

Monetico Paielement

Paielement sécurisé sur Internet

Service Etat Paielement



SOMMAIRE

1.	Introduction	3
1.1.	Principe	3
1.2.	Clé de sécurité commerçant	3
2.	Spécification des messages échangés	4
2.1.	Appel du module état paiement	4
2.1.1.	Calcul du sceau	5
2.2.	Réponse du module état paiement	5
2.2.1.	Eléments supplémentaires spécifiques à la version 3.0	14
2.2.2.	Liste des valeurs du code retour dans les messages XML (balise <cdr>)	21
3.	Utilisation du service	22
2.3.	En Test	22
2.4.	En Production	22
2.5.	Assistance technique	22
4.	Aides à l'installation	23
2.6.	Les problèmes les plus fréquents	23
4.1.1.	Problème de calcul du sceau de sécurité	23
4.1.2.	La commande ne peut pas être trouvée	24

1. Introduction

1.1. Principe

Le but du module « Etat paiement » est de permettre aux commerçants et partenaires d'obtenir des informations sur une demande de paiement effectuée antérieurement sur notre plateforme de paiement. Afin de vérifier la validité des données d'entrée, un sceau est calculé sur l'ensemble des données fournies par le commerçant.

1.2. Clé de sécurité commerçant

Une clé de sécurité, propre à chaque TPE, destinée à certifier les données d'entrée du commerçant, est indispensable pour utiliser le module « état paiement ». Un lien, permettant de télécharger cette clé de sécurité, est envoyé par notre centre de support au commerçant.

Le commerçant peut demander la régénération d'une nouvelle clé, périodiquement ou à l'occasion d'évènements tels qu'une mise en production, un changement d'hébergeur, un changement de prestataire, etc.

Il est de la responsabilité du commerçant de conserver cette clé de façon sûre et confidentielle en exploitant les meilleurs outils disponibles dans son environnement.

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

2. Spécification des messages échangés

2.1. Appel du module état paiement

Les informations de la demande sont envoyées au serveur de la banque par un message HTTPS, en utilisant le protocole de sécurisation des échanges TLS V1.2 uniquement. L'application du commerçant doit émettre une requête en méthode POST à destination du service « état paiement » sur les serveurs de la banque, contenant les champs suivants (obligatoires) :

Champs	Description	Remarque
version	Version du module état paiement utilisé Valeurs possibles : <ul style="list-style-type: none"> - 2.0 : version générique sans les informations spécifiques aux paiements à série - 3.0 : version ajoutant les informations spécifiques aux paiements à série 	
TPE	Numéro de TPE Virtuel du commerçant Format : 7 caractères alphanumériques Exemple : 1234567	
date	Date de la commande Format : JJ/MM/AAAA Exemple : 05/12/2022	
montant	Montant TTC de la commande Format : <ul style="list-style-type: none"> - Un nombre entier - Un point décimal (optionnel) - Un nombre entier de 2 chiffres (optionnel) - Une devise sur 3 caractères alphabétiques ISO4217 Exemples : 62.73EUR ou 1024USD	Un arrondi est effectué automatiquement s'il y a plus de 2 décimales
reference	Référence unique de paiement fournie lors de la demande de paiement Format : 12 caractères alphanumériques Exemple : ABERTYP00145	
societe	Libellé ou code permettant au commerçant d'utiliser le même TPE Virtuel pour des sites différents (paramétrages distincts) se rapportant à la même activité Format : alphanumérique Exemple : monSite1	Ce code est fourni par nos services

MAC	Sceau issu de la certification des données Format : 40 caractères hexadécimaux	Il ne s'agit pas de la clé MAC mais du sceau calculé à l'aide de celle-ci
------------	---	---

2.1.1. Calcul du sceau

Le sceau (à mettre dans le champ MAC) est calculé à l'aide d'une fonction de hachage cryptographique en combinaison avec une clé secrète respectant les spécifications de la RFC 2104.

