Exemple : PBX_SOURCE=RWD

11.1.2.21 PBX_TOKEN

Format : jusqu'à 250 caractères
Valeur par défaut : Champ absent.

Etiquette (token) du moyen de paiement généré lors d'une demande de création d'abonné (enregistrement du moyen de paiement) via les pages de paiement ou un appel à l'API.

Si cette variable est renseignée conjointement avec la variable PBX_REFABONNE, la carte de paiement enregistrée par votre client est reconstituée lors de l'affichage des pages de paiement et pré-saisie mais masquée. Il n'a pas besoin de la saisir pour réaliser son paiement.

Exemple : PBX_TOKEN=NODMIOOCUB1N0BETO0TA

Voir aussi : *8-Tokenisation – Gestion des abonnées*

11.1.2.22 PBX_TYPEPAIEMENT

Format : 5 à 10 caractères.
Valeur par défaut : Champ absent.

Précise aux pages de paiement quel est le **type de paiement souhaité** lorsque l'internaute arrive sur les pages hébergées par la plateforme Up2pay e-Transactions.

- Sur la page de présélection :
  - Permet de n'afficher que les moyens de paiement compatibles avec le type de paiement choisi

  Par exemple, si vous disposez du moyen de paiement Paypal mais vous souhaitez limiter les paiements uniquement par carte bancaire, il faut renseigner cette variable à « CARTE ».
  Ainsi, seules les options de type carte dont vous disposez sont affichées sur la page de présélection.

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

Les valeurs possibles de la variable PBX_TYPEPAIEMENT sont disponible au chapitre suivant *11.1.2.23-PBX_TYPECARTE*.

11.1.2.23 PBX_TYPECARTE

Format : min. 2 caractères.
Valeur par défaut : Champ absent.

Précise aux pages de paiement quel est le **moyen de paiement souhaité** lorsque votre client arrive sur les pages hébergées par la plateforme Up2pay e-Transactions.

SI cette variable est envoyée, la variable PBX_TYPEPAIEMENT (type de paiement souhaité) doit également être envoyé.

Si ces deux variables sont envoyées, elles permettent de ne pas afficher la page de présélection, et d'afficher directement la page de paiement adaptée au moyen de paiement souhaité.

Les combinaisons possibles entre le type de moyen de paiement (PBX_TYPEPAIEMENT) et le moyen de paiement (PBX_TYPECARTE) souhaités suivent le tableau suivant :

PBX_TYPEPAIEMENT	PBX_TYPECARTE
CARTE	CB *(pour CB, VISA, MASTERCARD, E_CARD, MAESTRO)*
	AMEX
	DINERS
	JCB
PAYPAL	PAYPAL
CREDIT	UNEURO
	34ONEY
PREPAYEE	PSC
	IDEAL
	ONEYKDO
	ILLICADO
LEETCHI	LEETCHI
WALLET	PAYLIB
LIMONETIK	CVCONNECT
	APETIZ *(pour Conecs)*
	SODEXO *(pour Conecs)*
	UPCHEQUDEJ *(pour Conecs)*

Tableau 17 : Valeurs possibles PBX_TYPEPAIMENT et PBX_TYPECARTE

11.1.2.24 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3

Format : 3 à 10 chiffres

Montant (en centimes, sans virgule ni point) des prochaines échéances d'un paiement fractionné. Le montant du paiement initial réalisé au moment de la commande est indiqué dans la variable PBX_TOTAL.

Pour un paiement en 2 fois, il faut indiquer le montant de la 2ème échéance dans PBX_2MONT1. Pour un paiement en 4 fois, il faut envoyer les montants des 2ème, 3ème et 4ème échéances dans PBX_2MONT1, PBX_2MONT2 et PBX_2MONT3.

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

Exemple : PBX_2MONT1=1233&PBX_2MONT2=1234
Si PBX_TOTAL=1233, cela correspond à un achat de 37,00€ fractionné en 3 échéances : 1ère échéance au moment de la commande de 12,33€, 2ème échéance de 12,33€ et 3ème échéance de 12,34€.

Voir aussi : *9.3-Paiement en plusieurs fois (4 fois maximum)* et *11.1.2.7-PBX_DATE1, PBX_DATE2, PBX_DATE3*

11.1.3 Variables spécifiques à certains moyens de paiement

11.1.3.1 PBX_1EURO_CODEEXTERNE

Format : 3 chiffres.

Uniquement utilisée pour la solution de paiement « 1Euro.com ».

Offre promotionnelle externe fournie par la solution 1Euro.com

Exemple : PBX_1EURO_CODEEXTERNE=111

11.1.3.2 PBX_1EURO_DATA

Format : jusqu'à 100 caractères.

Uniquement utilisée pour la solution de paiement « 1Euro.com ».

Données d'identification et de localisation de votre client.

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

RANG	DONNEE	PRECISION
#1	Civilité	
#2	Nom	
#3	Prénom	
#4	Adresse1	
#5	Adresse2	*vide si non pertinent mais # présent*
#6	Adresse3	*vide si non pertinent mais # présent*
#7	Code postal	
#8	Ville	
#9	Code pays	*FR pour France par exemple*
#10	Téléphone fixe	
#11	Téléphone portable	
#12	Flag indiquant si l'internaute est connu du commerçant	**0 :** Non connu - **1 :** Connu
#13	Flag indiquant si le commerçant a déjà eu des incidents de paiements avec cet internaute	**0 :** Pas d'incident - **1 :** Incident passé
#14	Code action COFIDIS	*valeur figée et fournie par COFIDIS*

Tableau 18 : Données PBX_1EURO_DATA

Exemple : PBX_1EURO_DATA=M#DUPONT#Jean#Rue Lecourbe#BatimentA##75010#PARIS#FR #0102030405##0#0#12#

11.1.3.3 PBX_CK_ONLY

Format : 1 lettre - O ou N.
Valeur par défaut : N

Uniquement utilisée pour les paiements avec des cartes cadeau

La valeur « O » permet de forcer le fait que le paiement soit réalisé uniquement avec des cartes cadeau. Dans le cas contraire (valeur par défaut « N »), votre client peut aussi utiliser sa carte ou un autre moyen de paiement pour compléter son paiement.

Exemple : PBX_CK_ONLY=O

11.1.3.4 PBX_NBCARTESKDO

Format : jusqu'à 2 chiffres.

Uniquement utilisée pour les paiements avec Cartes Cadeau.

Permet de limiter le nombre de Cartes Cadeau utilisables par vos clients.
Les valeurs autorisées sont entre 1 et 25.

Exemple : PBX_NBCARTESKDO=3

11.1.3.5 PBX_OPECOM

Format : 10 caractères.

Uniquement utilisée pour la solution Facilipay d'Oney Banque Accord.

Permet d'indiquer une opération commerciale. La valeur est définie par la solution Facilipay.

Exemple : PBX_OPECOM=3453234786

11.1.3.6 PBX_ONEY_DATA

Format : XML.

Uniquement utilisée pour la solution Facilipay d'Oney Banque Accord.

Données d'identification et de localisation de votre client. Le format précis est défini par la solution Facilipay.

11.1.3.7 PBX_PAYPAL_DATA

Format : jusqu'à 490 caractères.

Uniquement utilisée pour le moyen de paiement PAYPAL.

Données d'identification et de localisation de votre client.
Cette variable est obligatoire dans le cas d'un paiement avec création d'abonné (voir chapitre *8-Tokenisation – Gestion des abonnées*), conseillée dans les autres cas.

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

RANG	DONNEE	FORMAT
#1	Nom du client	32 caractères
#2	1ère ligne d'adresse	100 caractères
#3	2ème ligne d'adresse	100 caractères *vide si non pertinent mais # présent*
#4	Ville	40 caractères
#5	Etat / Région	40 caractères
#6	Code postal	20 caractères
#7	Code pays	2 caractères *FR pour France*
#8	Numéro de téléphone	20 caractères
#9	Description du paiement	127 caractères

Tableau 19 : Données PBX_PAYPAL_DATA

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

11.2 Authentification par API (RemoteMPI)

L'ensemble des variables de l'API d'authentification 3D-Secure (RemoteMPI) est résumé dans le tableau suivant :

VARIABLE	QUESTION	REPONSE	RESUME
Address1	X		Adresse de facturation de votre client - Ligne1
Address2	X		Adresse de facturation de votre client - Ligne2
Amount	X		Montant de la demande d'autorisation
CCExpDate	X		Date d'expiration de la carte
CCNumber	X		Numéro de carte
City	X		Ville de l'adresse de facturation de votre client
CountryCode	X		Code pays de l'adresse de facturation de votre client
Currency	X		Devise
CVVCode	X		Cryptogramme visuel
EmailPorteur	X		Adresse email de votre client
FirstName	X		Prénom de votre client

IdMerchant	X		Identifiant commerçant fourni par la solution Up2pay e-Transactions
IdSession	X	X	Identifiant de session unique
LastName	X		Nom de votre client
TotalQuantity	X		Nombre d'articles composant la commande
TypeCarte	X		Type de carte choisi par votre client
URLHttpDirect	X		URL de retour serveur à serveur
URLRetour	X		URL de retour depuis le navigateur du client
ZipCode	X		Code postal de l'adresse de facturation de votre 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	Indicateur E-Commerce (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 Up2pay e-Transactions
ID3D		X	Identifiant de contexte e-Transactions
StatusPBX		X	Statut de la demande d'authentification

Tableau 20 : Liste des variables RemoteMPI

11.2.1 Variables d'appel e-Transactions RemoteMPI

11.2.1.1 Address1

Format : 50 caractères. **Obligatoire.**

Adresse de facturation (ligne 1) de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Information : s'il ne s'agit pas d'un service ou d'un bien facturé (ex : don, paiement à une collectivité, …) les informations à fournir ici sont celles du payeur ou donateur.

