



E-transactions

MANUEL D'INTEGRATION

Remote MPI

VERSION DU

14/09/2015



E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

REFERENCES DOCUMENTATIONS

La plupart des documentations référencées ci-dessous sont téléchargeables sur le site Web <https://e-transactions.aveo-groupe.com>

REF.	DOCUMENT	DESCRIPTION
Ref 1	Manuel Intégration E-transactions	Manuel d'intégration de la solution E-transactions
Ref 2	Paramètres Test E-transactions	Manuel décrivant les environnements et paramètres de tests (pré-production).
Ref 3	Manuel Intégration Gestion Automatisée des Encaissements	Manuel d'intégration de la solution Gestion Automatisée des Encaissements

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

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	2
2. PRESENTATION DE LA SOLUTION « REMOTE MPI »	3
2.1 LE MPI ET 3-D SECURE	3
2.2 LISTE DES MOYENS DE PAIEMENT PRIS EN CHARGE PAR LE REMOTE MPI	4
2.3 SECURITE	4
3. PROTOCOLE D'ECHANGE	4
3.1 APPEL	4
3.2 REPONSE	5
4. CINEMATIQUE D'UN PAIEMENT 3-D SECURE AVEC GESTION AUTOMATISEE DES ENCAISSEMENTS	6
5. DICTIONNAIRE DE DONNEES	9
5.1 VARIABLES D'APPEL E-TRANSACTIONS REMOTE MPI	10
5.2 VARIABLES REPONSES E-TRANSACTIONS REMOTE MPI	12
6. ANNEXES	15
6.1 CODES ERREUR	15
6.2 URL D'APPEL ET ADRESSES IP	26
6.3 GLOSSAIRE	27
6.4 3D-SECURE	27

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

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.

- **Gestion Automatisée des Encaissements** est utilisée pour valider les encaissements des transactions préalablement autorisées via **E-transactions**, assurer des remboursements et annulations de serveur à serveur.
- **Gestion Automatisée des Encaissements** 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 **Gestion Automatisée des Encaissements** 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.

Le but de ce document est de décrire comment intégrer 3-D Secure pour le service **E-transactions**

La cinématique 3-D Secure mise en œuvre en amont de la demande d'autorisation permet de l'enrichir des informations d'authentification du porteur, dans le cadre d'un contrat de Vente A Distance Sécurisée.

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

2. PRESENTATION DE LA SOLUTION « REMOTE MPI »

2.1 Le MPI et 3-D Secure

Le MPI (**Merchant-Plug-In**) est un composant installé sur les serveurs E-transactions. Il permet l'authentification des 3 intervenants de la transaction (Commerçant, Client Acheteur, Banques) à travers un ensemble de dialogues dans le cadre du programme 3-D Secure.

C'est le même composant qui est intégré au service **E-transactions** et qui offre le service 3-D Secure par le biais d'un navigateur.

Ce dialogue est réalisé selon des spécifications VISA et MASTERCARD et se décompose en 2 échanges :

- 1) Un premier échange vérifie sur les Directory Serveurs VISA et MASTERCARD que la carte du porteur fait partie du programme 3-D Secure (porteur dit « enrôlé »).

Les messages sont le **VEReq** (Verify Enrollment Request) et le **VERes** (Verify Enrollment Response).

- 2) Si la carte fait partie du programme 3-D Secure, un deuxième échange redirige le porteur vers le site d'authentification de la banque émettrice de la carte.

Les messages sont le **PAReq** (Payer Authentication Request) et le **PARes** (Payer Authentication Response).

Le résultat de ces échanges permettra ou non de poursuivre le paiement avec un appel au service **E-transactions**.

La conception du module 'Remote MPI' a été prévue pour répondre à 2 critères :

Rester fidèle aux spécifications VISA et MASTERCARD

Les données en réponse sont celles fournies par le MPI et retournées au format défini dans les spécifications VISA et MASTERCARD.

Faciliter l'intégration avec les interfaces E-transactions existantes

Les données 3-D Secure nécessaires à la demande d'autorisation sont stockées sur notre plateforme.

Un unique identifiant de contexte retourné par E-transactions à la fin de la session 3-D Secure est réintroduit au niveau des interfaces **Gestion Automatisée des Encaissements** existantes et permet de récupérer toutes les informations d'authentification 3-D Secure du paiement en cours.

- ❗ Cet identifiant de contexte ne concerne que les données d'authentification 3-D Secure. Il reste tout de même nécessaire de renseigner en plus, les paramètres obligatoires et existants du service **Gestion Automatisée des Encaissements** (cf. **Ref 3 Manuel Intégration Gestion Automatisée des Encaissements**).

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

2.2 Liste des moyens de paiement pris en charge par le Remote MPI

CB VISA MASTERCARD

2.3 Sécurité

2.3.1 Identification

Un site Marchand est référencé auprès de nos serveurs par plusieurs éléments :

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

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 Marchand enverra à nos plateformes de paiement.