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.

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](#).

Exemple pour une demande :

```
TPE=1234567*date=25/10/2019*montant=457.15EUR*reference=4107e16d-1a30-407f-84a3-7732e3bddf64*societe=site*version=2.0
```

2.2. Réponse du module état paiement

Le module « Etat paiement » renvoie au commerçant un message au format XML.

La balise <cdr> du message de retour est présente uniquement si une erreur a été rencontrée lors de la requête de l'état d'une demande de paiement. Elle contient une valeur négative (<0).

Voici la description des balises des messages XML renvoyés au commerçant :

Balise	Description	Remarque
--------	-------------	----------

<cdr>	Code retour en cas d'erreur uniquement Valeurs possibles : voir section 2.2.2	Uniquement en cas d'erreur
<etat>	Etat dans lequel se trouve la demande de paiement Valeurs possibles : <ul style="list-style-type: none"> - EN : le client n'a pas encore renseigné sa carte - AU : autorisation accordée, en attente de mise en recouvrement - RE : autorisation refusée - GR : le client a atteint le nombre maximum de tentatives infructueuses ; la demande de paiement est invalidée - AN : demande de paiement annulée - PA : paiement recouvré - PP : paiement partiel accepté - PF : paiement fractionné accepté - PR : paiement récurrent accepté - TR : demande en cours de traitement - AP : demande de paiement refusée pour cause d'appel phonie (obsolète) 	
<protocole>	Le protocole utilisé pour la demande de paiement Valeurs possibles : Paypal	Obsolète, remplacé par <moyenpaiement> Uniquement présent pour un paiement Paypal
<cvx>	Indique si le cryptogramme visuel a été saisi au moment du paiement Valeurs possibles : oui, non	Uniquement si le paiement est un paiement carte
<vld>	Date de validité de la carte utilisée pour effectuer le paiement Format : MMAA Exemple : 2212	Uniquement si le paiement est un paiement carte
<brand>	Réseau/marque de la carte utilisée pour le paiement Valeurs possibles : <ul style="list-style-type: none"> - AM : American Express 	Uniquement si le paiement est un paiement carte

	<ul style="list-style-type: none"> - CB : GIE CB - MC : Mastercard - VI : Visa - na : non disponible 	
<status3d>	<p>Indicateur de résultat de l'échange 3DSecure</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - -1 : la transaction ne s'est pas faite selon le protocole 3DSecure, le risque d'impayé est élevé - 1 : la transaction s'est faite selon le protocole 3DSecure et le risque d'impayé est faible - 4 : la transaction s'est faite selon le protocole 3DSecure et le risque d'impayé est élevé 	Uniquement si le paiement est un paiement carte
<numauto>	<p>Numéro d'autorisation tel que fourni par la banque émettrice</p> <p>Format : chaîne de caractères à la discrétion de la banque émettrice (en général alphanumérique)</p>	Uniquement lorsque l'autorisation a été accordée pour les paiements immédiats, différés et fractionnés (1 ^{ère} échéance)
<montantcommande>	<p>Le montant de la commande</p> <p>Format :</p> <ul style="list-style-type: none"> - Un nombre entier - Un point décimal (optionnel) - Un nombre entier de 2 chiffres (optionnel) - Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) <p>Exemple : 62.73EUR ou 1024USD</p>	
<montantrecouvre>	<p>Le montant de la commande ayant déjà été recouvré</p> <p>Format :</p> <ul style="list-style-type: none"> - Un nombre entier - Un point décimal (optionnel) - Un nombre entier de 2 chiffres (optionnel) <p>Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.)</p> <p>Exemple : 62.73EUR ou 1024USD</p>	

