E-transactions

MANUEL INTEGRATION

Solution E-transactions

VERSION DU

21/09/2016

REFERENCES DOCUMENTATIONS

REF.	DOCUMENT	DESCRIPTION
Ref 1	Manuel Intégration Gestion Automatisée des Encaissements	Manuel d'intégration de la solution Gestion Automatisée des Encaissements
Ref 2	Paramètres Test E-transactions	Manuel décrivant les environnements et paramètres de test (pré-production).
Ref 3	Manuel Utilisateur Back-office E-transactions	Manuel Utilisateur du Back Office Commerçant
Ref 6	Personnalisation de la page et ticket de paiement	Manuel Intégrateur pour personnaliser la page de paiement aux couleurs de votre commerce
Ref 7	Note Paypal	Note d'intégration pour Paypal
Ref 8	Guide des bonnes pratiques de la sécurisation de la clé HMAC	Guide décrivant les bonnes pratiques relatives au stockage et à l'utilisation de la clé HMAC
Ref 9	Note Paylib	Note d'intégration pour Paylib
Ref 10	Note MasterPass	Note d'intégration pour MasterPass

AVERTISSEMENT

Les informations contenues dans ce document n'ont aucune valeur contractuelle. Elles peuvent faire l'objet de modification à tout moment. Elles sont à jour en date de rédaction au 01/03/2015.

E-transactions est une solution d'encaissement et de gestion des paiements à distance par carte bancaire, dans un environnement sécurisé, distribuée par les Caisses régionales de Crédit Agricole.
Renseignez-vous auprès de votre conseiller sur les conditions générales et tarifaires de cette solution.

Cette documentation peut être enrichie par vos commentaires. Vous pouvez nous envoyer un email à support@e-transactions.fr, en indiquant votre remarque aussi précisément que possible. Merci de préciser la référence du document ainsi que le numéro de la page.

.

ASSISTANCE

Pour tout renseignement ou assistance à l'installation et à l'utilisation de nos produits, nos Equipes restent à disposition des commerçants et Intégrateurs, du lundi au vendredi de 9H à 18H30 :

Support Technique & Fonctionnel :

E-mail : support@e-transactions.fr

Téléphone : 0 810 812 810 ***(1)***

(1) prix d'un appel local non surtaxé depuis un poste fixe

Pour tout contact auprès de nos services, il faut IMPERATIVEMENT communiquer les identifiants :

- numéro de SITE (7 chiffres)
- numéro de RANG (2 chiffres)
- numéro d'identifiant (1 à 9 chiffres)

TABLE DES MATIERES

1. OBJET DU DOCUMENT

Dans le domaine de la VAD et du e-commerce, le Crédit Agricole propose une solution de paiement sur internet appelée **E-**transactions, elle peut être intégrée au site commerçant de différentes façons en s'appuyant sur des interfaces techniques spécifiques :

- **E-**transactions s'interface avec le site marchand Internet ou mobile. Les clients acheteurs sont redirigés automatiquement sur les pages de paiement multilingues. Ces pages sont personnalisables pour les harmoniser avec l'identité graphique du site Marchand.

  E-transactions répond aux normes de sécurité des paiements par carte sur les sites d'e-commerce en affichant une page SSL 256 bits et en utilisant le protocole 3-DSecure.

- **G**estion **A**utomatisée des **E**ncaissements est utilisée pour valider les encaissements des transactions préalablement autorisées via **E-**transactions, assurer des remboursements et annulations de serveur à serveur.

- **G**estion **A**utomatisée des **E**ncaissements peut également assurer le traitement des paiements de façon transparente pour les clients acheteurs. L'application de vente du marchand doit collecter les informations sensibles telles que le n° de carte et les transmet à notre plateforme via un dialogue sécurisé de serveur à serveur. Le site marchand doit alors être PCIDSS.

  Compléter **E-**transactions avec la **G**estion **A**utomatisée des **E**ncaissements permet au commerçant de gagner en flexibilité en intégrant le pilotage des opérations post-autorisation en mode serveur à serveur depuis son application de vente (ou son back-office).

  Pour aller plus loin, l'Application de vente du commerçant peut demander à notre plateforme de conserver les données du moyen de paiement. Cette solution s'interface parfaitement en complément de **E-**transactions ou bien directement en mode serveur à serveur. Ce service permet au Commerçant de gérer des paiements en plusieurs fois ainsi que des paiements express (en un clic) où l'Acheteur ne redonne pas les données de son moyen de paiement à chaque nouvelle transaction.

- **T**raitement par **L**ot (pour E-transactions Téléphone Fax Courrier = gestion automatisée) : Cette solution assure un dialogue par échanges de fichiers structurés en mode off-line entre le commerçant et notre plateforme. L'application de vente du site Marchand doit collecter les informations sensibles telles que le n° de carte et les transmet à notre plateforme via un dialogue sécurisé de serveur à serveur.

  Traitement Par Lot est également utilisé pour valider les encaissements des transactions préalablement autorisées via **E-**transactions, mais également pour assurer des remboursements et annulations.

Le présent document est le manuel d'intégration de la solution **E-**transactions.

Il s'adresse aux personnes ayant besoin d'informations sur le fonctionnement de cette solution, sur la manière de s'y interfacer et de l'intégrer de la meilleure manière.

2. PRESENTATION DE LA SOLUTION E-transactions

2.1 Principe général de fonctionnement

E-transactions est un système sécurisé de gestion des paiements par cartes bancaires et privatives sur les sites marchands Internet ou mobile.

Pour intégrer E-transactions il n'y a aucun module à installer, ni sur le site marchand, ni chez le client qui veut effectuer un paiement.

Une fois le produit intégré dans le site marchand, votre client peut effectuer son paiement en toute sécurité : sa commande réalisée, il sera redirigé vers les serveurs E-transactions. Ces derniers établissent alors une connexion cryptée avec l'acheteur (en SSL 128 bits, afin que la saisie des informations confidentielles liées à la carte de paiement soit effectuée en toute sécurité) et lui affichent une page de paiement, en l'invitant à saisir ses informations Carte.

E-transactions vérifie alors la validité de la carte en effectuant une demande auprès du centre d'autorisation associé au moyen de paiement choisi, dans le respect des normes de paiement en vigueur. Si le paiement est accepté, un ticket est alors affiché sur l'écran de l'acheteur (optionnel). Ce même ticket lui sera envoyé par courrier électronique (e-mail) comme preuve du paiement. L'acheteur a alors la possibilité de revenir sur le site marchand pour effectuer d'autres achats.

E-transactions envoie également par e-mail un double du ticket de paiement au commerce. Il sera possible, pour le commerçant, de gérer de façon automatique le résultat de la tentative de paiement grâce à l'analyse des différents retours d'informations.

En fin de journée, E-transactions réunit sous forme de « remise » tous les paiements cartes bancaires réalisés sur le site commerçant et les envoie au centre de télécollecte du commerçant, afin que les transactions soient traitées.
Une fois la télécollecte effectuée, le commerçant recevra un ticket de compte-rendu par e-mail.
Pour les autres moyens de paiements, E-transactions respecte les modalités des différents fournisseurs.

2.2 Liste des moyens de paiement

Ci-dessous une liste complète des moyens de paiement acceptés par E-transactions :

MOYEN DE PAIEMENT	TYPE	COMMENTAIRE
CB, VISA, MASTERCARD	Cartes de crédit	
MAESTRO	Carte de débit	3-D Secure obligatoire
E-CARTE BLEUE	Carte de crédit virtuelle dynamique	Opérée par VISA France
AMERICAN EXPRESS	Carte de crédit	
JCB	Carte de credit	
DINERS	Carte de credit	
COFINOGA	Carte de financement	
CETELEM / AURORE	Carte de financement	
ILLICADO	Carte cadeau prépayée	
MAXICHEQUE	Carte cadeau prépayée	
PAYSAFECARD	Carte Prépayée	
1EURO.COM	Financement en ligne	
PAYPAL	Portefeuille électronique	
LEETCHI	Cagnotte en ligne	
ONEY	Financement en ligne Carte cadeau prépayée	
iDEAL	Moyen de paiement Carte cadeau prépayée	Pays-Bas
PAYBUTTON	Moyen de paiement	Belgique
PAYLIB	Moyen de paiement	
MASTERPASS	Moyen de paiement	

2.3 Sécurité

2.3.1 Identification

Un site Marchand est référencé auprès des serveurs E-transactions par plusieurs éléments :

- Le numéro de site
- Le numéro de rang

Ces éléments d'identification sont fournis par l'assistance E-transactions lors de la confirmation de l'inscription du commerçant à l'utilisation de nos services.
Ces informations sont obligatoires dans tous les messages que le site Marchand enverra à notre plateforme de paiement mais il est également nécessaire de les fournir lors de tout contact avec les équipes de l'assistance E-transactions.

2.3.2 Authentification

Afin de garantir une sécurité maximale aux paiements effectués sur le site Marchand du commerçant, celui-ci est authentifié par une clé secrète HMAC, qui ne doit être connue que par lui.
Cette clé sera utilisée pour signer tous les échanges entre le site Marchand et les serveurs E-transactions afin de garantir que la demande de paiement provient d'une source authentifiée.
Le commerçant doit générer lui-même sa clé HMAC et le chapitre ***Gestion de la clé d'authentification*** décrit cette procédure.

2.4 Présentation des pages E-transactions

Tout au long du processus de paiement, plusieurs pages peuvent s'afficher successivement.

2.4.1 Page de présélection du moyen de paiement

Sur cette première page seront présentés l'ensemble des moyens de paiement auxquels le commerçant a souscrit et qu'il souhaite proposer à ses clients. Chaque client, au moment du paiement, est alors invité à sélectionner le moyen de paiement qu'il souhaite utiliser, et en fonction de son choix, l'affichage de la page de paiement sera adapté.

Par exemple, il ne sera pas demandé de saisie d'un cryptogramme visuel pour la carte Diners, mais il en sera demandé un, pour les cartes American Express, Visa ou Mastercard.
Voici ci-dessous un exemple de page de choix du moyen de paiement :

Cette page ne sera pas affichée, si le commerçant a précisé dans son appel, quel moyen de paiement il souhaite proposer.

- Le Crédit Agricole préconise que le commerçant valorise lui-même sur son site e-commerce, sous la forme d'icônes cliquables, la liste des moyens de paiement acceptés. L'acheteur sera alors directement envoyé sur la page de paiement adaptée au moyen de paiement sélectionné.

- Pour Plus d'informations sur les types de carte et moyens de paiement, voir **« *§3.2 Forçage du type et moyen de paiement* ».**

Cette page de présélection du moyen de paiement est personnalisable.

2.4.2 Page de paiement

La page affichée ci-dessus est un exemple de page de paiement personnalisée par un commerçant. Pour rassurer les clients, il est possible de personnaliser beaucoup d'éléments pour que la page s'intègre au mieux dans la charte graphique du site Marchand.
Les éléments personnalisables sont notamment :

- Le logo en haut de page
- L'affichage du logo Crédit Agricole
- Les boutons de validation/annulation/retour boutique
- Les langues
- Le fond d'écran
- Et bien d'autres options via un fichier CSS

Pour découvrir comment configurer toutes ces options, se référer au document ***[Ref 6]*** ***E-transactions - Personnalisation de la page et ticket de paiement.***

Autre exemple de personnalisation Ticket de paiement

Une fois le paiement autorisé, le client ainsi que le commerçant reçoivent par e-mail un ticket de paiement (à l'identique d'un terminal de paiement physique) avec en début de ticket les 50 premiers caractères de la référence commande.

En pied du ticket commerçant se trouve également l'adresse e-mail du client.

Le client est aussi redirigé vers une page lui confirmant immédiatement le bon déroulement de sa transaction. Cette page se présente par défaut sous la forme suivante :

Ticket d'un paiement réussi

- Il est possible de passer outre cette page et de rediriger, avec les résultats du paiement, le client directement sur le site Marchand (avec le code refus ou n° d'autorisation). Voir ***§4 Gestion de la réponse***
- De la même manière que la page de paiement, il est possible d'apporter un certain nombre d'améliorations au ticket de paiement transmis au client après son paiement. Par exemple, il est possible d'y ajouter un logo et un texte personnalisé.

- Pour Plus d'informations sur ces possibilités, se référer au document ***[Ref 6] E-transactions - Personnalisation de la page et ticket de paiement***.

3. APPEL DE LA PAGE DE PAIEMENT

Pour afficher la page de paiement au client qui souhaite payer sur le site Marchand, il suffit d'envoyer à l'URL de E-transactions une requête HTTPS avec un certain nombre de variables.

