Up2pay e-Transactions

MANUEL D'INTEGRATION

Version du 01/03/2021

REFERENCES DOCUMENTATIONS

REF.	DOCUMENT	DESCRIPTION
Ref 1	Manuel Intégration Conecs et CV-Connect	Manuel d'intégration spécifique pour les moyens de paiement Conecs (titres restaurant) et CV_Connect (Chèques vacances)
Ref 2	Manuel Intégration Paypal	Manuel d'intégration spécifiques pour le moyen de paiement complémentaire Paypal
Ref 3	Manuel Intégration Paylib	Manuel d'intégration spécifique pour le moyen de paiement complémentaire Paylib
Ref 4	Manuel Intégration American Express	Manuel d'intégration spécifique pour le moyen de paiement complémentaire American Express (AMEX)
Ref 5	Réalisation des tests d'intégration e-Transactions	Manuel décrivant les environnements et paramètres pour réaliser les test (recette) de l'intégration de la solution Up2pay e-Transactions
Ref 6	Manuel Utilisateur Back-office Vision Air	Manuel Utilisateur du Back Office Commerçant de la solution Up2pay e-Transactions

.

TABLE DES MATIERES

Table des matières

PRINCIPES GENERAUX

1. Présentation d'Up2pay e-Transactions

Up2pay e-Transactions est un système sécurisé d'encaissement par cartes bancaires et/ou cartes privatives à destination des commerçants disposant d'un site e-commerce, des destinataires de donations (associations, …), des professionnels ayant besoin d'un système de paiement, des collectivités publiques.

1.1 Principe général de la Solution

Dans le domaine du e-commerce, le Crédit Agricole propose une solution de paiement sur internet appelée Up2pay **e-Transactions**, prévue pour être intégrée à votre site marchand de différentes façons en s'appuyant sur des interfaces techniques spécifiques :

- ✓ s'interface avec votre site marchand accessible depuis un navigateur web sur ordinateur, tablette et smartphone.
  Une fois votre solution de paiement intégrée à votre site marchand, vos clients peuvent effectuer des paiements en toute sécurité : ils sont redirigés vers la plateforme Up2pay **e-**Transactions suite à la réalisation d'une commande.
  Une connexion cryptée est établie avec le navigateur de vos clients, une page de paiement sécurisée et multilingue est affichée, et les invite à saisir leurs informations Carte.
  Cette page de paiement est personnalisable afin de pouvoir l'harmoniser à votre identité graphique.
  Notre solution de paiement répond aux normes de sécurité des paiements par carte en affichant une page HTTPS (sécurisée en TLS 1.2) et hébergée sur une plate-forme certifiée PCI-DSS.

- ✓ La **G**estion **A**utomatisée des **E**ncaissements (GAE dans le document), est une des fonctionnalités de l'offre, qui permet de communiquer avec la solution par API.
  Elle permet de valider directement depuis votre boutique, les transactions préalablement autorisées, d'effectuer des remboursements et des annulations.

  Elle peut également offrir un parcours de paiement confortable et simplifié pour vos clients directement sur votre site en se substituant à la page de paiement **e-**Transactions.
  Votre site collecte, via un formulaire de saisie, les informations bancaires de votre client pour les envoyer à la solution **e-**Transactions.

  Dans ce cas, votre site marchand joue le rôle de collecteur des informations sensibles telle que le numéro de carte et vous devez les transmettre à notre plateforme via un dialogue sécurisé de serveur à serveur. Vous devez être certifié PCI-DSS par les autorités compétentes.

  Le principe de ce fonctionnement est donc de :
  - Générer un formulaire de saisie des informations bancaires
  - Créer une session de communication sécurisée grâce à une trame HTTPS « question »,
  - Appeler une URL présente sur nos serveurs et envoyer les éléments du formulaire,

- Récupérer dans la même session HTTPS, la trame « réponse » retournée par la plateforme après traitement de la transaction, contenant entre autres, l'information sur l'acceptation ou le refus de la transaction.
- Fermer la session HTTPS

✓ Votre site marchand peut demander à notre plateforme de conserver les données du moyen de paiement carte ou Paypal utilisé lors d'un achat. Cette solution s'interface en complément du paiement en utilisant les pages de paiement de la solution Up2pay e-Transactions ou en utilisant les API.
Ce service vous permet entre autres de gérer des abonnements ainsi que des paiements en un clic (one-click) où l'Acheteur ne ressaisie pas les données de son moyen de paiement à chaque nouvelle transaction.

Une fois les informations bancaires saisies et reçues par notre serveur, **Up2pay e-Transactions** effectue une demande d'autorisation auprès de l'émetteur associé au moyen de paiement choisi, dans le respect des normes de paiement en vigueur pour chaque paiement.
A la suite du paiement, s'il est réalisé sur les pages de paiement hébergées par la solution, un ticket de paiement est envoyé à votre client. Vous pouvez également recevoir un ticket de paiement dans votre messagerie en cochant cette option dans votre Back-Office Vision (ce n'est pas le cas par défaut).

En parallèle, les informations relatives au paiement sont envoyées à votre site pour mise à jour automatique de l'état de la commande par IPN (*Instant Payment Notification*) et votre client est en parallèle redirigé sur une page de votre site (confirmation de commande ou refus de paiement ou choix d'un nouveau moyen de paiement en fonction de la situation).

Dans la nuit, **Up2pay e-Transactions** réunit sous forme d'un « fichier remise » tous les paiements cartes bancaires réalisés sur votre site et les envoie au centre de télécollecte du Crédit Agricole pour traitement des transactions.
Si vous avez effectué un ou plusieurs remboursements, ces transactions de remboursement seront également réunies dans le fichier de remise.
Vous recevez quotidiennement un e-mail (*Objet : « Compte rendu de teleparametrage »*) vous permettant de vous assurer de la mise à jour et du bon fonctionnement de votre contrat monétique (le téléparamétrage est une action quotidienne de synchronisation entre plusieurs serveurs de la solution).
Si vous avez réalisé des transactions et/ou des remboursements dans la journée : un ticket de compte-rendu de télécollecte vous est envoyé par e-mail (*objet : « Compte rendu de telecollecte »)* ainsi que 3 extractions de cette télécollecte sous plusieurs formats (TXT, CSV et XML – *Objet : « extraction [CSV/XML] telecollecte du DATE IDENTIFIANT-SITE-RANG »*).
Pour les autres moyens de paiements, Up2pay e-Transactions respecte les modalités des différents fournisseurs.

1.2 Principe général du document

Ce document vous présente le fonctionnement de **Up2pay e-Transactions** et décrit de manière exhaustive les fonctionnalités de l'offre, vous permettant d'interfacer notre solution de paiement sur votre site marchand, indépendamment du langage informatique utilisé pour le développer.

Il est organisé en 3 parties :

- La première vous permet de découvrir et appréhender la solution avec une vue d'ensemble.

- La seconde, « Intégration technique », dédiée notamment aux intégrateurs, contient les informations détaillées nécessaires à la mise en place.
- La troisième est composée d'annexes contenant des données complémentaires et des exemples illustrant la mise en place.

1.2.1 Vous avez souscrit à l'Offre Access

L'offre **Access** inclue les fonctionnalités essentielles pour tout commerçant souhaitant proposer une page de paiement sécurisée simple et rapide à mettre en place, proposant les fonctionnalités suivantes :

- Page de paiement RWD (*Responsive Web Design*) pour l'acceptation des paiements à distance sécurisée (CB, VISA, MASTERCARD)
- Protocole sécurisé de paiement 3D-Secure sur toutes les transactions éligibles*
- Intégration des pages de paiement en redirection ou intégrées à la boutique
- Accès au back-office Vision pour la gestion des transactions :
    - Suivi
    - Capture manuelle
    - Annulation
    - Remboursement total ou partiel

Il est possible de bénéficier de ces fonctionnalités :

- Moyens de paiement complémentaires :
    - Paylib
    - PayPal
- Débit différé (jusqu'à 7 jours)

Les chapitres faisant référence à cette offre sont les suivants :

- Chapitres 1 à 6
- Chapitre 10
- Annexes

1.2.2 Vous avez souscrit à l'Offre Premium

L'offre **Premium** permet de souscrire à l'ensemble des fonctionnalités et moyens de paiement disponibles dans Up2pay e-Transactions.

Elle s'adresse aux commerçants souhaitant proposer à leurs clients une expérience de paiement plus complète et personnalisée, avec des facilités de paiement, comme le paiement en plusieurs fois, le one-click, le débit à l'expédition, et bien d'autres fonctionnalités et cas d'usages décrits dans les chapitres de ce document. Elle permet également d'effectuer les opérations de caisse (capture, annulation, remboursement) directement à partir du back-office du site marchand

1.3 Prérequis

Up2pay e-Transactions vient s'imbriquer à votre site e-commerce pour permettre le déroulement de la vente en ligne jusqu'à la confirmation de la commande.

Dans le cas où votre boutique est développée à partir d'un CMS (Système de Gestion de Contenu) ou d'une solution SaaS (*Software As A Service*, ou *Logiciel En tant que Service*) assurez-vous d'avoir la possibilité d'y intégrer la solution e-Transactions.
En effet, certaines solutions propriétaires proposent un catalogue d'applications internes et n'autorisent pas de développement externe.

Nos modules e-Transactions compatibles avec les CMS suivants sont disponibles sur notre site Ca-moncommerce :
- Prestashop v1.5 *et supérieur*
- Wordpress WooCommerce 3.x *et supérieur*
- Magento 2.3.6 *et supérieur*

Les options et moyens de paiement étant optionnels, assurez-vous d'avoir souscrit à l'ensemble des fonctionnalités souhaitées afin de pouvoir les utiliser.

Dans le cas où vous utilisez la **G**estion **A**utomatisée des **E**ncaissements (intégration par API) pour collecter les informations de paiement, votre site doit faire l'objet d'une déclaration PCI-DSS.
Ce mode d'intégration étant plus complexe, sa mise en place sur votre site nécessite une capacité de développement avancée.

1.4 Compatibilité règlementaire

La solution Up2pay e-Transactions répond à l'ensemble des réglementations applicables aux solutions de paiement en ligne:

- Solution certifiée PCI-DSS
  - Pages de paiemen et échanges API en HTTPS (sur TLS 1.2)
- La directive des marchés financiers MIF
  - Le choix de la marque du moyen de paiement pour votre client
- La norme monétique
  - CB5.5
- Le protocole sécurisé de paiement 3D-Secure
  - 3DSv2

1.5 Liste des moyens de paiement

Ci-dessous une liste complète des moyens de paiement acceptés par **e-Transactions** :

MOYEN DE PAIEMENT	TYPE	PAIEMENT PAR API	COMMENTAIRE
CB, VISA, MASTERCARD	Cartes bancaire	**OUI**	
E-CARTE BLEUE	Carte virtuelle dynamique	**OUI**	Opérée par VISA France
AMERICAN EXPRESS	Carte bancaire	**OUI**	Nécessite de contractualiser avec American Express
PAYLIB	Portefeuille électronique	NON	

1EURO.COM	Financement en ligne	NON	Nécessite de contractualiser avec Cofidis
CONECS (cartes Apétiz, Up Chèque Déjeuner, Sodexo Pass Restaurant)	Moyen de paiement en titres restaurant	NON	Nécessite de contractualiser avec Conecs
CV-CONNECT	Moyen de paiement en Chèques-vacances	NON	Nécessite de contractualiser avec ANCV
DINERS	Carte bancaire	**OUI**	Nécessite de contractualiser avec Diners Club
FACILIPAY - 3X 4X ONEY	Financement en ligne	NON	Nécessite de contractualiser avec Oney
iDEAL	Moyen de paiement par virement	NON	Pays-Bas - Nécessite de contractualiser avec iDeal
ILLICADO	Carte cadeau prépayée	NON	Nécessite de contractualiser avec Illicado
JCB	Carte bancaire	**OUI**	Nécessite de contractualiser avec JCB
LEETCHI	Cagnotte en ligne	NON	Nécessite de contractualiser avec Leetchi
ONEY (ONEY KDO)	Carte cadeau prépayée	NON	Nécessite de contractualiser avec Oney
PAYPAL	Portefeuille électronique	NON	Nécessite de contractualiser avec Paypal
PAYSAFECARD	Carte prépayée	NON	Nécessite de contractualiser avec Paysafecard

Tableau 1 : Moyens de paiement

1.6 Présentation des pages

Tout au long du processus de paiement, plusieurs pages s'affichent successivement. Ce chapitre décrit ces différentes pages qui s'afficheront selon votre mode d'intégration.

1.6.1 Page de présélection du moyen de paiement

Sur cette première page, l'ensemble des moyens de paiement que vous avez souscrits sont proposés proposer à vos clients. Chaque client, au moment du paiement, est alors invité à sélectionner le moyen de paiement qu'il souhaite utiliser, et en fonction de son choix, l'affichage de la page de paiement sera adapté.

Un bouton unique « Carte bancaire » regroupent les logos CB, Visa et MasterCard.

Exemple de page de choix du moyen de paiement (avec paiement par carte bancaire CB/VISA/Mastercard et paiement par Paylib disponibles):

Figure 1 : Page de choix des Moyens de paiement

Cette page de présélection du moyen de paiement est personnalisable (voir chapitre *10 – Personnalisation de la page de paiement*).

La page de présélection du moyen de paiement modifie la page de paiement qui vient ensuite en fonction du choix effectué par votre client.
Par exemple, le cryptogramme visuel n'est pas demandé pour la carte Diners, mais il est demandé pour les cartes CB, American Express, Visa ou Mastercard.

- Cette page ne sera pas affichée, si vous avez précisé dans le formulaire de paiement, le moyen de paiement que vous souhaitez proposer (forçage du moen de paiement affiché).

➢ **Le Crédit Agricole vous préconise de valoriser sur votre site e-commerce, la liste des moyens de paiement acceptés sous la forme d'icônes cliquables. Vos clients seront alors directement envoyés sur la page de paiement adaptée au moyen de paiement sélectionné sur votre site.**

- Pour plus d'informations sur le forçage des types de carte et moyens de paiement, voir chapitre *3.1.2 Avec choix direct du moyen de paiement (forçage)).*

1.6.1.1 Détection de la marque de la carte

Lors de la saisie du numéro de carte par votre client, la page de paiement est modifiée en temps réel pour afficher le logo ou les logos de la marque de la carte inscrite.

Figure 2 : Page de paiement vierge

Figure 3 : Page de paiement - choix CB

Figure 4 : Page de paiement - Choix Visa

Figure 5 : Page de paiement - Choix MasterCard

1.6.1.2 Choix de la marque

La carte utilisée par votre client peut supporter plusieurs marques, par exemple :

- CB et Visa
- CB et MasterCard

Votre client peut cliquer sur le logo sous-titré « Cliquez pour changer » afin de sélectionner la marque de son choix. Il effectue son choix via l'interface suivante :

Figure 6 : Choix de la marque

Sans modification de votre part, le choix par défaut sera « CB ».
Vous pouvez changer cette préférence en faisant une demande auprès de votre conseiller professionnel.

1.6.1.3 Cryptogramme Visuel

Le champ « Cryptogramme visuel » (ou CVV) peut être décoché afin de permettre le paiement avec des cartes qui ne possèdent pas cette information.
Lorsque ce champ est décoché, un pop-up d'avertissement est affiché à votre client :

Figure 7 : CVV - Pop-up d'avertissement

1.6.2 Ticket de paiement

La solution Up2pay e-Transactions affiche le ticket de paiement à la fin d'un paiement (réussi ou en échec).

Il est possible de désactiver cet affichage et de retourner directement vers votre boutique avec le résultat du paiement en le configurant dans votre back-office Vision (document ***Ref6-Manuel Utilisateur Back-office Vision Air – Chapitre 9 « PARAMETRAGE »***).