Exemple : Address1=12 rue Test

11.2.1.2 Address2

Format : 50 caractères. **Facultatif.**

Adresse de facturation (ligne 2) de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.

La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Information : s'il ne s'agit pas d'un service ou d'un bien facturé (ex : don, paiement à une collectivité, …) les informations à fournir ici sont celles du payeur ou donateur.

Exemple : Address2=lieu dit Le Village

11.2.1.3 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 RemoteMPI et pour la demande d'autorisation de paiement par **API** (Gestion Automatisée des Encaissements) avec la **variable MONTANT**.

Exemple : pour 19€90 : Amount=0000001990

Equivalent API de paiement (GAE) : **MONTANT**

11.2.1.4 CCExpDate

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

Date de fin de validité de la carte.

Exemple : CCExpDate=1223 pour décembre 2023

Equivalent API de paiement (GAE) : **DATEVAL**

11.2.1.5 CCNumber

Format : 19 caractères. **Obligatoire.**

Numéro de carte du porteur (client) sans espace.

Exemple : CCNumber=1111222233334444

Equivalent API de paiement (GAE) : **PORTEUR**

11.2.1.6 City

Format : 50 caractères. **Obligatoire.**

Ville de l'adresse de facturation de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Information : s'il ne s'agit pas d'un service ou d'un bien facturé (ex : don, paiement à une collectivité, …) les informations à fournir ici sont celles du payeur ou donateur.

Exemple : City=Paris

11.2.1.7 CountryCode

Format : Numérique sur 3 positions – ISO-3166-1 Numérique. **Obligatoire.**

Code pays de l'adresse de facturation de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Correspond au code pays numérique de la norme ISO-3166-1 du pays de l'adresse de facturation.

Information : s'il ne s'agit pas d'un service ou d'un bien facturé (ex : don, paiement à une collectivité, …) les informations à fournir ici sont celles du payeur ou donateur.

Exemple : CountryCode=250 (pour la France)

11.2.1.8 Currency

Format : 3 chiffres. **Obligatoire.**

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

Exemples : Currency=978

Attention : La seule valeur autorisée est l'euro (€) : 978

Equivalent API de paiement (GAE) : **DEVISE**

11.2.1.9 CVVCode

Format : 3 ou 4 caractères. **Obligatoire.**

Cryptogramme visuel situé au dos de la carte bancaire.

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

Exemple : CVVCode=123

Equivalent API de paiement (GAE) : **CVV**

11.2.1.10 EmailPorteur

Format : alpha-numérique sur 120 caractères au format adresse email (incluant @ et .). **Obligatoire.**

Adresse email de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Exemple : EmailPorteur=test@client.com

11.2.1.11 FirstName

Format : 30 caractères incluant (/ - et '). **Obligatoire.**

Prénom de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Exemple : FirstName=Jean

11.2.1.12 IdMerchant

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

Identifiant e-Transactions de votre boutique fourni par la solution Up2pay e-Transactions dans le mail de bienvenue.

Exemple : IdMerchant=2

11.2.1.13 IdSession

Format : jusqu'à 250 caractères. **Obligatoire.**

Identifiant unique de la requête vous permettant de contrôler le retour reçu et de distinguer les réponses en cas de questions multiples et simultanées.
Chaque appel doit avoir un identifiant de session unique.

Exemple : IdSession=Session20201210154825360_001
(en utilisant la date/heure/minute/seconde/ms)

11.2.1.14 LasttName

Format : 30 caractères incluant (/ - et '). **Obligatoire.**

Nom de famille de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Exemple : LastName=Dupont

11.2.1.15 TotalQuantity

Format : Numérique de 1 à 99. **Obligatoire.**

Nombre de produit dans la commande et permettant à la banque de votre client d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Exemple : TotalQuantiy=9

11.2.1.16 TypeCarte

Format : Alpha-numérique. **Facultatif.**

Type de la carte choisie par votre client.

Les valeurs possibles sont :

CB	ELECTRON
VISA	MAESTRO
MASTERCARD	VPAY

Exemple : TypeCarte=CB

11.2.1.17 URLHttpDirect

Format : jusqu'à 250 caractères.

URL de retour de serveur à serveur. Si l'URL n'est pas présente, la plateforme utilise celle paramétrée sur votre fiche client visualisable et modifiable dans votre Back-office Vision.

L'URL indiquée dans URLHttpDirect doit être URL-encodée lors de l'appel à l'API RemoteMPI.

Exemple : URLHttpDirect=http://maboutique.com/retour%20MPI.php

11.2.1.18 URLRetour

Format : jusqu'à 250 caractères.

URL de retour vers votre boutique depuis le navigateur de votre client après avoir utilisé les pages d'authentification 3D-Secure. Si l'URL n'est pas présente, la plateforme utilise celle paramétrée par défaut pour le retour de paiement en succès (correspondant à l'URL de PBX_EFFECTUE sur les appels des pages de paiement). Cette URL est visualisable et modifiable dans votre client accessible dans votre Back-office Vision.

L'URL indiquée dans URLRetour doit être URL-encodée lors de l'appel à l'API RemoteMPI.

Exemple : URLRetour=http://maboutique.com/continuer%20commande.php

11.2.1.19 ZipCode

Format : 16 caractères. **Obligatoire.**

Code postal de l'adresse de facturation de votre client et permettant à sa banque d'évaluer le besoin d'authentification à réaliser en 3DSv2.
La solution Up2pay e-Transactions envoie les requêtes avec le choix « ne se prononce pas », c'est donc la banque de votre client qui choisit si elle déclenche ou non une authentification 3D-Secure. Si elle choisit une authentification passive vous êtes tout de même garanti.

Information : s'il ne s'agit pas d'un service ou d'un bien facturé (ex : don, paiement à une collectivité, …) les informations à fournir ici sont celles du payeur ou donateur.

Exemple : ZipCode=75001

11.2.2 Variables réponses e-Transactions RemoteMPI

11.2.2.1 IdSession

Format : jusqu'à 250 caractères.

Identifiant unique de la requête que vous avez soumis lors de l'appel. Cette variable vous permet de contrôler le retour reçu et de distinguer les réponses en cas de questions multiples et simultanées.

Rappel : chaque appel est effectué avec un identifiant de session unique.

Exemple : IdSession=Session20201210154825360_001
(en utilisant la date/heure/minute/seconde/ms)

11.2.2.2 StatusPBX

Format : Alphanumérique.

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

Ce résultat conditionne la possibilité d'effectuer un appel API (GAE) de demande d'autorisation à associer / contextualiser avec la cette demande d'authentification.
Si le résultat est négatif, vous ne devez pas effectuer une demande d'autorisation.

STATUSPBX	DESCRIPTION
Erreur	**Incident** propre aux traitements de la plateforme d'authentification. L'authentification du porteur n'a pas pu avoir lieu et la demande d'autorisation ne doit pas être effectuée. **Le paiement sera refusé.** Vous devez recommencer la demande d'authentification.
Autorisation à faire	**L'authentification a été réalisée avec succès.** Vous pouvez réaliser une demande d'autorisation avec le contexte de cette authentification. Si l'autorisation est également en succès, **le paiement sera réalisé.**
Autorisation à ne pas faire	**L'authentification a échouée.** La demande d'autorisation ne doit pas être effectuée. **Le paiement sera refusé.**
Timeout	Le porteur n'a pas effectué la demande d'authentification après un **délai d'attente de 5 minutes.** L'authentification du porteur n'a pas pu avoir lieu et la demande d'autorisation ne doit pas être effectuée. **Le paiement sera refusé.**

Tableau 21 : Valeurs possibles pour StatusPBX

Exemple : StatutPBX=Autorisation%20à%20faire

11.2.2.3 ID3D

Format : jusqu'à 20 chiffres.

Identifiant de contexte e-Transactions contentant les données d'authentification retournées par le MPI.

Ce contexte d'authentification est stocké pendant une durée de 5 minutes. Cela signifie que vous avez 5 minutes pour effectuer la demande d'autorisation en lien avec ce contexte. **Au-delà, les applications considèreront que la phase d'authentification de votre client n'est plus valide et le paiement sera refusé.**

Exemple : ID3D=9900000000012

11.2.2.4 Check

Format : jusqu'à 256 caractères.

