

Paybox



PAYBOX SYSTEM

MANUEL D'INTEGRATION

VERSION 6.2
05/06/2014



HISTORIQUE DES MODIFICATIONS

DATE	VERSION	DESCRIPTION	AUTEUR
18/04/2011	5.00	Version initiale après refonte. Document dédié Paybox System	Service Projets
27/05/2011	5.01	Version DRAFT	Service Projets
10/06/2011	5.02	Version après prise en compte des remarques de la réunion du 10/06/2011	Service Projets
02/12/2011	5.03	Modifications des URL d'appel Précisions sur la gestion de la signature	Service Projets
13/04/2012	5.05b	Mise à jour des moyens de paiement Gestion des abonnements	Service Projets
19/04/2012	5.06	Intégration MAXICHEQUE Révision HMAC	Service Projets
04/06/2012	5.08	Complément d'informations sur le HMAC	Service Projets
02/09/2013	6.00	Intégration BCMC, Nouvelles variables PBX_ATTENTE, PBX_NBCARTESKDO, PBX_CK_ONLY, PBX_GROUPE Personnalisation page de choix.	Service Projets
27/11/2013	6.1		Service Projets
05/06/2014	6.2	Changement de charte graphique	Service Projets





REFERENCES DOCUMENTATIONS

La plupart des documentations référencées ci-dessous sont téléchargeables sur le site Web Paybox www.paybox.com :

REF.	DOCUMENT	DESCRIPTION
Ref 1	ManuelIntegrationPayboxDirect_V6.2_FR.pdf	Manuel d'intégration de la solution Paybox Direct / Direct+
Ref 2	ParametresTestPaybox_V6.1_FR.pdf	Manuel décrivant les environnements et paramètres de test (pré-production).
Ref 3	GUIDE_UTILISATEUR_BACK_OFFICE_COMMERCE_PAYBOX.doc	Manuel Utilisateur du Back Office Commerçant
Ref 4	PAYBOX Fiche présentation 3D Secure.pdf	Fiche de présentation 3-D Secure : intérêt pour le commerçant et liste de questions/réponses
Ref 5	Paybox manuel en français V4_84.pdf	Manuel Intégrateur pour le mode historique d'intégration de Paybox par module CGI.
Ref 6	Paybox System - Personnalisation de la page et ticket de paiement.pdf	Manuel Intégrateur pour personnaliser la page de paiement aux couleurs de votre commerce
Ref 7	Note Paypal	Note d'intégration pour Paypal
Ref 8	Note Kwixo	Note d'intégration pour Kwixo
Ref 9	Note Oney	Note d'intégration pour Oney - Facilipay



AVERTISSEMENT



Ce document est la propriété exclusive de Paybox/Point Transaction Systems. Toute reproduction intégrale ou partielle, toute utilisation par des tiers, ou toute communication à des tiers est interdite sans accord préalable de Paybox/Point Transaction Systems.

Si vous découvrez une erreur dans cette documentation, vous pouvez nous envoyer un email aux adresses mail ci-dessous en décrivant l'erreur ou le problème aussi précisément que possible. Merci de préciser la référence du document, et le numéro de page.

INFORMATION

Pour tout renseignement nos Equipes restent à disposition des commerçants et Intégrateurs, du lundi au vendredi de 9H à 18H :

Service Commercial :

E-mail : contact@paybox.com

Téléphone : + 33 (0)1 61 37 05 70

ASSISTANCE

Pour tout renseignement ou assistance à l'installation et à l'utilisation de nos produits, nos Equipes restent à disposition des commerçants et Intégrateurs, du lundi au vendredi de 9H à 12H30 et 14H à 18H30 (17H30 le vendredi) :

Support Technique & Fonctionnel :

E-mail : support@paybox.com

Téléphone : + 33 (0)4 68 85 79 90

Pour tout contact auprès de nos services, il faut IMPERATIVEMENT communiquer les identifiants Paybox :

- numéro de SITE (7 chiffres)
- numéro de RANG (2 chiffres)
- numéro d'identifiant Paybox (1 à 9 chiffres)



TABLE DES MATIERES



1. INTRODUCTION	- 7 -
2. OBJET DU DOCUMENT	- 8 -
3. PRESENTATION DU PRODUIT « PAYBOX SYSTEM »	- 9 -
3.1 PRINCIPE GENERAL DE FONCTIONNEMENT	- 9 -
3.2 LISTE DES MOYENS DE PAIEMENT	- 10 -
3.3 SECURITE	- 11 -
3.4 PRESENTATION DES PAGES PAYBOX SYSTEM	- 11 -
4. APPEL DE LA PAGE DE PAIEMENT	- 15 -
4.1 PREPARATION DU MESSAGE	- 15 -
4.2 FORÇAGE DU TYPE ET MOYEN DE PAIEMENT	- 16 -
4.3 AUTHENTIFICATION DU MESSAGE PAR EMPREINTE	- 16 -
4.4 URL APPELEE	- 19 -
5. GESTION DE LA REPONSE	- 20 -
5.1 REDIRECTION DU CLIENT	- 20 -
5.2 GESTION DES PAIEMENTS EN ATTENTE DE VALIDATION	- 21 -
5.3 VALIDATION DES BONS DE COMMANDE	- 21 -
6. FONCTIONNALITES AVANCEES	- 26 -
6.1 INTEGRATION AVEC PAYBOX DIRECT PLUS	- 26 -
6.2 AUTORISATION SANS CAPTURE	- 27 -
6.3 PAIEMENT DIFFERE	- 28 -
6.4 PAIEMENT SUR MOBILE	- 29 -
7. OPTION GESTION DES ABONNEMENTS	- 30 -
7.1 PRINCIPE	- 30 -
7.2 CREATION D'UN ABONNEMENT	- 31 -
7.3 PAIEMENT EN PLUSIEURS FOIS (4 FOIS MAX)	- 32 -
7.4 FIN DES ABONNEMENTS	- 33 -
8. LE BACK-OFFICE COMMERÇANT	- 34 -
8.1 ACCES ET FONCTIONNALITES	- 34 -
8.2 GESTION DE LA CLE D'AUTHENTIFICATION	- 34 -
9. SUPPORT – ASSISTANCE - CONTACT	- 37 -
9.1 ACCES	- 37 -
9.2 FONCTIONS	- 37 -
9.3 PROCEDURE D'INSCRIPTION	- 38 -
10. ENVIRONNEMENT DE TESTS	- 39 -
11. DICTIONNAIRE DE DONNEES	- 40 -
11.1 CHAMPS OBLIGATOIRES POUR PAYBOX SYSTEM	- 41 -
11.2 CHAMPS OPTIONNELS POUR PAYBOX SYSTEM	- 46 -
11.3 VARIABLES SPECIFIQUES A CERTAINS MOYENS DE PAIEMENT	- 53 -

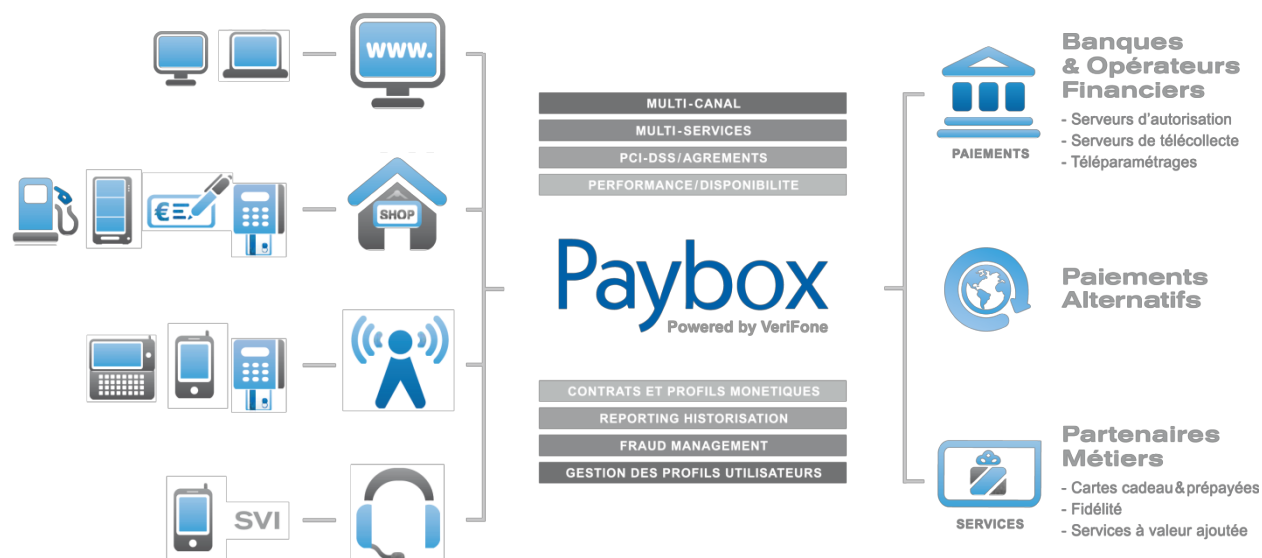


11.4	PAYBOX SYSTEM RESILIATION DES ABONNEMENTS : REQUETE	- 56 -
11.5	PAYBOX SYSTEM RESILIATION DES ABONNEMENTS : REPONSE	- 57 -
12.	ANNEXES	- 58 -
12.1	CODES REPONSES DU CENTRE D'AUTORISATION	- 58 -
12.2	CODES RETOUR HTTP	- 61 -
12.3	CODES ERREUR CURL	- 62 -
12.4	JEU DE CARACTERES PAYBOX	- 63 -
12.5	CARACTERES URL ENCODES	- 63 -
12.6	URL D'APPEL ET ADRESSES IP	- 64 -
12.7	GLOSSAIRE	- 65 -



1. INTRODUCTION

Paybox/Point Transaction Systems a développé et exploite sa propre plateforme pour assurer l'interface entre différentes sources de paiements et de services (moyen d'acquisition) et les destinations (opérateurs financiers, bancaires, partenaires métiers).



Il s'agit d'une plateforme multi-canal et multi-services :

- **Multi-canal** : la plateforme Paybox accepte différents systèmes d'accès autant physiques (paiement de proximité) que distants (VAD, E-Commerce) :
 - Site web marchand
 - Terminal de Paiement Electronique, ou ligne de caisse d'un magasin ou d'une enseigne
 - Automate de distribution
 - Téléphone mobile ou PDA
 - Centre d'appels, centre de saisie, serveur vocal interactif ...
- **Multi-services** : la plateforme Paybox gère une multitude de moyens de paiement :
 - cartes bancaires,
 - cartes privatives,
 - cartes de crédit,mais elle gère également de nombreux services et applications métiers :
 - les cartes cadeaux,
 - les cartes de fidélité,
 - la gestion de flotte,
 - la réservation de véhicules ...





2. OBJET DU DOCUMENT

Dans le domaine de la VAD et du E-Commerce, Paybox propose plusieurs solutions avec chacune des interfaces techniques spécifiques :

- **PAYBOX SYSTEM** : Paybox System s'interface avec le site marchand Internet ou mobile. Les clients acheteurs sont redirigés automatiquement sur les pages de paiement multilingues hébergées par Paybox. Ces pages sont personnalisables pour les harmoniser avec l'identité graphique du site Marchand. Paybox System répond aux normes de sécurité des paiements par carte sur les sites d'e-commerce en affichant une page SSL 256 bits et en utilisant le protocole 3-DSecure (si option souscrite).
- **PAYBOX DIRECT (PPPS)** : Paybox Direct assure le traitement des paiements de façon transparente pour les clients acheteurs. L'application de vente du marchand doit collecter les informations sensibles telles que le n° de carte et les transmet à Paybox via un dialogue sécurisé de serveur à serveur.
Paybox Direct est également utilisé pour valider les encaissements des transactions préalablement autorisées via Paybox System, assurer des remboursements et annulations de serveur à serveur. Compléter Paybox System avec Paybox Direct permet au commerçant de gagner en flexibilité en intégrant le pilotage des opérations post-autorisation en mode serveur à serveur depuis son application de vente (ou back-office).
- **PAYBOX DIRECT Plus** :
Désigne le service Paybox où l'Application de vente du commerçant demande à Paybox de conserver les données du moyen de paiement. Cette solution s'interface parfaitement en complément de Paybox System ou bien directement en mode serveur à serveur.

Paybox Version Plus permet au Commerçant via ce service de gérer des paiements en plusieurs fois et échancier ainsi que des paiements express ou 1 Clic où l'Acheteur ne redonne pas les données de son moyen de paiement à chaque nouvelle transaction.
- **PAYBOX TRAITEMENT PAR LOT** : Cette solution assure un dialogue par échanges de fichiers structurés en mode off-line entre le commerçant et Paybox. L'application de vente du site Marchand doit collecter les informations sensibles telles que le n° de carte et les transmet à Paybox via un dialogue sécurisé de serveur à serveur. Traitement Par Lot est également utilisé pour valider les encaissements des transactions préalablement autorisées via Paybox System, mais également assurer des remboursements et annulations.

Le présent document est le manuel d'intégration de la solution **Paybox System**.

Il s'adresse aux personnes ayant besoin d'informations sur le fonctionnement de cette solution, sur la manière de s'y interfacer et de l'intégrer de la meilleure manière.





3. PRESENTATION DU PRODUIT « PAYBOX SYSTEM »

3.1 Principe général de fonctionnement

Le produit « Paybox System » est un système sécurisé de gestion des paiements par cartes bancaires et privatives sur les sites marchands Internet ou mobile.

