9CFCAAF9BDC&texte-
libre=Ceci+est+un+test%2c+ne+pas+tenir+compte%2e&code-
retour=Annulation&cvx=oui&vld=0912&brand=MC&status3ds=-
1&motifrefus=filtrage&originecb=FRA&bincb=513283&hpancb=764AD24CFABBB818E8A
7DC61D4D6B4B89EA837ED&ipclient=10%2e45%2e166%2e76&originetr=inconnue&veres=
&pares=&filtragecause=4-&filtragevaleur=FRA-

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

TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%2e75EUR&refer
ence=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016c202e89947b04&texte-
libre=LeTexteLibre&code-retour=paiement&cvx=oui&vld=1208&brand=VI&
numauto=010101&originecb=FRA&bincb=010101&hpancb=74E94B03C22D786E0F2C2CADBF
C1C00B004B7C45&ipclient=127%2e0%2e0%2e1&originetr=FRA&cbenregistree=1&cbmas
quee=123456******7890&authentification=ewoJIn(…)KfQo=

3.7.2 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.

3.7.2.1 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.

3.7.2.2 Création de l'accusé de réception

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

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

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

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

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

Dès la phase de test, le commerçant doit nous fournir l'adresse d'une boîte aux lettres électronique régulièrement relevée. Pour passer en production, le serveur commerçant doit avoir renvoyé un accusé de réception avec un sceau validé pour les trois derniers tests.

4 Traitement du retour du service de paiement lorsqu'une action est demandée au commerçant

Ce paragraphe donne des précisions sur le traitement à effectuer lorsque le code retour du service est « 2 : Une action est attendue par le commerçant». Dans ce cas, il faut se référer à l'objet « next_step » :

- le champ « step » : il précise le type de traitement à réaliser. Les valeurs possibles sont
  - technical_information_collecting : le commerçant doit envoyer les informations techniques de l'environnement du porteur de carte de paiement à l'émetteur.
  - cardholder_authentication : le commerçant doit initier le traitement d'authentification du porteur de carte de paiement (processus 3D Secure)
- le champ « recommended_implementation » donne une recommandation d'implémentation pour effectuer le traitement.

4.1 La valeur du champ « step » est « technical_information_collecting »

Pour rappel, ce retour peut être fourni en retour de la phase 1 : Initialisation du paiement.

4.1.1 Exemple(s) de retour


```
{
   …
   "next_step":{
      "data":{
         "threeDSMethodData":"eyJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIjoiaHR0cHM6Ly90c3QtcGF5bWVudC1hcGktZS1pLWNvbS5jbS1jaWMuZnIvdGVzdC9wYXltZW50c2VydmljZS5jZ2kiLCJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjFlM2I4ZWIwLTM3ZjMtNGM0Ny1iY2E4LWQwNTYzYzQ0ZDcwOCJ9Cg=="
      },
      "recommended_implementation":[
         "invisible_iframe"
      ],
      "step":"technical_information_collecting",
      "url":"https://payment-api-e-i-com.cm-cic.fr/test/acstest.cgi"
   },
   "return_code":2,
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   …
}
```

4.1.2 Implémentation(s) recommandée(s)

Le commerçant doit récupérer le script accessible à l'url indiquée (avec un formulaire contenant un champ « threeDSMethodData ») puis l'exécuter sur le navigateur du client dans une iframe invisible :

Il existe plusieurs possibilités pour masquer un iframe en utilisant un style CSS tels que :

- style="display: none;"
- style="width:0;height:0;border:0; border:none;"

Le formulaire quant à lui peut s'implémenter de la sorte.

```
<form name="formulaire" id="formulaire"  action="http://url-acs-client/acs.cgi" method="post">
      <input type="text" name="threeDSMethodData"
                  value="eyJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIjoiaHR0cHM6Ly9ycX
                  QtcGF5bWVudC1hcGkuZS1pLmNvbS90ZXN0L3BheW1lbnRzZXJ2aWNlLmNnaSIsIn
                  RocmVlRFNTZXJ2ZXJUcmFuc0lEIjoiZDc4MmJkNzktODEwMi00ZTQyLThhZDEtOTR
                  mNjAyOGVhMDE5In0K">
      <input type="submit" value="Continuer">
</form>
```

La soumission peut-elle être réalisée via du JavaScript avec une directive basique telle que

```
document.getElementById(formulaire).submit();
```

4.2 Le retour effectué est « cardholder_authentication »

Pour rappel, ce retour peut être fourni en retour de la phase 2 : envoi des informations techniques au serveur d'authentification.