Signature électronique de la plateforme Up2pay e-Transactions sur l'ensemble des données renvoyées en paramètres. Vous devez réaliser la vérification de cette signature pour confirmer l'authenticité de la plateforme e-Transactions et confirmer l'intégrité des données transmises.

Exemple : Check=nLpPFrgGHqSbVW%2F5iHbxoBdRiYPzNIrXtBBZVUCWhfdAx3SH4DLUXnCylZPri%2BUHxpV9Lkl92n%2FwPp24wwtJ0sGv6wRBs%2Fiz9HSu3AifDI%2BQMD1ywK65kQNZOif6%2BNMetiscQwl80%2Bl6sgTOnAOJECEGlt1oDbxQ0mf%2Bs7UdUPE%3D

Voir aussi : *6-Authentification des messages reçus p*our le mécanisme de vérification des signatures en provenance de la plateforme Up2paye-Transactions.

11.2.2.5 3DCAVV

Format : 28 caractères.

Valeur reçue des ACS. URL-encodé.

11.2.2.6 3DCAVVALGO

Format : jusqu'à 64 caractères

Identifiant de l'algorithme ayant servi à l'identification de votre client sur l'ACS.

Exemple : 3DCAVVALGO=0000000001

11.2.2.7 3DECI

Format : 2 chiffres

Electronic Commerce Indicator. Permet de connaitre le niveau de sécurisation de la transaction renvoyé par les serveurs 3DS. Vous trouverez les informations sur les différentes valeurs ECI possibles pour chacun des réseaux de carte (VISA, MASTERCARD, CB, AMEX, …) dans les documentations diffusées par les réseaux carte.

Exemple : 3DECI=02

11.2.2.8 3DENROLLED

Format : 1 caractère

État sur l'enrôlement du Porteur au programme 3DS.

Valeurs possibles :

Y	Carte de votre client enrôlée
N	Carte de votre client non enrôlée
U	Erreur

Exemple : 3DENROLLED=Y

11.2.2.9 3DERROR

Format : jusqu'à 6 caractères

Numéro d'erreur renvoyé directement par le MPI et retranscris dans cette variable sans modification par la solution Up2pay e-Transactions.

Exemple : 3DERROR=100

Voir aussi : *12.6-Codes réponses de l'API RemoteMPI (Authentification 3D-Secure)*

11.2.2.10 3DSIGNVAL

Format : 1 caractère. « Y » ou « N »

Généré par le MPI, il indique le statut de la vérification de la signature du porteur.
Y : Vérifié, N : Non vérifié.

Exemple : 3DSIGNVAL=Y

11.2.2.11 3DSTATUS

Format : 1 caractère.

Statut final de la demande d'authentification remonté par le MPI.

Exemple : 3DSTATUS=Y

Valeurs possibles :

Y	Porteur authentifié
N	Porteur non authentifié
A	Authentification non réalisée par la banque de votre client (ex : erreur technique). Le paiement peut être réalisé.
U	Incident. L'authentification n'a pas pu être réalisé pour une raison technique

11.2.2.12 3DXID

Format : jusqu'à 28 caractères

Référence de la transaction d'authentification renvoyée par le MPI.
A communiquer en cas de besoin d'information du MPI.

Exemple : 3DXID=z9UKb06xLziZMOXBEmWSVA1kwG0%3D

11.3 Intégration avec les API (GAE)

11.3.1 Variables d'appel aux API

11.3.1.1 SITE

Format : 7 chiffres. **Obligatoire.**

Numéro de site fourni par la solution Up2pay e-Transactions dans votre mail de bienvenue.

Exemple : SITE=1999888

11.3.1.2 RANG

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

Numéro de rang fourni par la solution Up2pay e-Transactions dans votre mail de bienvenue

Remarque : si la valeur est envoyée sur 2 caractères elle sera préfixée par un 0 par la plateforme (réglementaire)

Exemple : RANG=001

11.3.1.3 VERSION

Format : 5 chiffres. **Obligatoire.**
Valeur fixe : 00104

Version du protocole d'API utilisée.
Une seule valeur est possible : 00104.

Exemple : VERSION=00104

11.3.1.4 TYPE

Format : 5 chiffres. **Obligatoire.**

Opération à réaliser.

Les API (GAE) permettent la réalisation de transactions, mais aussi de toutes les opérations de caisse liées à ces transactions : capture, remboursement, annulation, … Cette variable définit l'opération à réaliser.

Attention : Dans le cas d'un appel pour réaliser une capture (TYPE=00002) qui suit une demande d'autorisation 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 (ppps ou ppps1) que la demande d'autorisation seule afin d'éviter d'éventuels problèmes de réplication entre les plateformes.

Les valeurs possibles des opérations à réaliser sont les suivantes :

CODE	DESCRIPTION
00001	Autorisation seule
00002	Capture (confirmation du débit pour remise en banque)
00003	Autorisation + Capture

00005	Annulation d'une opération
00011	Vérification de l'existence d'une transaction
00013	Modification du montant d'une transaction
00014	Remboursement sur une précédente transaction
00017	Consultation d'une transaction
00018	Demande des marques associées à la carte du porteur (MIF)
00051	Autorisation seule sur un abonné
00052	Capture (confirmation de débit) sur un abonné
00053	Autorisation + Capture sur un abonné
00055	Annulation d'une opération sur un abonné
00056	Inscription d'un nouvel abonné
00057	Modification d'un abonné existant
00058	Suppression d'un abonné

Tableau 22 : Liste des TYPE d'opération par API

Exemple : TYPE=00002

11.3.1.5 DATEQ

Format : 14 chiffres. **Obligatoire.**

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

Attention : Pour un appel à l'API avec une question du TYPE=11 (« Vérification de l'existence d'une transaction »), c'est cette variable qui est utilisée pour faire la recherche de la transaction sur une journée donnée. Dans ce cas, vous devez l'envoyer au format JJMMAAAA (jour, mois année).
Exemple : DATEQ=13042021125959

11.3.1.6 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.

Conseil : Une solution pratique et efficace pour s'assurer de l'unicité par jour de la variable « NUMQUESTION » est d'utiliser l'horodatage de l'appel ramené sur 10 positions avec un 0 en début de valeur. Soit 0HHMMSSmi *(HH = heures sur 2 positions ; MM = minutes sur 2 positions ; SS = secondes sur 2 positions ; mi = millisecondes sur 3 positions).*

Exemple : 0145829183 *(pour 14h58mn29s et 183 ms)*

11.3.1.7 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 (valeurs identiques à la liste ci-dessous - sensible à la Casse/majuscules) :

SHA512	SHA256
RIPEMD160	SHA384
SHA224	MDC2

Les hachages en MD2/4/5 sont jugés trop faibles pour être utilisés et seront refusés (la page de paiement ne s'affichera pas)

Si la variable HMAC est présente dans les appels sans que HASH ne soit précisé, l'algorithme de hachage sélectionné sera SHA512.

Exemple : HASH=SHA512

11.3.1.8 HMAC

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

Permet de vous authentifier et vérifier l'intégrité du message. Il est calculé à partir de la liste des autres variables envoyées dans l'API à e-Transactions.

Exemple :
HMAC=AD4D2A87FB9C4FA7AD8AA122E9F417B568D5E2B8CA4AF9410B00B9CFCFDB9142F721CBD0B90F518A16A49F9A7BD248A86EFEA25831654395E1DED1BEA650361C

Voir aussi : *5.3-Authentification des messages*

11.3.1.9 MONTANT

Format : 10 chiffres (aligné à droite et complété par des zéros). **Obligatoire pour les questions de TYPE 1, 2, 3, 5, 11, 13, 14, 51, 52, 53, 55, 56, 57.**

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

Exemple : pour 19€90 : MONTANT=0000001990

11.3.1.10 DEVISE

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

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

Exemple :

- Euro : DEVISE=978

Attention : La seule valeur autorisée est l'euro (€) : 978

11.3.1.11 REFERENCE

Format : 1 à 250 caractères. **Obligatoire pour les questions de TYPE 1, 2, 3, 5, 11, 51, 52, 53, 55, 56.**

Votre référence de commande (champ libre). Ce champ vous permet de garder un lien entre votre boutique et la plateforme Up2pay e-Trasnsactions. Ce champ doit être unique à chaque appel.

Exemple : CMD9542124-01A5G

11.3.1.12 REFABONNE

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

Référence de l'abonné (client et son moyen de paiement) à utiliser pour les opérations de gestion de l'abonné : association d'une carte de paiement à enregistrer, réutilisation d'une carte de paiement enregistrée pour réaliser une nouvelle transaction, modification de la carte de paiement enregistrée, suppression de l'abonné.

Exemple : REFABONNE=Client_005287_Mdp_0001 ou REFABONNE=HcsqXh5YHkCb

11.3.1.13 PORTEUR

Format : jusqu'à 19 caractères. **Obligatoire pour les questions de TYPE 1, 3, 51, 53, 55, 56, 57.**

Numéro de carte du porteur (client) sans espace, cadré à gauche pour les opérations de paiement ou de gestion des abonnés (enregistrement des cartes de paiement).

