Objectif : réalisation d'un paiement simple (débit immédiat)
Le couple autorisation + capture, de TYPE 00003 ou 00053 vous permet de concilier les deux étapes citées ci-dessus, capturer une autorisation en une seule et même trame question/réponse

Opérations de Caisse
Objectif : consultation de transactions existantes et/ou action sur ces dernières
L'annulation de TYPE 00005 ou 00055 vous permet d'annuler une transaction autorisée mais non capturée ;
Le remboursement de TYPE 00014 vous permet de rembourser une transaction autorisée et capturée ;
La consultation de TYPE 00017 vous permet quant à elle, la consultation de n'importe quelle transaction.

Tokenisation
Objectif : enregistrement d'une empreinte de carte sur la plateforme Up2pay e-Transactions en vue d'une action ultérieur grâce au token renvoyé lors de l'enregistrement (fonctionnalité 1-clic)
L'inscription d'un abonné de TYPE 00056 vous permet l'enregistrement de la carte de votre client ;
La modification d'un abonné de TYPE 00057 vous permet d'agir sur un abonné existant ;
La suppression d'un abonné de TYPE 00058 vous permet de supprimer un abonné existant.
Suite à une création d'abonné, vous disposez d'un token vous permettant de faire appel à la carte bancaire d'un client sans avoir accès ni véhiculer de données cartes. Vous pouvez entre autre effectuer les opérations listées ci-dessus de TYPE 00051, 00052, 00053 ou 00055.

Gestion de la Marque
La requête MIF vous permet de connaitre les marques associées à la carte de votre client, ainsi que sa catégorie et le nombre de chiffres qui compose son numéro.

7.2 Calcul de la signature avec la clé HMAC

Afin de sécuriser les appels aux API de la solution Up2pay e-Transactions, c'est-à-dire d'authentifier que les appels proviennent bien de votre boutique et de garantir l'intégrité des données, la solution a choisi d'établir une authentification par empreinte HMAC servant de signature.

- **Etape 0 :** Si ce n'est déjà fait, vous devez générer et installer une clé secrète HMAC via l'accès à votre Back-Office Vision. La procédure est décrite au chapitre *2.4.1-Création de la clé HMAC dans votre Back-office Vision*.

- **Etape 1 :** Vous devez constituer une chaine de caractères à partir des paramètres envoyés lors de l'appel de l'API. Cette chaine est construite en concaténant l'ensemble des paramètres sous la forme « NOM_PARAMETRE=VALEUR » et séparés par le symbole « & ». Ci-dessous un exemple de chaine de caractères construite à partir de paramètres à envoyer :

```
VERSION=00104&TYPE=00003&SITE=1999887&RANG=32&NUMQUESTION=0000000002&MONTANT=1000&DEVISE=978&REFE
RENCE=Test&PORTEUR=1111222233334444&HASH=SHA512&DATEVAL=1017&CVV=123&ACTIVITE=024&DATEQ=24062015
```

  - **Attention**, l'ordre des paramètres concaténés dans la chaine de caractères doit être strictement identique à l'ordre dans lequel les paramètres sont envoyés à l'API.
  - **Attention**, vous devez utiliser les données « brutes » pour constituer la chaine de caractères. Par exemple, vous ne devez pas utiliser de fonctions pour « URL encoder » les valeurs.

- **Etape 2 :** procédez au calcul de l'empreinte HMAC, en utilisant :

- La chaine qui vient d'être construite
- La clé secrète obtenue via le Back Office
- Un sous-algorithme au choix que vous devez également préciser dans le paramètre HASH envoyé à la page de paiement (cf. *11.3.1.7-HASH* dans le Dictionnaire de Données). Attention, ce paramètre HASH est également intégré dans la chaine de caractères servant à calculer l'empreinte

- **Etape 3 :** le résultat obtenu (l'empreinte) doit alors être placé dans le champ HMAC de l'appel à l'API.

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

```
<html>
<body>
<?php
// On récupère la date au format ISO-8601
$dateTime = date("c");

// On crée la chaîne à hacher sans URLencodage
$msg ="VERSION=00104".
    "&TYPE=00003".
    "&SITE=1999887".
    "&RANG=32".
    "&NUMQUESTION=0000000002".
    "&MONTANT=1000".
    "&DEVISE=978".
    "&REFERENCE=Test".
    "&PORTEUR=1111222233334444".
    "&HASH=SHA512".
    "&DATEVAL=1017".
    "&CVV=123".
    "&ACTIVITE=024".
    "&DATEQ=24022021";

// On récupère la clé secrète HMAC (stockée dans une base de données cryptée) et que l'on renseigne
dans la variable $keyTest. Pour que le formulaire fonctionne, on prend la clef HMAC associée au
compte de test;
$keyTest =
"0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF012
3456789ABCDEF0123456789ABCDEF";

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

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

$hmac = strtoupper(hash_hmac('sha512', $msg, $binKey));

// La chaîne sera envoyée en majuscules, d'où l'utilisation de strtoupper()
// On crée le formulaire à envoyer à e-transactions
// ATTENTION : l'ordre des champs est extrêmement important, il doit
// correspondre exactement à l'ordre des champs dans la chaîne hachée
echo $hmac;  echo "\n"; echo $msg;
?>

<form method="POST" action="https://recette-ppps.e-transactions.fr/PPPS.php">
<input type="hidden" name="VERSION" value="00104">
```

```
<input type="hidden" name="TYPE" value="00003">
<input type="hidden" name="SITE" value="1999887">
<input type="hidden" name="RANG" value="32">
<input type="hidden" name="NUMQUESTION" value="0000000002">
<input type="hidden" name="MONTANT" value="1000">
<input type="hidden" name="DEVISE" value="978">
<input type="hidden" name="REFERENCE" value="Test">
<input type="hidden" name="PORTEUR" value="1111222233334444">
<input type="hidden" name="HASH" value="SHA512">
<input type="hidden" name="DATEVAL" value="1023">
<input type="hidden" name="CVV" value="123">
<input type="hidden" name="ACTIVITE" value="024">
<input type="hidden" name="DATEQ" value="24022021">
<input type="hidden" name="HMAC" value='<?php echo $hmac; ?>'>
<input type="submit" value="Envoyer">
</form>
</body>
</html>
```

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

7.3 Unicité des appels à l'API

Pour rappel, une variable « NUMQUESTION » envoyée dans les appels à l'API représente l'Identifiant Unique de la requête sur une journée permettant d'éviter les confusions au niveau des réponses en cas de questions multiples et simultanées.
Cette unicité permet également d'éviter la prise en compte en double d'un même ordre émis 2 fois par erreur.

Chaque appel doit avoir un numéro de question unique sur une journée **(y compris pour les tests).** Il peut 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).*

7.4 Effectuer un paiement

Un paiement par API est catégorisé dans l'une de ces deux typologies :

- Un paiement simple (de TYPE=0000X), vous permettant de réaliser une transaction (autorisation seule ou autorisation + capture) à l'acte, en transmettant les informations du porteur et de la carte à la solution Up2pay e-Transactions.
- Un paiement sur un abonné existant (de TYPE=0005X) vous permettant de réaliser une transaction (autorisation seule ou autorisation + capture) à partir d'une carte précédemment enregistrée de façon sécurisée par la plateforme Up2pay e-Transactions (abonné créé par les APIs ou en utilisant les pages de paiement de la solution e-Transactions).

Vous pouvez véhiculer une référence qui vous est propre quand vous réalisez des transactions en utilisant la variable ARCHIVAGE. Elle 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).

7.4.1 Contraintes

La collecte d'informations de paiement et leur transmission sécurisée à la solution Up2pay e-Transactions en mode API doit obligatoirement faire l'objet d'une déclaration auprès de l'organisme PCI :
https://www.pcisecuritystandards.org/

De plus, l'utilisation d'un certificat SSL sur votre boutique est hautement recommandé (requis dans la charte PCI) par les organismes de sécurité.

7.4.2 Authentification 3D-Secure

7.4.2.1 Principe

Le MPI (**M**erchant-**P**lug-**I**n) est un composant de la solution e-Transactions.
Il permet l'authentification des 3 acteurs de la transaction (Commerçant, Client Acheteur, Banques) à travers un ensemble de dialogues dans le cadre du programme 3D-Secure & American Express Safekey.

Pour rappel, le composant Remote MPI prend en charge les moyens de paiement suivants : CB, VISA, MASTERCARD, AMERICAN EXPRESS

Le dialogue est réalisé selon des spécifications CB / VISA / MASTERCARD et American Express et se décompose en 2 échanges :

1) Un premier échange vérifie sur les Directory Serveurs CB / VISA / MASTERCARD ET AMERICAN EXPRESS que la carte de votre client est enrôlée au programme 3D-Secure / American Express Safekey.

   Pour information : ces messages sont le VEReq (Verify Enrollment Request) et le VERes (Verify Enrollment Response).

2) Si la carte fait partie du programme 3D-Secure / American Express Safekey, un deuxième échange redirige votre client vers le site d'authentification de l'émetteur de la carte.

   Pour information : ces messages sont le PAReq (Payer Authentication Request) et le PARes (Payer Authentication Response).

Le résultat de ces échanges est un prérequis avant de poursuivre le processus de paiement avec un appel au service Up2pay e-Transactions.

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

Rester fidèle aux spécifications CB / VISA / MASTERCARD ET AMERICAN EXPRESS

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

Faciliter l'intégration avec les autres interfaces e-Transactions

Les données 3D-Secure / American Express Safekey nécessaires à la demande d'autorisation sont stockées sur notre plateforme et récupérer lors des opérations de paiement.

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

Cet identifiant de contexte ne concerne que les données d'authentification 3D-Secure / American Express Safekey. Il est tout de même nécessaire de renseigner en plus, les paramètres obligatoires et existants des appels à l'API d'opération de paiement.

Etapes du déroulement d'un paiement en utilisant le composant RemoteMPI et l'opération de paiement par appel des API :