3.1 Préparation du message

Les variables suivantes sont obligatoires dans toute requête :

- PBX_SITE = Numéro de site (fourni par l'assistance E-transactions)
- PBX_RANG = Numéro de rang (fourni par l'assistance)
- PBX_IDENTIFIANT = Identifiant interne (fourni par l'assistance)
- PBX_TOTAL = Montant total de la transaction
- PBX_DEVISE = Devise de la transaction
- PBX_CMD = Référence commande côté commerçant
- PBX_PORTEUR = Adresse E-mail de l'acheteur
- PBX_RETOUR = Liste des variables à retourner par E-transactions
- PBX_HASH = Type d'algorithme de hachage pour le calcul de l'empreinte
- PBX_TIME = Horodatage de la transaction
- PBX_HMAC = Signature calculée avec la clé secrète

La signification de ces différentes variables ainsi que des variables optionnelles sont disponibles dans la partie

Dictionnaire de données***.***

L'ensemble de ces variables doit être envoyé par la méthode POST l'URL E-transactions.

Ci-dessous un exemple de formulaire transmis en pré-production :

```
<form method="POST" action="https:// preprod-tpeweb.e-transactions.fr/cgi/MYchoix_pagepaiement.cgi">
        <input type="hidden" name="PBX_SITE" value="1999887">
        <input type="hidden" name="PBX_RANG" value="98">
        <input type="hidden" name="PBX_IDENTIFIANT" value="3">
        <input type="hidden" name="PBX_TOTAL" value="1000">
        <input type="hidden" name="PBX_DEVISE" value="978">
        <input type="hidden" name="PBX_CMD" value="TEST ca-cp">
        <input type="hidden" name="PBX_PORTEUR" value="test@gmail.com">
        <input type="hidden" name="PBX_RETOUR" value="Mt:M;Ref:R;Auto:A;Erreur:E">
        <input type="hidden" name="PBX_HASH" value="SHA512">
        <input type="hidden" name="PBX_TIME" value="2011-02-28T11:01:50+01:00">
        <input type="hidden" name="PBX_HMAC" value="F2A799494504F9E50E91E44C129A45BBA2
        6D23F2760CDF92B93166652B9787463E12BAD4C660455FB0447F882B22256DE6E703AD6669B73C59
        B034AF0CFC7E">
        <input type="submit" value="Envoyer">
</form>
```

Le seul élément visible sur la page présentée en exemple sera le bouton « Envoyer ».

Quand le client cliquera dessus, il sera automatiquement dirigé vers la page de paiement de E-transactions.

Dans cet exemple le paiement est de 1000 centimes d'euros (soit 10 €) et l'identification du paiement par rapport à la commande du commerçant est la référence « TEST ca-cp ».

Une fois le paiement effectué, si ce dernier est accepté, un ticket de paiement sera envoyé par mail au commerçant ainsi qu'au client à « client@test.com ».
L'identification du commerçant (site 1999888, rang 98, identifiant 3) correspond à la boutique de test E-transactions, accessible sur notre environnement de pré-production.

Des informations complémentaires concernant les conditions de test sur notre environnement de pré-production sont disponibles au chapitre ***§***8 **Erreur ! Source du renvoi introuvable.**.

Attention, l'exemple ci-dessus fait référence à une URL de serveur factice.
Les URL d'appel en production sont définies au chapitre ***§10.6 URL d'appel et Adresses IP.***

3.2 Forçage du type et moyen de paiement

Si le commerçant préfère se charger lui-même du choix du moyen de paiement, il est possible de fournir directement à l'appel de E-transactions l'information du moyen de paiement choisi. Ceci se fait par l'intermédiaire des variables PBX_TYPEPAIEMENT et PBX_TYPECARTE.

Ainsi, le client sera redirigé directement sur la page de paiement adaptée au moyen de paiement choisi, et ne verra donc pas la page de présélection du moyen de paiement E-transactions.

Exemple : Pour un paiement avec une carte CB classique, il faut valoriser PBX_TYPEPAIEMENT à « CARTE » et PBX_TYPECARTE à « CB ».

L'ensemble des valeurs possibles pour ces variables est disponible dans le ***§11***

Dictionnaire de données.

ATTENTION : Les 2 variables PBX_TYPEPAIEMENT et PBX_TYPECARTE doivent obligatoirement fonctionner conjointement et l'utilisation de l'une sans l'autre, ou bien une valorisation non conforme à ce qui est indiqué dans ce manuel technique, peut amener des risques d'erreurs d'accès à la page de paiement ou des comportements non attendus, lors de la phase de paiement.

3.3 Authentification du message par empreinte

Afin de sécuriser le paiement, c'est-à-dire assurer que c'est bien le commerçant qui en est à l'origine et que personne de malveillant n'a modifié une variable (le montant par exemple), le Crédit Agricole a choisi d'établir une authentification par empreinte HMAC.

- Etape 0 : Si ce n'est déjà fait, le commerçant doit générer et installer une clé secrète via l'accès Back-Office Vision. La procédure est décrite dans le paragraphe ***§7.2 Gestion de la clé d'authentification***.

- Etape 1 : il faut ensuite constituer le message à destination du serveur E-transactions, en concaténant l'ensemble des variables séparées par le symbole &. Pour l'exemple donné ci-avant, la chaine constituée sera la suivante :

> PBX_SITE=1999887&PBX_RANG=32&PBX_IDENTIFIANT=2&PBX_TOTAL=1000&PBX_DEVISE=978&PBX_CMD=TEST
> ca-cp&PBX_PORTEUR=test@gmail.com&PBX_RETOUR= Mt:M;Ref:R;Auto:A;Erreur:E
> &PBX_HASH=SHA512&PBX_TIME=2011-02-28T11:01:50+01:00

- Etape 2 : il faut procéder au calcul de l'empreinte HMAC, en utilisant :

    - La chaine qui vient d'être construite
    - La clé secrète obtenue via le Back Office
    - Un algorithme au choix précisé par la variable PBX_HASH (cf. PBX_HASH dans

- ***Dictionnaire de*** données)

- Etape 3 : le résultat obtenu (l'empreinte) doit alors être placé dans le champ PBX_HMAC de la requête.

- L'ordre dans la chaine à « hasher » doit être strictement identique à l'ordre des variables dans le formulaire.
- Dans la chaine à « hasher », il faut utiliser les données « brutes », c'est-à-dire ne pas utiliser les fonctions d'URL encodée.

Voici un exemple de code PHP permettant de calculer l'empreinte du message :

```
< ?php
// On récupère la date au format ISO-8601
$dateTime = date("c");
// On crée la chaîne à hacher sans URLencodage
$msg = "PBX_SITE=1999887".
"&PBX_RANG=32".
"&PBX_IDENTIFIANT=2".
"&PBX_TOTAL=".$_POST['montant'].
"&PBX_DEVISE=978".
"&PBX_CMD=".$_POST['ref'].
"&PBX_PORTEUR=".$_POST['email'].
"&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E".
"&PBX_HASH=SHA512".
"&PBX_TIME=".$dateTime;


// On récupère la clé secrète HMAC (stockée dans une base de données cryptée) et que l'on renseigne
dans la variable $keyTest;

// Si la clé est en ASCII, On la transforme en binaire
$binKey = pack("H*", $keyTest);

// On calcule l'empreinte (à renseigner dans le paramètre PBX_HMAC) grâce à la fonction hash_hmac et
// la clé binaire
// On envoie via la variable PBX_HASH l'algorithme de hachage qui a été utilisé (SHA512 dans ce cas)
// Pour afficher la liste des algorithmes disponibles sur votre environnement, décommentez la ligne
// suivante
// print_r(hash_algos());

$hmac = strtoupper(hash_hmac('sha512', $msg, $binKey));
// La chaîne sera envoyée en majuscules, d'où l'utilisation de strtoupper()

// On crée le formulaire à envoyer à e-transactions
// ATTENTION : l'ordre des champs est extrêmement important, il doit
// correspondre exactement à l'ordre des champs dans la chaîne hachée
?>
<form method="POST" action="https://urlserveur.e-transactions.fr/cgi/MYchoix_pagepaiement.cgi">
<input type="hidden" name="PBX_SITE" value="1999887">
<input type="hidden" name="PBX_RANG" value="32">
<input type="hidden" name="PBX_IDENTIFIANT" value="2">
<input type="hidden" name="PBX_TOTAL" value="<? echo $_POST['montant']; ?>">
<input type="hidden" name="PBX_DEVISE" value="978">
<input type="hidden" name="PBX_CMD" value="<? echo $_POST['ref']; ?>">
<input type="hidden" name="PBX_PORTEUR" value="<? echo $_POST['email']; ?>">
<input type="hidden" name="PBX_RETOUR" value="Mt:M;Ref:R;Auto:A;Erreur:E">
<input type="hidden" name="PBX_HASH" value="SHA512">
<input type="hidden" name="PBX_TIME" value="<? echo $dateTime; ?>">
<input type="hidden" name="PBX_HMAC" value="<? echo $hmac; ?>">
<input type="submit" value="Envoyer">
</form>
```

Si vous utilisez déjà l'ancienne méthode de communication avec E-transactions (par module CGI sur le serveur marchand), le premier appel HMAC bloquera les paiements par l'ancienne méthode.

3.4 URL appelée

La liste des URL des serveurs E-transactions est détaillée dans le tableau ***§10.6 URL d'appel***.

Un mécanisme de Global Load Balancer (GLB) permet de garantir une haute disponibilité des services E-transactions qui sont opérés par 2 serveurs redondés. Ce mécanisme évite aux développeurs de gérer la bascule entre les différents sites et unifie l'URL appelée.

4. GESTION DE LA REPONSE

Une fois le paiement réalisé sur la page de paiement E-transactions, le client sera redirigé sur le site commerçant par l'intermédiaire de 4 URL qui permette d'adapter les traitements au résultat du paiement.

Le commerçant pourra gérer de façon automatique la validation de ses bons de commandes suivant le résultat de la transaction par l'intermédiaire d'une 5ème URL nommée IPN (Instant Payment Notification).

4.1 Redirection du client

Le retour de E-transactions vers le site marchand peut se faire sur 4 adresses (URL) différentes le résultat du paiement : accepté, refusé, annulé ou en attente. Ces 4 adresses peuvent se définir de 2 manières :

- Soit en les définissant pour chaque transaction,
    - Cela permet d'afficher une page personnalisée pour chaque client.
    - Il faut alors les définir à chaque transaction en utilisant les variables PBX_EFFECTUE, PBX_REFUSE, PBX_ANNULE, PBX_ATTENTE.
- Soit en utilisant les valeurs par défaut enregistrées dans la base de données E-transactions
    - Ces valeurs doivent être données lors de l'inscription à E-transactions. Il est également possible de les modifier via l'accès Back Office Vision, onglet « Paramétrage ».

Le client sera dirigé sur une de ces pages après avoir cliqué sur le bouton « retour boutique » de la page récapitulative du paiement (phase d'affichage du ticket de paiement), ou de la page indiquant que la transaction n'a pas été autorisée.

Il est également possible de choisir un retour immédiat : il faut préciser cette option dans la fiche d'inscription ou auprès de l'assistance E-transactions. Dans ce cas-là, le ticket récapitulatif n'est pas affiché et le client est redirigé directement vers le site du commerçant.

L'utilisation des 4 URL est dépendante du comportement du client final. PBX_EFFECTUE n'est pas suffisante. Il est préférable d'utiliser la 5ème URL IPN pour valider les bons de commandes du site : voir chapitre ***§4.3 Validation des bons de commande***

En cas de présence dans l'URL à appeler de caractères HTML spéciaux, il faut utiliser les « URL Encoder », c'est-à-dire les convertir en un code spécial compatible avec l'encodage d'une URL.
Par exemple, si l'URL « PBX_EFFECTUE » contient le caractère « ; », il faut remplacer ce caractère par « %3B » :
`www.commerce.fr/effectue.jsp;id_session=134ERF47`
Il faudra donc documenter la variable « PBX_EFFECTUE » de la manière suivante :
`www.commerce.fr/effectue.jsp%3Bid_session=134ERF47`

Cette particularité est due à la gestion de la balise META HTTP-EQUIV pour Internet Explorer.

En Annexe se trouve une liste des caractères spéciaux les plus fréquents et leur valeur convertie « URL Encodée ».

4.2 Gestion des paiements en attente de validation

Certains moyens de paiement (exemples : Kwixo, Paypal, Oney-Facilipay, iDeal) peuvent nécessiter un délai de quelques heures à quelques jours avant de confirmer le paiement.

Pour vous informer de la situation, E-transactions vous envoie une première réponse dès la fin du paiement par le client, avec le code réponse 99999 sur l'URL PBX_ATTENTE et via l'IPN.

E-transactions se charge ensuite de mettre à jour la réponse, et quand une décision a été prise, E-transactions vous rappelle via l'IPN avec la réponse définitive (ex : 00000 si la transaction est autorisée).