Le contenu du ticket inclut les éléments suivants :

- La marque choisie (CB, Visa, MasterCard, etc.)
- La mention « VADS » caractérisant un **paiement à distance sécurisé**.
- La mention « DEBIT » ou « AUTORISATION » indiquant le type de transaction.
- L'URL de votre boutique
- Les 4 derniers chiffres du numéro de la carte utilisée pour le paiement
- Le numéro de commande envoyé à la page de paiement
- Le montant de la transaction
- Le numéro d'autorisation obtenu si le paiement est réussi

Figure 8 : Ticket de paiement accepté

Figure 9 : Ticket de Paiement refusé

Un ticket de paiement est envoyé par mail à votre client (identique au ticket édité sur un terminal de paiement électronique).
Vous pouvez également activer l'envoi par e-mail d'un ticket de paiement à votre destination dans votre back-office Vision.(document Ref3 [Manuel Utilisateur Back-office Vision Air] – Chapitre 9 « PARAMETRAGE »).
Pour répondre à des obligations réglementaires, votre client recevra toujours son ticket de paiement.

1.6.3 Personnalisation des pages de paiement

Pour rassurer vos clients, il est possible de personnaliser des éléments pour que la page de paiement s'intègre au mieux dans la charte graphique de votre site.

Les éléments personnalisables sont notamment :

- Votre logo en haut de page
- L'affichage du logo Crédit Agricole
- Les boutons de validation/annulation/ « retour boutique »
- La langue par défaut et les boutons de langues à afficher
- Le fond d'écran

D'autres éléments de la page de paiement peuvent être personnalisées en construisant vous-même une feuille de style (fichier CSS) à appliquer lorsque la page s'affiche pour votre contrat commerçant.

Référez-vous au chapitre : *10-Personnalisation de la page de paiement* pour des informations détaillées sur la personnalisation.

1.7 Fonctionnalités disponibles et réalisables

Au-delà de la fonction élémentaire de paiement, la solution Up2pay **e-Transactions** propose un des fonctionnalités additionnelles vous permettant de piloter plus souplement vos opérations et d'offrir à vos clients, des services à valeur ajoutée.

En fonction de l'intégration que vous souhaitez ou pouvez réaliser, vous pouvez tout ou partie des fonctionnalités disponibles selon le descriptif ci-dessous.

1.7.1 Intégration par pages en redirection e-Transactions uniquement

Les fonctionnalités possibles uniquement dans le cas d'une intégration des pages de paiement e-Transactions sont :

- Appel des pages en redirection
- Appel des pages en iFrame
- Choix du moyen de paiement ou forçage
- Paiement différé (nombre de jours – max 6 jours pour la garantie 3D-Secure)
- Certaines typologies d'abonnements
- Paiement en plusieurs fois (jusqu'à 4 fois)

1.7.2 Intégration par API uniquement

Toutes les fonctionnalités sont possibles en utilisant uniquement les API.
L'intégration via API apporte un élément supplémentaire : l'hébergement du formulaire de paiement directement sur votre boutique.

1.7.3 Intégration des pages de paiement en redirection et des API

En utilisant conjointement l'intégration des pages de paiement (paiement par redirection) et la Gestion Automatisée des Encaissements (GAE), il est possible d'accéder à des fonctions supplémentaires, comme entre autres :

- Paiement en 1 clic,
- Capture de la transaction en différé (par exemple sur évènement)
- Autorisation seule (auto)
- Autorisation + débit (auto+capture)
- Débit (sur une autorisation pré effectuée) (capture)
- Remboursement
- Annulation (d'une opération pré effectuée)

1.7.4 Utilisation de la gestion des abonnés

Lors du paiement par les pages de paiement ou en utilisant directement l'API, l'empreinte de la carte peut être sauvegardée (création d'un abonné).
A partir d'une étiquette (token) lié à cet abonné et retourné par la solution e-Transactions, votre boutique pour initier ultérieurement d'autres paiements en utilisant cet abonné et son étiquette (avec les pages de paiement ou en utilisant l'API). Dans ce cas, votre client n'a pas besoin de ressaisir ces données de carte.

Voir le chapitre *8-Tokenisation – Gestion des abonnées* pour plus de détail.

1.7.5 Cas particulier de l'abonnement

Il est possible d'utiliser la fonctionnalité simple de gestion des abonnements totalement intégrée à la solution Up2pay e-Transactions en utilisant les pages de paiement hébergées sur la plateforme Up2pay e-Transactions.

Pour une intégration plus avancée d'une gestion d'abonnement, vous pouvez intégrer vous-mêmes le déclenchement des échéances en utilisant les APIs (et la gestion des abonnés évoquée ci-dessus) avec vos propres règles de gestion.

Voir les chapitres *8.5-Paiement récurrents* et *9-Gestion des abonnements* pour plus de détail.

2. Principes d'intégration

Pour intégrer la solution e-Transactions, vous avez plusieurs possibilités que vous pouvez combiner.

Même si vous avez la possibilité d'intégrer vous-même un formulaire de paiement sur votre boutique et d'envoyer les informations aux serveurs d'e-Transactions pour réaliser l'encaissement, nous vous conseillons d'effectuer l'intégration complète sous la forme suivante :

- Faire appel aux pages de paiement de la solution pour enregistrer les informations de paiement et réaliser une autorisation seule ou un encaissement complet.
Ces pages peuvent être intégrées en redirigeant votre consommateur vers la page de paiement hébergée sur la plateforme de la solution ou directement en intégrant cette page de paiement hébergée sur la plateforme de la solution dans un emplacement sécurisé (iFrame) sur les pages de votre boutique. En retour, en fonction du résultat du paiement, votre consommateur est redirigé vers une page de votre choix vous permettant de lui afficher le résultat et votre serveur reçoit également une notification contenant ce résultat en provenance des serveurs de la solution (IPN – Instant Payment Notification).

Puis, vous pouvez soit :

- Confirmer le débit si vous avez choisi de ne réaliser qu'une autorisation seule.
Ce débit peut être déclenché sur votre Back-office Vision Air ou directement à partir de votre boutique par un appel – de serveur à serveur – aux API de la solution (aussi appelé Gestion Automatisée des Encaissements) dans un délai maximum de 75 jours.
Important : Tant que vous n'aurez pas confirmé le débit d'une autorisation obtenue, vous ne serez pas crédité sur votre compte bancaire et votre client ne sera pas débité. Vous pouvez ne confirmer qu'une partie de l'autorisation obtenue.
- Annuler votre transaction confirmée si votre débit n'a pas encore été transmis en banque (pour une autorisation seule en succès ou en échec, vous n'avez pas besoin d'effectuer une annulation).

Puis,

- Demander d'effectuer le remboursement du montant total d'une transaction ou seulement une partie de celui-ci. Le paiement doit être réalisé et confirmé.
Ce remboursement peut être effectué sur votre Back-office Vision Air ou directement à partir de votre boutique par un appel – de serveur à serveur – aux API de la solution (aussi appelé Gestion Automatisée des Encaissements) dans un délai maximum de 75 jours à partir de la transaction réalisée.

Dans cette documentation, vous trouverez les méthodes d'intégration des pages de paiement selon vos besoins, les méthodes de réalisation des échanges API avec la solution (aussi appelé Gestion Automatisée des Encaissements) et toutes les opérations de caisse possible en utilisant les API.

Une attention particulière est portée sur la sécurité des échanges et le calcul de signature des messages à envoyer vers les serveurs de la solution (pour les pages de paiement et pour les appels API) ainsi que le contrôle de la signature des messages reçus par la solution.

2.1 Identification

Un site Marchand est référencé auprès des serveurs de la solution e-Transactions par plusieurs éléments :

- Le numéro de site
- Le numéro de rang
- L'identifiant e-Transactions du site

Ces éléments d'identification vous sont envoyés dans votre mail de bienvenue de la solution e-Transactions lors de la confirmation de votre inscription à l'utilisation de nos services.

Ces informations sont obligatoires dans tous les échanges que vous réalisez avec la plateforme de paiement.

Il est également nécessaire de les fournir lors de tout contact avec les équipes de l'assistance **e-Transactions.**

2.2 Appels des pages de paiement

Pour afficher la page de paiement à vos clients qui souhaitent payer sur votre boutique, il suffit de faire appel à l'URL de la page de paiement **e-Transactions** par le biais d'une requête HTTPS véhiculée par le navigateur de votre client contenant des variables.

L'ensemble des variables est transmis par des couples « variable = valeur » soumis à la manière d'un formulaire HTML dont les variables sont émises via une méthode POST.
L'intégrité des données transmises aux pages de paiement est protégée par l'ajout d'un paramètre de sécurité calculé selon l'algorithme HMAC initialisé avec une clé privée partagée (clé HMAC).

Grâce à l'intégration des pages de paiement fournies par la solution e-Transactions, la collecte des informations de paiement (numéro de carte, date de validité, CVV) est réalisée de façon sécurisée et ne nécessite aucune mesure de sécurité supplémentaire sur votre boutique..

Les grandes étapes de l'intégration des pages de paiement de la solution sont :

1- Votre client a validé son panier ;
2- Votre page de choix du moyen de paiement lui est proposé, il choisit celui qu'il souhaite ;
3- Vous le redirigez vers la page de paiement choisie ou vous affichez une iFrame dont l'url est celle de la page de paiement choisie ;
4- Votre client renseigne les informations pour le paiement (numéro de carte, …)
5- Il est redirigé vers le site de sa banque pour réaliser son authentification 3D-Secure
6- Si l'authentification est réalisée avec succès, la solution e-Transactions effectue une demande d'autorisation à la banque de votre client ;
7- Votre client est redirigé vers votre boutique avec le résultat du paiement ;
    a. En cas de succès de l'authentification et du paiement, le consommateur est redirigé vers votre page de confirmation de commande.
    b. En cas d'erreur lors de l'authentification ou du paiement, le consommateur est redirigé vers votre page d'erreur de paiement, vous permettant de lui afficher l'erreur et éventuellement de lui proposer de recommencer son paiement ou de choisir un autre moyen de paiement.
8- En parallèle, votre serveur reçoit une notification de paiement (IPN) permettant de sécuriser la réception de l'information du résultat du paiement.

Vous trouverez la liste des URLs des pages de paiement que vous pouvez appeler au chapitre dédié : *2.7.2-URLs à appeler*.

2.2.1 Variable PBX_RETOUR

Lorsque vous utilisez les pages de paiement, outre les paramètres que vous envoyez à la plateforme de paiement pour le bon fonctionnement de ces pages et du paiement (montant, identifiants, mode de paiement, ...), il est possible de recevoir en retour des informations qui vous permettent de traiter le retour et d'alimenter votre système d'information avec des données liées au paiement réalisé.

Pour cela, il existe un paramètre PBX_RETOUR dans lequel vous indiquez les données disponibles sur la plateforme de paiement que vous souhaitez recevoir en retour ainsi que le nom des variables dans lesquelles vous recevrez ces données.

Ces données vont de celles envoyées aux pages de paiement (montant, référence de commande) à celles correspondant au résultat du paiement (code retour, code d'erreur, authentification 3D-Secure) en passant par celles qualifiants les données du paiement (derniers numéro de la carte, code pays de l'adresse IP, …).

Vous trouverez plus de détails sur la structure du paramètre PBX_RETOUR dans le chapitre dédié (*3.8-Indiquer les informations et variables à recevoir en retour*) ainsi que la liste de toutes les données disponibles à l'annexe :*11.1.1.8-PBX_RETOUR*.

2.2.2 Variables en réponse (fonction PBX_RETOUR)

Comme précisé au chapitre précédent, vous pouvez indiquer aux pages de paiement, les données que vous voulez recevoir en retour par le paramètre PBX_RETOUR envoyé aux pages de paiement.

Lorsque votre client est redirigé vers vos URLs de paiement en succès, en erreur ou en attente (en fonction du résultat du paiement), les données demandées vous sont renvoyées dans chacune des variables indiquées pour chaque donnée.
Ces variables vous sont renvoyées par la soumission d'un formulaire véhiculé par le navigateur de votre client. Par défaut, les variables sont renvoyées par la soumission du formulaire en méthode GET mais vous pouvez demander de les recevoir par la méthode POST (*11.1.2.19-PBX_RUF1*).

Lorsque vous recevez les notifications de paiement de serveur à serveur, vous recevez également ces variables contenant ces données souhaitées. Par défaut, les variables vous sont envoyées sur votre URL de réception des notifications de paiement (IPN).

Une variable importante, que vous pouvez recevoir en retour, est le résultat (code réponse) du paiement. Vous recevez ce code réponse en demandant la donnée « E » (*11.1.1.8-PBX_RETOUR*) dans PBX_RETOUR lors de l'appel aux pages de paiement.
En cas de succès du paiement, vous recevez la valeur « 00000 ». Tous les autres codes réponse que vous pouvez recevoir correspondent à une erreur lors du paiement. Vous trouvez la liste des codes d'erreur à l'annexe :*12.1-Codes de retour des pages de paiement (variable E avec PBX_RETOUR).*
Si vous recevez un code d'erreur au format « 001xx », il s'agit d'un code d'erreur du centre d'autorisation dont dépend le moyen de paiement (carte de paiement) saisi. Vous trouverez la liste des codes d'erreur de chaque centre d'autorisation à l'annexe :*12.3-Codes réponse du centre d'autorisation*.

Le code « 00100 » qui correspond à un succès du centre d'autorisation est modifié en « 00000 » pour signifier le succès du paiement, vous ne recevrez donc pas « 00100 » mais « 00000 ».

2.3 Appels en API (GAE)

La **G**estion **A**utomatisée des **E**ncaissements (GAE) permet d'envoyer une requête à la plateforme e-Transactions via une trame HTTPS **« question »**, et d'obtenir en retour de la même session HTTPS une trame **« réponse »** précisant le succès ou l'échec de la requête.

Le principe d'appel aux API est de :

- Créer une trame HTTPS **« question »** sécurisée ;
- Appeler une URL d'API présente sur les serveurs de la solution ;
- Récupérer, dans les données envoyées en retour de l'appel, la trame **« réponse »** retournée par la plateforme après traitement de la requête.

Vous trouverez les URL des API à appeler au chapitre dédié : *2.7.2-URLs à appeler*.

2.3.1 Trames « Question »

Les trames **« question »** sont formées par un assemblage de couples « variable = valeur » ((TYPE=00001, MONTANT=1000, SITE=1999887, …) à la manière d'un formulaire HTML dont les variables sont émises via une méthode POST. La méthode GET n'est pas autorisée par les API de la solution.

L'intégrité des données transmises aux API est protégée par l'ajout d'un paramètre de sécurité calculé selon l'algorithme HMAC initialisé avec une clé privée partagée (clé HMAC).

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

Une variable « NUMQUESTION » 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.
Chaque appel doit avoir un numéro de question unique sur une journée. Il pourra être réinitialisé chaque jour.

2.3.2 Trames « Réponse »

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

Les variables SITE, RANG et NUMQUESTION sont toujours retournées à l'identique de l'appel. Nous vous conseillons de vérifier la cohérence de ces valeurs.

La Gestion Automatisée des Encaissements renvoie aussi un code réponse (variable CODEREPONSE), indiquant le bon déroulement ou non de la requête. Par exemple, le code réponse 00000 signifie que la demande a bien été traitée. L'ensemble de ces codes doivent être gérés par votre site marchand.
Tout autre code de retour correspond à un échec du traitement de la requête. Vous retrouvez la liste des codes d'erreur de retour des API à l'annexe : *12.2-Codes réponse des APIs*.
Si vous recevez un code d'erreur au format « 001xx », il s'agit d'un code d'erreur du centre d'autorisation dont dépend le moyen de paiement concerné par la requête. Vous trouvez la liste des codes d'erreur de chaque centre d'autorisation à l'annexe : *12.3-Codes réponse du centre d'autorisation*.

Le code « 00100 » qui correspond à un succès du centre d'autorisation est modifié en « 00000 » pour signifier le succès de la requête, vous ne recevrez donc pas « 00100 » mais « 00000 ».
Si vous recevez un code d'erreur « 00201 », 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.

En cas d'erreur, la Gestion Automatisée des Encaissements fournit aussi un message d'erreur détaillé dans le champ COMMENTAIRE qui permettra, si besoin, une aide au diagnostic avec l'assistance e-Transactions.

2.4 Authentification – Signature HMAC – Clés publique/privée

Afin de garantir une sécurité maximale lors des paiements ou des opérations par API effectués à partir de votre boutique sur votre contrat de paiement, vous devez vous authentifier par une clé secrète HMAC
Vous devez être le seul à connaitre cette clé en dehors de la solution Up2pay e-Transactions.

