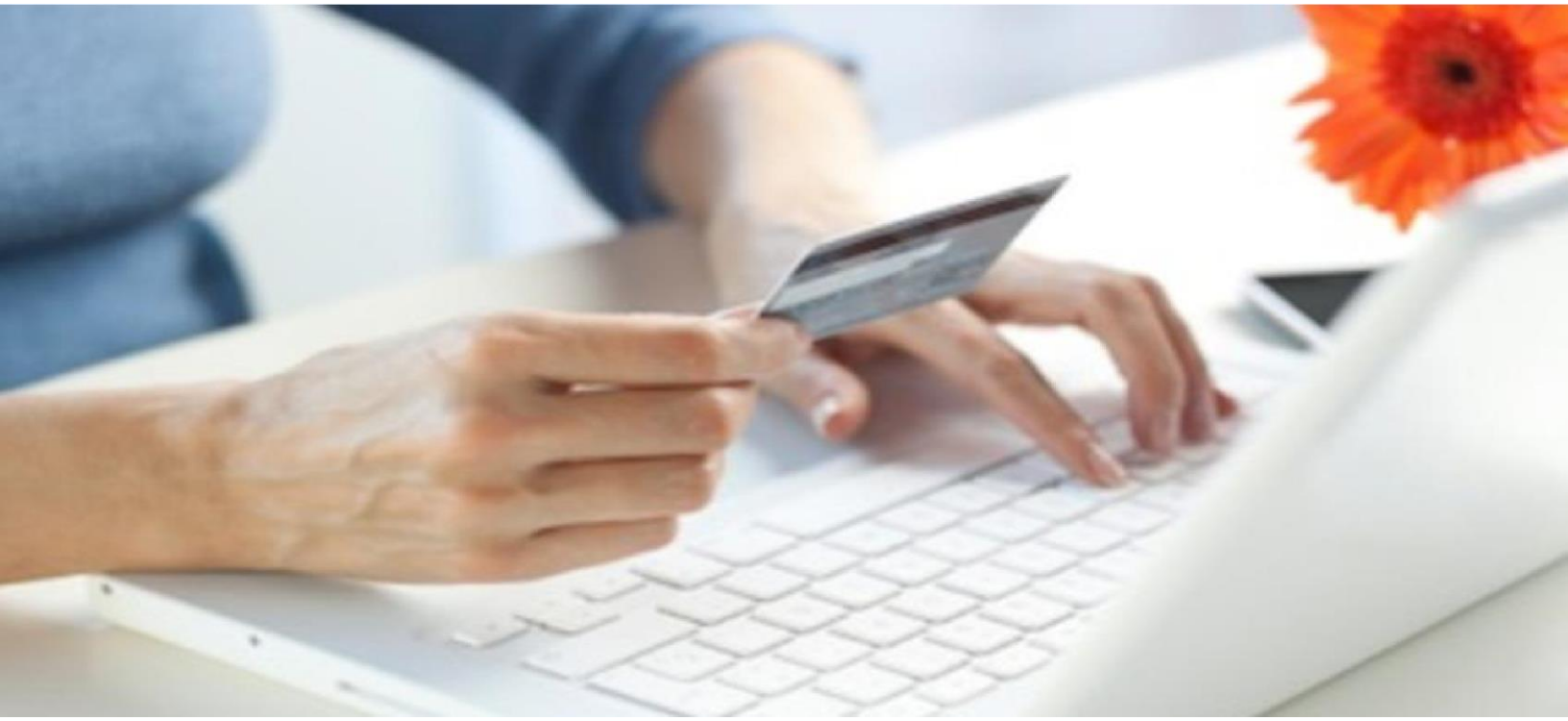
E-transactions

MANUEL INTEGRATION

Gestion Automatisée des Encaissements CB5.5

VERSION DU

30/09/2020



REFERENCES DOCUMENTATIONS

REF.	DOCUMENT	DESCRIPTION
Ref 1	Manuel Intégration E-transactions Internet	Manuel d'intégration de la solution Etransactions Internet
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 5	Manuel Intégration E-transactions RemoteMPI	Manuel d'intégration de la solution RemoteMPI permettant la mise en place de 3D-Secure avec la Gestion Automatisée des Encaissements (à utiliser pour une intégration directe du paiement sur un site marchand PCIDSS)
Ref 6	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 7	Note PayPal	Note d'intégration pour PayPal
Ref 8	Personnalisation de la page et ticket de paiement	Manuel Intégrateur pour personnaliser la page de paiement aux couleurs de votre commerce
Ref 9	Note Paylib	Note d'intégration pour Paylib

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 08/08/2017.

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 (3 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'ecommerce 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 **G**estion **A**utomatisée des **E**ncaissements **CB55**.

Il s'adresse aux personnes ayant besoin d'informations sur le fonctionnement de ces solutions, sur la manière de s'y interfacer et de les intégrer de la meilleure manière.

2. PRESENTATION DU PRODUIT GESTION AUTOMATISEE DES ENCAISSEMENTS CB55

2.1 Principe général de fonctionnement

La Gestion Automatisée des Encaissements permet d'envoyer une transaction à la plateforme Etransactions via une trame HTTPS « question », et d'obtenir en retour de la même session HTTPS une trame « réponse » précisant l'acceptation ou le refus de la requête.

Le principe de la Gestion Automatisée des Encaissements est donc de :

- Créer une trame HTTPS « question »,
- Appeler une URL présente sur nos serveurs,
- Récupérer dans la même session HTTPS la trame « réponse » retournée par la plateforme après traitement de la transaction.

2.2 Pré – Requis

Afin d'être en conformité avec la réglementation La Gestion Automatisée des Encaissements CB5.5, les modifications décrites dans les paragraphes ci-dessous seront nécessaires.

Pour être éligible à la procédure de migration, le marchand devra :

- Utiliser le Back Office Vision v8.2 pour visualiser et exploitation ses transactions.

2.3 Liste des moyens de paiement

Ci-dessous une liste complète des moyens de paiement acceptés par La Gestion Automatisée des Encaissements CB5.5:

MOYEN DE PAIEMENT	TYPE	COMMENTAIRE
CB, VISA, MASTERCARD	Cartes de crédit	
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	
ILLICADO	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
PAYLIB	Moyen de paiement	
e-ANCV	Moyen de paiement	

2.4 Sécurité

2.4.1 Identification

Un site du commerçant est déclaré dans le back office Vision avec plusieurs données dont :

- Le numéro de site
- Le numéro de rang
- Un identifiant

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

2.4.2 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 Etransactions 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.