Pour plus d'informations sur ces moyens de paiement, vous pouvez vous référer aux documents :

- ***[Ref 7] Note Paypal***

4.3 Validation des bons de commande

4.3.1 Principe du IPN (Instant Payment Notification)

Cette variable IPN est spécialement utilisée pour gérer de façon automatique la validation des bons de commandes.

Cette variable est une URL enregistrée dans la base de données E-transactions mais elle peut également être gérée dynamiquement comme les 4 URL précédentes via la variable « PBX_REPONDRE_A ».

L'avantage de cette URL est qu'elle est appelée de serveur à serveur dès que le client valide son paiement (que ce dernier soit autorisé ou refusé).

Cela permet ainsi de valider automatiquement le bon de commande correspondant même si le client coupe la connexion ou décide de ne pas revenir sur la boutique, car cet appel ne transite pas par le navigateur du porteur.

Lors de l'appel de cette URL, un script présent sur le serveur Marchand à l'emplacement spécifié par l'URL, va s'exécuter. Il n'y a pas de contrainte sur le langage de ce script (ASP, PHP, PERL, …). La seule limitation est que ce script ne doit pas faire de redirection et doit générer une page HTML vide.

L'URL précisée dans le paramètre IPN est appelée à chaque tentative de paiement, quel que soit le nombre de tentatives effectuées par le porteur.

Cette URL n'a aucun lien direct avec les trois autres : elle est gérée de façon complètement indépendante et peut être appelée sur les ports TCP 80, 443 (HTTPS), 8080, 8081, 8082, 8083, 8084 ou 8085.

4.3.2 Paramètres

Il est possible de configurer la liste des variables qui sont renvoyées au site Marchand dans les différentes URL de retour. Cette configuration est effectuée par la variable PBX_RETOUR, qui se configure en concaténant la liste des informations souhaitées sous le format suivant :

```
<nom de la variable que vous souhaitez>:<lettre e-transactions correspondante>;
```

Exemple :

```
ref:R;trans:T;auto:A;tarif:M;abonnement:B;pays:Y;erreur:E
```

Le nom des variables (montant, maref,…) est personnalisable. Pour voir l'ensemble des données disponibles, voir le paramètre ***PBX_RETOUR* en §9.1.7**.

Ces informations seront envoyées à toutes les URL de retour (PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE et PBX_REPONDRE_A). Par exemple, pour l'URL IPN, avec la valeur citée ci-dessus, la page appelée serait :

```
http://www.commerce.fr/cgi/verif_pmt.asp?ref=abc12&trans=71256&auto=30258&tarif=2000&abonnement=354341&pays=FRA&erreur=00000
```

Cet appel est par défaut effectué via la méthode « GET ». Si la méthode « POST » est préférée pour le transfert des paramètres, il faut l'indiquer dans la variable PBX_RUF1 en mettant la valeur POST.

4.3.3 Gestion des erreurs

Si une erreur se produit lors de l'appel de l'URL IPN, un mail d'avertissement sera envoyé sur la même adresse que celle utilisée pour les tickets de paiements. Par exemple, si l'URL d'appel est :

```
http://www.commerce.fr/cgi/verif_pmt.asp?ref=abc12&trans=71256&auto=30258&tarif=2000&abonnement=354341&pays=FRA&erreur=00000
```

Le message d'erreur reçu sera le suivant :

> Objet : WARNING!!
> Corps du message :
> WARNING: Impossible de joindre http://www.commerce.fr pour le paiement ref=abc12&trans=71256&auto=30258&tarif=2000&abonnement=354341&pays=FRA&erreur=00000 **(XXX-YYY)**

A la fin de ce message sont précisées entre parenthèses **(XXX-YYY)** des informations permettant de comprendre la cause de l'erreur :

- Le premier nombre **XXX** correspond au code retour du protocole HTTP
  - Voir la liste des codes retour HTTP en ***§10.2 Codes retour HTTP***
  - Seuls les codes retour commençant par un 2 ,sont considérés comme valides.
- Le second **YYY** est un complément d'information correspondant au code retour de la librairie "libcurl" assurant les échanges avec le serveur WEB Marchand.
  - Voir la liste des codes retour CURL en ***§10.3 Codes erreur CURL***

4.3.4 Vérification des valeurs

L'IPN est appelée quel que soit le résultat du paiement (accepté ou refusé).

Comme tous les messages et signatures transportés au moyen du protocole HTTP (GET ou POST), l'URL de l'IPN est encodée. Il faut donc la décoder pour l'exploiter.

Pour connaître le résultat du paiement, il est indispensable de vérifier le contenu des variables suivantes :

- Code erreur (E) :
  - Pour une transaction valide, il doit être à « 00000 »
  - Pour les autres valeurs, se reporter au ***§ 9.1.7 Tableau 2 : Codes réponse PBX_RETOUR***
  - Dans le cas d'un paiement refusé par le centre d'autorisation (code erreur à 001xx), les « xx » représentent le code renvoyé par le centre. Ce code permet de connaître la raison exacte du rejet de la transaction.
    Par exemple, pour une transaction refusée pour raison « provision insuffisante », le code erreur renvoyé sera 00151.
    Tous les codes sont précisés en ***§10.1 Codes réponses du centre d'autorisation***.
- Numéro d'autorisation (A) : alphanumérique, longueur variable.
  - Pour une transaction de test (pas de demande d'autorisation vers le serveur du Crédit Agricole ou l'établissement financier privatif), la variable vaut toujours « XXXXXX »
  - Pour une transaction refusée, la variable n'est pas envoyée

Pour s'assurer que la réponse provient bien de notre plateforme de paiements, **il est impératif** de vérifier le contenu des variables suivantes :

- Adresse IP d'origine
  - Pour améliorer la sécurité, il est possible de vérifier que l'appel de l' URL IPN provient bien d'un de nos serveurs (voir ***§***10.6 ***URL d'appel et Adresses IP***).
- Signature (K)
  Il vous faudra alors vérifier impérativement la signature électronique afin de s'assurer que :
    - les données renvoyées n'ont pas été altérées,
    - c'est bien E-transactions qui effectue un appel des URL du site.

Il est important de noter que la donnée K de la variable « PBX_RETOUR » doit toujours être située en dernière position. Par exemple :

- PBX_RETOUR=montant:M;auto:A;idtrans:S;sign:K est correcte
- PBX_RETOUR=montant:M;auto:A;sign:K;idtrans:S est incorrecte

La clé publique de E-transactions est en libre téléchargement depuis https://e-transactions.aveo-groupe.com à la rubrique « Téléchargements ». Pour être en conformité avec les règles de sécurité, le Crédit Agricole est susceptible de changer sa paire de clé publique/privée : il doit donc être possible de mettre en place différentes clés publiques au niveau des serveurs Marchand.

NB : K est la signature

- **Signature**

La signature est produite en chiffrant un condensé SHA-1 avec une clé privée RSA. La taille d'une empreinte SHA-1 étant de 160 bits et la clé E-transactions faisant 1024 bits de long, la signature est toujours une valeur binaire de taille [fixe] 128 octets (172 octets en Base64).

- **Vérification de la signature**

De par sa nature, la signature peut se vérifier directement dans les langages les plus répandus sur le web.
Par exemple en PHP, il suffit d'utiliser la fonction 'openssl_verify()' et en Java, la methode verify() en précisant "SHA1withRSA".

Il est également possible d'utiliser d'autres langages, packages, composants ou utilitaires, qui peuvent demander de prendre en charge les opérations intermédiaires (condensé ou chiffrement). Dans tous les cas, il faut utiliser la clé publique E-transactions, disponible en téléchargement.

- **Tests**

La manière la plus souple de tester un programme de vérification de signature dans votre environnement, est d'utiliser une paire de clé RSA de test.
Vous serez ainsi en mesure de signer vous-même des messages dont vous pourrez vérifier la signature. Ensuite, il suffira de substituer la clé publique de test par la clé publique E-transactions.

Exemple avec OpenSSL (http://www.openssl.org/docs/apps/openssl.html) :

Pour générer une clé privée RSA *prvkey.pem* et en extraire la clé publique *pubkey.pem*

```
openssl genrsa -out prvkey.pem 1024
openssl rsa -in prvkey.pem -pubout -out pubkey.pem
```

Signature d'une donnée contenue dans le fichier *data.txt*

```
openssl dgst -sha1 -binary -sign prvkey.pem -out sig.bin data.txt
openssl base64 -in sig.bin -out sig64.txt
rm sig.bin
```

Vérification de la signature en utilisant la clé publique *pubkey.pem*

```
openssl base64 -d -in sig64.txt -out sig.bin
openssl dgst -sha1 -binary -verify pubkey.pem -signature sig.bin data.txt
```

- **Encodage :**

Les messages et signatures transportés au moyen du protocole HTTP (GET ou POST) doivent être sur-encodés (URL encodage et/ou Base64).
De ce fait il faut procéder aux opérations inverses avant de vérifier la signature :

1) détacher la signature du message,
2) URL décoder la signature,
3) décodage Base64 de la signature,
4) vérification de la signature [binaire] sur les données (toujours encodées)

Avec l'URL IPN de notification (paramètre : PBX_REPONDRE_A), la signature électronique s'effectue uniquement par rapport au contenu de la variable PBX_RETOUR contrairement aux quatre autres URLs

(paramètres : PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE et PBX_ATTENTE) où la signature est calculée sur l'ensemble des variables.

Données signées :

a) lors de la réponse de serveur à serveur (URL IPN), seules les informations demandées dans la variable PBX_RETOUR sont signées,
b) dans les 4 autres cas (redirection via le navigateur du client, PBX_EFFECTUE, PBX_REFUSE et PBX_ANNULE, PBX_ATTENTE), ce sont toutes les données suivant le ' ? ' (les paramètres URL).

```
ex.:  http://  www.moncommerce.com  /mondir/moncgi.php  ?  monparam=mavaleur&
pbxparam1=val1&pbxparam2=val2    ...    &sign=df123dsfd3...1f1ffsre%20t321rt1t3e=
```

La signature (df123dsfd3...1f1ffsre%20t321rt1t3e=) porte sur la partie :
cas a) pbxparam1=val1&pbxparam2=val2 ...
cas b) monparam=mavaleur& pbxparam1=val1&pbxparam2=val2 ...

Rappel : si la signature n'est pas la dernière valeur demandée dans la liste PBX_RETOUR, les valeurs suivantes seront retournées, mais pas signées.

- **Signature non vérifiée :**

Si une signature ne peut être vérifiée, alors les cas suivants doivent être envisagés :

- erreur technique : bogue, environnement cryptographique mal initialisé ou mal configuré, ...
- utilisation d'une clé erronée
- données altérées ou signature contrefaite.

Le dernier cas est peu probable, mais grave. Il doit conduire à la recherche d'une intrusion dans les systèmes d'informations impliqués.

5. FONCTIONNALITES AVANCEES

Au-delà de la fonction élémentaire de paiement, E-transactions propose un certain nombre de fonctionnalités additionnelles permettant au commerçant de piloter plus souplement ses opérations et d'offrir aux clients finaux, des services à valeur ajoutée intéressants.

Certaines de ces fonctionnalités sont décrites ci-dessous.

Pour obtenir une liste exhaustive et une description des fonctionnalités disponibles, contacter le support E-transactions (voir ***§8 Environnement de Test***).

		CANAL DE PAIEMENT				MODALITES DE PAIEMENT							OPERATIONS		
		Internet	Mobile	Mail	Téléphone	Immediat	Différé Simple	Différé Avancé	Plusieurs Fois	Abonnemt Simple	Abonnemt Avancé	Express 1 clic	Capture	Annulation	Remboursement
Cartes bancaires	CB, VISA, MASTERCARD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	E-CARTE BLEUE	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗
	MAESTRO, ELECTRON	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✓
Cartes privatives	AMERICAN EXPRESS	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
	DINERS	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
	JCB	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Portefeuilles électroniques	PAYPAL	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓
	PAYLIB	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓	✓
	MASTERPASS	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
Cartes de Crédit	COFINOGA	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
	CETELEM AURORE	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓
	ONEY BANQUE ACCORD	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓
Dossier Crédit	FACILIPAY (3,4 X ONEY)	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓
	1EURO.COM	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Cartes prépayées	PAYSAFECARD	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Virements/ prélèvement	IDEAL	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
	PAYBUTTON														
Autres	LEETCHI	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
	ILLICADO														
	MAXICHEQUE														

5.1 Intégration avec Gestion Automatisée des Encaissements

5.1.1 Principe

En utilisant conjointement E-transactions et Gestion Automatisée des Encaissements, il est possible d'accéder à des fonctions supplémentaires, comme entre autres :

- Paiement en 1 clic,
- Capture de la transaction en différé,
- Autorisation seule
- Autorisation + débit
- Débit (sur une autorisation pré effectuée)
- Crédit
- Annulation (d'une opération pré effectuée)
- ….