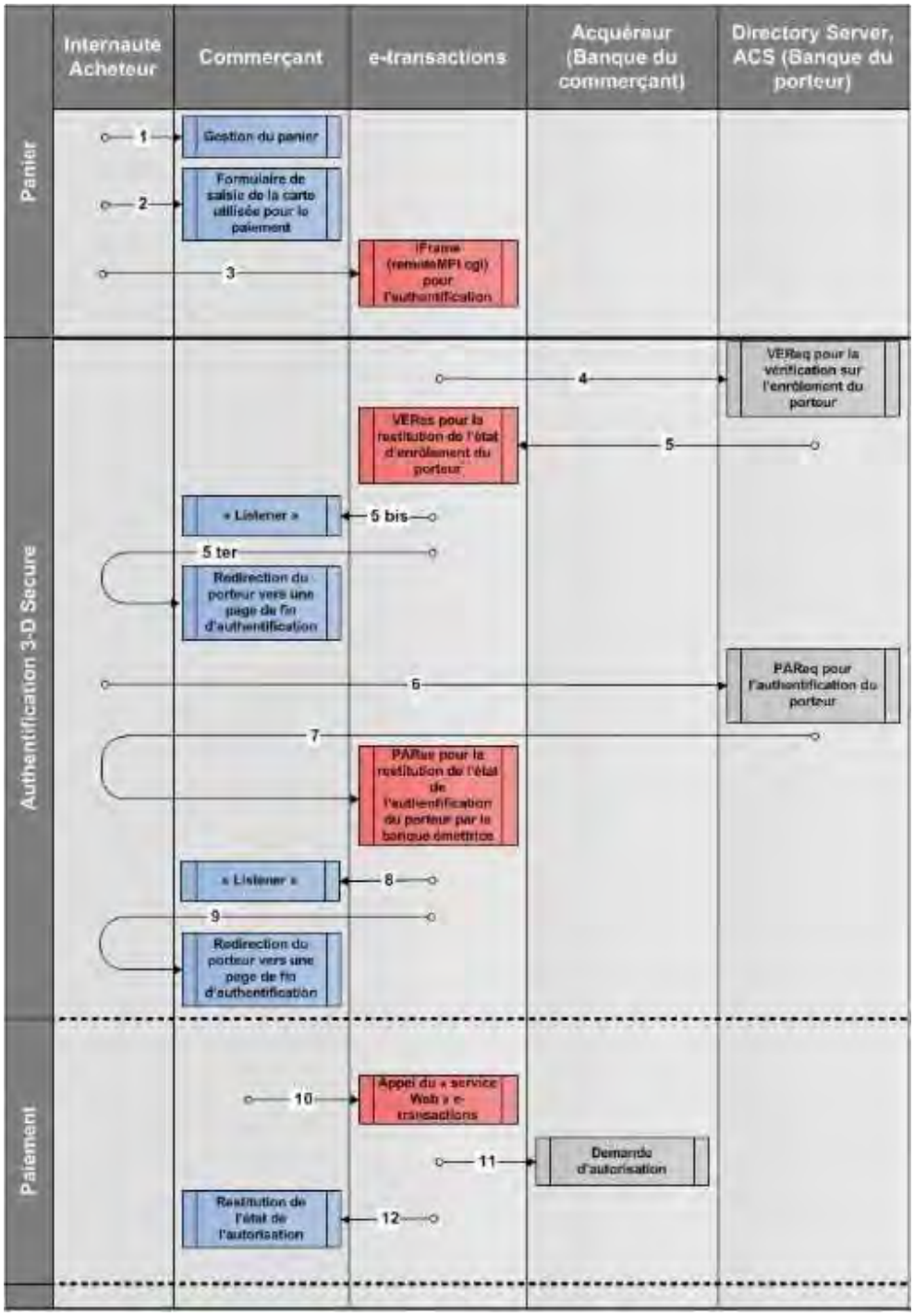

Figure 17 : Etapes d'authentification par RemoteMPI

ETAPE	IMPACT DANS VOTRE INTEGRATION	DESCRIPTION
1	**Oui**	L'acheteur passe une commande sur votre site marchand.
2	**Oui**	L'acheteur saisit ses informations carte (PAN, date d'expiration, cryptogramme visuel) sur votre site marchand.
3	**Oui**	Vous redirigez l'acheteur vers l'URL e-Transactions du service RemoteMPI en vue de son authentification «3D-Secure / American Express Safekey».
4	Non	Le composant vérifie l'enrôlement de la carte de votre client auprès des Directories Servers de CB, Visa ou MasterCard.
5	Non	Le composant récupère l'état de l'enrôlement de votre client et l'URL de redirection de votre client vers les pages d'authentification de sa banque.
5 bis	**Oui**	Appel de votre script serveur défini dans l'URL de retour de serveur à serveur (URLHttpDirect) dans les cas suivants : 1) Erreur d'accès au MPI **L'identifiant de contexte ID3D n'est pas renseigné.** 2) Erreur pendant la transmission des appels VEReq/VERes **L'identifiant de contexte ID3D n'est pas renseigné.** 3) La carte de votre client n'est pas enrôlée **L'identifiant de contexte ID3D est renseigné.** **Les étapes 6 à 9 de la cinématique ne sont pas réalisées.**
5 ter	**Oui**	Uniquement en cas de **NON enrôlement de la carte du client** au programme 3D-Secure / American Express Safekey, ce dernier est redirigé vers la page indiquée en URL de retour lors de l'appel à RemoteMPI. **Les étapes 6 à 9 de la cinématique ne sont pas réalisées.**
6	Non	Redirection de votre client vers les pages d'authentification de sa banque.
7	Non	Récupération de l'état sur l'authentification du client par sa banque.
8	**Oui**	Notification (appel serveur à serveur) sur l'état de l'authentification du client et sur la suite à donner pour la demande d'autorisation. **Si le client n'est pas authentifié vous ne devez pas effectuer la demande d'autorisation auprès de la banque acquéreur.**
9	**Oui**	Quel que soit l'état de l'authentification du client, ce dernier est redirigé vers la page indiquée en URL de retour lors de l'appel à RemoteMPI.
10	**Oui**	Votre serveur effetue une demande d'autorisation en utilisant les opérations de paiement de l'API de la solution Up2pay e-Transactions. Les informations sur l'état de l'authentification du client sont stockées sur la plateforme pendant 5 minutes et récupérables avec l'identifiant ID3D. Cet identifiant de contexte ID3D est à renseigner lors de l'appel aux API

		(GAE), en plus des autres paramètres nécessaires à l'opération de paiement.
11	Non	Demande d'autorisation faite par la plateforme auprès de l'acquéreur.
12	**Oui**	Restitution de l'état de la demande d'autorisation en retour de l'appel réalisé en étape 10.

Tableau 4 : Etapes d'authentification par RemoteMPI

7.4.2.2 Intégration de l'API (Remote MPI)

7.4.2.2.1 Appel

C'est un script installé sur nos serveurs qui donne l'accès au MPI e-Transactions via une API.

Retrouver l'URL d'appel à cette API au chapitre : *2.7.2-URLs à appeler*

Pour réaliser l'authentification de votre client, il faut le rediriger sur cette URL, en envoyant les paramètres par la méthode POST. La liste des paramètres est détaillée dans le paragraphe *11.2.1-Variables d'appel e-Transactions RemoteMPI*

Exemple d'appel via un formulaire HTML :

```
<html>
<body>
<form action="https://recette-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="1111222233334444" 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>
```

7.4.2.2.2 Réponse

Les données de retour se décomposent en 2 ensembles :

- Les **données utiles** à l'intégration
  - ID3D
  - StatusPBX
  - Check
- Les **données 3D-Secure / American Express Safekey** 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.

Récupération de l'ID de contexte 3D-Secure pour l'autorisation d'un paiement :
Pour faire référence à l'authentification 3D-Secure, vous devez a récupérer le contenu de la variable **ID3D** en retour de RemoteMPI et transmettre cette variable dans la requête Gestion Automatisée des Encaissements.

L'appel à l'API pour réaliser un paiement (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 3D-Secure.

Dans le cas d'un mauvais passage de paramètres à l'API RemoteMPI, seuls les champs IdSession, StatusPBX et Check sont renvoyés.

7.4.2.3 Gestion des erreurs

7.4.2.3.1 Codes erreur du programme Remote MPI

L'API RemoteMPI vérifie l'ensemble des paramètres envoyés et affiche en cas d'anomalie un numéro d'erreur.
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)

Voir codes d'erreur en annexe **:** *12.6-Codes réponses de l'API RemoteMPI (Authentification 3D-Secure)*

7.4.2.3.2 Codes erreur retournés par le MPI

Ces codes sont présents dans la variable 3DERROR. Il s'agit des numéros d'erreur renvoyés directement par le MPI et retranscris dans cette variable sans modification par la solution Up2pay e-Transactions.
Ils permettent de connaitre le résultat du déroulement de l'authentification 3D-Secure ainsi que le détail de l'échec ou la cause de l'erreur le cas échéant.

Voir codes d'erreur en annexe **:** *12.7-Codes d'erreur des serveurs MPI (Serveurs d'Authentification 3D-Secure)*

7.4.3 Effectuer une demande d'autorisation seule

Cette fonctionnalité permet de demander une autorisation bancaire sans confirmer la transaction, le porteur ne sera pas débité si vous n'adressez pas un 2ème message de confirmation à e-Transactions.
L'autorisation seule nécessite donc une seconde action pour que le débit intervienne, ce qui a pour conséquence la validation de la transaction.

Elle peut être utilisée pour les scenarii suivants :

- Débit après processus de validation (total ou partiel),
- Débit à l'expédition ou réception du colis (total ou partiel),
- Débit à la prise d'effet d'un contrat (total ou partiel),

- Autorisation simple pour vérifier la qualité de la carte transmise

Pour effectuer cette opération, vous devez utiliser un appel de TYPE=00001 ou TYPE=00051 (si utilisation d'un abonné déjà existant).

Attention : vous ne pouvez pas effectuer une demande d'autorisation seule sur une carte virtuelle dynamique (ex : e-CarteBleue) ou une carte à autorisation systématique. Celle-ci sera donc refusée. Dans ce cas, vous devez obligatoirement effectuer une demande de paiement avec débit immédiat ou différé.

Vous devez envoyer le contexte 3D-Secure (ID3D) récupéré lors de l'appel au composant RemoteMPI (voir *7.4.2-Authentification 3D-Secure*) pour que la solution Up2pay e-Transactions consolide les données de l'authentification 3D-Secure avec la demande d'autorisation.

Les variables échangées sont les suivantes (les données obligatoires sont en **rouge**) :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		**Contexte 3D-Secure renvoyé par la solution RemoteMPI**
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFABONNE	X		**Obligatoire si TYPE=00051 - Référence de l'abonné**
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction

TYPE	X		Type d'action à réaliser - **00001 ou 00051 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104
SELECTION	X		Indicateur de choix de la marque de la carte utilisée
EMAILPORTEUR	X		Adresse email de votre client ayant réalisé le paiement
MARQUE		X	Marque(s) de la carte qui a été utilisée
PRODUIT		X	Catégorie de la carte qui a été utilisée
LONGUEUR		X	Longueur de la carte qui a été utilisée

Tableau 5 : Liste des variables API pour paiement en autorisation seule

Pour plus de détail sur les variables des trames-question et des trames-réponse, reportez-vous à l'annexe *11.3-Intégration avec les API (GAE)*

Si vous recevez un code d'erreur « 00201 » (variable CODEREPONSE), il s'agit d'un code de refus indiquant qu'une demande d'authentification 3D-Secure n'a pas été réalisée avant la demande d'autorisation et qu'elle est requise par le centre d'autorisation de la banque de votre client. Dans ce cas, vous devez rediriger votre client vers l'authentification 3D-Secure (avec l'API RemoteMPI – Voir le chapitre *7.4.2-Authentification 3D-Secure)* et réaliser à nouveau une demande d'autorisation.

7.4.4 Effectuer une demande de débit immédiat (autorisation + capture)

Cette fonctionnalité permet d'effectuer directement une demande d'autorisation + une capture.
Cela signifie que lorsque la transaction de votre client est acceptée, il sera débité immédiatement et vous serez crédité, sans action requise de votre part. C'est automatique et vous serez crédité après traitement du fichier de remise par le Crédit Agricole.

Pour effectuer cette opération, vous devez utiliser un appel de TYPE=00003 ou TYPE=00053 (si utilisation d'un abonné déjà existant).

Vous devez envoyer le contexte 3D-Secure (ID3D) récupéré lors de l'appel au composant RemoteMPI (voir *7.4.2-Authentification 3D-Secure*) pour que la solution Up2pay e-Transactions consolide les données de l'authentification 3D-Secure avec la demande d'autorisation.