3. PROTOCOLE D'ECHANGE

3.1 Appel

C'est un CGI installé sur nos serveurs qui donne l'accès au MPI E-transactions. Ce CGI peut être appelé via les URL :

<https://tpeweb.e-transactions.fr/cgi/RemoteMPI.cgi>

Pour réaliser l'authentification porteur, il faut rediriger le client sur cette URL, en envoyant les paramètres par la méthode POST. La liste des paramètres est détaillée dans le paragraphe §5 **Dictionnaire de données**

Exemple d'appel via un formulaire HTML :

```
<html>
<body>

<form action="https://preprod-tpeweb.e-transactions.fr/cgi/RemoteMPI.cgi" method="post">

<input name="IdMerchant" value="109518543" type="hidden">
<input name="IdSession" value="DOC001" type="hidden">
<input name="Amount" value="1000" type="hidden">
<input name="Currency" value="978" type="hidden">
<input name="CCNumber" value="111122233334444" type="hidden">
<input name="CCExpDate" value="1014" type="hidden">
<input name="CVVCode" value="123" type="hidden">
<input name="URLRetour" value="https://maboutique.com/retour.php" type="hidden">
<input name="URLHttpDirect" value="https://maboutique.com/retourDirect.php" type="hidden">

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

3.2 Réponse

Les données de retour se décomposent en 2 ensembles.

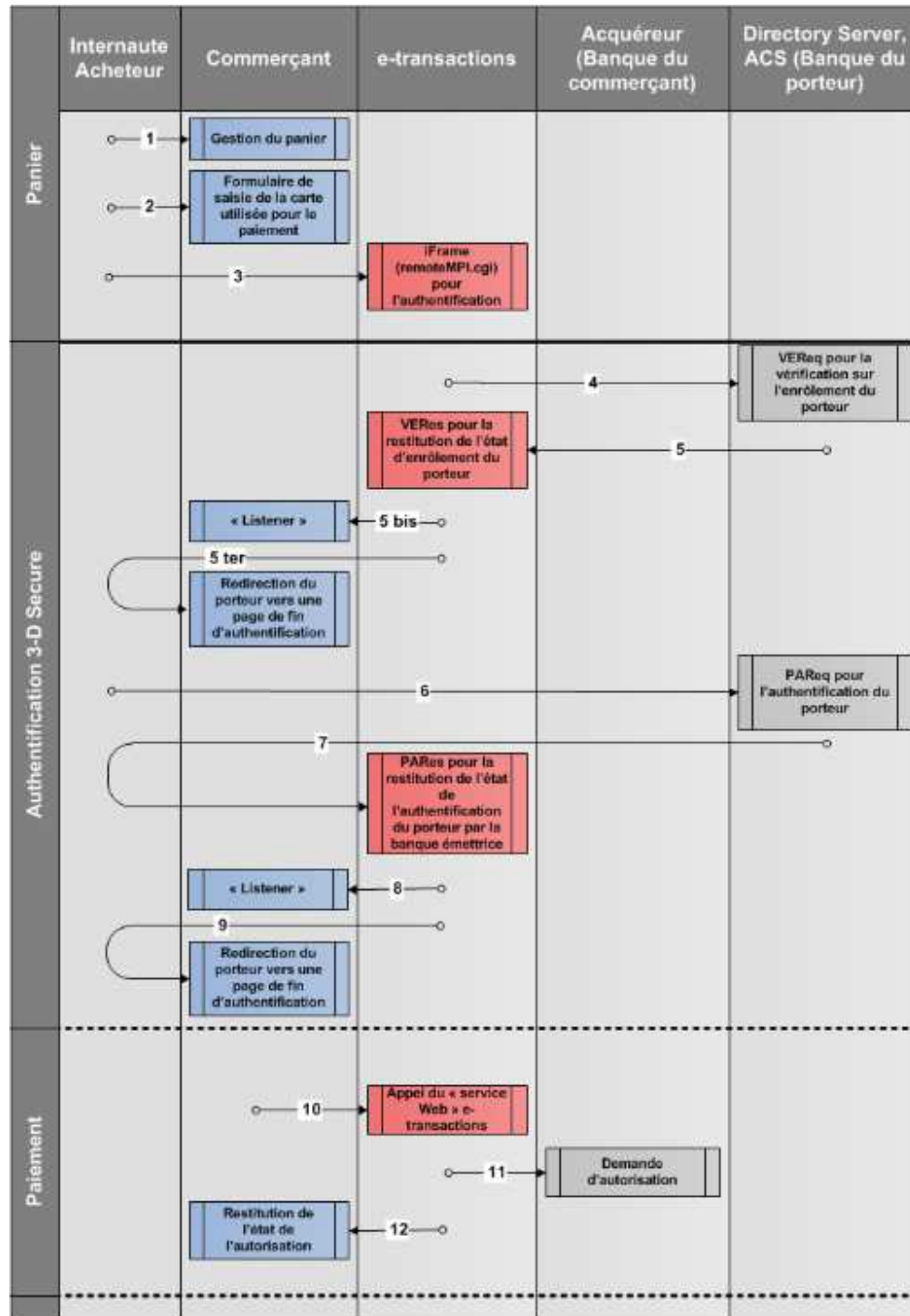
- Les données utiles à l'intégration.
 - o ID3D
 - o StatusPBX
 - o Check
- Les données 3-D Secure en sortie du MPI, présentes à titre informatif.

Si la variable StatusPBX a la valeur « **Autorisation à faire** », vous pouvez émettre une demande d'autorisation avec [Gestion Automatisée des Encaissements](#).

Pour faire référence à l'authentification 3D-Secure, vous devez aussi récupérer le contenu de la variable ID3D en retour de RemoteMPI et transmettre cette variable dans la requête [Gestion Automatisée des Encaissements](#).

- ! L'appel [Gestion Automatisée des Encaissements](#) doit être fait immédiatement après le retour du MPI. Passé un délai de 5 minutes, l'authentification sera considérée « expirée » et la plateforme n'effectuera pas la demande d'autorisation en mode 3-D Secure.
- ! Dans le cas d'un mauvais passage de paramètres au CGI, seuls les champs IdSession, StatusPBX et Check sont renvoyés.

4. CINEMATIQUE D'UN PAIEMENT 3-D SECURE AVEC GESTION AUTOMATISEE DES ENCAISSEMENTS



E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

ETAPE	IMPACT COMMERCANT	DESCRIPTION
1	Oui	L'acheteur passe une commande sur le site Web du commerçant.
2	Oui	L'acheteur saisit ses informations carte (PAN, date d'expiration, cryptogramme visuel) sur le site Web du commerçant.
3	Oui	Le commerçant redirige l'acheteur vers une URL E-transactions en vue de son authentification «3-D Secure».
4	Non	Demande de vérification de l'enrôlement du porteur auprès des Directories Servers de Visa et MasterCard.
5	Non	Récupération de l'état sur l'enrôlement du porteur et de l'URL de redirection du porteur vers sa banque.
5 bis	Oui	<p>Cette étape se produit uniquement dans les 3 cas de figure ci-dessous :</p> <p>1) Erreur d'accès au MPI 2) Erreur pendant la transmission du VEReq/VERes Pour les cas 1) et 2) :</p> <p style="text-align: center;">L'identifiant de contexte ID3D n'est pas renseigné.</p> <p style="text-align: center;">Une demande d'autorisation non 3-D Secure peut tout de même être effectuée en appelant les interfaces Gestion Automatisée des Encaissements, sans le paramètre ID3D.</p> <p>3) Le porteur n'est pas enrôlé</p> <p style="text-align: center;">L'identifiant de contexte ID3D est renseigné.</p> <p style="text-align: center;">Une demande d'autorisation non 3-D Secure peut tout de même être effectuée en appelant les interfaces Gestion Automatisée des Encaissements avec le paramètre ID3D.</p> <p>Les étapes 6 à 9 ne sont pas présentes dans la cinématique. Le porteur est alors redirigé vers une page du site Web du commerçant.</p>
5 ter	Oui	<p>En cas de non enrôlement du porteur au programme 3-D Secure, ce dernier est redirigé vers une page du site Web du commerçant.</p> <p>Etape présente uniquement en cas de non enrôlement du porteur et les étapes 6 à 9 ne sont pas présentes dans la cinématique.</p>
6	Non	Redirection du porteur vers sa banque en vue de son authentification.
7	Non	Récupération de l'état sur l'authentification du porteur par sa banque.
8	Oui	<p>Notification (appel serveur à serveur) sur l'état de l'authentification du porteur et sur la suite à donner pour la demande d'autorisation.</p> <p>Si le porteur n'est pas authentifié la demande d'autorisation n'est pas à faire auprès de la banque acquéreur.</p>