Lors du paiement par E-transactions, le contexte carte sera sauvegardé (création d'un abonné), et à partir d'un identifiant lié à cet abonné et retourné par E-transactions, le commerçant fera référence à cet abonné pour initier ultérieurement d'autres paiements sur la même carte via Gestion Automatisée des Encaissements, sans avoir à ressaisir ces données Carte.

5.1.2 Utilisation

5.1.2.1 APPEL E-TRANSACTIONS

Lors de l'appel E-transactions, il faut nécessairement utiliser les variables PBX_RETOUR et PBX_CMD et/ou PBX_REFABONNE.

- L'une des variables PBX_CMD ou PBX_REFABONNE doit contenir l'identifiant du contexte de la carte (ou abonné).
  - Si la variable PBX_REFABONNE est présente, c'est elle qui sera utilisée pour définir l'identifiant de l'abonné (et la carte associée), sinon ce sera PBX_CMD
  - Le choix de cet identifiant est laissé à la discrétion du commerçant
  - Il doit être unique pour un contrat commerçant (PBX_SITE).
- La variable PBX_RETOUR doit obligatoirement contenir au moins la variable « U »
  - Lors du retour, une chaine à conserver est retournée dans ce paramètre « U »
  - Cette chaine est au format suivant, les 3 champs étant séparés par '++' :

    `Handle_Numéro_De_Carte_Crypté++Date_De_Validité_De_La_Carte++---`

5.1.2.2 UTILISATION DANS GESTION AUTOMATISEE DES ENCAISSEMENTS

Pour faire référence à un abonné créé précédemment via E-transactions, 2 variables seront à utiliser dans Gestion Automatisée des Encaissements:

- La variable REFABONNE devra contenir la référence à l'abonné
  - C'est la valeur utilisée lors de l'appel E-transactions dans la variable PBX_REFABONNE si elle était présente, ou PBX_CMD sinon
- PORTEUR devra contenir le Handle de numéro de carte retourné par E-transactions dans la variable de retour U. Ce Handle a été retourné « URL encodé », il doit être à l'inverse « URL décodé » avant d'être utilisé dans Gestion Automatisée des Encaissements.
  - Ce numéro est incomplet pour des raisons de sécurité.

5.1.2.3 VOIR AUSSI

- ***[Ref 1]*** ***Manuel d'intégration Gestion Automatisée des Encaissements*** pour plus d'informations sur le fonctionnement général de cette application
- **§9**

- **Dictionnaire de** données, pour des informations sur les variables PBX_CMD, PBX_REFABONNE, PBX_RETOUR
- ***§***4 ***Gestion de la réponse***, pour l'utilisation de PBX_RETOUR

5.2 Autorisation sans capture

5.2.1 Principe

Cette option permet d'effectuer une demande d'autorisation vers le serveur de la banque ou de l'établissement financier privatif mais la transaction ne sera jamais confirmée et le porteur ne sera jamais débité si le commerçant n'adresse pas un 2ème message de confirmation à E-transactions.

Cette option peut être utilisée pour les scenarii suivants :

- Débit après processus de validation (total ou partiel),
- Débit au départ colis (total ou partiel),
- Débit à la prise d'effet d'un contrat (total ou partiel),
- Autorisation simple pour vérifier la qualité de la carte transmise

5.2.2 Utilisation

En positionnant le paramètre PBX_AUTOSEULE à 'O', seule l'autorisation sera réalisée et pas la télécollecte.
Si PBX_AUTOSEULE est à 'N' ou si la variable n'est pas présente, la transaction sera marquée pour être télécollectée le soir.

Néanmoins, même si la transaction est réalisée en mode PBX_AUTOSEULE='O', la transaction est bien enregistrée et elle peut être capturée (télécollectée) ultérieurement via les solutions Traitement par Lots ou Gestion Automatisée des Encaissements, dans un délai de 75 jours maximum.

- Pour les paiements par carte, le Crédit Agricole préconise au commerçant de ne pas dépasser 6 jours entre la date de la demande d'autorisation et la date de remise en banque (capture). Au-delà, le commerçant peut avoir à gérer des impayés pour encaissement tardif.

- Pour les paiements Paypal, la capture peut se faire dans les 29 jours. Cependant, Paypal ne garantit les fonds que durant les 4 premiers jours.

5.3 Paiement différé

5.3.1 Principe

E-transactions peut gérer les paiements différés, c'est à dire garder les transactions un certain nombre de jours avant de les envoyer vers le centre de télécollecte de la banque ou de l'établissement financier privatif pour débiter l'acheteur et créditer le commerçant.

Cette option peut s'avérer très utile, lorsque le commerçant désire s'assurer que la marchandise ou le service a été livré au client avant que ce dernier ne soit débité.

Sur la fiche d'inscription E-transactions, il est demandé de préciser le nombre de jours de différé souhaité par défaut :

- 1 : le paiement sera envoyé en banque le lendemain de l'achat par le porteur,
- 2 : le paiement sera envoyé en banque le surlendemain de l'achat par le porteur,
- etc…

- Pour les paiements par carte, le Crédit Agricole préconise au commerçant de ne pas dépasser 6 jours entre la date de la demande d'autorisation et la date effective de remise en banque. Au-delà, le commerçant peut avoir à gérer des impayés pour encaissement tardif.

5.3.2 Utilisation

Il suffit de préciser dans la variable PBX_DIFF le nombre de jours de décalage souhaité entre l'achat et la télécollecte. Ce nombre de jours de décalage peut être fixé à une valeur par défaut à l'ouverture du contrat.

5.4 Paiement sur mobile

5.4.1 Principe

Le fonctionnement est identique à un site Web classique sur Internet. Les pages Web affichées sur le mobile ou le smartphone sont soit des pages XHTML dédiées soit des pages gérées par une application chargée sur le smartphone. Au moment du paiement, le mobile se connecte sur notre plateforme qui traite ensuite la transaction normalement.
Aujourd'hui, les moyens de paiement utilisables sur mobile sont : CB, VISA, MASTERCARD, AMEX, PAYPAL.

5.4.2 Utilisation

Il faut renseigner dans la requête le paramètre PBX_SOURCE avec la valeur XHTML.

ATTENTION : les URL d'accès aux services E-transactions pour le paiement sur mobile sont spécifiques (voir ***§ 10.***66 ***URL d'appel et Adresses IP***).

6. OPTION GESTION DES ABONNEMENTS

Les fonctions décrites dans ce paragraphe nécessitent l'activation de l'option Gestion des abonnements.

Pour souscrire à cette option, rapprochez-vous de votre chargé de clientèle.

6.1 Principe

La gestion des paiements par abonnement permet au commerçant de gérer des prélèvements périodiques ou des paiements en plusieurs fois pour ses clients. Ainsi, une fois le paiement initial effectué, le client sera prélevé de façon cyclique suivant une fréquence choisie préalablement, par le commerçant.

- La gestion de l'abonnement sur E-transactions est une gestion de base : elle ne prévoit que des cas simples d'abonnements, basés sur la reconduction périodique de paiement d'une même somme, sur une période souhaitée initialement par le commerçant. Ces paramètres ne peuvent pas, par la suite, être modifiés.
- Malgré sa simplicité, le système offre une souplesse de paramétrage permettant notamment, avec la gestion des différés, un large éventail de déclenchement de la première reconduction de l'abonnement.
- Il est à noter qu'en cas d'échec (refus d'autorisation) sur une échéance, **la plateforme de paiement n'assure pas de représentation et stoppe les futures échéances.** (La solution Gestion Automatisée des Encaissements apporte plus de souplesse sur ce sujet).
- Le commerçant peut suivre ses abonnements via son accès au Back Office Vision E-transactions

Pour gérer cette option il faudra modifier le contenu de la variable PBX_CMD comme expliqué ci-dessous.

6.2 Création d'un abonnement

La gestion de l'abonnement s'effectue via différentes « sous-variables » devant être insérées à la fin de la référence commande commerçant précisée dans la variable « PBX_CMD ».
La taille des variables doit être respectée et le nom de celles-ci est fixe et en majuscule.

NOM VARIABLE	DESCRIPTION	TAILLE
PBX_2MONT	Montant des prochains prélèvements en centimes (0 = montant identique au paiement initial précisé dans PBX_TOTAL).	10 chiffres
PBX_NBPAIE	Nombre de prélèvements (0 = toujours).	2 chiffres
PBX_FREQ	Fréquence des prélèvements en mois.	2 chiffres
PBX_QUAND	Jour du mois auquel le prélèvement sera effectué (0 = le même jour que le paiement initial).	2 chiffres
PBX_DELAIS	Nombre de jours d'attente avant le déclenchement du début de l'abonnement.	3 chiffres

Les autres informations pour le paiement via le produit « E-transactions » ne changent pas. La devise

est passée par la variable PBX_DEVISE et le montant du premier règlement (qui peut être différent des prélèvements de l'abonnement) est passé dans la variable PBX_TOTAL.

Exemples d'abonnement :

Exemple 1 :

```
PBX_SITE=1999887&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1500&PBX_DEVISE=978&PBX
_CMD=ma_ref123PBX_2MONT0000000500PBX_NBPAIE00PBX_FREQ01PBX_QUAND28PBX_DELAIS005&
PBX_PORTEUR=test@gmail.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512
&PBX_TIME=2011-02-28T11:01:50+01:00
```

Si le paiement initial (15 euros, soit 1500 centimes) est effectué le 28 novembre par exemple, le premier prélèvement aura lieu le 03 décembre (car la prise en compte de l'abonnement se fait 5 jours plus tard via PBX_DELAIS).
Tous les prélèvements sont d'un montant de 5 euros (soit 500 centimes) (PBX_2MONT), réalisés le 28 (PBX_QUAND) de tous les mois (PBX_FREQ) jusqu'à une demande de résiliation (PBX_NBPAIE) de votre part ou un rejet du centre d'autorisation (si la carte bancaire est arrivée à expiration).

Exemple 2 :

```
PBX_SITE=1999887&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1500&PBX_DEVISE=978&PBX
_CMD=ma_ref123PBX_2MONT0000000550PBX_NBPAIE10PBX_FREQ03PBX_QUAND31&PBX_PORTEUR=t
est@gmail.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=201
1-02-28T11:01:50+01:00
```

Si le paiement initial (15 euros) est effectué le 28 novembre par exemple, le premier prélèvement aura lieu le 31 novembre (car la prise en compte de l'abonnement est immédiate via PBX_DELAIS qui est inexistante).
10 prélèvements (PBX_NBPAIE) d'un montant de 5,50 euros (PBX_2MONT) seront réalisés tous les 3 mois (PBX_FREQ) le dernier jour du mois (PBX_QUAND).

Lorsqu'un abonnement est créé, un mail « ticket de paiement » est envoyé au commerçant et au client avec une mention précisant le montant et la date de prochain règlement.

Mention précisée sur le mail envoyé au client :
Prochain prélèvement le xx/xx/xxxx d'un montant de xx.xx Eur
Pour toute réclamation adressez-vous à votre commerçant

Mention précisée sur le mail envoyé au commerçant :
Prochain prélèvement le xx/xx/xxxx d'un montant de xx.xx Eur
Pour toute résiliation de cet abonnement veuillez rappeler la référence xxxxxxx.

Attention :
- En cas d'utilisation de l'URL IPN, cette dernière sera également appelée aussi bien en cas de reconduction réussie, qu'échouée. La variable ETAT_PBX sera ajoutée à l'URL d'appel avec comme information PBX_RECONDUCTION_ABT.

Par exemple :
http://www.commerce.fr/traite.php?ETAT_PBX=PBX_RECONDUCTION_ABT&Mt=1200&Trans=12345678&Ref=MaReference&Autorisation=987654&NumAbonnement=56789"

6.3 Paiement en plusieurs fois (4 fois maximum)

Le paiement en plusieurs fois répond à un besoin légèrement différent de l'abonnement. Alors que l'abonnement est basé sur des montants fixes à échéances régulières, l'interface de paiement en plusieurs fois permet de configurer chaque échéance librement, en termes de montants et de dates, dans la limite de 3 paiements en plus du paiement initial (maximum 90 jours)

Pour mettre en œuvre ce paiement, il faut utiliser les groupes de variables PBX_2MONTx et PBX_DATEx (x variant de 1 à 3).

Exemple :

```
PBX_SITE=1999887&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1000&PBX_DEVISE=978&PBX_CMD=TESTcacp&PBX
_PORTEUR=test@gmail.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=2011-02-
28T11:01:50+01:00&PBX_2MONT1=2000&PBX_DATE1=01/02/2013&PBX_2MONT2=3000&PBX_DATE2=15/02/2013
```

Dans cet exemple, la somme de 10€ sera débitée immédiatement, puis la somme de 20€ sera débitée le 1er février, et enfin, 30€ seront débités de 15 février.