Les variables échangées sont les suivantes (les données obligatoires sont en **rouge**) :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATEQ	X		Date et heure d'envoi

DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		**Contexte 3D-Secure renvoyé par la solution RemoteMPI**
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFABONNE	X		**Obligatoire si TYPE=00053 - Référence de l'abonné**
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser - **00003 ou 00053 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104
SELECTION	X		Indicateur de choix de la marque de la carte utilisée
EMAILPORTEUR	X		Adresse email de votre client ayant réalisé le paiement
MARQUE		X	Marque(s) de la carte qui a été utilisée
PRODUIT		X	Catégorie de la carte qui a été utilisée
LONGUEUR		X	Longueur de la carte qui a été utilisée

Tableau 6 : Liste des variables API pour paiement en autorisation + capture

Pour plus de détail sur les variables des trames-question et des trames-réponse, reportez-vous à l'annexe *11.3-Intégration avec les API (GAE)*

Si vous recevez un code d'erreur « 00201 » (variable CODEREPONSE), il s'agit d'un code de refus indiquant qu'une demande d'authentification 3D-Secure n'a pas été réalisée avant la demande d'autorisation et qu'elle est requise par le centre d'autorisation de la banque de votre client. Dans ce cas, vous devez rediriger votre client vers l'authentification 3D-Secure (avec l'API RemoteMPI – Voir le chapitre *7.4.2-Authentification 3D-Secure)* et réaliser à nouveau une demande d'autorisation.

7.4.5 Effectuer un débit différé (automatique)

Il est possible de définir avec la variable « DIFFERE » le nombre de jours de différé (entre la transaction et sa capture (son débit) qui sera réalisé automatiquement sans action supplémentaire de votre part.

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

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

Attention : la garantie de paiement 3D-Secure n'est valable que 6 jours.

7.4.6 Trame-question

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour réaliser un paiement (autorisation seule, autorisation+capture ou autorisation + capture différée) est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête :

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

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

Pensez à bien ajuster la valeur des variables TYPE et DIFFERE afin de réaliser l'opération souhaitée :

- TYPE=00001 ou 000051, pas de variable DIFFERE : autorisation seule
- TYPE=00003 ou 000053, pas de variable DIFFERE : autorisation + capture immédiate
- TYPPE=00003 ou 000053, DIFFERE=**n** : autorisation + capture différée automatique après **n** jours

7.4.7 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci.

Les variables NUMTRANS et NUMAPPEL permettent, en cas d'autorisation seule, de réaliser plus tard une Capture (débit) de cette autorisation.

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.5 Confirmer un paiement (Capturer)

Cette requête permet de « capturer » - confirmer le débit pour que la transaction soit remise en banque - une transaction précédemment réalisée en autorisation seule. Cette précédente autorisation peut avoir été réalisée en utilisant les pages de paiement hébergées par la solution Up2pay e-Transactions (en redirection ou intégrées en iFrame) ou en utilisant les API (TYPE=00001 ou 00051).

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

Pour effectuer cette opération, vous devez utiliser un appel de TYPE=00002 ou TYPE=00052 (si utilisation d'un abonné déjà existant).

Important : Le montant peut être modifié uniquement s'il est inférieur au montant de la transaction initiale. Pour cela vous pouvez indiquer un montant différent dans la variable MONTANT.

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

- D'attendre quelques instants **(quelques secondes)** entre la demande d'autorisation seule et la capture
- D'envoyer la capture sur la même plateforme (url que vous utilisez pour effectuer vos appels – voir chapitre *2.7-URL à utiliser et adresses IP*) que la demande d'autorisation seule afin d'éviter d'éventuels problèmes de réplication entre les plateformes.

Les variables échangées sont les suivantes (les données obligatoires sont en **rouge**) :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte

HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFABONNE	X		**Obligatoire si TYPE=00052 - Référence de l'abonné**
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser - **00002 ou 00052 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104

Tableau 7 : Liste des variables API pour capture

7.5.1 Trame-question

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour capturer une transaction est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête :

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

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.5.2 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci.

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.6 Annuler un paiement

Cette requête permet d'annuler une transaction précédemment réalisée en autorisation seule. Cette précédente autorisation peut avoir été réalisée en utilisant les pages de paiement hébergées par la solution Up2pay e-Transactions (en redirection ou intégrées en iFrame) ou en utilisant les API (TYPE=00001 ou 00051).

Cette précédente autorisation ne doit pas avoir été déjà capturée sinon l'annulation ne pourra être réalisée et la trame-réponse vous renverra une erreur.

Pour effectuer cette opération, vous devez utiliser un appel de TYPE=00005 ou TYPE=00055 (si utilisation d'un abonné déjà existant).

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

Dans le cas des trames d'annulation qui suivent une demande d'auto seule, il est conseillé :

- D'attendre quelques instants **(quelques secondes)** entre la demande d'autorisation seule et l'annulation
- D'envoyer l'annulation sur la même plateforme (url que vous utilisez pour effectuer vos appels – chapitre *2.7-URL à utiliser et adresses IP*) que la demande d'autorisation seule afin d'éviter d'éventuels problèmes de réplication entre les plateformes.

Les variables échangées sont les suivantes (les données obligatoires sont en **rouge**) :

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

DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFABONNE	X		**Obligatoire si TYPE=00055 - Référence de l'abonné**
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser - **00005 ou 00055 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104

Tableau 8 : Liste des variables API pour annulation

7.6.1 Trame-question

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour annuler une transaction est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête :

```
VERSION=00104&TYPE=00005&SITE=1999887&RANG=063&NUMQUESTION=0667392882&MONTANT=1
000&DEVISE=978&REFERENCE=Test1&NUMAPPEL=0010736923&NUMTRANS=0005680492&ACTIVITE
=024&DATEQ=30012013&PAYS=&HASH=SHA512&HMAC=aa0d5822b7631bab3f63ad9738d6955cbbc0
bdeb7b6baaa566d68ab9b5b3e05d54ba011180633fbcf610a7d9cc46dd102529b356d8b489d752c
9d47658868643
```

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.6.2 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci.

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.7 Rembourser un paiement

Cette fonctionnalité permet d'effectuer le remboursement d'une transaction précédemment réalisée et remise en banque. Cette précédente transaction peut avoir été réalisée en utilisant les pages de paiement hébergées par la solution Up2pay e-Transactions (en redirection ou intégrées en iFrame) ou en utilisant les API (TYPE=00001+00002, 00051+00052, 00003 ou 00053).

Pour effectuer cette opération, vous devez utiliser un appel de TYPE=00014.

Vous devez indiquer le montant du remboursement que vous souhaitez réaliser dans la variable MONTANT qui peut être différent du montant de la transaction initiale.
Vous pouvez effectuer plusieurs remboursements pour une même transaction.

Attention : vous ne pouvez pas rembourser (en une fois ou en plusieurs fois) plus que le montant de la transaction initiale ou que le montant capturé de cette transaction si vous n'en avez capturé qu'une partie (voir *7.5-Confirmer un paiement (Capturer)).*

Pour faire référence à la transaction que vous souhaitez rembourser, vous devez réutiliser les variables NUMTRANS et NUMAPPEL transmis lors de la réponse obtenue à la réalisation de cette transaction ou lors de sa capture si la transaction a été réalisée en 2 temps : autorisation puis capture (surlignés en jaune).

Le remboursement par appel à l'API (total et partiel) est possible jusqu'à 75 jours à compter de la date de la transaction.
Pour tout remboursement de transaction au-delà 75 jours, vous devez effectuer l'action dans votre back-office Vision jusqu'à expiration de la carte utilisée pour le paiement inférieur à 13 mois.
Si la trasaction est supérieure à 13 mois, plus aucune action n'est réalisable via les applications Up2pay e-Transactions.

Les variables échangées sont les suivantes (les données obligatoires sont en **rouge**) :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser - **00014 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104

Tableau 9 : Liste des variables API pour remboursement

7.7.1 Trame-question

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour effectuer un remboursement sur une transaction est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête :

```
VERSION=00104&TYPE=00014&SITE=1999887&RANG=063&NUMQUESTION=0667392882&MONTANT=1
```

```
000&DEVISE=978&REFERENCE=Test1&NUMAPPEL=0010736923&NUMTRANS=0005680492&ACTIVITE
=024&DATEQ=30012013&PAYS=&HASH=SHA512&HMAC=aa0d5822b7631bab3f63ad9738d6955cbbc0
bdeb7b6baaa566d68ab9b5b3e05d54ba011180633fbcf610a7d9cc46dd102529b356d8b489d752c
9d47658868643
```

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.7.2 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci.

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.8 Consulter un paiement

Cette fonctionnalité vous permet de consulter l'état de la transaction dans le système Up2pay e-Transactions et de vous assurer ainsi de la cohérence et/ou de mettre à jour votre système de commande en fonction de l'état d'une transactions.

Pour effectuer cette opération, vous devez utiliser un appel de TYPE=00017.

Pour faire référence à la transaction que vous souhaitez consulter, vous devez réutiliser les variables NUMTRANS et NUMAPPEL transmis lors de la réponse obtenue à la réalisation de cette transaction ou lors de sa capture si la transaction a été réalisée en 2 temps : autorisation puis capture (surlignés en jaune).

Les variables échangées sont les suivantes (les données obligatoires sont en **rouge**) :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage
AUTORISATION	X	X	Numéro d'autorisation

CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser - **00017 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104

Tableau 10 : Liste des variables API pour consultation

7.8.1 Trame-question

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour consulter une transaction est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête :

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

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.8.2 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci.

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

7.9 Variables d'appel et de retour des APIs

Vous trouvez en annexe de ce document le détail complet de toutes les variables des trames-question et des trames-réponse : *11.3-Intégration avec les API (GAE)*

Cette annexe décrit pour chaque variable : sa description, son format, les TYPE d'opération pour lesquels elle est obligatoire (cas échéant) et un exemple d'utilisation.

8. Tokenisation – Gestion des abonnées

8.1 Principes

La création d'un nouvel abonné permet la prise d'empreinte de la carte de votre client (CB, VISA, MASTERCAD) pour différents cas d'utilisation ultérieurs, comme le paiement One-Click, l'abonnement, le débit différé complexe, etc.

Cette fonctionnalité est disponible uniquement avec l'option Gestion Automatisée des Encaissements (contrat Premium).

Par trame GAE, il est nécessaire de fournir à la solution e-Transactions les mêmes éléments que pour une demande d'autorisation, **avec un couple « variable = valeur » supplémentaire : une référence abonné unique**.

Dans le cas d'une création d'abonné, il est nécessaire de demander la sous-variable « U » dans PBX_RETOUR (voir chapitre 7.2.1 ci-dessous).

Lors d'une création d'abonné, la solution e-Transactions vérifie l'unicité de la référence abonné puis effectue les différents contrôles de validité de la carte saisie (date d'expiration, liste noire …).
Une fois la vérification terminée, une demande d'autorisation seule (sans débit) est effectuée. En cas de réponse positive du centre d'autorisation, ce nouvel abonné s'inscrit dans la liste des abonnés de votre contrat :

- Une partie du numéro de carte crypté est enregistrée sur le serveur sécurisé de la solution e-Transactions,
- L'autre partie du numéro vous est retournée sous forme d'un *token* ainsi que la date de fin de validité afin de les conserver avec la référence « abonné carte » sur votre serveur.

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

Pour les opérations de débit, crédit, annulation et suppression d'un abonné, il est nécessaire de fournir la référence abonné, le token de la carte en votre possession et la date de fin de validité, accompagnés des autres champs obligatoires dans le protocole d'échange de Gestion Automatisée des Encaissements.

Il est important de vérifier la date de validité de la carte notamment si la création de l'abonné a pour but d'initier un abonnement ou un paiement en plusieurs fois sur votre site. Vous pouvez donc vous assurer que la carte utilisée sera valable sur l'ensemble de l'échéancier et informer votre client avant l'échéance de sa carte (pour venir la modifier par exemple).

