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 Gestion Automatisée des Encaissements (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 Gestion Automatisée des Encaissements (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 Gestion Automatisée des Encaissements (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.

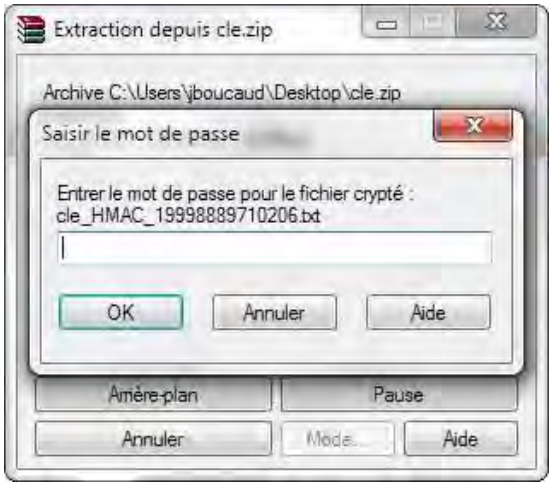
Si ce tiers doit récupérer la clé HMAC, vous devez générer la clé sur le Back Office Vision et lui transmettre via email (Voir procédure ci-dessous) ou autre échange sécurisé.

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 vou**s 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 (Gestion Automatisée des Encaissements):

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 :

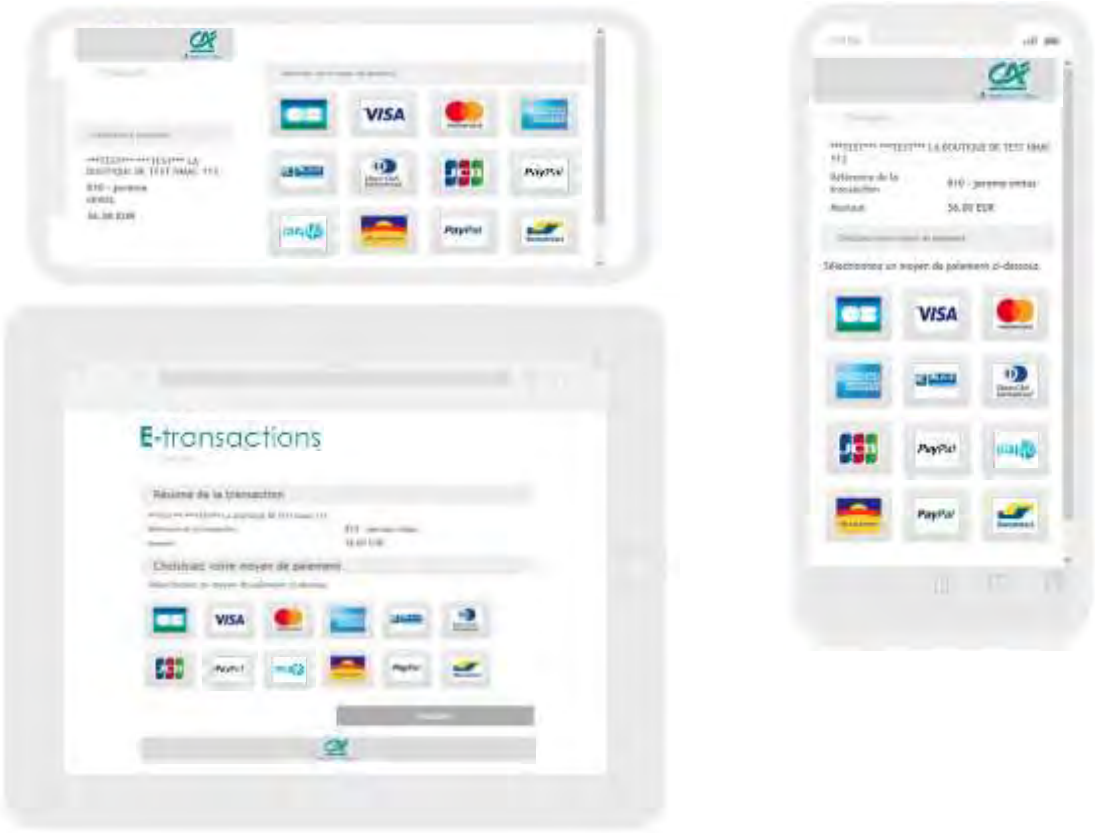


Figure 13 : Page de choix des Moyens de paiement sur différents médias

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

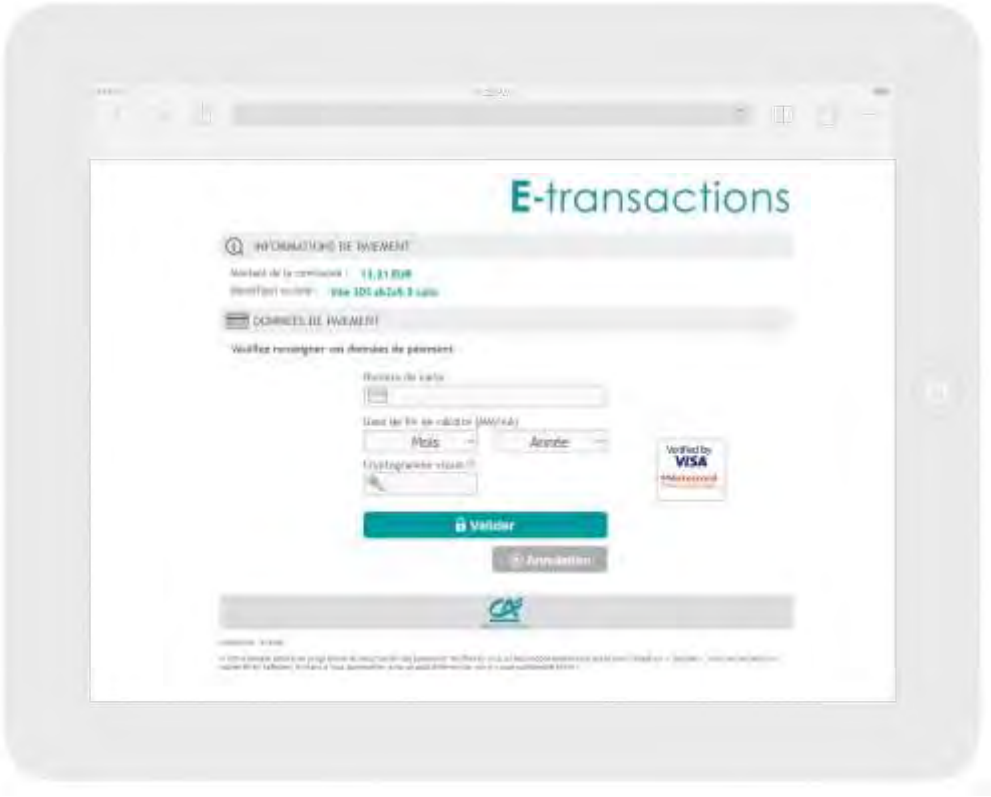


Figure 16 : Vue sur Tablette - Position horizontale

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=10 00&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

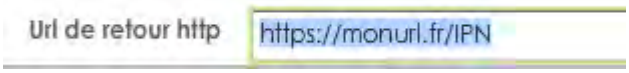
Cette variable IPN est spécialement utilisée pour gérer de façon automatique la validation des bons de commandes. Cette variable doit être utilisée pour valider vos bons de commandes car elle a l'avantage d'être appelée de serveur à serveur dès que le client valide son paiement (que ce dernier soit autorisé 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