HMAC (pour Hash-based Message Authentication Code) est un protocole standard (RFC 2104) permettant de vérifier l'intégrité d'une chaîne de données. Couplé avec une clé secrète, ce protocole est utilisé sur la solution e-Transactions pour vérifier l'authenticité et l'intégrité des messages techniques échangés.

Cette clé est indispensable. Elle permet d'authentifier tous les messages techniques qui sont échangés entre votre boutique et les serveurs de la solution e-Transactions. Cela permet à la solution de garantir que tous les échanges (demandes de paiement, opérations de caisse, …) proviennent d'une source fiable authentifiée ainsi que l'intégrité des données transmises.

Vous devez donc générer votre propre clé unique et confidentielle, et l'utiliser pour calculer une signature sur chacun de vos échanges ou pour vérifier la signature des messages reçus.

Parallèlement, pour que vous puissiez authentifier les appels venant des serveurs de la solution Up2pay e-Transactions et vérifier l'intégrité des données, un mécanisme de Clé privée / clé publique permet de vérifier la signature des messages.
La solution Up2pay e-Transactions utilise sa clé privée (qu'elle est seule à connaitre) pour signer l'ensemble des données envoyées. Vous pouvez vérifier la signature grâce à la clé publique en libre téléchargement depuis https://www.ca-moncommerce.com/module-etransaction/php/ dans le fichier zip module PHP / Répertoire Exemple.php fichier pubkey.pem .
Pour être en conformité avec les règles de sécurité, le Crédit Agricole est susceptible de changer sa paire de clé publique/privée : il doit donc être possible de mettre en place différentes clés publiques au niveau de vos serveurs.

Voir le chapitre *6-Authentification des messages reçus* sur l'utilisation de ces clés publique/privée pour vérifier les appels reçus en provenance de la solution Up2pay e-Transactions.

2.4.1 Création de la clé HMAC dans votre Back-office Vision

Cette clé valide votre identité et sécurise les échanges avec la solution e-Transactions. Elle ne doit en aucun cas être diffusée.

2.4.1.1 Génération

Pour générer une clé HMAC, vous devez vous rendre dans le Back Office VISION Air.

La clé HMAC est différente suivant l'environnement configuré dans votre boutique.

Pour cela, vous devez ouvrir votre application de portail « VISION Air » et vous connecter en positionnant le menu déroulant « Serveur » sur :

- « **Recette** » : si vous configurez votre boutique en mode « **test** »
- « **Production** » ou « **Production1** » : si vous configurez votre boutique en mode « **production** ».

L'interface de génération de la clé secrète HMAC est accessible en haut à droit de la fenêtre de gestion de vos paramètres du Back Office Vision (onglet « Paramétrage / Paramètres »).

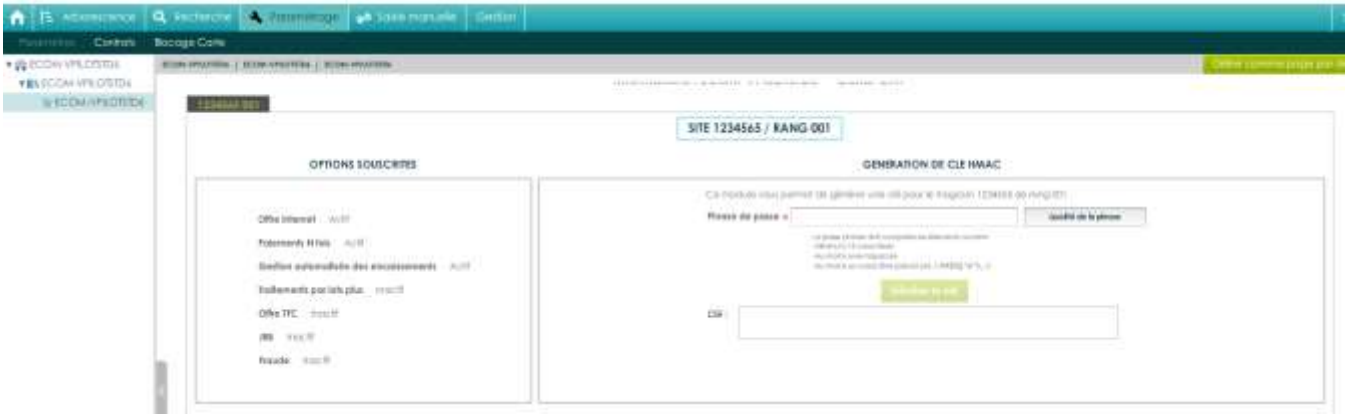


Figure 10 : Génération clé HMAC dans BO Vision

Le champ « Phrase de passe » peut être renseigné avec une phrase, un mot de passe ou tout autre texte.
Le champ « Qualité de la phrase» est mis à jour automatiquement lorsque la « phrase de passe » est saisie. Ce champ permet de vérifier que les règles de sécurité d'acceptation minimales de la « Phrase de passe » sont respectées (minimum 15 caractères, au moins une majuscule et au moins un caractère spécial et une force de 90 %).
La force de la « Phrase de passe » est calculée selon plusieurs critères spécifiques : le nombre de majuscules, minuscules, caractères spéciaux, etc. Il convient donc de varier les caractères saisis, de les alterner et d'éviter les répétitions qui tendent à diminuer le score final.

Le bouton « Générer la clé » est grisé et inactif par défaut et restera grisé et inactif tant que ces règles ne sont pas respectées.

Une fois votre « Phrase de passe » saisie en respectant les règles de sécurité et le bouton « Générer la clé » disponible, vous pouvez cliquer dessus.
Il permet de calculer la clé HMAC à partir de la « Phrase de passe » saisie. Ce calcul est une méthode standard assurant le caractère aléatoire de la clé et renforçant sa robustesse. Cette méthode de calcul étant fixe, il est possible à tout moment de retrouver sa clé en saisissant la même « Phrase de passe » et en relançant le calcul.

Il est possible que le calcul de la clé prenne quelques secondes, selon le la puissance de votre ordinateur. Vous devez patienter jusqu'à la fin du calcul.

Une fois le calcul terminé, la clé secrète HMAC sera affichée dans le champ « Clé ». Vous devez alors la copier et la coller dans le champ « HMAC » de la configuration de votre boutique (par exemple, dans la configuration de votre module e-Transactions).

Attention : La clé qui vient d'être générée n'est réellement active sur votre environnement qu'une fois la procédure de confirmation de création de la clé respectée (voir chapitre *2.4.1.2-Confirmation de création*).

Pour des raisons de sécurité, cette clé ne vous sera jamais transmise ni demandée par nos services.
Par conséquent, si cette clé est égarée, vous devrez en générer une nouvelle.
Veillez à bien conserver de manière sécurisée la clé d'authentification affichée, avant de quitter la page car celle-ci ne vous sera plus affichée une fois quitté la page.

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

2.4.1.2 Confirmation de création

Une fois l'enregistrement de la nouvelle clé effectuée, un email de demande de confirmation vous est envoyé. Cet email contient un lien permettant de valider la génération de cette nouvelle clé HMAC.

Attention : La clé, qui vient d'être générée, n'est réellement active qu'une fois la procédure décrite dans cet email est respectée.

Voici un exemple de mail que vous recevez après avoir généré une nouvelle clé HMAC :

Figure 11 : Mail de confirmation de clé HMAC

Après avoir cliqué sur le lien de confirmation présent dans l'email, vous devez voir apparaitre une page avec un message annonçant « Clé Hmac confirmée ».
La clé secrète HMAC entre alors immédiatement en fonction. Ce qui signifie que la clé qui vient d'être validée doit impérativement être aussi paramétrée et en fonction sur votre boutique.

Si vous utilisez déjà une précédente clé secrète HMAC et tant que vous ne cliquez pas sur ce lien, c'est toujours cette ancienne clé HMAC qui est valable et doit être encore en fonctionnement sur votre boutique.

Figure 12 : Installation de clé HMAC confirmée

2.4.2 Bonnes pratiques

La clé HMAC ne doit en aucun cas être transmise par e-mail SANS SECURISATION (fichier chiffré). Les services de la solution e-Transactions ne vous le demandera jamais (y compris les équipes du support e-Transactions). Vous devez donc être particulièrement vigilants quant aux demandes suspectes de transmission de la clé d'authentification HMAC, il s'agit probablement d'une tentative de phishing ou de social engineering.
En cas de perte de votre clé secrète HMAC, les services d'e-Transactions ne seront pas en mesure de vous la communiquer. Il vous faudra alors en générer une nouvelle via le Back Office Vision.

La compromission de la clé HMAC, clé utilisée pour le calcul de la signature HMAC, a pour conséquence de ne plus garantir l'intégrité des données transmises et votre identité lors des échanges techniques avec les serveurs de la solution.

Vous devez impérativement protéger cette clé aussi bien lors de son stockage que lors de son utilisation. Vous devez aussi conserver une copie sécurisée de la clé (archivage) afin de permettre une réactivation rapide du service en cas de dégradation ou de perte du support principal :

- L'archivage de la clé doit être réalisé sur un support durable, sécurisé (encrypté) et isolé du système opérationnel,
- La mise en œuvre opérationnelle de la clé doit aussi faire l'objet d'une sécurisation, support crypté, et contrôle d'accès au système l'hébergeant,

Le stockage « en clair » dans un fichier ou sur tout autres supports quelle qu'en soit la nature est à proscrire.

La communication de données sensibles doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées.

Concernant la confidentialité de la communication :

- Transmission par un support physique :

- Vous devez chiffrer les données avant leur enregistrement sur le support.

- Transmission via un réseau :
  - Si cette transmission utilise la messagerie électronique, vous devez chiffrer les pièces à transmettre.
  - S'il s'agit d'un transfert de fichiers, vous devez utiliser un protocole chiffré garantissant la confidentialité, tel que SFTP ;
  - Si cette transmission utilise le protocole HTTP, vous devez utiliser le protocole TLS 1.2 minimum (HTTPS) pour assurer l'authentification des serveurs et la confidentialité des communications.

- Dans tous les cas, la transmission du secret (clé de déchiffrement, mot de passe, etc.) garantissant la confidentialité du transfert doit s'effectuer dans une transmission distincte, si possible via un canal de nature différente de celui qui servira à la transmission des données (par exemple, envoi du fichier chiffré par mail et communication du mot de passe par téléphone ou SMS).

La gestion de la clé HMAC ne doit jamais se faire en communiquant à un tiers vos identifiants (login / mot de passe) de connexion au Back-office Vision.

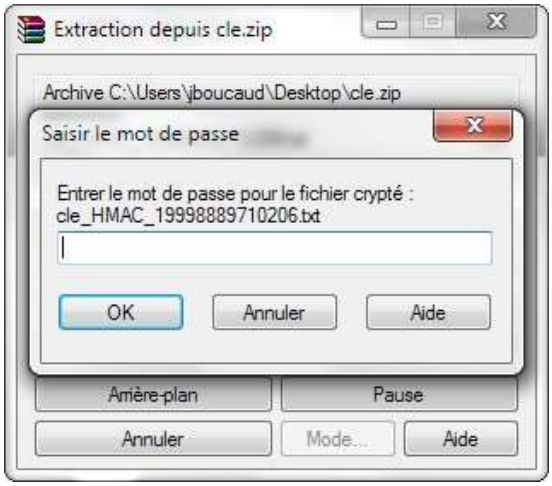
Si ce tiers doit récupérer la clé HMAC, vous devez générer la clé sur le Back Office Vision et lui transmettre via email (Voir procédure ci-dessous) ou autre échange sécurisé.

2.4.2.1 Envoi par email

Procédure à suivre :

- Générer et récupérer la clé HMAC depuis le Back-office Vision
- Copier la clé secrète HMAC dans un fichier texte
- Mettre le fichier texte dans une archive (fichier zip par exemple) protégée par un mot de passe.
- Envoyer ensuite l'archive avec mot de passe dans un 1er email.
- Envoyer le mot de passe associé à l'archive par un autre moyen (SMS …) afin que le destinataire puisse récupérer la clé HMAC.

Voici le rendu final, c'est-à-dire lors de l'ouverture de l'archive .zip



Une fois le mot de passe renseigné, l'accès aux fichier de l'archive est possible.

2.4.3 Utilisation de la clé HMAC

La clé secrète HMAC que vous avez généré sert à authentifier les messages entre votre boutique et les serveurs de la solution Up2pay e-Transactions. Elle garantit également l'intégrité des données transmises et que personne de malveillant n'a modifié un paramètre (le montant par exemple).

Le mécanisme de sécurisation repose donc sur les éléments suivants :

- Construction d'une chaine de caractères à partir de l'ensemble des éléments transmis dans le message et ordonné de la même façon
- Calcul d'une signature du message reposant sur l'algorithme HMAC. L'algorithme est initialisé à partir de votre clé secrète HMAC que vous et la solution sont seuls à connaitre. L'algorithme est appliqué à la chaine de caractères construite précédemment. Ceci génère donc une empreinte unique reproductible uniquement avec les mêmes données et la même clé secrète.
- L'empreinte calculée précédemment est également envoyée dans les paramètres du message en tant que signature.
- La solution Up2pay e-Transactions, destinataire du message, reproduit le même calcul (construction de la chaine de caractères avec les paramètres reçus (hors signature reçue), initialisation de l'algorithme HMAC avec la clé dédiée à votre boutique, application de l'algorithme HMAC sur la chaine de caractères) pour obtenir une empreinte du message.
- La solution Up2pay e-Transactions compare la signature reçue avec l'empreinte calculée de son côté. Si les valeurs sont identiques c'est que le message provient bien de votre boutique et que les données n'ont pas été modifiée entre l'envoi et la réception des paramètres.

La clé secrète HMAC est nécessaire dans les cas suivants :

- Affichage des pages de paiements vers laquelle votre client est redirigé (ou intégré dans votre boutique) : la page de paiement ne s'affiche que si votre contrat commerçant est bien authentifié et les données vérifiées (voir le chapitre *3.3-Calcul de la signature avec la clé HMAC)*;
- Utilisation des API pour effectuer des opérations entre votre boutique et la solution de serveur à serveur (opérations de paiement, captures, remboursements, …) : les opérations ne sont réalisées que si votre contrat commerçant est bien authentifié et les données vérifiées ;

Il est possible, en fonction de vos contraintes techniques de choisir le sous-algorithme à utiliser pour « hasher » (application de l'algorithme HMAC) la chaine de caractères contenant les données transmises et calculer la signature du message. Sauf contrainte, nous vous conseillons d'utiliser le sous-algorithme SHA512 pour effectuer le hashage HMAC.

2.5 Codes de retours

Lors de vos échanges avec la solution Up2pay e-Transactions (pages de paiement ou opération), celle-ci vous renvoit un Code de retour vous permettant de savoir si l'opération s'est bien déroulée.

Lors des appels aux pages de paiement, vous devez demander de récupérer la donnée E (Code retour) qui vous permet de récupérer ce résultat dans une variable.
Lors des appels aux API, le Code de retour vous est toujours renvoyé dans le paramètre CODEREPONSE.

En cas de succès du paiement ou de l'opération, vous recevez la valeur « 00000 ». Tous les autres codes réponse que vous pouvez recevoir correspondent à une erreur lors du paiement ou de l'opération. Vous trouverez la liste des codes d'erreur à l'annexe : *12.1-Codes de retour des pages de paiement (variable E avec PBX_RETOUR)*.

Si vous recevez un code d'erreur au format « 001xx », il s'agit d'un code d'erreur du centre d'autorisation dont dépend le moyen de paiement (carte de paiement) saisi.
Par exemple, pour une transaction refusée pour raison « provision insuffisante », le code erreur renvoyé sera 00151. Vous trouverez la liste des codes d'erreur de chaque centre d'autorisation à l'annexe : *12.3-Codes réponse du centre d'autorisation*.
Le code « 00100 » qui correspond à un succès du centre d'autorisation est modifié en « 00000 » pour signifier le succès du paiement, vous ne recevrez donc pas « 00100 » mais « 00000 ».
Lors des paiements réalisés uniquement avec les API, Si vous recevez un code d'erreur « 00201 », 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 chapitre *7.4.2-Authentification 3D-Secure)* et réaliser à nouveau une demande d'autorisation.