Pour intégrer le produit « Paybox System », il n'y a aucun module à installer, ni sur le site marchand, ni chez le client qui veut effectuer un paiement.

Une fois le produit intégré avec le site marchand, le client peut effectuer son paiement en toute sécurité : sa commande réalisée, il sera redirigé vers les serveurs de Paybox. Ces derniers établissent alors une connexion cryptée avec l'acheteur (en SSL 128 bits, afin que la saisie des informations confidentielles liées à la carte de paiement soit effectuée en toute sécurité) et lui affichent une page de paiement en l'invitant à saisir ses informations Carte.

Paybox System vérifie alors la validité de la carte en effectuant une demande auprès du centre d'autorisation associé au moyen de paiement choisi, dans le respect des normes de paiement en vigueur. Si le paiement est accepté, un ticket est alors affiché sur l'écran de l'acheteur (optionnel). Ce même ticket lui sera renvoyé par courrier électronique (e-mail) comme preuve du paiement. L'acheteur a alors la possibilité de revenir sur le site marchand pour effectuer d'autres achats.

Paybox System envoie également par e-mail un double du ticket de paiement au commerce. Il sera possible, pour le commerçant, de gérer de façon automatique le résultat de la tentative de paiement grâce à l'analyse des différents retours d'informations.

En fin de journée, Paybox System réunit sous forme de « remise » tous les paiements réalisés sur le site commerçant et les envoie au centre de télécollecte du commerçant afin que les transactions soient traitées.

Une fois la télécollecte effectuée, le commerçant recevra un ticket de compte-rendu par e-mail.






3.2 Liste des moyens de paiement

Ci-dessous une liste complète des moyens de paiement acceptés par Paybox :

MOYEN DE PAIEMENT	TYPE	COMMENTAIRE
CB, VISA, MASTERCARD	Cartes de crédit	
MAESTRO	Carte de débit	3-D Secure obligatoire
BANCONTACT MISTERCASH	Carte de débit	Carte locale belge 3-D Secure obligatoire
E-CARTE BLEUE	Carte de crédit virtuelle dynamique	Opérée par VISA France
AMERICAN EXPRESS	Carte de crédit	
JCB	Carte de credit	
DINERS	Carte de credit	
COFINOGA	Carte de financement	
SOFINCO	Carte de financement	
FINAREF	Carte de financement	Cartes SURCOUF, KANGOUROU, FNAC, CYRILLUS, PRINTEMPS, CONFORAMA
CETEM / AURORE	Carte de financement	
AVANTAGES		Carte Casino Avantages
CDGP	Carte de financement	Carte Cofinoga Quelle
RIVE GAUCHE		
PAYSAFECARD	Carte Prépayée	
WEXPAY	Carte prépayée	Non rechargeable
KADEOS	Carte cadeau prépayée	
SVS	Carte cadeau prépayée	Carte Cadeau Castorama et Etam
LASER	Carte cadeau prépayée	Carte Cadeau
1EURO.COM	Financement en ligne	
PAYPAL		
BUYSTER	Paiement via mobile	
KWIXO	Paiement CtoB et transfert CtoC	
LEETCHI	Cagnotte en ligne	





MAXICHEQUE	Chèques cadeau	
ONEY	Carte cadeau prépayée Financement en ligne	
PAYBUTTON ING	Paielement compte à compte	Nécessite un compte bancaire commerçant chez ING Belgique
iDEAL	Paielement compte à compte	Nécessite un compte bancaire commerçant aux Pays-Bas chez ABN AMRO ou ING NL

3.3 Sécurité

3.3.1 Identification

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

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

Ces éléments d'identification sont fournis par Paybox lors de la confirmation de l'inscription du commerçant à l'utilisation de nos services.

Ces informations sont obligatoires dans tous les messages que le site Marchand enverra à nos plateformes de paiement mais il est également nécessaire de les fournir lors de tout contact avec les équipes du support Paybox.

3.3.2 Authentification

Afin de garantir une sécurité maximale aux paiements effectués sur le site Marchand du commerçant, celui-ci est authentifié par une clé secrète qui ne doit être connue que par lui et par Paybox.

Cette clé sera utilisée pour signer tous les échanges entre le site Marchand et les serveurs de Paybox afin de garantir que la demande de paiement provient d'une source authentifiée.

Le commerçant doit générer lui-même sa clé secrète et le chapitre **Gestion de la clé d'authentification** décrit cette procédure.

3.4 Présentation des pages Paybox System

Tout au long du processus de paiement, plusieurs pages peuvent s'afficher successivement.

3.4.1 Page de présélection du moyen de paiement

Sur cette première page seront présentés l'ensemble des moyens de paiement auxquels le commerçant a souscrit et qu'il souhaite proposer à ses 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.

Par exemple, il ne sera pas demandé de saisie d'un cryptogramme visuel pour la carte Diners mais il en sera demandé un pour les cartes American Express, Visa ou Mastercard.



Voici ci-dessous un exemple de page de choix du moyen de paiement :

The screenshot displays the Paybox payment selection interface. At the top, the Paybox logo is visible alongside a language selector set to 'Français'. Below this, a dark header bar contains the text 'Informations de paiement'. The main content area shows transaction details: 'TEST PAYBOX 1', 'Référence de la transaction 207997761', and 'Montant 10,00 EUR'. A second dark header bar, 'Moyens de paiement', is followed by the instruction 'Choisissez votre moyen de paiement'. A grid of payment method icons is presented, including VISA, MasterCard, Maestro, maxi cheque.com, TICKET sur!, Aurore, cofinoga, and CORA. A 'Plus d'info' link is located below the maxi cheque.com icon. At the bottom, a row of currency conversion rates is displayed: '1,00 EUR = 1,21 CHF | 1,00 EUR = 1,32 USD | 1,00 EUR = 107 JPY | 1,00 EUR = 8,32 CNY | 1,00 EUR = 0,84 GBP'. The footer contains 'Paybox Services®', 'Infos Sécurité SSL', and an 'Annuler' button.

Figure 1 : Page de présélection du moyen de paiement (peut être évitée)

Cette page n'ayant pas d'intérêt s'il n'y a qu'un seul type de carte, elle ne sera pas affichée si le commerçant n'a pas souscrit d'option pour d'autres moyens de paiement. Le client sera alors directement redirigé vers la page de paiement CB.

- Paybox préconise que le commerçant valorise lui-même sur son site e-commerce, sous la forme d'icônes cliquables, la liste des moyens de paiement acceptés. L'acheteur sera alors directement envoyé sur la page de paiement adaptée au moyen de paiement sélectionné.
- Pour Plus d'informations sur les types de carte et moyens de paiement, voir « **§4.2 Forçage du type et moyen de paiement** ».

Cette page de présélection du moyen de paiement est personnalisable.

3.4.2 Page de paiement

The screenshot shows a payment interface for 'LA BOUTIQUE DE TEST'. At the top, it displays 'Paiement de 10.00 EUR'. Below this, the merchant name '***TEST*** LA BOUTIQUE DE TEST' is shown. The main form contains fields for 'Numéro de carte', 'Date de fin de validité (MM/AA)', and 'Cryptogramme visuel : 3 derniers chiffres au dos de la carte (?)'. There are 'Annuler' and 'Valider' buttons, and a 'Retour choix moyens de paiements' button. Below the form, there are flags for various countries and a list of currency conversion rates: 10.00 EUR, 12.08 CHF, 13.17 USD, 1070 JPY, 13.16 CNY, 18.36 GBP, 13.12 CAD. At the bottom, it says 'PAYBOX SERVICES® WWW.PAYBOX.COM'.

Figure 2 : Page de paiement personnalisable

La page affichée ci-dessus est un exemple de page de paiement personnalisée par un commerçant. Pour rassurer les clients et donner un rendu de meilleure qualité, il est possible de personnaliser beaucoup d'éléments pour que la page s'intègre au mieux dans la charte graphique du site Marchand.

Les éléments personnalisables sont notamment :

- Le logo en haut de page
- L'affichage du logo Paybox
- Les boutons de validation/annulation/retour boutique
- Les langues
- Le fond d'écran
- Et bien d'autres options via un fichier CSS

Pour découvrir comment configurer toutes ces options, se référer au document **[Ref 6] Paybox System - Personnalisation de la page et ticket de paiement.**

The screenshot shows a payment interface for 'LABORATOIRE LESCUYER'. At the top, the logo and name 'LABORATOIRE LESCUYER' are visible, along with the tagline 'Compléments Alimentaires Naturels'. A 'Service clients' button with the number '05 61 15 25 00' is also present. Below this, a navigation bar shows 'PANIER', 'LIVRAISON', 'PAIEMENT' (highlighted), and 'CONFIRMATION'. The main form displays 'Paiement de 10.00 EUR à LABORATOIRE LESCUYER'. It includes fields for 'Numéro de carte', 'Date de fin de validité (MM/AA)', and 'Cryptogramme visuel : 3 derniers chiffres au dos de la carte(?)'. There are 'ANNULER' and 'VALIDER' buttons. To the left of the form are logos for 'MasterCard', 'VISA', and 'eBLEUE'. To the right is the 'paybox' logo. Below the form, there are currency conversion rates: 10.00 EUR, 12.14 CHF, 13.10 USD, 1072 JPY, 11.58 CNY, 16.14 GBP, 13.01 CAD. At the bottom, it says 'PAYBOX SERVICES® WWW.PAYBOX.COM' and a link 'Infos Sécurité SSL'.

Figure 3 : Autre exemple de personnalisation

3.4.3 Ticket de paiement

Une fois le paiement autorisé, le client ainsi que le commerçant reçoivent par e-mail un ticket de paiement (à l'identique d'un terminal de paiement physique) avec en début de ticket les 50 premiers caractères de la référence commande. En pied du ticket commerçant se trouve également l'adresse e-mail du client.

Le client est aussi redirigé vers une page lui confirmant immédiatement le bon déroulement de sa transaction. Cette page se présente par défaut sous la forme suivante :

CARTE BANCAIRE	Paiement réalisé avec succès Merci de votre confiance. Ceci est une image du ticket électronique qui vous sera envoyé par E-mail. RETOUR COMMERCE
le 03/05/2011 à 12:24	
TEST PAYBOX 1	
1999888	
501767----- 1503	
86 099 170282 M DEBIT @	
AUTO: XXXXXX	
MONTANT = 10.00 EUR	
POUR INFORMATION 65.60 FRF	
1 EUR = 6.55957 FRF	
TICKET A CONSERVER	

Figure 4 : Ticket d'un paiement réussi

- Il est possible de passer outre cette page et de rediriger, avec les résultats du paiement, le client directement sur le site Marchand (avec le code refus ou n° d'autorisation). Voir [§5 Gestion de la réponse](#)
- De la même manière que la page de paiement, il est possible d'apporter un certain nombre d'améliorations au ticket de paiement transmis au client après son paiement. Par exemple, il est possible d'y ajouter un logo et un texte personnalisé.
- Pour Plus d'informations sur ces possibilités, se référer au document [\[Ref 6\] Paybox System - Personnalisation de la page et ticket de paiement](#).



4. APPEL DE LA PAGE DE PAIEMENT

Pour afficher la page de paiement au client qui souhaite payer sur le site Marchand, il suffit d'envoyer à l'URL de Paybox System une requête HTTPS avec un certain nombre de variables.

4.1 Préparation du message

Les variables suivantes sont obligatoires dans toute requête :

- PBX_SITE = Numéro de site (fourni par Paybox)
- PBX_RANG = Numéro de rang (fourni par Paybox)
- PBX_IDENTIFIANT = Identifiant interne (fourni par Paybox)
- PBX_TOTAL = Montant total de la transaction
- PBX_DEVISE = Devise de la transaction
- PBX_CMD = Référence commande côté commerçant
- PBX_PORTEUR = Adresse E-mail de l'acheteur
- PBX_RETOUR = Liste des variables à retourner par Paybox
- 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

La signification de ces différentes variables ainsi que des variables optionnelles est disponible dans la partie **11 Dictionnaire de données**.

L'ensemble de ces variables doit être envoyé par la méthode POST à l'un de nos serveurs de paiement.

Pour transmettre les variables, vous pouvez utiliser un formulaire comme celui-ci (à titre d'exemple, en pré-production) :

```
<form method="POST" action="https://urlserveur.paybox.com/cgi/MYchoix_pagepaiement.cgi">
  <input type="hidden" name="PBX_SITE" value="1999888">
  <input type="hidden" name="PBX_RANG" value="32">
  <input type="hidden" name="PBX_IDENTIFIANT" value="2">
  <input type="hidden" name="PBX_TOTAL" value="1000">
  <input type="hidden" name="PBX_DEVISE" value="978">
  <input type="hidden" name="PBX_CMD" value="TEST Paybox">
  <input type="hidden" name="PBX_PORTEUR" value="test@paybox.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="2011-02-28T11:01:50+01:00">
  <input type="hidden" name="PBX_HMAC" value="F2A799494504F9E50E91E44C129A45BBA2
6D23F2760CDF92B93166652B9787463E12BAD4C660455FB0447F882B22256DE6E703AD6669B73C59
B034AF0CFC7E">
  <input type="submit" value="Envoyer">
</form>
```

Ainsi, le seul élément visible sur la page sera un bouton « Envoyer ». Quand le client cliquera dessus, il sera automatiquement dirigé vers la page de paiement de Paybox System.





Le paiement sera de 1000 centimes d'euros (soit 10 €) et l'identification du paiement par rapport à la commande du commerçant sera la référence « TEST Paybox ».

Une fois le paiement effectué, si ce dernier est accepté, un ticket de paiement sera envoyé par mail au commerçant ainsi qu'au client à « client@test.com ».