9	Oui	Quel que soit l'état de l'authentification du porteur, ce dernier est redirigé vers une page du site Web du commerçant.
10	Oui	Appel du « service Web » pour la demande d'autorisation auprès de la banque du commerçant.

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

		<p>Les informations sur l'état de l'authentification du porteur sont stockées sur la plateforme pendant 5 minutes sous l'identifiant ID3D.</p> <p>L'identifiant de contexte ID3D est donc à renseigner lors de l'appel aux interfaces Gestion Automatisée des Encaissements, en plus des paramètres de bases.</p> <p>A partir de cette étape, les actions sont totalement désynchronisées des précédentes.</p>
11	Non	Demande d'autorisation faite par la plateforme auprès de l'acquéreur.
12	Oui	Restitution de l'état de la demande d'autorisation dans la même session de connexion que l'étape 10.

5. DICTIONNAIRE DE DONNEES

L'ensemble des variables d'interface est résumé dans le tableau suivant.

VARIABLE	QUESTION	REPOSE	RESUME
Amount	X		Montant de la demande d'autorisation
CCExpDate	X		Date d'expiration de la carte
CCNumber	X		Numéro de carte
Currency	X		Devise
CVVCode	X		Cryptogramme visuel
IdMerchant	X		Identifiant commerçant fourni par
IdSession	X	X	Identifiant de session unique
URLHttpDirect	X		URL de retour serveur à serveur
URLRetour	X		URL de retour depuis le navigateur du client
3DCAVV		X	Valeur reçue des ACS
3DCAVVALGO		X	Identifiant de l'algorithme ayant servi à l'identification du porteur sur l'ACS
3DECI		X	E-Commerce Indicator
3DENROLLED		X	Etat de l'enrôlement du porteur
3DERROR		X	Erreur renvoyée par le MPI
3DSIGNVAL		X	Statut de la vérification de la signature du porteur
3DSTATUS		X	Statut de la demande d'authentification
3DXID		X	Référence provenant du MPI
Check		X	Signature E-transactions
ID3D		X	Identifiant de contexte E-transactions
StatusPBX		X	Statut de la demande d'authentification

Tableau 1 : Liste des variables E-transactions Remote MPI

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

5.1 Variables d'appel E-transactions Remote MPI

5.1.1 Amount

Format : Numérique. **Obligatoire.**

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

- ⚠ Vous devez obligatoirement définir le même montant pour la demande d'authentification Remote MPI et pour la demande d'autorisation Gestion Automatisée des Encaissements.

Exemple : pour 19€90 :

- 0000001990
-

Equivalent Gestion Automatisée des Encaissements : MONTANT

5.1.2 CCExpDate

Format : Date (MMAA) **Obligatoire.**

Date de fin de validité de la carte.

Exemple : 1213 (décembre 2013)

Equivalent Gestion Automatisée des Encaissements : DATEVAL

5.1.3 CCNumber

Format : 19 caractères. **Obligatoire.**

Numéro de carte du porteur (client) sans espace.

Exemple : 1111222233334444

Equivalent Gestion Automatisée des Encaissements : PORTEUR

5.1.4 Currency

Format : 3 chiffres. **Obligatoire.**

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

Exemples :

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

- ⚠ Seul l'€ est proposé sur E-transactions.

Equivalent à Gestion Automatisée des Encaissements : DEVISE

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

5.1.5 CVVCode

Format : 3 ou 4 caractères. **Obligatoire pour les questions de type 1, 3, 4, 12.**

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

Equivalent Gestion Automatisée des Encaissements : CVV

5.1.6 IdMerchant

Format : Numérique. **Obligatoire.**

Identifiant du commerçant fourni lors de la souscription.

Exemple : 2

5.1.7 IdSession

Format : jusqu'à 250 caractères. **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 pour un commerçant donné.

Exemple : Session001

5.1.8 URLHttpDirect

Format : jusqu'à 250 caractères.

URL de retour de serveur à serveur. Si l'URL n'est pas présente, la plateforme utilisera celle paramétrée sur la fiche site du commerce.

Exemple : <http://maboutique.com/retourMPI.php>

5.1.9 URLRetour

Format : jusqu'à 250 caractères.

URL de retour depuis le navigateur du client. Si l'URL n'est pas présente, la plateforme utilisera celle paramétrée sur la fiche site du commerce (équivalent à PBX_EFFECTUE).

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

5.2 Variables réponses E-transactions Remote MPI

5.2.1 IdSession

Format : jusqu'à 250 caractères.

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 pour un commerçant donné.

Exemple : Session001

5.2.2 StatusPBX

Format : Alphanumérique.