3. PROTOCOLE D'ECHANGE

3.1 URL appelée

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.

3.2 Appel

Les trames sont formées par un assemblage de couples « variable, valeur » (…TYPE=00001&MONTANT=1000&SITE=1999887&…) à la manière d'un formulaire HTML dont les

variables sont émises via une méthode POST. La méthode GET n'est pas autorisée par les applications Gestion Automatisée des Encaissements.

La trame « question » sera émise vers nos serveurs en appelant l'URL de Gestion Automatisée des Encaissements CB5.5 (voir §6.4 ***URL d'appel et Adresses IP***).

Pour obtenir une réponse de la part de nos serveurs, les variables « SITE » et « RANG » doivent être renseignées et cohérentes.

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 ***§5.2*** **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 ciavant, la chaine constituée sera la suivante :

```
VERSION=00104&TYPE=00001&SITE=1999887&RANG=032&NUMQUESTION=780776682&MONTANT=1000&DEVISE=
978&REFERENCE=TestPaybox&PORTEUR=1111222233334444&DATEVAL=0216&CVV=123&ACTIVITE=024&DATEQ
=23062015&PAYS=&HASH=SHA512
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres)

- 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 HASH (cf. HASH dans **Dictionnaire de données**)

- Etape 3 : le résultat obtenu (l'empreinte) doit alors être placé dans le champ 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 :

```
<html>
<body>
<?php
// On récupère la date au format ISO-8601
$dateTime = date("c");
// On crée la chaîne à hacher sans URLencodage $msg
="VERSION=00104".
"&TYPE=00003".
"&SITE=1999887".
"&RANG=32".
"&NUMQUESTION=0000000002".
"&MONTANT=1000".
"&DEVISE=978".
"&REFERENCE=Test".
"&PORTEUR=1111222233334444".
"&HASH=SHA512".
"&DATEVAL=1017".
"&CVV=123".
"&ACTIVITE=024".
"&DATEQ=24062015";



// On récupère la clé secrète HMAC (stockée dans une base de données cryptée) et que l'on
renseigne dans la variable $keyTest. Pour que le formulaire fonctionne, on prend la clef
HMAC associée au compte de test;
$keyTest =
"0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF012345678
9ABCDEF0123456789ABCDEF0123456789ABCDEF";

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

// On calcule l'empreinte (à renseigner dans le paramètre HMAC) grâce à la fonction
hash_hmac et // la clé binaire
// On envoie via la variable 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
echo $hmac;  echo "\n"; echo $msg;
  ?>

  <form method="POST" action="https://preprod-ppps.paybox.com/PPPS.php">
  <input type="hidden" name="VERSION" value="00104">
  <input type="hidden" name="TYPE" value="00003">
  <input type="hidden" name="SITE" value="1999887">
  <input type="hidden" name="RANG" value="32">
  <input type="hidden" name="NUMQUESTION" value="0000000002">
  <input type="hidden" name="MONTANT" value="1000">
  <input type="hidden" name="DEVISE" value="978">
  <input type="hidden" name="REFERENCE" value="Test">
  <input type="hidden" name="PORTEUR" value="1111222233334444">
  <input type="hidden" name="HASH" value="SHA512">
  <input type="hidden" name="DATEVAL" value="1017">
  <input type="hidden" name="CVV" value="123">
  <input type="hidden" name="ACTIVITE" value="024">
  <input type="hidden" name="DATEQ" value="24062015">
  <input type="hidden" name="HMAC" value='<?php echo $hmac; ?>'>

  <input type="submit" value="Envoyer">
  </form>
  </body>
  </html>
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée.

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 Réponse

La réponse se fait dans le même format que l'appel. Un ensemble de variables est transmis dans le message HTTPS.

Les variables SITE, RANG et NUMQUESTION sont toujours retournées à l'identique de l'appel. Il est conseillé de vérifier la cohérence de ces valeurs.

La Gestion Automatisée des Encaissements renvoie aussi un code réponse (variable CODEREPONSE), indiquant le bon déroulement ou non de la requête. Par exemple, le code réponse 00000 signifie que la demande a bien été traitée. L'ensemble de ces codes doivent être gérés par le site marchand.

En cas d'erreur, la Gestion Automatisée des Encaissements fournit aussi un message d'erreur détaillé dans le champ COMMENTAIRE qui permettra, en cas d'anomalie grave, une aide au diagnostic avec l'assistance E-transactions.

4. DICTIONNAIRE DE DONNEES

Vous trouverez dans les tableaux ci-dessous l'ensemble des variables Gestion Automatisée des Encaissements en fonction du type de demandes. Le détail de chaque variable (format, contenu, exemples) est donné dans les pages qui suivent.

4.1 Type de demande : Demande d'auto simple (NoShow : enregistrement de l'empreinte)

Les variables obligatoires sont en rouge :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation Pour la trame Question, utilisé si appel phonie
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATENAISS	X		Spécifique COFINOGA
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme

NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
PRIV_CODETRAITEMENT	X		Spécifique SOFINCO/COFINOGA
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole

Tableau 1 : Liste des variables Gestion Automatisée des Encaissements

4.2 Type de demande : Capture (NoShow : capture totale ou partielle du montant initial)

Les variables obligatoires sont en rouge :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation Pour la trame Question, utilisé si appel phonie
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATENAISS	X		Spécifique COFINOGA

DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
PRIV_CODETRAITEMENT	X		Spécifique SOFINCO/COFINOGA
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole

Tableau 2 : Liste des variables Gestion Automatisée des Encaissements

4.3 Type de demande : Remboursement

Les variables obligatoires sont en rouge :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation Pour la trame Question, utilisé si appel phonie
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATENAISS	X		Spécifique COFINOGA
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
PRIV_CODETRAITEMENT	X		Spécifique SOFINCO/COFINOGA
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise

SHA-1	X	X	Indication que l'empreinte de la carte doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole

Tableau 3 : Liste des variables Gestion Automatisée des Encaissements

4.4 Type de demande : Consultation

Les variables obligatoires sont en rouge :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation Pour la trame Question, utilisé si appel phonie
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATENAISS	X		Spécifique COFINOGA
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI

MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
PRIV_CODETRAITEMENT	X		Spécifique SOFINCO/COFINOGA
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole

Tableau 4 : Liste des variables Gestion Automatisée des Encaissements

4.5 Type de demande : Création d'abonné (enregistrement d'une carte)

Les variables obligatoires sont en rouge :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation Pour la trame Question, utilisé si appel phonie
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)

CVV	X		Cryptogramme visuel de la carte
DATENAISS	X		Spécifique COFINOGA
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
PRIV_CODETRAITEMENT	X		Spécifique SOFINCO/COFINOGA
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REFABONNE	X	X	Numéro d'abonné (Vide en contexte hors abonnement)
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole

Tableau 5 : Liste des variables Gestion Automatisée des Encaissements

4.6 Type de demande : Débit de l'abonné

Les variables obligatoires sont en rouge :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation Pour la trame Question, utilisé si appel phonie
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATENAISS	X		Spécifique COFINOGA
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte

PRIV_CODETRAITEMENT	X		Spécifique SOFINCO/COFINOGA
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REFABONNE	X	X	Numéro d'abonné (Vide en contexte hors abonnement)
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole
MARQUE (MIF)		X	Marque réseau de la carte
PRODUIT (MIF)		X	Catégorie de la carte
LONGUEUR (MIF)		X	
SELECTION (MIF)	X		
EMAILPORTEUR (CMIF)	X		

Tableau 6 : Liste des variables Gestion Automatisée des Encaissements

4.6.1 Nouvelles Variables MIF

4.6.1.1 SELECTION

Format : 2 chiffres

Permet d'identifier comment le choix de la marque a été réalisé.

- « 00 » Il s'agit d'un choix par défaut.
- « 01 » Le choix a été fait par le porteur.

4.6.1.2 EMAILPORTEUR

Format: 6 à 150 caractères. Les caractères « @ » et « . » doivent être présents.

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

Exemple : test@ca-ps.com

Cette nouvelle variable sert à envoyer des tickets conforment à la réglementation en vigueur pour les débits (transaction liée à la commande), crédits (remboursement), et annulations. Aussi bien dans le cas d'une transaction acceptée ou refusée.

Le commerçant souhaitant générer lui-même les tickets pourra récupérer toutes les informations nécessaires dans le retour IPN.

4.6.1.3 MARQUE

Format : 1 caractère

Correspondance avec la marque réseau de la carte :

Code	Libellé
0	Maestro
1	CB
2	VISA
3	Mastercard (MCW)
8	Vpay
9	Electron
A	CB / VISA
B	CB / MCW
C	CB / Vpay
D	CB / Electron
E	CB / Maestro

4.6.1.4 PRODUIT

Format : 1 caractère

Correspondance avec la catégorie de carte :

Code	Libellé
C	Usage Crédit
D	Usage Débit
P	Usage Prépayé
U*	Usage Universel
E	Usage Commercial
Blanc*	Indéterminé

(*) : Ces 2 catégories de carte ne seront plus gérées dans la prochaine version de MPADS

4.6.1.5 LONGUEUR

Format : 2 chiffres

Correspondance avec la longueur de la carte :

Code	Commentaire
10	N° porteur sur 10 positions
11	N° porteur sur 11 positions
12	N° porteur sur 12 positions
13	N° porteur sur 13 positions
14	N° porteur sur 14 positions
15	N° porteur sur 15 positions
16	N° porteur sur 16 positions
17	N° porteur sur 17 positions
18	N° porteur sur 18 positions
19	N° porteur sur 19 positions
39	La valeur '39' est utilisée en diffusion des plages porteurs pendant une période indéterminée. Cette valeur indique qu'une plage porteur peut comporter des numéros de porteurs d'une longueur '13', '16' ou '19'.
90	La valeur '90' est utilisée en alimentation du fichier des Établissements par les représentants des organismes internationaux pour les plages de numéros porteurs étrangères et en diffusion du fichier des Établissements. Cette valeur indique qu'une plage porteur peut comporter des numéros de porteurs d'une longueur indéterminée, de '10' à '19'.

4.7 Variables d'appel Gestion Automatisée des Encaissements

4.7.1 SITE

Format : 7 chiffres. **Obligatoire.**

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

Exemple : 1999888

4.7.2 RANG

Format : 2 chiffres ou 3 chiffres. **Obligatoire.**

C'est le numéro de rang (ou « machine ») fourni par la banque du Commerçant.
La nouvelle réglementation modifie le format de ce champ qui passe de 2 chiffres à 3 chiffres.

Remarque : Dans le cas où le rang serait envoyé sur 2 chiffres après la migration du contrat, la valeur sera préfixée par un 0.

Exemple : 001

4.7.3 VERSION

Format : 5 chiffres. **Obligatoire.**

Version du protocole Gestion Automatisée des Encaissements

Valeurs :

Mettre « 00104 » pour la Gestion Automatisée des Encaissements

4.7.4 TYPE

Format : 5 chiffres. **Obligatoire.**

Gestion Automatisée des Encaissements permet la réalisation de transactions, mais aussi de toutes les opérations de caisse liées à ces transactions : capture, remboursement, annulation, … Cette variable définit l'action à réaliser.

Dans le cas des trames de capture (00002) qui suivent une demande d'auto seule, il est conseillé :

- D'attendre quelques instants (quelques secondes) entre la demande d'autorisation seule et la capture
- D'envoyer la capture sur la même plateforme (Nanterre ou Strasbourg) que la demande d'autorisation seule afin d'éviter d'éventuels problèmes de réplication entre les plateformes.

Un nouveau type de requête MIF est en place pour permettre au marchand de connaitre les marques associées à la carte du porteur ainsi que la catégorie et la longueur de cette dernière (00018). Cette requête est optionnelle.