Exemple : PORTEUR=1111222233334444

11.3.1.14 DATEVAL

Format : Date (MMAA). **Obligatoire pour les questions de TYPE 1, 3, 51, 53, 55, 56, 57.**

Date de fin de validité de la carte utilisée pour l'opération de paiement ou la gestion d'un abonné.

Exemple : DATEVAL=1213 (pour décembre 2013)

11.3.1.15 CVV

Format : 3 ou 4 caractères. **Obligatoire pour les questions de TYPE 1, 3, 56.**

Cryptogramme visuel situé au dos de la carte bancaire renseigné par votre client pour l'opération de paiement.

Remarque : Les cartes AMERICAN EXPRESS ont sur leur recto un CIN (Card Identification Number) sur 4 chiffres. C'est ce numéro qu'il faut indiquer dans cette variable.

Exemple : CVV=123

11.3.1.16 ACTIVITE

Format : 3 chiffres.
Valeur par défaut : 024 / 027 en fonction de l'opération effectuée

Environnement Réglementaire et Technique (ERT).

Permet à votre banque de différencier la provenance des différents flux monétiques envoyés pour renseigner les champs relatifs à l'ERT dans les flux monétiques véhiculés sur le réseau bancaire (obligation règlementaire).
Important : Il est nécessaire de renseigner de la manière la plus correcte possible cette valeur correspondant au contexte de l'opération de paiement.

Voici les valeurs possibles pour l'ERT :

CODE	DESCRIPTION
024	Demande par internet
027	Paiement récurrent

Exemple : ACTIVITE=024

11.3.1.17 ARCHIVAGE

Format : jusqu'à 12 caractères alphanumériques

Référence qui vous est propre et qui est transmise au serveur du Crédit Agricole au moment de la télécollecte. Elle doit être unique et peut permettre au Crédit Agricole de vous fournir une information en cas de litige sur un paiement.
C'est aussi un élément constitutif du rapprochement bancaire (référence reprise dans votre relevé bancaire et dans les journaux de rapprochement bancaire - JRB).

Attention : ce paramètre ne peut pas contenir de caractères spéciaux, ni de tiret (-) ou underscore (_).

Exemple : ARCHIVAGE=ID0001452158

11.3.1.18 DIFFERE

Format : 3 chiffres
Valeur maximum : 075 jours

Nombre de jours de différé (entre la transaction et sa remise en banque automatique).

A noter qu'il est possible de supprimer cette mise en attente à partir de votre Back-office Vision.

Par exemple, une transaction réalisée le 2 novembre et différée jusqu'au 4 novembre, peut être débloquée et envoyée en banque le 3 novembre par action manuelle.

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

Rappel : La valeur maximum pour cette variable est de 75 jours mais la garantie de paiement 3D-Secure n'est valable que 6 jours.

Exemple : DIFFERE=004 pour réaliser un différé de 4 jours

11.3.1.19 NUMAPPEL

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

Référence d'appel Up2pay e-Transactions de la transaction de paiement (réalisée précédemment) sur laquelle vous souhaitez effectuer l'opération (annulation, remboursement).

Lorsque le paiement a été réalisé par l'appel des pages de paiement de la solution Up2pay e-Transactions cette référence vous est renvoyée dans les paramètres de retour sur les différentes URLs dont la Notification de Paiement Instantanée (IPN) : donnée **T** de **PBX_RETOUR**.

Pour les opérations de paiement réalisées en utilisant les API (GAE), cette donnée est présente dans les données de la trame réponse à l'appel : **NUMAPPEL**.

Ce numéro d'appel est aussi visible dans votre Back-Office Vision dans le détail d'une opération.

Exemple : NUMAPPEL=1234567890

11.3.1.20 NUMTRANS

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

Référence transaction Up2pay e-Transactions de la transaction de paiement (réalisée précédemment) sur laquelle vous souhaitez effectuer l'opération (annulation, remboursement).

Lorsque le paiement a été réalisé par l'appel des pages de paiement de la solution Up2pay e-Transactions cette référence vous est renvoyée dans les paramètres de retour sur les différentes URLs dont la Notification de Paiement Instantanée (IPN) : donnée **S** de **PBX_RETOUR**.

Pour les opérations de paiement réalisées en utilisant les API (GAE), cette donnée est présente dans les données de la trame réponse à l'appel : **NUMTRANS**.

Ce numéro de transaction est aussi visible dans votre Back-Office Vision dans le détail d'une opération.

Exemple : NUMTRANS=1234567890

11.3.1.21 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 porteur si le paiement est accepté.

Lorsque le paiement a été réalisé par l'appel des pages de paiement de la solution Up2pay e-Transactions ce numéro d'autorisation vous est renvoyé dans les paramètres de retour sur les différentes URLs dont la Notification de Paiement Instantanée (IPN) : donnée **A** de **PBX_RETOUR**.

Pour les opérations de paiement réalisées en utilisant les API (GAE), cette donnée est présente dans les données de la trame réponse à l'appel : **AUTORISATION**.

Ce numéro d'autorisation est aussi visible dans votre Back-Office Vision dans le détail d'une opération.

Exemple : AUTORISATION=168753

11.3.1.22 PAYS

Format : <vide>.

Si ce champ est présent (même vide), l'API renvoie le code pays de la carte dans la trame-réponse de l'appel.

Exemple : PAYS=

11.3.1.23 ACQUEREUR

Format : jusqu'à 16 caractères.

Moyen de paiement autre que CARTE utilisé pour réaliser le paiement.

Les valeurs possibles sont :

Désignation	Valeur
Oney 3/4 fois	34ONEY
Oney Illicado	ILLICADO
Oney Carte Cadeau	ONEYKDO
Paypal	PAYPAL
Paysafecard	PSC
Limonetik	LIMOCB *(pour le complément par carte bancaire)*
CV-Connect	CVCONNECT
Conecs - Apétiz	APETIZ
Conecs - Sodexo Pass Restaurant	SODEXO
Conecs - Up Chèque Déjeuner	UPCHEQUDEJ

Tableau 23 : Liste des valeurs de la variable ACQUEREUR

Attention : Dans le cas d'opération de paiement réalisée par API mais ne concernant pas l'un de ces acquéreurs, ce champ ne doit pas être envoyé.

Exemple : ACQUEREUR=PAYPAL

11.3.1.24 TYPECARTE

Format : 2 à 30 caractères.

Marque de la carte de paiement à utiliser pour réaliser l'opération de paiement.

Les valeurs possibles sont :

CB	ELECTRON
VISA	MAESTRO
MASTERCARD	VPAY

Tableau 24 : Liste des valeurs pour la variable TYPECARTE

Si ce champ est présent mais vide, l'API renvoie le type de la carte détecté par la solution à partir du numéro de carte dans la trame-réponse de l'appel.

Exemple : TYPECARTE=VISA

11.3.1.25 SHA-1

Format : <vide>

Si ce champ est présent (même vide), l'API renvoie l'empreinte de la carte dans la trame-réponse de l'appel (pour un paiement par carte).

Le numéro de carte est hashé avec la méthode SHA-1. Cette empreinte est uniquement utilisable pour effectuer des contrôles de risque sur l'utilisation multiples de la même carte (sans la connaitre) ou l'utilisation de multiples cartes différentes (sans les connaitre).

Exemple : SHA-1=

11.3.1.26 ERRORCODETEST

Format : 5 chiffres.

Pour simuler des cas d'erreur lors des tests d'intégration ou de simulation de production, vous pouvez renseigner ce code erreur qui vous sera renvoyé dans la trame-réponse de l'appel.

Cette variable n'est pas prise en compte dans l'environnement de production.

Exemple : ERRORCODETEST=00157

Voir aussi : *12.2-Codes réponse des APIs*

11.3.1.27 ID3D

Format : 20 chiffres. **Obligatoire pour les questions de TYPE 1, 3, 51, 53, 55, 56, 57**.

Identifiant de contexte retournées par le MPI contenant les données d'authentification lors de l'appel à l'API RemoteAPI permettant de réaliser la phase d'authentification 3D-Secure.

Ce contexte d'authentification est stocké pendant une durée de 5 minutes. Cela signifie que vous avez 5 minutes pour effectuer la demande d'autorisation en lien avec ce contexte. **Au-delà, les applications considèreront que la phase d'authentification de votre client n'est plus valide et le paiement sera refusé.**

Exemple : ID3D=9900000000012

11.3.1.28 SELECTION

Format : 2 chiffres.

Indicateur permettant de préciser si le choix de la marque de la carte de paiement a été fait par défaut ou volontairement par le porteur de la carte.

Les valeurs possibles sont :

00	Le choix a été fait automatiquement et par défaut
01	Le choix a été fait manuellemnet par votre client

Exemple : SELECTION=01

11.3.1.29 EMAILPORTEUR

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

Adresse email de votre client ayant réalisé le paiement.

Exemple : EMAILPORTEUR=test@ca-ps.com

11.3.2 Variables réponse des API

11.3.2.1 SITE

Format : 7 chiffres.

Numéro de site fourni par la solution Up2pay e-Transactions dans votre mail de bienvenue

Correspond à la même valeur que la variable SITE transmise dans l'appel (trame-question)

Exemple : SITE=1999888

11.3.2.2 RANG

Format : 2 chiffres ou 3 chiffres.