En cas d'erreur, la Gestion Automatisée des Encaissements (API) fournit aussi un message d'erreur détaillé dans le champ COMMENTAIRE qui permettra, si besoin, une aide au diagnostic avec l'assistance e-Transactions.

2.6 Environnement de test

Avant de commencer à effectuer des paiements sur votre site en production, nous vous recommandons de vérifier l'intégration correcte de la solution Up2pay e-Transactions dans votre boutique. Pour cela, nous vous mettons à disposition une plateforme de recette, ainsi que des comptes et des paramètres de recette, entièrement destinés à la réalisation des tests.

Toutes les informations relatives à cet environnement de recette sont précisées dans la documentation ***Ref5-Réalisation des tests d'intégration e-Transactions*** accessible en téléchargement sur https://www.ca-moncommerce.com/.

2.7 URL à utiliser et adresses IP

2.7.1 Load-Balancer

Un mécanisme de Global Load Balancer (GLB) permet de garantir une haute disponibilité des services de la solution Up2pay e-Transactions qui sont opérés par 2 serveurs redondés. Ce mécanisme vous évite de gérer la bascule entre les différents sites et unifie l'URL appelée.

Pour autant, les 2 serveurs cités ci-dessus sont accessibles par des couples d'urls distinctes en fonction des services adressés (pages de paiement, API, …). Vous pouvez utiliser indifféremment l'une ou l'autre de ces urls dans votre intégration mais également prévoir un mécanisme de bascule de l'un vers l'autre si malgré le mécanisme de GLB, le service n'est pas fonctionnel et nécessite une bascule volontaire vers l'une ou l'autre de ces urls.

2.7.2 URLs à appeler

Les URLs pour initier une transaction avec une page de choix de moyen de paiement (RWD – Responsive Web Design – La page s'adapte au média utilisé) :

Plateforme	URL d'accès
Recette	https://recette-tpeweb.e-transactions.fr/php/
Production	https://tpeweb.e-transactions.fr/php/
Production	https://tpeweb1.e-transactions.fr/php/

Les URLs (sensibles à la casse) pour initier une transaction en redirigeant directement votre client sur la page de paiement correspondant au moyen de paiement choisi dans votre boutique (RWD – Responsive Web Design – La page s'adapte au média utilisé) :

Plateforme	URL d'accès
Recette	https://recette-tpeweb.e-transactions.fr/cgi/FramepagepaiementRWD.cgi
Production	https://tpeweb.e-transactions.fr/cgi/FramepagepaiementRWD.cgi
Production	https://tpeweb1.e-transactions.fr/cgi/FramepagepaiementRWD.cgi

PBX_TYPEPAIEMENT et PBX_TYPECARTE doivent être envoyés à ces URL, surtout si vous avez plus d'un moyen de paiement souscrit.
Vous pouvez aussi utiliser la page /php/ ci-dessus avec les champs PBX_TYPEPAIEMENT et PBX_TYPECARTE. Dans ce cas, votre client est redirigé automatiquement vers la bonne page de paiement (saut visible dans le navigateur).

Les URLs pour initier des transactions avec une page de paiement intégrée dans votre boutique (iFrame) :

Plateforme	URL d'accès
Recette	https://recette-tpeweb.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi
Production	https://tpeweb.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi
Production	https://tpeweb1.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi

Les URLs pour utiliser les API de la solution (**G**estion **A**utomatisée des **E**ncaissements):

Plateforme	URL d'accès
Recette	https://recette-ppps.e-transactions.fr/PPPS.php
Production	https://ppps.e-transactions.fr/PPPS.php
Production	https://ppps1.e-transactions.fr/PPPS.php

Les URLs pour utiliser réaliser l'authentification 3D-Secure pour les paiements effectués par API (services **e-Transactions Remote MPI)** :

Plateforme	URL d'accès

Recette	https://recette-tpeweb.e-transactions.fr/cgi/RemoteMPI.cgi
Production	https://tpeweb.e-transactions.fr/cgi/RemoteMPI.cgi
Production	https://tpeweb1.e-transactions.fr/cgi/RemoteMPI.cgi

2.7.3 Adresses IP

L'adresse IP entrante est l'adresse sur laquelle votre boutique se connecte pour réaliser la transaction ou les opérations par API.

L'adresse IP sortante est l'adresse avec laquelle votre boutique voit arriver les flux de retour en fin de transaction (appels de l'IPN par exemple).

Il est important que ces adresses entrantes et sortantes soient autorisées dans les éventuels filtres sur les adresses IP paramétrés sur l'infrastructure hébergeant votre boutique.

Plateforme	URL Entrante	Adresse IP Entrante	Adresse IP Sortante
Recette	recette-tpeweb.e-transactions.fr	195.25.7.147	195.25.67.22
	recette-ppps.e-transactions.fr	195.25.7.147	
Production	tpeweb.e-transactions.fr	194.2.160.85	194.2.122.190
	tpeweb1.e-transactions.fr	195.25.67.12	195.25.67.22
	ppps.e-transactions.fr	194.2.160.89	
	ppps1.e-transactions.fr	195.25.67.10	

Tableau 2 : Adresses IP

INTEGRATION TECHNIQUE

3. Afficher une page de paiement

3.1 En redirection

Il existe différentes façons d'afficher la page de paiement à vos clients.
Dans le cas de l'appel à la page de paiement en redirection, les variables suivantes sont obligatoires dans toute requête :

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

La signification de ces différentes variables ainsi que des variables optionnelles est disponible en ANNEXE, chapitre 11.

L'ensemble de ces variables doit être envoyé par la méthode POST vers l'URL de la page de paiement de la solution e-Transactions.

Ci-dessous un exemple de formulaire transmis en recette :

```
<form method="POST" action="https://recette-tpeweb.e-transactions.fr/php/">
<input type="hidden" name="PBX_SITE" value="9999999">
<input type="hidden" name="PBX_RANG" value="595">
<input type="hidden" name="PBX_IDENTIFIANT" value="3">
<input type="hidden" name="PBX_SOURCE" value="RWD">
<input type="hidden" name="PBX_TOTAL" value="1000">
<input type="hidden" name="PBX_DEVISE" value="978">
<input type="hidden" name="PBX_CMD" value="Ref_Cmd_001">
<input type="hidden" name="PBX_PORTEUR" value="test@gmail.com">
<input type="hidden" name="PBX_RETOUR" value="Mt:M;Ref:R;Auto:A;Erreur:E">
<input type="hidden" name="PBX_HASH" value="SHA512">
<input type="hidden" name="PBX_TIME" value="2021-02-28T11:01:50+01:00">
<input type="hidden" name="PBX_HMAC" value="F2A799494504F9E50E91E44C129A45BBA2
6D23F2760CDF92B93166652B9787463E12BAD4C660455FB0447F882B22256DE6E703AD6669B73C59 B034AF0CFC7E">
<input type="submit" value="Envoyer">
</form>
```

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

Après avoir cliqué sur ce bouton, le client sera automatiquement dirigé vers la page de paiement de e-Transactions. Le montant doit systématiquement être envoyé en centimes, dans cet exemple le montant est de 1000 centimes d'euros (soit 10 €) et l'identification de la transaction par rapport à la commande est la référence « Ref_Cmd_001 ».

Une fois le paiement effectué, si ce dernier est accepté, un ticket de paiement est envoyé par mail à l'adresse de votre client indiquée dans PBX_PORTEUR : *test@gmail.com* (vous recevez également ce ticket de paiement par e-mail si vous avez activé cette option dans votre Back-Office Vision – non activé par défaut).

L'identification du commerçant (site 9999999, rang 595, identifiant 3) correspond à la boutique de test e-Transactions, accessible sur notre environnement de recette.

Nous vous conseillons d'utiliser vos propres identifiants et votre clé HMAC de recette (à générer dans votre back-office e-Transactions, **serveur Recette**).
Les URL d'appel en production sont définies au chapitre *2.7.2-URLs à appeler*

Vous trouverez un exemple de code PHP pour afficher une page de paiement au chapitre *15.2-Exemple d'appel de la page de paiement avec clé HMAC.*

3.1.1 Vers la page de choix des moyens de paiement

L'appel à la page de paiement e-Transactions sans forçage des moyens de paiement, permet à vos clients d'accéder à la page de présélection des moyens de paiement.
Sur cette page, s'affichent les logos et libellés associés aux moyens de paiement souscrits dans votre offre.

Votre client peut alors faire son choix en cliquant sur le moyen de paiement à utiliser pour effectuer son paiement.

Si un nouveau moyen de paiement venait à s'ajouter à votre offre, il s'affichera automatiquement sur cette page de présélection.

L'appel à cette page de choix des moyens de paiement s'effectue si votre script de paiement est exempt des variables PBX_TYPEPAIEMENT et PBX_TYPECARTE.

La page de choix du moyen de paiement, qui est en mode responsive, s'adapte au média et à l'écran qu'utilise votre client :

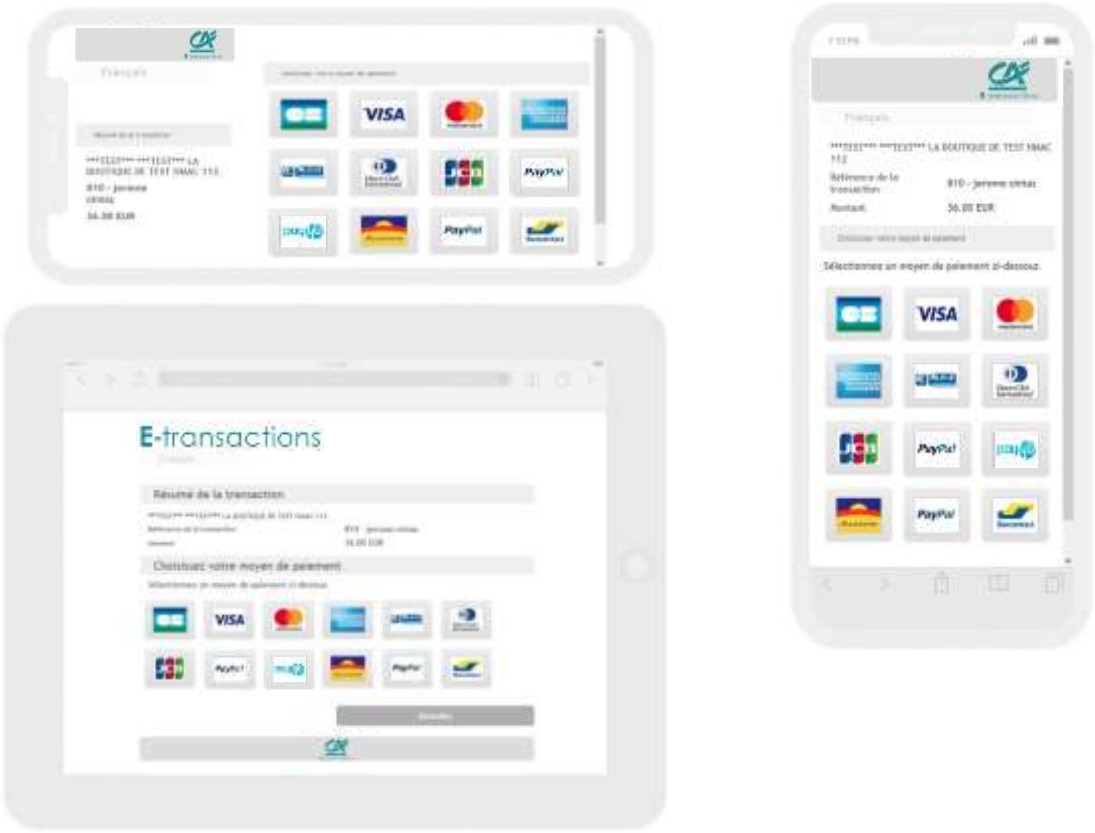


Figure 13 : Page de choix des Moyens de paiement sur différents médias

Attention, ces exemples ne sont pas contractuels

Attention : vous deviez systématiquement indiquer PBX_SOURCE=RWD dans vos appels pour que la page de choix des moyens de paiement affichée soit bien responsive design.

3.1.2 Avec choix direct du moyen de paiement (forçage)

Si vous préférez gérer vous-même de l'affichage du choix des moyens de paiement directement sur votre site, il est possible de fournir l'information du moyen de paiement choisi dans le formulaire de paiement.

Ceci se fait par l'intermédiaire des variables PBX_TYPEPAIEMENT et PBX_TYPECARTE.
Ainsi votre client est redirigé directement sur la page de paiement adaptée au moyen de paiement choisi, et ne voit pas la page de présélection du moyen de paiement e-Transactions.

L'intérêt pour vous est de proposer sur votre site, les moyens de paiement selon des critères que vous aurez définis, ou tout simplement réduire le nombre d'étapes dans le processus de paiement.
Néanmoins, vous devrez modifier votre paramétrage afin d'afficher et/ou supprimer chaque moyen de paiement supplémentaire souscrit ou supprimé.

Exemple : Pour un paiement avec Paylib, il faut valoriser PBX_TYPEPAIEMENT à « WALLET » et PBX_TYPECARTE à « PAYLIB ».
L'ensemble des valeurs possibles pour ces variables est disponible dans à l'annexe : *11.1.2.23-PBX_TYPECARTE*

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

Cas spécifique CB-VISA-MASTERCARD :
La page de paiement pour CB, VISA et MASTERCARD est la même sur la plateforme Up2pay e-Transactions. Vous pouvez donc n'utiliser qu'un choix pour vos clients de paiement par carte bancaire. Sur cette page de paiement, la ou les marques de la carte de paiement de votre client sont détectées pendant la saisie du numéro de carte. Votre client peut choisir la marque qu'il souhaite utiliser. Par défaut, CB sera choisi si la carte de votre client est compatible CB.

Pour ces trois cartes, PBX_TYPEPAIEMENT = CARTE suffit à diriger le porteur sur cette page de paiement pour CB, VISA et MASTERCARD.

Dans le cas où vous envoyez tout de même la variable PBX_TYPECARTE, **votre client sera malgré tout dirigé vers la page de paiement commune pour CB, VISA et MASTERCARD.**

3.1.3 Page de paiement

La page de paiement e-Transactions est responsive design, ce qui signifie qu'elle s'adapte aux dimensions de l'écran et au média qui la visualise, en utilisant des techniques CSS, et un code HTML optimisé.

Selon le matériel utilisé par le porteur, la page de paiement peut donc prendre des formes différentes.

Attention : vous deviez systématiquement indiquer PBX_SOURCE=RWD dans vos appels pour que la page de paiement affichée soit bien responsive design.

Voici quelques exemples (*copies d'écran non contractuelles)* :

Figure 14 : Vue sur smartphone - position verticale

Figure 15 : Vue sur smartphone - Position horizontale

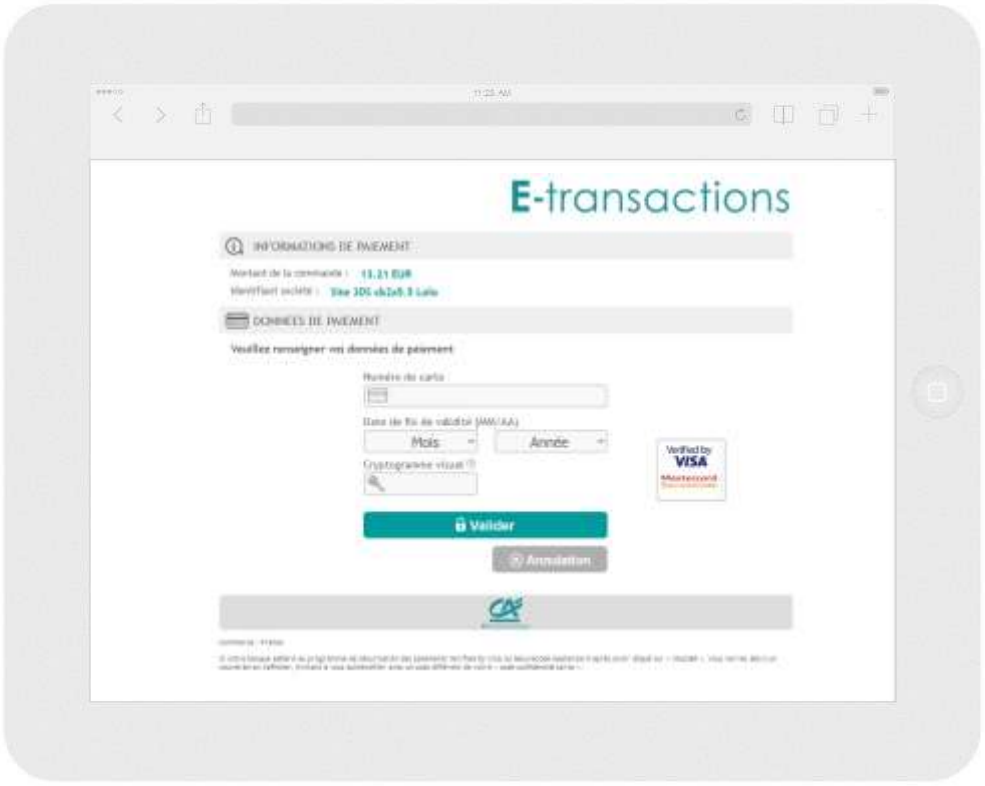


Figure 16 : Vue sur Tablette - Position horizontale

3.1.4 Déclenchement du 3D-Secure

Cette section concerne les moyens de paiement CB, VISA et MASTERCARD.