CODE	DESCRIPTION
00001	Autorisation seule
00002	Débit (Capture)
00003	Autorisation + Capture
00004	Crédit
00005	Annulation
00011	Vérification de l'existence d'une transaction
00012	Transaction sans demande d'autorisation

00013	Modification du montant d'une transaction
00014	Remboursement
00017	Consultation
00018	Demande des marques associées à la carte du porteur (MIF)
00051	Autorisation seule sur un abonné
00052	Débit sur un abonné
00053	Autorisation + Capture sur un abonné
00054	Crédit sur un abonné
00055	Annulation d'une opération sur un abonné
00056	Inscription nouvel abonné
00057	Modification abonné existant
00058	Suppression abonné
00061	Transaction sans demande d'autorisation (forçage)

4.7.5 DATEQ

Format : 14 chiffres. **Obligatoire.**

Date et heure d'envoi de la trame (date du jour) sous la forme JJMMAAAAHHMMSS (jour mois année heure minute seconde).

Utilisé dans les requêtes SQL pour la question du type 11 (format JJMMAAAA)

Exemple : 13042012125959

4.7.6 NUMQUESTION

Format : 10 chiffres (min : 0000000001 ; max : 2147483647). **Obligatoire.**

Identifiant unique de la requête permettant d'éviter les confusions au niveau des réponses en cas de questions multiples et simultanées.
Chaque appel doit avoir un numéro de question unique sur une journée. Il pourra être réinitialisé chaque jour.

Exemple : 0000000001

4.7.7 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 SHA256
- RIPEMD160 SHA384
- SHA224 MDC2

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

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.

4.7.8 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 :

- ***§3.3*** **Authentification du message**
- ***§6.6.3*** **Erreur ! Source du renvoi introuvable.**

4.7.9 MONTANT

Format : 10 chiffres. **Obligatoire pour les questions de type 1, 2, 3, 4,5,11, 12, 13, 14, 51, 52, 53, 54, 55, 56, 57, 61.**

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

Exemple : pour 19€90 :

- 0000001990

4.7.10 DEVISE

Format : 3 chiffres. **Obligatoire pour les questions de type 1, 2, 3, 4, 5, 11, 12, 13, 14, 51, 52, 53, 54, 55, 56, 57, 61.**

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

Exemples :

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

La seule valeur autorisée est l'€ : 978

4.7.11 REFERENCE

Format : 1 à 250 caractères. **Obligatoire pour les questions de type 1, 2, 3, 4, 5, 11, 12, 51, 52, 53, 54, 55, 56, 61.**

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.

Exemple : CMD9542124-01A5G

4.7.12 REFABONNE

Format : 1 à 250 caractères. **Obligatoire pour les questions de type 51, 52, 53, 54, 55, 56, 57, 58, 61.**

Référence du client du commerçant permettant de l'identifier clairement, dans la gestion des abonnements proposées par la solution de paiement

Exemple : AZERTY1234567

4.7.13 PORTEUR

Format : 19 caractères. **Obligatoire pour les questions de type 1, 3, 4, 12, 51, 53, 54, 55, 56, 57, 61.**

Numéro de carte du porteur (client) sans espace, cadré à gauche.

Exemple : 1111222233334444

:

4.7.14 DATEVAL

Format Date (MMAA) **Obligatoire pour les questions de type 1, 3, 4, 12, 51, 53, 54, 55, 56, 57, 61.**

Date de fin de validité de la carte.

Exemple : 1213 (décembre 2013)

4.7.15 CVV

Format : 3 ou 4 caractères. **Obligatoire pour les questions de type 1, 3, 4, 12, 56.**
Cryptogramme visuel situé au dos de la carte bancaire.

Remarque : Les cartes AMERICAN EXPRESS ont sur leur recto un CIN (Card Identification Number) sur 4 chiffres.

Exemple : 123 **4.7.16**

ACTIVITE

Format : 3 chiffres.
Valeur par défaut : 024 /027

Il s'agit pour la banque de différencier la provenance des différents flux monétiques envoyés ; ceci ayant pour but de renseigner de la manière la plus correcte possible les champs relatifs à l'ERT (Environnement réglementaire et technique)

Voici les valeurs possibles pour l'ERT :

CODE	DESCRIPTION
021	Demande par téléphone
022	Demande par correspondance
024	Demande par internet
027	Paiement récurrent

4.7.17 ARCHIVAGE

Format : jusqu'à 12 caractères alphanumériques

Référence transmise à E-transactions au moment de la télécollecte. Elle devrait être unique et permettra au Crédit Agricole de fournir au commerçant, une information en cas de litige sur un paiement.

:

4.7.18 DIFFERE

Format 3 caractères (75 jours maximum)

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 dans la fiche d'inscription. Si ce paramètre est envoyé dans l'appel, la valeur spécifiée dans l'appel est prioritaire sur celle par défaut.

Exemple : 004 pour gérer un différé de 4 jours

Rappel : la garantie de paiement 3Ds n'est valable que 6 jours.

4.7.19 NUMAPPEL

Format : 10 chiffres. **Obligatoire pour les questions de type 2, 5, 13, 14, 52, 55.**

Ce numéro est renvoyé par la plateforme E-transactions suite à la réalisation d'une transaction.
Pour E-transactions, il se trouve dans les paramètres de retour (IPN)
Pour Gestion Automatisée des Encaissements, il est présent dans le message de réponse.
Il est aussi visible dans le Back-Office.

4.7.20 NUMTRANS

Format : 10 chiffres. **Obligatoire pour les questions de type 2, 5, 13, 14, 17, 52, 55.**

Ce numéro est renvoyé par la plateforme E-transactions suite à la réalisation d'une transaction.
Pour E-transactions, il se trouve dans les paramètres de retour (IPN)
Pour Gestion Automatisée des Encaissements, il est présent dans le message de réponse.
Il est aussi visible dans le Back-Office.

4.7.21 AUTORISATION

Format : jusqu'à 10 caractères. Utilisable dans les questions de type 1, 3,13, 51, 56 et 57.

Numéro d'autorisation délivré par le centre d'autorisation de la banque du commerçant si le paiement est accepté.

Exemple : 123456

:

4.7.22 PAYS

Format : vide.

Si ce champ est présent (même vide), Gestion Automatisée des Encaissements renvoie le code pays de la carte dans la réponse.

4.7.23 PRIV_CODETRAITEMENT

Format 3 chiffres.

Valeur renseignée par le commerçant pour indiquer l'option de paiement qu'il propose au porteur de la carte SOFINCO (ou carte Partenaire-SOFINCO) ou COFINOGA.

4.7.24 DATENAISS

Format : Date JJMMAAAA (8 chiffres).

Date de naissance du porteur pour les cartes COFINOGA.