Numéro de rang fourni par la solution Up2pay e-Transactions dans votre mail de bienvenue.

Correspond à la même valeur que la variable RANG transmise dans l'appel (trame-question)

Remarque : si la valeur est envoyée sur 2 caractères elle sera préfixée par un 0 par la plateforme (réglementaire)

Exemple : RANG=001

11.3.2.3 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.

Correspond à la même valeur que la variable NUMQUESTION transmise dans l'appel (trame-question)

Exemple : 0145829183

11.3.2.4 NUMAPPEL

Format : 10 chiffres.

Référence de l'appel à la plateforme Up2pay e-Transactions qui vient d'être effectué et correspondant à cette trame-réponse.

Ce numéro d'appel est aussi visible dans votre Back-Office Vision dans le détail d'une opération.

Exemple : NUMAPPEL=0000782653

11.3.2.5 NUMTRANS

Format : 10 chiffres.

Référence transaction générée par la plateforme Up2pay e-Transactions de la transaction de paiement que vous venez de réaliser (avec succès ou non).

Ce numéro de transaction est aussi visible dans votre Back-Office Vision dans le détail d'une opération.

Exemple : NUMTRANS=1234567890

11.3.2.6 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 de votre client si le paiement est accepté.

Ce numéro d'autorisation est aussi visible dans votre Back-Office Vision dans le détail d'une opération.

Exemple : AUTORISATION=168753

11.3.2.7 CODEREPONSE

Format : 5 chiffres

Code réponse / erreur permettant de connaitre le résultat de l'opération exécutée : opération acceptée ou refusée.

En cas de succès de l'opération, vous recevez la valeur « 00000 ». Tous les autres codes réponse que vous pouvez recevoir correspondent à une erreur lors de l'exécution de l'opération. Vous trouvez la liste des codes d'erreur à l'annexe : *12.2-Codes réponse des APIs*.
Si vous recevez un code d'erreur au format « 001xx », il s'agit d'un code d'erreur du centre d'autorisation dont dépend le moyen de paiement (carte de paiement) saisi. Vous trouverez la liste des codes d'erreur de chaque centre d'autorisation à l'annexe : *12.3-Codes réponse du centre d'autorisation*.
Le code « 00100 » qui correspond à un succès du centre d'autorisation est modifié en « 00000 » pour signifier le succès de l'opération, vous ne recevrez donc pas « 00100 » mais « 00000 ».

Exemple : CODEREPONSE=00007 (date invalide)

11.3.2.8 REFABONNE

Format : jusqu'à 250 caractères

Référence de l'abonné (client et son moyen de paiement) utilisé pour les opérations de gestion de l'abonné : association d'une carte de paiement à enregistrer, réutilisation d'une carte de paiement enregistrée pour réaliser une nouvelle transaction, modification de la carte de paiement enregistrée, suppression de l'abonné.

Correspond à la même valeur que la variable REFABONNE transmise dans l'appel (trame-question).
Dans un contexte hors gestion d'abonné, cette variable est renvoyée vide (zéros binaires).

Exemple : REFABONNE=Client_005287_Mdp_0001 ou REFABONNE=HcsqXh5YHkCb

11.3.2.9 PORTEUR

Format : jusqu'à 19 caractères

Etiquette (token) du moyen de paiement généré lors des opérations (trames-question) de création ou de modification d'abonné (enregistrement du moyen de paiement).

Si cette variable est renseignée conjointement avec la référence d'abonné lors d'une prochaine opération, la carte de paiement enregistrée par votre client sera reconstituée par la plateforme Up2pay e-Transactions et permettra d'effectuer l'opération sans resaisie du numéro de carte par le porteur. Si le paiement est réalisé via les pages de paiement, la carte sera pré-saisie et masquée.

Exemple : TOKEN=NODMIOOCUB1N0BETO0TA

Voir aussi : *8-Tokenisation – Gestion des abonnées*

11.3.2.10 COMMENTAIRE

Format : jusqu'à 100 caractères

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

Exemple : COMMENTAIRE=e-Transactions + Gestion Automatisée des Encaissements

11.3.2.11 PAYS

Format : 3 caractères (code ISO-3166 alphabétique)

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

Exemple : PAYS=FRA

11.3.2.12 TYPECARTE

Format : jusqu'à 10 caractères

Type de carte / moyen de paiement utilisé pour le paiement.

Les valeurs possibles sont :

CB	ELECTRON
VISA	MAESTRO
MASTERCARD	VPAY

Correspond à la même valeur que la variable TYPECARTE si elle a été transmise dans l'appel (trame-question).

Si elle a été transmise dans l'appel (trame-question) mais vide, cette variable renvoie le type de carte détectée par la solution Up2pay e-Transactions à partir du numéro de carte fourni.

Exemple : TYPECARTE=VISA

11.3.2.13 SHA-1

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

Empreinte hashée SHA-1 du numéro de carte utilisé pour réaliser l'opération.
Le numéro de carte est hashé avec la méthode SHA-1. Cette empreinte est uniquement utilisable pour effectuer des contrôles de risque sur l'utilisation multiples de la même carte (sans la connaitre) ou l'utilisation de multiples cartes différentes (sans les connaitre).

Cette variable n'est renvoyée que si le champ SHA-1 est présent (même vide) lors de l'appel à l'API (trame-question).

Exemple : SHA-1= F8BF2903A1149E682BE599C5C20788788256AA46

11.3.2.14 STATUS

Format : jusqu'à 32 caractères

Envoyé uniquement dans les questions de TYPE 17 (Consultation d'une transaction).

Etat, sur la plateforme Up2pay e-Transactions, de la transaction pour laquelle vous demandez la consultation

Les valeurs possibles sont :

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

Exemple : STATUS=Capturé

11.3.2.15 REMISE

Format : jusqu'à 9 chiffres.

Envoyé uniquement dans les questions de TYPE 17 (Consultation d'une transaction).

Identifiant de télécollecte dans laquelle la transaction a été intégrée lors de sa remise en banque.

Exemple : REMISE= 509625890

11.3.2.16 MARQUE

Format : 1 caractère.

Correspondance avec la ou les marques de la carte qui a été utilisée.

Les valeurs suivantes peuvent être retournées :

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

Exemple : MARQUE=A

11.3.2.17 PRODUIT

Format : 1 caractère.

Correspondance avec la catégorie de la carte qui a été utilisée.

Les valeurs suivantes peuvent être retournées :

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 une prochaine version de protocole*

Exemple : PRODUIT=C

11.3.2.18 LONGUEUR

Format : 2 chiffres.

Correspondance avec la longueur de la carte qui a été utilisée.

Les valeurs suivantes peuvent être retournées :

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'.

Exemple : LONGUEUR=16

12. Codes retours

12.1 Codes de retour des pages de paiement (variable E avec PBX_RETOUR)

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue. Dans ce cas, il est souhaitable de faire une tentative sur l'autre site: tpeweb.e-transactions.fr ou tpeweb1.e-transactions.fr en fonction de celui que vous utilisez.
001xx	Paiement refusé par le centre d'autorisation [voir *12.3-Codes réponse du centre d'autorisation*]. En cas d'autorisation de la transaction par le centre d'autorisation de la banque ou de l'établissement financier privatif, le code erreur "00100" est remplacé directement par "00000".
00003	Erreur de la plateforme. Dans ce cas, il est souhaitable de faire une tentative sur l'autre site tpeweb.e-transactions.fr ou tpeweb1. e-transactions.fr en fonction de celui que vous utilisez.
00004	Numéro de porteur ou cryptogramme visuel invalide.
00006	Accès refusé ou site/rang/identifiant incorrect. Veuillez vérifier votre paramétrage ou le calcul de la signature HMAC (PBX_HMAC).
00008	Date de fin de validité incorrecte.
00009	Erreur de création d'un abonnement.
00010	Devise inconnue.
00011	Montant incorrect.
00015	Paiement déjà effectué.
00016	Abonné déjà existant (inscription nouvel abonné). Valeur 'U' de la variable PBX_RETOUR
00021	Carte non autorisée.
00029	Carte non conforme. Code erreur renvoyé lors de la documentation de la variable « PBX_EMPREINTE ».
00030	Temps d'attente > 15 mn par l'internaute/acheteur au niveau de la page de paiements.
00031	Réservé
00032	Réservé
00033	Code pays de l'adresse IP du navigateur de votre client non autorisé.
00040	Opération sans authentification 3D-Secure, bloquée par le filtre.
99999	Opération en attente de validation par l'émetteur du moyen de paiement.

Tableau 25 : Codes réponse de la donnée (E) PBX_RETOUR

12.2 Codes réponse des APIs

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 *12.3-Codes réponse 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".

00201	Le paiement est réalisé sans authentification 3D-Secure qui est requise par le centre d'autorisation de votre client. Vous devez réaliser une demande d'authentification avec le composant RemoteMPI. [voir *7.4.2-Authentification 3D-Secure*]
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.