<motifrefus>	<p>Motif du refus de la demande de paiement</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - Refus : la banque du client ou du commerçant 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 - Appel Phonie : la banque du client demande des informations complémentaires (obsolète) 	<p>Uniquement dans le cas où la demande de paiement est refusée</p> <p>Si la demande est acceptée, la valeur est un tiret « - »</p>
<motifrefusautorisation>	<p>Motif du refus détaillé de la demande d'autorisation</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - Refus banque : la banque du client ou du commerçant refuse d'accorder l'autorisation - Refus emetteur : la banque du client refuse d'accorder l'autorisation - Refus critique : la banque du client refuse d'accorder l'autorisation. Contrairement au « Refus banque » et au « Refus emetteur » ce refus est définitif - Refus repli VADS : la banque du client refuse d'accorder l'autorisation et requiert une authentification du client - Refus temporaire : la demande d'autorisation a été refusée mais pourrait être retentée - Refus technique : la demande d'autorisation a été refusée en raison d'un problème technique 	<p>Uniquement dans le cas où l'autorisation a été refusée (<motifrefus> indique alors Appel Phonie, Refus ou Interdit)</p>

	<ul style="list-style-type: none"> - Refus autres : autre motifs de refus. - Refus test : simulation d'un test de refus d'autorisation en environnement de validation. 	
<antifraude>	Nœud regroupant des informations liées à la prévention de la fraude	Uniquement en cas de souscription du module antifraude
<originecb>	<p>Code pays de la banque émettrice de la carte de paiement</p> <p>Format : 3 caractères alphabétiques respectant la norme ISO 3166-1 ou ZZZ si information non disponible</p> <p>Exemple : FRA</p>	<p>Sous-élément du nœud <antifraude></p> <p>Uniquement en cas de souscription du module antifraude pour un paiement carte</p>
<bincb>	<p>Code BIN de la banque du porteur de la carte de paiement</p> <p>Format :</p> <ul style="list-style-type: none"> - 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 <p>Exemple : 12345678 ou 123456XX</p>	<p>Sous-élément du nœud <antifraude></p> <p>Uniquement en cas de souscription du module antifraude pour un paiement carte</p>
<hpancb>	<p>Hachage irréversible du numéro de la carte de paiement utilisée pour effectuer le paiement (identifiant de manière unique une carte de paiement pour un commerçant donné)</p> <p>Format : chaîne hexadécimale</p> <p>Exemple : AFE79FC85D67EF90C43F8F798290F F935F849F91</p>	<p>Sous-élément du nœud <antifraude></p> <p>Uniquement en cas de souscription du module antifraude pour un paiement carte</p>
<ipclient>	Adresse IP du client ayant fait la transaction	<p>Sous-élément du nœud <antifraude></p> <p>Uniquement en cas de souscription du module antifraude</p>

<originetr>	<p>Code pays de l'origine de la transaction</p> <p>Format : 3 caractères alphabétiques respectant la norme ISO 3166-1 ou ZZZ si information non disponible</p> <p>Exemple : FRA</p>	<p>Sous-élément du nœud <antifraude></p> <p>Uniquement en cas de souscription du module antifraude</p>
<veres>	<p>Résultat d'enrôlement à 3D-Secure</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - Y : carte enrôlée - N : carte non enrôlée - U : problème technique ne permettant pas de conclure sur l'enrôlement 	<p>Sous éléments du nœud <antifraude></p> <p>Uniquement en cas de souscription du module antifraude pour un paiement carte</p>
<pares>	<p>Résultat d'authentification du client sur le serveur d'authentification de sa banque</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - Y : client authentifié - N : client non authentifié - A : la demande d'authentification a été acceptée en délégation et la banque assume l'authentification du client - U : non authentifié suite à un problème technique 	
<datecommerce>	<p>Date et heure du paiement envoyée par le commerçant</p> <p>Format : AAAA-MM-JJTHH:MM:SS (ISO 8601)</p> <p>Exemple : 2022-12-01T01:00:00</p>	
<dateutc>	<p>Date et heure UTC de la réception du paiement par le serveur Monetico Paiement</p> <p>Format : AAAA-MM-JJTHH:MM:SS (ISO 8601)</p> <p>Exemple : 2022-12-01T00:00:00</p>	
<referenceaccepteur>	<p>Référence de paiement transmise dans la demande d'autorisation vers la banque émettrice</p>	<p>Valeur identique au champ <reference> si elle respecte le format de la documentation</p>

