

Monetico Paielement

Paielement sécurisé sur Internet

**Documentation Technique
API Recrédit**



SOMMAIRE

1	<i>Cas d'utilisation de l'API de recrédit</i>	3
2	<i>Clé de sécurité commerçant</i>	3
3	<i>Demander le recrédit d'un paiement</i>	4
3.1	Appel au service de recrédit	4
3.1.1	Les informations à fournir	4
3.1.1	Cas particulier des paiements par carte et par Wallet ApplePay	7
3.1.2	Calcul du sceau	7
3.1.1	Contrôle de l'IP et limite du nombre de remboursements	8
3.1.2	Exemples de requête de recrédit	8
3.2	Réponse de la demande de recrédit	10
3.2.1	Les informations retournées	10
3.2.2	Exemples de messages retournés	12
4	<i>Aides à la résolution des problèmes les plus fréquents</i>	13
4.1	Problème de calcul du sceau de sécurité	13
4.2	Le commerçant ne peut pas être identifié	14
4.3	La commande ne peut pas être authentifiée	15
5	<i>Assistance technique</i>	16
6	<i>Annexes</i>	17
6.1	Contraintes générales de codage HTML des champs	17
6.2	Contrainte d'encodage	18
6.3	Calcul du sceau MAC	18
6.3.1	Exemple de chaînes permettant le calcul du sceau	19
6.4	URL des services	20
6.4.1	L'environnement de test dit « sandbox »	20
6.4.2	En Production	20

1 Cas d'utilisation de l'API de recrédit

Le but du service « recredit_paiement » est de permettre aux commerçants de rembourser leurs clients d'une partie ou de la totalité de leur achat, de façon sécurisée, via Internet.

Pour demander un remboursement, l'application du commerçant doit faire appel au service web de recrédit de Monetico Paiement (via un message HTTPS), en fournissant un certain nombre d'informations (le montant du remboursement, sa date, sa référence, le numéro du TPE virtuel du commerçant, etc.). Un sceau doit être calculé pour certifier les données échangées.

En réponse à cette demande, le serveur Monetico Paiement retourne le résultat de la demande de remboursement à l'application du commerçant : acceptée ou refusée.

2 Clé de sécurité commerçant

Une clé de sécurité, propre à chaque TPE, destinée à certifier les données échangées entre le serveur du commerçant et le serveur de paiement sécurisé Monetico Paiement, est indispensable pour utiliser le service de paiement par carte de paiement. Un lien, permettant de télécharger cette clé de sécurité, est envoyé par notre centre de support au commerçant.

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

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

La clé de sécurité est représentée de façon externe par 40 caractères hexadécimaux (par exemple : 0123456789ABCDEF0123456789ABCDEF01234567).

Cette représentation externe doit être convertie en une chaîne de 20 octets (représentation opérationnelle) avant utilisation.

L'ancienne clé reste reconnue par le système lors de la génération d'une nouvelle clé. C'est une utilisation avec succès de la nouvelle clé (en environnement de test, en environnement de production) qui viendra définitivement invalider l'ancienne (pour l'environnement respectif).

3 Demander le recrédit d'un paiement

3.1 Appel au service de recrédit

3.1.1 Les informations à fournir

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

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

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

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

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

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

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

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

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

Champ	montant_possible
Présence	Obligatoire si le champ montant_deja_recredite est absent Optionnel sinon
Description	Montant TTC de crédit maximum autorisé pour le numéro d'autorisation fourni
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Complément	Si un remboursement a déjà été effectué sur ce numéro d'autorisation, il doit être décompté par le commerçant. Par exemple, pour une commande de 100 €, si un remboursement de 10 € a déjà été effectué, le prochain remboursement présentera une valeur de « montant_possible » de 90 €.
Exemple	95.25EUR

Champ	montant_deja_recredite
--------------	-------------------------------

Présence	Obligatoire si le champ montant_possible est absent Optionnel sinon
Description	Montant TTC des recrédits réussit déjà effectués
Format Valeur(s) possible(s)	Un nombre entier Un point décimal (optionnel) Un nombre entier de 2 chiffres (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, etc.) [0-9]+(\.[0-9]{1,2})?[A-Z]{3}
Complément	Si des remboursements ont déjà été effectués sur ce numéro d'autorisation, ils doivent être renseignés par le commerçant. Par exemple, pour une commande de 100 €, si un remboursement de 10 € a déjà été effectué, le prochain remboursement présentera une valeur de « montant_deja_recredite » de 10 €.
Exemple	95.25EUR

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

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

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

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

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

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

3.1.1 Cas particulier des paiements par carte et par Wallet ApplePay

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

3.1.2 Calcul du sceau

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

3.1.1 Contrôle de l'IP et limite du nombre de remboursements

Pour des raisons de sécurité, les requêtes de remboursement ne peuvent être émises que depuis des serveurs avec une adresse IP connue de nos services. De plus, chaque adresse IP est limitée quotidiennement dans le nombre de requêtes de remboursement qu'elle est autorisée à effectuer.