4.7.25 ACQUEREUR

Format : jusqu'à 16 caractères.

Définit le moyen de paiement utilisé. Les valeurs possibles sont :

- PAYPAL
- PSC (Paysafecard)
- FINAREF
- 34ONEY

Dans le cas de requêtes Gestion Automatisée des Encaissements ne concernant pas l'un de ces acquéreurs, ce champ ne doit pas être envoyé.

4.7.26 TYPECARTE

Format : 2 à 30 caractères

Permet d'identifier la marque sélectionnée pour la tentative de paiement. Les valeurs possibles sont :

- CB ELECTRON
- VISA MAESTRO
- MASTERCARD* VPAY*
- e-ANCV

* Nouvelles variables misent en place pour implémenter le MIF

:

> **Remarque :** Si ce champ est présent (même vide), gestion Automatisée des Encaissements renvoie l'empreinte de la carte dans la réponse (pour un paiement par carte)

4.7.27 SHA-1

Format : vide

Si ce champ est présent (même vide), Gestion Automatisée des Encaissements renvoie l'empreinte de la carte dans la réponse (pour un paiement par carte).

Le numéro de carte est hashé avec la méthode SHA-1

4.7.28 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.

4.7.29 ID3D

Format : 20 chiffres

Identifiant de contexte contenant les données d'authentification retournées par le MPI (cf. documentation « E-transactions RemoteMPI »)

Ce contexte d'authentification est stocké pendant une durée de 5 minutes.

Au-delà, les applications de E-transactions considèreront que la phase d'authentification du porteur est non valide car en timeout.

4.8 NOUVELLE REQUETE MIF

Cette requête permet au marchand de récupérer les marques associées à la carte du porteur ainsi que la catégorie et la longueur de cette dernière.

> **Remarque :** Les infos sur les préférences commerçants ou sur les marques refusées ne sont pas envoyées dans ces trames. Elles sont associées au contrat et peuvent être consultées sur le BO Vision.

4.8.1 EXEMPLE D'APPEL

VERSION=00104&TYPE=00018&SITE=9999999&RANG=099&CLE=1999888I&NUMQUESTION=1301733467&PORTEUR=4970100000008298&DATEQ=15022017

4.8.2 EXEMPLE DE REPONSE

NUMQUESTION=1301733467&SITE=9999999&RANG=099&CODEREPONSE=00000&COMMENTAIRE=OK&PAYS=FRA**&MARQUE=1&PRODUIT=E&LONGUEUR=16**

⇨ Le porteur possède une carte :
- D'un émetteur français : PAYS = FRA ○
  De marque CB uniquement : MARQUE =1 ○
  De catégorie commerciale : PRODUIT = E ○
  Le PAN est de longueur 16 : LONGUEUR = 16

4.9 NOUVELLES BALISES

4.9.1 SELECTION

Balise <SelectionIndicator> :

Les valeurs possibles sont :

- Default
- CardHolder

4.9.2 EMAIL PORTEUR

Balise <CustomerEmail> :

Format: 6 à 150 caractères. Les caractères « @ » et « . » doivent être présents.

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

Exemple : test@ca-ps.com

4.10 BALISE MISE A JOUR

3 nouvelles valeurs sont possibles afin d'indiquer la marque choisie :

- Maestro
- Electron
- Vpay

4.11 Variables réponse Gestion Automatisée des Encaissements

4.11.1 SITE

Format : 7 chiffres.

C'est le numéro de site (TPE) fourni par la Caisse Régionale de Crédit Agricole, écho de la variable transmise à l'appel. Exemple : 1999888

4.11.2 RANG

Format : 2 ou 3 chiffres

C'est le numéro de rang (ou « machine ») fourni par la Caisse Régionale de Crédit Agricole, écho de la variable transmise à l'appel.

Exemple : 01 ou 001

4.11.3 NUMQUESTION

Format : 10 chiffres (min : 0000000001 ; max : 2147483647).

Identifiant unique de la requête permettant d'éviter les confusions au niveau des réponses en cas de questions multiples et simultanées.
Chaque appel doit avoir un numéro de question unique sur une journée. Il pourra être réinitialisé chaque jour.
Echo de la variable transmise à l'appel.

Exemple : 0000000001

4.11.4 NUMAPPEL

Format : 10 chiffres

Numéro de la requête gérée sur la plateforme E-transactions

Exemple : 0000782653

4.11.5 NUMTRANS

Format : 10 chiffres

Numéro de la transaction créée sur la plateforme E-transactions

Exemple : 0000563149

4.11.6 AUTORISATION

Format : jusqu'à 10 caractères maximum (généralement 6 chiffres)

Numéro d'autorisation délivré par le centre d'autorisation de la banque du client final, si le paiement est accepté.

Exemple : 168753

4.11.7 CODEREPONSE

Format : 5 chiffres

Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue.
001xx	Paiement refusé par le centre d'autorisation. [voir ***§6.1 Codes réponses du centre d'autorisation***]. En cas d'autorisation de la transaction par le centre d'autorisation de la banque, le résultat "00100" sera en fait remplacé directement par "00000".
00002	Une erreur de cohérence est survenue.
00003	Erreur Plateforme.
00004	Numéro de porteur invalide.
00005	Numéro de question invalide.
00006	Accès refusé ou site / rang incorrect.
00007	Date invalide.
00008	Date de fin de validité incorrecte.
00009	Type d'opération invalide.
00010	Devise inconnue.
00011	Montant incorrect.
00012	Référence commande invalide.
00013	Cette version n'est plus soutenue.
00014	Trame reçue incohérente.
00015	Erreur d'accès aux données précédemment référencées.

00016	Abonné déjà existant (inscription nouvel abonné).
00017	Abonné inexistant.
00018	Transaction non trouvée (question du type 11).
00019	Réservé.
00020	Cryptogramme visuel non présent.
00021	Carte non autorisée.
00022	Plafond atteint
00023	Porteur déjà passé aujourd'hui
00024	Code pays filtré pour ce commerçant
00037	HMAC invalide
00097	Timeout de connexion atteint.
00098	Erreur de connexion interne.
00099	Incohérence entre la question et la réponse. Refaire une nouvelle tentative ultérieurement.

Exemple : 00007 (date invalide)

4.11.8 REFABONNE

Format : jusqu'à 250 caractères

Numéro d'abonné donné dans la trame question. Vide (zéros binaires) en contexte hors abonnement.