Statut de la demande d'authentification (voir la liste des valeurs possibles dans le tableau ci-après).

Il conditionne l'appel en autorisation effectué via le produit Gestion Automatisée des Encaissements

STATUSPBX	DESCRIPTION
Erreur	Envoyé dans le cas d'un incident propre aux traitements de la plateforme. L'authentification du porteur a échoué et la demande d'autorisation ne doit pas être effectuée. Il faut recommencer la demande d'authentification.
Autorisation à faire	Envoyé après la procédure d'authentification indiquant que le paiement pourra être réalisé après une demande d'autorisation.
Autorisation à ne pas faire	Envoyé après la procédure d'authentification indiquant que le paiement ne pourra pas être réalisé avec succès et qu'une demande d'autorisation ne doit pas être effectuée car l'authentification du porteur a échoué.
Timeout	Envoyé lorsqu'il n'y a pas eu de retour du porteur, après la demande d'authentification au-delà de 5 minutes.

5.2.3 ID3D

Format : jusqu'à 20 chiffres.

Identifiant de contexte E-transactions contenant les données d'authentification retournées par le MPI.

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

Au-delà, les applications considéreront que la phase d'authentification du porteur est non valide

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

car en timeout.

Exemple : 9900000000012

5.2.4 Check

Format : jusqu'à 256 caractères.

Signature électronique de E-transactions sur l'ensemble des données passées en paramètre

Voir aussi : **Ref 1 Manuel Intégration E-transactions** pour les détails sur le calcul de la signature

5.2.5 3DCAVV

Format : 28 caractères.

Valeur reçue des ACS. URL-encodé.

5.2.6 3DCAVVALGO

Format : jusqu'à 64 caractères

Identifiant de l'algorithme ayant servi à l'identification du porteur sur l'ACS

Exemple : 0000000001

5.2.7 3DECI

Format : 2 chiffres

E-Commerce Indicator. Permet de connaître le niveau de sécurisation de la transaction.

5.2.8 3DENROLLED

Format : 1 caractère

État sur l'enrôlement du Porteur au programme 3DS

Valeurs possibles :

- Y : Carte/Porteur enrôlée
- N : Carte/Porteur non enrôlée
- U : Erreur

5.2.9 3DERROR

Format : jusqu'à 6 caractères

Numéro d'erreur renvoyé nativement par le MPI.

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

Voir aussi : §6.1.2 *Codes erreur retournés par* le MPI

5.2.10 3DSIGNAL

Format : 1 caractère.

Généré par le MPI, il indique le statut de la vérification de la signature du porteur (Y, N)

Valeurs possibles : Y ou N

5.2.11 3DSTATUS

Format : 1 caractère.

Statut de la demande d'authentification (Y, N, A, U)

Valeurs possibles :

- Y : Porteur authentifié
- N : Porteur non authentifié
- A : Forçage de l'authentification par l'émetteur
- U : Authentification n'a pas pu être réalisée pour raison technique

5.2.12 3DXID

Format : jusqu'à 28 caractères

Référence provenant du MPI

Exemple : 1111222233334444

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

6. ANNEXES

6.1 Codes erreur

6.1.1 Codes erreur du programme Remote MPI

Le CGI vérifie l'ensemble des paramètres envoyés et affiche en cas d'anomalie un numéro d'erreur (Voir tableau ci-dessous).

Ce N° d'erreur concerne le traitement RemoteMPI et non l'exécution du contrôle 3DS par le MPI.

Il n'y a pas de vérification sur la validité des URLs (URLRetour et URLHttpDirect)

CODE	SIGNIFICATION
1	Erreur accès au fichier de configuration (interne E-transactions)
2	Erreur accès aux paramètres de connexions à la base de données
3	Erreur de récupération des variables d'environnement locales
4	Erreur de récupération du chemin d'accès au MPI (MPI_PATH)
5	Erreur de connexion à la base de données
6	Erreur de préparation de la recherche du site (fsite)
7	Erreur de préparation de la recherche des transactions MPI (TransMPI)
101	Erreur absence montant (Amount)
102	Erreur absence date expiration (CCExpdate)
103	Erreur absence numéro de porteur (CCNumber)
104	Erreur absence devise (Currency)
105	Erreur absence identifiant marchand (IdMerchant)
106	Erreur absence identifiant session marchand (IdSession)
107	Erreur absence référence marchand (RefMarchand)
108	Erreur absence identifiant transMPI
110	Erreur taille numéro de porteur
111	Erreur type numéro de porteur
112	Erreur type montant
113	Erreur taille référence marchand
114	Erreur taille date expiration
115	Erreur type date expiration
116	Erreur valeur date expiration
117	Erreur longueur CVV (optionnel)
118	Erreur longueur identifiant TransMPI retourné par MPI
201	Erreur de recherche du site
202	Erreur de recherche dans TransMPI