Sécurité :
Ce système a une sécurité double :

- Une partie des données est stockée sur les serveurs de la solution e-Transactions, l'autre dans votre base de données
- La solution e-Transactions stocke de façon sécurisée et en respect des normes PCI-DSS la partie des informations cartes enregistrée.

Ainsi, votre site ne stocke pas les informations de la carte bancaire de votre client, mais une étiquette (token) permettant de reconstituer lors d'un nouveau paiement les informations de paiement à utiliser.

Afin de garantir un haut niveau de sécurité, il est nécessaire que votre site internet respecte les normes PCI-DSS.

8.2 Création d'un Abonné

La création d'un abonné peut se faire de deux façons, et nécessite l'option Gestion Automatisée des Encaissements (contrat Premium).

8.2.1 Par page de paiement par redirection

Il est possible de créer un nouvel abonné à partir de la page de paiement par redirection.
Pour cela, il faut demander le champ « Référence de l'abonné » (U) dans PBX_RETOUR. Ceci indiquera à la solution e-Transactions qu'il faut créer un abonné avec les éléments de la carte utilisée pour le paiement en cours et renvoyer son étiquette pour un usage ultérieur

Exemple :
PBX_RETOUR =
Mt:M;Ref:R;Auto:A;Appel:T;Abo:B;ChoixPaiement:P;ChoixCarte:C;Erreur:E;Transaction:S;Pays:Y;
Abo:U; Signature:K

Si le paiement est réalisé avec succès, la réponse de e-Transactions contiendra alors les 2 informations nécessaires à utilisation ultérieure de la carte :

- Etiquette de la carte (Token)
- Date de fin de validité.

Ces données doivent être conservées dans votre base de données accompagnées de la référence abonné.

Attention : Le champ « Référence de l'abonné » (U) dans PBX_RETOUR ne doit être utilisé que pour des transactions effectuées par CB, VISA ou MASTERCARD.
Un formulaire de paiement valorisé avec cette donnée pour tout autre moyen de paiement entrainera une erreur, rendant le paiement impossible.

8.2.2 Par API lors d'un paiement

Pour toutes les demandes du TYPE 00051, 00052, 00053, 00055, 00057 et 00058, une inscription préalable de l'abonné est obligatoire. Pour cela, une trame avec le TYPE d'opération 00056 devra être envoyée vers notre serveur.

Pour rappel voici les opérations qui sont réalisables mettant en jeu les abonnés :

CODE	DESCRIPTION
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 11 : TYPE d'opérations par API sur abonnés

La création d'un nouvel abonné (trame de TYPE 00056) génère une demande d'autorisation pour le montant précisé dans la trame, auprès de la banque, afin de s'assurer de la validité de la carte.
L'acceptation de la demande d'autorisation par la banque de votre client est nécessaire pour créer l'abonné au niveau de la base de données, gérée par la plateforme e-Transactions.
Si la demande d'autorisation est refusée, la création d'abonné est impossible.

Vous devez indiquer une référence de cet abonné pour pouvoir y faire référence ultérieurement avec la variable REFABONNE.

Cette requête permet d'enregistrer une carte sur la plateforme e-Transactions.

En réponse, la plateforme renvoie un token (champs PORTEUR) qui correspond à une partie de la carte bancaire cryptée.
La saisie des informations bancaires se faisant sur votre site, il est nécessaire d'enregistrer la date de validité de la carte, car elle n'est pas retournée par e-Transactions.

Ces données (Token et date de validité) doivent être conservées dans votre base de donnée accompagné de la référence abonné, dans le respect des normes PCI-DSS.

8.2.2.1 Trame-question

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour créer un abonné est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête :

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

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

8.2.2.2 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci dont le Token (variable **PORTEUR**) correspondant au moyen de paiement enregistré pour cet abonné (REFABONNE) avec le numéro de carte transmis.

Vous devez stocker de façon sécurisée ce token (variable PORTEUR) associé à cet abonné (variable REFABONNE).

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

8.3 Débit de l'abonné

A la suite de la création d'un abonné, il peut être envoyé directement une trame de débit sur un abonné (TYPE 00052) seulement si :

- Le montant précisé lors de la trame de création correspond au montant à débiter
- La demande d'autorisation (ou demande de création d'abonné) date de moins de 7 jours.

S'il ne s'agit pas du même montant ou que la date de création d'abonné est supérieure à 7 jours, il faut alors émettre une trame d'autorisation + capture (TYPE=00053) ou une trame d'autorisation seule (TYPE=00051) suivi d'une trame de capture (TYPE=00052).

Cette requête (TYPE=00052) permet de capturer une transaction réalisée lors de l'enregistrement de la carte ou une transaction réalisée en mode autorisation seule. Cette précédente autorisation peut avoir été réalisée en utilisant les pages de paiement hébergées par la solution Up2pay e-Transactions (en redirection ou intégrées en iFrame) ou en utilisant les API (TYPE=00051

Le token (champ PORTEUR) précédemment généré doit être envoyé à la place du numéro de carte (en bleu), accompagné de la date de validité de la carte (DATEVAL) et de la référence abonné (REFABONNE).

Il est aussi possible d'utiliser un abonné précédemment enregistré pour réaliser des paiements en autorisation seule (puis capture ou annulation) ou en autorisation + capture automatique (immédiate ou différée). Voir les chapitres *7.4.3-Effectuer une demande d'autorisation seule*, *7.4.4-Effectuer une demande de débit immédiat (autorisation + capture)*, *7.4.5-Effectuer un débit différé (automatique)*, *7.5-Confirmer un paiement (Capturer)*, *7.6-Annuler un paiement*.

Les variables échangées sont les suivantes (les données obligatoires pour une opération autorisation+capture sont en **rouge**) :

VARIABLE	QUESTION	REPONSE	RESUME
ACQUEREUR	X		Moyen de paiement à utiliser
ACTIVITE	X		Provenance du flux envoyé
ARCHIVAGE	X		Référence archivage

AUTORISATION	X	X	Numéro d'autorisation
CODEREPONSE		X	Code réponse concernant l'état de la question traitée : opération acceptée ou refusée.
COMMENTAIRE		X	Messages pour information (ex : messages d'erreur)
CVV	X		Cryptogramme visuel de la carte
DATEQ	X		Date et heure d'envoi
DATEVAL	X		Date de validité de la carte
DEVISE	X		Devise (monnaie)
DIFFERE	X		Nombre de jours pour un paiement différé
ERRORCODETEST	X		Code erreur à renvoyer (pour tests)
HASH	X		Type d'algorithme de hachage pour le calcul de l'empreinte
HMAC	X		Signature calculée avec la clé secrète
ID3D	X		Contexte 3D-Secure renvoyé par la solution RemoteMPI
MONTANT	X		Montant
NUMAPPEL	X	X	Numéro d'appel retourné par la plateforme
NUMQUESTION	X	X	Identifiant unique et séquentiel
NUMTRANS	X	X	Numéro de transaction retourné par la plateforme
PAYS	X	X	Indication du pays de la carte
PORTEUR	X		Numéro de carte
RANG	X	X	Numéro de rang fourni par la banque
REFERENCE	X		Référence de la transaction
REFABONNE	X	X	**Numéro d'abonné** (vide en contexte hors abonnement)
REMISE		X	Identifiant de la remise
SHA-1	X	X	Indication que l'empreinte de la carte qui doit être retournée
SITE	X	X	Numéro de site fourni par la banque
STATUS		X	Etat de la transaction
TYPE	X		Type d'action à réaliser - **00051 ou 00053 pour cette opération**
TYPECARTE	X	X	Indication du type de carte
VERSION	X		Version du protocole - Valeur unique 00104

Tableau 12 : Liste des variables API pour paiement sur abonné

8.3.1 Trame-question auto+capture sur abonné

La trame-question à constituer pour la soumettre par API à la solution e-Transactions pour réaliser un paiement en autorisation + capture sur un abonné est de la forme suivante :

Les variables obligatoires sont en rouge.

Exemple Requête en débit immédiat (auto+capture) :

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

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

Pour rappel, la trame-question est une chaine constituée des différentes variables à envoyer – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

8.3.2 Trame-réponse

La trame-réponse à l'appel API de la solution Up2pay e-Transactions est de la forme suivante :

Exemple Réponse :

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

Cette trame-réponse va vous permettre de connaitre le résultat de l'opération demandée (variable CODEREPONSE) et le détail de celle-ci.

Pour rappel, la trame-réponse est une chaine constituée des différentes variables réceptionnées – de la forme « VARIABLE=VALEUR » - concaténées avec le caractère « & ».

8.4 Paiement « One-Click »

Le paiement One-Click (paiement en 1-clic) est un usage très utilisé en e-commerce.

Le principe est le suivant :
Lors de la réalisation d'une commande sur votre site marchand, votre client a la possibilité de choisir d'enregistrer sa carte bancaire afin de gagner du temps lors de ses prochains achats.
Il n'aura alors plus à ressaisir l'intégralité de son numéro de carte.
La solution e-Transactions vous propose d'enregistrer une empreinte de carte de vos clients (cartes CB, VISA, MASTERCARD) afin de proposer des paiements 1-clic lors de leurs futures commandes.

Pour le mettre en place, il est nécessaire d'effectuer une prise d'empreinte de sa carte, possible grâce à la création d'un abonné (voir chapitre précédent *8.2-Création d'un Abonné*)

A la suite de la création de l'abonné, vous pouvez renvoyer directement une trame de débit sur un abonné (TYPE=00052) si le montant précisé lors de la trame de création correspond au montant à débiter, et que la commande date de moins de 7 jours.
S'il ne s'agit pas du même montant ou d'un délai supérieur à 7 jours, il faut émettre une trame d'autorisation + débit (TYPE=00053) ou une trame autorisation seule (TYPE=00051) suivi d'une trame débit (TYPE=00052).
Par extension, il est alors possible de créer un système de paiement « 1-Clic » qui, après la création d'un abonné, permet d'effectuer des paiements sans ressaisir les informations de paiement.

8.4.1 Avec utilisation des pages de paiement et demande d'authentification 3D-Secure

Contexte : Dans le cadre de transactions One-click, un risque important d'usurpation d'identité a été constaté : si un fraudeur parvient à obtenir le login et le mot de passe d'un compte client, il peut utiliser frauduleusement une carte enrôlée pour du paiement One-click.

L'objectif du 3DS One-click est de vous permettre de bénéficier d'une authentification additionnelle lors de paiements utilisant les empreintes des cartes enregistrées.

Principe :
Votre client déroule son paiement via les pages de paiement par redirection et ses données cartes seront pré-saisies et masquées. Une demande d'authentification (3D Secure) peut être réaliser afin de vérifier l'identité du payeur.
Votre client est redirigé vers la page d'authentification 3D-Secure de sa banque.
Si l'authentification 3D-Secure est réussie et la demande d'autorisation acceptée, vous bénéficiez de la garantie de paiement au titre du 3D-Secure.

8.4.1.1 Création du token

La création de token reste inchangée, elle est réalisée conformément aux éléments décrits dans le chapitre précédent *8.2-Création d'un Abonné*.

8.4.1.2 Génération de l'appel

Pour utiliser le token dans un appel à la page de paiement par redirection, les variables suivantes devront être ajoutées dans le formulaire d'd'appel :

- PBX_TOKEN
- PBX_REFABONNE

La variable PBX_DATEVAL est facultative, mais sa valorisation permet le pré-remplissage de la date de validité de la carte sur la page de paiement.