4.2.1 Exemple(s) de retour

Exemple de retour pour un paiement s'effectuant selon le processus 3D Secure V2


```
{
   …
   "next_step":{
      "data":{
         "creq":"ew0KICAgImFjc1RyYW5zSUQiIDogIjI1ZjE5MjliLWUwZGItNGE0Yi04YTdjLWE
0MzBiNDI2MTdmZSIsDQogICAiY2hhbGxlbmdlV2luZG93U2l6ZSIgOiAiMDUiLA0KICAgIm1lc3NhZ2V
UeXBlIiA6ICJDUmVxIiwNCiAgICJtZXNzYWdlVmVyc2lvbiIgOiAiMi4xLjAiLA0KICAgInRocmVlRFN
TZXJ2ZXJUcmFuc0lEIiA6ICI0YzI2MjFjMy0xNjQ4LTRjNTEtODU5Zi1mNDEzYjc2MWJjZDMiDQp9",
         "threeDSSessionData":"NmVlMjQ4YzktZjczZC00NTNhLThiZjktODI0ZTQ5YjczNTI0"
      },
      "recommended_implementation":[
         "iframe",
         "redirect"
      ],
      "step":"cardholder_authentication",
      "url":" http://url-acs-client/acs.cgi"
   },
   "return_code":2,
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   …
}
```


Exemple de retour pour un paiement s'effectuant selon le processus SecurePlus


```
{
   …
   "next_step":{
      "data":{
         "ACPReq":"<UPACPPay><MsgReq><version>5.0.0</version><encoding>UTF-
8</encoding><certId>69798631478</certId><signMethod>01</signMethod><txnType>79</t
xnType><txnSubType>10</txnSubType><bizType>000301</bizType><accessType>1</accessT
ype><channelType>07</channelType><frontUrl>https://www.merchant-backend-
url.com</frontUrl><backUrl>https://www.merchant-backend-
url.com</backUrl><acqInsCode>31310250</acqInsCode><merId>0145992</merId><merCatCo
de>7372</merCatCode><merName>MerchantName</merName><merAbbr>MerchantNameAbbreviat
ion</merAbbr><orderId>30eba822f18745c2a0d2</orderId><txnTime>20221230190712</txnT
ime><accType></accType><accNo>62228212XXXXXX17</accNo><currencyCode>978</currency
Code><txnAmt>501</txnAmt><reqReserved><id>bb2ffdf634774f519dc050a85c794c03</id></
reqReserved><reserved><country>250</country><merUrl>https://www.merchant-url.com
</merUrl></reserved><customerInfo></customerInfo><encryptCertId></encryptCertId><
relTxnType>01</relTxnType><customerIp></customerIp></MsgReq><Signature><Signature
Value>oBifHROeSfPIOtUAKzxHu4veQlrr/pr9V6mIkBHvxWE+qz1766rga3rX9f3ZsAc4vzeSRupc2mN
Z7wDJIjvAjes7eg/7ACpiqtVgAVRMXmemPHe4Zckxe4Dj7mxPNp+SBHpzi/yQcAZCIe3Kt6heI2r7+d+B
```

```
9vLeiX+8Str+tDNdOkJj2mtdWdUH2f99B+q5+exckr3ZidLp3x0DVK2KJaqVg/KhpszqSvD09Q9/3WyqG
A2oiTVMHYZW6Pnyz9j0Xnoj3VvBJPtqOK3OdijnfjvR1XVw5HEg7zfrBgsEyrLeNxTOK6hTmRKTyF4gYO
NtC6Y7bg0DenHZIT9k7yXCGg==</SignatureValue></Signature></UPACPPay>"
      },
      "recommended_implementation":[
         "redirect"
      ],
      "step":"cardholder_authentication",
      "url":" http://url-acs-client/acs.cgi"
   },
   "payment_token":"6ee248c9-f73d-453a-8bf9-824e49b73524",
   "return_code":2,
   …
}
```