L'identification du commerçant (site 1999888, rang 32 et identifiant 2) correspond à la boutique de test Paybox, accessible sur notre environnement de pré-production.

Des informations complémentaires concernant les conditions de test sur notre environnement de pré-production sont disponibles au chapitre **§10 Environnement de Tests**.

Attention, l'exemple ci-dessus fait référence à une URL de serveur factice.

Les URL d'appel en production sont définies au chapitre **§12.6 URL d'appel et Adresses IP**.

4.2 Forçage du type et moyen de paiement

Si le commerçant préfère se charger lui-même du choix du moyen de paiement, il est possible de fournir directement à l'appel de Paybox System l'information du moyen de paiement choisi. Ceci se fait par l'intermédiaire des variables PBX_TYPEPAIEMENT et PBX_TYPECARTE.

Ainsi, le client sera redirigé directement sur la page de paiement adaptée au moyen de paiement choisi, et ne verra donc pas la page de présélection du moyen de paiement Paybox System.

Exemple : Pour un paiement avec une carte CB classique, il faut documenter PBX_TYPEPAIEMENT à « CARTE » et PBX_TYPECARTE à « CB ».

L'ensemble des valeurs possibles pour ces variables est disponible dans le **§11 Dictionnaire de données**. **Erreur ! Source du renvoi introuvable.**

ATTENTION : Les 2 variables PBX_TYPEPAIEMENT et PBX_TYPECARTE doivent obligatoirement fonctionner conjointement et l'utilisation de l'une sans l'autre ou bien 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.

4.3 Authentification du message par empreinte

Afin de sécuriser le paiement, c'est-à-dire assurer que c'est bien le commerçant qui en est à l'origine et que personne de malveillant n'a modifié une variable (le montant par exemple), Paybox a choisi d'établir une authentification par empreinte HMAC.

- Etape 0 : Si ce n'est déjà fait, le commerçant doit générer une clé secrète via l'accès Back-Office commerçant. La procédure est décrite dans le paragraphe **§8.2 Gestion de la clé d'authentification**.
- Etape 1 : il faut ensuite, lors de la création d'un message à destination des serveurs de Paybox, concaténer l'ensemble des variables en séparant chaque variable par le symbole « & ». Pour le message ci-dessus (§4.1), il faut donc se baser sur la chaîne suivante :





```
PBX_SITE=1999888&PBX_RANG=32&PBX_IDENTIFIANT=2&PBX_TOTAL=1000&PBX_DEVISE=978&PBX_CMD=TEST  
Paybox&PBX_PORTEUR=test@paybox.com&PBX_RETOUT= Mt:M;Ref:R;Auto:A;Erreur:E  
&PBX_HASH=SHA512&PBX_TIME=2011-02-28T11:01:50+01:00
```

- Etape 2 : il est alors possible de lancer le calcul de l'empreinte HMAC en utilisant
 - La chaîne qui vient d'être construite
 - La clé secrète obtenue via le Back Office
 - Un algorithme au choix (cf. PBX_HASH dans §11.1.9 PBX_HASH)
- Etape 3 : le résultat obtenu (l'empreinte) doit alors être placé dans le champ PBX_HMAC de la requête.
- L'ordre dans la chaîne à hasher doit être strictement identique à l'ordre des variables dans le formulaire.
- Dans la chaîne à hasher, il faut utiliser les données « brutes », c'est-à-dire ne pas utiliser les fonctions d'encodage URL

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
$msg = "PBX_SITE=1999888".
"&PBX_RANG=32".
"&PBX_IDENTIFIANT=2".
"&PBX_TOTAL="._POST['montant'].
"&PBX_DEVISE=978".
"&PBX_CMD="._POST['ref'].
"&PBX_PORTEUR="._POST['email'].
"&PBX_RETOUT=Mt:M;Ref:R;Auto:A;Erreur:E".
"&PBX_HASH=SHA512".
"&PBX_TIME=".$dateTime;

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

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

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

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

// On crée le formulaire à envoyer à Paybox System
// ATTENTION : l'ordre des champs est extrêmement important, il doit
// correspondre exactement à l'ordre des champs dans la chaîne hachée
?>
<form method="POST" action="https://urlserveur.paybox.com/cgi/MYchoix_pagepaiement.cgi">
<input type="hidden" name="PBX_SITE" value="1999888">
<input type="hidden" name="PBX_RANG" value="32">
<input type="hidden" name="PBX_IDENTIFIANT" value="2">
<input type="hidden" name="PBX_TOTAL" value="<? echo $_POST['montant']; ?>">
<input type="hidden" name="PBX_DEVISE" value="978">
<input type="hidden" name="PBX_CMD" value="<? echo $_POST['ref']; ?>">
<input type="hidden" name="PBX_PORTEUR" value="<? echo $_POST['email']; ?>">
<input type="hidden" name="PBX_RETOUT" 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>
```

- ❗ Si vous utilisez déjà l'ancienne méthode de communication avec Paybox (par module CGI sur le serveur marchand), le premier appel HMAC bloquera les paiements par l'ancienne méthode.





4.4 URL appelée

La liste des URL des serveurs Paybox est détaillée dans le tableau **§12.6 URL d'appel et Adresses IPErreur ! Source du renvoi introuvable..**

En cas d'indisponibilité de cette URL, des URL de secours sont disponibles. Il est de la responsabilité du site Marchand de vérifier la disponibilité d'une URL avant de rediriger le client.

Il est possible de tester la disponibilité des serveurs en essayant d'accéder à une page HTML « load.htm ». Cette page contient uniquement la chaîne « OK » qui confirme que le serveur est accessible.

Ci-dessous un exemple de code PHP pour tester la disponibilité des serveurs Paybox (attention les URLs indiquées dans l'exemple sont factices, elles sont à remplacer par les vraies URL de production) :

```
<?php
$serveurs = array('tpeweb.paybox.com', //serveur primaire
                  'tpeweb1.paybox.com'); //serveur secondaire

$serveurOK = "";

foreach($serveurs as $serveur){
    $doc = new DOMDocument();
    $doc->loadHTMLFile('https://'.$serveur.'/load.html');

    $server_status = "";
    $element = $doc->getElementById('server_status');
    if($element){
        $server_status = $element->textContent;
    }

    if($server_status == "OK"){
        //Le serveur est prêt et les services opérationnels
        $serveurOK = $serveur;
        break;
    }
    // else : La machine est disponible mais les services ne le sont pas.
}

if(!$serveurOK){
    die("Erreur : Aucun serveur n'a été trouvé");
}
```



5. GESTION DE LA REPONSE

Une fois le paiement réalisé sur la page de paiement Paybox, le client a la possibilité de revenir sur le site commerçant par l'intermédiaire de 4 URL.

Le commerçant pourra gérer de façon automatique la validation de ses bons de commandes suivant le résultat de la transaction par l'intermédiaire d'une 5ème URL nommée IPN (Instant Payment Notification).

5.1 Redirection du client

Le retour de Paybox System vers le site marchand peut se faire sur 4 adresses (URL) différentes selon si le paiement est 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.
- Soit en utilisant les valeurs par défaut enregistrées dans la base de données Paybox
 - Ces valeurs doivent être données lors de l'inscription à Paybox System. Il est également possible de les modifier via l'accès Back Office du Commerçant, onglet « Informations ».

Le client sera dirigé sur 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.

Il est également possible de choisir un retour immédiat : il faut préciser cette option dans la fiche d'inscription ou auprès du support technique Paybox. Dans ce cas-là, le ticket récapitulatif n'est pas affiché et le client est redirigé directement vers le site du commerçant.

! Il est fortement déconseillé d'utiliser exclusivement la variable « PBX_EFFECTUE » pour valider les bons de commandes du site Marchand : cette variable n'est pas sécurisée par Paybox et n'est pas garantie comme étant lancée systématiquement. En effet, un acheteur qui a réalisé son paiement peut ne pas vouloir revenir sur le site ou couper sa connexion. Pour plus de précisions, voir chapitre **§5.3 Validation des bons de commande**

! En cas de présence dans l'URL à appeler de caractères HTML spéciaux, il faut les « 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 « ; », il faut remplacer ce caractère par « %3B » :

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

Il faudra donc documenter la variable « PBX_EFFECTUE » de la manière suivante :

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

Cette restriction s'appelle l'URL Encodage et 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 ».





5.2 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, Paybox 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.

Paybox se charge ensuite de mettre à jour la réponse, et quand une décision a été prise, Paybox vous rappelle via l'IPN avec la réponse définitive (ex : 00000 si la transaction est autorisée).

Pour plus d'informations sur ces moyens de paiement, vous pouvez vous référer aux documents :

- [\[Ref 7\] Note Paypal](#)
- [\[Ref 8\] Note Kwixo](#)
- [\[Ref 9\] Note Oney](#)

5.3 Validation des bons de commande

5.3.1 Principe du IPN (Instant Payment Notification)

Ce paramètre IPN est spécialement utilisé pour gérer de façon automatique la validation des bons de commandes.

Ce paramètre est une URL enregistrée dans la base de données Paybox mais elle peut également être gérée dynamiquement comme les 3 URL précédentes via la variable « PBX_REPONDRE_A ».

L'avantage de cette URL est qu'elle est appelée de serveur à serveur dès que le client valide son paiement (que ce dernier soit autorisé ou refusé).

Cela permet ainsi de valider automatiquement le bon de commande correspondant même si le client coupe la connexion ou décide de ne pas revenir sur la boutique, car cet appel ne transite pas par le navigateur du porteur.

Lors de l'appel de cette URL, un script présent sur le serveur Marchand à l'emplacement spécifié par l'URL va s'exécuter. Il n'y a pas de contrainte sur le langage de ce script (ASP, PHP, PERL, ...). La seule limitation est que ce script ne doit pas faire de redirection et doit 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 trois autres : elle est gérée de façon complètement indépendante et peut être appelée sur les ports TCP 80, 443 (HTTPS), 8080, 8081, 8082, 8083, 8084 ou 8085.

5.3.2 Paramètres

Il est possible de configurer la liste des variables qui sont renvoyées au site Marchand dans les





différentes URL de retour. Cette configuration est effectuée par la variable PBX_RETOUR, qui se configure en concaténant la liste des informations souhaitées sous le format suivant :

<nom de la variable que vous souhaitez>:<lettre Paybox correspondante>;

Exemple :

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

Le nom des variables (montant, mref,...) est personnalisable. Pour voir l'ensemble des données disponibles, voir le paramètre **PBX RETOUR** en §11.1.7.

Ces informations seront envoyées à toutes les URL de retour (PBX_EFFECTUE, PBX_ANNULE, PBX_REFUSE et PBX_REPONDRE_A). Par exemple, pour l'URL IPN, avec la valeur citée ci-dessus, la page appelée serait :

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

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.

5.3.3 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 mail utilisée pour envoyer les tickets de paiements. 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 : PAYBOX: 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=00000 (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 en **§12.3 Codes retour HTTP**
 - Seuls les codes retour commençant par un 2 sont considérés comme valides.
- Le second **YYY** correspond au code retour de la librairie "libcurl" assurant les échanges avec le serveur WEB Marchand.
 - Voir la liste des codes retour CURL en **§12.4 Codes erreur CURL**

5.3.4 Vérification des valeurs

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

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





- Numéro d'autorisation (A) : alphanumérique, longueur variable.
 - Pour une transaction de test (pas de demande d'autorisation vers le serveur de la banque ou l'établissement financier privatif), la variable vaut toujours « XXXXXX »
 - Pour une transaction refusée, la variable n'est pas envoyée
- Code erreur (E) :
 - Pour une transaction valide, il doit être à « 00000 »
 - Pour les autres valeurs, se reporter au **§ 12.3 Tableau 3 : Codes réponse PBX_RETOUR**

Pour s'assurer que la réponse provient bien de Paybox, il est fortement conseillé de vérifier le contenu des variables suivantes :

- Signature Paybox (K)
 - Voir paragraphe ci-dessous
- Adresse IP d'origine
 - Pour améliorer la sécurité, il est possible de vérifier que l'appel de l'URL IPN provient bien d'un des serveurs Paybox (voir **§12.6 URL d'appel et Adresses IP**).

Il vous faudra alors vérifier impérativement le numéro d'autorisation, le code erreur, le montant et la signature électronique : si le numéro d'autorisation existe (dans l'exemple précédent il est égal à 30258), que le code erreur est égal à « 00000 », que le montant est identique au montant d'origine et que la signature électronique est vérifiée, cela signifie que le paiement est accepté.

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 en **§12.1 Codes réponses du centre d'autorisation**.

5.3.4.1 Signature Paybox

En utilisant la signature Paybox dans les variables à retourner vers les URL du site Marchand, ce dernier peut s'assurer que :

- les données renvoyées n'ont pas été altérées,
- c'est bien Paybox qui effectue un appel des URL du site.

Il est important de noter que la donnée K de la variable « PBX_RETOUR » doit être toujours être située en dernière position. 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 clé publique de Paybox est en libre téléchargement depuis le site www.paybox.com à la rubrique « Téléchargements ». Pour être en conformité avec les règles de sécurité, Paybox est susceptible de changer sa paire de clé publique/privée : il doit donc être possible de mettre en place différentes clés publiques au niveau des serveurs Marchand.





- **Signature Paybox**

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

- **Vérification de la signature**

De par sa nature, la signature Paybox 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 Paybox, disponible en téléchargement.

- **Tests**

La manière la plus souple de tester un programme de vérification de signature dans votre environnement, est d'utiliser une paire de clé RSA de test.

Vous serez ainsi en mesure de signer vous-même des messages dont vous pourrez vérifier la signature. Ensuite, il suffira de substituer la clé publique de test par la clé publique Paybox.

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

Pour générer une clé privée RSA *privkey.pem* et en extraire la clé publique *pubkey.pem*

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

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