8.4.1.3 Page de Choix

La page de choix des moyens de paiement n'est jamais affichée dans le cadre d'un paiement avec réutilisation d'un abonné existant donc avec envoi des variables PBX_REFABONNE et PBX_TOKEN.

Dans ce cas, votre client est automatiquement redirigé vers la page de paiement sans passer par la page de choix.

8.4.1.4 Page de Paiement et pré-remplissage des champs

Les formulaires de la page de paiement sont pré-remplis sur la base des informations associées au token.

Le PAN (Primary Account Number : numéro de la carte) est reconstitué sur les serveurs e-Transactions et un affichage masqué est réalisé.
Les premiers caractères sont remplacés par « # » et sont suivis des 4 derniers chiffres.

Ce champ ne peut pas être modifié par votre client.

La date de validité est pré-remplie avec la valeur fournie par le champ PBX_DATEVAL (si renseigné).
Ce champ peut être modifié par votre client.

Le cryptogramme visuel de la carte (CVV – 3 derniers chiffres au dos de la carte) ne sera, lui, jamais pré-saisie et votre client devra le renseigner pour soumettre le formulaire de paiement.

Il est possible de forcer le type de carte à utiliser en valorisant les variables PBX_TYPEPAIEMENT et PBX_TYPECARTE:

Moyen de paiement	PBX_TYPEPAIEMENT	PBX_TYPECARTE
CB	CARTE	CB
VISA	CARTE	VISA
MASTERCARD	CARTE	MASTERCARD

Tableau 13 : Type de carte forcé sur abonné

Figure 18 : Page de paiement e-Transactions pré-remplie (avec token et dateval)

8.4.1.5 Demande d'autorisation et vie de la transaction

Le reste du processus de paiement est identique à celui décrit pour réaliser un paiement avec les pages de paiement hébergées par la solution Up2pay e-Transactions (voir *3-Afficher une page de paiement*).

8.4.1.6 Exemple

8.4.1.6.1 Création d'abonné /prise d'empreinte

Un appel demandant la création d'un abonné est de la forme suivante en paiement par redirection (liste des variables envoyées) :

PBX_SITE = 9999999
PBX_RANG = 9595
PBX_TOTAL = 4000
PBX_IDENTIFIANT = 2
PBX_DEVISE = 978

PBX_CMD = 8qAzg4eOaNxl
PBX_PORTEUR = test@e-transactions.fr
PBX_REFABONNE = Client_123456_1
PBX_LANGUE = FRA
PBX_ANNULE = https://www.e-transactions.fr/index.html?CANCEL
PBX_EFFECTUE = https://www.e-transactions.fr/index.html?OK
PBX_REFUSE = https://www.e-transactions.fr/index.html?NOK
PBX_ATTENTE = https://www.e-transactions.fr/index.html?WAIT
PBX_REPONDRE_A= https://www.e-transactions.fr/index.html?CONFIRM
PBX_RETOUR = Mt:M;Ref:R;Auto:A;Appel:T;ChoixPaiement:P;ChoixCarte:C;Erreur:E;Transaction:S;
Pays:Y;Abo:U; Signature:K
PBX_SOURCE = RWD
PBX_TIME = 2021-01-20 09:35:05+100
PBX_HASH=SHA512
PBX_HMAC=…

8.4.1.6.2 Réponse obtenue

En réponse à l'exemple du formulaire d'appel précédent, les données suivantes ont été obtenues :

Mt=4000
Ref=8qAzg4eOaNxl
Auto=XXXXXX
Appel=190005979
ChoixPaiement=CARTE
ChoixCarte=CB
Erreur=00000
Transaction=190004884
Pays=FRA
Abo=SLDLrcsLMPC++2402++---
Signature=ZwHb16qLupNBzZcuKhfUpU%2FXEv%2BhKRCqOHOrGfLFfpfRqQ8uZEGn3MXwuvyFQGY0
YTAXCuHC2qiSvlWf9zZhyTx9Q%2B4nlvYQQF4Nk8QxJhMd0CCo7CBh8KwgcHXHxRAVmZL5GhRzEx
LD1qUsJ93FkZBkfV5fssx08RxCcij2WVc%3D

Attention : la date de validité de la carte qui est retournée au format AAMM (ici 2402 pour Février 2024). Lorsque vous réutiliserez cette carte, vous devrez indiquer sa date de validité au format MMAA (soit 0224 ici).

8.4.1.6.3 Utilisation du token

Pour un nouveau paiement à réaliser par votre client, vous pourrez faire référence à ce moyen de paiement enregistré (Token).
Ci-dessous un exemple des paramètres que vous enverrez à la page de paiement pour que le numéro de carte et la date de validité soient pré-saisis :

PBX_SITE = 1666666
PBX_RANG = 16
PBX_TOTAL = 5000
PBX_IDENTIFIANT = 2
PBX_DEVISE = 978
PBX_CMD = HcsqXh5YHkCb
PBX_PORTEUR = test@e-transactions.fr

PBX_LANGUE = FRA
PBX_ANNULE = https://www.e-transactions.fr/index.html?CANCEL
PBX_EFFECTUE = https://www.e-transactions.fr/index.html?OK
PBX_REFUSE = https://www.e-transactions.fr/index.html?NOK
PBX_ATTENTE = https://www.e-transactions.fr/index.html?WAIT
PBX_REPONDRE_A= https://www.e-transactions.fr/index.html?CONFIRM
PBX_RETOUR = Mt:M;Ref:R;Auto:A;Appel:T;Abo:B;ChoixPaiement:P;ChoixCarte:C;Erreur:E;
Transaction:S;Pays:Y;Signature:K
PBX_TYPECARTE = CB
PBX_TYPEPAIEMENT = CARTE
PBX_SOURCE = RWD
PBX_REFABONNE = Client_123456_1
PBX_DATEVAL = 0224
PBX_TOKEN = SLDLrcsLMPC
PBX_TIME = 2021-02-20 09:40:05+100
PBX_HASH=SHA512
PBX_HMAC=…

8.5 Paiement récurrents

Un paiement récurrent est défini selon un montant, une périodicité, une fréquence, pour un client donné.
Il s'agit d'un abonnement (exemple), pour lequel votre client sera débité sans intervention de sa part à chaque mensualité.
L'utilisation du token via la création d'abonné permet de répondre à ce besoin en tout flexibilité :
En effet, c'est votre site marchant qui crée et gère les paiements par l'envoi de trames d'autorisation seule ou d'autorisation + capture sur abonné (trames de TYPE=00051+00052 ou 00053) en suivant l'échéancier que vous avez préalablement défini.

C'est votre système informatique qui gère l'ensemble des échéances et déclenchent les paiements au bon moment. Vous devez donc faire en sorte de pouvoir visualiser les échéances à venir, stopper, si besoin, l'échéancier ou ajouter des fonctionnalités avancées qui vous sont propres. Dans votre Back-office Vision Air, vous ne verrez que les paiements que vous aurez réalisés.

Pour tout paiement récurrent, il convient de vérifier la date de validité de la carte afin de prévenir votre client avant expiration de celle-ci, vous permettant alors d'effectuer une mise à jour grâce à la trame de modification d'un abonné (TYPE=00057).

9. Gestion des abonnements

Les fonctions décrites dans ce paragraphe concernent l'intégration des paiements avec la page de paiement (voir chapitre *3-Afficher une page de paiement*).

Cette fonction est uniquement disponible si vous avez souscrit l'offre PREMIUM Up2pay e-Transactions.

9.1 Principe

La gestion des paiements par abonnement vous permet de gérer des échéances de paiement périodiques et déterminées à l'avance selon les conditions définies entre vous et vos clients. Ainsi, une fois le paiement initial effectué, votre client est débité de façon cyclique suivant une fréquence que vous avez préalablement définie.

Avantages et inconvénients de cette fonctionnalité :

- La gestion de l'abonnement sur e-Transactions est une gestion de base : elle ne prévoit que des cas simples d'abonnements, basés sur la reconduction périodique de paiement d'une même somme, sur une période souhaitée initialement. Ces paramètres ne peuvent pas, par la suite, être modifiés en accord avec ce qui a été convenu avec votre client.

- Notre système offre une souplesse de paramétrage permettant notamment, avec la gestion des différés, un large éventail de déclenchement de la première reconduction de l'abonnement.

- Il est à noter qu'en cas d'échec (refus d'autorisation bancaire) sur une échéance**, la plateforme de paiement n'assure pas de représentation et stoppe les futures échéances. L'abonnement prend alors fin.**

- Vous pouvez suivre vos abonnements via votre accès au Back Office Vision Air.

La mise en place de cette option nécessite la modification du contenu de la variable PBX_CMD comme expliqué ci-dessous, par l'ajout de « sous-variables » représentant la définition de l'abonnement (montant, fréquence, durée, date d'échéance, délai de mise en place).

Attention : L'URL IPN (voir chapitre *5-Notifications de Paiement Instantanées (IPN)*) est également appelée aussi bien en cas de reconduction réussie, qu'échouée. La variable ETAT_PBX est ajoutée à l'URL d'appel avec comme information PBX_RECONDUCTION_ABT permettant de distinguer cet appel.

Par exemple :
http://www.commerce.fr/traite.php?ETAT_PBX=PBX_RECONDUCTION_ABT&Mt=1200&Trans=1234567
8&Ref=MaReference&Autorisation=987654&NumAbonnement=56789"

9.2 Création d'un abonnement

La gestion de l'abonnement s'effectue via différentes « sous-variables » devant être insérées à la fin de la référence commande précisée dans la variable « PBX_CMD ».

La taille des variables doit être respectée et le nom de celles-ci est fixe et en majuscule.

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

Tableau 14 : Liste des variables pour abonnements simples

La valeur de chaque variable est directement ajoutée après le nom de la variable. PBX_QUAND03 pour indiquer que les échéances ont lieu le 3 de chaque mois d'échéance.

Les autres informations du formulaire de paiement ne changent pas.
La devise (uniquement Euro) est indiquée grâce à la variable PBX_DEVISE et le montant du premier règlement (qui peut être différent des prélèvements de l'abonnement) est présent dans la variable PBX_TOTAL.

Attention : PBX_TOTAL correspond au montant du 1er paiement qui est réalisé le jour de la commande, et qui permet de débuter l'abonnement. Si ce 1er paiement est réalisé en autorisation seule (voir *3.6-Paiement en autorisation seule*) et que vous ne capturez pas cette transactions, l'abonnement est tout de même créé avec le moyen de paiement utilisé lors du 1er paiement mais ce 1er paiement peut ne pas être débité.

Exemples d'abonnements :

Exemple 1 :

```
PBX_SITE=1999887&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1500&PBX_DEVISE=978&PBX
_CMD=ma_ref123PBX_2MONT0000000500PBX_NBPAIE00PBX_FREQ01PBX_QUAND28PBX_DELAIS005&
PBX_PORTEUR=test@gmail.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512
&PBX_TIME=2011-0228T11:01:50+01:00
```

Si le paiement initial (15 euros, soit 1500 centimes) est effectué le 28 novembre par exemple, la création de l'abonnement aura lieu le 03 décembre (car la prise en compte de l'abonnement se fait 005 jours plus tard via PBX_DELAIS).
Tous les prélèvements sont d'un montant de 5 euros (soit 500 centimes) (PBX_2MONT), réalisés le 28 (PBX_QUAND) de tous les mois (PBX_FREQ=01) jusqu'à une demande de résiliation (PBX_NBPAIE=00) de votre part ou un rejet du centre d'autorisation (si la carte bancaire est arrivée à expiration par exemple).
La première échéance, suite au paiement initial, sera déclenchée le 28 janvier de l'année suivante.