Exemple : AZERTY1234567

4.11.9 PORTEUR

Format : jusqu'à 19 caractères

Numéro porteur partiel (Token) rendu par la plateforme E-transactions lors de l'inscription ou de la modification d'un abonnement.

Exemple : 1111222233334444

4.11.10 COMMENTAIRE

Format : jusqu'à 100 caractères

Messages divers pour information (explications d'erreurs notamment).

Exemple : E-transactions + Gestion Automatisée des Encaissements

4.11.11 PAYS

Format : 3 caractères (code ISO3166 alphabétique)

Code pays du porteur de la carte. La valeur « ??? » sera retournée si le code pays est inconnu. Exemple : FRA

4.11.12 TYPECARTE

Format : jusqu'à 10 caractères

Type de carte utilisée pour le paiement

Exemple : VISA

PBX_TYPEPAIEMENT	PBX_TYPECARTE
CARTE	CB, VISA, EUROCARD_MASTERCARD, E_CARD
	MAESTRO
	AMEX
	DINERS
	JCB
	COFINOGA
	SOFINCO
	AURORE
	VPAY
	e-ANCV
PAYPAL	PAYPAL
CREDIT	UNEURO
	34ONEY
PREPAYEE	PSC
	IDEAL
	ONEYKDO
	MAXICHEQUE
	ILLICADO
LEETCHI	LEETCHI
PAYBUTTONS	PAYBUTTING
WALLET	PAYLIB

4.11.13 SHA-1

Format : 40 caractères (SHA-1 codé en hexadécimal)

Empreinte SHA-1 du N° de carte utilisé.

Exemple : F8BF2903A1149E682BE599C5C20788788256AA46

4.11.14 STATUS

Format : jusqu'à 32 caractères

Envoyé uniquement dans les questions de type 17.
Etat de la transaction. Les valeurs possibles sont :

- Annulé
- Autorisé
- Capturé
- Crédit,
- Refusé
- Demande de solde (pour les Cartes cadeaux)
- Crédit Annulé
- Rejet support

4.11.15 REMISE

Format : jusqu'à 9 chiffres.

Envoyé uniquement dans les questions de type 17.
Identifiant de la remise télécollectée.

Exemple : 509625890

4.12 Gestion Automatisée des Encaissements (précision sur la gestion des abonnements et par extension au paiement en un clic)

4.12.1 Principe

Lors de l'inscription d'un nouvel abonné (i.e. internaute ayant souscrit un abonnement sur le site du commerçant), le site du commerçant fournira à la plateforme les mêmes champs que pour une demande d'autorisation ainsi que la référence abonné (unique).

La plateforme vérifiera l'unicité de la référence abonné et effectuera sur la carte associée les différents contrôles de validité (expiration, liste noire …), ensuite elle effectuera une demande d'autorisation seule (sans débit). En cas de réponse positive du centre d'autorisation, ce nouvel abonné sera inscrit dans la liste des abonnés avec une partie du numéro porteur, l'autre partie du numéro porteur sera retournée au commerçant afin qu'il la conserve avec la référence abonné et la date de fin de validité carte.

La même opération sera effectuée pour la demande de modification d'un abonné.

Pour les opérations de débit, crédit, annulation et suppression d'un abonné, le commerçant devra fournir la référence abonné, la partie du N° porteur en sa possession et la date de fin de validité accompagnés des autres champs obligatoires dans le protocole d'échange Gestion Automatisée des Encaissements.

4.12.2 Fonctionnement

Pour toutes les demandes du type 51, 52, 53, 54, 55, 57 et 58 une inscription préalable de l'abonné est obligatoire § 4.1.4 TYPE. Pour cela, une trame avec le type d'opération 56 devra être envoyée vers notre serveur.

La création d'un nouvel abonné génère une demande d'autorisation, pour le montant précisé dans la trame, auprès de la banque, afin de s'assurer de la validité de la carte. En cas d'acceptation de la part de la banque, l'abonné sera créé au niveau de la base de données, gérée par la plateforme E-transactions, mais pas, dans le cas contraire.

A la suite de la création d'un abonné, il peut être envoyé directement une trame du type 52 (débit sur un abonné) si le montant précisé lors de la trame de création correspond au montant à débiter. S'il ne s'agit pas du même montant, il faudra alors émettre une trame d'autorisation + débit (53) ou une trame autorisation seule (51) suivi d'une trame débit (52).

Il est aussi possible de créer un nouvel abonné à partir d'**E-**transactions. Pour cela, il faut demander le champ « Référence de l'abonné » (U) dans PBX_RETOUR. La réponse **E-**transactions contiendra alors les 3 informations utiles : Numéro de carte partiel, date de fin de validité et CVV. Seules les 2 premières données doivent être conservées pour effectuer l'appel.

Pour plus d'informations, consultez le manuel d'intégration **E-**transactions.

5. 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, …).

5.1 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***

5.2 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.

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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.

6. ANNEXES

6.1 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 ***§4.11.7 CODEREPONSE***

6.1.1 Réseau Carte Bancaire, American Express et Diners

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès
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

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
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

6.1.2 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

6.1.3 Réseau Finaref

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
000	OK
101	Carte expirée. Porteur en validité dépassée
103	Commerçant inconnu. Identifiant de commerçant incorrect
110	Montant incorrect
111	Compte/porteur inconnu
115	Service non ouvert. Plafond nul. Code fonction/traitement inconnu
116	Provision insuffisante
117	1er ou 2ème code faux
119	Compte/Porteur avec statut bloqué. Compte/Porteur avec statut invalide. Carte bloquée
120	Commerçant invalide. Code monnaie incorrect. Compte non autorisé. Opération Commerciale inconnue/invalide
121	Plafond insuffisant
125	Carte non active
126	Code secret absent. Erreur de format de la date de début de contrôle ou des infos de sécurité
128	Erreur de contrôle de l'historique des codes faux
129	CVV2 faux
183	Compte / porteur invalide

