



# **Païement sécurisé sur Internet**

## **Service TPE Virtuel**

**(sécurisé par le protocole SSL)**

### **Spécifications Techniques**



## SOMMAIRE

<b>1</b>	<b>Mise en place du service « TPE Virtuel Via Internet »</b>	<b>3</b>
1.1	Open Kits : exemples d'int�gration	3
1.2	Open Tools : prise en charge des param�tres	3
1.3	Cl� de s�curit� commer�ant	4
<b>2</b>	<b>Sp�cifications des messages �chang�s</b>	<b>5</b>
2.1	Rappel de la cin�matique	5
2.2	Phase aller du paielement (interface « Aller »)	6
	Cr�ation du formulaire	6
	Exemple de formulaire de paielement	7
	Messages d'erreur	8
2.3	Phase retour du paielement (interface « Retour »)	9
	Param�tres renvoy�s par la banque	10
	Compl�ment « retourPLUS »	11
	Validation du sceau	12
	Cr�ation de l'accus� de r�ception	13
2.4	Sp�cification des formats	14
	Contraintes g�n�rales de codage HTML des champs	14
	Contraintes particuli�res selon le champ	14
<b>3</b>	<b>URLs des serveurs de paielement</b>	<b>15</b>
3.1	En Test	15
3.2	En Production	15
<b>4</b>	<b>Aides � l'installation</b>	<b>16</b>
4.1	Utilisation de l'outil « Open Tools » de configuration	16
4.2	Foire aux questions	19

# 1 Mise en place du service « TPE Virtuel Via Internet »

Les éléments nécessaires à la mise en place du paiement sécurisé sur votre Terminal de Paiement Electronique Virtuel (TPEV) vous seront fournis par notre centre de support (boîte aux lettres [centecom@e-i.com](mailto:centecom@e-i.com)) sous forme de liens de téléchargement sur le site sécurisé de votre banque. Vous recevrez ces informations par e-mail lors des différentes phases d'installation et de test.

Vous devrez utiliser la documentation fournie pour créer les deux programmes d'interface :

- Interface « Aller » : génération du formulaire de demande de paiement
- Interface « Retour » : réception de la confirmation du paiement

Le travail à réaliser nécessite des compétences avancées en programmation :

- recevoir et contrôler des paramètres en méthode POST
- manipuler des chaînes de caractères
- utiliser une fonction ou une classe conforme à la RFC2104 implémentant le HMAC SHA1 ou MD5
- sauvegarder le contexte de paiement en fichier ou base de données
- suivre le déroulement pas à pas d'un programme dans un outil de débogage ou en programmant des traces.

## 1.1 Open Kits : exemples d'intégration

A titre d'information, des exemples en PHP, ASPX, ASP, Python, Java et C de chacun des deux programmes d'interface avec notre solution vous sont fournis avec la documentation.

Vous pourrez utiliser ces exemples comme point de départ et vous devrez les modifier selon les spécificités de votre environnement et de votre application. En particulier, le stockage des clés devra être revu pour exploiter les meilleurs outils de confidentialité disponibles dans votre environnement. Les exemples proposent un stockage en base de données ou en 2 fichiers textes complémentaires de manière à ce que la compromission accidentelle d'un seul fichier ne compromette pas la clé.

## 1.2 Open Tools : prise en charge des paramètres

Cet outil s'exécute en local et génère, à partir des paramètres du terminal (clé, numéro de TPE, code société, etc.), les sections de code de personnalisation correspondant à chacun des exemples proposés. Les blocs de code générés sont à revoir, comme il a été dit plus haut, pour exploiter au mieux les outils de sécurisation de données dont vous disposez pour protéger les secrets et, de façon générale, pour exploiter au mieux les possibilités de votre environnement.

## 1.3 Clé de sécurité commerçant

Une clé de sécurité, propre au terminal, destinée à certifier les données échangées entre le serveur du commerçant et le serveur de paiement sécurisé de la banque, est attribuée par la banque à chaque TPE virtuel. Cette clé, associée au TPE virtuel du commerçant, est indispensable pour utiliser le service de paiement par carte bancaire.

Un lien de téléchargement sécurisé (lien codé, protocole SSL, authentification du souscripteur de contrat par son identifiant/mot de passe) est envoyé par notre centre de support. Le commerçant, après authentification, téléchargera cette clé sous forme d'un fichier texte scellé de 4 lignes à conserver sur un support externe. Le nom proposé par défaut au téléchargement est `<numéro de TPE>.key` (par exemple : `1234567.key`), mais il n'y a pas de contrainte de nom.