Avant de pouvoir effectuer des requêtes de remboursement dans l'environnement de production, il vous faudra donc communiquer par courriel à l'assistance technique (voir chapitre 7 Assistance technique) la liste des adresses IP à autoriser, ainsi que le nombre de remboursement quotidiens maximum pour chacune d'entre elles.

3.1.2 Exemples de requête de recrédit

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

Requête :

```
POST /recredit_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 328

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&date_commande=03%2F12%2F2006
&date_remise=04%2F12%2F2006
&num_autorisation=1234A6
&montant=100.00EUR
&montant_recredit=32.00EUR
&montant_possible=100EUR
&reference=ABERTPY00145
&lgu=FR
&societe=monSite1
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

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

Exemple 2 : recrédit total sur une commande de 100€

Requête :

```
POST /recredit_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 326

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&date_commande=03%2F12%2F2006
&date_remise=04%2F12%2F2006
&num_autorisation=1234A6
&montant=100.00EUR
&montant_recredit=100EUR
&montant_possible=100EUR
&reference=ABERTPY00145
&lgu=FR
&societe=monSite1
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

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

Requête :

```
POST /recredit_paiement.cgi HTTP/1.0
Pragma: no-cache
Connection: close
User-Agent : AuthClient
Host: p.monetico-services.com
Accept: */*
Content-type: application/x-www-form-urlencoded
Content-length: 326

version=3.0
&TPE=1234567
&date=05%2F12%2F2006%3A11%3A55%3A23
&date_commande=03%2F12%2F2006
&montant=100.00EUR
&montant_recredit=100EUR
&montant_deja_recedite=0EUR
&reference=ABERTPY00145
&lgu=FR
&societe=monSite1
&MAC=78bc376c5b192f1c48844794cbdb0050f156b9a2
```

3.2 Réponse de la demande de recrédit

3.2.1 Les informations retournées

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

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

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

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

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

Champ	reference
Description	Référence de la commande

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

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

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

cdr	lib	Description	Remarque
0	recredit effectue	La demande de recrédit a été prise en compte	
-1	recredit refuse	La demande de recrédit n'a pas été prise en compte	
-30	Commerçant non identifie	Les paramètres servant à identifier le site commerçant ne sont pas corrects	Vérifier les paramètres societe, TPE et lgue
-31	signature non validee	La signature MAC est invalide	
-32	recredit non autorise	Votre TPE n'est pas autorisé à effectuer des crédits	Contactez l'assistance technique
-33	demande de recredit expiree	La date de recrédit dépasse le délai autorisé (+/- 24h)	Vérifier le paramètre date
-34	montant de recredit errone	Le montant à recréditer est incorrect	Vérifier le paramètre montant_recredit
-35	Les montants transmis sont incorrects	Les montants transmis ne sont pas en phase avec ceux du serveur bancaire	Vérifier les champs montant_recredit et montant_possible
-36	le maximum de recredit a été atteint	Le nombre maximum de crédits pour votre TPE a été atteint	
-37	la commande est inexistante	La commande n'existe pas	Vérifier que les champs permettant d'identifier la commande sont corrects
-38	la commande ne peut pas donner lieu a un recredit	La commande n'a pas encore été payée, aucun recrédit ne peut être effectué	
-39	le paiement est inexistant	Une demande d'autorisation a déjà été délivrée pour cette commande	
-40	le montant total des credits ne peut dépasser le seuil	Le montant à recréditer est incorrect	
-41	un probleme technique est survenu	Problème technique	Réitérer la demande
-42	la devise est incorrecte	La devise transmise ne correspond pas à la devise de la commande	Vérifier le paramètre devise
-43	parametres invalides	Un ou plusieurs paramètres ne respectent pas le format requis	Vérifier la longueur des champs et le format des dates
-44	autre traitement en cours	Une autre transaction est en cours de traitement sur la même référence ; cela peut être un autre traitement que recredit_paiement	Réitérer la demande
-45	verification carte echouee	L'état de la carte ne permet plus d'opération (carte opposée, volée ...)	
-46	la commande est deja entierement recreditee	La commande est entièrement recréditée.	Vérifier la cohérence de la demande (paramètres d'appels) par rapport aux crédits déjà effectués
-47	plusieurs traitements ont ete trouves	Impossible de déterminer le paiement Cofidis à recréditer en raison de l'absence de la référence Cofidis	Vérifier le paramètre ref_remise
-48	echec du recredit, recredit potentiellement partiel	Le recrédit PayPal n'a pas réussi entièrement	Vérifier la cohérence de la demande (paramètres d'appels)

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

3.2.2 Exemples de messages retournés

- Cas d'un recredit accepté

```
version=1.0
reference=000000000145
cdr=0
lib=recredit effectue
```
- Cas d'une erreur

```
version=1.0
reference=000000000145
cdr=-31
lib=les montants transmis sont incorrects
```
- Cas d'un recredit accepté en pré autorisation

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

4 Aides à la résolution des problèmes les plus fréquents

4.1 Problème de calcul du sceau de sécurité

Message d'erreur en requête de recrédit

```
version=1.0  
reference=<votre référence>  
cdr=-31  
lib= signature non validee
```

Causes possibles

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

Résolution du problème

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

Attention : ne sautez pas d'étape !