184	Incohérence de date de validité avec fichier Porteurs en saisie manuelle
188	Mode de saisie invalide. Identification matériel incohérente
196	Problème d'accès fichiers
206	3ème code secret faux. Compteur de codes faux déjà à 3
207	Porteur en opposition (alors que statut carte=3)
208	Carte non parvenue. Carte volée. Usage abusif. Suspicion de fraude, Carte perdue
210	Incohérence de date de validité avec fichier porteurs en lecture piste ou puce.
	CVV faux
380	OK avec dépassement
381	OK avec augmentation capital
382	OK NPAI
385	Autorisation partielle

6.2 Jeu de caractères

Le jeu de caractères supporté par les applications E-transactions est présenté dans le tableau cidessous. 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

6.3 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

6.4 URL d'appel et Adresses IP

Pour utiliser les services Gestion Automatisée des Encaissements:

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-ppps.e-transactions.fr/PPPS.php
Production	https://ppps.e-transactions.fr/PPPS.php

L'adresse IP entrante est l'adresse sur laquelle le système d'information du Marchand va se connecter pour réaliser la transaction.
L'adresse IP sortante est l'adresse avec laquelle le système d'information du Marchand verra arriver les flux de retour en fin de transaction (appels de URL HTTP 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 systèmes d'information du Marchand.

PLATE-FORME	ADRESSE ENTRANTE	ADRESSE SORTANTE
Préproduction	195.101.99.73 (RedHat 5) 195.101.99.67 (CentOS 7)	N/A
Production	ppps.paybox.com/ppps0.paybox.com : 194.2.160.81 ppps.e-transactions.fr : • 194.2.160.89 (Rueil Malmaison) • 195.25.67.9 (Val de Rueil – GSLB) ppps1.paybox.com : 195.25.67.1 ppps2.paybox.com : 195.25.7.145 (sic) ppps1.e-transactions.fr : • 194.2.160.90 (Rueil Malmaison – GSLB) • 195.25.67.10 (Val de Rueil)	N/A

6.5 Exemples de trames Gestion Automatisée des Encaissements

Ci-dessous sont présentés, pour chacun des principaux types de demandes Gestion Automatisée des Encaissements, des exemples de trames requêtes et réponses.

6.5.1 Demande d'auto simple (NoShow : enregistrement de l'empreinte)

Les variables obligatoires sont en rouge.

Requête :

```
VERSION=00104&TYPE=00001&SITE=1999887&RANG=063&NUMQUESTION=0667392880&MONTANT=1
 000&DEVISE=978&REFERENCE=Test1&PORTEUR=1111222233334444&DATEVAL=0516&CVV=123&AC
 TIVITE=024&DATEQ=30012013&PAYS=&HASH=SHA512&HMAC=c5812341e2cafa5417420978adc1fd
 0606f78a827d96265142747606117a7983e758620e49e06801e3793c049475ef9a03878c0ffd7c6
24a9370b1ab3e7b450f
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres).

Réponse :

```
NUMTRANS=0005680492&NUMAPPEL=0010736923&NUMQUESTION=0667392880&SITE=1999887&RAN
G=63&AUTORISATION=XXXXXX&CODEREPONSE=00000&COMMENTAIRE=Demande traitée avec
succès&REFABONNE=&PORTEUR=
```

6.5.2 Capture (NoShow : capture totale ou partielle du montant initial)

Cette requête permet de « capturer » (confirmer) la transaction réalisée dans l'exemple précédent. Pour faire référence à la transaction, vous devez réutiliser les variables NUMTRANS et NUMAPPEL transmis lors de la réponse (surlignés en jaune).
Le montant peut être changé à condition de rester en dessous du montant initial

Les variables obligatoires sont en rouge.

Requête :

```
VERSION=00104&TYPE=00002&SITE=1999887&RANG=063&NUMQUESTION=0667392881&MONTANT=1
 000&DEVISE=978&REFERENCE=Test1&NUMAPPEL=0010736923&NUMTRANS=0005680492&DATEQ=30
 012013&PAYS=&HASH=SHA512&HMAC=8a5be4fa3fdc88d0c47e90a462c4fd95b884313c082d00c77
9930279fa5c9f179d4f8ad38756b6f9f8a6742e103a6467c25aa0b33615c3bf8b013b731919fba3
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres).

Réponse :

```
NUMTRANS=0005680492&NUMAPPEL=0010736923&NUMQUESTION=0667392881&SITE=1999887&RAN
G=63&AUTORISATION=XXXXXX&CODEREPONSE=00000&COMMENTAIRE=Demande traitée avec
succès&REFABONNE=&PORTEUR=
```

6.5.3 Remboursement

Pour faire référence à la transaction, vous devez réutiliser les variables NUMTRANS et NUMAPPEL transmis lors de la réponse (surlignés en jaune).

Les variables obligatoires sont en rouge.

Requête :

```
VERSION=00104&TYPE=00014&SITE=1999887&RANG=063&NUMQUESTION=0667392882&MONTANT=1
 000&DEVISE=978&REFERENCE=Test1&NUMAPPEL=0010736923&NUMTRANS=0005680492&ACTIVITE
 =024&DATEQ=30012013&PAYS=&HASH=SHA512&HMAC=aa0d5822b7631bab3f63ad9738d6955cbbc0
 bdeb7b6baaa566d68ab9b5b3e05d54ba011180633fbcf610a7d9cc46dd102529b356d8b489d752c
9d47658868643
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres).

Réponse :

```
NUMTRANS=0005680540&NUMAPPEL=0010736923&NUMQUESTION=0667392882&SITE=1999887&RAN
G=63&AUTORISATION=XXXXXX&CODEREPONSE=00000&COMMENTAIRE=Demande traitée avec
succès&REFABONNE=&PORTEUR=
```

6.5.4 Consultation

Cette requête permet de consulter l'état de la transaction dans le système E-transactions et de vous assurer ainsi de la cohérence par exemple, avec le statut enregistré dans votre SI.

Les variables obligatoires sont en rouge.

Requête :

```
VERSION=00104&TYPE=00017&SITE=1999887&RANG=063&NUMQUESTION=0667392883&MONTANT=1
 000&DEVISE=978&REFERENCE=Test1&NUMAPPEL=0010736923&NUMTRANS=0005680492&DATEQ=30
 012013&PAYS=&HASH=SHA512&HMAC=42daf73012efca2cebb1ce6c5eb4c1137e7d4ed7c99df2d52
831c21f99331e2f8181a95c88c1e1dfe8a4b17c6d37353d1766694e951ee4e26857b4fb30d4b581
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres).