4.2.2 Implémentation(s) recommandée(s)

4.2.2.1 3D Secure V2

4.2.2.1.1 Utilisation d'un formulaire

Le commerçant devra rediriger le client, à l'aide d'un formulaire employant la méthode POST, sur l'URL du serveur d'authentification de sa banque (champ « url » fourni en retour).

Le formulaire devra comporter les champs suivants :

Champ	Description
action	La valeur de ce champ est à récupérer directement du champ « url » fourni lors du retour du service de demande de paiement par API.
creq	La valeur de ce champ est à récupérer directement du champ « CReq » fourni lors du retour du service de demande de paiement par API.
threeDSSessionData	La valeur de ce champ est à récupérer directement du champ « threeDSSessionData» fourni lors du retour du service de demande de paiement par API.

Exemple(s) de formulaire:

```
<form name="formulaire" id="formulaire" action="http://url-acs-client/acs.cgi" method="post">
      <input type="hidden" name="creq"
                  value="IT8ubu+5z4YupUCOEHKsbiPep8UzIAcPKJlzD8H0iGQRauaas9dX65ghj321rt
                  y63ffhg632r65ghj321rty63ffhMLODrtyghjEHKsbiPep8UzIAcPKJEjpwGlzD8HEHKsbiP
                  ep8UzIAcPKJEjpwGlzD8HrypeUCOEHKsbiPdfg5jh8353213587ert5ezer">
      <input type="hidden" name="threeDSSessionData"
                  value="NmVlMjQ4YzktZjczZC00NTNhLThiZjktODI0ZTQ5YjczNTI0">
      <input type="submit" value="Cliquez ici pour vous authentifier sur le serveur de votre banque">
</form>
```

4.2.2.1.2 Utilisation d'une iframe

Le commerçant doit récupérer le code html nécessaire pour l'affichage de la fenêtre de « challenge ». Pour cela, il doit placer le formulaire décrit ci-dessus au sein de l'iframe : la différence entre les deux implémentations est uniquement la localisation de ce formulaire (soit dans la page principale, soit dans une iframe).

4.2.2.2 SecurePlus

Le commerçant devra rediriger le client, à l'aide d'un formulaire employant la méthode POST, sur l'URL du serveur d'authentification de sa banque (champ « url » fourni en retour).

Le formulaire devra comporter les champs suivants :

Champ	Description
action	La valeur de ce champ est à récupérer directement du champ « url » fourni lors du retour du service de demande de paiement par API.
ACPReq	La valeur de ce champ est à récupérer directement du champ « ACPReq » fourni lors du retour du service de demande de paiement par API.