	Format : 12 caractères alphanumériques Exemple : ABERTYP00145	technique ; référence générée par Monetico Paiement dans le cas contraire
<idautorisationacquireur>	Identifiant de la transaction d'autorisation fourni par l'acquéreur Format : chaîne de caractère à la discrétion de l'acquéreur	Uniquement si la valeur est fournie par l'acquéreur
<idpaiementacquireur>	Identifiant de la transaction de paiement fourni par l'acquéreur Format : chaîne de caractère à la discrétion de l'acquéreur	
<modalitepaiement>	Modalité de paiement utilisée Valeurs possibles : <ul style="list-style-type: none"> - PI : paiement immédiat - PD : paiement différé - PF : paiement fractionné - PP : paiement partiel - PR : paiement récurrent 	
<moyenpaiement>	Moyen de paiement utilisé Valeurs possibles : CB , paypal , 1euro , 3xcb , 4xcb , lyfpay , sofort ou giropay	
<wallet>	Wallet électronique utilisé Valeurs possibles : applepay	Uniquement si le moyen de paiement utilisé est une carte enregistrée au préalable dans un wallet électronique (<moyenpaiement> indique alors CB)
<cbmasquee>	Le numéro de carte tronqué en conformité avec PCI DSS Format: <ul style="list-style-type: none"> - 8 premiers et 2 derniers chiffres de la carte de paiement du client, séparés par des caractères 'X' pour les numéros de carte ayant une longueur de 16 chiffres ou plus - 6 premiers chiffres, 6 caractères 'X', le reste des chiffres de la carte de paiement du client pour les numéros de carte ayant une 	Uniquement si le moyen de paiement utilisé est une carte (<moyenpaiement> indique alors CB)

	longueur de moins de 16 chiffres Exemple : 12345678XXXXXX90 ou 123456XXXXXX890	
<usage>	Précise le type de carte utilisée pour réaliser la transaction Valeurs possibles : <ul style="list-style-type: none"> - credit : carte de crédit ou à débit différé - debit : carte de débit - prepayee : carte prépayée - inconnu : impossible de déterminer le type de carte ou information indisponible 	

Exemple de flux XML de retour :