301	Erreur ajout enregistrement TransMPI
401	Erreur de taille de la référence marchand reçue du MPI
402	Erreur de taille du code erreur du MPI
403	Erreur de taille du XID reçu du MPI
410	Erreur absence de la référence marchand reçue du MPI
411	Erreur de type de la référence marchand
412	Erreur de type du code erreur

Tableau 2 : Codes réponses du programme Remote MPI

6.1.2 Codes erreur retournés par le MPI

Ces codes sont présents dans la variable 3DERROR

CODE	SIGNIFICATION
0	No Error
100	AuthReq received is invalid
101	Merchant is not known
102	Merchant is not active
103	invalid referrer
104	An error occurred during processing
105	Currency is not supported
106	Transaction not found
107	Brand is not supported
108	The validation post to the merchant failed
1300	the HTTP return code is not found
1301	the HTTP return code is not valid
1302	the received message contains no XML
1303	not possible to import the xml in JDOM
1304	incorrect root element
1305	the element message is not defined
1306	the attribute id is not defined for
1307	the attribute id is not defined for Extension
1308	the attribute id and critical are not defined for Extension
1309	the attribute critical is not defined for Extension
1310	the element Extension is not correct
1311	the element version is not found
1312	the version of the ThreeDSecureMessage is too old
1313	the attribute critical is defined for Extension with value true
1314	Root element invalid
1315	Message element not found or invalid
1330	CRReq - the element Merchant is not found
1331	CRReq - the element acqBIN is not found
1332	CRReq - the element merID is not found
1333	CRReq - the element password is not found

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1334	CRReq - the element CRReq is not found
1335	CRReq - the element version is not valid
1336	CRReq - the element Merchant.acqBIN is not valid
1337	CRReq - the element Merchant.merID is not valid
1338	CRReq - the element Merchant.password is not valid
1339	CRReq - the element serialNumber is not valid
1350	CRRes - the element begin is not found
1351	CRRes - the element end is not found
1352	CRRes - the element action is not found
1353	CRRes - the element CRRes is not found
1354	CRRes - the element serialnumber is not found
1355	CRRes - the element version is not valid
1356	CRRes - the element begin is not valid
1357	CRRes - the element end is not valid
1358	CRRes - the element action is not valid
1359	CRRes - the element serialNumber is not valid
1360	CRRes - the element vendorcode is too long
1361	CRRes - the element iReqCode is not found
1362	CRRes - the element IReqCode has bad format
1401	VEReq - the element pan is not found
1402	VEReq - the element Merchant is not found
1403	VEReq - the element acqBIN is not found
1404	VEReq - the element merID is not found
1405	VEReq - the element password is not found
1406	VEReq - the element VEReq is not found
1407	VEReq - the element version is not valid
1408	VEReq - the element pan is not valid
1409	VEReq - the element Merchant.acqBIN is not valid
1410	VEReq - the element Merchant.merID is not valid
1411	VEReq - the element Merchant.password is not valid
1412	VEReq - the element Merchant.password is not valid
1501	VERes - the element VERes is not found
1502	VERes - the element version is not valid
1503	VERes - the element enrolled is not valid

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1504	VERes - the element acctId is empty
1505	VERes - the element acctId is too long
1506	VERes - the element url is empty
1507	VERes - the element url has a bad protocol
1508	VERes - the element url is malformed
1509	VERes - the element protocol is empty
1510	VERes - the element protocol is not valid
1511	VERes - the element vendorcode is too long
1512	VERes - the element CH is not found
1513	VERes - the element enrolled is not found
1514	VERes - the element acctId is not found
1515	VERes - the element url is not found
1516	VERes - the element protocol is not found
1517	VERes - the element IReq is not found
1518	VERes - the element iReqCode is not found
1519	VERes - the element IReqCode has bad format
1520	VERes - the element acctId is the same as the pan
1601	PAReq - the element version is not valid
1602	PAReq - the element PAReq is not found
1603	PAReq - the element Merchant is not found
1604	PAReq - the element acqBIN is not found
1605	PAReq - the element merID is not found
1606	PAReq - the element name is not found
1607	PAReq - the element country is not found
1608	PAReq - the element url is not found