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 valeur de clé utilisée dans les fonctions de HMAC est une chaîne de 20 octets représentée de façon externe par 40 chiffres hexadécimaux (par exemple : `0123456789ABCDEF0123456789ABCDEF01234567`). Cette représentation externe doit être convertie en une chaîne de 20 octets (représentation opérationnelle) avant utilisation.

L'outil « Open Tools » construit les différentes représentations opérationnelles de la clé, selon les langages et les met en situation dans les exemples, à partir du fichier clé unique.

## 2 Spécifications des messages échangés

### 2.1 Rappel de la cinématique

Action	Intervenant
Le serveur commerçant obtient l'accord de l'internaute sur la chose et le prix	Site web du commerçant
Le serveur du commerçant rassemble les données du paiement à effectuer ...	Interface « Aller » sur le serveur du commerçant
... puis crée le formulaire de paiement scellé : fonction <code>creer_formulaire()</code> ...	
... puis met en page ce formulaire de paiement à destination de l'internaute	
L'internaute clique sur le bouton correspondant au formulaire de paiement et accède au serveur de paiement	Serveur de paiement de la banque
Le serveur bancaire vérifie la validité du sceau et entame le dialogue de paiement avec l'internaute	
L'internaute dialogue avec le serveur bancaire et paye (ou ne paye pas) par carte bancaire	
Le serveur bancaire renvoie un résultat de paiement scellé au serveur du commerçant sur son interface « Retour »	
Le serveur du commerçant vérifie la validité du sceau : fonction <code>tester_HMAC()</code> ...	Interface « Retour » sur le serveur du commerçant
... puis prend en compte le résultat de paiement ...	
... puis répond au serveur bancaire : fonction <code>creer_accuse_reception()</code>	
Le serveur affiche le résultat du paiement (avec le numéro d'autorisation si autorisation)	Serveur de paiement de la banque
L'internaute peut imprimer (ou sauvegarder) cette page	
Le serveur propose à l'internaute de revenir sur le site du commerçant via un lien hypertexte	
S'il suit ce lien, l'internaute quitte le serveur de paiement et revient sur le site du commerçant	
Le serveur du commerçant adapte son dialogue en fonction du résultat de paiement reçu (ou non reçu) et sauvegardé par l'interface « Retour »	Site web du commerçant

## 2.2 Phase aller du paiement (interface « Aller »)

### Cr ation du formulaire

La fonction `creer_formulaire()` met en forme les param tres du terminal et les donn es de la commande en un formulaire HTML scell  afin de transmettre la demande de paiement au serveur de la banque via le navigateur du client.

Champs	Description	Remarque
<b>Action</b>	URL du service de paiement de la banque	En test ou en production
<b>version</b>	Version du syst�me de paiement utilis�e	Version actuelle <code>1.2open</code>
<b>TPE</b>	Num�ro de TPE Virtuel du commer�ant (cha�ne num�rique sur 7 positions)	exemple : <code>1234567</code>
<b>date</b>	Date de la commande au format <code>JJ/MM/AAAA:HH:MM:SS</code>	Exemple : <code>05/12/2006:11:55:23</code>
<b>montant</b>	Montant TTC de la commande format�e de la mani�re suivante : Un nombre entier Un point d�cimal (optionnel) Un nombre entier (optionnel) Une devise sur 3 caract�res alphab�tiques ISO4217 ( <code>EUR</code> , <code>USD</code> , <code>GBP</code> , <code>CHF</code> , etc.)	Exemples : <code>62.73EUR</code> <code>10GBP</code>
<b>reference</b>	R�f�rence unique de la commande sur 12 caract�res alphanum�riques (A..Z, a..z, 0..9) permettant d'identifier de mani�re unique la commande	Exemple : <code>ABERTYP00145</code>
<b>texte-libre</b>	Zone de texte libre (taille maximale : 100 caract�res)	
<b>lgue</b>	Code langue (en majuscules), parmi <code>FR</code> , <code>EN</code> , <code>DE</code> , <code>IT</code> , <code>ES</code> , <code>NL</code>	
<b>societe</b>	Code alphanum�rique � usage interne uniquement permettant au commer�ant d'utiliser le m�me TPE Virtuel pour des sites diff�rents (param�trages distincts) se rapportant � la m�me activit�	Exemple : <code>monSite1</code>
<b>url_retour</b>	URL par laquelle l'acheteur revient sur la page d'accueil de la boutique	
<b>url_retour_ok</b>	URL de la page de retour de l'acheteur sur le site du commer�ant suite � un paiement accept�	Attention : � ne pas confondre avec l'URL de l'interface « Retour », aussi appel�e URL de confirmation des paiements
<b>url_retour_err</b>	URL de la page de retour de l'acheteur sur le site du commer�ant suite � un paiement refus�	
<b>MAC</b>	Sceau issu de la certification des donn�es	
<b>Bouton</b>	Texte du bouton de paiement	