```
openssl dgst -sha1 -binary -sign privkey.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
```

- **Encodage :**

Les messages et signatures transportés au moyen du protocole HTTP (GET ou POST) doivent être sur-encodés (URL encodage et/ou Base64).

De ce fait il faut procéder aux opérations inverses avant de vérifier la signature :

- 1) détacher la signature du message,
- 2) URL décoder la signature,
- 3) décodage Base64 de la signature,
- 4) vérification de la signature [binaire] sur les données (toujours encodées)

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 trois autres URL où la signature est calculée sur l'ensemble des variables.





Données signées :

- a) lors de la réponse Paybox de serveur à serveur (URL IPN), seules les informations demandées dans la variable PBX_RETOUT 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 '?' (les paramètres URL).

ex.: `http:// www.moncommerce.com /mondir/moncgi.php ? monparam=mavaleur&pbxparam1=val1&pbxparam2=val2 ... &sign=df123dsfd3...1f1ffsre%20t321rt1t3e=`

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

cas a) `pbxparam1=val1&pbxparam2=val2 ...`

cas b) `monparam=mavaleur& pbxparam1=val1&pbxparam2=val2 ...`

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

- **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.





6. FONCTIONNALITES AVANCEES

Au-delà de la fonction élémentaire de paiement, Paybox System propose un certain nombre de fonctionnalités additionnelles permettant au commerçant de piloter plus souplement ses opérations et d'offrir aux clients finaux des services à valeur ajoutée intéressants.

Certaines de ces fonctionnalités sont décrites ci-dessous.

Pour obtenir une liste exhaustive et une description des fonctionnalités disponibles et pour souscrire à ces options, contacter le service Commercial (voir **§9 Support – Assistance - Contact**).

6.1 Intégration avec Paybox Direct Plus

6.1.1 Principe

En utilisant conjointement Paybox System version PLUS et Paybox Direct Plus, il est possible d'accéder à des fonctions supplémentaires, comme entre autres :

- Paiement en 1 clic,
- Capture de la transaction en différé,
- Autorisation seule
- Autorisation + débit
- Débit (sur une autorisation pré effectuée)
- Crédit
- Annulation (d'une opération pré effectuée)
-

Lors du paiement par Paybox System, le contexte carte sera sauvegardé (création d'un abonné), et à partir d'un identifiant lié à cet abonné et retourné par Paybox System, le commerçant fera référence à cet abonné pour initier ultérieurement d'autres paiements sur la même carte via Paybox Direct Plus, sans avoir à ressaisir ces données Carte.

6.1.2 Utilisation

6.1.2.1 Appel Paybox System version Plus

Lors de l'appel Paybox System version PLUS, il faut nécessairement utiliser les variables PBX_RETOUR et PBX_CMD et/ou PBX_REFABONNE.

- L'une des variables PBX_CMD ou PBX_REFABONNE doit contenir l'identifiant du contexte de la carte (ou abonné).
 - Si la variable PBX_REFABONNE est présente, c'est elle qui sera utilisée pour définir l'identifiant de l'abonné (et la carte associée), sinon ce sera PBX_CMD
 - Le choix de cet identifiant est laissé à la discrétion du commerçant
 - Il doit être unique pour un contrat commerçant (PBX_SITE).
- La variable PBX_RETOUR doit obligatoirement contenir au moins la variable « U »
 - Lors du retour, une chaîne à conserver est retournée dans ce paramètre « U »
 - Cette chaîne est au format suivant, les 3 champs étant séparés par '++' :
Handle_Numéro_De_Carte_Crypté++Date_De_Validité_De_La_Carte++CVV





6.1.2.2 Utilisation dans Paybox Direct Plus

Pour faire référence à un abonné créé précédemment via Paybox System, 2 variables seront à utiliser dans Paybox Direct Plus:

- La variable REFABONNE devra contenir la référence à l'abonné
 - C'est la valeur utilisée lors de l'appel Paybox System dans la variable PBX_REFABONNE si elle était présente, ou PBX_CMD sinon
- PORTEUR devra contenir le Handle de numéro de carte retourné par Paybox System dans la variable de retour U. Ce Handle a été retourné « URL encodé », il doit être à l'inverse « URL décodé » avant d'être utilisé dans Paybox Direct.
 - Ce numéro est incomplet pour des raisons de sécurité.

6.1.2.3 VOIR AUSSI

- **[Ref 1] Manuel d'intégration Paybox Direct/Direct Plus** pour plus d'informations sur le fonctionnement général de cette application
- **§11 Dictionnaire de données** Erreur ! Source du renvoi introuvable., pour des informations sur les variables PBX_CMD, PBX_REFABONNE, PBX_RETOUT
- **§5 Gestion de la réponse**, pour l'utilisation de PBX_RETOUT

6.2 Autorisation sans capture

6.2.1 Principe

Cette option permet d'effectuer une demande d'autorisation vers le serveur de la banque ou de l'établissement financier privatif mais la transaction ne sera jamais confirmée et le porteur ne sera jamais débité si le commerçant n'adresse pas un 2^{ème} message de confirmation à Paybox.

Cette option peut être utilisée pour les scénarios suivants :

- Débit après processus de validation (total ou partiel),
- Débit au départ 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

6.2.2 Utilisation

En positionnant le paramètre PBX_AUTOSEULE à 'O', seule l'autorisation sera réalisée et pas la télécollecte.

Si PBX_AUTOSEULE est à 'N' ou si la variable n'est pas présente, la transaction sera marquée pour être télécollectée le soir.

Néanmoins, même si la transaction est réalisée en mode PBX_AUTOSEULE='O', la transaction est bien enregistrée et elle peut être capturée (télécollectée) ultérieurement via les solutions Traitement par Lots ou Paybox Direct, dans un délai de 75 jours maximum.





- Pour les paiements par carte, Paybox préconise au commerçant de ne pas dépasser 7 jours entre la date de la demande d'autorisation et la date de remise en banque (capture). Au-delà, le commerçant peut avoir à gérer des impayés pour encaissement tardif.
- Pour les paiements Paypal, la capture peut se faire dans les 29 jours. Cependant, Paypal ne garantit les fonds que durant les 4 premiers jours.
- Pour les paiements Buyster, le commerçant dispose de 30 jours pour faire la capture.

6.3 Paiement différé

6.3.1 Principe

Paybox System peut gérer les paiements différés, c'est à dire garder les transactions un certain nombre de jours avant de les envoyer vers le centre de télécollecte de la banque ou de l'établissement financier privatif pour débiter l'acheteur et créditer le commerçant.

Cette option peut s'avérer très utile, lorsque le commerçant désire s'assurer que la marchandise ou le service a été livré au client avant que ce dernier soit débité.

Sur la fiche d'inscription Paybox System, 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 par le porteur,
- 2 : le paiement sera envoyé en banque le surlendemain de l'achat par le porteur,
- etc...
- Pour les paiements par carte, Paybox préconise au commerçant de ne pas dépasser 7 jours entre la date de la demande d'autorisation et la date effective de remise en banque. Au-delà, le commerçant peut avoir à gérer des impayés pour encaissement tardif.
- Pour les paiements Buyster, la durée maximum est de 6 jours. Pour toute demande supérieure, le paiement est refusé par Paybox.

6.3.2 Utilisation

Il suffit de préciser dans la variable PBX_DIFF le nombre de jours de décalage souhaité entre l'achat et la télécollecte. Ce nombre de jours de décalage peut être fixé à une valeur par défaut dans la fiche d'inscription ou en l'indiquant au service Support.



6.4 Paiement sur mobile

6.4.1 Principe

Le fonctionnement est identique à un site Web classique sur Internet. Les pages Web affichées sur le mobile ou le smartphone sont soit des pages XHTML dédiées soit des pages gérées par une application chargée sur le smartphone. Au moment du paiement, le mobile se connecte sur Paybox qui traite ensuite la transaction normalement.

Aujourd'hui, les moyens de paiement utilisables sur mobile sont : CB, VISA, MASTERCARD, AMEX, PAYPAL.

The image displays three screenshots of a mobile payment interface. The first screenshot, titled 'INFORMATIONS DE PAIEMENT', shows a VeriSign Secured logo and order details: 'Montant de la commande : 1.01 EUR' and 'Identifiant société : TEST PAYBOX 1'. Below this, under 'MOYENS DE PAIEMENT', it says 'Choisissez votre moyen de paiement' and lists logos for VISA, MasterCard, and PayPal. A link for 'Annulation/Retour' is at the bottom. The second screenshot, titled 'DONNEES DE PAIEMENT', also shows the VeriSign Secured logo and the same order details. It prompts the user to 'Veuillez renseigner vos données de paiements' and includes fields for 'Numéro de carte', 'Date de fin de validité (MM/AA)', and 'Cryptogramme visuel'. A 'VALIDER >>' button and an 'Annulation / Retour' link are at the bottom. The third screenshot is a 'Connexion' screen for 'Test Store'. It shows 'Mon total : €1,03 EUR' and the PayPal logo. It prompts for 'Connexion à l'aide d'une adresse email et d'un mot de passe' with input fields for 'Email' and 'Mot de passe', and a 'Connexion' button. At the bottom, it asks 'Vous n'avez pas de compte PayPal ?' with a 'Payer par carte' link, and provides links for 'Rendez-vous sur le site de PayPal pour payer.' and 'Problème de connexion ?'.

6.4.2 Utilisation

Il faut renseigner dans la requête le paramètre PBX_SOURCE avec la valeur XHTML.

ATTENTION : les URL d'accès aux services Paybox pour le paiement sur mobile sont spécifiques (voir §12.6 URL d'appel et Adresses IP).





7. OPTION GESTION DES ABONNEMENTS

Les fonctions décrites dans ce paragraphe nécessitent l'activation de l'option Gestion des abonnements.

Pour souscrire à cette option, pour souscrire à ces options, contacter le service Commercial (voir §9 **Support – Assistance - Contact**).

7.1 Principe

La gestion des paiements par abonnement permet au commerçant de gérer des prélèvements périodiques ou des paiements en plusieurs fois pour ses clients. Ainsi, une fois le paiement initial effectué, le client sera prélevé de façon cyclique suivant une fréquence choisie préalablement par le commerçant.

- La gestion de l'abonnement sur Paybox System est une gestion de base : elle ne prévoit que des cas simples d'abonnements, basés sur la reconduction périodique de paiement d'une même somme, sur une période souhaitée initialement par le commerçant. Ces paramètres ne peuvent pas, par la suite, être modifiés.
- Malgré sa simplicité, le système offre une souplesse de paramétrage permettant notamment, avec la gestion des différés, un large éventail de déclenchement de la première reconduction de l'abonnement.
- Il est à noter qu'en cas d'échec (refus d'autorisation) sur une échéance, Paybox n'assure pas de représentation et stoppe les futures échéances. (La solution Paybox Direct *Plus* apporte plus de souplesse sur ce sujet).
- Le commerçant peut suivre ses abonnements via son accès au Back Office Commerçant

Pour gérer cette option uniquement disponible pour le produit « Paybox System », il faudra en faire la demande auprès de notre service commercial et technique et modifier le contenu de la variable PBX_CMD comme expliqué ci-dessous.





7.2 Création d'un abonnement

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

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

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

Les autres informations pour le paiement via le produit « Paybox System » ne changent pas. La devise est passée par la variable PBX_DEVISE et le montant du premier règlement (qui peut être différent des prélèvements de l'abonnement) est passé dans la variable PBX_TOTAL.

Exemples d'abonnement :

Exemple 1 :

```
PBX_SITE=1999888&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1500&PBX_DEVISE=978&PBX_CMD=ma_ref123PBX_2MONT0000000500PBX_NBPAIE00PBX_FREQ01PBX_QUAND28PBX_DELAIS005&PBX_PORTEUR=test@paybox.com&PBX_RETOUT=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=2011-02-28T11:01:50+01:00
```

Si le paiement initial (15 euros, soit 1500 centimes) est effectué le 28 novembre par exemple, le premier prélèvement aura lieu le 03 décembre (car la prise en compte de l'abonnement se fait 5 jours plus tard via PBX_DELAIS).

Tous les prélèvements sont d'un montant de 5 euros (soit 500 centimes) (PBX_2MONT), réalisés le 28 (PBX_QUAND) de tous les mois (PBX_FREQ) jusqu'à une demande de résiliation (PBX_NBPAIE) de votre part ou un rejet du centre d'autorisation (si la carte bancaire est arrivée à expiration).

Exemple 2 :