Tableau 26 : Codes réponse des APIs

12.3 Codes réponse du centre d'autorisation

Cette information est transmise dans les informations de retour en fin de transaction.

Concernant le paiement avec les pages de paiement, si la donnée « **E** » est demandée lors de l'appel dans la variable **PBX_RETOUR** (voir *11.1.1.8-PBX_RETOUR*), vous retrouvez ces valeurs dans les 2 derniers chiffres du code d'erreur retourné si sa valeur est de la forme **001xx** *(où xx représentent les codes réponse du centre d'autorisation)*.

Concernant les opérations de paiement par API, vous retrouvez ces valeurs dans les 2 derniers chiffres du code d'erreur retourné (CODEREPONSE) si sa valeur est de la forme **001xx** *(où xx représentent les codes réponse du centre d'autorisation)*.

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

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès
01	Contacter l'émetteur de carte
02	Contacter l'émetteur de carte
03	Commerçant invalide
04	Conserver la carte
05	Ne pas honorer
07	Conserver la carte, conditions spéciales
08	Approuver après identification du porteur
12	Transaction invalide
13	Montant invalide
14	Numéro de porteur invalide
15	Emetteur de carte inconnu
17	Annulation client
19	Répéter la transaction ultérieurement
20	Réponse erronée (erreur dans le domaine serveur)
24	Mise à jour de fichier non supportée
25	Impossible de localiser l'enregistrement dans le fichier
26	Enregistrement dupliqué, ancien enregistrement remplacé
27	Erreur en « edit » sur champ de mise à jour fichier
28	Accès interdit au fichier
29	Mise à jour de fichier impossible
30	Erreur de format
33	Carte expirée
38	Nombre d'essais code confidentiel dépassé
41	Carte perdue
43	Carte volée
51	Provision insuffisante ou crédit dépassé
54	Date de validité de la carte dépassée
55	Code confidentiel erroné
56	Carte absente du fichier
57	Transaction non permise à ce porteur
58	Transaction interdite au terminal
59	Suspicion de fraude
60	L'accepteur de carte doit contacter l'acquéreur
61	Dépasse la limite du montant de retrait
63	Règles de sécurité non respectées
68	Réponse non parvenue ou reçue trop tard
75	Nombre d'essais code confidentiel dépassé
76	Porteur déjà en opposition, ancien enregistrement conservé
89	Echec de l'authentification

90	Arrêt momentané du système
91	Emetteur de cartes inaccessible
94	Demande dupliquée
96	Mauvais fonctionnement du système
97	Echéance de la temporisation de surveillance globale

Tableau 27 : Codes réponses du centre d'auto CB

12.4 Codes de retour HTTP

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

CLASSE DES CODES	DESCRIPTION
1xx	Information – Requête reçue, traitement en cours
2xx	La demande a été reçue avec succès reçue, comprise et acceptée *Exemple : 200 - La page a été fournie avec succès*
3xx	Redirection
4xx	Erreur de Client - La demande contient une mauvaise syntaxe ou ne peut pas être accomplie. *Exemple : 404 - La page demandée n'existe pas*
5xx	Erreur de serveur - Le serveur a échoué à accomplir une demande apparemment valable *Exemple : 500 - Incident serveur*

Tableau 28 : Codes retour HTTP

Pour plus de détails et la liste complète des codes retour HTTP, référez-vous à la norme du protocole HTTP1.1, nommée RFC2616.

12.5 Codes de retour de la librairie cUrl (erreurs des appels IPN)

Vous retrouvez ces codes d'erreur dans le mail qui vous est envoyé en cas d'erreur d'appel de votre URL IPN (Notification de Paiement Instantanée) indiquée à partir des serveurs de la solution Up2pay e-Transactions.

L'interprétation de ces codes d'erreur vous permet d'identifier le problème présent sur votre boutique empêchant la solution de vous envoyer les informations sur les transactions réalisées par les pages de paiement de la solution e-Transactions.

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

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

Tableau 29 : Codes erreur CURL

12.6 Codes réponses de l'API RemoteMPI (Authentification 3D-Secure)

Cette API vérifie l'ensemble des paramètres envoyés et affiche, renvoie un numéro d'erreur (Voir tableau ci-dessous) dans le BODY HTTP de la réponse à l'appel à en cas d'anomalie.
Ce numéro d'erreur concerne le traitement de l'API RemoteMPI et non l'exécution du contrôle 3DS-ecure par le MPI.

Rappel : Il n'y a pas de vérification effectuée 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 (RefMarchant)
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 duMPI
402	Erreur de taille du code erreur du MPI
403	Erreur de taille du XID reçu du MP
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 30 : Codes réponses du programme RemoteMPI

12.7 Codes d'erreur des serveurs MPI (Serveurs d'Authentification 3D-Secure)

Ces codes sont présents dans la variable 3DERROR des retours de l'API RemoteMPI. Ces codes sont retournés directement par les serveurs d'authentification 3D-Secure.

Attention : Ils ne sont pas à confondre avec les codes d'erreur de l'API qui sont retournés dans le BODY HTTP de la réponse à l'appel à l'API.

CODE	SIGNIFICATION	CODE (suite)	SIGNIFICATION (suite)
0	No Error	**1724**	PARes - the element TX.vendorCode is not valid
100	AuthReq received is invalid	**1725**	PARes - the element TX.eci is not valid
101	Merchant is not known	**1726**	PARes - the element Merchant is not found
102	Merchant is not active	**1727**	PARes - the element acqBIN is not found
103	invalid referrer	**1728**	PARes - the element merID is not found
104	An error occured during processing	**1729**	PARes - the element Purchase is not found
105	Currency is not supported	**1730**	PARes - the element xid is not found
106	Transaction not found	**1731**	PARes - the element date is not found
107	Brand is not supported	**1732**	PARes - the element purchAmount is not found
108	The validation post to the merchant failed	**1733**	PARes - the element currency is not found
1300	the HTTP return code is not found	**1734**	PARes - the element exponent is not found
1301	the HTTP return code is not valid	**1735**	PARes - the element pan is not found
1302	the received message contains no XML	**1736**	PARes - the element tx is not found
1303	not possible to import the xml in JDOM	**1737**	PARes - the element time is not found
1304	incorrect root element	**1738**	PARes - the element status is not found
1305	the element message is not defined	**1739**	PARes - the element cavv is not found
1306	the attibuut id is not defined for	**1740**	PARes - the element eci is not found
1307	the attibuut id is not defined for Extension	**1741**	PARes - the element cavvAlgorithm is not found
1308	the attibuut id and critical are not defined for Extension	**1742**	PARes - the element iReqCode is not found
1309	the attibuut critical is not defined for Extension	**1743**	PARes - the element Purchase.currency has not the same value as the one in the PAReq
1310	the element Extension is not correct	**1744**	PARes - the element Purchase.exponent has not the same value as the one in the PAReq
1311	the element version is not found	**1745**	the Signature.xmlns namespace is not found
1312	the version of the ThreeDSecureMessage is too old	**1746**	the Signature.xmlns namespace has a bad format
1313	the attribute critical is defined for Extension with value true	**1747**	the Signature.SignedInfo has a bad format
1314	Root element invalid	**1748**	the Signature.CanonicalizationMethod has a bad format
1315	Message element not found or invalid	**1749**	the Signature.CanonicalizationMethod has different namespace
1330	CRReq - the element Merchant is not found	**1750**	the Signature.SignatureMethod has a bad format
1331	CRReq - the element acqBIN is not found	**1751**	Signature.SignatureMethod has different namespace
1332	CRReq - the element merID is not found	**1752**	Signature.SignedInfo.Reference.URI not found
1333	CRReq - the element password is not found	**1753**	Signature.SignedInfo.Reference.URI has a bad format
1334	CRReq - the element CRReq is not found	**1754**	Signature.SignedInfo.Reference.DigestValue not found