Après avoir renseigné ses informations bancaires sur la page de paiement, le porteur clique sur le bouton pour valider le paiement.
La solution e-Transactions interroge la banque du porteur afin de le rediriger vers la page de demande d'authentification de celle-ci pour authentifier la transaction (3D-Secure).

Le porteur est automatiquement redirigé vers la page de demande d'authentification hébergée par sa banque, afin de valider l'étape 3D-Secure :

- Si l'authentification est réussie, la banque du porteur envoie les informations d'authentification dans un jeton à la plateforme e-Transactions, confirmant l'authentification.
  Après cette étape, e-Transactions émet une demande d'autorisation bancaire à la banque du porteur en indiquant le jeton précédemment reçu.

- Si l'authentification a échoué, il n'y a pas de demande d'autorisation et la transaction est refusée. Un jeton est également transmis à la plateforme e-Transactions confirmant l'échec d'authentification.

Le porteur peut retenter jusqu'à deux fois d'effectuer le paiement de sa commande soit 3 tentatives au total.

3.2 Intégration dans les pages du commerçant (Seamless - iFrame)

Si vous souhaitez intégrer la page de paiement hébergée par la plateforme e-Transactions directement à l'intérieur d'une page de votre boutique, vous devez :

- Préparer l'ensemble des variables requises par les pages de paiement et les intégrer dans un formulaire web tel que décrit au paragraphe : §3.1 en redirection
- Définir un espace dans votre page pour accueillir le formulaire de paiement en utilisant une iFrame
- Soumettre le formulaire précédemment préparé avec l'iFrame comme cible (target). Une action javascript dans votre page peut, par exemple, effectuer cette soumission.
- Une fois le paiement réalisé (en succès ou en échec), votre client est redirigé vers une page de votre choix à l'intérieur de l'iFrame. Vous pouvez à ce moment-là prendre en compte ce retour puis rediriger votre client vers une autre url de votre page principale.
- En parallèle vous recevez également l'appel de notification de paiement instantanée (IPN). Grâce à celle-ci vous pouvez mettre à jour votre commande. Vous pouvez également vous en servir pour indiquer à votre page de paiement en attente de retour qu'elle peut rediriger votre client vers la page de confirmation de commande ou d'échec de paiement.

Si vous souhaitez l'intégration d'un formulaire simplifié, ne présentant que les champs de saisie numéro de carte, CVV et date d'expiration, vous devez utiliser l'URL dédiée à cet usage : voir *2.7.2-URLs à appeler*.

3.2.1 Déclenchement du 3D-Secure

Lorsque la page de paiement est intégrée sous forme d'iFrame le fonctionnement du 3D-Secure reste inchangé (voir chapitre ci-dessus 3.1.4).
Néanmoins le formulaire de paiement étant contenu dans une iFrame, cette dernière s'actualise afin d'afficher la page d'authentification 3D-Secure de la banque du porteur.
Le client peut alors s'authentifier sur cette page et poursuivre le processus de paiement.

3.3 Calcul de la signature avec la clé HMAC

Afin de sécuriser l'envoi vers les différentes pages de paiement, c'est-à-dire d'authentifier que les appels proviennent bien de votre boutique et de garantir l'intégrité des données, la solution Up2pay e-Transactions 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 qui vont être envoyés aux serveurs de la solution e-Transactions. 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 :
-

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

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 la page de paiement.
- 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 :** Vous devez procéder au calcul de l'empreinte HMAC, en utilisant :
  - La chaine qui vient d'être construite
  - La clé secrète obtenue via le Back Office
  - Un sous-algorithme au choix que vous devez également préciser dans le paramètre PBX_HASH envoyé à la page de paiement (cf. *11.1.1.9-PBX_HASH*). Attention, ce paramètre PBX_HASH est donc 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 PBX_HMAC de la requête.

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

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



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


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


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


$hmac = strtoupper(hash_hmac('sha512', $msg, $binKey));
// La chaîne sera envoyée en majuscules, d'où l'utilisation de strtoupper()
// On crée le formulaire à envoyer à e-transactions
// ATTENTION : l'ordre des champs est extrêmement important, il doit
// correspondre exactement à l'ordre des champs dans la chaîne hachée  ?>
<form method="POST" action="https://tpeweb.e-transactions.fr/php/">
<input type="hidden" name="PBX_SITE" value="1999887">
<input type="hidden" name="PBX_RANG" value="32">
<input type="hidden" name="PBX_IDENTIFIANT" value="2">
<input type="hidden" name="PBX_SOURCE" value="RWD">
<input type="hidden" name="PBX_TOTAL" value="<? echo $_POST['montant']; ?>">
<input type="hidden" name="PBX_DEVISE" value="978">
<input type="hidden" name="PBX_CMD" value="<? echo $_POST['ref']; ?>">
<input type="hidden" name="PBX_PORTEUR" value="<? echo $_POST['email']; ?>">
<input type="hidden" name="PBX_RETOUR" value="Mt:M;Ref:R;Auto:A;Erreur:E">
```

```
<input type="hidden" name="PBX_HASH" value="SHA512">
<input type="hidden" name="PBX_TIME" value="<? echo $dateTime; ?>">
<input type="hidden" name="PBX_HMAC" value="<? echo $hmac; ?>">
<input type="submit" value="Envoyer">
</form>
```

3.4 Personnalisation des pages de paiement

Pour rassurer vos clients, il est possible de personnaliser des éléments pour que la page de paiement s'intègre au mieux dans la charte graphique de votre site.

Les éléments personnalisables sont notamment :

- Votre logo en haut de page
- L'affichage du logo Crédit Agricole
- Les boutons de validation/annulation/ « retour boutique »
- La langue par défaut et les boutons de langues à afficher
- Le fond d'écran

D'autres éléments de la page de paiement peuvent être personnalisées en construisant vous-même une feuille de style (fichier CSS) à appliquer lorsque la page s'affiche pour votre contrat commerçant.

Référez-vous au chapitre : *10-Personnalisation de la page de paiement* pour des informations détaillées sur la personnalisation.

3.5 Paiement avec débit immédiat (autorisation + capture) (Mode par défaut)

Par défaut, le paiement d'une commande se caractérise par une demande d'autorisation + 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.

Le formulaire d'exemple d'une page de paiement « En redirection » (*3.1-En redirection*) est un formulaire d'autorisation + capture.

3.5.1 Principe

Après l'authentification 3D-Secure réussie dans le parcours de paiement, la demande d'autorisation bancaire s'effectue. Si elle est accordée par la banque du porteur, la transaction est automatiquement acceptée et se place dans un fichier de remise des transactions qui sera automatiquement envoyée en banque lors de la prochaine télécollecte.
La télécollecte de la remise, c'est-à-dire l'envoi en banque des transactions vers votre banque Crédit Agricole et/ou vers votre établissement financier privatif selon le moyen de paiement, s'effectue quotidiennement entre minuit et 5h00, vous êtes crédité à J+1 et votre client débité, selon les délais interbancaires.

Les avantages :

- Mode par défaut, simple à mettre en place
- Pas d'action manuelle ou d'intégration technique supplémentaire nécessaire de votre part : débit après envoi en banque automatique

- Crédit en compte à J + 1
- Annulation totale possible avant la télécollecte
- Remboursement possible après la télécollecte, partiel ou total
-

Inconvénients :

- Pas d'annulation partielle possible
- Votre client est débité immédiatement, ce qui peut être un frein commercial si votre stock est insuffisant, retard d'expédition, ou qu'il demande une modification de la commande.

3.6 Paiement en autorisation seule

3.6.1 Principe

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

3.6.2 Utilisation

En ajoutant la variable PBX_AUTOSEULE=''O' (la lettre O en majuscule) au formulaire soumis à la page de paiement hébergée par la solution, seule l'autorisation sera réalisée. Il n'y aura pas de capture automatique pour l'envoi en banque (télécollecte).

Si PBX_AUTOSEULE est valorisé à 'N' ou si cette variable est absente du formulaire de paiement, la transaction est réalisé en mode par défaut (autorisation + capture) : elle est « marquée » pour être télécollectée le soir même.

3.6.3 Complément d'utilisation

Lorsque la transaction est réalisée en mode autorisation seule, elle est enregistrée sur la plateforme e-Transactions.
Elle peut être capturée (télécollectée) ultérieurement dans un délai de 75 jours maximum, via :

- l'utilisation des API (Gestion Automatisée des Encaissements),
- le back-office Vision Air

Pour les paiements par carte, le Crédit Agricole vous préconise de ne pas dépasser 6 jours entre la date de la demande d'autorisation et la date de remise en banque (capture). Au-delà, vous perdez la garantie 3D-Secure, et pouvez être débité d'impayés pour encaissement tardif.

Pour les paiements PayPal, la capture peut se faire jusqu'à 29 jours après la demande d'autorisation. Cependant, PayPal ne garantit les fonds que durant les 4 premiers jours.

3.7 Paiement différé automatique en nombre de jours

3.7.1 Principe

La solution e-Transactions gére les paiements différés, c'est-à-dire conserver les transactions un nombre de jours déterminés par vos soins avant de les envoyer vers le centre de télécollecte de votre banque ou de l'établissement financier privatif pour débiter votre client et vous créditer.
Cette fonctionnalité peut s'avérer très utile, lorsque vous désirez vous assurer que la marchandise ou le service a été expédié au client avant que ce dernier ne soit débité.

Sur la fiche de souscription de votre contrat e-Transactions, il est demandé de préciser le nombre de jours de différé souhaité par défaut :

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

Vous avez également la possibilité de définir un différé dans votre script de paiement. Ce point est détaillé ci-dessous.

Pour les paiements par carte, le Crédit Agricole vous préconise de ne pas dépasser 6 jours entre la date de la demande d'autorisation et la date de remise en banque (capture).
Au-delà, vous perdez la garantie 3D-Secure, et pouvez être débité d'impayés pour encaissement tardif.

3.7.2 Utilisation

Pour définir un nombre de jours de différé, il convient de rajouter la variable PBX_DIFF à votre script de paiement et lui affecter une valeur numérique correspondant au nombre de jours de décalage souhaité entre l'achat et la télécollecte.
Attention, votre transaction sera intégrée à la prochaine télécollecte qui suit le décalage indiqué. Par exemple, pour une transaction passée 1h après une télécollecte et un différé indiqué de 2 jours, celle-ci sera prise en compte dans la télécollecte qui interviendra 71h plus tard (et non 48h plus tard).

Exemple pour un décalage de 3 jours : `PBX_DIFF=3`

Ce nombre de jours de décalage peut être fixé à une valeur par défaut à l'ouverture du contrat, mais si vous ajoutez cette variable à votre script de paiement, il primera sur la valeur définie sur votre contrat.

3.8 Indiquer les informations et variables à recevoir en retour

Il est possible de configurer la liste des variables qui sont renvoyées à votre site marchand dans les différentes URL de retour.
Les informations demandées vous seront retournées quel que soit le résultat de la demande d'autorisation si elles sont pertinentes (ex : pas de numéro d'autorisation suite à un échec d'autorisation).

Cette configuration est effectuée par la variable PBX_RETOUR, qui se construit en concaténant la liste des informations souhaitées sous le format suivant :

```
<nom de la variable renvoyée>:<lettre de la donnée e-Transactions souhaitée>;
```

Exemple :

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

Le nom que vous donnez aux variables (montant, maref,…) est personnalisable.
Le nombre de caractères total de la variable PBX_RETOUR étant limité à 250, nous vous conseillons d'utiliser des noms courts.

Selon les options disponibles sur votre contrat, le moyen de paiement et la méthode choisis, toutes les informations souhaitées ne sont pas disponibles.
Par exemple, il n'est pas possible de demander à recevoir « U » (token suite à la création d'un abonné) pour certains moyens de paiement ou si vous ne disposez pas d'une offre Premium avec option Gestion Automatisée des Encaissements.

Pour voir l'ensemble des données disponibles, voir le paramètre **PBX_RETOUR (***11.1.1.8-PBX_RETOUR***)**.
Ces informations seront envoyées à toutes les URL de retour (PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE et PBX_REPONDRE_A).

Voir les chapitres *4-Récupérer le retour de la page de paiement sur votre site* et *5-Notifications de Paiement Instantanées (IPN)* pour la récupération et l'interprétation de ces informations.

4. Récupérer le retour de la page de paiement sur votre site

Une fois le paiement réalisé sur la page de paiement e-Transactions, le client sera redirigé sur votre site par l'intermédiaire de 4 URL qui permettent d'adapter les traitements au résultat du paiement.

L'utilisation des 4 URL est dépendante du comportement du client final : ces URL sont appelées uniquement si le client poursuit le processus de paiement jusqu'à son retour sur votre site marchand. Il est préférable d'utiliser la 5ème URL IPN pour gérer de façon automatique la validation de vos bons de commandes suivant le résultat de la transaction par l'intermédiaire de 5ème URL nommée IPN (Instant Payment Notification).**(voir le chapitre** *5-Notifications de Paiement Instantanées (IPN)***)**

4.1 Intégration

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

- Soit en les définissant pour chaque transaction,
  - Cela permet d'afficher une page personnalisée pour chaque client
  - Il faut alors les définir à chaque transaction en utilisant les variables PBX_EFFECTUE, PBX_REFUSE, PBX_ANNULE, PBX_ATTENTE dans le formulaire de paiement

- Soit en utilisant les valeurs par défaut enregistrées dans la base de données e-Transactions
  - Ces valeurs peuvent être renseignées sur votre Back Office Vision Air, onglet « Paramétrage ».

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

Il est également possible de choisir un retour immédiat : il faut préciser cette option en contactant l'assistance e-Transactions.
Dans ce cas-là, le ticket récapitulatif n'est pas affiché et le client est redirigé directement vers votre site.

En cas de présence de caractères HTML spéciaux dans l'URL à appeler, il faut « URL Encoder », c'est-à-dire les convertir en un code spécial compatible avec l'encodage d'une URL.

Par exemple, si l'URL « PBX_EFFECTUE » contient le caractère « ; » :

```
www.commerce.fr/effectue.jsp;id_session=134ERF47
```

Il faudra documenter la variable « PBX_EFFECTUE » de la manière suivante en remplaçant ce caractère par %3B :