```
PBX_SITE=1999888&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1500&PBX_DEVISE=978&PBX_CMD=ma_ref123PBX_2MONT0000000550PBX_NBPAIE10PBX_FREQ03PBX_QUAND31&PBX_PORTEUR=test@paybox.com&PBX_RETOUT=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=2011-02-28T11:01:50+01:00
```

Si le paiement initial (20 euros) est effectué le 28 novembre par exemple, le premier prélèvement aura lieu le 31 novembre (car la prise en compte de l'abonnement est immédiate via PBX_DELAIS qui est inexistante).





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

Lorsqu'un abonnement est créé, un mail « ticket de paiement » est envoyé au commerçant et au client avec une mention précisant le montant et la date un prochain prélèvement.

Mention précisée sur le mail envoyé au client :

**Prochain prélèvement le xx/xx/xxxx d'un montant de xx.xx Eur
(pour toute réclamation adressez vous à votre commerçant).**

Mention précisée sur le mail envoyé au commerçant :

**Prochain prélèvement le xx/xx/xxxx d'un montant de xx.xx Eur
Pour toute résiliation de cet abonnement veuillez rappeler la référence PAYBOX xxxxxxxx.**

Attention :

- En cas d'utilisation de l'URL IPN, cette dernière sera également appelée aussi bien en cas de reconduction réussie qu'échouée. La variable ETAT_PBX sera ajoutée à l'URL d'appel avec comme information PBX_RECONDUCTION_ABT.

Par exemple :

http://www.commerce.fr/traite.php?ETAT_PBX=PBX_RECONDUCTION_ABT&Mt=1200&Trans=12345678&Ref=MaReference&Autorisation=987654&NumAbonnement=56789

7.3 Paiement en plusieurs fois (4 fois max)

Le paiement en plusieurs fois répond à un besoin légèrement différent de l'abonnement. Alors que l'abonnement est basé sur des montants fixes à échéances régulières, l'interface de paiement en plusieurs fois permet de configurer chaque fois librement, en termes de montants et de dates, dans la limite de 3 paiements en plus du paiement initial.

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

Exemple :

PBX_SITE=1999888&PBX_RANG=99&PBX_IDENTIFIANT=2&PBX_TOTAL=1000&PBX_DEVISE=978&PBX_CMD=TESTPaybox&PBX_PORTEUR=test@paybox.com&PBX_RETOUT=Mt:M;Ref:R;Auto:A;Erreur:E&PBX_HASH=SHA512&PBX_TIME=2011-02-28T11:01:50+01:00&PBX_2MONT1=2000&PBX_DATE1=01/02/2013&PBX_2MONT2=3000&PBX_DATE2=15/02/2013

Dans cet exemple, la somme de 10€ sera débitée immédiatement, puis la somme de 20€ sera débitée le 1er février, et enfin, 30€ seront débités de 15 février.

Comme pour les abonnements, l'échéancier est conservé par Paybox, et une fois le premier paiement terminé, le commerçant n'a plus à gérer de nouveaux appels vers Paybox pour déclencher les paiements.





7.4 Fin des abonnements

L'abonnement peut se terminer de 3 façons différentes :

- **Fin normale**
Lorsque toutes les échéances d'un abonnement ont été traitées avec succès, l'abonnement se termine de lui-même.
- **Fin en échec**
Lorsque l'une des échéances échoue, il n'y a pas de représentation de l'échéance ultérieurement. L'abonnement est clôturé et le commerçant est informé de ce résultat par un mail.
- **Résiliation par le commerçant**
Le commerçant peut choisir à tout moment d'arrêter l'abonnement en cours. Pour cela, il peut se rendre sur le Back-Office, ou bien exécuter un appel à la plateforme Paybox pour l'arrêter. Les paramètres de cet appel sont décrits ci-après.
Lorsque le commerçant résilie un abonnement, le client porteur en est informé par mail.

7.4.1 Résiliation par appel serveur-serveur

Pour intégrer la gestion des abonnements avec le système d'informations du commerçant, Paybox met à disposition un utilitaire permettant de résilier l'abonnement sans intervention manuelle.

L'URL à appeler est disponible en annexe dans le tableau **§12.6 URL d'appel et Adresses IP**, section Résiliation des abonnements. L'appel peut être fait via la méthode GET ou POST et consiste en un assemblage de variables.

Il est possible d'identifier l'abonnement à résilier de 2 manières :

- **Par numéro d'abonnement**
Ce numéro est transmis dans la réponse Paybox System
Exemple :
`VERSION=001&TYPE=001&SITE=1999888&MACH=099&IDENTIFIANT=2&ABONNEMENT=1`
- **Par référence commande**
C'est la référence transmise lors de l'appel
Exemple :
`VERSION=001&TYPE=001&SITE=1999888&MACH=099&IDENTIFIANT=2&REFERENCE=refcmd`

En réponse, le serveur renvoie lui aussi une succession de variables. La variable ACQ permet de connaître le bon déroulement ou non de la résiliation.

En plus, la référence transmise à l'appel est retransmise dans la réponse (ABONNEMENT ou REFERENCE)

Exemples :

Réponse en cas de succès : `ACQ=OK&IDENTIFIANT=2&ABONNEMENT=1`

Réponse en cas d'échec de résiliation : `ACQ=NO&ERREUR=9&IDENTIFIANT=2&REFERENCE=refcmd1`

Il est à noter qu'il n'y a pas d'émission de la part de Paybox System d'un email vers le porteur lors de la résiliation d'un abonnement par le commerçant sauf lors d'une résiliation via le backoffice.





8. LE BACK-OFFICE COMMERÇANT

Dès que le commerçant a souscrit un service auprès de Paybox, il se voit automatiquement attribuer un accès au Back Office Commerçant (BOC), tableau de bord en ligne et sécurisé qui lui permet de consulter ses transactions et effectuer diverses opérations (exports, annulations/remboursements, gestion des télécollectes différées, ...).

8.1 Accès et fonctionnalités

Les conditions d'accès à ce Back Office Commerçant ainsi que l'ensemble des fonctionnalités disponibles (Journal, Export, Validation/Annulation/Remboursement de transactions, ...) sont détaillées dans le document **[Ref 3] Guide Utilisateur du Back Office**, accessible ici :

<http://www1.paybox.com/espace-integrateur-documentation/manuels/>

8.2 Gestion de la clé d'authentification

Cette clé est indispensable, elle permet d'authentifier tous les messages échangés entre le site Marchand et les serveurs Paybox. Le commerçant doit donc générer sa propre clé unique et confidentielle et l'utiliser pour calculer une empreinte sur ses messages.

8.2.1 Génération

L'interface de génération de la clé secrète d'authentification se trouve dans l'onglet « Informations » du Back Office Commerçant, en bas de la page.

Voici à quoi ressemble cette interface :

Modification de la clé HMAC	
Phrase de passe	●●●●●●●●●●●●●●●●
Cacher	<input checked="" type="checkbox"/>
Complexité	Très fort
Force	100%
Clé	
<input type="button" value="VALIDER"/>	

Générer une clé

Figure 5 : Génération d'une clé secrète

Le champ « Phrase de passe » peut être renseigné avec une phrase, un mot de passe, ou tout autre texte.

L'affichage par défaut du champ « Phrase de passe » est caché, les caractères apparaissent comme un champ « mot de passe ». Il est possible de choisir d'afficher cette phrase de passe en décochant la case « Cacher ».





Les champs « Complexité » et « Force » sont mis à jour automatiquement lorsque la phrase de passe est saisie. Ces champs permettent de définir des règles d'acceptation minimales de la phrase de passe. Les règles fixées actuellement demandent une phrase de passe d'au moins 15 caractères de long et d'une force de 90%. Le bouton « VALIDER » restera grisé tant que ces limitations ne sont pas respectées.

La force de la phrase de passe est calculée selon certains critères spécifiques, à savoir le nombre de majuscules, minuscules, caractères spéciaux, etc. Il conviendra donc de varier les caractères saisis, de les alterner et d'éviter les répétitions qui tendent à diminuer le score final.

Le bouton « Générer une clé » permet de calculer la clé d'authentification 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 retapant la même phrase de passe et en relançant le calcul.

- ⚠ Attention, il est possible que le calcul de la clé prenne quelques secondes, selon le navigateur Internet utilisé et la puissance de l'ordinateur. Au cours du calcul, il se peut que le navigateur Internet Explorer demande s'il faut « arrêter l'exécution de ce script ». Il faut répondre « Non » à cette alerte, et patienter jusqu'à la fin du calcul.

Une fois le calcul terminé, la clé sera affichée dans le champ « Clé ». Il est alors possible de copier/coller cette clé d'authentification pour l'intégrer dans la base de données du site Marchand, ou autre mode de stockage, de préférence sécurisé.

Il est également possible de saisir dans le champ « Clé » sa propre clé d'authentification (au format hexadécimal) qui aurait été calculée grâce à un autre moyen que cette interface. La taille minimale de la clé à saisir correspond à une génération de clé en SHA-1, soit 40 caractères hexadécimaux. Cependant, si cette méthode de saisie d'une clé d'authentification « externe » est utilisée, une alerte s'affichera pour rappeler que Paybox ne peut pas en garantir la robustesse.

Le bouton « VALIDER » est grisé par défaut. Les 2 actions qui peuvent activer le bouton sont :

- Saisir une phrase de passe de plus de 15 caractères et dont la force est de plus de 90%
- Saisir une clé hexadécimale de plus de 40 caractères.

Si après avoir saisi une phrase de passe répondant aux critères minimaux, le bouton « VALIDER » est cliqué sans avoir cliqué sur « Générer une clé », alors le calcul de la clé d'authentification se lancera automatiquement.

Après validation du formulaire, un message récapitulatif sera affiché sur la page, expliquant qu'un email de demande de confirmation a été envoyé à l'adresse mail du commerçant. La clé qui vient d'être générée ne sera pas active tant que les indications de validation décrites dans cet email n'auront pas été appliquées.

La clé est affichée sur ce récapitulatif. Pour des raisons de sécurité, cette clé ne sera plus transmise ni demandée par nos services. Par conséquent, si cette clé est égarée, il sera nécessaire d'en générer une nouvelle. Il est donc important de veiller à copier la clé d'authentification affichée avant de quitter la page.

- ⚠ La clé est dépendante de la plateforme sur laquelle elle est générée. Cela signifie qu'il faut générer une clé pour l'environnement de test et une pour l'environnement de production.





8.2.2 Validation

Une fois l'enregistrement de la nouvelle clé effectué, un email de demande de confirmation sera envoyé au commerçant. Dans cet email se trouvera un lien pointant sur le programme « CBDValid.cgi », par exemple :

<https://admin.paybox.com/cgi/CBDValid.cgi?id=5475C869BB64B33F35D0A37DF466568475BC9601>

Le paramètre « id » n'est pas la clé saisie, il s'agit d'un « token » généré aléatoirement qui correspond à la clé à valider. Comme dit précédemment, la clé ne sera pas transmise dans l'email.

Après avoir cliqué sur ce lien, si un message annonce « Votre clé est activée », alors la clé est immédiatement en fonction. Ce qui signifie que la clé qui vient d'être validée devrait aussi être en fonction sur le site Marchand.

8.2.3 Expiration

Lorsque la clé est validée, celle-ci se voit affectée une date d'expiration. Cette date correspond à la date d'activation plus 31 jours.

Quand cette date sera atteinte, la clé ne sera pas directement désactivée, pour permettre au site Marchand de continuer à fonctionner, mais le commerçant sera averti par email et sur la page d'accueil du Back Office Commerçant que cette clé est expirée. Il est fortement recommandé de générer une nouvelle clé d'authentification dans ce cas-là.

8.2.4 Transmission

La clé secrète d'authentification ne doit en aucun cas être transmise par e-mail. Paybox ne la demandera jamais au commerçant. Les commerçants doivent donc être particulièrement vigilants quant aux demandes suspectes de transmission de la clé d'authentification, il s'agit probablement d'une tentative de phishing ou social engineering.

En cas de perte de la clé secrète, nous ne serons donc pas en mesure de la redonner, il faudra donc en générer une nouvelle via le Back Office Commerçant.





9. SUPPORT – ASSISTANCE - CONTACT

9.1 Accès

INFORMATION

Pour tout renseignement nos Equipes restent à disposition des commerçants et Intégrateurs, du lundi au vendredi de 9H à 18H :

Service Commercial :

e-mail : contact@paybox.com

Téléphone : + 33 (0)1 61 37 05 70

ASSISTANCE

Pour tout renseignement ou assistance à l'installation et à l'utilisation de nos produits, nos Equipes restent à disposition des commerçants et Intégrateurs, du lundi au vendredi de 9H à 12H30 et 14H à 18H30 (17H30 le vendredi) :

Support Technique & Fonctionnel :

e-mail : support@paybox.com

Téléphone : + 33 (0)4 68 85 79 90

Pour tout contact auprès de nos services, il faut IMPERATIVEMENT communiquer les identifiants Paybox :

- numéro de SITE (7 chiffres)
- numéro de RANG (2 chiffres)
- numéro d'identification Paybox (1 à 9 chiffres)

9.2 Fonctions

Les fonctions du support sont :

- Support à l'intégration et maintenance auprès des clients qui le sollicitent
- Surveillance des processus
- Analyses conjointes avec les différentes équipes (R&D, Exploitation, Réseau, ...) pour résoudre d'éventuels problèmes





9.3 Procédure d'inscription