Réponse :

```
NUMTRANS=0005680492&NUMAPPEL=0010736923&NUMQUESTION=0667392883&SITE=1999887&RAN
G=63&AUTORISATION=XXXXXX&CODEREPONSE=00000&COMMENTAIRE=Demande traitée avec
succès&REFABONNE=&PORTEUR=&STATUS=Remboursé
```

6.5.5 Création d'abonné (enregistrement d'une carte)

Cette requête permet d'enregistrer une carte sur la plateforme E-transactions. En réponse, la plateforme renvoie un token (champs PORTEUR) que vous pourrez utiliser pour débiter cette carte.

Les variables obligatoires sont en rouge.

Requête :

```
VERSION=00104&TYPE=00056&SITE=1999887&RANG=063&NUMQUESTION=0667392885&MONTANT=1
 000&DEVISE=978&REFERENCE=Test2&PORTEUR=1111222233334444&DATEVAL=0516&CVV=123&RE
 FABONNE=CLIENT&ACTIVITE=027&DATEQ=30012013&PAYS=&HASH=SHA512&HMAC=8e4bd0d9f1aa7
 b4d58b6d5754ab3caf57d29336dce838494989fa2cdb9a498fcbcf6670a54fadc7552ba2f5006a6
775fdd1ba392364536c5b0a6de7d3c07365a
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres).

Réponse :

```
NUMTRANS=0005680600&NUMAPPEL=0010737043&NUMQUESTION=0667392885&SITE=1999887&RAN
G=63&AUTORISATION=XXXXXX&CODEREPONSE=00000&COMMENTAIRE=Demande traitée avec
succès&REFABONNE=CLIENT&PORTEUR=SLDLrcsLMPC
```

6.5.6 Débit de l'abonné

Cette requête permet de débiter une carte précédemment enregistrée. La carte a pu être enregistrée par la solution E-transactions ou Gestion Automatisée des Encaissements, cela ne change pas l'appel pour débiter. Il faut transmettre le token (champs PORTEUR) précédemment généré à la place du numéro de carte (en bleu), et renseigner la date de validité de la carte.

Les variables obligatoires sont en rouge.

Requête :

```
VERSION=00104&TYPE=00053&SITE=1999887&RANG=063&NUMQUESTION=0667392902&MONTANT=1
 00&DEVISE=978&REFERENCE=Test3&PORTEUR=SLDLrcsLMPC&DATEVAL=0516&REFABONNE=CLIENT
 &ACTIVITE=027&DATEQ=30012013&PAYS=&HASH=SHA512&HMAC=49e019906884dfca1f04d1cb843
 e07c4f8ab41416b605489ae41bcb2337a75dcddf2cc5fd21de3a75757a66222fb0d887659cfa5bc
9099a012a1506747ea3bd6
```

Pour rejouer ce formulaire après une tentative réussie, il faudra incrémenter la variable NUMQUESTION car celle-ci doit être unique par journée (Format : 10 chiffres).

Réponse :

```
NUMTRANS=0005680706&NUMAPPEL=0010737169&NUMQUESTION=0667392902&SITE=1999887&RAN
G=63&AUTORISATION=XXXXXX&CODEREPONSE=00000&COMMENTAIRE=Demande traitée avec
succès&REFABONNE=CLIENT&PORTEUR=SLDLrcsLMPC
```

6.6 Glossaire

6.6.1 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.

6.6.2 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.

6.6.3 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.

6.6.4 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.

6.6.5 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).

6.6.6 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.

6.6.7 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

6.6.8 URL encodée

Tous les caractères ne sont pas autorisés dans les URL (voir la définition de URL ci-dessus). 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.

6.6.9 MPADS

Sigle de Manuel de Paiement A Distance Sécurisé rédigé par le GCB (Groupement des cartes bancaires), il s'agit des règles définissants le fonctionnement attendu d'une solution de paiement Ecommerce européenne. La version 5.5 s'attache en particulier à l'implémentation des MIF.

6.6.10 MIF

Acronyme de Multilateral Interchange Fees, il s'agit d'une commission payée par la banque acquéreur du marchand à la banque émettrice de la carte. Le montant de la commission d'interchange varie selon la marque et la catégorie de carte (commerciale, crédit, débit…).

Ce montant varie aussi selon que le paiement est transfrontalier ou domestique.

6.6.11 Exemple PHP avec la lib Curl

Cet exemple utilise la lib curl afin d'effectuer les appels HTTPS de type POST. Elle doit être installée sur votre environnement de développement (Cf. http://php.net/manual/fr/book.curl.php).

```php
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>Test Paybox direct</title>
</head>
<body>
<h1>Test Paybox direct</h1>
<?php

// initialisation de la session https
$curl = curl_init('https://preprod-ppps.paybox.com/PPPS.php');

// Précise que la réponse est souhaitée
curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);

// Présise que le session est nouvelle
curl_setopt($curl, CURLOPT_COOKIESESSION, true);

$postfields = array(
'VERSION'     => '00104',
'TYPE'        => '00001',
'SITE'        => '1999888',
'RANG'        => '32',
'IDENTIFIANT' => '107904482',
'CLE'         => '1999888I',

'NUMQUESTION' => '0000000010',
'MONTANT'     => '1000',
'DEVISE'      => '978',
'REFERENCE'   => 'Hello World',

'PORTEUR'     => '1111222233334444',
'DATEVAL'     => '1214',
'CVV'         => '123',

'DATEQ'       => '15102013'
);

// Crée la chaine url encodée selon la RFC1738 à partir du tableau de paramètres séparés par
$trame = http_build_query($postfields, '', '&');

// Présise le type de requête HTTP : POST
curl_setopt($curl, CURLOPT_POST, true);

// Présise le Content-Type
curl_setopt($curl,CURLOPT_HTTPHEADER, array('Content-Type: application/x-www-form-urlencoded

// Ajoute les paramètres
curl_setopt($curl, CURLOPT_POSTFIELDS, $trame);

// Envoi de la requête et obtention de la réponse
$response = curl_exec($curl);

echo "<PRE>";
echo "Réponse Paybox direct pour la demande 'autorize' ";
var_dump($response);
```

```
58 echo "</PRE>";
59
60 // fermeture de la session
61 curl_close($curl);
62
63 ?>
64 </body>
65 </html>
```