Comme pour les abonnements, l'échéancier est conservé par notre plateforme, et une fois le premier paiement terminé, le commerçant n'a plus à gérer de nouveaux appels vers la plateforme pour déclencher les paiements suivants.

6.4 Fin des abonnements

L'abonnement peut se terminer de 3 façons différentes :

- Fin normale
  Lorsque toutes les échéances d'un abonnement ont été traitées avec succès, l'abonnement se termine de lui-même.
- Fin en échec
  Lorsque l'une des échéances échoue, il n'y a pas de représentation de l'échéance ultérieurement. L'abonnement est clôturé et le commerçant est informé de ce résultat par un mail.
- Résiliation par le commerçant
  Le commerçant peut choisir à tout moment d'arrêter l'abonnement en cours. Pour cela, il peut se rendre sur le Back-Office, ou bien exécuter un appel à la plateforme pour l'arrêter. Les paramètres de cet appel sont décrits ci-après.
  Lorsque le commerçant résilie un abonnement, le client porteur en est informé par mail.

6.4.1 Résiliation par appel serveur-serveur

Pour intégrer la gestion des abonnements avec le système d'informations du commerçant, le Crédit Agricole met à disposition un utilitaire permettant de résilier l'abonnement sans intervention manuelle.

L'URL à appeler est disponible en annexe dans le tableau ***§10.***66 ***URL d'appel et Adresses IP***, section Résiliation des abonnements. L'appel peut être fait via la méthode GET ou POST et consiste en un assemblage de variables.

Il est possible d'identifier l'abonnement à résilier de 2 manières :

- Par numéro d'abonnement

  Ce numéro est transmis dans la réponse E-transactions
  Exemple :
  VERSION=001&TYPE=001&SITE=1999888&MACH=099&IDENTIFIANT=2&ABONNEMENT=1

- Par référence commande

  C'est la référence transmise lors de l'appel
  Exemple :
  VERSION=001&TYPE=001&SITE=1999887&MACH=099&IDENTIFIANT=2&REFERENCE=refcmd

En réponse, le serveur renvoie lui aussi une succession de variables. La variable ACQ permet de connaitre le bon déroulement ou non de la résiliation.
De plus, la référence transmise à l'appel est renvoyée dans la réponse (ABONNEMENT ou REFERENCE)

Exemples :
Réponse en cas de succès : ACQ=OK&IDENTIFIANT=2&ABONNEMENT=1
Réponse en cas d'échec de résiliation : ACQ=NO&ERREUR=9&IDENTIFIANT=2&REFERENCE=refcmd1

Il est à noter qu'il n'y a pas d'émission de la part de E-transactions d'un email vers le porteur lors de la résiliation d'un abonnement par le commerçant sauf lors d'une résiliation via le back office Vision.

7. LE BACK-OFFICE VISION

Dès que le commerçant a souscrit E-transactions, il se voit automatiquement attribuer un accès au Back Office Vision, portail en ligne, sécurisé, qui lui permet de consulter ses transactions et d'effectuer diverses opérations (exports, annulations/remboursements, gestion des télécollectes différées, …).

7.1 Accès et fonctionnalités

Les conditions d'accès à ce Back Office ainsi que l'ensemble des fonctionnalités disponibles (Journal, Export, Validation/Annulation/Remboursement de transactions, …) sont détaillées dans le document ***[Ref 3] Manuel Utilisateur du Back Office***

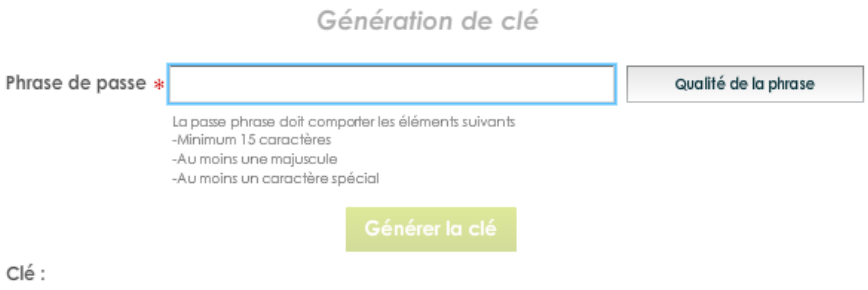
7.2 Gestion de la clé d'authentification HMAC

Cette clé est indispensable, elle permet d'authentifier tous les messages échangés entre le site Marchand et les serveurs E-transactions. Le commerçant doit donc générer sa propre clé unique et confidentielle et l'utiliser pour calculer une empreinte sur ses messages.

7.2.1 Génération

L'interface de génération de la clé secrète HMAC d'authentification se trouve dans l'onglet « Paramètres» du Back Office Vision, en bas de la page.

Voici à quoi ressemble cette interface :



Le champ « Phrase de passe » peut être renseigné avec une phrase, un mot de passe ou tout autre texte.

Le champ « Qualité de la phrase» est mis à jour automatiquement lorsque la « phrase de passe » est saisie. Ce champ permet de vérifier que les règles de sécurité d'acceptation minimales de la « phrase de passe » sont respectées (minimum 15 caractères, au moins une majuscule et au moins un caractère spécial et une force de 90 %). Le bouton « Générer la clé » restera grisé tant que ces limitations ne sont pas respectées.

La force de la « phrase de passe » est calculée selon plusieurs critères spécifiques : le nombre de majuscules, minuscules, caractères spéciaux, etc. Il conviendra donc de varier les caractères saisis, de les alterner et d'éviter les répétitions qui tendent à diminuer le score final.

Le bouton « Générer la clé » permet de calculer la clé HMAC à partir de la « phrase de passe » saisie. Ce calcul est une méthode standard assurant le caractère aléatoire de la clé et renforçant sa robustesse. Cette méthode de calcul étant fixe, il est possible à tout moment de retrouver sa clé en retapant la même phrase de passe et en relançant le calcul.

Attention, il est possible que le calcul de la clé prenne quelques secondes, selon le navigateur Internet utilisé et la puissance de l'ordinateur. Au cours du calcul, il se peut que le navigateur Internet Explorer demande s'il faut « arrêter l'exécution de ce script ». Il faut répondre « Non » à cette alerte, et patienter jusqu'à la fin du calcul.

Une fois le calcul terminé, la clé sera affichée dans le champ « Clé ». Il faut alors copier/coller la clé HMAC dans le champ « HMAC » de la configuration du module sur le site marchand.

S'il est également possible de saisir dans le champ « Clé » sa propre clé d'authentification (au format hexadécimal) qui aurait été calculée avec à un autre moyen que cette interface. La taille minimale de la clé à saisir est de 40 caractères hexadécimaux. Cependant, si cette méthode de saisie d'une clé d'authentification « externe » est utilisée, une alerte s'affichera pour rappeler que E-transactions ne peut ni contrôler ni garantir la robustesse de cette clé. Par conséquent nous vous déconseillons d'utiliser cette méthode.

Le bouton « Générer la clé » est grisé par défaut. Les 2 actions qui peuvent activer le bouton sont :

- Saisir une « phrase de passe » de plus de 15 caractères et dont la force est de plus de 90%
- Saisir une clé hexadécimale de plus de 40 caractères.

Après validation du formulaire, le marchand va recevoir un email de demande de confirmation de création de clé HMAC (avec lien de confirmation).

La clé qui vient d'être générée n'est active qu'une fois la procédure décrite dans l'email respectée.

La clé est affichée sous le bouton « Générer la clé ». Pour des raisons de sécurité, cette clé ne sera jamais transmise ni demandée par nos services. Par conséquent, si cette clé est égarée, il sera nécessaire d'en générer une nouvelle. **Il est important de veiller conserver de manière sécurisée la clé d'authentification affichée, avant de quitter la page.**

La clé est dépendante de l'environnement dans lequel elle est générée. Cela signifie qu'il faut générer une clé pour l'environnement de test **et** une pour l'environnement de production.

7.2.2 Validation

Une fois l'enregistrement de la nouvelle clé effectué, un email de demande de confirmation est envoyé au commerçant. Dans cet email se trouvera un lien pointant sur le programme "CBDValid.cgi", par exemple :

https://admin.e-transactions.fr/cgi/CBDValid.cgi?id=5475C869BB64B33F35D0A37DF466568475BC9601

Après avoir cliqué sur ce lien, si un message annonce « Clé Hmac confirmée », alors la clé est immédiatement en fonction. Ce qui signifie que la clé qui vient d'être validée doit impérativement être aussi en fonction sur le site Marchand.

7.2.3 Expiration

Lorsque la clé est validée, celle-ci est valable 1 an.

Passé ce délai, pour permettre au site marchand de continuer à fonctionner, la clé n'est pas désactivée. Cependant le commerçant est averti par email, et sur la page d'accueil du Back Office E-transactions de la nécessité de générer une nouvelle clé HMAC afin de garantir une sécurité optimale.

7.2.4 Transmission

La clé HMAC ne doit en aucun cas être transmise par e-mail. E-transactions ne la demandera jamais au commerçant. Les commerçants doivent donc être particulièrement vigilants quant aux demandes suspectes de transmission de la clé d'authentification, il s'agit probablement d'une tentative de phishing ou de social engineering.

En cas de perte de la clé secrète, E-transactions ne sera pas en mesure de la redonner. Il faudra en générer une nouvelle via le Back Office Vision.

8. ENVIRONNEMENT DE TEST

Avant de commencer à effectuer des paiements sur le site en production, Le Crédit Agricole recommande au Commerçant de vérifier l'intégration correcte des solutions E-transactions. Pour cela, le Crédit Agricole met à disposition des commerçants une plateforme de pré-production, ainsi que des comptes et des paramètres de tests, entièrement destinés à la réalisation de tests.

Toutes les informations relatives à cet environnement de tests sont précisées dans la documentation [Ref1] « **Paramètres Test E-transactions** » accessible en téléchargement ici : https://e-transactions.aveo-groupe.com

9. DICTIONNAIRE DE DONNEES

L'ensemble des variables E-transactions est résumée dans ce tableau. Le détail de chaque variable (format, contenu, exemples) est donné dans les pages qui suivent.

VARIABLE	RESUME	
PBX_1EURO_CODEEXTERNE	Données spécifique 1euro.com	C
PBX_1EURO_DATA	Données spécifique 1euro.com	C
PBX_2MONT*n*	Paiement en plusieurs fois : Montant des échéances	F
PBX_3DS	Désactivation 3-D Secure ponctuelle	F
PBX_ANNULE	URL de retour en cas d'abandon	F
PBX_ARCHIVAGE	Référence archivage	F
PBX_ATTENTE	URL de retour en cas de paiement en attente de validation	F
PBX_AUTOSEULE	Ne pas envoyer ce paiement à la banque immédiatement	F
PBX_CK_ONLY	Forçage d'un mode de paiement Carte Cadeau uniquement (non mixte)	F
PBX_CMD	Référence commande	**O**
PBX_CODEFAMILLE	Données spécifique Cofinoga	C
PBX_CURRENCYDISPLAY	Configuration des devises affichées	F
PBX_DATE*n*	Paiement en plusieurs fois : Dates des échéances	F
PBX_DEVISE	Devise (monnaie)	**O**
PBX_DIFF	Nombre de jours pour un paiement différé	F
PBX_DISPLAY	Timeout de la page de paiement	F
PBX_EFFECTUE	URL de retour en cas de succès	F
PBX_EMPREINTE	Empreinte fournie lors d'un premier paiement	F
PBX_ENTITE	Référence numérique d'une subdivision	F
PBX_ERRORCODETEST	Code erreur à renvoyer (pour tests)	F
PBX_HASH	Algorithme utilisé pour la signature du message	**O**
PBX_HMAC	Signature du message	**O**
PBX_IDABT	Numéro d'abonnement	F
PBX_IDENTIFIANT	Identifiant client	**O**
PBX_LANGUE	Langue de la page de paiement	F
PBX_ONEY_DATA	Données spécifique Oney	C
PBX_PAYPAL_DATA	Données spécifiques à Paypal	C
PBX_PORTEUR	Adresse mail du client	**O**

PBX_RANG	Numéro de rang fourni par la banque	**O**
PBX_REFABONNE	Référence de l'abonne (version GAE)	C
PBX_REFUSE	URL de retour en cas de refus du paiement	F
PBX_REPONDRE_A	URL IPN	F
PBX_RETOUR	Configuration de la réponse	**O**
PBX_RUF1	Méthode d'appel de l'URL IPN	F
PBX_SITE	Numéro de site fourni par la banque	O
PBX_SOURCE	Format de la page de paiement (pour paiement mobile)	F
PBX_TIME	Date et heure de la signature	**O**
PBX_TOTAL	Montant	**O**
PBX_TYPECARTE	Forçage du moyen de paiement	F
PBX_TYPEPAIEMENT	Forçage du moyen de paiement	F

Légende : O = Obligatoire ; F = Facultatif ; C = Conditionnel

9.1 Champs obligatoires pour E-transactions

9.1.1 PBX_SITE

Format : 7 chiffres. **Obligatoire.**

C'est le numéro de site (TPE) fourni par le Crédit Agricole.