Pour s'abonner aux services Paybox, le client doit contacter le Service Commercial de Paybox (voir coordonnées ci-dessus), ou prendre contact avec nous via le formulaire présent en rubrique « **Contact** » sur le site Paybox **www.paybox.com**, ou bien envoyer un e-mail à **contact@paybox.com**.

Il sera envoyé au commerçant un formulaire (fiche d'inscription) pour l'enregistrement par Paybox des paramètres utiles aux services Paybox.

Au préalable, le commerçant devra contacter sa banque ou son établissement financier privatif pour demander l'ouverture d'un contrat de VAD/VPC, sur son compte bancaire normal. Les modalités du contrat VAD/VPC varient selon les établissements.

La banque remettra alors au commerçant un numéro de SITE (7 chiffres) et un numéro de RANG (2 ou 3 chiffres) : ces numéros serviront d'identification auprès de Paybox.

Les informations à préciser sur la fiche d'inscription sont :

- ! les coordonnées du commerçant,
- ! les coordonnées de l'hébergeur ou intermédiaire (si le commerce ne gère pas directement son serveur),
- ! les informations monétiques (à remplir avec la banque),

Si le commerçant souhaite accepter des paiements dans une monnaie autre que l'Euro, il faut le préciser lors de l'ouverture du contrat VAD/VPC auprès de la banque.

Pour les autres moyens de paiements, le commerçant peut contacter le service commercial qui lui indiquera la procédure à suivre en fonction des moyens de paiement souhaités.





10. ENVIRONNEMENT DE TESTS

Avant de commencer à effectuer des paiements sur le site en production, Paybox recommande au commerçant de vérifier l'intégration correcte des solutions Paybox. Pour cela, Paybox met à disposition des commerçants une plateforme de pré-production, ainsi que des comptes et des paramètres de tests, entièrement destinés à la réalisation de tests.

Toutes les informations relatives à cet environnement de tests sont précisées dans la documentation [Ref1] « **ParametresTestPaybox_V6.1_FR.pdf** » accessible en téléchargement ici :

<http://www1.paybox.com/espace-integrateur-documentation/manuels/>





11. DICTIONNAIRE DE DONNEES

L'ensemble des variables Paybox System est résumée dans ce tableau. Le détail de chaque variable (format, contenu, exemples) est donné dans les pages qui suivent.

VARIABLE	RESUME	
PBX_1EURO_CODEEXTERNE	Données spécifique 1euro.com	C
PBX_1EURO_DATA	Données spécifique 1euro.com	C
PBX_2MONT n	Paieement en plusieurs fois : Montant des échéances	F
PBX_3DS	Désactivation 3-D Secure ponctuelle	F
PBX_ANNULE	URL de retour en cas d'abandon	F
PBX_ARCHIVAGE	Référence archivage	F
PBX_ATTENTE	URL de retour en cas de paiement en attente de validation	F
PBX_AUTOSEULE	Ne pas envoyer ce paiement à la banque immédiatement	F
PBX_CK_ONLY	Forçage d'un mode de paiement Carte Cadeau uniquement (non mixte)	F
PBX_CMD	Référence commande	O
PBX_CODEFAMILLE	Données spécifique Cofinoga	C
PBX_CURRENCYDISPLAY	Configuration des devises affichées	F
PBX_DATE n	Paieement en plusieurs fois : Dates des échéances	F
PBX_DEVISE	Devise (monnaie)	O
PBX_DIFF	Nombre de jours pour un paiement différé	F
PBX_DISPLAY	Timeout de la page de paiement	F
PBX_EFFECTUE	URL de retour en cas de succès	F
PBX_EMPREINTE	Empreinte fournie lors d'un premier paiement	F
PBX_ENTITE	Référence numérique d'un subdivision	F
PBX_ERRORCODETEST	Code erreur à renvoyer (pour tests)	F
PBX_GROUPE	Groupe pour Paybox Version ++	C
PBX_HASH	Algorithme utilisé pour la signature du message	O
PBX_HMAC	Signature du message	O
PBX_IDABT	Numéro d'abonnement	F
PBX_IDENTIFIANT	Identifiant client Paybox	O
PBX_LANGUE	Langue de la page de paiement	F
PBX_MAXICHEQUE_DATA	Donnée spécifique Maxichèque	C



PBX_NBCARTESKDO	Nombre max de cartes cadeau utilisables par le porteur	F
PBX_NETRESERVE_DATA	Données spécifique Net Reserve	C
PBX_ONEY_DATA	Données spécifique Oney	C
PBX_PAYPAL_DATA	Données spécifiques à Paypal	C
PBX_PORTEUR	Adresse mail du client	O
PBX_RANG	Numéro de rang fourni par la banque	O
PBX_REFABONNE	Référence de l'abonné (version Plus)	C
PBX_REFUSE	URL de retour en cas de refus du paiement	F
PBX_REPONDRE_A	URL IPN	F
PBX_RETOUR	Configuration de la réponse	O
PBX_RUF1	Méthode d'appel de l'URL IPN	F
PBX_SITE	Numéro de site fourni par la banque	O
PBX_SOURCE	Format de la page de paiement (pour paiement mobile)	F
PBX_TIME	Date et heure de la signature	O
PBX_TOTAL	Montant	O
PBX_TYPECARTE	Forçage du moyen de paiement	F
PBX_TYPEPAIEMENT	Forçage du moyen de paiement	F

Tableau 1 : Liste des variables Paybox System

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

11.1 Champs obligatoires pour Paybox System

11.1.1 PBX_SITE

Format : 7 chiffres. **Obligatoire.**

C'est le numéro de site (TPE) fourni par la banque du commerçant.

Exemple : 1999888

11.1.2 PBX_RANG

Format : 2 chiffres. **Obligatoire.**

C'est le numéro de rang (ou « machine ») fourni par la banque du Commerçant.

Exemple : 01





11.1.3 PBX_TOTAL

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

Format Direct : 10 chiffres. **Obligatoire.**

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

Exemple : pour 19€90 :

- 1990

11.1.4 PBX_DEVISE

Format : 3 chiffres. **Obligatoire.**

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

Exemples :

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

Attention : Avant d'effectuer un paiement en devises, assurez-vous que votre banque et que votre contrat l'autorisent.

Certains moyens de paiement ne supportent que l'euro. Dans ce cas, ils ne seront pas affichés sur la page de choix de moyen de paiement.

11.1.5 PBX_CMD

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

C'est la référence commande côté commerçant (champ libre). Ce champ permet au commerçant de garder un lien entre sa plate-forme de e-commerce et la plate-forme de paiement de Paybox. Ce champ doit être unique à chaque appel.

Dans le cas de l'utilisation de Paybox System version PLUS, la valeur contenue dans ce champ est aussi utilisée comme référence d'abonné, utilisable dans Paybox Direct Plus.

Exemple : CMD9542124-01A5G

11.1.6 PBX_PORTEUR

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

Adresse email de l'acheteur (porteur de carte).

Exemple : test@paybox.com





11.1.7 PBX_RETOUR

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


Variables renvoyées par Paybox.

Voir aussi : **§5 Gestion de la réponse**

Ci-dessous, la liste complète des variables disponibles

CODE	DESCRIPTION
M	M ontant de la transaction (précisé dans PBX_TOTAL).
R	R éférence commande (précisée dans PBX_CMD) : espace URL encodé
T	Numéro d'appel Paybox
A	numéro d' A utorisation (numéro remis par le centre d'autorisation) : URL encodé
B	numéro d' a Bonnement (numéro remis par Paybox)
C	Type de C arte retenu (cf. PBX_TYPECARTE)
D	D ate de fin de validité de la carte du porteur. Format : AAMM
E	Code réponse de la transaction (cf. <u>Tableau 3 : Codes réponse PBX_RETOUR</u>)
F	Etat de l'authenti F ication du porteur vis-à-vis du programme 3-D Secure : <ul style="list-style-type: none">• Y:Porteur authentifié• A:Authentification du porteur forcée par la banque de l'acheteur• U:L'authentification du porteur n'a pas pu s'effectuer• N:Porteur non authentifié
G	G arantie du paiement par le programme 3-D Secure. Format : O ou N
H	Empreinte de la carte
I	Code pays de l'adresse I P de l'internaute. Format : ISO 3166 (alphabétique)
J	2 derniers chiffres du numéro de carte du porteur
K	Signature sur les variables de l'URL. Format : url-encodé
N	6 premiers chiffres (« bi N 6 ») du numéro de carte de l'acheteur
O	Enr O lement du porteur au programme 3-D Secure : <ul style="list-style-type: none">• Y:Porteur enrôlé• N:Porteur non enrôlé• U:Information non connue
o	<i>Spécifique Cetelem</i> : Option de paiement sélectionnée par le client : <ul style="list-style-type: none">• 005 : Comptant• 001 : Crédit
P	Type de P aielement retenu (cf. PBX_TYPEPAIEMENT)
Q	Heure de traitement de la transaction. Format : HH:MM:SS (24h)
S	Numéro de Tran S action Paybox






U	<p>Gestion des abonnements avec le traitement Paybox Direct Plus.</p> <p><u>Pour les paiements par carte :</u></p> <p>Handle_Numéro_De_Carte_Crypté++Date_De_Validité_De_La_Carte+---</p> <p>Ce champ est URL-encodé. Vous devez conserver la valeur.</p> <p><u>Pour les paiements avec Paypal :</u></p> <p>Ce champ contient l'identifiant de l'autorisation fourni par Paypal. Il ne vous sera pas nécessaire pour les paiements suivants.</p>
W	Date de traitement de la transaction sur la plateforme Paybox. Format : JJMMAAAA
Y	Code paYs de la banque émettrice de la carte. Format : ISO 3166 (alphabétique)
Z	Index lors de l'utilisation des paiements mixtes (cartes cadeaux associées à un complément par carte CB/Visa/MasterCard/Amex)

Tableau 2 : Variables PBX_RETOUT

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue. Dans ce cas, il est souhaitable de faire une tentative sur le site secondaire : tpeweb1.paybox.com.
001xx	<p> Paiement refusé par le centre d'autorisation [voir \$12.1 Codes réponses du centre d'autorisation].</p> <p>En cas d'autorisation de la transaction par le centre d'autorisation de la banque ou de l'établissement financier privatif, le code erreur "00100" sera en fait remplacé directement par "00000".</p>
00003	Erreur Paybox. Dans ce cas, il est souhaitable de faire une tentative sur le site secondaire FQDN tpeweb1.paybox.com.
00004	Numéro de porteur ou cryptogramme visuel invalide.
00006	Accès refusé ou site/rang/identifiant incorrect.
00008	Date de fin de validité incorrecte.
00009	Erreur de création d'un abonnement.
00010	Devise inconnue.
00011	Montant incorrect.
00015	Paiement déjà effectué.
00016	Abonné déjà existant (inscription nouvel abonné). Valeur 'U' de la variable PBX_RETOUT.
00021	Carte non autorisée.
00029	Carte non conforme. Code erreur renvoyé lors de la documentation de la variable « PBX_EMPREINTE ».
00030	Temps d'attente > 15 mn par l'internaute/acheteur au niveau de la page de





	paiements.
00031	Réservé
00032	Réservé
00033	Code pays de l'adresse IP du navigateur de l'acheteur non autorisé.
00040	Opération sans authentification 3-DSecure, bloquée par le filtre.
99999	Opération en attente de validation par l'émetteur du moyen de paiement.

Tableau 3 : Codes réponse PBX_RETOUT

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

11.1.8 PBX_IDENTIFIANT

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

Identifiant Paybox fourni par Paybox au moment de l'inscription du commerçant.

Exemple : 200814357

11.1.9 PBX_HASH

Format : Texte. **Obligatoire.**

Valeur par défaut : SHA512

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

Cet algorithme doit être choisi parmi la liste suivante :

- SHA512
- RIPEMD160
- SHA224
- SHA256
- SHA384
- MDC2

Les hachages en MD2/4/5 sont jugés trop faibles pour être utilisés, nous ne les accepterons donc pas.

PBX_HASH doit être renseigné avec une des valeurs de cette liste, en respectant la casse (majuscules), et doit bien entendu correspondre au hachage utilisé pour le calcul du HMAC.

Si PBX_HASH n'est pas renseigné mais que dans les trames d'appel la variable PBX_HMAC est quand même renseignée (voir ci-dessous), l'algorithme de hachage sélectionné sera SHA512.

11.1.10 PBX_HMAC

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

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





Voir aussi :

- **§4.3 Authentification du message**,
- **§12.7 Glossaire**

11.1.11 PBX_TIME

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

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

11.2 Champs optionnels pour Paybox System

Les champs suivants sont triés par ordre alphabétique.

11.2.1 PBX_ARCHIVAGE

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

Référence transmise à la banque du commerçant au moment de la télécollecte. Elle devrait être unique et peut permettre à la banque du commerçant de lui fournir une information en cas de litige sur un paiement.

11.2.2 PBX_AUTOSEULE

Format : O ou N.

Valeur par défaut : N

Si la variable vaut « O », la transaction sera uniquement en mode autorisation, c'est-à-dire qu'elle ne sera pas envoyée à la banque du commerçant au moment de la télécollecte.

Cependant, elle sera quand même bien enregistrée, et il sera possible de la capturer ultérieurement en utilisant les produits Paybox Traitement Par Lot ou Paybox Direct.

11.2.3 PBX_ANNULE

Format : jusqu'à 150 caractères

Valeur par défaut : valeur enregistrée dans la fiche client du commerçant

Page de retour de Paybox vers le site Marchand après paiement annulé.

Les variables définies dans PBX_RETOUR seront envoyées à cette page

Exemple : <http://www.commerce.fr/annulation.html>

Voir aussi : **§5 Gestion de la réponse**





11.2.4 PBX_ATTENTE

Format : jusqu'à 150 caractères

Valeur par défaut : valeur enregistrée dans la fiche client du commerçant

Page de retour de Paybox vers le site Marchand après paiement en attente de validation par l'émetteur.