1335	CRReq - the element version is not valid	**1755**	Signature.SignatureValue not found
1336	CRReq - the element Merchant.acqBIN is not valid	**1756**	Signature.KeyInfo not found
1337	CRReq - the element Merchant.merID is not valid	**1801**	Error - the element Error is not found
1338	CRReq - the element Merchant.password is not valid	**1802**	Error - the element version is not valid
1339	CRReq - the element serialNumber is not valid	**1803**	Error - the element errorCode is not valid
1350	CRRes - the element begin is not found	**1804**	Error - the element errorMessage is empty
1351	CRRes - the element end is not found	**1805**	Error - the element errorDetail is empty
1352	CRRes - the element action is not found	**1806**	Error - the element vendorCode is too long
1353	CRRes - the element CRRes is not found	**1807**	Error - the element errorCode is not found
1354	CRRes - the element serialnumber is not found	**1808**	Error - the element errorMessage is not found
1355	CRRes - the element version is not valid	**1809**	Error - the element errorDetail is not found
1356	CRRes - the element begin is not valid	**1901**	PATransReq - the element PATransReq is not found
1357	CRRes - the element end is not valid	**1902**	PATransReq - the element version is not valid
1358	CRRes - the element action is not valid	**1903**	PATransReq - the element Merchant.name is not valid
1359	CRRes - the element serialNumber is not valid	**1904**	PATransReq - the element Merchant.country is not valid
1360	CRRes - the element vendorcode is too long	**1905**	PATransReq - the element Merchant.url is not valid
1361	CRRes - the element iReqCode is not found	**1906**	PATransReq - the element amount is not found
1362	CRRes - the element IReqCode has bad format	**1907**	PATransReq - the element url is empty
1401	VEReq - the element pan is not found	**1908**	PATransReq - the element url has a bad protocol
1402	VEReq - the element Merchant is not found	**1909**	PATransReq - the element url is malformed
1403	VEReq - the element acqBIN is not found	**1910**	PATransReq - the element amount has bad format
1404	VEReq - the element merID is not found	**1911**	PATransReq - the element desc has bad format
1405	VEReq - the element password is not found	**1912**	PATransReq - the element frequency has bad format
1406	VEReq - the element VEReq is not found	**1913**	PATransReq - the element endRecur has bad format
1407	VEReq - the element version is not valid	**1914**	PATransReq - the element install has bad format
1408	VEReq - the element pan is not valid	**1915**	PATransReq - the element date has bad format
1409	VEReq - the element Merchant.acqBIN is not valid	**1916**	PATransReq - the element name has bad format
1410	VEReq - the element Merchant.merID is not valid	**1917**	PATransReq - the element fullpan has bad format
1411	VEReq - the element Merchant.password is not valid	**1918**	PATransReq - the element expiry has bad format
1412	VEReq - the element Merchant.password is not valid	**1919**	PATransReq - the element acs Id id has bad format
1501	VERes - the element VERes is not found	**1920**	PATransReq - the element login Id has bad format
1502	VERes - the element version is not valid	**1921**	PATransReq - the element password has bad format
1503	VERes - the element enrolled is not valid	**1922**	PATransReq - the element signed pares has bad format
1504	VERes - the element accId is empty	**1925**	PATrans - the element version is not valid
1505	VERes - the element accId is to long	**1926**	PATrans - the element PATransReq is not found
1506	VERes - the element url is empty	**1927**	PATrans - the element Merchant.id is not found
1507	VERes - the element url has a bad protocol	**1928**	PATrans - the element Merchant.name is not valid

1508	VERes - the element url is malformed	**1929**	PATrans - the element Merchant.country is not valid
1509	VERes - the element protocol is empty	**1930**	PATrans - the element Merchant.url is not valid
1510	VERes - the element protocol is not valid	**1931**	PATrans - the element Purchase.id is not found
1511	VERes - the element vendorcode is too long	**1932**	PATrans - the element Purchase.xid is not found
1512	VERes - the element CH is not found	**1933**	PATrans - the element Purchase.date is not valid
1513	VERes - the element enrolled is not found	**1934**	PATrans - the element Purchase.amount is not valid
1514	VERes - the element acctid is not found	**1935**	PATrans - the element Purchase.rawamount is not valid
1515	VERes - the element url is not found	**1936**	PATrans - the element Purchase.currency is not valid
1516	VERes - the element protocol is not found	**1937**	PATrans - the element Purchase.desc is not valid
1517	VERes - the element IReq is not found	**1938**	PATrans - the element Purchase.recurring is not valid
1518	VERes - the element iReqCode is not found	**1939**	PATrans - the element Purchase.installment is not valid
1519	VERes - the element IReqCode has bad format	**1940**	PATrans - the element CH.name is not valid
1520	VERes - the element acctId is the same as the pan	**1941**	PATrans - the element CH.pan is not valid
1601	PAReq - the element version is not valid	**1942**	PATrans - the element CH.exp is not valid
1602	PAReq - the element PAReq is not found	**1943**	PATrans - the element TX.time is not valid
1603	PAReq - the element Merchant is not found	**1944**	PATrans - the element TX.status is not valid
1604	PAReq - the element acqBIN is not found	**1945**	PATrans - the element TX.detail is not valid
1605	PAReq - the element merID is not found	**1946**	PATrans - the element TX.stain is not valid
1606	PAReq - the element name is not found	**1947**	PATrans - the element TX.eci is not valid
1607	PAReq - the element country is not found	**1948**	PATrans - the element TX.vendorCode is not valid
1608	PAReq - the element url is not found	**1949**	PATrans - the element SignedPARes is not valid
1609	PAReq - the element Purchase is not found	**1951**	PATransRes - the element PATransRes is not found
1610	PAReq - the element xid is not found	**1952**	PATransRes - the element version is not valid
1611	PAReq - the element date is not found	**1953**	PATransRes - the element iReq.IReqCode is not found
1612	PAReq - the element amount is not found	**1954**	PATransRes - the element iReq.IReqCode is not found
1613	PAReq - the element purchAmount is not found	**1955**	PATransRes - the element iReq.IReqCode is not valid
1614	PAReq - the element currency is not found	**1956**	PATransRes - the element iReq.IReqCode is not valid
1615	PAReq - the element exponent is not found	**1971**	CAVV - the element xid is not found
1616	PAReq - the element frequency is not found	**1972**	CAVV - the element pan is not valid
1617	PAReq - the element endRecur is not found	**1973**	CAVV - the element authResultCode is not valid
1618	PAReq - the element CH is not found	**1974**	CAVV - the element secondFactorAuthCode is not valid
1619	PAReq - the element CH.acctID is not found	**1975**	CAVV - the element cavvKeyIndicator is not valid
1620	PAReq - the element CH.expiry is not found	**1976**	CAVV - the element cardSequenceNumber is not valid
1621	PAReq - the element Merchant.acqBIN is not valid	**1977**	CAVV - the element cvr is not valid
1622	PAReq - the element Merchant.merID is not valid	**1978**	CAVV - the element unpredictableNumber is not valid
1623	PAReq - the element Merchant.name is not valid	**1979**	CAVV - the element atn is not found
1624	PAReq - the element Merchant.country is not valid	**5100**	Expiry date is invalid
1625	PAReq - the element Merchant.url is not valid	**5101**	Pan not found in local cache
1626	PAReq - the element url is empty	**5102**	No brand details foudn for that Merchant

1627	PAReq - the element url has a bad protocol	**5103**	Error occured during validate of VEReq"
1628	PAReq - the element url is malformed	**5104**	Error occured during build of VEReq
1629	PAReq - the element xid has bad format	**5105**	ThreeDSecureMessage Exception occured during validate and build of VEReq
1630	PAReq - the element date has bad format	**5106**	No connection details where found for that specific brand, merchant and pan
1631	PAReq - the element amount has bad format	**5107**	Exception occured during the post of the VEReq message to the VisaDirectory
1632	PAReq - the element purchAmount has bad format	**5108**	Invalid Handler/ Locator or Generator configured during processing of VEReq
1633	PAReq - the element currency has bad format	**5109**	Error occured during validate of Error"
1634	PAReq - the element exponent has bad format	**5110**	Error occured during build of Error
1635	PAReq - the element desc has bad format	**5111**	ThreeDSecureMessage Exception occured during validate and build of Error
1636	PAReq - the element frequency has bad format	**5112**	Exception occured during the post of the Error message to the VisaDirectory
1637	PAReq - the element endRecur has bad format	**5113**	Received an Error message instead of a VERes
1638	PAReq - the element install has bad format	**5114**	Unkown error
1639	PAReq - the element acctID has bad format	**5115**	Pan is not enrolled for 3D-Secure
1640	PAReq - the element expiry has bad format	**5116**	ThreeDSecure is not supported by the Issuer!
1641	PAReq - the element exponent is not numeric	**5117**	Recieved a badly formatted VERes, so we had to send an error to the VSD
1642	PAReq - the element gmtOffset is not found	**5118**	Version is too old
1643	PAReq - the element brands is not found	**5119**	Currency code not found
1644	PAReq - the element desc is not found	**5120**	Error occured during validate of PAReq"
1645	PAReq - the element pan is not found	**5121**	ThreeDSecureMessage Exception occured during validate and build of PAReq
1646	PAReq - the element gmtOffset is not valid	**5122**	No termUrl is found for the MPI
1647	PAReq - the element brands is not valid	**5123**	Exception occured during creation of the PaReq Form
1648	PAReq - the element recurring is not valid	**5124**	Unknown error occured during processing of VERes
1649	PAReq - the element installment is not valid	**5125**	Exception occured during decode and inflate of pares
1701	PARes - the element PARes is not found	**5126**	Recieved a badly formatted PARes, so we had to send an error to the VSD
1702	PARes - the element version is not valid	**5127**	An error occured during the validation of the xml signature
1703	PARes - the element Merchant.acqBIN is not valid	**5128**	An error occured during the logging process of the PAReq message
1704	PARes - the element Merchant.merID is not valid	**5129**	An error occured during the logging process of the PARes message
1705	PARes - the element xid has bad format	**5130**	An Exception occured when getting the PAReq from the cache, or during the parse and validate of it
1706	PARes - the element date has bad format	**5131**	An Exception occured during encryption/decryption of sensative data
1707	PARes - the element amount has bad format	**5132**	An error occured during parse and validate of the VERes message
1708	PARes - the element purchAmount has bad format	**5133**	An error occured during parse and validate of the PARes message
1709	PARes - the element currency has bad format	**5134**	The XML-signature of the PARes message is not a valid one
1710	PARes - the element exponent has bad format	**5135**	Error occured during validate of CRReq