Exemple : 1999888

9.1.2 PBX_RANG

Format : 2 chiffres. **Obligatoire.**

C'est le numéro de rang (ou « machine ») fourni par la banque du Commerçant.

Exemple : 01

9.1.3 PBX_TOTAL

Format E-transactions : 3 à 10 chiffres. **Obligatoire.**
Format Gestion automatisée: 10 chiffres. **Obligatoire.**

Montant total de la transaction en centimes (sans virgule ni point).

Exemple : pour 19€90 : 1990

9.1.4 PBX_DEVISE

Format : 3 chiffres. **Obligatoire.**

Code monnaie de la transaction suivant la norme ISO 4217 (code numérique)

Exemples :

- Euro : 978
- US Dollar : 840
- CFA : 952

Attention : La seule valeur autorisée est l'€ : 978

9.1.5 PBX_CMD

Format : 1 à 250 caractères. **Obligatoire.**

C'est la référence commande côté commerçant (champ libre). Ce champ permet au commerçant de garder un lien entre sa plate-forme de e-commerce et la plate-forme de paiement. Ce champ doit être unique à chaque appel.

Dans le cas de l'utilisation de la **G**estion **A**utomatisée des **E**ncaissements, la valeur contenue dans ce champ est utilisée comme référence d'abonné.

Exemple : CMD9542124-01A5G

9.1.6 PBX_PORTEUR

Format : 6 à 120 caractères. **Obligatoire.** Les caractères « @ » et « . » doivent être présents.

Adresse email de l'acheteur (porteur de carte).

Exemple : test@gmail.com

9.1.7 PBX_RETOUR

Format : <nom de variable>:<lettre>; **Obligatoire.**

Variables renvoyées par la plateforme E-transactions.

Voir aussi : *§*4 ***Gestion de la réponse***

Page suivante, la liste complète des variables disponibles

CODE	DESCRIPTION

M	**M**ontant de la transaction (précisé dans PBX_TOTAL).
R	**R**éférence commande (précisée dans PBX_CMD) : espace URL encodé
T	Numéro d'appel
A	numéro d'**A**utorisation (numéro remis par le centre d'autorisation) : URL encodé
B	numéro d'abonnement (numéro remis par la plateforme)
C	Type de **C**arte retenu (cf. PBX_TYPECARTE)
D	**D**ate de fin de validité de la carte du porteur. Format : AAMM
E	Code réponse de la transaction (cf. Tableau 2 : Codes réponse PBX_RETOUR)
F	Etat de l'authenti**f**ication du porteur vis-à-vis du programme 3-D Secure : • Y : Porteur authentifié • A : Authentification du porteur forcée par la banque de l'acheteur • U : L'authentification du porteur n'a pas pu s'effectuer • N : Porteur non authentifié
G	**G**arantie du paiement par le programme 3-D Secure. Format : O ou N
H	Empreinte de la carte
I	Code pays de l'adresse **I**P de l'internaute. Format : ISO 3166 (alphabétique)
J	2 derniers chiffres du numéro de carte du porteur
K	Signature sur les variables de l'URL. Format : url-encodé
N	6 premiers chiffres (« bi**n**6 ») du numéro de carte de l'acheteur
O	Enr**ô**lement du porteur au programme 3-D Secure : • Y : Porteur enrôlé • N : Porteur non enrôlé • U : Information non connue
O	*Spécifique Cetelem :* Option de paiement sélectionnée par le client : • 005 : Comptant • 001 : Crédit
P	Type de **P**aiement retenu (cf. PBX_TYPEPAIEMENT)
Q	Heure de traitement de la transaction. Format : HH:MM:SS (24h)
S	Numéro de Transaction
U	Gestion des abonnements avec le traitement **G**estion **A**utomatisée des **E**ncaissements Pour les paiements par carte : `Handle_Numéro_De_Carte_Crypté++Date_De_Validité_De_La_Carte++---` Ce champ est URL-encodé. Vous devez conserver la valeur. Pour les paiements avec Paypal : Ce champ contient l'identifiant de l'autorisation fourni par Paypal. Il ne vous sera pas nécessaire pour les paiements suivants.
W	Date de traitement de la transaction sur la plateforme. Format : JJMMAAAA

Y	Code pa**Y**s de la banque émettrice de la carte. Format : ISO 3166 (alphabétique)
Z	Index lors de l'utilisation des paiements mixtes (cartes cadeaux associées à un complément par carte CB/Visa/MasterCard/Amex)

Tableau 1 : Variables PBX_RETOUR

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue. Dans ce cas, il est souhaitable de faire une tentative sur le site secondaire : tpeweb1.e-transactions.fr
001xx	Paiement refusé par le centre d'autorisation [voir ***§10.1 Codes réponses du centre d'autorisation***]. En cas d'autorisation de la transaction par le centre d'autorisation de la banque ou de l'établissement financier privatif, le code erreur "00100" sera en fait remplacé directement par "00000".
00003	Erreur de la plateforme. Dans ce cas, il est souhaitable de faire une tentative sur le site secondaire FQDN tpeweb1. e-transactions.fr
00004	Numéro de porteur ou cryptogramme visuel invalide.
00006	Accès refusé ou site/rang/identifiant incorrect.
00008	Date de fin de validité incorrecte.
00009	Erreur de création d'un abonnement.
00010	Devise inconnue.
00011	Montant incorrect.
00015	Paiement déjà effectué.
00016	Abonné déjà existant (inscription nouvel abonné). Valeur 'U' de la variable PBX_RETOUR.
00021	Carte non autorisée.
00029	Carte non conforme. Code erreur renvoyé lors de la documentation de la variable « PBX_EMPREINTE ».
00030	Temps d'attente > 15 mn par l'internaute/acheteur au niveau de la page de paiements.
00031	Réservé
00032	Réservé
00033	Code pays de l'adresse IP du navigateur de l'acheteur non autorisé.
00040	Opération sans authentification 3-DSecure, bloquée par le filtre.
99999	Opération en attente de validation par l'émetteur du moyen de paiement.

Tableau 2 : Codes réponse PBX_RETOUR

Exemple : Mt:M;Ref:R;Auto:A;Appel:T;Abo:B;Reponse:E;Transaction:S;Pays:Y;Signature:K

9.1.8 PBX_IDENTIFIANT

Format : 1 à 9 chiffres. **Obligatoire.**

Identifiant fourni au moment de l'inscription du commerçant.

Exemple : 200814357

9.1.9 PBX_HASH

Format : Texte. **Obligatoire.**
Valeur par défaut : SHA512

Définit l'algorithme de hachage utilisé lors du calcul du HMAC.

Cet algorithme doit être choisi parmi la liste suivante :

- SHA512
- RIPEMD160
- SHA224
- SHA256
- SHA384
- MDC2

Les hachages en MD2/4/5 sont jugés trop faibles pour être utilisés et seront refusés (ça ne fonctionnera pas)

PBX_HASH doit préciser l'algorithme retenu et correspondre à l'une des valeurs de la liste ci-dessus, en respectant la forme (ou Casse) : majuscules, libellé.

Si la variable PBX_HASH est présente dans les trames sans que PBX_HASH soit précisé, l'algorithme de hachage sélectionné sera SHA512.

9.1.10 PBX_HMAC

Format : Texte (format hexadécimal). **Obligatoire.**

Permet l'authentification du commerçant et la vérification de l'intégrité du message. Il est calculé à partir de la liste des autres variables envoyées à E-transactions.

Voir aussi :

- ***§0***

- ***Authentification du*** message,
- ***§08***
- **Glossaire**

9.1.11 PBX_TIME

Format : Date au format ISO8601. **Obligatoire.**

Date à laquelle l'empreinte HMAC a été calculée. Doit être URL-encodée.

Exemple : 2015-01-28T01 :00 :00+01:00 correspond au 28 janvier 2015, à 1h du matin heure locale

9.1.12 PBX_ARCHIVAGE

Format : jusqu'à 12 caractères alphanumériques (hors caractères spéciaux)

Référence transmise au Crédit Agricole du commerçant au moment de la télécollecte. Elle devrait être unique et peut permettre au Crédit Agricole de fournir au commerçant une information en cas de litige sur un paiement. **C'est aussi un élément constitutif du rapprochement bancaire.**

9.2 Champs optionnels pour E-transactions

Les champs suivants sont triés par ordre alphabétique.

9.2.1 PBX_AUTOSEULE

Format : O ou N.
Valeur par défaut : N

Si la variable vaut « O », la transaction sera uniquement en mode autorisation, c'est-à-dire qu'elle ne sera pas envoyée à la banque du commerçant au moment de la télécollecte.

Cependant, elle sera quand même bien enregistrée, et il sera possible de la capturer ultérieurement en utilisant les produits **T**raitement par **L**ot ou **G**estion **A**utomatisée des **E**ncaissements.

9.2.2 PBX_ANNULE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans la fiche client du commerçant

Page de retour de la plateforme vers le site Marchand après paiement annulé.

Les variables définies dans PBX_RETOUR seront envoyées à cette page

Exemple : http://www.commerce.fr/annulation.html
Voir aussi : ***§***4 ***Gestion de la réponse***

Les URL doivent être encodées.

9.2.3 PBX_ATTENTE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans la fiche client du commerçant

Page de retour de la plateforme vers le site Marchand après paiement en attente de validation par l'émetteur.

Les variables définies dans PBX_RETOUR seront envoyées à cette page

Exemple : http://www.commerce.fr/attente.html
Voir aussi :

- ***§4 Gestion de la réponse***

Les URL doivent être encodées.

9.2.4 PBX_CURRENCYDISPLAY

Format : jusqu'à 23 caractères (6 x 3 codes séparés par des virgules)
Valeur par défaut : toutes les devises sont affichées

Liste des codes monnaie à afficher au niveau de la page de paiements.

Les codes disponibles sont les suivants :

- EUR : Euro
- CHF : Franc suisse
- USD : Dollar US
- JPY : Yen
- CNY : Yuan
- GBP : Livre Sterling
- CAD : Dollar canadien
- NO_CURR : valeur spéciale pour n'afficher aucune devise

Exemple : `EUR,USD,GBP`

9.2.5 PBX_DATEVALMAX

Format : Date au format AAMM

Date d'expiration à ne pas dépasser.

Si la date de fin de validité de la carte est inférieure à la limite fixée par cette variable, le paiement sera refusé. Ceci est utile dans le cas des paiements en plusieurs fois / abonnement et paiement en 1 clic, pour éviter qu'une reconduction échoue pour cause de date d'expiration de la carte dépassée.

Exemple :
Echéancier 04/05/2013, 08/06/2013 et 30/07/2013
PBX_DATEVALMAX=1307
Si la carte expire avant la fin juillet 2013, le paiement initial sera refusé avec le code erreur 00008.

9.2.6 PBX_DATE1, PBX_DATE2, PBX_DATE3

Format : Date au format JJ/MM/AAAA

Date de la seconde échéance d'un paiement fractionné (respectivement troisième et quatrième échéances pour PBX_DATE2 et PBX_DATE3).

Ces paramètres sont à utiliser obligatoirement en combinaison avec PBX_2MONT1, PBX_2MONT2, PBX_2MONT3.

Exemple : 30/06/2012
Voir aussi :

- ***§6.3 Paiement en plusieurs fois (4 fois maximum)***
- ***§***9.2.22

- ***PBX_2MONT1, PBX_2MONT2, PBX_***2MONT3

9.2.7 PBX_DIFF

Format : 2 chiffres

Nombre de jours de différé (entre la transaction et sa capture).

A noter qu'il est possible de supprimer cette mise en attente à partir du back office commerçant. Par exemple, une transaction réalisée le 2 novembre et différée jusqu'au 4 novembre, peut être débloquée et envoyée le 3 novembre par action manuelle.

Une valeur par défaut de ce paramètre peut avoir été définie à la signature du contrat. Si ce paramètre est envoyé dans l'appel, la valeur spécifiée dans l'appel est prioritaire sur celle par défaut.

Exemple : 04 pour gérer un différé de 4 jours
Voir aussi :

- ***§5.3 Paiement différé***,

9.2.8 PBX_DISPLAY

Format : 3 à 10 chiffres
Valeur par défaut : 900

TimeOut de la page de paiement (en secondes). Une fois cette période dépassée, la transaction estabandonnée.