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
```

```
<xml>
  <etat>PA</etat>
  <cvx>oui</cvx>
  <vld>1109</vld>
  <brand>na</brand>
  <status3DS>-1</status3DS>
  <montantcommande>1.01EUR</montantcommande>
  <montantrecouvre>1.01EUR</montantrecouvre>
  <numauto>000000</numauto>
  <motifrefus>-</motifrefus >
  <antifraude>
    <originecb>51x</originecb>
    <bincb>49778332</bincb>
    <hpancb>AB319D71559923294B30223182137B369A0D2EF5</hpancb>
    <ipclient>10.45.166.40</ipclient>
    <originetr>ZZZ</originetr>
    <veres>-</veres>
    <pares>-</pares>
  </antifraude>
  <referenceaccepteur>REF123456789</referenceaccepteur>
  <datecommerce>2018-04-10T11:00:00</datecommerce>
  <dateutc>2018-04-10T09:00:00</dateutc>
  <idautorisationacquireur>035661</idautorisationacquireur>
  <idpaiementacquireur>035675</idpaiementacquireur>
  <modalitepaiement>PI</modalitepaiement >
  <moyenpaiement>CB</moyenpaiement>
  <cbmasquee>49778332XXXXXX08</cbmasquee >
  <usage>debit</usage >
</xml>
```

Remarque pour l'intégration :

Le message de retour est au format XML. Dans le futur, celui-ci pourra faire l'objet d'enrichissements par ajout de nouveaux éléments XML (nouvelles balises).

Afin d'éviter tout problème de rupture de compatibilité suite à une mise à jour de notre service, il est nécessaire de ne prendre en compte que les balises XML vous intéressant et d'ignorer les autres.

2.2.1. Éléments supplémentaires spécifiques à la version 3.0

Balise	Description	Remarque
<action_differe>	Informations sur l'action automatique qui sera effectuée à la fin du différé	Nœud contenant des sous éléments Uniquement pour le paiement différé et la 1ère échéance du paiement fractionné
<date_traitement_automatique>	Date à laquelle le traitement automatique différé sera réalisé Format : AAAA-MM-JJ Exemple : 2022-11-10	Sous élément du nœud <action_differe>
<traitement_automatique>	Nature du traitement automatique à la fin du délai de différé Valeurs possibles : recouvrement ou annulation	Sous élément du nœud <action_differe>
<recouvrements>	Listes des recouvrements effectués pour l'échéancier	Nœud contenant des sous éléments
<recouvrement>	Détails d'un recouvrement	Sous élément du nœud <recouvrements> Nœud contenant des sous éléments
<dateheure_gmt>	Date et heure GMT de la demande de recouvrement Format : AAAA-MM-JJ HH:MM:SS Exemple : 2022-01-13 15:30:01	Sous élément du nœud <recouvrements>
<date_remise>	Date de la remise suite à la demande de recouvrement Format : AAAA-MM-JJ Exemple : 2022-01-14	Sous élément du nœud <recouvrements>
<montant>	Montant du recouvrement Format : <ul style="list-style-type: none"> - Un nombre entier - Un point décimal (optionnel) - Un nombre entier de 2 chiffres (optionnel) 	Sous élément du nœud <recouvrements>

	<ul style="list-style-type: none"> - Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) <p>Exemple : 62.73EUR ou 1024USD</p>	
<resultat>	<p>Résultat du recouvrement</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - 0 : échec - 1 : succès 	<p>Sous élément du nœud</p> <p><recouvrement></p>
<numero_autorisation>	<p>Numéro d'autorisation</p> <p>Format : chaîne de caractères à la discrétion de la banque émettrice (en général alphanumérique)</p> <p>Exemple : 543091</p>	<p>Sous élément du nœud</p> <p><recouvrement></p>
<recredits>	<p>Liste des recredits associés à un recouvrement donné</p>	<p>Sous élément du nœud</p> <p><recouvrements></p> <p>Nœud contenant des sous éléments</p>
<recredit>	<p>Détails d'un recredit</p>	<p>Sous élément du nœud <recredits></p> <p>Nœud contenant des sous éléments</p>
<date_GMT>	<p>Date GMT du recredit</p> <p>Format : AAAA-MM-JJ</p> <p>Exemple : 2022-01-14</p>	<p>Sous élément du nœud <recredit></p>
<heure_GMT>	<p>Heure GMT du recredit</p> <p>Format : HH:MM:SS</p> <p>Exemple : 22:00:00</p>	<p>Sous élément du nœud <recredit></p>