```
www.commerce.fr/effectue.jsp%3Bid_session=134ERF47
```

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

En Annexe se trouve une liste des caractères spéciaux les plus fréquents et leur valeur convertie « URL Encodée » voir *14-Caractères URL Encodés*).

4.2 Authentification des messages

Pour garantir la sécurité de ces retours effectués sur les pages de votre boutique après le paiement, vous devez en vérifier l'authenticité et l'intégrité des données.

Il est **impératif** de vérifier les éléments suivants :

- **Signature (donnée K)**
  - Reportez-vous au chapitre *6-Authentification des messages reçus* pour plus de détail sur les vérifications de signature à effectuer.

4.3 Interprétation du retour

En fonction des informations et variables souhaitées en retour de la page de paiement et configuré dans le paramètre PBX_RETOUR de l'appel à la page de paiement (voir « Indiquer les informations et variable à recevoir en retour »), celles-ci sont envoyées à toutes les URL de retour (PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE, PBX_ATTENTE et PBX_REPONDRE_A).

Vous recevez en retour autant de variables que vous avez définies. Ces variables sont nommées comme vous les avez paramétrées dans PBX_RETOUR et contiennent les valeurs associées au paiement en cours comme prévu par la variable de la solution que vous avez mappée.

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

Par exemple, si vous avez indiqué vouloir recevoir le Code d'erreur de la page dans la variable code_erreur mappée sur la variable E (PBX_RETOUR=code_erreur:E;), vous n'avez qu'à lire votre variable _GET['code_erreur'] pour connaitre le résultat du paiement.

Par exemple, pour l'URL de paiement en succès (PBX_EFFECTUE) avec la valeur citée ci-dessus, la page de redirection de votre client après un paiement en succès serait :

```
http://www.commerce.fr/front/paiement_ok.php?ref=abc12&trans=71256&auto=30258&tarif=2000
&abonnement=354341&pays=FRA&code_erreur=00000
```

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

- Code erreur (variable E) :
  - Pour une transaction valide, il doit être à « 00000 »
  - Pour les autres valeurs, se reporter au chapitre *12.1-Codes de retour des pages de paiement (variable E avec PBX_RETOUR)*
  - Dans le cas d'un paiement refusé par le centre d'autorisation (code erreur à 001xx), les «xx» représentent le code renvoyé par le centre. Ce code permet de connaître la raison exacte du rejet de la transaction.
    Par exemple, pour une transaction refusée pour raison « provision insuffisante », le code erreur renvoyé sera 00151.
    Tous les codes sont précisés au chapitre *12.3-Codes réponse du centre d'autorisation*.

- Numéro d'autorisation (variable A) : alphanumérique, longueur variable.
  - Pour une transaction de test (pas de demande d'autorisation vers le serveur du Crédit Agricole ou l'établissement financier privatif), la variable vaut toujours « XXXXXX »
  - Pour une transaction refusée, la variable n'est pas envoyée

4.4 Gestion des paiements en attente de validation

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

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

La solution e-Transactions se charge ensuite de mettre à jour la réponse, et quand une décision a été prise, e-Transactions envoie via l'IPN la réponse définitive (ex : 00000 si la transaction est autorisée).

Pour plus d'informations sur ces moyens de paiement, vous pouvez vous référer au document d'intégration des moyens de paiement complémentaires (Ref1).

5. Notifications de Paiement Instantanées (IPN)

5.1 Principe

Cette variable IPN est spécialement utilisée pour gérer de façon automatique la validation des bons de commandes. Cette variable doit être utilisée pour valider vos bons de commandes car elle a l'avantage d'être appelée de serveur à serveur dès que le client valide son paiement (que ce dernier soit autorisé ou refusé), contrairement aux précédentes URL de retour qui dépendent d'une action du client.

Elle est beaucoup plus sûre car elle permet de valider automatiquement le bon de commande correspondant même si le client coupe la connexion ou décide de ne pas revenir sur votre boutique, car cet appel ne transite pas par le navigateur du client.

5.2 URL appelée par les serveurs de la solution e-Transactions

Cette variable est une URL quoi doit être créée sur votre serveur, et qui peut être communiquée à e-Transactions de deux manières :

- enregistrée dans la base de données e-Transactions : url à renseigner par vos soins dans le champs « Url de retour http » disponible dans le paramétrage de votre contrat sur votre back-office Vision Air

- gérée dynamiquement par votre boutique comme les 4 URL précédentes via la variable « PBX_REPONDRE_A ».

Si la variable PBX_REPONDRE_A est gérée dynamiquement par votre boutique, elle est prioritaire par rapport à l'information enregistrée en base de donnée e-Transactions.

Lors de l'appel de cette URL, un script présent sur le serveur de votre boutique à l'emplacement spécifié par l'URL, va s'exécuter afin de récupérer et traiter les informations de retour sur la transaction.
Il n'y a pas de contrainte sur le langage de ce script (ASP, PHP, PERL, …).
Les seules obligations sont de ne pas réaliser de redirection à l'aide de ce script et de générer une page HTML vide.

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

Cette URL n'a aucun lien direct avec les **URLs de retour (voir chapitre** *4-Récupérer le retour de la page de paiement sur votre site*) : elle est gérée de façon complètement indépendante et peut être appelée même si vous la mettez à disposition sur certains ports TCP spécifiques de votre serveur web (un port TCP est une porte numérotée de votre serveur derrière laquelle un service attend d'être appelé).
Vous pouvez indiquer une URL en https:// (port 443) ou préciser que le script est disponible derrière les ports TCP suivants 8080, 8081, 8082, 8083, 8084 ou 8085 (URL du type https://www.maboutique.com:8083/monscript).

5.3 Authentification des messages

Pour garantir la sécurité de ces appels reçus, vous devez vérifier l'origine ainsi que l'authenticité et l'intégrité des données.

Il est **impératif** de vérifier les éléments suivants :

- **Adresse IP d'origine**
  - Vérifiez que l'appel à l'URL IPN que vous avez défini provient bien de l'adresse sortante d'un de nos serveurs (voir ***§***10.6 ***URL d'appel et Adresses IP***).

- **Signature (donnée K)**
  - Reportez-vous au chapitre *6-Authentification des messages reçus* pour plus de détails sur les vérifications de signature à effectuer.

5.4 Interprétation du retour

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

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

En fonction des informations et variables souhaitées en retour de la page de paiement et configurées dans le paramètre PBX_RETOUR de l'appel à la page de paiement (voir « Indiquer les informations et variables à recevoir en retour »), celles-ci seront envoyées à toutes les URL de retour dont l'appel du serveur de la solution de paiement à l'URL IPN.

Vous recevez en retour autant de variables que vous aurez définies. Ces variables sont nommées comme vous les avez paramétrées dans PBX_RETOUR et contiendront les valeurs associées au paiement en cours comme prévu par la variable de la solution que vous avez mappée.

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

Par exemple, si vous avez indiqué vouloir recevoir le Code d'erreur de la page dans la variable code_erreur mappée sur la variable E (PBX_RETOUR=code_erreur:E;), par simple lecture de votre variable _GET['code_erreur'] vous récupérez le résultat du paiement.

Par exemple, pour l'URL IPN, avec la valeur citée ci-dessus, la page appelée est :