Exemple 2 :

```
PBX_SITE=1999887&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1500&PBX_DEVISE=978&PBX
_CMD=ma_ref123PBX_2MONT0000000550PBX_NBPAIE10PBX_FREQ03PBX_QUAND31&PBX_PORTEUR=t
est@gmail.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=201 1-
0228T11:01:50+01:00
```

Si le paiement initial (15 euros) est effectué le 28 novembre par exemple, le premier prélèvement aura lieu le 31 décembre (car la prise en compte de l'abonnement est immédiate via PBX_DELAIS qui est inexistante).

10 prélèvements (PBX_NBPAIE) d'un montant de 5,50 euros (PBX_2MONT) seront réalisés tous les 3 mois (PBX_FREQ) le dernier jour du mois (PBX_QUAND).

Lorsqu'un abonnement est créé, un mail « ticket de paiement » vous est envoyé (à condition d'avoir activé la réception des tickets de paiement dans votre back-office Vision Air) ainsi qu'à votre client avec une mention précisant le montant et la date du prochain règlement.

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

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

9.3 Paiement en plusieurs fois (4 fois maximum)

Le paiement en plusieurs fois répond à un besoin légèrement différent de l'abonnement. Alors que l'abonnement est basé sur des montants fixes à échéances régulières, le paiement en plusieurs fois permet de configurer chaque échéance librement, en termes de montants et de dates, dans la limite de 3 paiements en plus du paiement initial pour une durée ne pouvant excéder 89 jours (strictement inférieur à 90 jours).

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

Contrairement à l'abonnement qui se paramètre en « sous-variables » dans PBX_CMD, le paiement en plusieurs fois fait appel à des variables principales envoyées aux pages de paiement hébergées par la solution Up2pay e-Transactions.

Exemple :

```
PBX_SITE=1999887&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1000&PBX_DEVISE=978&PBX_CMD=TESTcacp&PBX
_PORTEUR=test@gmail.com&PBX_RETOUR=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=20110228T11:01:5
0+01:00&PBX_2MONT1=2000&PBX_DATE1=01/02/2013&PBX_2MONT2=3000&PBX_DATE2=15/02/2013
```

Dans cet exemple, la somme de 10€ sera débitée immédiatement, puis la somme de 20€ sera débitée le 1er février, et enfin, 30€ seront débités de 15 février.
Comme pour les abonnements, l'échéancier est conservé par notre plateforme e-Transactions, et une fois le premier paiement terminé, le commerçant n'a plus à gérer de nouveaux appels vers la plateforme pour déclencher les paiements suivants.

9.4 Fin des abonnements

L'abonnement peut se terminer de3 façons différentes :

- Fin à échéance programmée : lorsque toutes les échéances d'un abonnement ont été traitées avec succès, l'abonnement se termine de lui-même.
- Fin en échec : lorsque l'une des échéances échoue, la représentation de l'échéance ultérieurement est impossible. L'abonnement est clôturé et vous êtes informé de ce résultat par un mail.

- Résiliation par vos soins : vous pouvez arrêterà tout moment l'abonnement en cours en vous rendant sur votre Back-Office Vision Air.

10. Personnalisation de la page de paiement

10.1 Principe

La page de paiement affichée par défaut est la page « standard » de la plateforme Up2pay e-Transactions.

La solution e-Transactions vous offre des d'options permettant d'afficher une page de paiement reprenant des éléments de votre charte graphique.

Nous vous offrons une méthode simple et efficace pour personnaliser votre page de paiement en utilisant un logo et votre 'thème couleur'.

Voici la page de paiement (en responsive web design) sans aucune personnalisation :

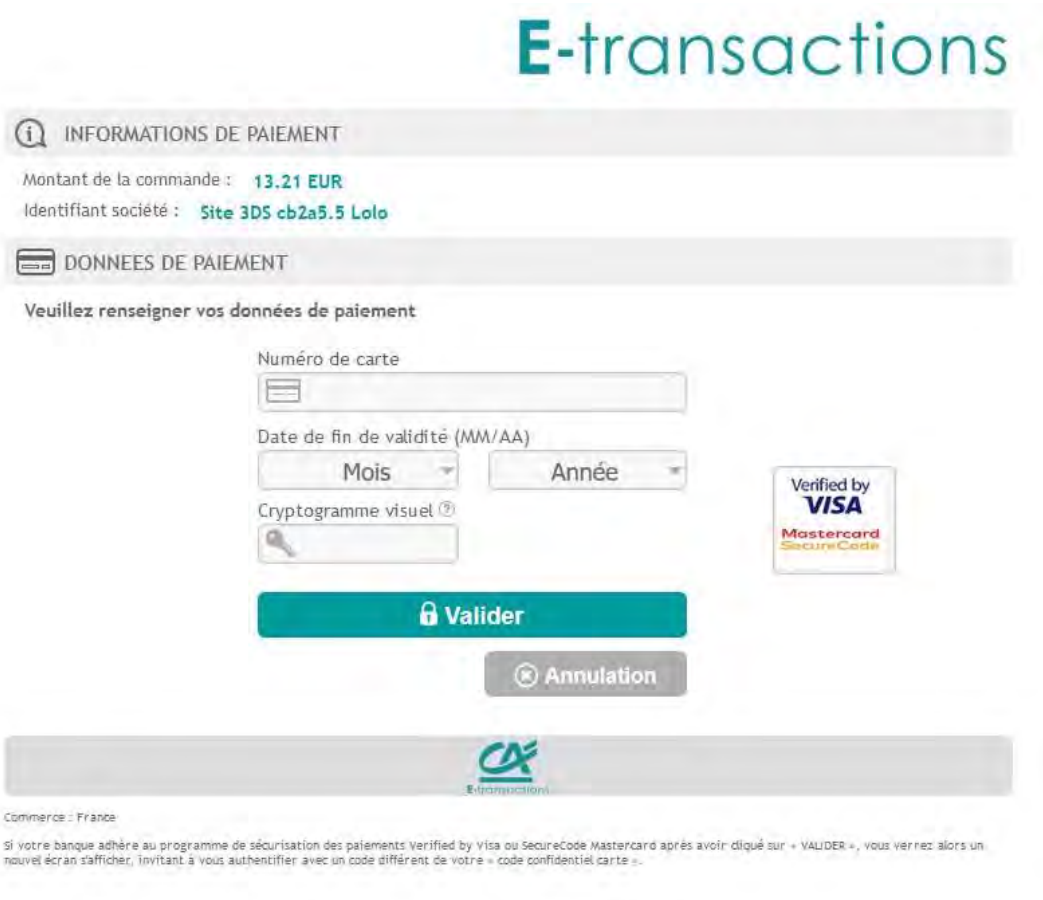

Figure 19 : Page de paiement en responsive

Procédure pour transmettre les éléments de personnalisation

Tous les éléments permettant la personnalisation de la page de paiement du commerçant doivent être transmis au Support Technique par mail à l'adresse support@e-transactions.fr en indiquant votre N° de SITE, RANG et IDENTIFIANT (informations présente dans votre mail de bienvenue).

E-mail : support@e-transactions.fr
Téléphone : 0 810 812 810 (1)

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

10.2 Page de choix des moyens de paiement

La page de présélection des types et moyens de paiement s'affiche avant la page de paiement si votre contrat dispose de moyens de paiement alternatifs actifs : American Express, JCB Card, PayPal, Paylib, Titres Restaurant, Cv-Connect,.

Cette page de choix de moyens de paiement est également personnalisable comme la page de paiement (chapitre suivant).

Figure 20 : Page de choix des Moyens de paiement personnalisée

10.3 Page de paiement

10.3.1 Le logo « commerce » en en-tête de page

Vous pouvez positionner votre logo en haut de la page de paiement affiché par la plateforme e-Transactions.

Figure 21 : Page de paiement personnalisée

Méthode pour ajouter votre logo sur la page de paiement :

```
/*logo for the merchant*/

#pbx-logo {
       background: url("logo_e-transactions.png") no-repeat center top;
       background-size:contain;

       height:40px;
}
```

10.3.2 Les boutons

La page de paiement e-Transactions intègre par défaut les boutons suivants :

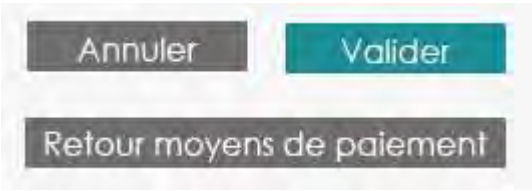

Figure 22 : Personnalisation des boutons de page de paiement

Vous pouvez personnaliser vos propres boutons, ces derniers doivent être envoyés au format « gif » dans toutes les langues que vous souhaitez.

Figure 23 : Page de paiement avec boutons personnalisés

10.3.3 Le choix de la langue d'affichage de la page

Les différents textes dans la page de paiement, ainsi que les boutons « Valider », « Annuler », « Retour boutique », « Retour choix paiement », … peuvent être affichés dans différentes langues.

Vous devez impérativement nous fournir les boutons dans les langues que vous souhaitez intégrer en plus de celles proposées (par défaut ou en option).

Les langues proposées par défaut sont :

- Français,
- Anglais,
- Allemand,
- Espagnol.

En contactant le Service Support e-Transactions, vous pouvez demander à enlever une des langues proposées par défaut ou à rajouter une langue optionnelle.

Les langues « optionnelles » sont :

- Italien,
- Néerlandais,
- Suédois,
- Portugais.

10.3.4 Le fond d'écran

Le fond de la page de paiement peut être également personnalisé.

Pour cela, vous devez transmettre au Service Support e-Transactions, le fichier électronique avec l'image souhaitée.

Ce fichier doit être du type « gif » (20 Ko maximum).

Par défaut, le fond de la page est blanc.

10.3.5 La police et la couleur du texte

Si vous souhaitez harmoniser le style et la couleur de police du texte de votre page de paiement à votre site marchnad , transmettez au Service Support e-Transactions une « feuille de style » (fichier .css).

A défaut de ce fichier, la couleur et le type de police utilisés sont ceux paramétrés dans le navigateur du client.

Un fichier de style web CSS (Cascading Style Sheets) permet de personnaliser la mise en page des différents éléments qui composent votre document. Ainsi, en fonction des éléments décrits dans ce fichier, les pages de paiement peuvent prendre différentes présentations (fond d'écran coloré, texte et police d'écriture identique à celle de votre site marchand, etc.).)

Figure 24 : Exemple de fichier CSS

10.3.6 La couleur du thème

Une couleur de thème principale, correspondante à votre charte graphique, peut être utilisée.

Plusieurs éléments de la page de paiement sont personnalisables afin de l'adapter à votre image :

- **L'en-tête** en modifiant le style du bloc « pbx-logo » [uniquement couleur et logo modifiables]

```
/* for 480px width or less */
/* when on a small width screen the header is changed to mimum*/
@media all and (max-width: 480px) {
       #pbx-logo{     position:absolute;     background:#009b9d; }
}
```

- **Le montant à payer et le texte identifiant votre entreprise en utilisant une couleur unique** (ou une différente)

```
/*the order amount and company identifier*/

#pbx-transaction-summary .label {
        color: #009b9d;
}
```

- **Les blocs divers de la page et des boutons de validation** :

```
/*Header for the frames, validation button and footer*/

.pbx-frame h1, #pbx-mean-payment-header, #pbx-footer, #pbx-button-validate {
     background-color: #009b9d;

}
```

- **Les autres boutons** :

```
/*the secondary buttons*/

#pbx-button-cancel,#pbx-button-back,#pbx-mean-payment-content-cancel {
     background-color: #7F7C7C;

}
```

Grâce à toutes ces méthodes, vous pouvez totalement personnaliser tous les éléments de la page, afin d'adapter celle-ci plus précisément, à votre image.