Le sceau (  mettre dans le champs MAC) est calcul    l'aide de la fonction

```

HMAC-SHA1 (
    <donn es   certifier>,
    <cl  de s curit  commer ant sous forme op rationnelle>
)

```

fournie dans les exemples d'impl mentation (ou   l'aide de toute autre fonction respectant les sp cifications de la RFC 2104). Les donn es   certifier seront pr sent es sous la forme d'une concat nation dans un ordre pr cis des informations du formulaire :

```

<TPE>* <date>* <montant>* <reference>* <texte-libre>*
<version>* <l gue>* <soci te>*

```

Exemple :

```

1234567*05/12/2006:11:55:23*62.73EUR*ABERTYP00145*Exemple
TexteLibre*1.2open*FR*monSite1*

```

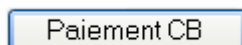
## Exemple de formulaire de paiement

```

<form method="post" name="FormulaireEncodeConforme" target="_top"
    action="https://paiement.creditmutuel.fr/paiement.cgi">
    <input type="hidden" name="version" value="1.2open">
    <input type="hidden" name="TPE" value="1234567">
    <input type="hidden" name="date" value="05/12/2006:11:55:23">
    <input type="hidden" name="montant" value="62.73EUR">
    <input type="hidden" name="reference" value="ABERTYP00145">
    <input type="hidden" name="MAC" value="78bc376c5b192f1c48844794cbdb0050f156b9a2">
    <input type="hidden" name="url_retour"
        value="http://url.retour.com/ko.cgi?order_ref:votreRF12345">
    <input type="hidden" name="url_retour_ok"
        value="http://url.retour.com/ok.cgi?order_ref:votreRF12345">
    <input type="hidden" name="url_retour_err"
        value="http://url.retour.com/err.cgi?order_ref:votreRF12345">
    <input type="hidden" name="l gue" value="FR">
    <input type="hidden" name="soci te" value="monSite1">
    <input type="hidden" name="texte-libre" value="ExempleTexteLibre">
    <input type="submit" name="bouton" value="Paiement CB">
</form>

```

La seule partie visible de ce formulaire est le bouton de paiement :



Les champs de ce formulaire doivent tous  tre encod s en HTML. Les sp cifications d'encodage sont d crites en fin de document.

Cet encodage est pr conis  pour la s curit  du site commer ant. En effet, le code qui doit r aliser la fonction `creer_formulaire()` recevra dans la pratique l'essentiel des valeurs de ces champs depuis un programme distinct, appartenant   la solution de commerce. Or, il est de bonne pratique de coder en HTML tout champ

à afficher provenant d'une source tierce, à commencer bien entendu par les champs saisis par les utilisateurs. Le code `creer_formulaire()` n'a pas d'informations sur l'origine première de ces champs, il doit donc les encoder tous.

Notez bien que le formulaire suivant, dont les valeurs de champs ne sont pas codées en HTML, n'est pas conforme à nos spécifications.

```
<form method="post" name="Formulaire_NON_Conforme" target="_top"
  action="https://paiement.creditmutuel.fr/paiement.cgi">
  <input type="hidden" name="version" value="1.2open">
  <input type="hidden" name="TPE" value="1234567">
  <input type="hidden" name="date" value="05/12/2006:11:55:23">
  <input type="hidden" name="montant" value="62.73EUR">
  ...
</form>
```

## Messages d'erreur

Voici les erreurs les plus courantes qui peuvent être renvoyées par le serveur de paiement suite à l'envoi par le commerçant d'un formulaire de paiement.