1609	PAReq - the element Purchase is not found
1610	PAReq - the element xid is not found
1611	PAReq - the element date is not found
1612	PAReq - the element amount is not found
1613	PAReq - the element purchAmount is not found
1614	PAReq - the element currency is not found
1615	PAReq - the element exponent is not found
1616	PAReq - the element frequency is not found
1617	PAReq - the element endRecur is not found

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1618	PAReq - the element CH is not found
1619	PAReq - the element CH.acctID is not found
1620	PAReq - the element CH.expiry is not found
1621	PAReq - the element Merchant.acqBIN is not valid
1622	PAReq - the element Merchant.merID is not valid
1623	PAReq - the element Merchant.name is not valid
1624	PAReq - the element Merchant.country is not valid
1625	PAReq - the element Merchant.url is not valid
1626	PAReq - the element url is empty
1627	PAReq - the element url has a bad protocol
1628	PAReq - the element url is malformed
1629	PAReq - the element xid has bad format
1630	PAReq - the element date has bad format
1631	PAReq - the element amount has bad format
1632	PAReq - the element purchAmount has bad format
1633	PAReq - the element currency has bad format
1634	PAReq - the element exponent has bad format
1635	PAReq - the element desc has bad format
1636	PAReq - the element frequency has bad format
1637	PAReq - the element endRecur has bad format
1638	PAReq - the element install has bad format
1639	PAReq - the element acctID has bad format
1640	PAReq - the element expiry has bad format
1641	PAReq - the element exponent is not numeric
1642	PAReq - the element gmtOffset is not found
1643	PAReq - the element brands is not found
1644	PAReq - the element desc is not found
1645	PAReq - the element pan is not found
1646	PAReq - the element gmtOffset is not valid
1647	PAReq - the element brands is not valid
1648	PAReq - the element recurring is not valid
1649	PAReq - the element installment is not valid
1701	PARes - the element PARes is not found
1702	PARes - the element version is not valid

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1703	PARes - the element Merchant.acqBIN is not valid
1704	PARes - the element Merchant.merID is not valid
1705	PARes - the element xid has bad format
1706	PARes - the element date has bad format
1707	PARes - the element amount has bad format
1708	PARes - the element purchAmount has bad format
1709	PARes - the element currency has bad format
1710	PARes - the element exponent has bad format
1711	PARes - the element exponent is not numeric
1712	PARes - the element TX.time is not valid
1713	PARes - the element TX.status is not valid
1714	PARes - the element pan is not valid
1715	PARes - the element TX.cavv is not valid
1716	PARes - the element TX.eci is not valid
1717	PARes - the element TX.cavvAlgorithm is not valid
1718	PARes - the element IReq.iReqCode is not valid
1719	PARes - the element IReq.vendorCode is not valid
1720	PARes - the element desc is not valid
1721	PARes - the element CH.exp is not valid
1722	PARes - the element TX.detail is not valid
1723	PARes - the element TX.stain is not valid
1724	PARes - the element TX.vendorCode is not valid
1725	PARes - the element TX.eci is not valid
1726	PARes - the element Merchant is not found
1727	PARes - the element acqBIN is not found
1728	PARes - the element merID is not found
1729	PARes - the element Purchase is not found
1730	PARes - the element xid is not found
1731	PARes - the element date is not found
1732	PARes - the element purchAmount is not found
1733	PARes - the element currency is not found
1734	PARes - the element exponent is not found
1735	PARes - the element pan is not found
1736	PARes - the element tx is not found

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1737	PARes - the element time is not found
1738	PARes - the element status is not found
1739	PARes - the element cavv is not found
1740	PARes - the element eci is not found
1741	PARes - the element cavvAlgorithm is not found
1742	PARes - the element iReqCode is not found
1743	PARes - the element Purchase.currency has not the same value as the one in the PARes
1744	PARes - the element Purchase.exponent has not the same value as the one in the PARes
1745	the Signature.xmlns namespace is not found
1746	the Signature.xmlns namespace has a bad format
1747	the Signature.SignedInfo has a bad format
1748	the Signature.CanonicalizationMethod has a bad format
1749	the Signature.CanonicalizationMethod has different namespace