Les variables définies dans PBX_RETOUR seront envoyées à cette page

Exemple : <http://www.commerce.fr/attente.html>

Voir aussi :

- **§5 Gestion de la réponse**

11.2.5 PBX_CURRENCYDISPLAY

Format : jusqu'à 23 caractères (6 x 3 codes séparés par des virgules)

Valeur par défaut : toutes les devises sont affichées

Liste des codes monnaie à afficher au niveau de la page de paiements.

Les codes disponibles sont les suivants :

- EUR : Euro
- CHF : Franc suisse
- USD : Dollar US
- JPY : Yen
- CNY : Yuan
- GBP : Livre Sterling
- CAD : Dollar canadien
- NO_CURR : valeur spéciale pour n'afficher aucune devise

Exemple : EUR, USD, GBP

11.2.6 PBX_DATEVALMAX

Format : Date au format AAMM

Date d'expiration à ne pas dépasser.

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

Exemple :

Echéancier 04/05/2013, 08/06/2013 et 30/07/2013

PBX_DATEVALMAX=1307

Si la carte expire avant la fin juillet 2013, le paiement initial sera refusé avec le code erreur 00008.





11.2.7 PBX_DATE1, PBX_DATE2, PBX_DATE3

Format : Date au format JJ/MM/AAAA

Date de la seconde échéance d'un paiement fractionné (respectivement troisième et quatrième échéances pour PBX_DATE2 et PBX_DATE3).

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

Exemple : 30/06/2012

Voir aussi :

- **§7.3 Paiement en plusieurs fois (4 fois max)**
- **§11.2.24 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3**

11.2.8 PBX_DIFF

Format : 2 chiffres

Nombre de jours de différé (entre la transaction et sa capture).

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

Une valeur par défaut de ce paramètre peut avoir été définie dans la fiche d'inscription. Si ce paramètre est envoyé dans l'appel, la valeur spécifiée dans l'appel est prioritaire sur celle par défaut.

Exemple : 04 pour gérer un différé de 4 jours

Voir aussi :

- **§6.3 Paiement différé.**

11.2.9 PBX_DISPLAY

Format : 3 à 10 chiffres

Valeur par défaut : 900

TimeOut de la page de paiement (en secondes). Une fois cette période dépassée, la transaction est comptée comme annulée.

11.2.10 PBX_EFFECTUE

Format : jusqu'à 150 caractères

Valeur par défaut : valeur enregistrée dans votre fiche client

Page de retour de Paybox vers votre site après paiement accepté.
Les variables définies dans PBX_RETOUTOUR seront envoyées à cette page.

Exemple : <http://www.commerce.fr/confirmation.html>

Voir aussi : **§5 Gestion de la réponse**





11.2.11 PBX_EMPREINTE

Format : 64 caractères

Empreinte fournie par Paybox au moment d'un premier paiement via la variable « H » de « PBX_RETOUR ».

11.2.12 PBX_ENTITE

Format : 1 à 9 chiffres

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

11.2.13 PBX_ERRORCODETEST

Format : 5 chiffres

Code erreur à retourner lors de l'intégration dans l'environnement de pré-production. Variable non prise en compte dans l'environnement de production.

Voir aussi :

§11.1.7 Tableau 3 : Codes réponse PBX_RETOUR

11.2.14 PBX_GROUPE

Format : jusqu'à 10 chiffres

Variable obligatoire pour l'utilisation de Paybox Version ++.

Définit le groupe de commerçants qui pourront réutiliser la même référence abonné pour débiter un même client.

11.2.15 PBX_IDABT

Format : 9 chiffres

Numéro d'abonnement renvoyé via la variable 'B' de PBX_RETOUR.

La documentation de cette variable permet de mettre à jour le numéro de carte associé à un abonnement. L'abonnement avait été initialement créé via le produit Paybox System.

Voir aussi :

- ***§7 Option Gestion des Abonnements***





11.2.16 PBX_LANGUE

Format : 3 caractères

Valeur par défaut : FRA

Langue utilisée par Paybox pour l'affichage de la page de paiement.

Valeurs possibles :

- FRA : Français
- GBR : Anglais
- ESP : Espagnol
- ITA : Italien
- DEU : Allemand
- NLD : Hollandais
- SWE : Suédois
- PRT : Portugais

11.2.17 PBX_REFABONNE

Format : jusqu'à 250 caractères

Référence abonné affectée par le commerçant via le produit Paybox Direct Plus ou Paybox System version PLUS.

La documentation de cette variable permet de mettre à jour le numéro de carte associé à un abonné ou profil s'il existe déjà, ou de le créer s'il n'existe pas.

Voir aussi :

- **§6.1 Intégration avec Paybox Direct Plus***Intégration* avec

11.2.18 PBX_REFUSE

Format : jusqu'à 150 caractères

Valeur par défaut : valeur enregistrée dans votre fiche client

Page de retour de Paybox vers le site Marchand après paiement refusé.

Les variables définies dans PBX_RETOUR seront envoyées à cette page.

Exemple : <http://www.commerce.fr/refus.html>

Voir aussi :

- **§5 Gestion de la réponse**

11.2.19 PBX_REPONDRE_A

Format : jusqu'à 150 caractères

Valeur par défaut : valeur enregistrée par Paybox à l'inscription dans la fiche client du commerçant

URL d'appel serveur à serveur après chaque tentative de paiement. Aussi appelée « IPN », cette URL est appelée séparément du navigateur du client, et permet donc de valider les commandes de manière sûre.





Les variables définies dans PBX_RETOUR seront envoyées à cette URL.

Exemple : http://www.commerce.fr/validation_paiement.cgi

Voir aussi :

- **§5 Gestion de la réponse**

11.2.20 PBX_RUF1

Format : « GET » ou « POST »

Valeur par défaut : GET

Méthode (au sens HTTP) utilisée pour l'appel de l' « IPN »

Voir aussi :

- **§5 Gestion de la réponse**
- **§11.2.19 PBX_REPONDRE_A**

11.2.21 PBX_SOURCE

Format : 3 à 5 caractères.

Valeur par défaut : HTML

Définit le format de la page du choix du moyen de paiement. Cette variable est à modifier en fonction du type de navigateur. Les valeurs possibles sont les suivantes :

- HTML : adaptée aux ordinateurs fixes
- WAP : format WML, pour téléphones compatibles WAP
- IMODE : format iHTML
- XHTML : page allégée, adaptée aux terminaux mobiles (type smartphones/ tablettes)

Remarque : Paybox ne fait pas de détection automatique du navigateur.

11.2.22 PBX_TYPEPAIEMENT

Format : 5 à 10 caractères.

Valeur par défaut : <vide>

Privilégie un type de carte.

- Sur la page de présélection : permet de n'afficher que les moyens de paiement choisis
 - Si le commerçant dispose de l'option Paypal par exemple mais qu'il souhaite limiter un achat aux paiements par carte, il faut documenter cette variable à « CARTE ».
 - Ainsi, seules les options de type carte dont le commerçant dispose seront affichées sur la page de présélection.
- Sur la page de paiement : utilisée avec PBX_TYPECARTE, permet de ne pas afficher la page de présélection, et d'afficher la page de paiement adaptée directement.

Les valeurs possibles sont présentées dans le **Tableau 4 : Valeurs possibles PBX_TYPEPAIEMENT et PBX_TYPECARTE**

Voir aussi :

§11.2.23 PBX_TYPECARTE





11.2.23 PBX_TYPECARTE

Format : min. 2 caractères.

Valeur par défaut : <vide>

Définit le type de carte à utiliser sur la page de paiement, dans le cas où la page de présélection du moyen de paiement fournie par Paybox n'est pas utilisée.

S'utilise toujours conjointement à PBX_TYPEPAIEMENT.

PBX_TYPEPAIEMENT	PBX_TYPECARTE
CARTE	CB, VISA, EUROCARD_MASTERCARD, E_CARD
	MAESTRO
	AMEX
	DINERS
	JCB
	COFINOGA
	SOFINCO
	AURORE
	CDGP
	24H00
	RIVEGAUCHE
PAYPAL	PAYPAL
CREDIT	UNEURO
	34ONEY
NETRESERVE	NETCDGP
PREPAYEE	SVS
	KADEOS
	PSC
	CSHTKT
	LASER
	EMONEO
	IDEAL
	ONEYKDO
	ILLICADO
	WEXPAY
	MAXICHEQUE
FINAREF	SURCOUF
	KANGOUROU
	FNAC
	CYRILLUS
	PRINTEMPS
	CONFORAMA
BUYSTER	BUYSTER
LEETCHI	LEETCHI
PAYBUTTONS	PAYBUTTING

Tableau 4 : Valeurs possibles PBX_TYPEPAIEMENT et PBX_TYPECARTE





11.2.24 PBX_2MONT1, PBX_2MONT2, PBX_2MONT3

Format : 3 à 10 chiffres

Montant en centimes (donc sans virgule ni point) des échéances suivantes d'un paiement fractionné. L'option gestion des abonnements doit être activée.

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

Voir aussi :

- **§7.3 Paiement en plusieurs fois (4 fois max)**
- **§11.2.7 PBX_DATE1, PBX_DATE2, PBX_DATE3**

11.2.25 PBX_3DS

Format : 'N' : Pas d'authentification 3-D Secure du porteur

Permet de ne pas effectuer une authentification 3-D Secure du porteur, uniquement pour cette transaction, même si le commerçant est enrôlé au programme 3-D Secure.

Ne pas renseigner cette variable lorsque l'authentification 3-D Secure est demandée.

Voir aussi :

- Une définition du 3D Secure en **§11.7.1 3-D Secure**

11.3 Variables spécifiques à certains moyens de paiement

11.3.1 PBX_1EURO_CODEEXTERNE

Format : 3 chiffres. Uniquement pour la solution de paiement « 1Euro.com ».

Offre promotionnelle externe

11.3.2 PBX_1EURO_DATA

Format : jusqu'à 100 caractères. Uniquement pour la solution de paiement « 1Euro.com ».
Données d'identification et de localisation du client.

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

- ✓ Civilité,
- ✓ Nom,
- ✓ Prénom,
- ✓ Adresse1,
- ✓ Adresse2,
- ✓ Adresse3,
- ✓ Code postal,
- ✓ Ville,
- ✓ Code pays (FR pour France par exemple),





- ✓ Téléphone fixe,
- ✓ Téléphone portable,
- ✓ Flag indiquant si l'internaute est connu du commerçant (0 :Non connu, 1 :Connu),
- ✓ Flag indiquant si le commerçant a déjà eu des incidents de paiements avec cet internaute,
- ✓ Code action COFIDIS (valeur figée et fournie par COFIDIS)

Exemple :

M#DUPONT#Jean#Rue Lecourbe#BatimentA##75010#PARIS#FR#0102030405##0#0#12#

11.3.3 PBX_CK_ONLY

Format : O ou N. Uniquement pour les cartes cadeau

La valeur « O » permet de forcer le paiement avec des cartes cadeau seulement.
Sinon, le client peut aussi utiliser sa carte ou un autre moyen de paiement pour compléter son paiement.

11.3.4 PBX_CODEFAMILLE

Format : 3 chiffres. Uniquement pour les applications SOFINCO, COFINOGA et CDGP.

Valeur renseignée par le commerçant pour indiquer l'option de paiement qu'il propose au porteur de la carte SOFINCO (ou carte partenaire SOFINCO), COFINOGA ou CDGP.

11.3.5 PBX_MAXICHEQUE_DATA

Format : jusqu'à 255 caractères alphanumériques. Uniquement pour l'application MAXICHEQUE.

Décrit la famille du produit acheté. Voir documentation Maxichèque pour plus de détails.

11.3.6 PBX_NBCARTESKDO

Format : jusqu'à 2 chiffres. Uniquement pour les cartes cadeau.

Permet de limiter le nombre de cartes Cadeau utilisables par un porteur.
Les valeurs autorisées sont entre 1 et 25.

11.3.7 PBX_NETRESERVE_DATA

Format : jusqu'à 250 caractères. Uniquement pour l'application Net Reserve.

Données d'identification et de localisation du client.

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

1. Prénom (25 caractères),
2. Nom (25 caractères),
3. Adresse1 (25 caractères),





4. Adresse2 (25 caractères),
5. Code postal (10 caractères),
6. Ville (25 caractères),
7. Code pays (2 caractères : FR pour France par exemple),
8. Email (50 caractères),
9. Téléphone (25 caractères)

Exemple :

11.3.8 Jean#DUPONT#Rue
Lecourbe##75010#PARIS#FR#jean.dupont@gmail.com#0102030405#

11.3.9 PBX_OPECOM

Format : 5 chiffres. Uniquement pour les paiements FINAREF avec la carte SURCOUF

Format : 10 caractères. Uniquement pour la solution Facilipay d'Oney Banque Accord.

Opération commerciale.

11.3.10 PBX_ONEY_DATA

Format : XML. Uniquement pour la solution Facilipay d'Oney Banque Accord.

Pour plus d'informations sur l'intégration de moyen de paiement, référez-vous au document **[Ref 10]**
Note Oney.

11.3.11 PBX_PAYPAL_DATA

Format : jusqu'à 490 caractères. Uniquement pour l'application PAYPAL

Uniquement pour les paiements via Paypal : données d'identification de localisation du client.

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

- ✓ Nom du client (32 caractères),
- ✓ 1ère ligne d'adresse (100 caractères),
- ✓ 2ème ligne d'adresse (100 caractères) ,
- ✓ Ville (40 caractères),
- ✓ Etat / Région (40 caractères),
- ✓ Code postal (20 caractères),
- ✓ Code pays (FR pour France) (2 caractères),
- ✓ Numéro de téléphone (20 caractères)
- ✓ Description du paiement (127 caractères)

Cette variable est obligatoire dans le cas d'un paiement avec création d'abonné (Paybox System version PLUS), conseillée dans les autres cas.

Exemple :

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





11.4 Paybox System Résiliation des Abonnements : Requête

11.4.1 VERSION

Format : 3 chiffres. **Obligatoire.**

Valeur par défaut : 001

Version de protocole : 001

11.4.2 TYPE

Format : 3 chiffres. **Obligatoire.**

Valeur par défaut : 001

Type de demande : 001 = Résiliation

11.4.3 SITE

Format : 7 chiffres. **Obligatoire.**

Numéro de site.

Fourni par Paybox lors de l'inscription.

11.4.4 MACH

Format : 3 chiffres. **Obligatoire.**

Numéro de rang.

Fourni par Paybox lors de l'inscription.

11.4.5 IDENTIFIANT

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

Identifiant du commerçant pour Paybox.

Fourni par Paybox lors de l'inscription.

11.4.6 HMAC

Format : Texte. **Obligatoire.**

Permet l'authentification du commerçant et la vérification de l'intégrité du message. Son calcul se fait de la même manière que pour l'appel Paybox System.

Voir aussi :

- **§4.3 Authentification du message,**

11.4.7 TIME

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