Cette transaction ne sera pas remontée dans Vision

9.2.9 PBX_EFFECTUE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client

Page de retour de la plateforme vers votre site après paiement accepté.

Les variables définies dans PBX_RETOUR seront envoyées à cette page.

Exemple : http://www.commerce.fr/confirmation.html
Voir aussi : ***§***4 ***Gestion de la réponse***
Les URL doivent être encodées.

9.2.10 PBX_EMPREINTE

Format : 64 caractères

Empreinte fournie par la plateforme E-transactions au moment d'un premier paiement via la variable « H » de « PBX_RETOUR ».

9.2.11 PBX_ENTITE

Format : 1 à 9 chiffres

Référence numérique d'une subdivision géographique, fonctionnelle, commerciale, …

9.2.12 PBX_ ERRORCODETEST

Format : 5 chiffres

Pour simuler des cas d'erreur lors des tests d'intégration ou de simulation de production, ce code erreur est à renseigner. Variable non prise en compte dans l'environnement de production.

Voir aussi :

§9.1.7 Tableau 2 : Codes réponse PBX_RETOUR

9.2.13 PBX_IDABT

Format : 9 chiffres

Numéro d'abonnement renvoyé via la variable 'B' de PBX_RETOUR.

La documentation de cette variable permet de mettre à jour le numéro de carte associé à un abonnement. L'abonnement avait été initialement créé via le produit E-transactions Internet.

Voir aussi :

- ***§***6 ***Option Gestion des Abonnements***

9.2.14 PBX_LANGUE

Format : 3 caractères
Valeur par défaut : FRA

Langue utilisée par E-transactions pour l'affichage de la page de paiement.

Valeurs possibles :

- FRA : Français
- GBR : Anglais
- ESP : Espagnol
- ITA : Italien
- DEU : Allemand
- NLD : Hollandais
- SWE : Suédois
- PRT : Portugais

9.2.15 PBX_REFABONNE

Format : jusqu'à 250 caractères

Référence abonné affectée par le commerçant via le produit **G**estion **A**utomatisée des **E**ncaissements.

La documentation de cette variable permet de mettre à jour le numéro de carte associé à un abonné ou profil s'il existe déjà, ou de le créer s'il n'existe pas.

Voir aussi :

- ***§5.1 Intégration avec***

9.2.16 PBX_REFUSE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client

Page de retour de la plateforme vers le site Marchand après paiement refusé.

Les variables définies dans PBX_RETOUR seront envoyées à cette page.

Exemple : http://www.commerce.fr/refus.html
Voir aussi :

- ***§4 Gestion de la réponse***

Les URL doivent être encodées.

9.2.17 PBX_REPONDRE_A

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée par le Support à l'inscription dans la fiche client du commerçant

URL d'appel serveur à serveur après chaque tentative de paiement. Aussi appelée « IPN », cette URL est appelée séparément du navigateur du client, et permet donc de valider les commandes de manière sûre. Les variables définies dans PBX_RETOUR seront envoyées à cette URL.

Exemple : http://www.commerce.fr/validation_paiement.cgi
Voir aussi :

- ***§4 Gestion de la réponse***

  Les URL doivent être encodées.

9.2.18 PBX_RUF1

Format : « GET » ou « POST »
Valeur par défaut : GET

Méthode (au sens HTTP) utilisée pour l'appel de l' « IPN »

Voir aussi :

- ***§4 Gestion de la réponse***

9.2.19 PBX_SOURCE

Format : 3 à 5 caractères.
Valeur par défaut : HTML

Définit le format de la page du choix du moyen de paiement. Cette variable est à modifier en fonction du type de navigateur. Les valeurs possibles sont les suivantes :

- HTML : adaptée aux ordinateurs fixes
- WAP : format WML, pour téléphones compatibles WAP
- IMODE : format iHTML
- XHTML : page allégée, adaptée aux terminaux mobiles (type smartphones/ tablettes)

Remarque : la plateforme ne fait pas de détection automatique du navigateur.
Cette variable permet de formater la page du choix du moyen de paiement afin d'adapter la page à un appareil spécifique

9.2.20 PBX_TYPEPAIEMENT

Format : 5 à 10 caractères.
Valeur par défaut : <vide>

Privilégie un type de carte.

- Sur la page de préselection : permet de n'afficher que les moyens de paiement choisis
  - Si le commerçant dispose de l'option Paypal par exemple mais qu'il souhaite limiter un achat aux paiements par carte, il faut documenter cette variable à « CARTE ».
  - Ainsi, seules les options de type carte dont le commerçant dispose seront affichées sur la page de présélection.

- Sur la page de paiement : utilisée avec PBX_TYPECARTE, permet de ne pas afficher la page de présélection, et d'afficher la page de paiement adaptée directement.

Les valeurs possibles sont présentées dans le **Tableau 3 : Valeurs possibles PBX_TYPEPAIMENT et PBX_TYPECARTE**

Voir aussi tableau ci-dessous :

9.2.21 PBX_TYPECARTE

Format : min. 2 caractères.
Valeur par défaut : <vide>

Définit le type de carte à utiliser sur la page de paiement, dans le cas où la page de présélection du moyen de paiement fournie par la plateforme n'est pas utilisée.
S'utilise toujours conjointement à PBX_TYPEPAIEMENT.

PBX_TYPEPAIEMENT	PBX_TYPECARTE
CARTE	CB, VISA, EUROCARD_MASTERCARD,
	E_CARD
	MAESTRO
	AMEX
	DINERS
	JCB
	COFINOGA
	AURORE
PAYPAL	PAYPAL
CREDIT	UNEURO
	34ONEY
PREPAYEE	PSC
	IDEAL
	ONEYKDO
	MAXICHEQUE
	ILLICADO
LEETCHI	LEETCHI
WALLET	PAYLIB
	MASTERPASS

Tableau 3 : Valeurs possibles PBX_TYPEPAIMENT et PBX_TYPECARTE

9.2.22 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3

Format : 3 à 10 chiffres

Montant en centimes (donc sans virgule ni point) des échéances suivantes d'un paiement fractionné. L'option gestion des abonnements doit être activée.

Ces paramètres sont à utiliser obligatoirement en combinaison avec PBX_DATE1, PBX_DATE2, PBX_DATE3.

Voir aussi :

- ***§6.3 Paiement en plusieurs fois (4 fois maximum)***
- ***§9.2.6 PBX_DATE1, PBX_DATE2, PBX_DATE3***

9.2.23 PBX_3DS

Format : 'N' : Pas d'authentification 3-D Secure du porteur

Permet de ne pas effectuer une authentification 3-D Secure du porteur, uniquement pour cette transaction, même si le commerçant est enrôlé au programme 3-D Secure.

Ne pas renseigner cette variable lorsque l'authentification 3-D Secure est demandée.

Voir aussi :

- Une définition du 3DSecure en ***§10.8.1 3-D Secure***

9.3 Variables spécifiques à certains moyens de paiement

9.3.1 PBX_1EURO_CODEEXTERNE

Format : 3 chiffres. Uniquement pour la solution de paiement « 1Euro.com ».

Offre promotionnelle externe

9.3.2 PBX_1EURO_DATA

Format : jusqu'à 100 caractères. Uniquement pour la solution de paiement « 1Euro.com ».
Données d'identification et de localisation du client.

Les données sont séparées par le caractère # et doivent respecter l'ordre suivant :

- ✓ Civilité,
- ✓ Nom,
- ✓ Prénom,
- ✓ Adresse1,
- ✓ Adresse2,
- ✓ Adresse3,
- ✓ Code postal,
- ✓ Ville,
- ✓ Code pays (FR pour France par exemple),
- ✓ Téléphone fixe,
- ✓ Téléphone portable,

- ✓ Flag indiquant si l'internaute est connu du commerçant (0 : Non connu, 1 : Connu),
- ✓ Flag indiquant si le commerçant a déjà eu des incidents de paiements avec cet internaute,
- ✓ Code action COFIDIS (valeur figée et fournie par COFIDIS)

Exemple :

```
M#DUPONT#Jean#Rue Lecourbe#BatimentA##75010#PARIS#FR#0102030405##0#0#12#
```

9.3.3 PBX_CK_ONLY

Format : O ou N. Uniquement pour les cartes cadeau

La valeur « O » permet de forcer le paiement avec des cartes cadeau seulement.
Sinon, le client peut aussi utiliser sa carte ou un autre moyen de paiement pour compléter son paiement.

9.3.4 PBX_CODEFAMILLE

Format : 3 chiffres. Uniquement pour les applications COFINOGA et CDGP.

Valeur renseignée par le commerçant pour indiquer l'option de paiement qu'il propose au porteur de la carte COFINOGA ou CDGP.

9.3.5 PBX_NBCARTESKDO

Format : jusqu'à 2 chiffres. Uniquement pour les cartes cadeau.

Permet de limiter le nombre de cartes Cadeau utilisables par un porteur.
Les valeurs autorisées sont entre 1 et 25.

9.3.6 PBX_OPECOM

Format : 10 caractères. Uniquement pour la solution Facilipay d'Oney Banque Accord.

Opération commerciale.

9.3.7 PBX_ONEY_DATA

Format : XML. Uniquement pour la solution Facilipay d'Oney Banque Accord.

9.3.8 PBX_PAYPAL_DATA

Format : jusqu'à 490 caractères. Uniquement pour l'application PAYPAL

Uniquement pour les paiements via Paypal : données d'identification de localisation du client.

Les données sont séparées par le caractère # et doivent respecter l'ordre suivant :

- ✓ Nom du client (32 caractères),
- ✓ 1ère ligne d'adresse (100 caractères),
- ✓ 2ème ligne d'adresse (100 caractères) ,
- ✓ Ville (40 caractères),
- ✓ Etat / Région (40 caractères),

- ✓ Code postal (20 caractères),
- ✓ Code pays (FR pour France) (2 caractères),
- ✓ Numéro de téléphone (20 caractères)
- ✓ Description du paiement (127 caractères)

Cette variable est obligatoire dans le cas d'un paiement avec création d'abonné (E-transactions version PLUS), conseillée dans les autres cas.

Exemple :

```
PBX_PAYPAL_DATA=David VINCENT#11 Rue Jacques
CARTIER##GUYANCOURT##78280#FR#0161370570#Ordinateur Portable
```

9.4 E-transactions Résiliation des Abonnements : Requête

9.4.1 VERSION

Format : 3 chiffres. **Obligatoire.**
Valeur par défaut : 001

Version de protocole : 001

9.4.2 TYPE

Format : 3 chiffres. **Obligatoire.**
Valeur par défaut : 001

Type de demande : 001 = Résiliation

9.4.3 SITE

Format : 7 chiffres. **Obligatoire.**

Numéro de site.
Fourni lors de l'inscription.

9.4.4 MACH

Format : 3 chiffres. **Obligatoire.**

Numéro de rang.
Fourni lors de l'inscription.

9.4.5 IDENTIFIANT

Format : 1 à 9 chiffres. **Obligatoire.**

Identifiant du commerçant.
Fourni lors de l'inscription.

9.4.6 HMAC

Format : Texte. **Obligatoire.**

Permet l'authentification du commerçant et la vérification de l'intégrité du message. Son calcul se fait de la même manière que pour l'appel E-transactions.

Voir aussi :

- ***§0***

- ***Authentification du*** message,

9.4.7 TIME

Format : Date au format ISO8601. **Obligatoire.**

Date de calcul de l'empreinte HMAC.

9.4.8 ABONNEMENT

Format : 1 à 9 chiffres. **Obligatoire si pas de référence de commande précisée.**

Numéro d'abonnement à résilier.

9.4.9 REFERENCE

Format : 1 à 250 caractères. **Obligatoire si pas de numéro d'abonnement précisé.**

Référence commande de l'abonnement à préciser.

9.5 E-transactions Résiliation des Abonnements : Réponse

La réponse est fournie par l'intermédiaire de trois variables indiquant si la résiliation a réussi ou non, le motif de refus et un rappel sur l'abonnement.

9.5.1 ACQ

Format : 2 caractères. **Obligatoire.**

OK : Succès
NO : Echec

9.5.2 ERREUR

Format : 1 chiffre. **Obligatoire en cas d'échec.**

Numéro de l'erreur en cas d'échec :

- 1 : Incident technique (Configuration),
- 2 : Données non cohérentes,
- 3 : Incident technique (Accès à la base de données),
- 4 : Site inconnu,
- 9 : Echec de la résiliation. Aucun abonnement résilié

9.5.3 IDENTIFIANT

Format : 1 à 9 chiffres. **Obligatoire.**

Valeur transmise dans la requête initiale.

9.5.4 ABONNEMENT

Format : 1 à 9 chiffres. **Obligatoire si pas de référence de commande précisée.**

Valeur transmise dans la requête initiale.