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

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

- la valeur de la variable **MAC** correspond-elle à une chaîne de 40 caractères hexadécimaux (valeurs autorisées : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) ?
- la valeur de la variable **version** correspond-elle à 3.0 ?
- la valeur de la variable **date** est-elle bien au format JJ/MM/AAAA:HH:MM:SS ?
- la valeur de la variable **reference** est-elle bien une chaîne ne contenant que des lettres (non accentuées) et des chiffres pour une longueur maximale de 12 caractères ?
- la variable **texte-libre** est-elle correctement orthographiée, en respectant la casse et avec le caractère tiret ('-') et non le caractère souligné ('_') ?

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

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

Etape 4 : vérifiez que vous utilisez la bonne clé de sécurité :

- vous devez utiliser la dernière clé qui vous a été fournie par nos services,
- vérifiez que la clé correspond à votre algorithme de calcul de sceau (SHA1 ou MD5),
- Contactez notre service de support afin de valider ensemble que vous utilisez bien la bonne clé, et afin de valider que la version de votre formulaire (champ « version ») correspond à la version paramétrée dans notre système.

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

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

4.2 Le commerçant ne peut pas être identifié

Message d'erreur

```
version=1.0  
reference=<votre référence>  
cdr=-30  
lib= Commerçant non identifie
```

Causes possibles

- le numéro de TPE est incorrect ou inexistant
- le code société est incorrect ou inexistant
- le code langue est incorrect ou inexistant
- l'adresse IP du serveur commerçant n'est pas autorisée à faire du recrédit

Résolution du problème

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

4.3 La commande ne peut pas être authentifiée

Message d'erreur

```
version=1.0  
reference=<votre référence>  
cdr=0  
lib=commande non authentifiée
```

Causes possibles

- la référence est incorrecte ou inexistante
- la date de commande est incorrecte ou inexistante

Résolution du problème

Vérifiez que les variables `reference` et `date_commande` sont présentes dans le formulaire, correctement orthographiées, respectent la casse et respectent les éventuelles restrictions sur le format et les caractères autorisés.

Vérifiez que la référence de commande à capturer a bien été autorisée ou enregistrée à la date que vous fournissez

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 : centrecom@e-i.com
 - CIC : centrecom@e-i.com
- Par téléphone : en appelant le **0820 821 735**

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

6 Annexes

6.1 Contraintes générales de codage HTML des champs

Tous les champs de la requête d'appel, à l'exception de la version et des montants, doivent être codés en HTML avant la mise en forme dans le formulaire (c'est à dire immédiatement après le calcul du MAC).

Les caractères à coder sont les codes ASCII de 0 à 127 réputés risqués :

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

Les fonctions de type « `HTML_ENCODE` » (cf IETF RFC1738) des langages conviennent parfaitement, elles encodent beaucoup plus de caractères, typiquement tout ce qui n'est pas :

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

Enfin, les champs ne doivent pas contenir les caractères ASCII 10 et 13 (CR et LF).

6.2 Contrainte d'encodage

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

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

6.3 Calcul du sceau MAC

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

Cette fonction générera le sceau à partir de données à certifier et de la clé de sécurité commerçant sous sa forme opérationnelle.

Les données à certifier sont structurées :

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

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

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

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

Remarque :

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

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

6.3.1 Exemple de chaînes permettant le calcul du sceau

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

6.4 URL des services

6.4.1 L'environnement de test dit « sandbox »

Le rôle de notre serveur de test est de vous permettre de valider vos développements. Bien sûr, toutes les opérations effectuées par notre serveur de paiement de test sont fictives et ne débouchent sur aucun mouvement bancaire réel.

Pour effectuer des demandes de paiement dans cet environnement, nous mettons à votre disposition des cartes de paiement de test, accessibles en cliquant sur l'icône « Carte de Test » de la page de paiement.

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

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

Le tableau de bord commerçant de test vous permet de gérer et contrôler les paiements effectués dans l'environnement de test. Il est disponible à l'adresse suivante :

- <https://www.monetico-services.com/fr/test/>

6.4.2 En Production

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

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

Vous pouvez consulter les paiements opérés sur votre TPE via le tableau de bord commerçant disponible à l'adresse suivante :

- <https://www.monetico-services.com/fr/>

Nous attirons votre attention sur le fait que les requêtes adressées au serveur de production seront des opérations réelles.