Le site de votre commerçant n'a pas été identifié par notre serveur.

Les informations transmises par votre interface « Aller » ne sont pas reconnues par le serveur de la banque :

- vérifiez que vous avez bien répondu aux questions qui sont posées dans le mail de fourniture de la clé
- vérifiez que les paramètres {numéro de TPE ; code société (respectez les majuscules et les minuscules) ; langue} transmis par votre interface « Aller », correspondent aux informations que vous nous avez envoyées par courriel
- vérifiez que l'URL d'appel à la page de paiement est correcte (et correspond bien à celle de test)

Les informations transmises par votre commerçant ont une signature non valide : le niveau de sécurité exigé n'est pas atteint.

Le champ `MAC` transmis par votre interface « Aller » n'est pas valide ou n'a pas pu être calculé :

- affichez le code source du formulaire généré et vérifiez que le champ `MAC` est valorisé par une suite de chiffres hexadécimaux ;
- vérifiez que vous avez bien intégré la clé : comparez le champ de contrôle affiché par les exemples fournis, avec le champ de contrôle affiché dans l'outil de prise en charge de clé ;
- Vérifiez que vous avez la bonne clé : transmettez le champ de contrôle produit par l'outil de prise en charge de clé au centre de support (ne transmettez que ce champ et non la clé elle-même).



Si vous avez le moindre doute sur une action ou un oubli de votre part qui pourrait avoir porté la clé à la connaissance de personnes non autorisées, contactez le centre de support pour la génération d'une nouvelle clé.

Votre commande a déjà été traitée.

Ce message signifie que vous passez une commande sur une référence déjà utilisée.

La date de validité de votre commande est dépassée.

Deux cas sont possibles :

- Soit la référence de commande est en instance de paiement depuis un délai trop important (typiquement plus d'une heure) : dans ce cas, testez un formulaire mis à jour avec une nouvelle référence de commande
- Soit le formulaire de commande a été créé depuis un délai trop important, typiquement plus de 12 heures : dans ce cas, testez un nouveau formulaire et vérifiez la date système de votre machine

Mode de paiement non disponible.

Deux cas sont possibles :

- Soit il y a une erreur de syntaxe dans le formulaire soumis (par exemple « **S**ociete=... » à la place de « **s**ociete=... »)
- Demande d'un mode de paiement non souscrit par le commerçant

## 2.3 Phase retour du paiement (interface « Retour »)

Après avoir traité la demande de paiement, en dialogue avec l'internaute payant par carte, le serveur de la banque informe directement le serveur du commerçant du résultat de la demande de paiement en émettant une requête HTTP on-line, contenant le résultat de la demande de paiement, sur l'URL de confirmation des paiements (interface « Retour ») ; URL que vous devez nous indiquer au moment de la mise en place du système.

L'interface « Retour » est chargée de recevoir cette requête de confirmation du paiement, d'en extraire les différentes informations, dont le résultat du paiement, de mettre à jour l'état de la commande dans les bases commerçant, et de répondre par un accusé de réception.

Pour cela il doit implémenter les fonctionnalités `tester_HMAC()` (prise en compte des aspects de sécurisation des échanges) et `creer_accuse_reception()` (génération de l'accusé de réception à renvoyer au serveur de la banque).

## Paramètres renvoyés par la banque

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

Champs	Description	Remarque
<b>MAC</b>	Sceau résultant de la certification des données (voir plus bas)	
<b>TPE</b>	Numéro de TPE Virtuel du commerçant (chaîne numérique sur 7 positions)	Le serveur de la banque renvoie ici les données telles qu'elles ont été reçues lors de la phase aller du paiement
<b>date</b>	Date de la commande au format JJ/MM/AAAA_a_HH:MM:SS	
<b>montant</b>	Montant TTC de la commande formatée de la manière suivante : Un nombre entier Un point décimal (optionnel) Un nombre entier (optionnel) Une devise sur 3 caractères alphabétiques ISO4217 (EUR, USD, GBP, CHF, etc.)	
<b>reference</b>	Référence unique de la commande sur 12 caractères alphanumériques (A..Z, a..z, 0..9) permettant d'identifier de manière unique la commande	
<b>texte-libre</b>	Zone de texte libre (taille maximale : 100 caractères)	
<b>code-retour</b>	Le résultat du paiement, parmi : payetest paiement accepté (en TEST uniquement) paiement paiement accepté (en Production uniquement) Annulation paiement refusé	
<b>retourPLUS</b>	Liste d'informations complémentaires, séparées par « -- »	Exemple : --optionA--optionB