9.5.5 REFERENCE

Format : 1 à 250 caractères. **Obligatoire si pas de numéro d'abonnement précisé.**

Valeur transmise dans la requête initiale.

10. ANNEXES

10.1 Codes réponses du centre d'autorisation

Cette information est transmise dans les informations de retour en fin de transaction si la variable E a été spécifiée à l'appel.

Voir ***§9.1.7 PBX_RETOUR*** et §4 ***Gestion de la réponse***

10.1.1 Réseaux CB, Visa, Mastercard, American Express et Diners

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès
01	Contacter l'émetteur de carte
02	Contacter l'émetteur de carte
03	Commerçant invalide
04	Conserver la carte
05	Ne pas honorer
07	Conserver la carte, conditions spéciales
08	Approuver après identification du porteur
12	Transaction invalide
13	Montant invalide
14	Numéro de porteur invalide
15	Emetteur de carte inconnu
17	Annulation client
19	Répéter la transaction ultérieurement
20	Réponse erronée (erreur dans le domaine serveur)
24	Mise à jour de fichier non supportée
25	Impossible de localiser l'enregistrement dans le fichier
26	Enregistrement dupliqué, ancien enregistrement remplacé
27	Erreur en « edit » sur champ de mise à jour fichier
28	Accès interdit au fichier
29	Mise à jour de fichier impossible
30	Erreur de format
33	Carte expirée
38	Nombre d'essais code confidentiel dépassé

41	Carte perdue
43	Carte volée
51	Provision insuffisante ou crédit dépassé
54	Date de validité de la carte dépassée
55	Code confidentiel erroné
56	Carte absente du fichier
57	Transaction non permise à ce porteur
58	Transaction interdite au terminal
59	Suspicion de fraude
60	L'accepteur de carte doit contacter l'acquéreur
61	Dépasse la limite du montant de retrait
63	Règles de sécurité non respectées
68	Réponse non parvenue ou reçue trop tard
75	Nombre d'essais code confidentiel dépassé
76	Porteur déjà en opposition, ancien enregistrement conservé
89	Echec de l'authentification
90	Arrêt momentané du système
91	Emetteur de cartes inaccessible
94	Demande dupliquée
96	Mauvais fonctionnement du système
97	Echéance de la temporisation de surveillance globale

Tableau 4 : Codes réponses du centre d'auto CB

10.1.2 Réseau Cetelem/Aurore et Rive Gauche

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès.
01	Numéro de commerçant incorrect ou inconnu
02	Numéro de carte incorrect
03	Date de naissance ou code secret erronés
04	Carte non finançable
05	Problème centre serveur CETELEM
06	Carte inconnue
07	Demande de réserve refusée
08	Carte périmée

09	Incompatibilité carte/commerçant
10	Inconnu
11	Annulé
12	Code devise incorrect
13	Référence de l'opération non renseignée
14	Montant de l'opération incorrect
15	Modalité de paiement incorrect
16	Sens de l'opération incorrect
17	Mode de règlement incorrect

Tableau 5 : Codes réponses du centre d'auto Cetelem

10.2 Codes retour HTTP

Le premier chiffre indique la classe de réponse. Il en existe 5 valeurs :

CODE	DESCRIPTION
1xx	Information – Requête reçue, traitement en cours
2xx	La demande a été reçue avec succès reçue, comprise et acceptée
3xx	Redirection
4xx	Erreur de Client - La demande contient une mauvaise syntaxe ou ne peut pas être accomplie
5xx	Erreur de serveur - Le serveur a échoué à accomplir une demande apparemment valable

Tableau 6 : Codes retour http

Pour plus de détails et la liste complète des codes retour, se référer à la norme du protocole HTTP1.1, nommée RFC2616.

10.3 Codes erreur CURL

CODE	DESCRIPTION
1	Protocole non supporté
2	Echec durant la phase d'initialisation
3	URL mal formatée
4	URL mal formatée
5	Résolution du proxy impossible
6	Résolution du host impossible
7	Connexion impossible avec le host

22	(HTTP) Page non atteinte
34	(HTTP) Méthode post en erreur
35	Connexion SSL en erreur
42	Callback annulée
43	Erreur interne
44	Erreur interne
45	Erreur d'interface
47	Trop de redirections
51	Certificat SSL distant incorrect
52	Le serveur ne répond à rien
53	Moteur de cryptographie SSL non trouvé
54	Problème d'initialisation du moteur de cryptographie SSL
55	Envoi de données en erreur
56	Réception de données en erreur
57	Erreur interne
58	Problème avec le certificat local
59	Impossible d'utiliser le chiffrement SSL indiqué

Tableau 7 : Codes erreur CURL

10.4 Jeu de caractères

Le jeu de caractères supporté par les applications est présenté dans le tableau ci-dessous. Tous les autres caractères autres que ceux présents dans le tableau ci-dessous seront, suivant les applications, supprimés ou la trame rejetée :

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	\0									\t	\n			\r		
1																
2		!	"	#	$	%	&		(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	O
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
8																
9																
A		¡				¦						«				
B												»				¿
C	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
D	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
E	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	Ï
F	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	Ÿ

10.5 Caractères URL Encodés

Ci-dessous dans la colonne de gauche (Caractère) est définie une liste des caractères spéciaux les plus fréquents qu'il faut convertir en valeur « URL Encodée » s'ils sont présents dans une URL.
Ces caractères doivent être remplacés par la valeur précisée dans la colonne « URL Encodé ».

CARACTERE	URL ENCODE
;	%3B
?	%3F
/	%2F
:	%3A
#	%23
&	%26
=	%3D
+	%2B
$	%24
,	%2C
<espace>	%20
%	%25
@	%40

10.6 URL d'appel et Adresses IP

Les URLs d'appel pour effectuer des transactions en E-transactions **classique** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.e-transactions.fr/cgi/MYchoix_pagepaiement.cgi
Production	https://tpeweb.e-transactions.fr/cgi/MYchoix_pagepaiement.cgi https://tpeweb1.e-transactions.fr/cgi/MYchoix_pagepaiement.cgi

Les URLs d'appel pour effectuer des transactions en E-transactions **version Light (iFrame)** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi
Production	https://tpeweb.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi https://tpeweb1.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi

Les URLs d'appel pour effectuer des transactions en E-transactions **version Mobile** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.e-transactions.fr/cgi/ChoixPaiementMobile.cgi
Production	https://tpeweb.e-transactions.fr/cgi/ChoixPaiementMobile.cgi https://tpeweb1.e-transactions.fr/cgi/ChoixPaiementMobile

Les URLs d'appel pour effectuer des **Résiliation des abonnements** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https:// preprod-tpeweb.e-transactions.fr/cgi-bin/ResAbon.cgi
Production	https://tpeweb.e-transactions.fr/cgi-bin/ResAbon.cgi https://tpeweb1.e-transactions.fr/cgi-bin/ResAbon.cgi

L'adresse IP entrante est l'adresse sur laquelle le site Marchand va se connecter pour réaliser la transaction.
L'adresse IP sortante est l'adresse avec laquelle le site Marchand verra arriver les flux de retour en fin de transaction (appels de l'IPN par exemple).

Il est important que ces adresses entrantes et sortantes soient autorisées dans les éventuels filtres sur les adresses IP paramétrés sur les infrastructures hébergeant les sites marchands.

PLATE-FORME	ADRESSES IP PUBLIQUES AFFECTÉES AUX INFRASTRUCTURES E-TRANSACTIONS	ADRESSES IP SORTANTES DEPUIS LES INFRASTRUCTURES E-TRANSACTIONS
Pré-production	195.101.99.68	195.101.99.76
Production	194.2.160.69 194.2.160.76 194.2.160.85 194.2.160.92 195.25.7.149 195.25.7.158 195.25.67.5 195.25.67.12	194.2.122.158 194.2.122.190 195.25.7.166 195.25.67.22

10.7 Glossaire

10.7.1 3-D Secure

La plupart des sites de commerce électronique, qui proposent de faire du paiement en ligne, utilisent les protocoles SSL pour chiffrer les informations sensibles telles que le numéro de carte bancaire. Ces protocoles ont été conçus pour assurer la confidentialité des informations échangées entre deux entités et s'avèrent insatisfaisants par rapport aux exigences requises pour des paiements sécurisés.

Dans ce contexte, MasterCard et VISA ont conçu l'architecture 3D-Secure dont la finalité est de permettre aux banques d'authentifier leurs porteurs par le moyen de leur choix, via un mécanisme technique mis en place à la fois par les banques des commerçants et des porteurs de cartes.

3D-Secure permet :

- de s'assurer que l'internaute qui réalise la transaction est bien le titulaire de la carte utilisée pour le paiement,
- de garantir au commerçant les transactions et d'introduire en cas de contestation du porteur de carte, un transfert de responsabilité vers la banque de ce dernier.

L'authentification du porteur est gérée par la banque du porteur de carte. Le porteur visualise donc toujours la même page d'authentification. La Banque de France préconise une authentification forte non rejouable (ANR) : code envoyé par SMS ou SVI, calculette …

En France, toutes les banques émettrices de cartes adhèrent au programme 3D-Secure.

Le commerçant E-transactions visualise dans son back-office si la transaction est ou non garantie 3DSecure. Les indicateurs suivant sont disponibles :

- *Paiement 3D-Secure* : Indique si la transaction a été exécutée avec un contrôle 3DSecure
  - « OUI » Avec 3D-Secure
  - « NON » Sans 3D-Secure

- *Porteur authentifié* : Indique si la carte de l'acheteur est enrôlée à 3D-Secure et s'il a réussi à s'authentifier

  - Y L'authentification s'est déroulée avec succès
  - N Le porteur n'est pas parvenu à s'authentifier, la transaction est interdite
  - U L'authentification n'a pu être finalisée suite à un problème technique
  - A L'authentification n'était pas disponible, mais une preuve de tentative d'authentification a été générée

- *Garantie* : Indique l'état de la garantie de la transaction selon les règles 3D-Secure
  - « OUI » Garantie
  - « OUI expirée » Non Garantie car remise au-delà du délai maxi de 7 Jours
  - « NON » Non Garantie

  Seules les transactions marquées « OUI » font l'objet d'une garantie 3D-Secure

Si une transaction garantie 3DSecure (indicateur à « OUI ») est contestée par le porteur, l'impayé sera supporté par la banque émettrice. Par contre, si le commerce envoie en banque une transaction non garantie, il prend le risque d'assumer le coût des impayés en cas de contestation du porteur.

Les échéances postérieures au 1er paiement lors d'un paiement en plusieurs fois ou d'un abonnement ne sont pas garanties car elles ne sont pas réalisées par l'internaute en mode 3DSecure mais générées automatiquement.

Même s'il a souscrit à 3DSecure, le commerçant doit toujours rester vigilant lorsque la transaction lui semble frauduleuse.

10.7.2 Encodage URL (url-encodé)

Tous les caractères ne sont pas autorisés dans les URL (voir la définition de URL ci-dessous). L'encodage URL permet de transformer certains caractères spéciaux afin que les données puissent être transmises.
Exemple : « ! » devient « %21 », « @ » devient « %40 »

Des fonctions sont disponibles dans la plupart des langages afin de faire la conversion. urlencode() et urldecode() peuvent être utilisées en PHP, par exemple.

10.7.3 FTP

Le FTP (File Transfer Protocol) est un protocole de transfert de fichiers permettant de télécharger des données choisies par l'internaute d'un ordinateur à un autre, selon le modèle client-serveur.

10.7.4 HMAC

HMAC (pour Hash-based Message Authentication Code) est un protocole standard (RFC 2104) permettant de vérifier l'intégrité d'une chaîne de données et utilisé sur les solutions E-transactions pour vérifier l'authenticité du site Marchand qui se connecte.

Des fonctions sont disponibles dans la plupart des langages de programmation pour calculer un HMAC.

10.7.5 HTTP

HTTP (HyperText Transport Protocol) est le protocole de base du Web, utilisé pour transférer des documents hypertextes (comme une page Web) entre un serveur et un navigateur sur un poste Client.

10.7.6 IP (adresse IP)

L'adresse IP (IP pour Internet Protocol) est l'adresse unique d'un ordinateur connecté sur un réseau donné (réseau local ou World Wide Web).

10.7.7 SSL

Le protocole SSL (Secure Sockets Layer) permet la transmission sécurisée de données (par exemple de formulaires ou pages HTML sur le Web) et peut donc servir à des transactions financières en ligne nécessitant l'utilisation d'une carte de crédit. Un pirate qui « écouterait » sur cette connexion ne pourrait pas déchiffrer les informations qui y circulent.

10.7.8 URL

Les URL (Uniform Resource Locators) sont les adresses de ressources sur Internet. Une ressource peut être un serveur http, un fichier sur votre disque, une image…

Exemple : http://www.maboutique.com/site/bienvenue.html