<montant_recredite>	<p>Montant recredité</p> <p>Format :</p> <ul style="list-style-type: none"> - Un nombre entier - Un point décimal (optionnel) - Un nombre entier de 2 chiffres (optionnel) - Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) <p>Exemple : 62.73EUR ou 1024USD</p>	<p>Sous élément du nœud <recredit></p>

<ip>	IP à l'origine du recrédit	Sous élément du nœud <recredit>
<methode>	Canal / Service utilisé pour le recrédit Valeurs possibles : - IP : recrédit via appel au cgi de recrédit - TB : pour recrédit via le tableau de bord	Sous élément du nœud <recredit>
<identifiant>	Identifiant tableau de bord utilisé pour faire le recrédit Format : chaîne de caractère alphanumérique Ex : 102783333333300B	Sous élément du nœud <recredit> Uniquement si recrédit effectué par la canal tableau de bord
<echeancier>	Liste des échéances du paiement N fois	Nœud contenant des sous éléments Uniquement pour les paiements fractionnés
<echeance>	Détail d'une échéance du paiement N fois	Sous élément du nœud <echeancier> Nœud contenant des sous éléments
<numero>	Numéro de l'échéance Valeurs possibles : 1, 2, 3 ou 4	Sous élément du nœud <echeancier>
<date>	Date prévisionnelle du recouvrement de l'échéance Format : AAAA-MM-JJ Exemple : 2022-01-14	Sous élément du nœud <echeancier>
<montant>	Montant de l'échéance Format : - Un nombre entier - Un point décimal (optionnel) - Un nombre entier de 2 chiffres (optionnel) - Une devise sur 3 caractères alphanumériques ISO4217 (EUR, USD, etc.) Exemple : 62.73EUR ou 1024USD	Sous élément du nœud <echeancier>

<resultat>	<p>Résultat du recouvrement de l'échéance</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - I : échéance créée sur laquelle aucun traitement n'a encore été fait - P : échéance payée en état final - R : échéance refusée mais pour laquelle d'autres tentatives de recouvrement sont possibles - M : échéance refusée après 4 tentatives et qu'il n'est plus possible de recouvrer - C : échéance ayant fait l'objet d'un refus critique (mise en opposition, carte perdue ...) et qu'il n'est plus possible de recouvrer - X : échéance annulée 	<p>Sous élément du nœud</p> <p><echeancier></p>
<report>	<p>Indique si l'échéance sera remontée dans le fichier de reporting spécifique des échéances > 1</p> <p>Valeurs possibles :</p> <ul style="list-style-type: none"> - I : à ne pas remonter dans le fichier (cas des 1ères échéances) - F : à remonter dans le fichier (situation initiale pour toutes les échéances en dehors de la première) - C : remontée dans le fichier (échéances déjà remontées) 	<p>Sous élément du nœud</p> <p><echeancier></p>
<compteur_essais>	<p>Nombre de tentatives de recouvrements de l'échéance</p> <p>Format : nombre entier entre 1 et 4</p> <p>Ex : 4</p>	<p>Sous élément du nœud</p> <p><echeancier></p>
<mensualites>	Liste des mensualités d'un paiement récurrent	<p>Nœud contenant des sous éléments</p> <p>Uniquement pour les paiements récurrents</p>
<mensualite>	Mensualité d'un paiement récurrent	<p>Sous élément du nœud</p> <p><mensualites></p>

<date_banque_gmt>	Date GMT de création de la mensualité Format : AAAA-MM-JJ Exemple : 2022-01-14	Sous élément du nœud <mensualite>
<etat>	Etat de la mensualité	Sous élément du nœud <mensualite>
<recouvrements>	Informations sur les recouvrements effectués pour cette mensualité	Sous élément du nœud <mensualite>
<recredits>	Liste des crédits de la commande	Sous élément du nœud <recouvrements> Nœud contenant des sous éléments
<recredit>	Détails d'un crédit, identique au balises <recredit> du nœud <recouvrements>	Sous élément du nœud <recredits> Nœud contenant des sous éléments
<total>	Total des crédits sur la commande	Sous élément du nœud <recredits>

Exemple de flux XML de retour pour un paiement fractionné :