Exemple de données envoyées par le serveur de paiement de la banque à l'interface « Retour » :

```
TPE=1234567&date=05%2f12%2f2006%5fa%5f11%3a55%3a23&montant=62%
2e75EUR&reference=ABERTYP00145&MAC=e4359a2c18d86cf2e4b0e646016
c202e89947b04&texte-libre=reference+commande+tres+tres+longue&
code-retour=paiement&retourPLUS=--optionA--optionB
```

## Complément « retourPLUS »

Sur la version actuelle de la solution de paiement (1.2open), un champ « retourPLUS » est ajouté aux informations que le serveur de paiement de la banque transmet à l'interface « Retour » du commerçant. Selon la méthode utilisée pour appeler l'interface « Retour » (en http ou en HTTPS), ce champ peut contenir diverses informations :

Info	Description	Si HTTP	Si HTTPS
--cvx	oui si le cryptogramme visuel (obligatoire pour les cartes Visa et MasterCard) a été saisi non sinon	✓	✓
--hpan	Hachage irréversible (HMAC-SHA1) du numéro de la carte de crédit utilisée pour effectuer le paiement (identifiant de manière unique une carte de crédit pour un commerçant donné)		✓
--vld	Date de validité de la carte de crédit utilisée pour effectuer le paiement		✓
--bin	Code BIN de la banque du porteur de la carte de crédit		✓
--3Dve	Y La carte de crédit utilisée pour le paiement est également adossée au programme « 3DSecure » N La carte de crédit utilisée pour le paiement n'est pas adossée à ce programme	✓	✓
--3Dpa	Y La banque émettrice de la carte utilisée pour le paiement a validé que votre client est bien le propriétaire de la carte N La banque émettrice de la carte utilisée pour le paiement suspecte que votre client utilise une carte qui n'est pas la sienne, ou n'est pas en mesure de le déterminer Remarque : cette option n'a de signification que si l'option 3Dve vaut Y	✓	✓

Exemple :

retourPLUS=--cvxoui--hpan1A2B3C4D5E6F70819203A2B3C4D5E6F708192031

## Validation du sceau

Le message de confirmation reçu est scellé par un sceau **MAC** qui a été calculé par le serveur de paiement de la banque à l'aide de la clé de sécurité commerçant attribuée à votre terminal de paiement.

La fonctionnalité `tester_HMAC()` 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, elle 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** on pourra s'aider de la fonction

```
HMAC-SHA1 (  
    <données à certifier>,  
    <clé de sécurité commerçant sous forme opérationnelle>  
)
```

fournie dans les exemples d'implémentation (ou de toute autre fonction respectant les spécifications de la RFC 2104).

Les données à certifier seront présentées sous la forme d'une concaténation dans un ordre précis des informations envoyées par le serveur de la banque :

```
<retourPLUS><TPE>+<date>+<montant>+<reference>+<texte-  
libre>+1.2open+<code-retour>+
```

Exemple :

```
--optionA--optionB1234567+05/12/2006:11:55:23+62.73EUR+ABE  
RTYP00145+ExempleTexteLibre+1.2open+paiement+
```

## Création de l'accusé de réception

La réponse renvoyée par l'interface « Retour » au serveur de paiement de la banque 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
Oui	<code>Pragma: no-cache&lt;LF&gt;</code> <code>Content-type : text/plain&lt;LF&gt;</code> <code>Version: 1&lt;LF&gt;</code> <code>OK&lt;LF&gt;</code>
Non	<code>Pragma: no-cache&lt;LF&gt;</code> <code>Content-type : text/plain&lt;LF&gt;</code> <code>Version: 1&lt;LF&gt;</code> <code>Document falsifiée&lt;LF&gt;</code>

Lorsque le serveur de la banque ne reçoit pas d'accusé de réception « OK » (time out, erreur, ...), il envoie un courriel d'alerte sur une boîte aux lettres électronique de surveillance indiquée par le commerçant et refait une seconde tentative.

Pour cela, 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 fait au moins un test complet avec accusé de réception « OK ».