Exemple(s) de formulaire :

```
<form name="formulaire" id="formulaire" action="http://url-acs-client/acs.cgi" method="post">
    <input type="hidden" name="ACPReq"
        value="<UPACPPay><MsgReq><version>5.0.0</version><encoding>UTF-
        8</encoding><certId>69798631478</certId><signMethod>01</signMethod><txnType
        >79</txnType><txnSubType>10</txnSubType><bizType>000301</bizType><access
        Type>1</accessType><channelType>07</channelType><frontUrl>https://www.merch
        ant-backend-url.com</frontUrl><backUrl>https://www.merchant-backend-
        url.com</backUrl><acqInsCode>31310250</acqInsCode><merId>0145992</merId><
        merCatCode>7372</merCatCode><merName>MerchantName</merName><merAbb
        r>MerchantNameAbbreviation</merAbbr><orderId>30eba822f18745c2a0d2</orderId
        ><txnTime>20221230190712</txnTime><accType></accType><accNo>62228212XX
        XXXX17</accNo><currencyCode>978</currencyCode><txnAmt>501</txnAmt><reqR
        eserved><id>bb2ffdf634774f519dc050a85c794c03</id></reqReserved><reserved><c
        ountry>250</country><merUrl>https://www.merchant-url.com
        </merUrl></reserved><customerInfo></customerInfo><encryptCertId></encryptCertId
        ><relTxnType>01</relTxnType><customerIp></customerIp></MsgReq><Signature><
        SignatureValue>oBifHROeSfPIOtUAKzxHu4veQlrr/pr9V6mIkBHvxWE+qz1766rga3rX
        9f3ZsAc4vzeSRupc2mNZ7wDJIjvAjes7eg/7ACpiqtVgAVRMXmemPHe4Zckxe4Dj7mx
        PNp+SBHpzi/yQcAZCIe3Kt6heI2r7+d+B9vLeiX+8Str+tDNdOkJj2mtdWdUH2f99B+q5
        +exckr3ZidLp3x0DVK2KJaqVg/KhpszqSvD09Q9/3WyqGA2oiTVMHYZW6Pnyz9j0Xn
        oj3VvBJPtqOK3OdijnfjvR1XVw5HEg7zfrBgsEyrLeNxTOK6hTmRKTyF4gYONtC6Y7b
        g0DenHZIT9k7yXCGg==</SignatureValue></Signature></UPACPPay>">
    <input type="submit" value="Cliquez ici pour vous authentifier sur le serveur de votre banque">
</form>
```

5 Annexes

5.1 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 : paiement@cm.monetico-services.com
  - CIC : paiement@cic.monetico-services.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.

5.2 Glossaire 3D-Secure

Terme	Description	Version 3D Secure
ACS	Serveur sécurisé d'authentification 3D-Secure d'un émetteur de carte de paiement.	
MPI	Plug-in marchand : module logiciel qui permet de vérifier l'enrôlement 3D-Secure d'une carte de paiement et de retourner l'adresse du site Web du serveur d'authentification de la banque du porteur.	
AReq	Message initial du flux d'authentification. Il peut contenir des informations sur le titulaire de la carte, le paiement et l'appareil pour la transaction.	2.1.0
ARes	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.	2.1.0
CReq	Initie une interaction de titulaire de carte dans un flux de challenge et peut être utilisé pour transporter des données d'authentification provenant du titulaire de carte.	2.1.0
CRes	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.	2.1.0
3DS method	Permet à un système ACS de collecter des informations supplémentaires sur le navigateur avant la réception du message AReq afin de faciliter l'évaluation du risque de transaction. L'utilisation de la méthode 3DS par un ACS est facultative.	2.1.0
ACPReq	Requête d'authentification du client pour les cartes UnionPay.	
ACPRes	Résultat de la requête d'authentification du client pour les cartes UnionPay.	

5.3 Liste complète des valeurs du champ « return_code »

5.3.1 Valeurs possibles dans les cas nominaux

Valeur	Description	Commentaire
0	Paiement non effectué	L'autorisation bancaire n'a pas été délivrée : la demande d'autorisation a été refusée.
1	Demande d'autorisation acceptée	L'autorisation bancaire a été délivrée et la mise en recouvrement a été effectuée.
2	Une action est attendue par le commerçant. Se référer à l'objet « next_step » pour plus de détail.	Le commerçant doit maintenant effectuer les actions nécessaires pour envoyer les informations techniques au serveur d'authentification