1750	the Signature.SignatureMethod has a bad format
1751	Signature.SignatureMethod has different namespace
1752	Signature.SignedInfo.Reference.URI not found
1753	Signature.SignedInfo.Reference.URI has a bad format
1754	Signature.SignedInfo.Reference.DigestValue not found
1755	Signature.SignatureValue not found
1756	Signature.KeyInfo not found
1801	Error - the element Error is not found
1802	Error - the element version is not valid
1803	Error - the element errorCode is not valid
1804	Error - the element errorMessage is empty
1805	Error - the element errorDetail is empty
1806	Error - the element vendorCode is too long
1807	Error - the element errorCode is not found
1808	Error - the element errorMessage is not found
1809	Error - the element errorDetail is not found
1901	PATransReq - the element PATransReq is not found
1902	PATransReq - the element version is not valid
1903	PATransReq - the element Merchant.name is not valid
1904	PATransReq - the element Merchant.country is not valid

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1905	PATransReq - the element Merchant.url is not valid
1906	PATransReq - the element amount is not found
1907	PATransReq - the element url is empty
1908	PATransReq - the element url has a bad protocol
1909	PATransReq - the element url is malformed
1910	PATransReq - the element amount has bad format
1911	PATransReq - the element desc has bad format
1912	PATransReq - the element frequency has bad format
1913	PATransReq - the element endRecur has bad format
1914	PATransReq - the element install has bad format
1915	PATransReq - the element date has bad format
1916	PATransReq - the element name has bad format
1917	PATransReq - the element fullpan has bad format
1918	PATransReq - the element expiry has bad format
1919	PATransReq - the element acs Id id has bad format
1920	PATransReq - the element login Id has bad format
1921	PATransReq - the element password has bad format
1922	PATransReq - the element signed pares has bad format
1925	PATrans - the element version is not valid
1926	PATrans - the element PATransReq is not found
1927	PATrans - the element Merchant.id is not found
1928	PATrans - the element Merchant.name is not valid
1929	PATrans - the element Merchant.country is not valid
1930	PATrans - the element Merchant.url is not valid
1931	PATrans - the element Purchase.id is not found
1932	PATrans - the element Purchase.xid is not found
1933	PATrans - the element Purchase.date is not valid
1934	PATrans - the element Purchase.amount is not valid
1935	PATrans - the element Purchase.rawamount is not valid
1936	PATrans - the element Purchase.currency is not valid
1937	PATrans - the element Purchase.desc is not valid
1938	PATrans - the element Purchase.recurring is not valid
1939	PATrans - the element Purchase.installment is not valid
1940	PATrans - the element CH.name is not valid

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

1941	PATrans - the element CH.pan is not valid
1942	PATrans - the element CH.exp is not valid
1943	PATrans - the element TX.time is not valid
1944	PATrans - the element TX.status is not valid
1945	PATrans - the element TX.detail is not valid
1946	PATrans - the element TX.stain is not valid
1947	PATrans - the element TX.eci is not valid
1948	PATrans - the element TX.vendorCode is not valid
1949	PATrans - the element SignedPAREs is not valid
1951	PATransRes - the element PATransRes is not found
1952	PATransRes - the element version is not valid
1953	PATransRes - the element iReq.IReqCode is not found
1954	PATransRes - the element iReq.IReqCode is not found
1955	PATransRes - the element iReq.IReqCode is not valid
1956	PATransRes - the element iReq.IReqCode is not valid
1971	CAVV - the element xid is not found
1972	CAVV - the element pan is not valid
1973	CAVV - the element authResultCode is not valid
1974	CAVV - the element secondFactorAuthCode is not valid
1975	CAVV - the element cavvKeyIndicator is not valid
1976	CAVV - the element cardSequenceNumber is not valid
1977	CAVV - the element cvr is not valid
1978	CAVV - the element unpredictableNumber is not valid
1979	CAVV - the element atn is not found
5100	Expiry date is invalid
5101	Pan not found in local cache
5102	No brand details found for that Merchant
5103	Error occurred during validate of VEReq"
5104	Error occurred during build of VEReq
5105	ThreeDSecureMessage Exception occurred during validate and build of VEReq
5106	No connection details were found for that specific brand, merchant and pan