## 2.4 Spécification des formats

### Contraintes générales de codage HTML des champs

Tous les champs de formulaire (interface « Aller ») 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 impérativement sont les codes ASCII de 0 à 127 réputés risqués :

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

Les fonctions de type « **HTML\_ENCODE** » des langages conviennent parfaitement, elles encodent beaucoup plus de caractères, typiquement tout ce qui n'est pas :

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

Si vous utilisez dans le champ « **texte-libre** » des caractères hors de la plage ascii commune imprimable (31<ascii<127), vous devez coder ce champ avant tout traitement relatif au paiement pour éviter tout problème de calcul du sceau MAC.

### Contraintes particulières selon le champ

Champs	Contenu / format avant codage HTML	Taille maximale après codage HTML
tpe	A-Z a-z 0-9	7
Version	1.2open	Fixe
Date		40
Montant		20
Référence	A-Z a-z 0-9	12
MAC	0-9 A-F a-f	40
Lgue	A-Z	2
Societe	A-Z a-z 0-9	20
Texte-libre	Base 64	3200
retourPLUS	A-Z a-z 0-9 _ . -	2048
URLs		1024

## 3 URLs des serveurs de paiement

### 3.1 En Test

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

Sur ce serveur, le seul contrôle effectué est un contrôle de structure du numéro de carte. 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.

Afin de tester les différents codes de retour du serveur bancaire, vous avez la possibilité d'utiliser plusieurs cartes de tests dont les coordonnées sont affichables en cliquant sur l'icône « Carte de Test » de la page de paiement bancaire.

Les environnements de test sont disponibles aux adresses suivantes :

- Pour les banques et fédérations du Crédit Mutuel :  
<https://paiement.creditmutuel.fr/test/paiement.cgi>
- Pour les banques du Groupe CIC :  
<https://ssl.paiement.cic-banques.fr/test/paiement.cgi>
- Pour la banque OBC : <https://ssl.paiement.banque-obc.fr/test/paiement.cgi>

### 3.2 En Production

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

- Pour les banques et fédérations du Crédit Mutuel :  
<https://paiement.creditmutuel.fr/paiement.cgi>
- Pour les banques du Groupe CIC :  
<https://ssl.paiement.cic-banques.fr/paiement.cgi>
- Pour la banque OBC : <https://ssl.paiement.banque-obc.fr/paiement.cgi>

**Nous attirons votre attention sur le fait que les formulaires de paiement adressés au serveur de production seront des paiements réels.**

## 4 Aides à l'installation

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

- Par mail : boîte aux lettres « **Commerce Electronique** » ([centrecom@e-i.com](mailto:centrecom@e-i.com))<sup>1</sup>
- Par téléphone : **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.

### 4.1 Utilisation de l'outil « Open Tools » de configuration

Cet outil, nommé « Extract HMAC », vous aide à mettre en place la clé de cryptage dans votre environnement. Cet outil est disponible pour les clés SHA1 et MD5. Avant de commencer la configuration, veuillez prendre note des recommandations suivantes :

- Lisez attentivement toutes les documentations et licences
- Prenez les meilleures dispositions pour protéger et stocker de manière sécurisée les deux parties de la clé
- Vous pouvez évaluer le processus complet d'intégration avec l'option « clef fictive », mais cela ne vous permettra pas d'interagir avec nos serveurs

L'utilisation de l'outil est détaillée étape par étape ci-dessous :

---

<sup>1</sup> La boîte aux lettres ETS TPE VIRTUEL est désormais renvoyée sur la boîte aux lettres « Commerce Electronique » ; elle sera prochainement supprimée. La boîte aux lettres « Commerce Electronique » devient donc désormais le seul point d'entrée pour le support de la solution.





Boite à outils Hmac-SHA1 personnalisée pour  
Hmac-SHA1 ToolBox custom for



Lire les licences ☐ Read licenses

The screenshot shows a web-based HMAC-SHA1 tool interface. It includes a text area for pasting a key (callout 1), a field for a key value (callout 2), a field for a TPE number and a 'Calculer le HMAC de Contrôle' button (callout 3), a section for site code and button text (callout 4), fields for OK and Not OK URLs (callout 5), a dropdown for kit selection (callout 6), a dropdown for bank selection (callout 7), a 'Code Source' button (callout 8), and a section with multiple text fields for output (callout 9).