ANNEXES

11. Dictionnaire de Données

11.1 Affichage des pages de paiement

L'ensemble des variables à envoyer à la plateforme e-Transactions pour afficher les pages de paiement est résumé dans ce tableau.
Le détail de chaque variable (format, contenu, exemples) est communiqué dans les pages suivantes.

VARIABLE	RÉSUMÉ	OBLIGATOIRE
PBX_1EURO_CODEEXTERNE	Données spécifiques 1euro.com	C
PBX_1EURO_DATA	Données spécifiques 1euro.com	C
PBX_2MONTn	Paiement en plusieurs fois : montant des échéances n	F
PBX_ANNULE	URL de retour en cas d'abandon	F
PBX_ARCHIVAGE	Référence archivage	F
PBX_ATTENTE	URL de retour en cas de paiement en attente de validation	F
PBX_AUTOSEULE	Ne pas envoyer ce paiement à la banque immédiatement	F
PBX_BILLING	Informations sur votre client nécessaire à sa banque pour l'évaluation du besoin d'authentification en 3DSv2	O
PBX_CK_ONLY	Forçage d'un mode de paiement Carte Cadeau uniquement (non mixte)	F
PBX_CMD	Référence commande	O
PBX_DATEn	Paiement en plusieurs fois : dates des échéances n	F
PBX_DEVISE	Devise (monnaie) : **Euro Obligatoire**	O
PBX_DIFF	Nombre de jours avant la remise en banque pour un paiement différé	F
PBX_DISPLAY	Durée en secondes du timeout de la page de paiement	F
PBX_EFFECTUE	URL de retour en cas de succès	F
PBX_EMPREINTE	Empreinte fournie lors d'un premier paiement	F
PBX_ENTITE	Référence numérique d'une subdivision	F
PBX_ERRORCODETEST	Code erreur à renvoyer (pour tests)	F
PBX_HASH	Algorithme utilisé pour la signature du message	O
PBX_HMAC	Signature du message	O
PBX_IDABT	Numéro d'abonnement	F
PBX_IDENTIFIANT	Identifiant client de votre boutique fourni par e-Transactions	O
PBX_LANGUE	Langue de la page de paiement à utiliser	F
PBX_ONEY_DATA	Données spécifiques Oney	C
PBX_PAYPAL_DATA	Données spécifiques Paypal	C
PBX_PORTEUR	Adresse mail de votre client (internaute)	O
PBX_RANG	Numéro de rang fourni par e-Transactions	O

PBX_REFABONNE	Référence de l'abonné (pour l'enregistrement du moyen de paiement)	C
PBX_REFUSE	URL de retour en cas de refus du paiement	F
PBX_REPONDRE_A	URL UPN (Notification de Paiement)	F
PBX_RETOUR	Configuration de la réponse	O
PBX_RUF1	Méthode d'appel de l'URL IPN	F
PBX_SHOPPINGCART	Nombre de produits dans le panier pour l'évaluation du besoin d'authentification par la banque de votre client en 3DSv2	O
PBX_SITE	Numéro de site fourni par e-Transactions	O
PBX_SOURCE	Valeur obligatoire : RWD	F
PBX_TIME	Date et heure de la signature	O
PBX_TOTAL	Montant (en centimes)	O
PBX_TYPECARTE	Forçage du moyen de paiement	F
PBX_TYPEPAIEMENT	Forçage du moyen de paiement	F

Tableau 15 : Liste des variables pour les pages de paiement

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

11.1.1 Champs obligatoires pour e-Transactions

11.1.1.1 PBX_SITE

Format : 7 chiffres. **Obligatoire.**

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

Exemple : PBX_SITE=1999888

11.1.1.2 PBX_RANG

Format : 2 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 : PBX_RANG=01

11.1.1.3 PBX_IDENTIFIANT

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

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

Exemple : PBX_IDENTIFIANT=200814357

11.1.1.4 PBX_TOTAL

Format : 3 à 10 chiffres. **Obligatoire.**

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

Exemple : pour 19€90 : PBX_TOTAL=1990 – pour 12€ : PBX_TOTAL=1200

11.1.1.5 PBX_DEVISE

Format : 3 chiffres. **Obligatoire.**

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

Exemple :

- Euro : PBX_DEVISE=978

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

11.1.1.6 PBX_CMD

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

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

Dans le cas de la création d'un abonné (enregistrement d'une carte bancaire) lors de l'utilisation d'une page de paiement, la valeur contenue dans ce champ est utilisée comme référence d'abonné si celle-ci n'est pas précisée dans la variable PBX_REFABONNE.

Exemple : PBX_CMD=CMD9542124-01A5G

11.1.1.7 PBX_PORTEUR

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

Adresse email de votre client (porteur de carte).

Exemple : PBX_PORTEUR=test@gmail.com

11.1.1.8 PBX_RETOUR

Format : <nom de variable>:<lettre>;<nom de variable2>:<lettre2>;etc.; **Obligatoire.**

Variables demandées à être retournées à votre boutique par la plateforme e-Transactions après l'affichage des pages de paiement et lors de la Notification de Paiement (IPN).

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

Voir aussi : *3.8-Indiquer les informations et variables à recevoir en retour*

M	**M**ontant de la transaction (précisé dans PBX_TOTAL).
R	**R**éférence commande (précisée dans PBX_CMD) : espace URL encodé
T	Numéro d'appel
A	Numéro d'**A**utorisation (numéro remis par le centre d'autorisation) : URL encodé
B	Numéro d'abonnement (numéro remis par la plateforme)
C	Type de **C**arte retenu (cf. PBX_TYPECARTE pour les types de carte possibles)
D	**D**ate de fin de validité de la carte du porteur. Format : AAMM
E	Code réponse/**E**rreur de la transaction (cf. *12.1-Codes de retour des pages de paiement (variable E avec PBX_RETOUR))*
F	Etat de l'authenti**F**ication du client vis-à-vis de l'authentification 3D-Secure : • Y : Client authentifié • A : Authentification non réalisée par la banque de l'acheteur (ex : erreur technique). Le paiement peut être réalisé. • U : L'authentification du porteur n'a pas pu s'effectuer (risque d'impayé) • N : Porteur non authentifié (risque d'impayé)
G	**G**arantie du paiement 3D-Secure. Format : O ou N
H	Empreinte de la carte
I	Code pays de l'adresse **I**P de l'internaute. Format : ISO 3166 (alphabétique)
J	2 derniers chiffres du numéro de carte de votre client
j	*(j minuscule)* 4 derniers chiffres du numéro de carte de votre client
K	Signature de vérification du message. Format : url-encodé/base64 (voir chapitre signature des messages)
N	6 premiers chiffres (« BI**N**6 ») du numéro de carte de l'acheteur
O	Enr**ô**lement de la carte de votre client au programme 3D-Secure : • Y : Carte enrôlée • N : Carte non enrôlée • U : Information non connue
P	Type de **P**aiement retenu (cf. PBX_TYPEPAIEMENT pour les types de paiement possibles)
Q	Heure de traitement de la transaction. Format : HH:MM:SS (24h)
S	Numéro de Tran**s**action
U	Token (étiq**U**ette) de l'abonné créé pour l'enregistrement d'un moyen de paiement et Date de validité de la carte Handle_Numéro_De_Carte_Crypté**++**Date_De_Validité_De_La_Carte**++---** Ce champ est URL-encodé. Vous devez conserver la valeur du token pour un usage ultérieur du moyen de paiement **Attention pour les paiements avec Paypal :**

	Ce champ contient l'identifiant de l'autorisation fourni par Paypal. (pas nécessaire pour les paiements suivants).
v	*(v minuscule)* Version du protocole 3DS utilisé (3DS**v**1 ou 3DS**v**2)
W	Date de traitement de la transaction sur la plateforme. Format : JJMMAAAA
Y	Code pa**Y**s de la banque émettrice de la carte. Format : ISO 3166 (alphabétique)
Z	Index lors de l'utilisation des paiements mixtes (cartes cadeaux associées à un complément par carte CB/Visa/MasterCard/American Express)

Tableau 16 : Données disponibles par PBX_RETOUR

Remarque 1: Si les variables « **H** – *Empreinte de la carte* », « **N** – *6 premiers chiffres du numéro de carte* » et « **J** – *2 derniers chiffres du numéro de carte* » sont demandées simultanément, seule la variable « **H** » sera retournée pour des raisons de sécurité sur le numéro de carte.

Remarque 2: Pour les mêmes raisons, si les variables « **j** – *4 derniers chiffres du numéro de carte* » et « **N** – *6 premiers chiffres du numéro de carte* » sont demandées simultanément, seule la variable « **j** » sera retournée.

Remarque 3 : Les variables **« N »** et **« J »** peuvent être demandées simultanément. Pour être conforme à la réglementation elles ne doivent pas être affichées sur un ticket. Seule la variable **« j »** est conforme.

11.1.1.9 PBX_HASH

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

Définit l'algorithme de hachage utilisé lors du calcul du HMAC.
Exemple : PBX_HASH=SHA512

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 PBX_HMAC est présente dans les appels sans que PBX_HASH ne soit précisé, l'algorithme de hachage sélectionné sera SHA512.

11.1.1.10 PBX_HMAC

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

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

Exemple :
PBX_HMAC=AD4D2A87FB9C4FA7AD8AA122E9F417B568D5E2B8CA4AF9410B00B9CFCFDB9142F7
21CBD0B90F518A16A49F9A7BD248A86EFEA25831654395E1DED1BEA650361C

Voir aussi : *3.3-Calcul de la signature avec la clé HMAC*

11.1.1.11 PBX_TIME

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

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

Exemple : PBX_TIME=2021-01-28T01 :00 :00+01:00
(correspond au 28 janvier 2021, à 1h du matin heure locale)

11.1.1.12 PBX_BILLING

Format : flux XML. **Obligatoire.**

Information concernant 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.

Voici les données à indiquer dans le flux XML avec la balise principale : <Billing> :

Nom	Description	Type	Obligatoire
Billing	Balise XML à la racine	XML	O
Address	Balise XML	XML	O
FirstName	Prénom du client	ANP30 (incluant / - ')	O
LastName	Nom du client	ANP30 (incluant / - ')	O
Address1	Adresse de facturation - Ligne1	ANS50	O
Address2	Adresse de facturation - Ligne2	ANS50	F
ZipCode	Code postal de l'adresse de facturation	ANS16	O
City	Ville de l'adresse de facturation	ANS50	O
CountryCode	Code pays de l'adresse de facturation	N3 - Code ISO-3166-1 numérique	O

Tableau 32 : Structure du flux XML PBX_BILLING

Légende : O : Obligatoire – **F** : Facultatif

ANP : Alpha Numérique avec les espaces et caractères accentués
ANS : Alpha Numérique avec caractères spéciaux
N : Numérique uniquement

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 : <?xml version="1.0" encoding="utf-8" ?><Billing><Address><FirstName>Jean</Firstname>
<LastName>Dupont</LastName><Address1>12 rue Test</Address1><ZipCode>75001</ZipCode>
<City>Paris</City><CountryCode>250</CountryCode></Address></Billing>

11.1.1.13 PBX_SHOPPINGCART

Format : flux XML. **Obligatoire.**

Nombre de produits dans le panier 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.