```
<?xml version="1.0" encoding="utf-8"?>
<xml>
  <etat>PA</etat>
  <cvx>oui</cvx>
  <vld>1019</vld>
  <brand>VI</brand>
  <status3DS>-1</status3DS>
  <montantcommande>1.01EUR</montantcommande>
  <montantrecouvre>1.01EUR</montantrecouvre>
  <numauto></numauto>
  <motifrefus>-</motifrefus>
  <antifraude>
    <originecb>FRA</originecb>
    <bincb>49742270</bincb>
    <hpancb>AFE79FC85D67EF90C43F8F798290FF935F849F91</hpancb>
    <ipclient>10.30.166.102</ipclient>
    <originetr>ZZZ</originetr>
    <veres>-</veres>
    <pares>-</pares>
  </antifraude>
```

```

<datecommerce>2018-09-27T15:08:13</datecommerce>
<dateutc>2018-09-27T13:08:29</dateutc>
<modalitepaiement>CB</modalitepaiement>
<moyenpaiement>PF</moyenpaiement>
<cbmasquee>49742270XXXXXX68</cbmasquee>
<usage>credit</usage>
<referenceaccepteur>E1538053693</referenceaccepteur>
<tpe>9000004</tpe>
<reference>E1538053693</reference>
<echeancier>
  <echeance>
    <numero>1</numero>
    <date>2018-09-27</date>
    <montant>0.34EUR</montant>
    <resultat>P</resultat>
    <report>I</report>
    <compteur_essais>1</compteur_essais>
  </echeance>
  <echeance>
    <numero>2</numero>
    <date>2018-10-27</date>
    <montant>0.34EUR</montant>
    <resultat>P</resultat>
    <report>C</report>
    <compteur_essais>1</compteur_essais>
  </echeance>
  <echeance>
    <numero>3</numero>
    <date>2018-11-27</date>
    <montant>0.33EUR</montant>
    <resultat>P</resultat>
    <report>C</report>
    <compteur_essais>1</compteur_essais>
  </echeance>
</echeancier>
<action_differe>
  <date_traitement_automatique>2018-10-
04</date_traitement_automatique>
  <traitement_automatique>recouvrement</traitement_automatique>
</action_differe>
<recouvrements>
  <recouvrement>
    <dateheure_gmt>2018-11-27 09:12:35</dateheure_gmt>
    <date_remise>2018-11-27</date_remise>
    <montant>0.33EUR</montant>
    <resultat>1</resultat>
    <numero_autorisation>543091</numero_autorisation>
    <recredits>
      <recredit>

```

```

        <date_GMT>2022-10-28</date_GMT>
        <heure_GMT>10:26:06</heure_GMT>
        <montant_recredite>0.10EUR</montant_recredite>
        <ip>10.46.222.2</ip>
        <methode>IP</methode>
    </recredit>
</recredits>
</recouvrement>
<recouvrement>
    <dateheure_gmt>2018-10-27 08:15:34</dateheure_gmt>
    <date_remise>2018-10-28</date_remise>
    <montant>0.34EUR</montant>
    <resultat>1</resultat>
    <numero_autorisation>124262</numero_autorisation>
    <recredits>
        <recredit>
            <date_GMT>2022-10-26</date_GMT>
            <heure_GMT>06:19:29</heure_GMT>
            <montant_recredite>0.34EUR</montant_recredite>
            <ip>10.46.222.2</ip>
            <methode>TB</methode>
            <identifiant>1027833333333300B</identifiant>
        </recredit>
    </recredits>
</recouvrement>
<recouvrement>
    <dateheure_gmt>2018-10-23 20:38:50</dateheure_gmt>
    <date_remise>2018-10-23</date_remise>
    <montant>0.34EUR</montant>
    <resultat>1</resultat>
    <numero_autorisation>491887</numero_autorisation>
</recouvrement>
</recouvrements>
<recredits>
    <recredit>
        <date_GMT>2022-10-26</date_GMT>
        <heure_GMT>06:19:29</heure_GMT>
        <montant_recredite>0.34EUR</montant_recredite>
        <ip>10.46.222.2</ip>
        <methode>TB</methode>
        <identifiant>1027833333333300B</identifiant>
    </recredit>
    <recredit>
        <date_GMT>2022-10-28</date_GMT>
        <heure_GMT>10:26:06</heure_GMT>
        <montant_recredite>0.10EUR</montant_recredite>
        <ip>10.46.222.2</ip>
        <methode>IP</methode>
    </recredit>

```