1. Remplacez le contenu de ce cadre par le contenu du fichier clé que nous vous avons fourni (<numéro de TPE>.key)
2. Renseignez ce champ avec une phrase clé ou cliquez sur le bouton pour en générer une de manière automatique
3. Saisissez le numéro de TPE puis cliquez sur le bouton « Calculer le HMAC de contrôle »
4. Renseignez le code société
5. Renseignez les URL « OK » et « Not OK »
6. Indiquez le kit choisi
7. Choisissez la banque concernée
8. Une fois les étapes précédentes réalisées, le bouton « Code Source » devient actif ; cliquez sur ce bouton
9. Du code est apparu dans un ou plusieurs de ces champs, sous chaque champ rempli, se trouve un bouton indiquant un nom de fichier ; pour chaque champ, copiez le contenu et insérez-le dans le fichier indiqué sur le bouton (voir l'exemple ci-dessous)

Code Société / Site Code siteTest	Texte du Bouton / Button Text Paielement CB - Card Payment
URL OK http://url.retour.com/ok.cgi	URL Not OK http://url.retour.com/ko.cgi
Kit choisi / Choose your kit PHP>=4.3.0	Serveur bancaire / Bank server Crédit Mutuel
<input type="button" value="Code Source &gt;"/> <input type="button" value="Reset"/>	
<pre>define("CMCIC_DIR", "/test/"); define("CMCIC_SERVER", "paielement.creditmutuel.fr/V&amp;D" ); function CMCIC_hmac(\$CMCIC_Tpe, \$data="") {     \$pass = "fia07V7Wnk+Q5t9tIu-1";</pre> <p><b>Ce code doit être inséré dans le fichier</b></p> <p>Select custom code for "CMCIC_HMAC.inc.php"</p>	
<pre>\$MyTpe = array ( "tpe" =&gt;"00000001", "soc" =&gt; "siteTest", "key" =&gt; "6e0462415ffc7a68c8fe088508ae8a1cf46258c0" ); \$MyTpe["retourok"] = "http://url.retour.com/ok.cgi"; \$MyTpe["retourko"] = "http://url.retour.com/ko.cgi"; \$MyTpe["submit"] = "Paielement CB - Card Payment";</pre> <p><b>Ce code doit être inséré dans le fichier</b></p> <p>Select custom code for "MyTpeCMCIC.inc.php"</p>	
<p>Keep in mind to do your best about storing splitted keys safe and secure. Prendre les meilleures dispositions pour stocker et protéger les 2 parties de la clef.</p> <p><b>Ici il n'y a rien à copier, le bouton est donc vide</b></p>	

## 4.2 Foire aux questions

### Peut-on personnaliser la page de paiement ?

Non, la page de paiement est une page spécifique au serveur de paiement de la banque, vous ne pouvez pas intervenir sur son aspect. Pour vous, le fait d'être sur le serveur de la banque est aussi une façon de crédibiliser le paiement électronique vis-à-vis des acheteurs. Seul le logo de votre société peut être mis en place.

### Comment afficher mon logo sur votre page de paiement ?

Vous devez nous transmettre par courriel au centre de support ([centrecom@e-i.com](mailto:centrecom@e-i.com)) l'URL d'une image représentant votre logo. Cette image doit être au format GIF et d'une taille de 120 pixels x 120 pixels maxi.

### Quel est le temps maximum dont dispose mon client pour effectuer le paiement (saisie du numéro de carte) suite à une commande sur mon site ?

L'internaute dispose de 45 minutes, à partir de l'arrivée sur la page de paiement, pour saisir les informations relatives à sa carte bancaire. Au-delà de ce délai, toute saisie sera refusée.

### Quel est le nombre d'essai pour saisir les numéros de carte bleue ?

Le nombre d'essai maximum pour un paiement est de 3.

### Où peut-on trouver des numéros de carte pour effectuer des tests ?

Sur la page de paiement, vous trouverez une icône clignotante « TEST » ; en cliquant sur cette icône, une fenêtre présentant différents numéros de cartes de test s'ouvre. Il vous suffit alors de sélectionner l'une des cartes et le formulaire de la page de paiement se remplit automatiquement.