1711	PARes - the element exponent is not numeric	**5136**	Error occured during build of CRReq
1712	PARes - the element TX.time is not valid	**5137**	ThreeDSecureMessage Exception occured during validate and build of CRReq
1713	PARes - the element TX.status is not valid	**5138**	Exception occured during the post of the CRReq message to the VisaDirectory
1714	PARes - the element pan is not valid	**5139**	unknown error occure during processing of CRRes
1715	PARes - the element TX.cavv is not valid	**5140**	Recieved a badly formatted CRRes, so we had to send an error to the VSD
1716	PARes - the element TX.eci is not valid	**5141**	Error occured during build of Veres
1717	PARes - the element TX.cavvAlgorithm is not valid	**5142**	Error occured during decode and inflate of PAReq
1718	PARes - the element IReq.iReqCode is not valid	**5143**	Unable to start authentication flow
1719	PARes - the element IReq.vendorCode is not valid	**5144**	Authentication was not successfull
1720	PARes - the element desc is not valid	**5145**	Error Getting VEReq out of transaction cache
1721	PARes - the element CH.exp is not valid	**5146**	Received status U
1722	PARes - the element TX.detail is not valid	**5147**	Received an Error message instead of a PARes
1723	PARes - the element TX.stain is not valid	**10000**	Unspecified error occured

Tableau 31 : Codes réponses des MPI (serveurs d'authentification)

13. Jeu de caractères

Le jeu de caractères supporté par les applications est présenté dans le tableau ci-dessous (sur base du code hexadécimal – ligne/colonne – de chaque caractère accepté). 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

14. 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

15. Exemples de codes

15.1 Exemple d'appel de l'API en 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);
```

```
echo "</PRE>";

// fermeture de la session
curl_close($curl);

?>
</body>
</html>
```

15.2 Exemple d'appel de la page de paiement avec clé HMAC

L'extrait de code suivant permet de calculer la clé HMAC et fournit le formulaire permettant d'appeler la plateforme de paiement :

```
<?php
// On récupère la date au format ISO-8601
$dateTime = date("c");
// On crée la chaîne à hacher sans URLencodage
$msg = "PBX_SITE=1999888".
"&PBX_RANG=32".
"&PBX_IDENTIFIANT=2".
"&PBX_TOTAL=".$_POST['montant'].
"&PBX_DEVISE=978".
"&PBX_CMD=".$_POST['ref'].
"&PBX_PORTEUR=".$_POST['email'].
"&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E".
"&PBX_HASH=SHA512".
"&PBX_TIME=".$dateTime;


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

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

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

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

// On crée le formulaire à envoyer
// ATTENTION : l'ordre des champs est extrêmement important, il doit
// correspondre exactement à l'ordre des champs dans la chaîne hachée
?>
<form method="POST" action="https://urlserveur.paybox.com/cgi/MYchoix_pagepaiement.cgi">
<input type="hidden" name="PBX_SITE" value="1999888">
<input type="hidden" name="PBX_RANG" value="32">
<input type="hidden" name="PBX_IDENTIFIANT" value="2">
<input type="hidden" name="PBX_TOTAL" value="<? echo $_POST['montant']; ?>">
<input type="hidden" name="PBX_DEVISE" value="978">
<input type="hidden" name="PBX_CMD" value="<? echo $_POST['ref']; ?>">
<input type="hidden" name="PBX_PORTEUR" value="<? echo $_POST['email']; ?>">
<input type="hidden" name="PBX_RETOUR" value="Mt:M;Ref:R;Auto:A;Erreur:E">
<input type="hidden" name="PBX_HASH" value="SHA512">
<input type="hidden" name="PBX_TIME" value="<? echo $dateTime; ?>">
<input type="hidden" name="PBX_HMAC" value="<? echo $hmac; ?>">
<input type="submit" value="Envoyer"> </form>
```

16. Glossaire

16.1 Autorisation (Auto)

Correspond au résultat positif d'une demande d'autorisation de paiement d'un montant donné auprès de la banque de votre client du moyen de paiement utilisé.
Sans autorisation acceptée, le paiement est refusé et la transaction n'a pas lieu.

Dans un contexte 3D-Secure, la demande d'autorisation n'est réalisée qu'après avoir effectué avec succès une demande d'authentification du titulaire de la carte par sa banque. Si la demande d'authentification n'est pas effectuée avec succès, la demande d'autorisation ne doit pas être réalisée.

Une autorisation seule doit être capturée (confirmée) pour pouvoir être remise en banque. SI vous effectuez un paiement en autorisation+capture (AUTORISATION SEULE=NON), la capture a lieu automatiquement et immédiatement après l'autorisation obtenue avec succès.

16.2 Capture

La capture d'une transaction précédemment autorisée (voir ci-dessus Autorisation), permet de la confirmer vis-à-vis de la solution Up2pay e-Transactions et de déclencher sa remise en banque (télécollecte).

Une autorisation seule doit être capturée (confirmée) pour pouvoir être remise en banque. SI vous effectuez un paiement en autorisation+capture (AUTORISATION SEULE=NON), la capture a lieu automatiquement et immédiatement après l'autorisation obtenue avec succès.

Tant que la transaction n'est pas capturée, votre client n'est pas débité et vous n'êtes pas crédité.

16.3 3D-Secure / American Express Safekey

La plupart des sites de commerce électronique, qui proposent de faire du paiement en ligne, utilisent les protocoles TLS 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 mais ne permettent pas l'authentification d'un client avec sa banque comme requis pour des paiements sécurisés et garantis.

Dans ce contexte, MasterCard et VISA ont conçu l'architecture 3D-Secure dont la finalité est de permettre aux banques d'authentifier les titulaires de la carte 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 / American Express Safekey permet :

- De s'assurer que le client 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.

Pour renforcer la protection des acheteurs lors de paiements à distance (online), la directive européenne DSP2 rend obligatoire l'authentification SCA (Strong Customer Authentication) de l'acheteur pour tout paiement électronique qu'il initie.

Ce traitement permet l'échange de données avec le commerçant et l'émetteur afin que ce dernier décide de l'authentification. Dorénavant, plus le commerçant envoie de donner au moment de l'authentification, plus les paiements ont des chances d'être autorisés.

La directive sur les Services de Paiement (DSP2) impose l'application de nouvelles normes à appliquer (Regulatory Technical Standards (RTS) dont une authentification forte (Strong Customer Authentication SCA) lors de paiement en ligne pour votre client : c'est à dire authentification à 2 facteurs.

La solution Up2pay e-Transactions transmet la demande d'authentification avec le choix « ne se prononce pas ». De ce fait, notre solution laisse la banque de votre client choisir le fait d'effectuer une demande d'authentification à son client ou non. Ainsi, vous êtes conforme à la réglementation et vous bénéficiez du transfert de responsabilité vers la banque de votre client en cas de contestation disant « ne pas être à l'origine de la transaction ».

Vous visualisez dans son back-office si la transaction est ou non garantie 3D-Secure / American Express Safekey. Les indicateurs suivant sont disponibles :

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

- ***Porteur authentifié*** *:* Indique si la carte de l'acheteur est enrôlée à 3D-Secure / American Express Safekey 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 / American Express Safekey

Si une transaction garantie 3D-Secure / American Express Safekey (indicateur à « OUI ») est contestée par votre client, l'impayé est supporté par la banque émettrice de la carte.
Par contre, si vous envoyez en banque une transaction non garantie, vous prenez le risque d'assumer le coût des impayés en cas de contestation du porteur.

Attention : 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 votre client en mode 3D-Secure mais générées automatiquement.

Même si vous avez obtenu la garantie 3D-Secure sur une transaction, vous devez toujours rester vigilant lorsque la transaction vous semble frauduleuse.

16.4 Encodage URL (url-encodé)

Tous les caractères ne sont pas autorisés dans les URL (voir la définition de URL ci-dessous). L'encodage URL permet de transformer certains caractères spéciaux afin que les données puissent être transmises.

Exemple : « ! » devient « %21 », « @ » devient « %40 »

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

16.5 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.

16.6 HMAC

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

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

16.7 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.

16.8 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).

16.9 TLS

Le protocole TLS (Transport Layer Security) permet la transmission sécurisée de données (par exemple de formulaires ou pages HTML sur le Web) et peut 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.

16.10 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`

16.11 Fichiers CSS

CSS est l'acronyme de « Cascading Style Sheets » ce qui signifie « feuille de style en cascade ».
Le CSS correspond à un langage informatique permettant de mettre en forme des pages web (HTML ou XML).

Ce langage est donc composé des fameuses « feuilles de style en cascade » également appelées fichiers CSS (extention « .css ») et contient des éléments de codage et d'indications définissant le style et le visuel des pages : polices de caractères, couleurs, positionnement des éléments, images de fond, encadrés, …

16.12 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.

16.13 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.