```
http://www.commerce.fr/cgi/verif_pmt.asp?ref=abc12&trans=71256&auto=30258&tarif=2
000&abonnement=354341&pays=FRA&erreur=00000
```

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

- Code erreur (variable E) :
  - Pour une transaction valide, il doit être à « 00000 »
  - Pour les autres valeurs, se reporter au chapitre *12.1-Codes de retour des pages de paiement (variable E avec PBX_RETOUR)*

- Dans le cas d'un paiement refusé par le centre d'autorisation (code erreur à 001xx), les « xx » représentent le code renvoyé par le centre. Ce code permet de connaître la raison exacte du rejet de la transaction.
  Par exemple, pour une transaction refusée pour raison « provision insuffisante », le code erreur renvoyé sera 00151.
  Tous les codes sont précisés au chapitre *12.3-Codes réponse du centre d'autorisation*.

- Numéro d'autorisation (variable A) : alphanumérique, longueur variable.
  - Pour une transaction de test (pas de demande d'autorisation vers le serveur du Crédit Agricole ou l'établissement financier privatif), la variable vaut toujours « XXXXXX »
  - Pour une transaction refusée, la variable n'est pas envoyée

5.5 Gestion des erreurs

Si une erreur se produit lors de l'appel de l'URL IPN, un mail d'avertissement sera envoyé sur la même adresse que celle utilisée pour les tickets de paiements. Il est donc très important de prendre en compte ces messages de votre côté afin de régler le souci qui empêche la solution e-Transactions de vous envoyer les notifications de paiement.
Sans cela, vous risquez de ne pas mettre à jour correctement le statut de vos commandes suite au paiement en succès ou en erreur.

Par exemple, si l'URL d'appel est :

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

Le message d'erreur reçu sera le suivant :

Objet : WARNING!!
Corps du message : WARNING: Impossible de joindre http://www.commerce.fr pour le paiement ref=abc12&trans=71256&auto=30258&tarif=2000&abonnement=354341& pays=FRA&erreur=000 00 **(XXX-YYY)**

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

- Le premier nombre **XXX** correspond au code retour du protocole http
  - Voir la liste des codes retour HTTP au chapitre *12.4-Codes de retour HTTP*
  - Seuls les codes retour commençant par un 2, sont considérés comme valides.
- Le second **YYY** est un complément d'information correspondant au code retour de la librairie "libcurl" assurant les échanges avec le serveur WEB Marchand.
  - Voir la liste des codes retour CURL au chapitre *12.5-Codes de retour de la librairie cUrl (erreurs des appels IPN)*

6. Authentification des messages reçus

Lorsque vous recevez des appels ou des retours de vos clients vers votre boutique, vous devez vérifier que ces appels ont bien été construits par la solution Up2pay e-Transactions et que les données n'ont pas été altérées.

Vous devez donc impérativement vérifier l'élément suivant :

- **Signature (K)**
  - Vérifier impérativement la signature électronique communiquée dans l'appel à votre page ou à votre URL IPN définie afin de s'assurer que :
    - les données renvoyées n'ont pas été altérées,
    - l'appel vers votre boutique provient de la solution e-Transactions et qu'il vous est bien dédié.

  - **Attention :** pour effectuer cette vérification, vous devez demander la réception de la donnée K (signature) lors de l'appel des pages de paiement pour le recevoir en retour lors du retour de votre client sur les pages de votre boutique ou dans l'appel IPN. La demande de cette donnée doit TOUJOURS être indiqué comme la dernière donnée à recevoir du paramètre PBX_RETOUR envoyé à la page de paiement pour que l'ensemble des données transmises soient inclues dans la signature.
  Par exemple :
    - PBX_RETOUR=montant:M;auto:A;idtrans:S;**sign:K ➔ est correcte**
    - PBX_RETOUR=montant:M;auto:A;**sign:K;**idtrans:S **➔ est incorrecte**

  - La signature est effectuée à partir d'un couple clé privée / clé publique. La solution Up2pay e-Transactions utilise sa clé privée (qu'elle est seule à connaitre) pour signer l'ensemble des données envoyées. Vous pouvez vérifier la signature grâce à la clé publique en libre téléchargement depuis https://www.ca-moncommerce.com/module-etransaction/php/ dans le fichier zip module PHP / Répertoire Exemple.php fichier pubkey.pem . *Pour être en conformité avec les règles de sécurité, le Crédit Agricole est susceptible de changer sa paire de clé publique/privée : il doit donc être possible de mettre en place différentes clés publiques au niveau de vos serveurs.*

6.1 Signature

La signature est produite en chiffrant un condensé SHA-1 avec une clé privée RSA (connue uniquement de la solution Up2pay e-Transactions). La taille d'une empreinte SHA-1 étant de 160 bits et la clé Up2pay e-Transactions faisant 1024 bits de long, la signature est toujours une valeur binaire de taille [fixe] de 128 octets (172 octets en Base64).

6.2 Algorithme de vérification de la signature

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

Il est également possible d'utiliser d'autres langages, packages, composants ou utilitaires, qui peuvent demander de prendre en charge les opérations intermédiaires (condensé ou chiffrement).

Dans tous les cas, il faut utiliser la clé publique Up2pay e-Transactions, disponible en téléchargement (voir ci-dessus)

6.3 Données utilisées pour la signature

Suivant le contexte de l'appel reçu les données utilisées pour signer le message sont différentes :

a) lors de la réponse de serveur à serveur (URL IPN), seules les informations demandées dans la variable PBX_RETOUR sont signées,
b) dans les 4 autres cas (redirection via le navigateur du client, PBX_EFFECTUE, PBX_REFUSE et PBX_ANNULE, PBX_ATTENTE), ce sont toutes les données suivant le ' ? ' (tous les paramètres de l'URL) qui sont utilisés *(y compris ceux que vous auriez pu inclure dans l'URL à utiliser).*

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

(où monparam=mavaleur correspond à une valeur propre à ma boutique indiquée dans l'url de retour et où pbxparam1=val1&pbxparam2=val2 correspondent à des données demandées dans PBX_RETOUR)

La signature (df123dsfd3…1f1ffsre%20t321rt1t3e=) porte sur la partie :

cas a) pbxparam1=E&pbxparam2=J …
cas b) **monparam=mavaleur**&pbxparam1=E&pbxparam2=J ...

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

6.4 Décodage

Les messages et signatures transportés au moyen du protocole HTTP (GET ou POST) doivent être sur-encodés (URL encodage et/ou Base64) pour éviter des altérations de donnée dues au protocole.

De ce fait, il faut procéder aux opérations inverses (décodage) sur la signature avant de vérifier.

Attention :

- Les données sont automatiquement URL décodées dans la plupart des langages web lors de la récupération unitaire de chaque variable reçue en méthode GET ou POST. Il ne faut donc pas décoder une 2ème fois la signature si elle est récupérée de cette manière. Si elle est récupérée dans la chaine représentant tous les paramètres reçus en méthode GET (QUERY_STRING) ou POST (content / body), vous devez la décoder (URL decode) avant de l'utiliser.
- Les autres données du message sont signées une fois encodées URL. Vous ne devez donc pas les décoder pour vérifier la signature mais les utilisées telles que reçues. Vous devez donc les récupérer dans la chaine représentant tous les paramètres reçus en méthode GET (QUERY_STRING) ou POST (content / body) sans modification de votre part avant vérification.

6.5 Vérification de la signature

Pour réaliser la vérification de la signature et suite aux éléments précédemment évoqués, vous devez suivre la procédure suivante :

1) Détachement de la signature de l'ensemble du message reçu et contenant toutes les variables ;
2) Décodage URL de la signature ;
3) Décodage Base64 de la signature ;

4) Vérification de la signature [binaire] sur les autres données (toujours encodées) en utilisant la clé publique de la solution e-Transactions et via un outil de vérification de signature RSA sur clé publique/privée (ex : openssl/verify). Cet algorithme déchiffre la signature et vérifie que le résultat correspond à l'ensemble des données reçues.

Rappel : Avec l'URL IPN de notification (paramètre : PBX_REPONDRE_A), la signature électronique s'effectue uniquement par rapport au contenu de la variable PBX_RETOUR contrairement aux quatre autres URLs (paramètres : PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE et PBX_ATTENTE) où la signature est calculée sur l'ensemble des variables. Dans le premier cas, si vous avez indiqués d'autres paramètres dans l'URL à appeler, vous devez les enlever des données à vérifier avec la signature et la clé publique.

C'est uniquement après avoir vérifié avec succès la signature du message reçu que vous pouvez utiliser les données et effectuer les traitements appropriés.

6.6 Tests

La manière la plus facile et souple de tester un programme de vérification de signature dans votre environnement, est d'utiliser une paire de clé RSA de test que vous pouvez générer directement sur votre serveur.

Vous êtes ainsi en mesure de signer vous-même des messages dont vous pouvez vérifier la signature. Ensuite, il suffit de substituer la clé publique de test par la clé publique Up2pay e-Transactions.

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

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

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

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

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

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

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

Une fois ce 1er test effectué, vous pouvez utiliser OpenSSL pour calculer la signature d'un appel fictif. Vous soumettez ensuite un appel avec cette signature à votre script de vérification de signature tel que le ferait le serveur de la solution Up2pay e-Transactions en utilisant par exemple un navigateur ou un appel serveur (en utilisant cUrl ou wget par exemple).

6.7 Signature non vérifiée

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

- Erreur technique : bogue, environnement cryptographique mal initialisé ou mal configuré, …
- Utilisation d'une clé erronée
- Données altérées ou signature contrefaite.

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

7. Pilotage par API (GAE)

En tant que solution de paiement autonome ou complément de la page de paiement Up2pay e-Transactions par redirection, le pilotage par API (ou **G**estion **A**utomatisée des **E**ncaissements) vous permet une mise en place personnalisée de votre solution de paiement.

Ce modèle d'intégration via des trames questions / réponses, vous offre une flexibilité dans la gestion de vos transactions.

7.1 Fonctionnalités disponibles

L'intégration de la solution Up2pay e-Transactions via API vous permet d'effectuer de nombreuses opérations directement à partir de votre boutique :

Réaliser des demandes d'autorisations de paiement sur une carte bancaire afin d'obtenir une autorisation permettant de réaliser un débit ultérieur (garanti jusqu'à J+6), de vérifier la validité d'une carte et/ou d'enregistrer celle-ci via notre protocole de tokenisation.

Exemples : *prise d'empreintes, 1-clic (tokenisation) …*

Capturer une transaction afin de débiter votre client de manière immédiate ou différée / totale ou partielle.

Exemples : *paiement différé, paiement à l'expédition, gestion de stock en flux tendu …*

Effectuer des opérations de caisse afin d'agir sur l'état d'une transaction, par le biais d'une consultation, d'un remboursement ou d'une annulation.

Obtenir des informations sur les marques associées aux cartes bancaires de vos clients ainsi que leur type.

Gérer les abonnés correspondant aux cartes enregistrées dans la solution (via la Tokenisation) : inscription, réutilisation, modification, suppression.

7.1.1 Utilisation du champ TYPE

Le champ « TYPE » envoyée dans la trame-question permet de définir l'opération à réaliser. C'est le champ qui structure chaque trame-question envoyée à l'API.

En fonction de l'opération choisie, des données sont à envoyer obligatoirement et un retour spécifique est renvoyé par la solution Up2pay e-Transactions après exécution de l'opération et en fonction des contraintes et du contexte de celle-ci.

Vous trouverez ci-dessous les différentes valorisations du champ TYPE en cohérence avec les fonctionnalités précédemment citées :

CODE	DESCRIPTION
00001	Autorisation seule
00002	Capture (confirmation du débit pour remise en banque)
00003	Autorisation + Capture
00005	Annulation d'une opération
00011	Vérification de l'existence d'une transaction
00013	Modification du montant d'une transaction
00014	Remboursement sur une précédente transaction
00017	Consultation d'une transaction
00018	Demande des marques associées à la carte du client (MIF)
00051	Autorisation seule sur un abonné
00052	Capture (confirmation de débit) sur un abonné
00053	Autorisation + Capture sur un abonné
00055	Annulation d'une opération sur un abonné
00056	Inscription d'un nouvel abonné
00057	Modification d'un abonné existant
00058	Suppression d'un abonné

Tableau 3 : TYPE d'opérations par API

7.1.2 Cas d'usage

Vous trouverez ci-dessous une liste non-exhaustive de cas d'usage que vous pouvez mettre en place en utilisant l'intégration direct des API dans votre boutique.

Autorisation Seule
Objectifs : vérification de la validité d'une carte bancaire, réalisation d'une autorisation de paiement en vue d'une capture ultérieure …
L'autorisation seule de TYPE 00001 ou 00051 vous permet de déclencher la première phase du processus de paiement. Celle-ci vous permet une potentielle capture ultérieure.

Capture d'une transaction
Objectifs : réalisation d'un débit différé (paiement à l'expédition), débit total ou partiel (gestion de stock / vente au poids) …
La capture de TYPE 00002 ou 00052 vous permet de déclencher la seconde phase du processus de paiement. Celle-ci consiste à capturer une autorisation déjà réalisée par le passé. La capture peut être effectuée aussi bien sur une transaction réalisée via les pages de paiement hébergées sur la solution e-Transactions (en redireciton ou en iFrame) que sur une transaction réalisée à l'aide de l'API en Autorisation seule (cas d'usage ci-dessus).
Veuillez cependant respecter un délai maximum de 6 jours entre l'autorisation et la capture, si vous souhaitez conserver les garanties d'autorisation et du 3D Secure.

Autorisation + Capture

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 :

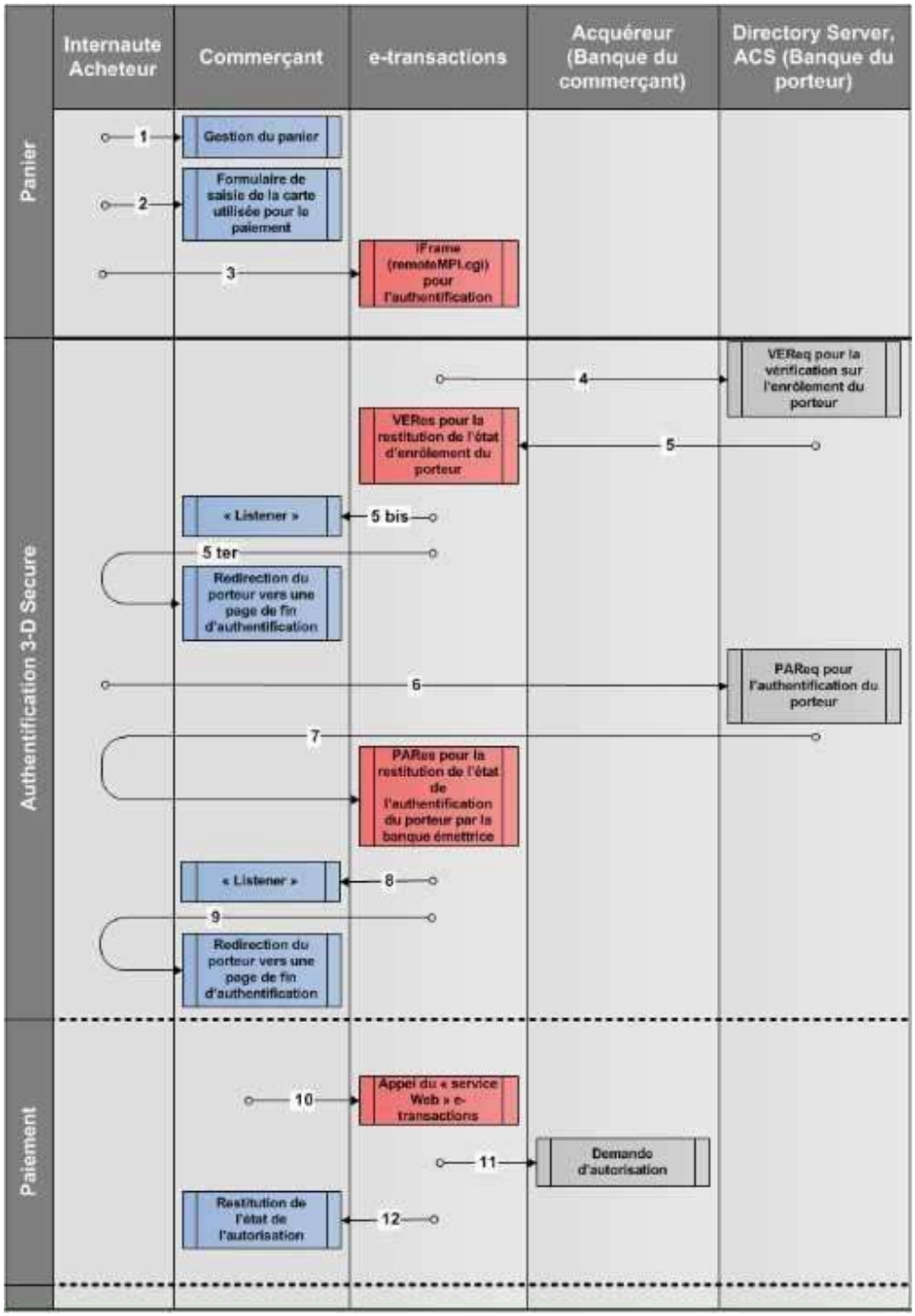


Figure 17 : Etapes d'authentification par RemoteMPI

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-Authentification3D-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-Authentification3D-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
0606f78a827d9626514274760611 7a7983e758620e49e06801e3793c049475ef9a03878c0ffd7c6
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%2B4nIvYQQF4Nk8QxJhMd0CCo7CBh8KwgcHXHxRAVmZL5GhRzEx
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=12345678&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 :

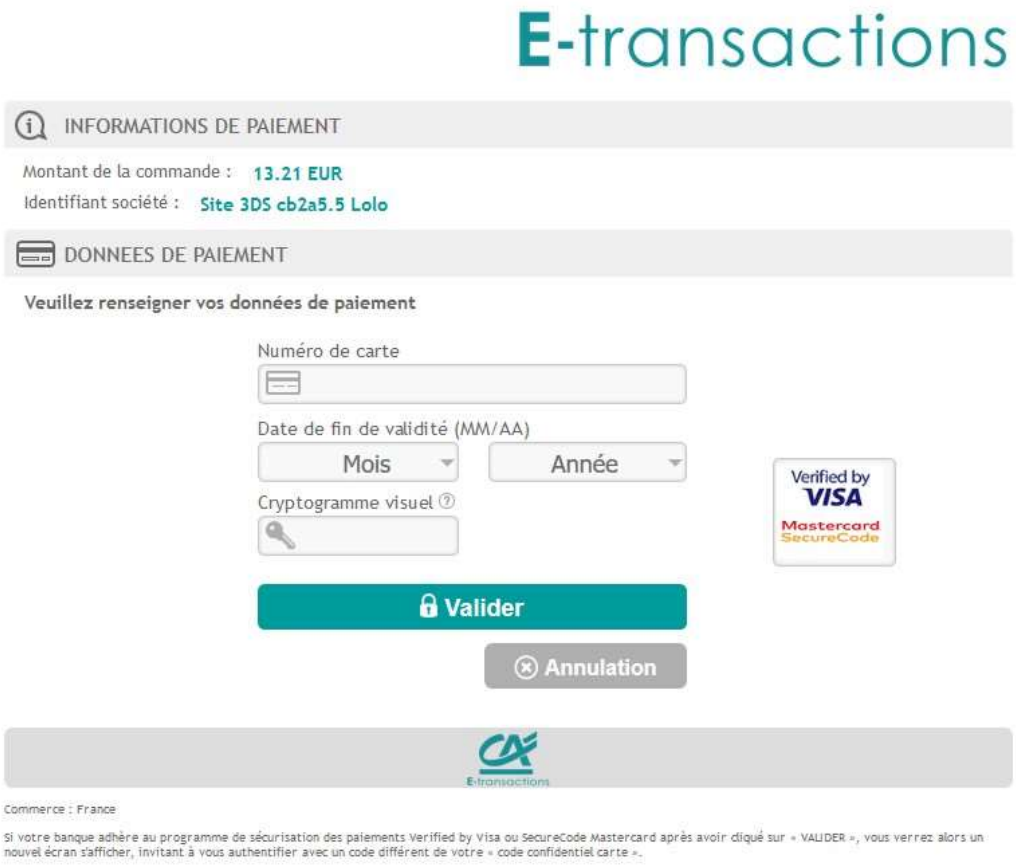


Figure 19 : Page de paiement en responsive

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).

Exemple : PBX_SOURCE=RWD

11.1.2.21 PBX_TOKEN

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

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

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

Exemple : PBX_TOKEN=NODMIOOCUB1N0BETO0TA

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

11.1.2.22 PBX_TYPEPAIEMENT

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

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

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

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

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

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

11.1.2.23 PBX_TYPECARTE

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

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

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

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

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

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

Tableau 17 : Valeurs possibles PBX_TYPEPAIMENT et PBX_TYPECARTE

11.1.2.24 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3

Format : 3 à 10 chiffres

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

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

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

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

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

11.1.3 Variables spécifiques à certains moyens de paiement

11.1.3.1 PBX_1EURO_CODEEXTERNE

Format : 3 chiffres.

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

Offre promotionnelle externe fournie par la solution 1Euro.com

Exemple : PBX_1EURO_CODEEXTERNE=111

11.1.3.2 PBX_1EURO_DATA

Format : jusqu'à 100 caractères.

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

Données d'identification et de localisation de votre client.

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

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

Tableau 18 : Données PBX_1EURO_DATA

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

11.1.3.3 PBX_CK_ONLY

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

Uniquement utilisée pour les paiements avec des cartes cadeau

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

Exemple : PBX_CK_ONLY=O

11.1.3.4 PBX_NBCARTESKDO

Format : jusqu'à 2 chiffres.

Uniquement utilisée pour les paiements avec Cartes Cadeau.

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

Exemple : PBX_NBCARTESKDO=3

11.1.3.5 PBX_OPECOM

Format : 10 caractères.

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

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

Exemple : PBX_OPECOM=3453234786

11.1.3.6 PBX_ONEY_DATA

Format : XML.

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

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

11.1.3.7 PBX_PAYPAL_DATA

Format : jusqu'à 490 caractères.

Uniquement utilisée pour le moyen de paiement PAYPAL.

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

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

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

Tableau 19 : Données PBX_PAYPAL_DATA

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

11.2 Authentification par API (RemoteMPI)

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

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

IdMerchant	X		Identifiant commerçant fourni par la solution Up2pay e-Transactions
IdSession	X	X	Identifiant de session unique
LastName	X		Nom de votre client
TotalQuantity	X		Nombre d'articles composant la commande
TypeCarte	X		Type de carte choisi par votre client
URLHttpDirect	X		URL de retour serveur à serveur
URLRetour	X		URL de retour depuis le navigateur du client
ZipCode	X		Code postal de l'adresse de facturation de votre client
3DCAVV		X	Valeur reçue des ACS
3DCAVVALGO		X	Identifiant de l'algorithme ayant servi à l'identification du porteur sur l'ACS
3DECI		X	Indicateur E-Commerce (E-Commerce Indicator)
3DENROLLED		X	Etat de l'enrôlement du porteur
3DERROR		X	Erreur renvoyée par le MPI
3DSIGNVAL		X	Statut de la vérification de la signature du porteur
3DSTATUS		X	Statut de la demande d'authentification
3DXID		X	Référence provenant du MPI
Check		X	Signature Up2pay e-Transactions
ID3D		X	Identifiant de contexte e-Transactions
StatusPBX		X	Statut de la demande d'authentification

Tableau 20 : Liste des variables RemoteMPI

11.2.1 Variables d'appel e-Transactions RemoteMPI

11.2.1.1 Address1

Format : 50 caractères. **Obligatoire.**

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

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

Exemple : Address1=12 rue Test

11.2.1.2 Address2

Format : 50 caractères. **Facultatif.**

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

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

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

Exemple : Address2=lieu dit Le Village

11.2.1.3 Amount

Format : Numérique. **Obligatoire.**

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

Vous devez obligatoirement définir le même montant pour la demande d'authentification RemoteMPI et pour la demande d'autorisation de paiement par **API** (Gestion Automatisée des Encaissements) avec la **variable MONTANT**.

Exemple : pour 19€90 : Amount=0000001990

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

11.2.1.4 CCExpDate

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

Date de fin de validité de la carte.

Exemple : CCExpDate=1223 pour décembre 2023

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

11.2.1.5 CCNumber

Format : 19 caractères. **Obligatoire.**

Numéro de carte du porteur (client) sans espace.

Exemple : CCNumber=1111222233334444

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

11.2.1.6 City

Format : 50 caractères. **Obligatoire.**

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

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

Exemple : City=Paris

11.2.1.7 CountryCode

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

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

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

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

Exemple : CountryCode=250 (pour la France)

11.2.1.8 Currency

Format : 3 chiffres. **Obligatoire.**

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

Exemples : Currency=978

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

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

11.2.1.9 CVVCode

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

Cryptogramme visuel situé au dos de la carte bancaire.

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

Exemple : CVVCode=123

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

11.2.1.10 EmailPorteur

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

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

Exemple : EmailPorteur=test@client.com

11.2.1.11 FirstName

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

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

Exemple : FirstName=Jean

11.2.1.12 IdMerchant

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

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

Exemple : IdMerchant=2

11.2.1.13 IdSession

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

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

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

11.2.1.14 LasttName

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

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

Exemple : LastName=Dupont

11.2.1.15 TotalQuantity

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

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

Exemple : TotalQuantiy=9

11.2.1.16 TypeCarte

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

Type de la carte choisie par votre client.

Les valeurs possibles sont :

CB	ELECTRON
VISA	MAESTRO
MASTERCARD	VPAY

Exemple : TypeCarte=CB

11.2.1.17 URLHttpDirect

Format : jusqu'à 250 caractères.

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

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

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

11.2.1.18 URLRetour

Format : jusqu'à 250 caractères.

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

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

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

11.2.1.19 ZipCode

Format : 16 caractères. **Obligatoire.**

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

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

Exemple : ZipCode=75001

11.2.2 Variables réponses e-Transactions RemoteMPI

11.2.2.1 IdSession

Format : jusqu'à 250 caractères.

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

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