Vous disposez de plusieurs cartes de test :

- 2 cartes 16 pan : l'une pour provoquer un paiement accepté et l'autre pour provoquer un paiement refusé
- 2 cartes 15 pan (cartes étrangères) sur le même principe

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

- Français
- Anglais
- Allemand
- Espagnol
- Italien
- Néerlandais

### Peut-on être prévenu par courriel pour chaque demande de paiement ?

Une notification peut être envoyée par courriel à chaque fois qu'une demande d'autorisation est effectuée (une demande d'autorisation est effectuée si le format du numéro de carte a été validé). Il faut demander l'activation de cette option en s'adressant au centre de support ([centrecom@e-i.com](mailto:centrecom@e-i.com)).

### Comment connaître le nom et l'adresse des porteurs de carte ?

Nous ne disposons pas des informations relatives aux coordonnées de l'acheteur sur notre serveur de paiement ; en effet, le client ne saisit que les informations concernant sa carte bancaire (numéro, date d'expiration et cryptogramme visuel).

Il n'est pas prévu dans le cadre de notre solution de paiement que le commerçant puisse nous transmettre des informations sur le client. Nous ne proposons pas de moyen de déduire l'identité du porteur à partir des informations de la carte.

### Peut-on re-créditer un paiement ?

Oui, pour cela il faut demander l'option « re-crédit » à votre conseiller commercial. Cette fonction est ensuite disponible sur le tableau de bord commerçant.

### A quoi correspondent les différentes « URL RETOUR » du paramétrage ?

- **url\_retour** : correspond au lien affiché en bas de notre page de paiement, avant que le client ne valide sa saisie ; ce lien permet à l'acheteur de revenir sur une page de votre boutique sans avoir effectué de paiement
- **url\_retour\_ok** : correspond au lien (permettant à l'acheteur de retourner sur une page de votre boutique) affiché en bas de notre page de paiement une fois le paiement effectué et accepté
- **url\_retour\_err** : correspond au lien (permettant à l'acheteur de retourner sur une page de votre boutique) affiché en bas de notre page de paiement une fois le paiement effectué et refusé

Il ne faut pas confondre ces URL avec l'URL de l'interface « Retour ».

### A quoi sert l'« URL de confirmation CGI2 » ?

Cette URL est celle de votre interface « Retour », dont le rôle est de recevoir le message de confirmation du paiement émis par le serveur banque.

### Où doit-on paramétrer l'« URL de confirmation CGI2 » ?

Cette URL est renseignée dans nos bases ; vous devez nous la fournir lors de la phase de mise en place de la solution. Vous devez également nous notifier de tout changement d'adresse de votre interface « Retour » (en vous adressant au centre de support : [centrecom@e-i.com](mailto:centrecom@e-i.com)).

### Que faire lorsque je rencontre une erreur « CGI2 NOT OK » ?

Vous devez tout d'abord effectuer les vérifications de base suivantes :

- L'adresse de l'interface « Retour » que vous nous avez fournie est-elle valide ?
- Cette adresse est-elle accessible sur votre serveur depuis l'extérieur ?
- Le port sur lequel s'adresser à votre interface « Retour » est-il bien 80 (http) ou 443 (https) ? En effet, notre serveur de paiement n'accepte de s'adresser qu'à ces deux ports

Si le problème persiste, veuillez effectuer les vérifications supplémentaires suivantes :

- le traitement entre le retour de notre serveur et votre envoi d'accusé de réception ne doit pas durer trop longtemps (moins de 30 secondes)

- il ne doit pas être fait de redirection à la réception du code retour paiement
- la vérification du MAC (fonctionnalité `tester_HMAC()`) doit être faite avant la génération de l'accusé de réception (fonctionnalité `creer_accuse_reception()`)

J'obtiens le message « Ce TPE est fermé » lors d'une demande de paiement sur le serveur de TEST ?

Les TPE de test non utilisés pendant 30 jours glissants sont automatiquement fermés par nos services. Il ne sont cependant pas supprimés : vous pouvez utiliser la fonctionnalité de réouverture d'un TPE de TEST sur votre tableau de bord.

Peut-on avoir un TPE pour plusieurs sites ?

Oui, mais cela nécessite en amont une demande auprès de votre conseiller commercial. Il faut cependant que les différents sites répondent à la même activité. Le paramétrage étant spécifique pour chaque site, il vous faut nous transmettre toutes les informations (URLs de retour, adresse de l'interface « Retour », logo, etc.).

Peut-on obtenir un fichier relevé des paiements ?

Une telle prestation peut vous être fournie par votre banque ; vous pouvez vous adresser à votre conseiller commercial.