5107	Exception occurred during the post of the VEReq message to the VisaDirectory
5108	Invalid Handler/ Locator or Generator configured during processing of VEReq
5109	Error occurred during validate of Error"

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

5110	Error occured during build of Error
5111	ThreeDSecureMessage Exception occured during validate and build of Error
5112	Exception occured during the post of the Error message to the VisaDirectory
5113	Received an Error message instead of a VERes
5114	Unkown error
5115	Pan is not enrolled for 3-D Secure
5116	ThreeDSecure is not supported by the Issuer!
5117	Recieved a badly formatted VERes, so we had to send an error to the VSD
5118	Version is too old
5119	Currency code not found
5120	Error occured during validate of PAREq"
5121	ThreeDSecureMessage Exception occured during validate and build of PAREq
5122	No termUrl is found for the MPI
5123	Exception occured during creation of the PaReq Form
5124	Unknown error occured during processing of VERes
5125	Exception occured during decode and inflate of pares
5126	Recieved a badly formatted PAREs, so we had to send an error to the VSD
5127	An error occured during the validation of the xml signature
5128	An error occured during the logging process of the PAREq message
5129	An error occured during the logging process of the PAREs message
5130	An Exception occured when getting the PAREq from the cache, or during the parse and validate of it
5131	An Exception occured during encryption/decryption of sensative data
5132	An error occured during parse and validate of the VERes message
5133	An error occured during parse and validate of the PAREs message
5134	The XML-signature of the PAREs message is not a valid one
5135	Error occured during validate of CRReq
5136	Error occured during build of CRReq
5137	ThreeDSecureMessage Exception occured during validate and build of CRReq
5138	Exception occured during the post of the CRReq message to the VisaDirectory
5139	unknown error occure during processing of CRRes
5140	Recieved a badly formatted CRRes, so we had to send an error to the VSD
5141	Error occured during build of Veres
5142	Error occured during decode and inflate of PAREq

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

5143	Unable to start authentication flow
5144	Authentication was not successfull
10000	Unspecified error occured
5145	Error Getting VEReq out of transaction cache
5146	Received status U
5147	Received an Error message instead of a PAREs

Tableau 3 : Codes réponses du MPI

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

6.2 URL d'appel et Adresses IP

Pour utiliser les services **E-transactions Remote MPI** :

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

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	ADRESSES IP PUBLIQUES AFFECTEES 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

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

6.3 Glossaire

6.3.1 3-D Secure

6.4 3D-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, calculatrice ...

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 3D-Secure. Les indicateurs suivants sont disponibles :

- *Paiement 3D-Secure* : Indique si la transaction a été exécutée avec un contrôle 3D-Secure
 - o « OUI » Avec 3D-Secure
 - o « 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
 - o Y L'authentification s'est déroulée avec succès
 - o N Le porteur n'est pas parvenu à s'authentifier, la transaction est interdite
 - o U L'authentification n'a pu être finalisée suite à un problème technique
 - o 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
 - o « OUI » Garantie
 - o « OUI expirée » Non Garantie car remise au-delà du délai maxi de 7 Jours
 - o « NON » Non Garantie

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

E-transactions Remote MPI	Version du 14/09/2015
Manuel d'intégration	

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.

6.4.1 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.

6.4.2 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.

6.4.3 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).

6.4.4 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.

6.4.5 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>

6.4.6 URL encodée

Tous les caractères ne sont pas autorisés dans les URL (voir la définition de l'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.

Document non contractuel propriété de Crédit Agricole S.A

Il ne peut être reproduit ou communiqué à des tiers sans autorisation