5.3.2 Valeurs possibles dans les cas d'erreurs

Valeur	Description	Commentaire
-1	Problème technique	Un problème technique est survenu : réitérer la demande
-2	Commerçant non identifié	Les paramètres servant à identifier le site commerçant ne sont pas corrects, vérifier les champs "configuration", "language" et "point_of_sale"
-3	Commande non authentifiée	La signature MAC est invalide
-4	CB expirée	La date de validité de la carte de paiement n'est pas valide
-5	Numéro de CB erroné	Le numéro de la carte de paiement n'est pas valide
-6	Commande expirée	La date de la commande dépasse le délai autorisé (+/- 24h)
-7	Montant erroné	Le montant transmis est mal formaté ou est égal à zéro
-8	Date erronée	La date transmise est erronée
-9	CVX erroné	Le cryptogramme visuel transmis est erroné
-10	Paiement déjà autorisé	Une autorisation a déjà été délivrée pour cette demande de paiement, il est toujours possible de mettre en recouvrement le paiement
-11	Paiement déjà accepté	Le paiement relatif à cette commande a déjà fait l'objet d'un recouvrement
-12	Paiement déjà annulé	Le paiement a été annulé : aucune opération ne peut plus être effectuée sur ce paiement.
-13	Traitement en cours	Le paiement est en cours de traitement
-14	Commande grillée	Le nombre maximal de tentatives de fourniture de carte a été atteint (3 tentatives sont acceptées), la commande n'est plus acceptée par le serveur bancaire
-15	Erreur paramètres	Les paramètres transmis sont erronés
-16	Erreur résultat d'authentification 3D-Secure	Le résultat d'authentification 3D Secure transmis est invalide
-17	Le montant des échéances est erroné	Le montant des échéances transmis est mal formaté. La somme des échéances n'est pas égale au montant de la commande.
-18	La date des échéances est erronée	L'une des dates transmise est mal formatée. La différence entre les dates n'est pas d'un mois.
-19	Le nombre d'échéance n'est pas correct	Le nombre d'échéance doit être compris entre 2 et 4.
-20	La version envoyée n'est pas correcte	La version doit être égale à « 3.0 »

-21	Le paiement a été bloqué par l'option de filtrage du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « filtering » de l'objet « risk_management ».
-22	CB séquestrée expirée	La date de la carte de paiement séquestrée utilisée est expirée
-23	Le paiement a été bloqué par l'option de scoring du Module de Prévention de Fraude	Les raisons du blocage sont présents dans la balise « scoring » de l'objet « risk_management ».
-24	CVV non présent	Le CVV n'a pas été fourni et est obligatoire
-25	TPE fermé	Le TPE utilisé est fermé. Uniquement retourné pour les paiements effectués dans l'environnement de test (sandbox)
-26	AVS manquant	Le TPE utilisé est configuré pour réaliser une vérification de l'adresse du porteur (Address Verification System) mais l'adresse n'a pas été fournie lors de l'appel.
-27	Réseau de la carte de paiement non accepté	Le réseau de la carte de paiement n'est pas accepté par la banque ou par le commerçant

5.4 Liste complète des retours du Module Prévention Fraude

La fonctionnalité de filtrage des paiements s'appuie sur un ensemble de neuf filtres, librement paramétrable sur le tableau de bord. Chacun de ces filtres agit sur un critère spécifique, comme l'adresse IP du client, son adresse 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	Nombre de transactions cumulées sur la période	

	sur une période donnée	donnée associée à l'adresse IP du client	
15	Testeurs de cartes	Nombre de transactions cumulées sur la période donnée associée à l'adresse IP du client	
16	Limitation en nombre d'alias par CB	Les alias déjà associés à la carte utilisée pour le paiement	Uniquement en cas de souscription de l'option paiement express Fonctionne uniquement pour les paiements par carte. Fonctionne uniquement pour les paiements par carte

5.5 Calcul du sceau MAC pour l'appel à l'interface retour.

Le sceau (à mettre dans le champ MAC) est calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.
Cette fonction générera le sceau à partir de données à certifier et de la clé de sécurité commerçant sous sa forme opérationnelle.

Les données à certifier sont structurées :

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

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

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

Remarque :

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

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

5.5.1 Exemple de chaînes permettant le calcul du sceau lors de la phase retour

Paiement simple avec inscription au module prévention fraude et à l'option 3D Secure

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