Voici les données à indiquer dans le flux XML avec la balise principale : <shoppingcart> :

Nom	Description	Type	Obligatoire
shoppingcart	Balise XML à la racine	XML	**O**
total	Balise XML	XML	**O**
totalQuantity	Nombre de produits dans le panier	N2 - 1 à 99	**O**

Tableau 33 : Structure du flux XML PBX_SHOPPINGCART

Légende : O : Obligatoire – **F** : Facultatif

N : Numérique uniquement

Exemple : <?xml version="1.0" encoding="utf-8" ?><shoppingcart><total>
<totalQuantity>12</totalQuantity></total></shoppingcart>

Information : Cette donnée est restreinte à 2 caractères dans le protocole 3DSv2 et ne peut donc excéder la valeur 99. Si celle-ci doit être supérieure à 99, elle doit être limitée à 99.
Cette donnée sert à détecter les commandes comportant plus de produits que le nombre habituel de produits dans vos commandes. Dans le cas où la majorité de vos commandes contiennent un nombre important de produits, vous pouvez effectuer un comptage différent du nombre de produits (nombre de produits distincts, lots de produits).

11.1.2 Champs optionnels pour e-Transactions

Les champs suivants sont triés par ordre alphabétique.

11.1.2.1 PBX_ARCHIVAGE

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

Référence qui vous ai propre et qui est transmise au serveur du Crédit Agricole au moment de la télécollecte. Elle doit être unique et permet 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 journaux de rapprochement bancaire - JRB).**

Exemple : PBX_ARCHIVAGE=ID_TRANS_INTERNE_00014521

11.1.2.2 PBX_AUTOSEULE

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

Si la variable vaut « O », la transaction est uniquement en mode autorisation seule, c'est-à-dire qu'elle n'est pas envoyée à votre banque au moment de la télécollecte tant que vous ne l'avez pas confirmée (capturée).

Cependant, elle est bien enregistrée, et il est possible de la capturer ultérieurement en utilisant votre Back-office Vision ou en réalisant une demande de capture par appel d'API.

Exemple : PBX_AUTOSEULE=O

11.1.2.3 PBX_ANNULE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client visible et modifiable dans votre Back-office Vision

Page de retour de la plateforme vers votre boutique après une annulation du paiement effectuée volontairement par votre client sur la page de paiement.

Les variables de retour définies dans PBX_RETOUR vous seront envoyées sur cette URL.
L'URL indiquée dans PBX_ANNULE doit être URL-encodée lors de l'envoi aux pages de paiement.

Exemple : PBX_ANNULE=https://www.commerce.fr/annulation%20commande.html

Voir aussi : *4-Récupérer le retour de la page de paiement sur votre site*

11.1.2.4 PBX_ATTENTE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client visible et modifiable dans votre Back-office Vision

Page de retour de la plateforme vers votre boutique après paiement mis en attente de validation par l'émetteur (ex : avec Paypal).

Les variables de retour définies dans PBX_RETOUR vous seront envoyées sur cette URL.
L'URL indiquée dans PBX_ATTENTE doit être URL-encodée lors de l'envoi aux pages de paiement.

Exemple : PBX_ATTENTE=https://www.commerce.fr/attente%20annulation.html

Voir aussi : *4-Récupérer le retour de la page de paiement sur votre site*

11.1.2.5 PBX_DATEVAL

Format : MMAA
Valeur par défaut : Champ absent.

Date de validité de la carte à pré-remplir sur la page de paiement lors de l'utilisation d'une carte de paiement déjà enregistrée (utilisée conjointement avec PBX_REFABONNE et PBX_TOKEN). Cette variable est facultative.

Exemple : PBX_DATEVAL=1223

> Remarque : La variable PBX_DATEVAL est au format MMAA et la date de validité retournée par le paramètre U est au format AAMM.

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

11.1.2.6 PBX_DATEVALMAX

Format : Date au format AAMM

Date d'expiration minimum que la carte utilisée doit dépasser. La date correspond à la fin du mois indiqué.

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

Exemple : PBX_DATEVALMAX=2207
Echéancier 04/05/2022, 08/06/2022 et 30/07/2022
Si la carte expire avant fin juillet 2022, le paiement initial sera refusé avec le code erreur 00008.

11.1.2.7 PBX_DATE1, PBX_DATE2, PBX_DATE3

Format : Date au format JJ/MM/AAAA

Dates des prochaines échéances d'un paiement fractionné. Le paiement initial réalisé au moment de la commande constitue la 1ère échéance.

Pour un paiement en 2 fois, il faut indiquer la 2ème échéance dans PBX_DATE1. Pour un paiement en 4 fois, il faut envoyer les 2ème, 3ème et 4ème échéances dans PBX_DATE1, PBX_DATE2 et PBX_DATE3.

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

Exemple : PBX_DATE1=30/06/2022&PBX_DATE2=31/07/2022

Voir aussi : *9.3-Paiement en plusieurs fois (4 fois maximum)* et *11.1.2.24-PBX_2MONT1, PBX_2MONT2, PBX_2MONT3*

11.1.2.8 PBX_DIFF

Format : 2 chiffres
Valeur maximum : 75 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 la page de paiement, 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 : PBX_DIFF=04 pour indiquer un différé de 4 jours avant remise en banque.

Voir aussi : *3.7-Paiement différé automatique en nombre de jours*

11.1.2.9 PBX_DISPLAY

Format : 3 à 10 chiffres
Valeur par défaut : 900

Délai d'expiration (TimeOut) de la page de paiement (en secondes). Une fois cette période dépassée, la transaction est abandonnée si votre client n'a pas effectué son paiement.

Cette transaction n'est pas remontée dans votre Back-office Vision et identifiée comme un paiement abandonné par votre boutique.

11.1.2.10 PBX_EFFECTUE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client visible et modifiable dans votre Back-office Vision

Page de retour de la plateforme vers votre boutique après un paiement effectué avec succès (paiement accepté) par votre client sur la page de paiement.

Les variables de retour définies dans PBX_RETOUR vous sont envoyées sur cette URL.
L'URL indiquée dans PBX_EFFECTUE doit être URL-encodée lors de l'envoi aux pages de paiement.

Exemple : PBX_EFFECTUE=https://www.commerce.fr/confirmation%20commande.html

Voir aussi : *4-Récupérer le retour de la page de paiement sur votre site*

11.1.2.11 PBX_EMPREINTE

Format : 64 caractères

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

11.1.2.12 PBX_ENTITE

Format : 1 à 9 chiffres

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

Exemple : PBX_ENTITE=001

11.1.2.13 PBX_ 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 est renvoyé par les pages de paiement.

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

Exemple : PBX_ERRORCODETEST=00157

Voir aussi : *12.1-Codes de retour des pages de paiement (variable E avec PBX_RETOUR)*

11.1.2.14 PBX_IDABT

Format : 9 chiffres

Numéro d'abonnement renvoyé dans la donnée '**B**' de **PBX_RETOUR** lors d'un précédent paiement par abonnement (création de l'abonnement à cette occasion).

Si vous renseignez cette variable, cela permet de mettre à jour la carte de paiement actuellement associée à un abonnement dans la plateforme Up2pay e-Transactions si le nouveau paiement est réalisé avec succès. Les futures échéances de l'abonnement utiliseront donc désormais cette nouvelle carte de paiement. Ce paiement est réalisé comme tout autre paiement. Si vous réalisez ce paiement en autorisation seule (voir *3.6-Paiement en autorisation seule*) et que vous ne le capturez pas, la carte de l'abonnement est tout de même remplacée par cette nouvelle carte mais ce paiement n'est pas débité.

Exemple : PBX_IDABT=254687459

Voir aussi : *9-Gestion des abonnements*

11.1.2.15 PBX_LANGUE

Format : 3 caractères
Valeur par défaut : FRA

Langue à utiliser pour l'affichage de la page de paiement de la plateforme Up2pay e-Transactions
Les valeurs possibles pour la langue d'affichage sont les suivantes :

FRA	Français	**ITA**	Italien	**SWE**	Suédois
GBR	Anglais (UK)	**DEU**	Allemand	**PRT**	Portugais
ESP	Espagnol	**NLD**	Hollandais		

Exemple : PBX_LANGUE=FRA

11.1.2.16 PBX_REFABONNE

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

Référence de l'abonné (client et son moyen de paiement) auquel est affecté la carte de paiement à enregistrer.
Si utilisée conjointement avec l'envoi de PBX_TOKEN récupéré lors d'un précédent enregistrement de carte de paiement, elle permet de faire référence à cet abonné et d'afficher la page de paiement avec les données de cartes pré-saisies et masquées.

L'envoi de cette variable permet de mettre à jour la carte de paiement associée à un abonné ou profil s'il existe déjà, ou de le créer s'il n'existe pas.
Si vous ne précisez pas cette variable lors d'un paiement avec demande d'enregistrement de moyen de paiement, la référence de la commande envoyée dans PBX_CMD est utilisée comme référence de l'abonné.

Vous devez conserver cette référence d'abonné pour l'utiliser lors d'un paiement ultérieur car elle ne vous sera pas retournée.

Cette fonctionnalité n'est utilisable que si vous avez souscrit un contrat PREMIUM.

Exemple : PBX_REFABONNE=Client_005287_Mdp_0001 ou PBX_REFABONNE=HcsqXh5YHkCb

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

11.1.2.17 PBX_REFUSE

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client visible et modifiable dans votre Back-office Vision

Page de retour de la plateforme vers votre boutique après un paiement refusé sur la page de paiement (après 3 tentatives en échec ou après 1 tentative en échec et clic sur le bouton « Annuler »).

Les variables de retour définies dans PBX_RETOUR vous sont envoyées sur cette URL.
L'URL indiquée dans PBX_REFUSE doit être URL-encodée lors de l'envoi aux pages de paiement.

Exemple : PBX_REFUSE=https://www.commerce.fr/refus%20paiement.html

Voir aussi : *4-Récupérer le retour de la page de paiement sur votre site*

11.1.2.18 PBX_REPONDRE_A

Format : jusqu'à 150 caractères
Valeur par défaut : valeur enregistrée dans votre fiche client visible et modifiable dans votre Back-office Vision

URL d'appel serveur à serveur après chaque tentative de paiement. Aussi appelée « Notification de Paiement Instantanée » ou « IPN ». Cette URL est appelée en dehors du navigateur du client, et permet donc de valider les commandes de manière sûre.

Les variables de retour définies dans PBX_RETOUR vous seront envoyées sur cette URL.
L'URL indiquée dans PBX_REPONDRE_A doit être URL-encodée lors de l'envoi aux pages de paiement.

Exemple : PBX_REPONDRE_A=https://www.commerce.fr/back/retour%20paiement.php

Voir aussi : *5-Notifications de Paiement Instantanées (IPN)*

11.1.2.19 PBX_RUF1

Format : valeur possible « POST »
Valeur par défaut : GET

Méthode (au sens protocole http/HTTPS) utilisée pour l'appel de l'URL de Notification de Paiement Instantanée ou « IPN ».

Si le paramètre est renseigné, il ne peut valoir que « POST ». S'il n'est pas renseigné, l'appel est fait avec la méthode GET.

Exemple : PBX_RUF1=POST

Voir aussi : *5-Notifications de Paiement Instantanées (IPN)*

11.1.2.20 PBX_SOURCE

Format : 3 à 5 caractères – seule valeur possible « RWD »
Valeur par défaut : RWD

Définit le format de la page du choix du moyen de paiement.
Cette variable doit être renseignée avec la valeur « RWD », permettant l'affichage « responsive design » de la page de paiement donc automatiquement compatible sur plusieurs médias (ordinateur, tablette, mobile).