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

11.2.2.2 StatusPBX

Format : Alphanumérique.

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

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

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

Tableau 21 : Valeurs possibles pour StatusPBX

Exemple : StatutPBX=Autorisation%20à%20faire

11.2.2.3 ID3D

Format : jusqu'à 20 chiffres.

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

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

Exemple : ID3D=9900000000012

11.2.2.4 Check

Format : jusqu'à 256 caractères.

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

Exemple : Check=nLpPFrgGHqSbVW%2F5iHbxoBdRiYPzNIrXtBBZVUCWhfdAx3SH4DLUXnCylZPri%2BUHxpV9Lkl92n%2FwPp24wwtJ0sGv6wRBs%2Fiz9HSu3AifDl%2BQMD1ywK65kQNZOif6%2BNMetiscQwl80%2Bl6sgTOnAOJECEGlt1oDbxQ0mf%2Bs7UdUPE%3D

Voir aussi : *6-Authentification des messages reçus p*our le mécanisme de vérification des signatures en provenance de la plateforme Up2pay e-Transactions.

11.2.2.5 3DCAVV

Format : 28 caractères.

Valeur reçue des ACS. URL-encodé.

11.2.2.6 3DCAVVALGO

Format : jusqu'à 64 caractères

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

Exemple : 3DCAVVALGO=0000000001

11.2.2.7 3DECI

Format : 2 chiffres

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

Exemple : 3DECI=02

11.2.2.8 3DENROLLED

Format : 1 caractère

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

Valeurs possibles :

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

Exemple : 3DENROLLED=Y

11.2.2.9 3DERROR

Format : jusqu'à 6 caractères

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

Exemple : 3DERROR=100

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

11.2.2.10 3DSIGNVAL

Format : 1 caractère. « Y » ou « N »

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

Exemple : 3DSIGNVAL=Y

11.2.2.11 3DSTATUS

Format : 1 caractère.

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

Exemple : 3DSTATUS=Y

Valeurs possibles :

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

11.2.2.12 3DXID

Format : jusqu'à 28 caractères

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

Exemple : 3DXID=z9UKb06xLziZMOXBEmWSVA1kwG0%3D

11.3 Intégration avec les API (GAE)

11.3.1 Variables d'appel aux API

11.3.1.1 SITE

Format : 7 chiffres. **Obligatoire.**

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

Exemple : SITE=1999888

11.3.1.2 RANG

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

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

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

Exemple : RANG=001

11.3.1.3 VERSION

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

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

Exemple : VERSION=00104

11.3.1.4 TYPE

Format : 5 chiffres. **Obligatoire.**

Opération à réaliser.

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

Attention : Dans le cas d'un appel pour réaliser une capture (TYPE=00002) qui suit une demande d'autorisation seule, il est conseillé :
- D'attendre quelques instants (quelques secondes) entre la demande d'autorisation seule et la capture ;

D'envoyer la capture sur la même plateforme (ppps ou ppps1) que la demande d'autorisation seule afin d'éviter d'éventuels problèmes de réplication entre les plateformes.

Les valeurs possibles des opérations à réaliser sont les suivantes :

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

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

Tableau 22 : Liste des TYPE d'opération par API

Exemple : TYPE=00002

11.3.1.5 DATEQ

Format : 14 chiffres. **Obligatoire.**

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

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

11.3.1.6 NUMQUESTION

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

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

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

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

11.3.1.7 HASH

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

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

Cet algorithme doit être choisi parmi la liste suivante (valeurs identiques à la liste ci-dessous - sensible à la Casse/majuscules) :

SHA512	SHA256
RIPEMD160	SHA384
SHA224	MDC2

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

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

Exemple : HASH=SHA512

11.3.1.8 HMAC

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

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

Exemple :
HMAC=AD4D2A87FB9C4FA7AD8AA122E9F417B568D5E2B8CA4AF9410B00B9CFCFDB9142F721CBD0B90F518A16A49F9A7BD248A86EFEA25831654395E1DED1BEA650361C

Voir aussi : *5.3-Authentification des messages*

11.3.1.9 MONTANT

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

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

Exemple : pour 19€90 : MONTANT=0000001990

11.3.1.10 DEVISE

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

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

Exemple :

- Euro : DEVISE=978

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

11.3.1.11 REFERENCE

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

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

Exemple : CMD9542124-01A5G

11.3.1.12 REFABONNE

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

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

Exemple : REFABONNE=Client_005287_Mdp_0001 ou REFABONNE=HcsqXh5YHkCb

11.3.1.13 PORTEUR

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

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

Exemple : PORTEUR=1111222233334444

11.3.1.14 DATEVAL

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

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

Exemple : DATEVAL=1213 (pour décembre 2013)

11.3.1.15 CVV

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

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

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

Exemple : CVV=123

11.3.1.16 ACTIVITE

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

Environnement Réglementaire et Technique (ERT).

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

Voici les valeurs possibles pour l'ERT :

CODE	DESCRIPTION
024	Demande par internet
027	Paiement récurrent

Exemple : ACTIVITE=024

11.3.1.17 ARCHIVAGE

Format : jusqu'à 12 caractères alphanumériques

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

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

Exemple : ARCHIVAGE=ID0001452158

11.3.1.18 DIFFERE

Format : 3 chiffres
Valeur maximum : 075 jours

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

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

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

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

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

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

11.3.1.19 NUMAPPEL

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

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

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

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

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

Exemple : NUMAPPEL=1234567890

11.3.1.20 NUMTRANS

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

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

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

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

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

Exemple : NUMTRANS=1234567890

11.3.1.21 AUTORISATION

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

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

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

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

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

Exemple : AUTORISATION=168753

11.3.1.22 PAYS

Format : <vide>.

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

Exemple : PAYS=

11.3.1.23 ACQUEREUR

Format : jusqu'à 16 caractères.

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

Les valeurs possibles sont :

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

Tableau 23 : Liste des valeurs de la variable ACQUEREUR

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

Exemple : ACQUEREUR=PAYPAL

11.3.1.24 TYPECARTE

Format : 2 à 30 caractères.

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

Les valeurs possibles sont :

CB	ELECTRON
VISA	MAESTRO
MASTERCARD	VPAY

Tableau 24 : Liste des valeurs pour la variable TYPECARTE

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

Exemple : TYPECARTE=VISA

11.3.1.25 SHA-1

Format : <vide>

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

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

Exemple : SHA-1=

11.3.1.26 ERRORCODETEST

Format : 5 chiffres.

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

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

Exemple : ERRORCODETEST=00157

Voir aussi : *12.2-Codes réponse des APIs*

11.3.1.27 ID3D

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

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

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

Exemple : ID3D=9900000000012

11.3.1.28 SELECTION

Format : 2 chiffres.

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

Les valeurs possibles sont :

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

Exemple : SELECTION=01

11.3.1.29 EMAILPORTEUR

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

Adresse email de votre client ayant réalisé le paiement.

Exemple : EMAILPORTEUR=test@ca-ps.com

11.3.2 Variables réponse des API

11.3.2.1 SITE

Format : 7 chiffres.

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

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

Exemple : SITE=1999888

11.3.2.2 RANG

Format : 2 chiffres ou 3 chiffres.

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

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

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

Exemple : RANG=001

11.3.2.3 NUMQUESTION

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

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

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

Exemple : 0145829183

11.3.2.4 NUMAPPEL

Format : 10 chiffres.

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

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

Exemple : NUMAPPEL=0000782653

11.3.2.5 NUMTRANS

Format : 10 chiffres.

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

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

Exemple : NUMTRANS=1234567890

11.3.2.6 AUTORISATION

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

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

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

Exemple : AUTORISATION=168753

11.3.2.7 CODEREPONSE

Format : 5 chiffres

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

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

Exemple : CODEREPONSE=00007 (date invalide)

11.3.2.8 REFABONNE

Format : jusqu'à 250 caractères

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

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

Exemple : REFABONNE=Client_005287_Mdp_0001 ou REFABONNE=HcsqXh5YHkCb

11.3.2.9 PORTEUR

Format : jusqu'à 19 caractères

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

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

Exemple : TOKEN=NODMIOOCUB1N0BETO0TA

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

11.3.2.10 COMMENTAIRE

Format : jusqu'à 100 caractères

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

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

11.3.2.11 PAYS

Format : 3 caractères (code ISO-3166 alphabétique)

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

Exemple : PAYS=FRA

11.3.2.12 TYPECARTE

Format : jusqu'à 10 caractères

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

Les valeurs possibles sont :

CB	ELECTRON
VISA	MAESTRO
MASTERCARD	VPAY

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

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

Exemple : TYPECARTE=VISA

11.3.2.13 SHA-1

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

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

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

Exemple : SHA-1= F8BF2903A1149E682BE599C5C20788788256AA46

11.3.2.14 STATUS

Format : jusqu'à 32 caractères

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

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

Les valeurs possibles sont :

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

Exemple : STATUS=Capturé

11.3.2.15 REMISE

Format : jusqu'à 9 chiffres.

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

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

Exemple : REMISE= 509625890

11.3.2.16 MARQUE

Format : 1 caractère.

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

Les valeurs suivantes peuvent être retournées :

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

Exemple : MARQUE=A

11.3.2.17 PRODUIT

Format : 1 caractère.

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

Les valeurs suivantes peuvent être retournées :

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

** : Ces 2 catégories de carte ne seront plus gérées dans une prochaine version de protocole*

Exemple : PRODUIT=C

11.3.2.18 LONGUEUR

Format : 2 chiffres.

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

Les valeurs suivantes peuvent être retournées :

Code	Commentaire
10	N° porteur sur 10 positions
11	N° porteur sur 11 positions
12	N° porteur sur 12 positions
13	N° porteur sur 13 positions

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

Exemple : LONGUEUR=16

12. Codes retours

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

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

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

12.2 Codes réponse des APIs

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue.
001xx	Paiement refusé par le centre d'autorisation. [voir *12.3-Codes réponse du centre d'autorisation*]. En cas d'autorisation de la transaction par le centre d'autorisation de la banque, le résultat "00100" sera en fait remplacé directement par "00000".

00201	Le paiement est réalisé sans authentification 3D-Secure qui est requise par le centre d'autorisation de votre client. Vous devez réaliser une demande d'authentification avec le composant RemoteMPI. [voir *7.4.2-Authentification 3D-Secure*]
00002	Une erreur de cohérence est survenue.
00003	Erreur Plateforme.
00004	Numéro de porteur invalide.
00005	Numéro de question invalide.
00006	Accès refusé ou site / rang incorrect.
00007	Date invalide.
00008	Date de fin de validité incorrecte.
00009	Type d'opération invalide.
00010	Devise inconnue.
00011	Montant incorrect.
00012	Référence commande invalide.
00013	Cette version n'est plus soutenue.
00014	Trame reçue incohérente.
00015	Erreur d'accès aux données précédemment référencées.
00016	Abonné déjà existant (inscription nouvel abonné).
00017	Abonné inexistant.
00018	Transaction non trouvée (question du type 11).
00019	Réservé.
00020	Cryptogramme visuel non présent.
00021	Carte non autorisée.
00022	Plafond atteint
00023	Porteur déjà passé aujourd'hui
00024	Code pays filtré pour ce commerçant
00037	HMAC invalide
00097	Timeout de connexion atteint.
00098	Erreur de connexion interne.
00099	Incohérence entre la question et la réponse. Refaire une nouvelle tentative ultérieurement.

Tableau 26 : Codes réponse des APIs

12.3 Codes réponse du centre d'autorisation

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

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

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

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

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

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

Tableau 27 : Codes réponses du centre d'auto CB

12.4 Codes de retour HTTP

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

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

Tableau 28 : Codes retour HTTP

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

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

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

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

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

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

Tableau 29 : Codes erreur CURL

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

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

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

CODE	SIGNIFICATION
1	Erreur accès au fichier de configuration (interne e-Transactions)
2	Erreur accès aux paramètres de connexions à la base de données
3	Erreur de récupération des variables d'environnement locales
4	Erreur de récupération du chemin d'accès au MPI(MPI_PATH)
5	Erreur de connexion à la base de données
6	Erreur de préparation de la recherche du site (fsite)
7	Erreur de préparation de la recherche des transactions MPI (TransMPI)
101	Erreur absence montant (Amount)
102	Erreur absence date expiration (CCExpdate)
103	Erreur absence numéro de porteur (CCNumber)
104	Erreur absence devise (Currency)
105	Erreur absence identifiant marchand (IdMerchant)
106	Erreur absence identifiant session marchand (IdSession)
107	Erreur absence référence marchand (RefMarchant)
108	Erreur absence identifiant transMPI

110	Erreur taille numéro de porteur
111	Erreur type numéro de porteur
112	Erreur type montant
113	Erreur taille référence marchand
114	Erreur taille date expiration
115	Erreur type date expiration
116	Erreur valeur date expiration
117	Erreur longueur CVV (optionnel)
118	Erreur longueur identifiant TransMPI retourné par MPI
201	Erreur de recherche du site
202	Erreur de recherche dans TransMPI
301	Erreur ajout enregistrement TransMPI
401	Erreur de taille de la référence marchand reçue duMPI
402	Erreur de taille du code erreur du MPI
403	Erreur de taille du XID reçu du MP
410	Erreur absence de la référence marchand reçue du MPI
411	Erreur de type de la référence marchand
412	Erreur de type du code erreur

Tableau 30 : Codes réponses du programme RemoteMPI

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

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

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

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

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

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

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

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

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

13. Jeu de caractères

Le jeu de caractères supporté par les applications est présenté dans le tableau ci-dessous (sur base du code hexadécimal – ligne/colonne – de chaque caractère accepté). Tous les autres caractères autres que ceux présents dans le tableau ci-dessous seront, suivant les applications, supprimés ou la trame rejetée :

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

14. Caractères URL Encodés

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

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

15. Exemples de codes

15.1 Exemple d'appel de l'API en PHP avec la lib Curl

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

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

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

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

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

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

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

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

'DATEQ'       => '15102013'
);

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

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

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

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

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

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

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

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

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

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


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

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

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

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

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

16. Glossaire

16.1 Autorisation (Auto)

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

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

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

16.2 Capture

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

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

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

16.3 3D-Secure / American Express Safekey

La plupart des sites de commerce électronique, qui proposent de faire du paiement en ligne, utilisent les protocoles TLS pour chiffrer les informations sensibles telles que le numéro de carte bancaire. Ces protocoles ont été conçus pour assurer la confidentialité des informations échangées entre deux entités mais ne permettent pas l'authentification d'un client avec sa banque comme requis pour des paiements sécurisés et garantis.

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

3D-Secure / American Express Safekey permet :

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

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

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

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

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

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

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

- ***Porteur authentifié*** *:* Indique si la carte de l'acheteur est enrôlée à 3D-Secure / American Express Safekey et s'il a réussi à s'authentifier
  - **Y** : L'authentification s'est déroulée avec **succès**
  - **N** : Le porteur n'est **pas parvenu à s'authentifier**, la transaction est interdite
  - **U** : L'authentification n'a pu être finalisée suite à un **problème technique**
  - **A** : L'authentification **n'était pas disponible**, mais une preuve de tentative d'authentification a été générée

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

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

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

Attention : Les échéances postérieures au 1er paiement lors d'un paiement en plusieurs fois ou d'un abonnement ne sont pas garanties car elles ne sont pas réalisées par votre client en mode 3D-Secure mais générées automatiquement.

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

16.4 Encodage URL (url-encodé)

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

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

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

16.5 FTP

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

16.6 HMAC

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

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

16.7 HTTP

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

16.8 IP (adresse IP)

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

16.9 TLS

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

16.10 URL

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

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

16.11 Fichiers CSS

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

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

16.12 MPADS

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

16.13 MIF

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

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