```

<total>0.44EUR</total>
</recredits>
</xml>

```

2.2.2. Liste des valeurs du code retour dans les messages XML (balise <cdr>)

Valeur balise <cdr>	Description	Commentaire
-1	Problème technique	Problème technique, il faut réitérer la demande
-2	Erreur dans les paramètres d'entrée	Les paramètres servant à identifier la commande site ne sont pas corrects, vérifier les champs version, société, date, référence, montant et TPE. Vérifier si un des champs n'est pas nul ou si la longueur d'un champ ne dépasse pas la taille maximale autorisée.
-3	Montant erroné	Le montant transmis est mal formaté ou égale à zéro.
-4	Erreur demande d'autorisation	La date de validité de la carte de paiement n'est pas valide
-5	MAC erroné	Vérifier la valeur des paramètres d'entrée TPE, date, référence, montant et MAC. Vérifier en particulier le calcul du MAC et la valeur de la clé MAC.
-6	Date erronée	La date d'entrée est erronée. Vérifier que le format de la date est du type JJ/MM/AAAA.
-7	Transfert des données	Les données doivent être transmises avec la méthode POST.
-8	Sémaphore verrouillée	Le programme a déjà été lancé en parallèle sur le même paiement et est en cours d'exécution ou la page de paiement est en cours.
-9	Problème recherche commande	La commande ne peut pas être trouvée. Vérifier la valeur des paramètres d'entrée.
-10	Version erronée	La version transmise est mal formatée ou non renseignée.

3. Utilisation du service

2.3. En Test

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

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

- <https://payment-api.e-i.com/test/etatpaiement.cgi>

2.4. En Production

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

- <https://payment-api.e-i.com/etatpaiement.cgi>

2.5. 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.

4. Aides à l'installation

2.6. Les problèmes les plus fréquents

4.1.1. Problème de calcul du sceau de sécurité

Message d'erreur

```
<xml>  
  <cdr>-5</cdr>  
</xml>
```

Causes possibles

- Le formulaire que vous nous avez envoyé ne contient pas toutes les informations requises
- Le calcul du sceau MAC est erroné
- Le calcul du sceau MAC est effectué avec une mauvaise clé

Résolution du problème

Suivez scrupuleusement le cheminement décrit ci-dessous ; à la fin de chaque étape pour laquelle vous avez effectué des changements dans votre implémentation, effectuez de nouveaux tests de paiement. S'ils ne sont pas fructueux, passez à l'étape suivante.

Attention : ne sautez pas d'étape !

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

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

- la valeur MAC correspond-elle à une chaîne de 40 caractères hexadécimaux (valeurs autorisées : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) ?
- la valeur de la variable date est-elle bien au format JJ/MM/AA ?
- la valeur de la variable référence est-elle bien une chaîne ne contenant que des lettres (non accentuées) et des chiffres ?

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

TPE=<TPE>*date=<date>*montant=<montant>*reference=<reference>*societe=<societe>*version=<version>

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

Etape 4 : vérifiez que vous utilisez la bonne clé :

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

Si malgré toutes ces vérifications vous obtenez toujours ce message d'erreur, le problème réside dans l'intégration de notre solution dans votre système d'information.

La grande diversité des langages et des spécificités liées à l'environnement utilisés pour l'implémentation de notre solution de paiement, sont autant de paramètres dont nous ne maîtrisons pas tous les aspects et par conséquent, ils ne nous permettent pas de vous fournir un support personnalisé plus ample.

4.1.2. La commande ne peut pas être trouvée

Message d'erreur

```
<xml>
  <cdr>-9</cdr>
</xml>
```

Causes possibles

- le numéro de TPE est incorrect ou inexistant
- le code société est incorrect ou inexistant
- la référence est incorrecte ou inexistante

Résolution du problème

Vérifiez que les variables TPE, societe et référence sont présentes dans le formulaire, correctement orthographiées, respectent la casse et les éventuelles restrictions sur le format et les caractères autorisés.