Date de calcul de l'empreinte HMAC.





11.4.8 ABONNEMENT

Format : 1 à 9 chiffres. **Obligatoire si pas de référence de commande précisée.**

Numéro d'abonnement à résilier.

11.4.9 REFERENCE

Format : 1 à 250 caractères. **Obligatoire si pas de numéro d'abonnement précisé.**

Référence commande de l'abonnement à préciser.

11.5 Paybox System Résiliation des Abonnements : Réponse

La réponse est fournie par l'intermédiaire de trois variables indiquant si la résiliation a réussi ou non, le motif de refus et un rappel sur l'abonnement.

11.5.1 ACQ

Format : 2 caractères. **Obligatoire.**

OK : Succès

NO : Echec

11.5.2 ERREUR

Format : 1 chiffre. **Obligatoire en cas d'échec.**

Numéro de l'erreur en cas d'échec :

- 1 : Incident technique (Configuration),
- 2 : Données non cohérentes,
- 3 : Incident technique (Accès à la base de données),
- 4 : Site inconnu,
- 9 : Echec de la résiliation. Aucun abonnement résilié

11.5.3 IDENTIFIANT

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

Valeur transmise dans la requête initiale.

11.5.4 ABONNEMENT

Format : 1 à 9 chiffres. **Obligatoire si pas de référence de commande précisée.**

Valeur transmise dans la requête initiale.

11.5.5 REFERENCE

Format : 1 à 250 caractères. **Obligatoire si pas de numéro d'abonnement précisé.**

Valeur transmise dans la requête initiale.





12. ANNEXES

12.1 Codes réponses du centre d'autorisation

Cette information est transmise dans les informations de retour en fin de transaction si la variable E a été spécifiée à l'appel.

Voir **§11.1.7 PBX RETOUR** et **§5 Gestion de la réponse**

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

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès
01	Contactez l'émetteur de carte
02	Contactez l'émetteur de carte
03	Commerçant invalide
04	Conservez la carte
05	Ne pas honorer
07	Conservez la carte, conditions spéciales
08	Approuver après identification du porteur
12	Transaction invalide
13	Montant invalide
14	Numéro de porteur invalide
15	Émetteur de carte inconnu
17	Annulation client
19	Répéter la transaction ultérieurement
20	Réponse erronée (erreur dans le domaine serveur)
24	Mise à jour de fichier non supportée
25	Impossible de localiser l'enregistrement dans le fichier
26	Enregistrement dupliqué, ancien enregistrement remplacé
27	Erreur en « edit » sur champ de mise à jour fichier
28	Accès interdit au fichier
29	Mise à jour de fichier impossible
30	Erreur de format
33	Carte expirée
38	Nombre d'essais code confidentiel dépassé





41	Carte perdue
43	Carte volée
51	Provision insuffisante ou crédit dépassé
54	Date de validité de la carte dépassée
55	Code confidentiel erroné
56	Carte absente du fichier
57	Transaction non permise à ce porteur
58	Transaction interdite au terminal
59	Suspicion de fraude
60	L'accepteur de carte doit contacter l'acquéreur
61	Dépasse la limite du montant de retrait
63	Règles de sécurité non respectées
68	Réponse non parvenue ou reçue trop tard
75	Nombre d'essais code confidentiel dépassé
76	Porteur déjà en opposition, ancien enregistrement conservé
89	Echec de l'authentification
90	Arrêt momentané du système
91	Emetteur de cartes inaccessible
94	Demande dupliquée
96	Mauvais fonctionnement du système
97	Echéance de la temporisation de surveillance globale

Tableau 5 : Codes réponses du centre d'auto CB

12.1.2 Réseau Cetelem/Aurore et Rive Gauche

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès.
01	Numéro de commerçant incorrect ou inconnu
02	Numéro de carte incorrect
03	Date de naissance ou code secret erronés
04	Carte non finançable
05	Problème centre serveur CETELEM
06	Carte inconnue
07	Demande de réserve refusée
08	Carte périmée






09	Incompatibilité carte/commerçant
10	Inconnu
11	Annulé
12	Code devise incorrect
13	Référence de l'opération non renseignée
14	Montant de l'opération incorrect
15	Modalité de paiement incorrect
16	Sens de l'opération incorrect
17	Mode de règlement incorrect

Tableau 6 : Codes réponses du centre d'auto Cetelem

12.1.3 Réseau Finaref

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
000	OK
101	Carte expirée. Porteur en validité dépassée
103	Commerçant inconnu. Identifiant de commerçant incorrect
110	Montant incorrect
111	Compte/porteur inconnu
115	Service non ouvert. Plafond nul. Code fonction/traitement inconnu
116	Provision insuffisante
117	1er ou 2ème code faux
119	Compte/Porteur avec statut bloqué. Compte/Porteur avec statut invalide. Carte bloquée
120	Commerçant invalide. Code monnaie incorrect. Compte non autorisé. Opération Commerciale inconnue/invalide
121	Plafond insuffisant
125	Carte non active
126	Code secret absent. Erreur de format de la date de début de contrôle ou des infos de sécurité
128	Erreur de contrôle de l'historique des codes faux
129	CVV2 faux
183	Compte / porteur invalide
184	Incohérence de date de validité avec fichier Porteurs en saisie manuelle
188	Mode de saisie invalide. Identification matériel incohérente
196	Problème d'accès fichiers
206	3ème code secret faux. Compteur de codes faux déjà à 3





207	Porteur en opposition (alors que statut carte=3)
208	Carte non parvenue. Carte volée. Usage abusif. Suspicion de fraude, Carte perdue
210	Incohérence de date de validité avec fichier porteurs en lecture piste ou puce. CVV faux
380	OK avec dépassement
381	OK avec augmentation capital
382	OK NPAI
385	Autorisation partielle

Tableau 7 : Codes réponses du centre d'auto Finaref

12.1.4 Buyster

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
12	Paramètre invalide
17	Annulation du porteur
24	Opération impossible
25	Transaction inconnue
3	Destinataire du paiement inconnu
30	Paramètre obligatoire non rempli
34	Suspicion de fraude
40	Vous ne possédez pas les droits pour l'opération demandée
5	Transaction refusée
63	Paramètres d'authentification marchande invalides
75	Nombre d'identifications porteur dépassé (3 tentatives)
94	Référence transaction déjà utilisée
99	Problème technique au niveau du serveur Buyster

Tableau 8 : Codes réponses du centre d'auto Buyster

12.2 Codes retour HTTP

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

CODE	DESCRIPTION
1xx	Information – Requête reçue, traitement en cours
2xx	La demande a été reçue avec succès reçue, comprise et acceptée
3xx	Redirection





4xx	Erreur de Client - La demande contient une mauvaise syntaxe ou ne peut pas être accomplie
5xx	Erreur de serveur - Le serveur a échoué à accomplir une demande apparemment valable

Tableau 9 : Codes retour HTTP

Pour plus de détails et la liste complète des codes retour, se référer à la norme du protocole HTTP1.1, nommée [RFC2616](#).

12.3 Codes erreur CURL

CODE	DESCRIPTION
1	Protocole non supporté
2	Echec durant la phase d'initialisation
3	URL mal formatée
4	URL mal formatée
5	Résolution du proxy impossible
6	Résolution du host impossible
7	Connexion impossible avec le host
22	(HTTP) Page non atteinte
34	(HTTP) Méthode post en erreur
35	Connexion SSL en erreur
42	Callback annulée
43	Erreur interne
44	Erreur interne
45	Erreur d'interface
47	Trop de redirections
51	Certificat SSL distant incorrect
52	Le serveur ne répond à rien
53	Moteur de cryptographie SSL non trouvé
54	Problème d'initialisation du moteur de cryptographie SSL
55	Envoi de données en erreur
56	Réception de données en erreur
57	Erreur interne
58	Problème avec le certificat local
59	Impossible d'utiliser le chiffrement SSL indiqué

Tableau 10 : Codes erreur CURL





12.4 Jeu de caractères Paybox

Le jeu de caractères supporté par les applications de Paybox est présenté dans le tableau ci-dessous. Tous les autres caractères autres que ceux présents dans le tableau ci-dessous seront, suivant les applications, supprimés ou la trame rejetée :

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

12.5 Caractères URL Encodés

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

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



12.6 URL d'appel et Adresses IP



Les URLs d'appel pour effectuer des transactions en **Paybox System classique** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.paybox.com/cgi/MYchoix_pagepaiement.cgi
Principale	https://tpeweb.paybox.com/cgi/MYchoix_pagepaiement.cgi
Secours	https://tpeweb1.paybox.com/cgi/MYchoix_pagepaiement.cgi

Les URLs d'appel pour effectuer des transactions en **Paybox System version Light (iFrame)** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.paybox.com/cgi/MYframepagepaiement_ip.cgi
Principale	https://tpeweb.paybox.com/cgi/MYframepagepaiement_ip.cgi
Secours	https://tpeweb1.paybox.com/cgi/MYframepagepaiement_ip.cgi

Les URLs d'appel pour effectuer des transactions en **Paybox System version Mobile** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.paybox.com/cgi/ChoixPaiementMobile.cgi
Principale	https://tpeweb.paybox.com/cgi/ChoixPaiementMobile.cgi
Secours	https://tpeweb1.paybox.com/cgi/ChoixPaiementMobile.cgi

Les URLs d'appel pour effectuer des **Résiliation des abonnements** :

PLATE-FORME	URL D'ACCÈS
Pré-production	https://preprod-tpeweb.paybox.com/cgi-bin/ResAbon.cgi
Principale	https://tpeweb.paybox.com/cgi-bin/ResAbon.cgi
Secours	https://tpeweb1.paybox.com/cgi-bin/ResAbon.cgi

L'**adresse IP entrante** est l'adresse sur laquelle le site Marchand va se connecter pour réaliser la transaction.

L'**adresse IP sortante** est l'adresse avec laquelle le site Marchand verra 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 les infrastructures hébergeant les sites marchands.

PLATE-FORME	ADRESSE ENTRANTE	ADRESSE SORTANTE
Pré-production	195.101.99.73	195.101.99.76
Principale	194.2.160.66	194.2.122.158
Secours	195.25.7.146	195.25.7.166





12.7 Glossaire

12.7.1 3-D Secure

Le protocole 3-D SECURE a été mis en place par VISA et MASTERCARD pour répondre à la problématique de répudiation.

Si le titulaire d'une carte bancaire conteste un achat réalisé sur Internet, le marchand qui utilise le service 3-D Secure a alors les moyens de prouver que le porteur de la carte est bien l'acheteur.

Le protocole 3-D Secure se concrétise par une phase d'authentification du porteur de la carte avant le paiement, en cas d'échec de l'authentification du porteur le paiement n'est pas effectué.

La banque émettrice de la carte met au point un moyen d'authentification du porteur et se rend responsable en cas d'impayé.

On parle de **transfert de responsabilité** de la banque du commerçant vers la banque du porteur de la carte.

Il est important pour le commerçant de vérifier avant l'activation du service 3-D Secure que le contrat qu'il détient auprès de sa banque est bien de type VADS (Vente A Distance Sécurisée), un simple contrat de type VAD ne permet aucun recours en cas d'impayé.

Paybox est une plate-forme technique entre le commerçant et la banque auprès de laquelle il a souscrit un contrat.

La demande d'activation du service 3-D Secure peut émaner aussi bien du commerçant que de sa banque qui en cas de fraude avérée peut exiger la mise en place du service.

Paybox est alors tenu d'activer le service et d'en avertir la banque et le commerçant.

Une fois le service 3-D Secure activé, tous les paiements ne bénéficient pas forcément du transfert de responsabilité.

Le Back-Office commerçant permet une visualisation de l'état des paiements 3-D Secure dans la colonne **Garantie** de l'onglet journal.

Un détail décrivant le résultat de l'authentification du porteur est également présent sous la mention **Statut Porteur 3-D Secure**.

Le protocole 3-D Secure se décompose en 2 temps :

1 – Paybox vérifie si la carte du porteur fait partie du programme 3-D Secure auprès de VISA ou Mastercard, on dit alors que le porteur est **inscrit** au programme 3-D Secure.

2 – Paybox redirige l'internaute sur la page d'authentification de la banque émettrice de la carte, sur laquelle il doit saisir un code personnel pour s'authentifier.

Les règles dictées par VISA et Mastercard concernant le **transfert de responsabilité** (ou bien **Garantie**) sont basées sur le résultat de ces échanges.

Paybox restitue systématiquement pour chaque paiement le résultat de ces échanges.

Pour plus d'informations, consultez notre fiche d'information **[Ref 4] « Fiche présentation 3D Secure »**.





12.7.2 Encodage URL (url-encodé)

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

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

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

12.7.3 FTP

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

12.7.4 HMAC

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

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

12.7.5 HTTP

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

12.7.6 IP (adresse IP)

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

12.7.7 SSL

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

12.7.8 URL

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

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

